Guia de Soluções do Arcserve® Unified Data Protection

Versão 8.x

arcserve®

Ajuda online de soluções do Arcserve® Unified Data Protection

Versão 8.x

A lista de conteúdo é exibida no painel à esquerda. Para exibir todos os tópicos, clique no ícone TOC disponível na parte superior.

arcserve®

Aviso legal

A presente Documentação, que inclui os sistemas de ajuda incorporados e os materiais distribuídos eletronicamente (doravante denominada Documentação), destina-se apenas a fins informativos e está sujeita a alterações ou revogação por parte da Arcserve a qualquer momento. Esta Documentação contém informações confidenciais da Arcserve e não pode ser copiada, transferida, reproduzida, divulgada, modificada nem duplicada, no todo ou em parte, sem o prévio consentimento por escrito da Arcserve.

Se o Cliente for um usuário licenciado do(s) produto(s) de software constante(s) na Documentação, é permitido que ele imprima ou, de outro modo, disponibilize uma quantidade razoável de cópias da Documentação para uso interno seu e de seus funcionários referente ao software em questão, contanto que todos os avisos de direitos autorais e legendas da Arcserve estejam presentes em cada cópia reproduzida.

O direito à impressão ou disponibilizar cópias da documentação está limitado ao período de vigência no qual a licença aplicável a tal software permanece em pleno vigor e efeito. Em caso de término da licença, por qualquer motivo, fica o usuário responsável por garantir à Arcserve, por escrito, que todas as cópias, parciais ou integrais, da Documentação sejam devolvidas à Arcserve ou destruídas.

ATÉ O LIMITE PERMITIDO PELA LEI APLICÁVEL, A ARCSERVE FORNECE ESTA DOCUMENTAÇÃO “NO ESTADO EM QUE SE ENCONTRA”, SEM NENHUM TIPO DE GARANTIA, INCLUINDO, ENTRE OUTRAS, QUAISQUER GARANTIAS IMPLÍCITAS DE COMERCIABILIDADE, ADEQUAÇÃO A UM DETERMINADO FIM OU NÃO VIOLAÇÃO. EM NENHUMA OCASIÃO, A ARCSERVE SERÁ RESPONSÁVEL PERANTE O USUÁRIO OU TERCEIROS POR QUAISQUER PERDAS OU DANOS, DIRETOS OU INDIRETOS, RESULTANTES DO USO DA DOCUMENTAÇÃO, INCLUINDO, ENTRE OUTROS, LUCROS CESSANTES, PERDA DE INVESTIMENTO, INTERRUPÇÃO DOS NEGÓCIOS, FUNDO DE COMÉRCIO OU PERDA DE DADOS, MESMO QUE A ARCSERVE TENHA SIDO EXPRESSAMENTE ADVERTIDA SOBRE A POSSIBILIDADE DE TAIS PERDAS E DANOS.

O uso de qualquer produto de software mencionado na documentação é regido pelo contrato de licença aplicável, sendo que tal contrato de licença não é modificado de nenhum modo pelos termos deste aviso.

O fabricante desta Documentação é a Arcserve.

Fornecido nos termos de "Direitos restritos". O uso, a duplicação ou a divulgação pelo Governo dos Estados Unidos estão sujeitos às restrições definidas nas seções 12.212, 52.227-14 e 52.227-19(c)(1) – (2) da FAR e na seção 252.227-7014(b)(3) da DFARS, conforme aplicável, ou suas sucessoras.

© 2014-2021 Arcserve, incluindo suas afiliadas e subsidiárias. Todos os direitos reservados. Quaisquer marcas comerciais ou direitos autorais de terceiros pertencem a seus respectivos proprietários.

Referências de produtos da Arcserve

Este documento faz referência aos seguintes produtos da Arcserve:

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

Contato Suporte da Arcserve

A equipe do Suporte da Arcserve oferece uma ampla gama de recursos para solucionar seus problemas técnicos e fornece acesso fácil a informações importantes sobre o produto.

Entrar em contato com o suporte

Com o Suporte da Arcserve:

- É possível ter contato direto com a mesma biblioteca de informações compartilhada internamente por nossos especialistas do Suporte da Arcserve. Este site fornece acesso aos documentos de nossa base de conhecimento. A partir daqui, é fácil pesquisar e localizar os artigos da base de conhecimento relacionados ao produto que contêm soluções testadas em campo para muitos dos problemas principais e comuns.
- Você pode usar nosso link para o Bate-papo ao vivo para iniciar instantaneamente uma conversa em tempo real entre você e a equipe do Suporte da Arcserve. Com o Bate-papo ao vivo, você poderá obter respostas imediatas para suas dúvidas e preocupações, sem deixar de manter o acesso ao produto.
- É possível participar da Comunidade global de usuários da Arcserve para fazer perguntas e responder a perguntas de outros usuários, compartilhar dicas e truques, discutir práticas recomendadas e iniciar conversas com colegas.
- É possível abrir um ticket de suporte. Ao abrir um ticket de suporte online, é possível esperar um retorno de chamada de um de nossos especialistas na área do produto sobre o qual está perguntando.
- Você pode acessar outros recursos úteis adequados ao seu produto da Arcserve.

Conteúdo

Ajuda online de soluções do Arcserve® Unified Data Protection 2

Capítulo 1: Recursos e aprimoramentos 29

Novos recursos 30

Aprimoramentos de recursos 32

Aprimoramentos do agente do Linux 33

Suporte à plataforma e ao banco de dados 34

Aprimoramentos de terceiros e de segurança 35

Aprimoramentos do appliance do Arcserve 36

Suporte interrompido 37

Capítulo 2: Entendendo o Arcserve UDP 39

Introdução 40

Como o Arcserve UDP funciona 42

IVM (Instant Virtual Machine - Máquina Virtual Instantânea) versus VSB (Virtual Standby Machine - Máquina Virtual no Modo de Espera) 44

Segurança do usuário 47

Funções dos serviços do Arcserve UDP 48

Privilégios de usuário das funções do Arcserve UDP 50

Capítulo 3: Instalando o Arcserve UDP 61

Como instalar o Arcserve UDP 62

Verificar os pré-requisitos e as considerações 63

Decidir o tipo de instalação 64

Instalar o Arcserve Unified Data Protection usando o assistente de instalação 65

Instalar o Arcserve Unified Data Protection usando a linha de comando 69

Instalar o Arcserve UDP usando o programa de instalação unificado 74

Verificar a instalação 76

Portas de comunicação usadas pelo Arcserve UDP 77

Como o processo de instalação afeta os sistemas operacionais 97

Como instalar atualizações do Arcserve UDP 103

Analisar as considerações para a instalação de atualizações 104

Especificar as preferências de atualizações 105

Verificar e instalar as atualizações 111

Atualizar agentes em nós remotos usando um gateway 112

Atualizar o RPS no servidor remoto usando o gateway 113

(Opcional) Instalar atualizações do Arcserve UDP no modo silencioso 114

Verifique se as atualizações foram instaladas com êxito 115
Como desinstalar o Arcserve UDP 116
Desinstalação padrão 117
Desinstalação silenciosa 118
Remover componentes ignorados pelo programa de desinstalação 120
Capítulo 4: Atualizar para o Arcserve UDP versão 8.0 123
Versões com suporte para atualização 124
Sequência de atualização do Arcserve Appliance 125
Atualizar o appliance do Arcserve que é executado como console e RPS do Arcserve UDP 126
Atualizar o appliance do Arcserve que é executado somente como RPS do Arcserve UDP 127
Atualizar etapas quando dois ou mais appliances do Arcserve são usados no ambiente 128
Atualizar o agente do Arcserve para Linux no appliance do Arcserve UDP 129
Atualizar o Arcserve Backup no appliance do Arcserve 130
Diretiva suporte à compatibilidade com versões anteriores 131
Diretiva de suporte à compatibilidade com versões anteriores do Arcserve UDP 8.0 131
Diretiva de suporte à compatibilidade com versões anteriores para o Arcserve UDP versão 7.x 134
Diretiva de suporte à compatibilidade com versões anteriores para Arcserve UDP versão 6.5, Atualização 4 137
Suporte à compatibilidade com versões anteriores para o servidor de backup Linux 140
Sequência de atualização para o console do UDP, o RPS e o agente 141
Como atualizar para o Arcserve UDP 8.0 de uma release anterior 142
Como atualizar para o Arcserve UDP 8.0 usando o único programa de instalação 145
Como atualizar para o Arcserve UDP 8.0 ou Arcserve Backup 18.0 para ativar a cópia em fita 149
Como migrar o console do Arcserve UDP de um servidor para outro 152
Como fazer atualização de gateway para a mesma versão de seu Console registrado 153
Como executar a migração do console do Arcserve UDP 153
Capítulo 5: Explorar e configurar o Arcserve UDP 157
Efetuar logon no console do Arcserve UDP usando a autenticação multifator 157
Verificar os pré-requisitos 157
Como efetuar logon no console do Arcserve UDP usando MFA 158
Arcserve Unified Data Protection Interface do usuário 163
Navegando no Arcserve UDP 164
Guias 166
Caixa de diálogo Monitor de tarefas 181

Como configurar o Arcserve UDP 182
Configurar o protocolo de comunicação do servidor 183
Configurar banco de dados 185
Configurar a sincronização de dados de backup do Arcserve 189
Configurar o SRM 191
Configuração de detecção de nó 193
Configurar emails e alertas 195
Definir configurações de proxy 197
Atualizar a configuração 199
Configurar a conta de administrador 201
Configurações da implantação remota 202
Mapear o plano para a conta de usuário 203
Gerenciamento do usuário 205
Configurar a duração do tempo limite do console 206
Como migrar pontos de recuperação do Arcserve r16.5 para Arcserve UDP 207
Criar um repositório de dados para replicar os dados de um ponto de recuperação do Arcserve r16.5 208
Replicar os dados do Arcserve r16.5 para o repositório de dados do UDP 209
Configurar o assistente de configuração 210
Capítulo 6: Trabalhando com os principais recursos do Arcserve UDP 213
Entendendo o recurso Nutanix no Arcserve UDP 214
Entendendo o recurso OneDrive no Arcserve UDP 215
Entendendo o recurso Exchange Online no Arcserve UDP 216
Entendendo o recurso de instantâneo de hardware no UDP 217
Entendendo o recurso de nuvem no UDP 218
Entendendo o recurso do caminho UNC/NFS no UDP 220
Entendendo o recurso SharePoint Online no UDP 221
Pré-requisitos 221
Capítulo 7: Usar a administração com base em função do Arcserve UDP 223
Acessar o console de gerenciamento de usuários 224
Iniciar o console de gerenciamento de usuários do Arcserve UDP 224
Configurando a autenticação multifator 225
Adicionar usuário, excluir usuários e alterar senha 231
Configurar o gerenciamento de usuário 232
Funções predefinidas 233
Atribuir uma função pré-definida 237

Exibir e cancelar uma função 238
Adicionar uma nova função 239
Pesquisar usuários e funções 241
Integrar o Arcserve UDP ao Active Directory 242
Como integrar o Arcserve UDP 8.0 ao Active Directory usando grupos do Windows 243
Como integrar o Arcserve UDP 8.0 ao Active Directory usando grupos do Active Directory 246
Acesso ao Arcserve UDP usando a autenticação integrada do Windows 252
Solução de problemas da IWA (Integrated Windows Authentication - Autenticação Integrada do Windows) 253
O console do Arcserve UDP não oferece suporte a IWA se a conexão de banco de dados do Console usar o modo de autenticação do Windows 255
Solução de problemas 257
Capítulo 8: Adicionando e gerenciando nós de origem 259
Como adicionar nós no console 260
Verificar os pré-requisitos 261
Adicionar nós 262
Detectar nós 267
Importar nós 270
Como gerenciar nós 277
Verificar os pré-requisitos 278
Atualizar informações do hipervisor 279
Especificar o hipervisor 280
Atualizar informações da VM 282
Atualizar nós 283
Exportar nó 287
Pausar nós 288
Retomar nós 289
Sincronizar dados 290
Excluir nós do console 291
Implantar o agente em nós 292
Executar verificações prévias para as tarefas de backup 293
Como adicionar e gerenciar um caminho UNC/NFS 309
Adicionar um caminho UNC/NFS 310
Atualizar um caminho UNC/NFS 313
Excluir um caminho UNC/NFS 314
Como adicionar e gerenciar grupos de nós 315
Verificar os pré-requisitos 317

Adicionar grupos de nós ... 318
Modificar grupos de nós ... 319
Excluir grupos de nós ... 320
Como gerenciar nós para a nuvem ... 321
Baixar o ponto de recuperação a partir da nuvem ... 322
Fazer upload do ponto de recuperação para a nuvem ... 324
Copiar ponto de recuperação para o disco local ou compartilhamento de rede ... 327
Adicionar uma matriz de armazenamento ... 330
Adicionar uma matriz de armazenamento para o NetApp ... 332
Adicionar detalhes do HPE RMC que gerencia a matriz de armazenamento de sto-reserve de HPE 3PAR ... 338
Adicionar uma matriz de armazenamento Nimble ... 340
Como adicionar e gerenciar um site ... 342
Especificar o nome do site ... 344
Compartilhar instruções de registro ... 345
Verificar e adicionar o site ... 346
Modificar o URL do Console ... 347
Modificar o site ... 348
Excluir um site ... 349
Configurar um servidor proxy para o gateway ... 350
Como gerenciar nós do Exchange Online ... 353
Adicionar um nó do Microsoft Exchange Online ... 354
Atualizar um nó do Microsoft Exchange Online ... 356
Excluir um nó do Microsoft Exchange Online ... 357
Oferecer suporte a uma caixa de correio de pasta pública para a proteção do Exchange Online ... 358
Como gerenciar nós do SharePoint Online ... 359
Adicionar um nó do SharePoint Online ... 360
Atualizar um nó do SharePoint Online ... 361
Excluir um nó do SharePoint Online ... 362
Como gerenciar o nó do OneDrive gere ... 362
Adicionar um nó do OneDrive ... 363
Excluir um nó do OneDrive Online ... 363
Como gerenciar nós do grupo do banco de dados Oracle ... 363
Atualizar nó do banco de dados Oracle ... 363
Exportar nó ... 364
Fazer backup do nó do banco de dados Oracle ... 364

Cancelar a tarefa de backup dos nós do banco de dados Oracle 366
Excluir nós do banco de dados Oracle 366
Capítulo 9: Adicionando e gerenciando destinos 369
Como adicionar um destino 370
Como adicionar um destino 371
Adicionar servidores do Arcserve Backup 385
Adicionar um console remoto 387
Adicionar uma conta de nuvem 389
Adicionar uma conta de nuvem do Arcserve 424
Como gerenciar um repositório de dados 427
Verificar os pré-requisitos 428
Modificar um repositório de dados 429
Iniciar um repositório de dados 438
Interromper um repositório de dados 439
Excluir um repositório de dados do console 441
Excluir os dados do nó de um repositório de dados 442
Monitorar a capacidade de espaço do repositório de dados 443
Procurar pontos de recuperação em um repositório de dados 451
Suporte a FQDN para um repositório de dados 453
Executar uma tarefa de mesclagem manual ou por demanda 454
Modificar o limite de nós ativos simultâneos para backup manual 455
Solução de problemas: como usar um armazenamento de dados quando uma ou várias pastas estiverem cheias 456
Como gerenciar um servidor do ponto de recuperação 459
Verificar os pré-requisitos 460
Atualizar um servidor de ponto de recuperação 461
Excluir um servidor de ponto de recuperação do Console 462
Importar um repositório de dados 463
Instalar/atualizar o servidor de ponto de recuperação 465
Como gerenciar servidores de backup do Arcserve 466
Atualizar um servidor de backup Arcserve 467
Excluir um servidor de backup Arcserve 468
Como gerenciar a pasta compartilhada 469
Modificar uma pasta compartilhada 470
Excluir uma pasta compartilhada 471
Como gerenciar um console remoto 472
Modificar um console remoto 473

Excluir um console remoto 474
Testar conexão do console remoto 475
Capítulo 10: Criando planos para proteger os dados 477
Compreendendo o plano e as tarefas 478
Como criar um plano de backup do Windows 482
Verificar os pré-requisitos e as considerações 483
Criar um plano de backup com uma tarefa de backup 489
(Opcional) Executar um backup manual 512
Verificar o backup 515
Como criar um plano de backup do Nutanix 516
Como criar um modo de espera virtual para o Nutanix AHV 517
Como criar uma máquina virtual instantânea no Nutanix AHV 517
Como criar um plano de recuperação garantida e proteger o Nutanix AHV para o nó do Linux 517
Como fazer backup de volumes compartilhados do agrupamento 517
Modificar configurações da máquina do agente para fazer backup de volumes CSV 519
Como fazer backup de volumes sem letra de unidade 520
Verificar pré-requisitos 521
Montar volume sem letra de unidade na pasta NTFS 521
Especificar volume sem letra de unidade no Registro 522
Como fazer backup do volume selecionado 522
Como criar um plano de backup do Linux 524
Verificar os pré-requisitos e as considerações 525
Criar um plano de backup 526
(Opcional) Executar um backup manual 549
Verificar o backup 552
Solução de problemas 553
Como criar um plano de backup de máquina virtual com base em host 555
Verificar os pré-requisitos e as considerações 557
Criar um plano de backup com base em host 563
(Opcional) Executar um backup manual 600
Verificar o plano 603
Como criar um modo de espera virtual para o plano do AWS EC2 604
Verificar os pré-requisitos e as considerações 605
Criar um plano com uma tarefa de backup 613
Adicionar ao plano uma tarefa de modo de espera virtual para EC2 630
(Opcional) Executar a tarefa no modo de espera virtual para EC2 manualmente 636

Pausar e retomar a tarefa do modo de espera virtual 637
Verificar o plano 639
Encerrar os recursos do EC2 639
Como criar um modo de espera virtual para o plano do Microsoft Azure 641
Verificar os pré-requisitos e as considerações 642
Criar um plano com uma tarefa de backup 643
Adicione uma Tarefa no modo de espera virtual ao plano 644
(Opcional) Execute a tarefa no modo de espera virtual manualmente 652
Pausar e retomar sinal de monitoramento 653
Pausar e retomar a tarefa do modo de espera virtual 654
Verificar o plano 656
Como criar um plano no modo de espera virtual 657
Verificar os pré-requisitos e as considerações 658
Criar um plano com uma tarefa de backup 660
Adicionar uma tarefa no modo de espera virtual ao plano 677
(Opcional) Execute a tarefa no modo de espera virtual manualmente 691
Pausar e retomar sinal de monitoramento 692
Pausar e retomar a tarefa do modo de espera virtual 693
Verificar o plano 695
Como criar um plano de recuperação garantida 696
Verificar os pré-requisitos e as considerações 697
Adicionar ao plano uma tarefa de recuperação garantida 699
(Opcional) Executar a tarefa do teste de recuperação garantida manualmente 713
Como criar um plano de backup de caminho UNC/NFS 716
Verificar os pré-requisitos e as considerações 717
Criar um compartilhamento de arquivos 717
Criar um plano de backup com uma tarefa de caminho UNC/NFS 722
(Opcional) Executar um backup manual 742
Outras tarefas no plano do UNC/NFS 745
Verificar o backup 746
Como proteger máquinas em modo de espera virtual 747
Verificar os pré-requisitos e as considerações 748
Ligar máquinas do Virtual Standby 749
Proteger máquinas no modo de espera virtual depois de serem ligadas 755
Verifique se a máquina em modo de espera virtual está protegida 757
Como proteger máquinas virtuais instantâneas 758

Verificar os pré-requisitos e as considerações 759
Ligar máquinas virtuais instantâneas a partir do ponto de recuperação 760
Proteger uma máquina virtual instantânea quando ela está ligada 761
Verificar se a máquina virtual instantânea está protegida 762
Como replicar dados entre repositórios de dados gerenciados de um console do UDP 763
Verificar os pré-requisitos e as considerações 764
Criar uma tarefa de backup 765
Adicionar uma Tarefa de replicação ao Plano 766
(Opcional) Executar uma replicação manual 769
Verificar o plano 770
Como replicar dados entre repositórios de dados gerenciados a partir de diferentes consoles do UDP 771
Verificar os pré-requisitos 774
Criar uma conta de usuário para o console de origem 775
Criar um plano para definir o repositório de dados de destino 776
Mapear o plano para a conta de usuário 779
Enviar o plano e os detalhes da conta de usuário para o administrador de origem 781
Receber o plano e os detalhes da conta de usuário do administrador de destino 782
Criar um plano de replicação para enviar dados ao console de destino 783
Verificar se os dados estão replicados 787
Como executar uma replicação de dados offline usando o início rápido do RPS 788
Verificar os pré-requisitos 791
Criar um repositório de dados temporário em um dispositivo externo 792
Replicar os dados de origem para o repositório de dados temporário 793
Excluir o repositório de dados temporário do console de origem 794
Enviar o dispositivo externo para o local de destino 795
Receber o dispositivo externo 796
Importar o repositório de dados temporário do dispositivo externo 797
Criar um repositório de dados de destino 798
Replicar dados do repositório de dados temporário para o repositório de dados de destino 799
Verificar se os dados são replicados 800
(Opcional) Definir a contagem de nós simultâneos para o início rápido do RPS 801
Como executar a replicação inversa 801
Verificar os pré-requisitos 801
Executar replicação ad hoc 802
Executar a replicação inversa do console remoto para o servidor RPS local 809

Como criar um plano de pontos de recuperação de cópia 817
Verificar os pré-requisitos e as considerações 818
Criar um plano com uma tarefa de backup 819
Adicionar uma tarefa de Copiar pontos de recuperação ao plano 835
Verificar o plano 844
Como criar um plano de cópia de arquivo 845
Verificar os pré-requisitos e as considerações 846
Criar um plano com uma tarefa de backup 847
Adicionar uma Tarefa de cópia de arquivo ao plano 864
(Opcional) Executar uma cópia de arquivo manual 875
Verificar o plano 876
Como criar um plano de arquivo morto 877
Verificar os pré-requisitos e as considerações 878
Criar um plano com uma tarefa de backup 879
Adicionar uma tarefa de arquivo morto ao plano 896
(Opcional) Executar uma cópia de arquivo manual 907
Verificar o plano 908
Como criar um plano de cópia em fita 909
Verificar os pré-requisitos e as considerações 910
Crie um plano com uma tarefa de backup 911
Adicionar uma tarefa de Cópia em fita ao plano 912
Como criar e gerenciar uma máquina virtual instantânea no Microsoft Azure 921
Rever os pré-requisitos de uma máquina virtual instantânea no Microsoft Azure 922
Criar uma máquina virtual instantânea no Microsoft Azure 923
Gerenciar uma máquina virtual instantânea 932
Como criar e gerenciar uma máquina virtual instantânea em servidores Hyper-V e VMware ESX 935
Revisar os pré-requisitos de uma máquina virtual instantânea 937
Criar uma máquina virtual instantânea 940
Gerenciar uma máquina virtual instantânea 956
Como criar e gerenciar uma máquina virtual instantânea no Amazon EC2 962
Rever os pré-requisitos de uma máquina virtual instantânea no Amazon EC2 963
Criar uma máquina virtual instantânea no Amazon EC2 964
Gerenciar uma máquina virtual instantânea 973
Como criar um plano para replicação entre sites 979
Criar um plano para a replicação entre sites 981
Como proteger os dados do Microsoft Office 365 983

Autenticação moderna ... 983
Como criar um plano de backup do Exchange Online ... 990
Como criar um plano de backup do SharePoint Online ... 1021
Como criar um plano de backup do Microsoft Office 365 OneDrive ... 1041
Gerenciando o backup e a restauração do Microsoft Teams ... 1059
Verificar os pré-requisitos e as considerações ... 1062
Adicionar o grupo e a função necessários à conta de backup do Exchange Online para executar backup e restauração ... 1064
Criar um plano de backup do Exchange Online ... 1066
Especificar a origem ... 1068
Especificar o destino ... 1077
Especificar a programação ... 1078
Noções básicas sobre a programação avançada e retenção ... 1082
Especificar as configurações avançadas ... 1085
Verificar os pré-requisitos ... 1107
Criar um plano de backup do SharePoint Online ... 1108
Especificar a origem ... 1110
Especificar o destino ... 1115
Especificar a programação ... 1116
Especificar as configurações avançadas ... 1120
Como criar e configurar máquinas virtuais instantâneas simultâneas em vários hipervisores ... 1137
Selecionar um servidor de ponto de recuperação de origem ... 1139
Selecionar o local das VMs ... 1141
Selecionar os servidores de recuperação ... 1145
Definir as configurações das máquinas virtuais ... 1147
Verificar o resumo ... 1152
Como configurar as máquinas simultâneas no modo de espera virtual ... 1155
Capítulo 12: Usando o instantâneo de hardware para backup ... 1159
Como usar o instantâneo de hardware para backup ... 1160
Usar o instantâneo de hardware para o backup sem agente da VMware ... 1161
Considerações sobre o suporte a iSCSI/FC do NetApp para VMware ... 1163
Considerações sobre o suporte a NFS da VMware ... 1167
Considerações sobre o armazenamento Nimble quando a autenticação CHAP está ativada ... 1170
Usar o instantâneo de hardware para o backup sem agente do Hyper-V ... 1172
Usar o instantâneo de hardware para o backup com base em agente ... 1174
Verificar se o backup usou o instantâneo de hardware ... 1175

Capítulo 13: Restaurando dados protegidos 1177

Como restaurar a partir de um ponto de recuperação 1178

Verificar os pré-requisitos e as considerações para restauração 1180

Especifique as informações do ponto de recuperação para restauração 1189

Restaure o conteúdo do ponto de recuperação 1202

Verificar se o conteúdo foi restaurado 1203

Como restaurar a partir de uma cópia de arquivo 1204

Revisar os pré-requisitos e as considerações para restauração 1206

Especificar as informações de cópia de arquivo para restauração 1209

Restaurar o conteúdo da cópia de arquivo 1222

Verificar se o conteúdo foi restaurado 1224

Como restaurar a partir de um arquivo morto 1225

Revisar os pré-requisitos e as considerações para restauração 1226

Especificar as informações de cópia de arquivo para restauração 1228

Restaure o conteúdo do ponto de recuperação 1241

Verificar se o conteúdo foi restaurado 1243

Como restaurar arquivos/pastas 1244

Verificar os pré-requisitos e as considerações para restauração 1247

Especificar as informações de arquivo/pasta a serem restauradas 1257

Restaurar o arquivo/pasta 1275

Verificar se o arquivo/pasta foi restaurado 1277

Como executar uma recuperação bare metal usando uma VM no modo de espera virtual ou VM instantânea 1278

Rever os pré-requisitos e considerações da BMR 1280

Definir as opções da BMR 1282

Verificar se a BMR foi bem-sucedida 1305

Informações de referência da BMR 1306

Solução de problemas da BMR 1314

Como restaurar uma máquina virtual 1321

Revisar os pré-requisitos e as considerações para restauração 1323

Especificar as informações da máquina virtual a ser restaurada 1324

Restaurar a máquina virtual 1342

Verificar se a máquina virtual foi restaurada 1343

Como restaurar o Filestream SQL 1343

Como aplicar o patch T00002266 1345

Restaurar o banco de dados SQL no local original 1345

Restaurar o banco de dados SQL em uma instância alternativa no mesmo servidor 1349

Restaurar o banco de dados SQL em uma instância alternativa em um servidor diferente ... 1354
Restaurar o banco de dados SQL em um local alternativo na mesma instância ... 1361
Modo de restauração por meio da chave do Registro ... 1364
Como usar o utilitário GRT (Exchange Granular Restore- Restauração granular do Exchange) ... 1371
Introdução ... 1372
Verificar os pré-requisitos e as considerações ... 1373
Como restaurar dados do Microsoft Exchange usando o utilitário GRT (Exchange Granular Restore - Restauração granular do Exchange) ... 1374
Como restaurar um aplicativo do Microsoft Exchange ... 1380
Revisar os pré-requisitos e as considerações para restauração ... 1382
Especificar as informações de restauração do Microsoft Exchange ... 1384
Restaurar o aplicativo do Microsoft Exchange ... 1390
Verificar se o aplicativo do Microsoft Exchange foi restaurado ... 1392
Como restaurar dados do Exchange em uma máquina virtual do VMware ... 1393
Como fazer download de arquivo/pastas sem restaurar ... 1394
Como fazer download de arquivos/pastas sem restaurar para nós do Linux ... 1396
Como restaurar um aplicativo do Microsoft SQL Server ... 1398
Revisar os pré-requisitos e as considerações para restauração ... 1400
Especificar as informações do Microsoft SQL Server a serem restauradas ... 1403
Restaurar o aplicativo do Microsoft SQL Server ... 1409
Verificar se o aplicativo do Microsoft SQL Server foi restaurado ... 1411
Como restaurar a partir de um caminho UNC/NFS ... 1412
Verificar os pré-requisitos e as considerações para restauração ... 1413
Especificar as informações de caminho UNC/NFS a serem restauradas ... 1414
Restaurar arquivos/pastas e o conteúdo localizados no caminho UNC/NFS ... 1424
Verificar se o conteúdo foi restaurado ... 1426
Como restaurar um banco de dados Oracle ... 1427
Verificar os pré-requisitos e as considerações ... 1429
Restaurar o arquivo de parâmetros do servidor ... 1430
Restaurar o arquivo de parâmetros ... 1431
Restaurar os logs de repetição arquivados ... 1432
Restaurar os espaços para tabelas ou arquivos de dados ... 1433
Restaurar sistema, desfazer espaços para tabelas ou arquivos de dados ... 1435
Restaurar todos os espaços para tabelas e arquivos de dados ... 1437
Restaurar arquivos de controle ... 1439
Restaurar todo o banco de dados (espaços para tabelas e arquivos de controle) ... 1441

Recuperar o banco de dados Oracle usando recuperação bare metal 1443
Como executar uma recuperação em nível de arquivo em nós Linux 1444
Verificar os pré-requisitos 1446
(Opcional) Recuperar dados do volume iSCSI para o computador de destino 1447
Especifique o ponto de recuperação para o backup com base em agente 1449
Especificar os detalhes da máquina de destino 1455
Especificar as configurações avançadas 1458
Criar e executar a tarefa de restauração 1463
Verificar se os arquivos foram restaurados 1465
Como executar uma recuperação em nível de arquivo de backup sem agente com base em host para nós do Linux 1466
Verificar os pré-requisitos 1467
Especificar o ponto de recuperação 1468
Especificar os detalhes da máquina de destino 1472
Especificar as configurações avançadas 1475
Criar e executar a tarefa de restauração 1480
Verificar se os arquivos foram restaurados 1481
Como executar uma migração da IVM (de um ponto de recuperação do Linux) da nuvem para o local 1482
Verificar os pré-requisitos e as considerações da migração da IVM 1483
Realizar a migração de IVM da nuvem para o local 1484
Como executar uma BMR (Bare Metal Recovery - Recuperação Bare Metal) para computadores Linux 1485
Verificar os pré-requisitos da BMR 1488
Obter o endereço IP do computador de destino usando o Live CD 1489
(Opcional) Recuperar dados para o volume iSCSI do computador de destino 1491
(Opcional) Recuperar dados do volume iSCSI para o computador de destino 1493
Analisar o servidor de backup 1495
Especificar os pontos de recuperação 1497
Especificar os detalhes do computador de destino 1499
Especificar as configurações avançadas 1501
Criar e executar a tarefa de restauração 1507
Verificar se o nó de destino foi restaurado 1515
Como executar uma BMR de migração em computadores Linux 1516
Verifique os pré-requisitos para a BMR de migração 1517
Executar uma BMR para o computador temporário 1518
Realizar uma BMR de migração 1520
Verificar se o nó de destino foi restaurado 1522

Como executar uma BMR usando um backup 1523
Rever os pré-requisitos e considerações da BMR 1525
Definir as opções da BMR 1527
Verificar se a BMR foi bem-sucedida 1546
Informações de referência da BMR 1547
Solução de problemas da BMR 1555
Como restaurar nós agrupados e discos compartilhados da Microsoft 1563
Verificar os pré-requisitos 1565
Restaurar os arquivos do disco compartilhado de um agrupamento 1566
Restaurar um nó específico em um agrupamento 1567
Restaurar um disco compartilhado de um agrupamento corrompido 1568
Restaurar os nós agrupados e disco compartilhado inteiros 1569
Como restaurar um Active Directory 1571
Verificar os pré-requisitos e as considerações para restauração 1573
Restaurar um Active Directory 1574
Verificar se o Active Directory foi restaurado 1578
Como restaurar dados do Active Directory usando o utilitário de restauração no nível de objeto do Active Directory do Arcserve UDP 1578
Como restaurar os dados do Microsoft Office 365 1586
Como restaurar dados da caixa de correio do Exchange Online 1587
Como restaurar dados da coleção de sites do SharePoint Online 1601
Como restaurar dados do OneDrive 1611
Procurar ponto de recuperação de cópia em fita para restauração 1622
Como executar uma restauração pontual 1622
Pré-requisitos 1623
Considerações 1623
Executar uma restauração pontual 1624
Como restaurar volumes compartilhados do agrupamento 1627
Verificar os pré-requisitos e as considerações 1628
Especificar as informações do CSV a serem restauradas 1636
Restaurar o conteúdo do CSV 1645
Capítulo 2: Gerenciando o backup e a restauração em fita 1647
Como fazer backup de um repositório de dados de redução de redundância em uma fita 1648
Como restaurar um repositório de dados de redução de redundância de uma fita 1649
Verificar os pré-requisitos 1651
Restaurar de uma mídia de fita para um local alternativo 1652

Importar o repositório de dados restaurado para o RPS 1653
Capítulo 3: Usando a interface do PowerShell 1655
Como usar a interface do PowerShell 1656
Verificar o pré-requisito 1657
Usando a interface do PowerShell para Arcserve UDP 1658
Sintaxe do PowerShell e parâmetros 1659
Exemplos do PowerShell 1672
Arquivo de configuração e propriedades do PowerCLI 1676
Capítulo 4: Protegendo o sistema Oracle usando o RMAN (Recovery Manager - Gerenciador de recuperação) 1679
Revisar os pré-requisitos do banco de dados Oracle com RMAN (Windows e Linux) 1680
Como criar um plano de backup para o banco de dados Oracle (Windows e Linux) 1688
Criar um plano de backup com uma tarefa de backup 1689
Adicionar ao plano uma tarefa de recuperação garantida 1711
(Opcional) Executar um backup manual 1720
Como restaurar um banco de dados Oracle usando o RMAN 1722
Selecionar os itens do banco de dados Oracle para restauração 1723
Definir as opções de restauração 1731
Limitações 1744
Capítulo 5: Proteger o ambiente do Microsoft SharePoint 1747
Considerações sobre a instalação em um ambiente do Microsoft SharePoint 1748
Como fazer backup de servidores do Microsoft SharePoint 1749
Verificar as considerações 1750
Executar um backup do servidor SharePoint 1751
Como restaurar um ambiente do SharePoint 1753
Restaurar usando uma VM instantânea 1754
Restaurar usando a interface de usuário do agente do Arcserve UDP 1764
Restaurar usando Montar banco de dados do ponto de recuperação 1770
Criar uma rede isolada para a recuperação do SharePoint 1794
Como criar uma rede isolada para recuperação do SharePoint para VM VMware 1795
Como criar uma rede isolada para a recuperação do SharePoint para VM do Hyper-V 1800
Capítulo 6: Gerando relatórios do Arcserve UDP 1803
Entendendo relatórios do Arcserve UDP 1804
Relatórios do Arcserve UDP 1805
Usando filtros e ações 1819
Trabalhando com relatórios do Arcserve UDP 1821

Criar um perfil de SLA ... 1822
Programar emails ... 1825
Enviar relatório por email ... 1830
Gerar um relatório ... 1832
Personalizar dias de retenção para um relatório de status de tarefa ... 1833
Tamanho dos dados brutos no relatório de capacidade gerenciado para o backup da VM sem agente com base em host ... 1834
Visualizar valores reais na origem e no destino para tipos de tarefas ... 1838
Capítulo 7: Gerenciando a alta disponibilidade ... 1843
Como funciona a alta disponibilidade ... 1844
Gerenciar serviços de controle de alta disponibilidade ... 1845
Gerenciar licenças de alta disponibilidade ... 1846
Gerenciar cenários ... 1847
Instalação remota ... 1861
Relatórios de alta disponibilidade ... 1864
Capítulo 8: Usando o utilitário VSphereConfig ... 1865
Ativar ou desativar a marcação VSPhereBackupNFC usando o prompt de comando ... 1865
Capítulo 9: Usando o Utilitário de diagnóstico ... 1873
Coletar informações de diagnóstico ... 1874
Coletar informações de diagnóstico a partir de um agente autônomo ... 1876
Carregar informações de diagnóstico para o site do Arcserve usando FTP ... 1877
Descompactar logs de agente ... 1879
Descompactar os logs do console ... 1880
Ignorar conteúdo da pasta de histórico de logs usando o Registro ... 1881
Coletar o log do computador gateway usando a linha de comando ... 1881
Coletar logs do RPS usando a linha de comando ... 1882
Coletar logs stub do Hyper-V com o agente instalado ... 1882
Coletar mensagens do Visualizador de eventos do Hyper-V ... 1883
Coletar arquivos OLF e a pasta Ca_lic ... 1884
Coletar listagem de diretório dos diretórios do repositório de dados/destino de backup ... 1884
Capítulo 10: Instalando manualmente o Sophos Intercept X Advanced for Server no Arcserve UDP ... 1887
Capítulo 11: Aplicando práticas recomendadas ... 1893
Práticas recomendadas para proteger o servidor Arcserve UDP ... 1894
Excluir arquivos da verificação do antivírus ... 1895
Configurar parâmetros de multitransmissão ... 1896

Assuntos relacionados ao Exchange online 1897
Configuração para desempenho ideal 1898
Práticas recomendadas de Backup 1899
Prática recomendada para restauração 1901
Perguntas frequentes sobre o Exchange on-line 1902
Assuntos relacionados ao Microsoft Azure 1903
Práticas recomendadas para uma máquina virtual instantânea no Microsoft Azure 1903
Implantar o Arcserve UDP no Microsoft Azure 1903
Capítulo 12: Solução de problemas 1905
Falhas relacionadas com comunicação do Arcserve UDP 1906
O Arcserve UDP não consegue se comunicar com nós do Windows 1907
Não é possível receber alertas de email da conta do Gmail 1908
O Arcserve UDP não consegue se comunicar com o servidor de backup Linux do Arcserve UDP em nós remotos 1909
O Arcserve UDP não consegue se comunicar com o servidor de ponto de recuperação do Arcserve UDP em nós remotos 1910
O Arcserve UDP não consegue se comunicar com o servidor de backup do Arcserve UDP em nós remotos 1912
O Arcserve UDP não consegue se comunicar com o site remoto 1913
Plano, tarefa e configurações relacionadas 1914
Falha da tarefa de backup após a alteração do nome do host/endereço IP do console 1915
Como adicionar senha de criptografia em um destino criptografado existente 1916
Não é possível aplicar as configurações de backup para o nó 1917
Falha de implantação do plano após a alteração de senha do computador de proxy de backup sem agente 1918
Configurações desativadas ao abrir a interface do usuário do agente 1919
Pausar e retomar falham quando o agente não está conectado à rede 1920
O serviço do Agente do Arcserve UDP é executado lentamente 1921
Configurar o registro para executar novamente uma tarefa de cópia em fita 1923
Configurar o registro para copiar em fita vários pontos de recuperação do mesmo tipo na mesma tarefa 1924
Não inclusão de arquivo/pasta no backup da pasta NFS compartilhada ou conversão de nome de arquivo/pasta em um nome ilegível 1925
Falha no backup da pasta NFS compartilhada 1925
Redefinir o console do UDP com MFA ativado quando o TOTP não estiver disponível 1925
Assuntos relacionados à VM instantânea 1932
Falha ao criar uma VM instantânea em VMware devido à duplicação do nome do repositório de dados NFS 1933
Falha ao criar uma VM instantânea com o Windows 2008 R2 como o servidor de recuperação para VMware ou Windows 2008 R2 Hyper-V Server 1934

Falha ao inicializar uma VM instantânea se o computador de origem for um servidor Windows 2008/2012/2016 do AD 1935

Falha ao ligar VM após restauração do Hyper-V 1937

Falha na tarefa de VM instantânea devido a um erro de serviço do Windows NFS 1938

A pasta de arquivo da VM instantânea não pode ser acessada ou excluída mesmo com privilégio de administrador. 1939

Falha da máquina virtual instantânea ao inicializar no Hyper-V após reiniciar o servidor de recuperação 1940

Falha ao criar o repositório de dados NFS da VMware e erro Não foi possível resolver o nome do host 1941

Falha ao implantar o serviço de integração na VM convidada no Hyper-V 1943

Falha da VM instantânea do Linux no servidor do Hyper-V em idioma diferente do inglês 1944

Consumo de licença extra para os caminhos UNC que residem em uma VM sob um Hyper-V licenciado 1945

É exibido um erro de falha de licença quando você altera a edição/o tipo de licença e cria uma VM instantânea 1945

Assuntos relacionados ao agente do Linux 1947

Configurações de destino de backup desativadas ao abrir a interface de usuário do agente do Linux 1948

O status de tarefas, histórico de tarefas e o log de atividades não são visíveis 1949

Falha ao restaurar o volume do sistema do SUSE15 com o sistema de arquivos XFS 1950

Relacionado à restauração 1951

Impossível restaurar arquivos 1952

Adicionar o banco de dados de conteúdo restaurado para o aplicativo web original 1953

O banco de dados não pode ser montado ao restaurar o banco de dados do Microsoft Exchange 1956

O campo De não é exibido corretamente para emails enviados por usuários que têm permissões "em nome de" para uma caixa de correio compartilhada 1958

Falha nas tarefas de restauração após backups leves de integração 1959

A restauração em uma pasta NFS compartilhada altera o nome de arquivo para um nome ilegível 1959

Gateway, RPS, repositório de dados, console e bancos de dados relacionados 1961

O nome do repositório de dados já está em uso 1962

Não é possível se conectar ao repositório de dados devido a problema de DNS 1963

O repositório de dados altera para o modo somente de restauração 1964

Erro quando a versão do RPS é inferior à versão do Console 1966

Não há suporte para adicionar o mesmo recurso em sites diferentes 1967

Como ativar os truncamentos de log quando o banco de dados SQL está no modo de recuperação completa 1968

Procurar pontos de recuperação não mostra os pontos de recuperação disponíveis quando RPS é configurado com FQDN 1970

Acesso negado ao se adicionar o RPS 1971
Atribuindo privilégios e funções de administrador a um usuário de domínio 1972
Não é possível alterar a exibição do UDP para o ponto de recuperação 1975
Acesso negado ao adicionar ou atualizar nós 1976
O Console do UDP não abre quando a senha de administrador do SQL é alterada 1978
Falha ao montar os pontos de recuperação pois o tempo limite se esgotou 1979
Como atualizar as credenciais do servidor de gateway 1980
Como atualizar o gateway quando as credenciais do proxy do gateway são alteradas 1982
O console exibe a mensagem Serviço de identidade está iniciando 1984
Relacionado à restauração e backup de máquina virtual 1985
Adicionar permissões para VDDK no Nível do vCenter Server 1988
A tarefa de backup para o modelo de VM é sempre convertida em backup completo, e o tamanho dos dados de backup é o tamanho de provisionamento do disco virtual 1995
Discos independentes são ignorados pela tarefa de backup do modelo de VM 1997
A tarefa de backup para a VM no compartilhamento do SMB 3.0 falha com uma mensagem de erro 1999
A tarefa de recuperação da VM falha ao restaurar a VM para um compartilhamento de arquivos padrão do Windows 2000
Informações de volume não disponíveis para o ponto de recuperação 2001
Converter backup incremental em backup de verificação, pois os instantâneos da máquina virtual foram alterados desde a última tarefa de backup ou precisam de consolidação 2002
Backup sem agente para VM da VMware falha se o dispositivs de CD/DVD da VM estiver conectado a uma imagem ISO que reside em um repositório de dados do NFS desconectado 2003
Falha do backup sem agente com base em host para VM do Hyper-V após a atualização do Arcserve UDP 2004
Falha no backup sem agente com base em host no VMware ESXi 6.0 2005
O backup sem agente com base em host trava ao usar o Windows 2003 R2 de 64 bits como proxy de backup 2007
O backup sem agente com base em host não usa o modo de transporte hotadd 2008
A tarefa de backup sem agente com base em host ou restauração usa o modo de transporte NBD ou NBDSSL mesmo quando o modo SAN é possível 2009
Falha ao criar um instantâneo para máquinas virtuais do Hyper-V quando várias tarefas estão sendo executadas 2011
Falha do Hyper-V ao criar um instantâneo VSS 2013
Falha ao fazer backup de um disco virtual devido a um erro do sistema = [O dispositivo não está pronto (21)] 2014
Falha na tarefa de backup 2015
Falha ao importar as VMs da VMware a partir do vCenter 2017
Os backups falham devido à licença ESXi 2018

O modo de transporte HotAdd não funciona durante a tentativa de fazer backup de uma VM da VMware ... 2019
Controle mais granular de VSS em encerramentos do sistema operacional convidado Windows ... 2021
Não é possível configurar a máquina virtual para ativar o parâmetro "Disk.EnableUUID" 2023
As operações de recuperação falham durante a recuperação de dados usando o modo de transporte HOTADD ou SAN ... 2025
Falha na operação de recuperação da VM quando uma porta não padrão é especificada ... 2027
A tarefa de backup completo ou incremental programada falha para a VM do Hyper-V 2028
Falha no gravador de VSS NTDS do Hyper-V ao criar o instantâneo de VSS na VM ... 2029
As alterações do endereço MAC não são retidas após a recuperação da VM ... 2030
A recuperação de VM falhou com o erro - não é possível abrir arquivos VMDK ... 2031
Problemas causados por UUID da VM duplicado ... 2033
Falha na tarefa de catálogo do sistema de arquivos ou falha de verificação do ponto de recuperação para backup sem agente com base em host ... 2035
O backup incremental converte para backup de verificação ou o tamanho do backup aumenta no Hyper-V ... 2037
Falha no backup com base em host da VM do Hyper-V que tem uma configuração de disco diferencial especial ... 2038
A tarefa de backup falha para uma máquina virtual VMware ... 2039
Desativar nova verificação de adaptadores HBA durante o backup incremental ... 2041
Desativar a criação de instantâneo consecutivo na VM do VMware para um backup ... 2042
Quando restaurada de uma versão superior do host ESXi para uma versão anterior do host ESXi, a VM trava na fase de inicialização ... 2044
A utilização de RAM atinge 99% quando as tarefas de backup são enviadas para a VM ... 2045
Falha na tarefa de restauração do Hyper-V, não é possível se conectar ao utilitário no Host ... 2046
A proteção automática falha ao detectar e proteger a VM ... 2048
Definir o tamanho do bloco de leitura ao fazer backup do arquivo VMDK ... 2051
A reserva de espaço de LUN é herdada durante a execução do clone de LUN ... 2051
Assuntos relacionados ao modo de espera virtual ... 2053
Sistema operacional não encontrado ... 2054
Falha em tarefas no modo de espera virtual devido a erros internos ... 2055
Falha nas tarefas do modo de espera virtual usando o modo de transporte hotadd ... 2058
Falha em tarefas de modo de espera virtual para sistemas Hyper-V ... 2060
Problema relacionado à UUID duplicada do agente ... 2061
As modificações na nuvem privada virtual em tarefas no modo de espera virtual não refletem no Amazon EC2 ... 2061
A opção recursos de EC2 do terminal não é exibida ... 2062
Assuntos relacionados à cópia dos pontos de recuperação ... 2063

Configurar o registro para tarefa de cópia de ponto de recuperação 2064
Congestionamento de largura de banda com tarefas de cópia do ponto de recuperação para a nuvem 2065
Tarefa de mesclagem ignorada 2067
Relatórios relacionados do Arcserve UDP 2069
Como exibir os gráficos para visualizar relatórios do Arcserve UDP 2070
Assuntos relacionados ao Exchange Online do Microsoft Office 365 2073
Não é possível exibir a lista de caixas de correio no diálogo Selecionar o destino 2073
Acesso ou permissão negada para o grupo do Exchange Online 2074
Capítulo 13: Apêndice 2077
Ferramenta de linha de comandos para o repositório de dados de redução de redundância 2078
Como exibir a opção Verificação de ponto de recuperação 2082
Como aplicar versão diferente do VDDK da versão integrada no Arcserve UDP 2085
Modificando o VDDK manualmente para o backup no modo de espera virtual (VSB) 2085
Modificando o VDDK manualmente para o backup com base em host (HBBU) 2086
Como migrar os dados de backup do Arcserve D2D r16.5 dos dois servidores com o mesmo nome de host para o repositório de dados do RPS 2088
Como implantar o Arcserve UDP no Microsoft Azure 2089
Entendendo o fluxo de processos 2089
Considerações 2090
Planejando a implantação do Arcserve UDP no Microsoft Azure 2091
Implantar o Arcserve UDP no Microsoft Azure 2103
Termos e definições do Arcserve UDP 2115
Backup com base em agente 2115
Compactação 2115
configuração 2116
Painel 2116
Repositório de dados 2116
Destino 2116
Nós detectados 2116
Criptografia 2117
Redução de redundância global 2119
Backup sem agente com base em host 2119
Modo de transporte HOTADD 2119
Tarefa 2119
tarefas 2119
Modo de transporte NBD 2120

Modo de transporte NBDSSL 2120
Nós 2120
Plano 2120
Nós protegidos 2120
Evento recente 2120
Ponto de recuperação 2120
Servidor do ponto de recuperação 2121
Replicar 2121
Recursos 2121
Modo de transporte SAN 2121
Sistemas 2121
Tarefas 2121
Nós não protegidos 2122
Redução de redundância de dados 2123
Tipos de redução de redundância de dados 2124
Como a redução de redundância de dados funciona 2125
Quando você deve usar a redução de redundância 2127
Configurando os repositórios de dados da redução de redundância no Arcserve UDP 2128
Redução de redundância, criptografia e compactação 2130
Limitações de redução de redundância 2131

Capítulo 1: Recursos e aprimoramentos

Esta seção explica os recursos ou aprimoramentos fornecidos em cada release do Arcserve UDP. A solução Arcserve UDP fornece uma solução integrada para problemas de armazenamento de última geração de organizações que estão tentando proteger os seus dados em um mundo virtual, de nuvem e de serviços em constante mudança. A solução faz isso fornecendo uma única interface do usuário para uma ampla gama de funcionalidades que trata de problemas de preparação contra desastre e de continuidade operacional multi-site.

Esta seção fornece informações sobre novos recursos, aprimoramentos e suporte.

Esta seção contém os seguintes tópicos:

Novos recursos

Importante: Para obter informações sobre os recursos mais recentes, consulte o UDP 8.1.

A seguir, apresentamos uma lista dos novos recursos disponíveis no Arcserve UDP 8.0.

- **Backup e restauração de volumes ocultos:** permissão para fazer backup e restaurar dados de volumes ocultos. Volume oculto é um volume montado sem uma letra de unidade ou um caminho de pasta no sistema operacional. Volumes ocultos podem ser acessados usando o GUID de volume correspondente.
- **Configurações de exportação e importação:** configurações de exportação e importação permitidas usando o arquivo JSON no agente do Windows.
- **Suporte a OneDrive:** opções de restauração permitidas para os locais original ou alternativo.
- **Suporte do SharePoint Online:** Os seguintes recursos estão disponíveis para o suporte do SharePoint Online:
  - Permissão para fazer backup de listas e bibliotecas de sites pessoais.
  - Permissão para adicionar várias coleções de sites de uma vez.
  - Permissão para adicionar as coleções de sites recém-adicionadas automaticamente no plano.
- **Suporte ao Oracle RMAN:** o Arcserve UDP agora oferece uma maneira de proteger o sistema Oracle usando o RMAN (Recovery Manager - Gerenciador de recuperação). O RMAN é um utilitário Oracle que executa tarefas de backup, restauração e recuperação em bancos de dados e automatiza a administração de estratégias de backup. Para obter mais informações, consulte Protegendo o sistema Oracle usando o RMAN.
- **Suporte ao grupo do Office 365:** suporte ao grupo ativado para usuários do Office 365.
- **Replicação inversa:** replicação ativada de dados (ponto de recuperação) da nuvem, do MSP ou do RPS gerenciado remotamente para o UDP local ou o servidor RPS no local. Para obter mais informações, consulte Como executar a replicação inversa.
- **Nutanix Files:** o Arcserve UDP agora oferece uma maneira de proteger o Nutanix Files usando a opção UNC/NFS do Arcserve UDP. O Nutanix Files é uma solução de armazenamento de arquivos dimensionada definida por

software que fornece um repositório para dados não estruturados, como diretórios iniciais, perfis de usuários, compartilhamentos departamentais, logs de aplicativos, backups e arquivos. Para obter mais informações, consulte Protegendo o caminho UNC/NFS.

- **Suporte ao Teams:** o suporte a backup e restauração de dados está ativado para o MS Teams, que é uma plataforma com base em bate-papo para comunicação de negócios. Para obter mais informações, consulte Gerenciando o backup e a restauração do Microsoft Teams.
- **Suporte ao armazenamento imutável para o ponto de recuperação de cópia:** permissão para criar armazenamento imutável no Amazon S3 usando o recurso de bloqueio de objeto.
- **Substituição do Adobe Flash:** o Adobe Flash não é mais necessário e a instalação do .NET Framework permite exibir gráficos.

Aprimoramentos de recursos

Importante: Para obter informações sobre os últimos aprimoramentos de recursos, consulte o UDP 8.1.

- **Alterações do PowerCLI:** as seguintes opções estão ativadas para os arquivos de log UDPPowerCLI.log:
  - Permissão para alterar o local dos arquivos de log do UDP PowerCLI.
  - Permissão para controlar o tamanho máximo dos arquivos de log usando a circulação de logs.
  - O carimbo de data/hora nos arquivos de log é alterado para o formato de 24 horas.
  - Diretiva de retenção permitida com base no período de retenção dos arquivos de log UDP PowerCLI.
  - Diretiva de retenção permitida com base no número de retenção dos arquivos de log UDP PowerCLI.
- **Aprimoramento do instantâneo:** o plano de backup do agente do Arcserve UDP (Windows/Linux) e o plano de backup sem agente com base em host (Nutanix/ESXI/Hyper-V) permitidos para executar o script posterior ao instantâneo, mesmo quando o instantâneo falha.
- **Autenticação moderna:** autenticação moderna ativada para backup e restauração do Office 365.
- **Especificar rede para restauração e replicação:** ative a restauração e a replicação usando uma rede para estabelecer a comunicação entre o agente do Windows e o servidor de ponto de recuperação.
- **Especificar rede para Linux:** backup e restauração ativados usando uma rede para estabelecer a comunicação entre o agente do Linux e o servidor de ponto de recuperação.
- **IVM simultânea:** permissão para criar e configurar máquinas virtuais instantâneas simultâneas em vários hipervisores usando o console do Arcserve UDP.
- **VSB simultâneo:** permissão para configurar máquinas simultâneas no modo de espera virtual usando o console do Arcserve UDP.

Aprimoramentos do agente do Linux

Importante: Para obter informações sobre os últimos aprimoramentos do agente do Linux, consulte o UDP 8.1.

- Novas plataformas com suporte:
  - 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
- **Especificar rede para Linux:** backup e restauração ativados usando uma rede para estabelecer a comunicação entre o agente do Linux e o servidor de ponto de recuperação.
- **IVM simultânea:** permissão para criar e configurar máquinas virtuais instantâneas simultâneas em vários hipervisores usando o console do Arcserve UDP.
- **Aprimoramento do instantâneo:** o plano de backup do agente do Arcserve UDP Linux para executar o script posterior ao instantâneo, mesmo quando o instantâneo falha.
- **Substituição do Adobe Flash:** o Adobe Flash não é mais necessário para exibir gráficos no agente Linux.

Suporte à plataforma e ao banco de dados

Importante: Para obter informações sobre o suporte ao banco de dados e plataforma mais recente, consulte o 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, Atualização 1
- Banco de dados Oracle 19c
- Nutanix Files 3.8.z, 3.7.z, 3.6.z

Aprimoramentos de terceiros e de segurança

Importante: Para obter informações sobre as melhorias de segurança e de terceiros mais recentes, consulte o UDP 8.1.

- **Suporte ao Open JDK:** a versão do Open JDK foi atualizada para 1.8.0.265.b01
- **Suporte ao VMware VDDK (Virtual Disk Development Kit - Kit de Desenvolvimento de Disco Virtual):** a versão do VDDK é atualizada para 7.0. 1.40833
- **Suporte ao VMware vSphere Web Services SDK:** a versão do SDK será atualizada para 6.7.1
- **Suporte ao WSO2:** a versão do WSO2 foi atualizada para v5.7.0
- **Suporte ao Apache:** a versão do Apache foi atualizada para 2.4.46
- **Suporte ao OpenSSL:** a versão do OpenSSL foi atualizada para 1.1.1i
- **Suporte ao Tomcat:** a versão do Tomcat foi atualizada para 9.0.37
- **Suporte ao SQLite:** a versão do SQLite foi atualizada para 3.26
- **AWS SDK para Java:** a versão do AWS SDK para Java foi atualizada para 1.11.852
- **AWS SDK para C++:** a versão do AWS SDK para C++ foi atualizada para 1.6.53

Aprimoramentos do appliance do Arcserve

Importante: Para obter informações sobre os últimos aprimoramentos do Appliance, consulte UDP 8.1.

Os clientes existentes do Appliance podem ser atualizados para o Arcserve UDP 8.0. Para obter mais informações, consulte Instalação.

Suporte interrompido

Importante: Para obter informações sobre os itens de suporte ignorados, consulte o UDP 8.1.

- Suporte ao vSphere 5.5. É altamente recomendável atualizar o ambiente (vCenter/ESXi) para a versão mais recente com suporte do VMware. Para obter mais informações sobre o fim do suporte geral ao vSphere 5.5, consulte o artigo da base de conhecimento.
- Nutanix AHV 5.5.3.1.

Capítulo 2: Entendendo o Arcserve UDP

Esta seção contém os seguintes tópicos:

Introdução

O Arcserve Unified Data Protection é uma solução abrangente para proteger ambientes de TI complexos. A solução protege os dados que residem em diversos tipos de nós, como Windows, Linux e máquinas virtuais em servidores VMware ESX, Microsoft Hyper-V ou Nutanix AHV. É possível fazer backup de dados tanto para um computador local ou um servidor de ponto de recuperação. Um ponto de recuperação é um servidor central onde os backups de várias origens são armazenados.

O Arcserve UDP fornece os seguintes recursos:

- Protege vários tipos de nós de origem, incluindo aqueles com base em agente, sem agente, CIFS, Exchange Online, SharePoint Online, OneDrive etc.
- Faz o backup de dados em servidores de ponto de recuperação
- Replica dados de backup para servidores de ponto de recuperação locais e remotos
- Monitora o Arcserve High Availability
- Arquiva dados
- Copia:
  - Arquivos de origem selecionados para um local de backup secundário
  - Pontos de recuperação para lugares na nuvem e locais, como a pasta de compartilhamento e o AWS EC2
  - Pontos de recuperação em fitas
- Cria
  - Máquinas no modo de espera virtual a partir de dados de backup para o hipervisor local (Hyper-V, ESX, Nutanix), AWS EC2 ou Microsoft Azure
  - Máquina virtual instantânea para o hipervisor local (Hyper-V ESX, Nutanix) para Windows
  - Máquina virtual instantânea para o hipervisor local (Hyper-V, ESX, Nutanix), AWS EC2 ou Microsoft Azure para Linux
- Restaura
  - Dados do backup e executa a BMR (Bare Metal Recovery – Recuperação Bare Metal)
  - Objetos de email e que não são de email do Microsoft Exchange usando o utilitário de Restauração granular do Exchange do Arcserve UDP.

Observação: para obter mais detalhes sobre as especificações, funções e outros recursos suportados, consulte o Guia do Usuário da Restauração Granular do Exchange (esr.pdf).

- Suporta
  - Administração com base em função
  - Instantâneo de hardware
  - Teste de recuperação garantida para pontos de recuperação
  - Relatório de SLA para RTO e RPO

O Arcserve UDP duplica dados de backup que estão salvos como pontos de recuperação de um servidor para outro servidor de ponto de recuperação. Também é possível criar máquinas virtuais de dados de backup que podem agir como computadores em espera quando o nó de origem falhar. A máquina virtual do modo de espera é criada por meio da conversão de pontos de recuperação em VMware ESX, máquina virtual do Microsoft Hyper-V ou formato do Nutanix AHV.

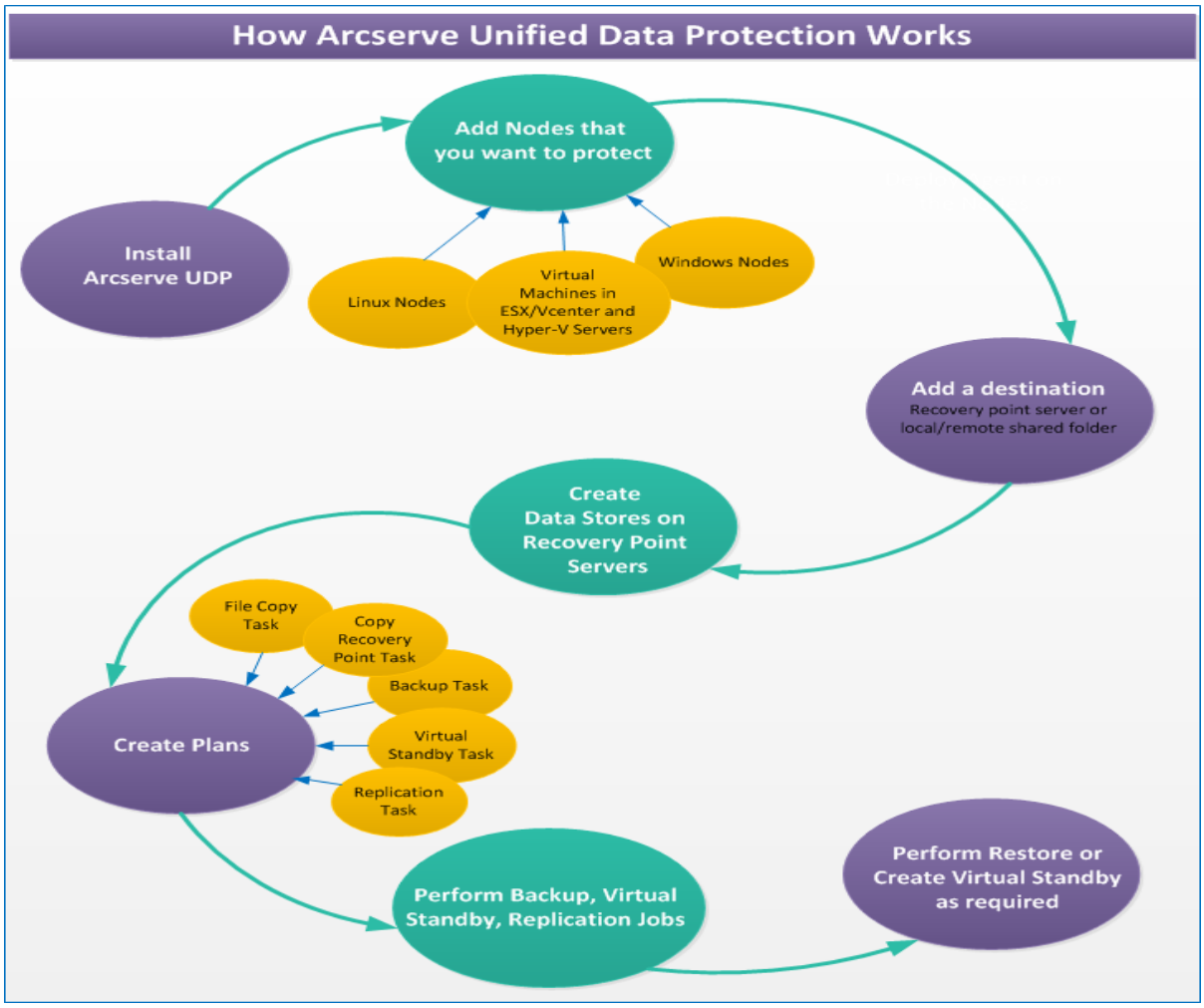
A solução Arcserve UDP fornece integração com o Arcserve High Availability. Depois de criar cenários no Arcserve High Availability, é possível gerenciar e monitorar seus cenários, além de executar operações como adicionar ou excluir máquinas de destino.

Como o Arcserve UDP funciona

O Arcserve UDP é uma solução unificada de proteção de dados que permite proteger os seus sistemas de computador. Use as seguintes etapas de alto nível para proteger seus sistemas usando o Arcserve UDP.

1. Instalar o Arcserve Unified Data Protection.
2. Adicionar os nós que deseja proteger. É possível adicionar nós e máquinas virtuais do Windows ou do Linux nos servidores ESX/vCenter, Hyper-V e Nutanix AHV.
3. Adicionar um destino. Um destino pode ser um servidor de ponto de recuperação, uma pasta local ou uma pasta compartilhada remota.
4. Criar armazenamentos de dados no servidor de ponto de recuperação. Um armazenamento de dados é uma área física em um disco. É possível criar armazenamentos de dados de redução de redundância e de não redução de redundância.
5. Criar um plano. Um plano é um grupo de tarefas para gerenciar backup, replicação, ponto de recuperação da cópia, cópia em fita, criação de máquinas no modo de espera virtual ou teste de recuperação garantida. Também é possível adicionar um caminho UNC, um nó do Office 365 Exchange Online, do SharePoint Online ou do OneDrive, e criar tarefas relacionadas.
6. Execute tarefas como backup, criar modo de espera virtual e replicar.
7. Execute uma restauração simples ou uma recuperação bare metal.

O diagrama a seguir ilustra as etapas de alto nível que você deve executar para proteger os dados:


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

IVM (Instant Virtual Machine - Máquina Virtual Instantânea) versus VSB (Virtual Standby Machine - Máquina Virtual no Modo de Espera)

Durante a restauração de dados após uma falha ou durante o treinamento de recuperação de falhas, poderá ser necessário iniciar instâncias virtualizadas de servidores que eram protegidos anteriormente pelo Arcserve UDP.

O Arcserve UDP fornece os dois seguintes recursos que permitem iniciar a máquina virtual a partir de pontos de recuperação:

- **Máquina virtual instantânea (IVM)**: cria uma máquina virtual instantaneamente a partir de um ponto de recuperação. Usar uma máquina virtual instantânea ajuda você a obter acesso imediato aos dados e aos aplicativos presentes nas sessões de backup do Arcserve UDP. Uma máquina virtual instantânea elimina o downtime associado a uma conversão ou restauração tradicional da sessão de backup para uma máquina física ou virtual.

  Para obter mais detalhes sobre Máquina virtual instantânea, consulte Como criar e gerenciar uma máquina virtual instantânea.

- **Máquina de espera virtual (VSB)**: converte os pontos de recuperação em formatos da máquina virtual e prepara um instantâneo para facilitar a recuperação de seus dados quando necessário. Este recurso oferece a capacidade com alta disponibilidade também e garante que a máquina virtual pode assumir o controle imediatamente quando o computador de origem falhar. A máquina virtual do modo de espera é criada pela conversão de pontos de recuperação em qualquer VMware, uma máquina virtual Hyper-V ou um formato de máquina virtual do Nutanix AHV.

  Para obter mais detalhes sobre o Modo de espera virtual, consulte Como criar um plano no modo de espera virtual.

Para determinar qual recurso funciona melhor, é preciso considerar seu RTO (Objetivo de tempo de recuperação) e o cenário. A tabela a seguir fornece a comparação entre os recursos IVM e VSB:

RECURSOS	IVM	VSB
Ligue as VMs no modo de espera a partir do ponto de recuperação mais recente	Sim (nenhuma conversão necessária)	Sim, SOMENTE se a tarefa VSB foi adicionada ao plano de backup. Por exemplo, Planejamento antecipado necessário)
Requer o processamento de tempo de backup	Não necessário	Obrigatório, é necessário adicionar uma tarefa VSB ao

		plano que é usado para fazer backup da máquina de origem.
Tempo de inicialização da VM	Um processo mais lento (até 30%) devido ao redirecionamento de E/S.	Mesmo tempo que qualquer outra VM no mesmo hipervisor.
Requisitos de espaço em disco	Espaço de armazenamento mínimo no disco filho do host ou armazene as alterações durante a execução de uma VM.	Sim, o espaço de armazenamento é utilizado no hipervisor de destino em que a VM no modo de espera VSB é mantida. Requer espaço de armazenamento igual ou maior que o tamanho da máquina de origem.
Opção de alta disponibilidade	N/D	DISPONÍVEL Monitora a máquina de origem e pode iniciar a VM VSB se a máquina de origem se tornar indisponível.
Desempenho da VM	Pode executar mais lentamente em comparação com VMs regulares (até 30%) devido ao redirecionamento de E/S; no entanto, o desempenho depende da natureza da carga de trabalho do aplicativo.	O desempenho é o mesmo que das VMs regulares.
Gerenciamento/Configuração	Gerenciada a partir do console do UDP, é possível iniciar ou interromper a IVM sob demanda quando for necessário acesso pelo usuário.	Adicionada como uma tarefa a um plano para que todos os dados armazenados em backup sejam convertidos automaticamente em um formato de VM. A tarefa VSB é aplicada a todos os nós que são protegidos pelo plano.
Dados persistentes e migração da VM para produção	O disco virtual da IVM se refere aos blocos de dados no ponto de recuperação a partir do qual a VM foi iniciada. Portanto, quando a IVM acessa blocos de dados em seu disco virtual, os dados são soli-	O disco virtual ou os discos da VM VSB já contêm a maioria dos dados recentes a partir do ponto de recuperação correspondente. Uma vez que o redirecionamento de E/S não

	citados, na verdade, a partir do RPS (esse processo é transparente para o usuário). Tal redirecionamento de E/S apresenta algum volume adicional de desempenho. Se você planeja usar IVM em produção, então é recomendável manter a IVM e hidratar o disco virtual da máquina virtual com os dados reais. A hidratação da IVM pode ser obtida pela cópia/replicação da VM. Dependendo do tipo de hipervisor usado em seu ambiente de produção, para manter os dados da IVM, você pode usar o VMware Storage vMotion ou a migração/replicação do armazenamento de VM do Hyper-V para copiar a IVM em um local em que os dados se tornem permanentes.	ocorra (que seja igual à IVM), o desempenho da VM VSB será o mesmo das VMs regulares, em que não há qualquer dependência no RPS ou no ponto de recuperação (em comparação com o cenário IVM).

Segurança do usuário

Esta seção contém os seguintes tópicos:

- Funções dos serviços do Arcserve UDP
- Privilégios de usuário das funções do Arcserve UDP

Funções dos serviços do Arcserve UDP

A tabela a seguir descreve as funções dos serviços do Arcserve UDP:

Serviço	Descrição	Em execução na função
Monitoramento de log de eventos do Arcserve	Fornece o serviço do SDK de licenciamento para aceitar as chaves de licença.	Console/RPS/Agente
Serviço de extensão do Explorer do agente do Arcserve UDP	Forneça o serviço de back-end para o modo de exibição do UDP no Windows Explorer.	RPS/Agente
Serviço do agente do Arcserve UDP	Fornece a interface de usuário da web e o Serviço web do agente do Arcserve UDP, incluindo o envio da tarefa de backup/restauração.	RPS/Agente
Serviço de identidade do Arcserve UDP	Forneça o serviço de autenticação e de autorização para o Console do Arcserve Unified Data Protection.	Console
Serviço de compartilhamento de porta do Gerenciamento do Arcserve UDP	Forneça o serviço de compartilhamento de porta que permite que o console, o gateway e o servidor de identidade compartilhem uma porta.	Console
Serviço de gerenciamento do Arcserve UDP	Fornece o serviço web para o console de gerenciamento central do Arcserve Unified Data Protection.	Console
Serviço do gateway de gerenciamento remoto do Arcserve	Forneça a capacidade de lidar com solicitações bidirecionalmente entre o console e o gateway na intranet ou na internet.	Gateway
Serviço de armazenamento de dados de RPS do Arcserve UDP	Fornece o serviço web para o gerenciamento do repositório de dados do UDP, incluindo a criação, a modificação, a exclusão, a iniciação e o interrompimento.	RPS
Serviço de compartilhamento da porta RPS do Arcserve UDP	Exponha apenas uma porta para que o servidor RPS realize a comunicação com o serviço/interface do usuário da web do agente, o serviço web do RPS e a tarefa de replicação.	RPS

Serviço de atualização do Arcserve UDP	Detecte a atualização do Arcserve UDP e faça download se disponível.	Console/RPS/Agente

Privilégios de usuário das funções do Arcserve UDP

A tabela a seguir descreve os privilégios do usuário das funções do Arcserve UDP:

Funções	Usuário	Privilégio	Comentários
Instalação	**Grupo de administradores locais**	**Grupo de administradores locais**	
Console e Gateway	**Grupo de administradores locais**	**Grupo de administradores locais**	
Servidor de ponto de recuperação	**Grupo de administradores locais**	**Grupo de administradores locais**	
Backup de cliente do Windows	**Grupo de administradores locais**	**Grupo de administradores locais** Políticas de segurança: • Atuar como parte do sistema operacional • Efetuar logon localmente • Efetuar logon como serviço • Efetuar logon em tarefa em lote	**Várias operações relacionadas a backup, como o instantâneo VSS, requerem privilégios de administrador.**
Compartilhamento de rede para um repositório de dados sem redução de redundância	Se o RPS UAC estiver ativado, a conta de domínio ou o administrador interno.		
Truncamento de log do SQL	Grupo de administradores locais	Administrador local com o sysadmin SQL ou função de banco de dados corrigida db_owner.	Truncamento de log requer consultar banco de dados de backup, o log de backup e reduzir consultas (reduzir banco de

			dados).
Truncamento de log do Exchange	Grupo de administradores de domínios	Grupo de administradores de domínios	É necessário ter acesso ao banco de dados do Exchange
Proteção do Active Directory	Grupo de administradores de domínios	Grupo de administradores de domínios	
Restauração do cliente do Windows			
Compartilhamento de rede para um repositório de dados sem redução de redundância	Se o RPS UAC estiver ativado, a conta de domínio ou o administrador interno.		
SQL	Grupo de administradores locais	Administrador local com o sysadmin SQL ou função de banco de dados corrigida db_owner.	
Exchange	Grupo de administradores de domínios	Grupo de administradores de domínios	É necessário ter acesso ao banco de dados do Exchange
Active Directory	Grupo de administradores de domínios	Grupo de administradores de domínios	
Utilitário Exchange Granular Restore	Restaurar na caixa de correio: a conta usada para restauração deve ter privilégio de personificação na caixa de correio de destino. Para outras opções de restauração, a conta não precisa de requisito especial.	Restaurar para a caixa de correio: a conta usada para restauração deve ter privilégio de personificação na caixa de correio de destino. Para obter outras opções de restauração, não há nenhum requisito especial na conta.	
Backup sem agente com base em host			
Adicionar o nó da VM a partir do vCenter/ESXi	• vCenter: administrador interno		Para o vCenter, se não for usado

	• ESXi: raiz		nenhum administrador interno, consulte o link.
Adicionar o nó da VM a partir do Nutanix AHV	Administrador de agrupamento ou administrador de usuário	Administrador de agrupamento ou administrador de usuário	
Adicionar o nó da VM a partir do Hyper-V	• Hyper-V autônomo: administrador local interno, o administrador de domínio interno ou conta de domínio que é integrante do grupo de administradores locais. • Cluster do Hyper-V: administrador de domínio interno ou conta de domínio que é integrante do grupo de administradores locais.		Se outra conta administrativa for usada, o acesso remoto de UAC precisará ser desativado. Consulte o link.
Alterar o método de encerramento de instantâneo da VMware no plano	Administrador local interno ou administrador de domínio interno **Observação:** as credenciais necessárias aqui são definidas pelo nó de atualização		Se outra conta administrativa for usada, o UAC precisará ser desativado. Consulte o link.
Restauração no nível do banco de dados do aplicativo para a VM do Hyper-V/Nutanix	Administrador local interno, administrador de domínio interno ou conta de domínio que é integrante do grupo de administradores locais **Observações:** • as credenciais necessárias aqui são definidas pela opção Atualizar nó • Se o sistema ope-		Se outra conta administrativa for usada, o acesso remoto de UAC precisará ser desativado. Consulte o link.

	racional convidado da VM for a versão de cliente do Windows (por exemplo, o Windows 10), será necessário configurar manualmente o firewall para permitir a WMI (Windows Management Instrumentation - Instrumentação de Gerenciamento do Windows)		
PFC	• VM da VMware: administrador local interno ou administrador do domínio interno • VM do Hyper-V: administrador local interno, administrador de domínio interno ou conta de domínio que é integrante do grupo de administradores locais. • VM do Nutanix: administrador local interno, administrador de domínio interno ou conta de domínio que é integrante do grupo de administradores locais. **Observações:** • as credenciais necessárias aqui		Se outra conta administrativa for usada: • Para VM do VMware, o UAC precisará ser desativado. Consulte o link. • Para VM do Hyper-V, o acesso remoto de UAC precisará ser desativado. Consulte o link.

	são definidas pela opção Atualizar nó • Para a VM do Hyper-V/Nutanix, se o sistema operacional convidado da máquina virtual for a versão de cliente do Windows (por exemplo, o Windows 10), será necessário configurar manualmente o firewall para permitir a WMI (Windows Management Instrumentation - Instrumentação de Gerenciamento do Windows)		
Comandos anteriores e posteriores	• VM da VMware: administrador local interno ou administrador do domínio interno • VM do Hyper-V: administrador local interno, administrador de domínio interno ou conta de domínio que é integrante do grupo de administradores locais. • VM do Nutanix: administrador local interno, administrador de domínio interno ou conta de domínio que é integrante do grupo de admi-		Para o uso das credenciais definidas na opção Atualizar nó e na guia Avançado de um plano, consulte o link.

	nistradores locais. **Observações:** • as credenciais necessárias aqui são definidas pela opção Atualizar nó e na guia Avançado de um plano. • Para a VM do Hyper-V, se o sistema operacional convidado da máquina virtual for a versão de cliente do Windows (por exemplo, o Windows 10), será necessário configurar manualmente o firewall para permitir a WMI (Windows Management Instrumentation - Instrumentação de Gerenciamento do Windows) • Para a VM do Hyper-V/Nutanix, se o sistema operacional convidado da máquina virtual for a versão de cliente do Windows (por exemplo, o Windows 10), será necessário configurar manualmente o firewall para per-		

	mitir a WMI (Windows Management Instrumentation - Instrumentação de Gerenciamento do Windows)		
Truncamento de log do SQL	Mesmo que comando anterior/posterior		Mesmo que comando anterior/posterior
Truncamento de log do Exchange	Mesmo que comando anterior/posterior		Mesmo que comando anterior/posterior
Restauração em nível de arquivo no local original	Administrador local interno, administrador de domínio interno ou conta de domínio que é integrante do grupo de administradores locais **Observações:** • as credenciais necessárias aqui são definidas pela opção Atualizar nó • Para a VM do Hyper-V/Nutanix, se o sistema operacional convidado da máquina virtual for a versão de cliente do Windows (por exemplo, o Windows 10), será necessário configurar manualmente o firewall para permitir a WMI (Windows Management Instrumentation - Instrumentação de Gerenciamento do		Se outra conta administrativa for usada, o acesso remoto de UAC precisará ser desativado de acordo com o link.

	Windows)		
Modo de espera virtual			
Para o Hyper-V	• Administrador local interno • Administrador de domínio interno • A conta de domínio deve ser integrante do grupo de Administradores locais • A conta local deve ser integrante do grupo administradores locais	Grupo de administradores locais	Se a conta administrativa local for usada, o acesso remoto de UAC precisará ser desativado. Consulte o link.
Para o Nutanix	Administrador de agrupamento	Administrador de agrupamento	
Para o VMware	• vCenter: administrador interno • ESXi: raiz		Para o vCenter, se não for usado nenhum administrador interno, consulte o link.
Máquina virtual instantânea/recuperação garantida			
Para o Hyper-V	• Administrador local interno • Administrador de domínio interno • A conta de domínio deve ser integrante do grupo de Administradores locais • A conta local deve ser integrante do grupo administradores locais		Se a conta administrativa local for usada, o acesso remoto de UAC precisará ser desativado. Consulte o link.
Para o VMware	• vCenter: administrador interno • ESXi: raiz	Grupo de administradores locais	Para o vCenter, se não for usado nenhum administrador interno, consulte o link.
Arquivo morto e cópia	**Grupo de admi-**	**Grupo de admi-**	

de arquivo	**nistradores locais**	**nistradores locais**	
Copiar o ponto de recuperação para a nuvem	**Grupo de administradores locais**	**Grupo de administradores locais**	
Proteção do caminho UNC/NFS	**Todos os usuários podem efetuar logon e ser representados**	**Permissão de leitura para o caminho UNC/NFS**	
Modo de espera virtual para AWS EC2	**Os usuários do Amazon IAM que têm as permissões necessárias para a interação com a API do AWS**		Para AWS EC2, consulte este link.
Modo de espera virtual para Microsoft Azure	**Aplicativo**	**Função de contribuidor da assinatura selecionada**	
Linux			
Instalar o	raiz	Leitura, gravação, execução	
Registro do Console	administrador do Console		
Backup com base em agente			
-Compartilhamento de rede	administrador de armazenamento	Leitura, gravação	
--Conexão do nó	raiz/não raiz/sudo	Leitura, gravação, execução	
Restauração em nível de arquivo			
-Compartilhamento de rede	administrador de armazenamento	Leitura, gravação	
--Conexão do nó	raiz/não raiz/sudo	Leitura, gravação, execução	usuário raiz pode restaurar em qualquer lugar; outros usuários podem restaurar somente em diretórios de sua propriedade
BMR		Informações de acesso ao hardware	
BMR de migração			
VM instantânea para o Hyper-V			

VM instantânea para a VMware			
VM instantânea para o Nutanix AHV	administrador de agrupamento	administrador de agrupamento	
VM instantânea para Amazon EC2	**Usuário do IAM**	**Acesso completo ao EC2**	
VM instantânea para Microsoft Azure	**Aplicativo**	**Função de contribuidor da assinatura selecionada**	
Proteção do Exchange Online	**Qualquer conta do Exchange Online**	**Tem privilégio de representação de aplicativo nas contas protegidas**	
Proteção do SharePoint Online	**Administrador do conjunto de sites do SharePoint Online**	**Administrador do conjunto de sites do SharePoint Online**	
OneDrive	**Administradores do Azure Active Directory**	**Administradores do Azure Active Directory**	

Capítulo 3: Instalando o Arcserve UDP

Esta seção contém os seguintes tópicos:

Como instalar o Arcserve UDP

Arcserve UDP - Cheio: após a instalação, você efetua logon no Console do Arcserve UDP e executa as funções de gerenciamento de dados. O console permite gerenciar e monitorar nós, servidores de ponto de recuperação, backups, restauração e replicação.

Arcserve UDP – Agente: instala apenas o agente do Arcserve UDP. Instale o agente nos nós que deseja proteger. Execute essa etapa apenas quando você deseja instalar o agente manualmente em um nó. Geralmente, o agente é automaticamente implantado nos nós do Console quando você cria um plano.

O que fazer a seguir?

1. Verificar os pré-requisitos e as considerações
2. Decidir o tipo de instalação
3. Instalar o Arcserve Unified Data Protection usando o assistente de instalação
4. Instalar o Arcserve Unified Data Protection usando a linha de comando
5. Instalar o Arcserve Unified Data Protection usando o programa de instalação unificado
6. Verificar a instalação
7. (Opcional) Portas de comunicação usadas
8. (Opcional) Como o processo de instalação afeta os sistemas operacionais

Verificar os pré-requisitos e as considerações

Verifique os pré-requisitos de instalação e as considerações a seguir antes de instalar o Arcserve UDP:

Pré-requisitos

- Verifique as Notas da Versão do Arcserve UDP 8.0. As Notas da Versão descrevem os requisitos do sistema, os sistemas operacionais suportados e uma lista de problemas conhecidos dessa release.
- Verifique se os seus sistemas atendem aos requisitos de software e hardware necessários para a instalação de componentes do Arcserve Unified Data Protection.
- Verifique se sua conta do Windows tem privilégios de administrador ou equivalente para instalar o software nos sistemas em que planeja instalar os componentes do Arcserve Unified Data Protection.
- Verifique se você tem os nomes de usuário e senhas dos sistemas em que você está instalando os componentes do Arcserve Unified Data Protection.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Considerações

Antes da instalação, você deve determinar como configurar a instalação do Arcserve Unified Data Protection:

- O sistema no qual você deseja instalar o Console.
- Os nós que deseja proteger.
- O número de servidores de ponto de recuperação que podem funcionar como destinos de backup.
- O número de servidores de réplica que podem replicar servidores de ponto de recuperação.

Decidir o tipo de instalação

É possível instalar o Arcserve UDP usando um dos seguintes métodos:

- **Instalação padrão usando o Assistente de instalação:** esse método permite instalar o Arcserve Unified Data Protection usando o Assistente de instalação. Neste método, você será solicitado, em cada etapa, escolher as opções desejadas.
- **Instalação silenciosa usando a linha de comando:** esse método permite executar uma instalação autônoma usando a linha de comando do Windows.
- **Instalação usando o programa de instalação unificado:** esse método permite instalar o Arcserve UDP, o Arcserve Backup e o Arcserve RHA a partir de um único programa de instalação. É possível optar por instalar todos os três produtos ao mesmo tempo ou instalar cada produto separadamente. É possível fazer download do programa de instalação do site da Arcserve.

Instalar o Arcserve Unified Data Protection usando o assistente de instalação

Usando o Arcserve Unified Data Protection, é possível gerenciar e monitorar de maneira centralizada os nós, servidores de ponto de recuperação, máquinas virtuais nos servidores vCenter, ESX ou Microsoft Hyper-V, servidores de réplica e relatórios do Arcserve Unified Data Protection.

Instalar o Arcserve Unified Data Protection em um servidor no qual você pode gerenciar nós protegidos e outros componentes do Arcserve Unified Data Protection.

Siga estas etapas:

1. Acesse o pacote de instalação do Arcserve UDP do site do Arcserve ou do CD do produto.

   Observação: se um dos sistemas operacionais suportados que não estejam em inglês for detectado, você precisa selecionar o idioma para a instalação do produto.

2. Clique duas vezes no pacote de instalação.

   A caixa de diálogo do **Contrato de licença** será exibida.

3. Leia e aceite os termos do contrato de licença e clique em **Avançar**.

   A caixa de diálogo **Tipo de instalação** é exibida.

4. Selecione um dos tipos de instalação.

   Instalação padrão

   Permite instalar o agente ou todos os componentes do Arcserve Unified Data Protection.

   Arcserve Unified Data Protection - Agente

   Instala o Agente do Arcserve UDP somente.

   Para obter mais informações, consulte *Instalar o Agente do Arcserve Unified Data Protection para Windows usando o assistente de instalação* no *Guia do Usuário do Agente do Arcserve UDP para Windows*.

   Arcserve Unified Data Protection- Completo

   Instala o Console do Arcserve Unified Data Protection, o servidor de ponto de recuperação e o Agente.

   Instalação avançada

Permite instalar um ou mais dos seguintes componentes do Arcserve Unified Data Protection:

- Agente do UDP do Arcserve
- Servidor de ponto de recuperação do Arcserve UDP
- Console do Arcserve UDP

5. Especifique se deseja instalar o driver de controle de alterações do Agente do Arcserve Unified Data Protection para Windows.

   Por padrão, esta opção está ativada.

   - Sem esse driver instalado, o Agente do Arcserve Unified Data Protection para Windows sempre executa o backup completo.
   - Com esse driver instalado, você ainda precisa ter uma licença válida do Agente do Arcserve Unified Data Protection para Windows para executar um backup local.
   - Esse driver não é necessário se o agente for usado como monitor de modo de espera virtual ou servidor proxy de backup da VM com base em host.

     Observação: é possível instalar esse driver, a qualquer momento, após a instalação estar concluída, executando o utilitário InstallDriver.bat no seguinte local:

     <Pasta de instalação do Arcserve UDP>\Engine\BIN\DRIVER

6. Clique em **Avançar**.

   A caixa de diálogo **Pasta de destino** é exibida.

7. Especifique a pasta em que você deseja instalar o Arcserve Unified Data Protection e clique em **Avançar**.

   A caixa de diálogo **Configuração** é aberta.

8. Na caixa de diálogo **Configuração**, especifique as seguintes informações:

   a. Selecione o protocolo.

      Observação: para uma comunicação segura, selecione o protocolo HTTPS.

   b. Digite o número da porta para o agente, se aplicável. Geralmente, o número de porta é 8014.

   c. Digite o número da porta para o console, se aplicável. Geralmente, o número de porta é 8015.

   d. Digite o nome e a senha de administrador do Windows.

e. Especifique se você deseja exibir o monitor do agente do Arcserve UDP para todos os usuários ou apenas para o usuário atual.

9. Clique em **Avançar**.

   A caixa de diálogo **Configurações de banco de dados** é aberta.

10. Na caixa de diálogo **Configurações do BD**, clique na lista suspensa **Banco de dados** para escolher um tipo de banco de dados. É possível especificar um dos seguintes:

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

      Importante: Quando há mais de 500 nós para gerenciar do console, verifique se selecionou o Microsoft SQL Server e não o SQLExpress.

    Depois que você especificar banco de dados, as opções necessárias para o banco de dados especificado são exibidas na caixa de diálogo **Configurações do banco de dados.** Forneça detalhes de configurações de banco de dados para um dos bancos de dados que você selecionar.

    Microsoft SQL Server 2014 Express (incluso):

    Na caixa de diálogo **Configurações do BD**, preencha o seguinte:

    a. Especifique o local no qual deseja instalar o Microsoft SQL Server 2014 Express. É possível aceitar o caminho padrão ou especificar um caminho alternativo.

    b. Especifique o local em que deseja instalar o arquivo de dados para o banco de dados padrão do Arcserve Unified Data Protection. É possível aceitar o caminho padrão ou especificar um caminho alternativo.

       Observação: o Microsoft SQL Server 2014 Express não oferece suporte à comunicação remota. Portanto, instale o banco de dados padrão e o arquivo de dados no computador em que você está instalando o aplicativo.

    Bancos de dados do Microsoft SQL Server

    Na caixa de diálogo **Configurações do BD**, preencha o seguinte:

    a. **Tipo de SQL Server**: especifique o tipo de comunicação que o aplicativo deve usar para se comunicar com o banco de dados do SQL Server.

       Local: especifique Local quando o aplicativo e o SQL Server estiverem instalados no mesmo computador.

       Remoto: especifique Remoto quando o aplicativo e o SQL Server estiverem instalados em computadores diferentes.

b. **Nome do SQL Server**: se o tipo do SQL Server for Remoto, especifique o nome do SQL Server remoto. Se o SQL Server for local, selecione o servidor na lista suspensa.

c. **Segurança**: especifique o tipo de credenciais que deseja usar para autenticar o SQL Server.

   Usar segurança do Windows: autentica usando suas credenciais do Windows. É possível efetuar logon usando as credenciais do console do Arcserve UDP.

   Usar segurança do SQL Server: autentica usando as credenciais do SQL Server. Insira a ID de logon e a senha para acessar a conta do SQL Server.

11. Clique em **Avançar**. A caixa de diálogo **Exceções do firewall** é exibida.

    A caixa de diálogo **Exceções do firewall** lista os serviços e programas a serem registrados no firewall do Windows como exceções para o Arcserve UDP.

    Observação: as exceções do firewall são necessárias caso você deseje configurar e gerenciar o Arcserve UDP a partir de computadores remotos.

12. Clique em **Avançar**. A caixa de diálogo **Mensagem** é exibida.

13. Clique em **Avançar**. A caixa de diálogo **Resumo** é exibida.

14. Clique em **Instalar** para iniciar o processo de instalação.

    A caixa de diálogo **Andamento da instalação** é exibida indicando o status da instalação. Quando a instalação for concluída, a caixa de diálogo **Relatório de instalação** é exibida.

    (Opcional) Se desejar verificar se há atualizações mais recentes do produto, siga estas etapas:

    a. Selecione **Verificar agora se há atualizações** e, em seguida, clique em **Concluir**.

       A caixa de diálogo **Verificar se há atualizações** é exibida.

    b. Selecione o servidor no qual deseja fazer o download de atualizações e clique em **Fazer download e instalar atualizações**.

       A caixa de diálogo **Processo de atualização** é exibida indicando o status do download.

       Quando a atualização for concluída, uma mensagem de alerta é exibida.

    (Opcional) Para instalar o agente do Arcserve UDP para Linux, siga a instrução na seção **Instalar o agente de Proteção de dados unificada do arcserve para Linux**.

15. Clique em **Concluir**.

    O Arcserve UDP foi instalado no computador.

Instalar o Arcserve Unified Data Protection usando a linha de comando

Você pode instalar o Arcserve Unified Data Protection de modo silencioso. O processo de instalação silenciosa elimina a necessidade de interação com o usuário. As etapas a seguir descrevem como instalar o aplicativo no modo silencioso usando a linha de comando do Windows.

Siga estas etapas:

1. Abra a linha de comando do Windows no computador onde deseja iniciar o processo de instalação silenciosa.
2. Faça download do pacote de instalação de autoextração para seu computador.

   Inicie o processo de instalação silenciosa usando a seguinte sintaxe da linha de 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>

   Exemplo:

   Arcserve_Unified_Data_Protection.exe -s -a -q -Products:Agent -User:administrator -Password:test
3. Configure a instalação silenciosa usando a sintaxe e os argumentos a seguir:

   Importante: se os parâmetros incluírem algum dos seguintes caracteres especiais, coloque os parâmetros entre aspas:

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

   Por exemplo: se a senha for abc^*123, a entrada deverá ser -Password:"abc^*123".

   s

   Executa o pacote de arquivo executável no modo silencioso.

   a

   Especifica quaisquer outras opções da linha de comando.

   -q

   Instala o aplicativo no modo silencioso.

   -Products:<ProductList>

(Opcional) Especifica os componentes que deseja instalar no modo silencioso. Se você não especificar um valor para esse argumento, o processo de instalação silenciosa instalará todos os componentes. É possível especificar os seguintes componentes:

Agente: instala o componente Agente de proteção de dados.

RPS: instala o componente Servidor do ponto de recuperação.

Console: instala o componente Console.

Tudo: instala todos os componentes do Arcserve Unified Data Protection.

Exemplo:

Para instalar o agente de proteção de dados:

-Products:Agent

Para instalar o servidor do ponto de recuperação:

-Products:Agent,RPS

Para instalar o agente de proteção de dados, o servidor do ponto de recuperação e o console de proteção de dados:

-Products:Agent,RPS,Console

Para Instalar todos os componentes na compilação:

-Products:All

-User:<UserName>

Especifica o nome de usuário que você deseja usar para instalar e executar o aplicativo.

Observação: o nome de usuário deve ser de administrador ou uma conta com privilégios administrativos.

-Password:<Password>

Especifica a senha do nome de usuário.

-Https:<HTTPS>

(Opcional) Especifica o protocolo de comunicação. As opções são 0 e 1. Use 0 para http e 1 para https.
Padrão: 0
Exemplo:

-https:1

-Path:<INSTALLDIR>

(Opcional) Especifica o caminho de instalação de destino do Agente de proteção de dados.

Exemplo:

-Path:C:\Program Files\Arcserve\Unified Data Protection

Observação: se o valor de INSTALLDIR contiver um espaço, coloque o caminho entre aspas. Além disso, o caminho não pode terminar com um caractere de barra invertida.

-ConsolePort:<Port Number>

(Opcional) Especifica o número da porta de comunicação para o console.

Padrão: 8015

Exemplo:

-ConsolePort:8015

Observação: use essa opção quando desejar instalar o Console.

-AgentPort:<Port Number>

(Opcional) Especifica o número da porta de comunicação para acessar o Agente do Arcserve Unified Data Protection.

Padrão: 8014

Exemplo:

-AgentPort:8014

Observação: use essa opção quando desejar instalar o Agente do Arcserve Unified Data Protection.

-Driver:<DRIVER>

(Opcional) Especifica se é preciso instalar o driver de rastreamento de alteração do Agente do Arcserve Unified Data Protection. As opções são 0 e 1.

0: não instala o driver
1: Instala o driver

Padrão:1

Exemplo:

-driver:1

-MonitorFlag:<MONITORFLAG>

(Opcional) Especifica o monitor do Agente do Arcserve Unified Data Protection a ser exibido para os usuários. As opções são 0 e 1.

0: exibe o monitor do agente para todos os usuários.
1: exibe o monitor do agente apenas para o usuário atual.

Padrão: 0.

Exemplo:

-MonitorFlag:0

-StopUA:< STOPUA >

(Opcional) Especifica se o serviço do agente universal do Arcserve deve ser interrompido.

0: não interrompe o serviço do agente universal do Arcserve se ele estiver em execução durante o processo de instalação.
1: interrompe o serviço do agente universal do Arcserve se ele estiver em execução durante o processo de instalação.
Padrão: 0

Exemplo:

-StopUA:1

Observação: use essa opção durante a atualização para uma nova versão. Verifique se você definiu o valor para 1 ou interrompa o serviço antes de iniciar o processo de atualização. Isso ajuda a garantir que a instalação não falhe.

-SummaryPath:<SUMMARYPATH>

(Opcional) Especifica o caminho de destino para gerar o arquivo de resumo da instalação.

Exemplo:

-SummaryPath:C:\Result

Observação: se o valor de SUMMARYPATH contiver um espaço, coloque o caminho entre aspas. Além disso, o caminho não pode terminar com um caractere de barra invertida.

-AutoReboot:<AUTOREBOOT>

(Opcional) Permite que o programa de instalação reinicialize o computador após a instalação se a instalação exigir uma reinicialização. As opções são 0 e 1.

0: não reinicializa o computador.

1: Reinicializa o computador se a instalação exigir uma reinicialização.

Padrão: 0

Exemplo:

-AutoReboot:1

Observação: se a instalação não exigir uma reinicialização, o programa de instalação não reiniciará o computador, mesmo se esse parâmetro estiver definido como 1.

Você concluiu a instalação silenciosa com êxito.

Instalar o Arcserve UDP usando o programa de instalação unificado

O Arcserve UDP permite instalar todos os seus componentes usando um único programa de instalação unificado. Com base em seus requisitos, o programa de instalação sugere a melhor licença para atender às suas necessidades e, em seguida, faz download e instala os componentes.

Siga estas etapas:

1. Faça download do arquivo ASDownloader no site do Arcserve.

   Observação: se um dos sistemas operacionais suportados que não estejam em inglês for detectado, você precisa selecionar o idioma para a instalação do produto.

2. Clique duas vezes no pacote de instalação.

   A caixa de diálogo do **Contrato de licença** será exibida.

3. Leia e aceite os termos do contrato de licença e clique em **Avançar**.

   A caixa de diálogo **Introdução** é aberta.

4. Clique em **Avançar**.

   A caixa de diálogo **Escolher os componentes a serem baixados** abre.

5. Selecione uma ou mais das opções a seguir, de acordo com suas necessidades, e clique em **Avançar**.

   Arcserve Unified Data Protection

   Instala o Arcserve UDP. O Arcserve UDP permite proteger nós físicos e virtuais do Windows e do Linux. É possível gerenciar todas as suas necessidades de proteção de dados em um único console. É possível usar a redução de redundância, a replicação, a replicação remota e outros recursos do lado da origem global para gerenciar os dados.

   Arcserve Backup

   Instala o Arcserve Backup. Quando utilizado em conjunto com o Arcserve UDP, é possível gerenciar o backup de fita do Console do Arcserve UDP e aproveitar todos os benefícios do Arcserve UDP.

   A caixa de diálogo **Download de produto** é exibida.

6. Clique em **Fazer download**.

   O download do produto começa a ser feito em um formato zip. É possível verificar o status do download na barra de andamento. Também é possível pausar e

retomar o download. Dependendo da largura de banda e do número de componentes para download, isso pode levar algum tempo.

Até que o download esteja concluído, o botão Avança fica inativo.

7. Quando o download for concluído, clique em **Avançar**.

   A caixa de diálogo **Método de instalação** abre.

8. Selecione um dos tipos de instalação.

   Instalação expressa

   Instala os componentes usando a configuração padrão. Clique em **Exibir componentes e configuração padrão** para verificar os componentes que serão instalados.

   Instalação avançada

   Permite instalar cada componente separadamente.

9. Clique em **Avançar**.

   A caixa de diálogo **Configuração de conta** abre.

10. Especifique o nome de usuário e a senha e clique em **Instalar**.

    A instalação é iniciada. É possível verificar o andamento na caixa de diálogo. Após a conclusão da instalação, feche o assistente.

    O Arcserve UDP foi instalado no computador.

Verificar a instalação

Siga estas etapas:

1. Verifique se o ícone do Arcserve UDP está exibido na bandeja do sistema.
2. Verifique se os serviços do servidor e do agente estão sendo executados a partir do Gerenciador de serviços do Windows.

   Você instalou com êxito o Arcserve Unified Data Protection e está pronto para fazer backup da máquina Windows.

Portas de comunicação usadas pelo Arcserve UDP

Esta seção fornece informações sobre as portas usadas para os seguintes componentes:

- Componentes instalados no Microsoft Windows
- Componentes instalados no Linux
- Componentes instalados no hipervisor

As portas listadas são necessárias para backup e outras tarefas quando você tiver um ambiente de LAN.

*Compartilhamento de porta é suportado para tarefas de replicação. Todos os dados nas portas diferentes podem ser encaminhados para a porta 8014 (porta padrão para o servidor de UDP, pode ser modificada durante a instalação). Quando uma tarefa de duplicação é executada entre dois servidores de ponto de recuperação na rede WAN, somente a porta 8014 precisa ser aberta.

Da mesma forma, para as replicações remotas, o administrador remoto precisa abrir ou encaminhar a porta 8014 (para replicação de dados) e a porta 8015 (porta padrão para o console de UDP, pode ser modificada durante a instalação) para que os servidores de ponto de recuperação local obtenham o plano de replicação designado.

Componentes instalados no Microsoft Windows

Esta seção fornece informações sobre as portas usadas no Console do UDP e o servidor de ponto de recuperação do UDP (RPS):

- Console do UDP
- RPS (Recovery Point Server - Servidor de Ponto de Recuperação) do UDP
- Agente do UDP Windows

Console do UDP

A tabela a seguir lista as portas usadas pelo Console do Arcserve UDP:

Número da porta	Tipo de porta	Iniciado por	Processo de escuta	Porta interna/externa	Descrição
1433	TCP	Java remoto	sqlsvr.exe	Externa	A porta padrão de comunicação entre o console de UDP e os bancos de dados do Microsoft SQL Server quando eles residem em computadores diferentes. **Observação:** é possível modificar a porta padrão de comunicação durante a instalação do SQL Server.
6052	TCP	Painel global do Arcserve Backup	Arcserve.CommunicationFoundation.WindowsService.exe	Externa	Comunicação que permite que o console do UDP e o Ser-

					vidor principal do painel global do Arcserve Backup sincronizem dados. **Observação:** essa porta só é necessária quando você deseja sincronizar os dados do painel global do Arcserve Backup com o console do UDP.
6054	TCP	Servidor principal do Arcserve Backup	Arcserve.CommunicationFoundation.WindowsService.exe	Externa	Comunicação que permite que o console e o servidor principal do Arcserve Backup sincronizem dados. **Observação:** essa porta só é necessária quando você deseja sincronizar os dados do painel global do Arcserve Backup

					com o console do UDP.
8012	TCP	Console do UDP	java.exe	Interna	Porta padrão internamente usada pelo serviço de identidade do console do UDP. **Observação:** não foi possível personalizar a porta e poderá ser ignorada na configuração do firewall. Se a porta 8012 estiver ocupada por outros programas, o programa de instalação do UDP atribuirá dinamicamente outra porta disponível.
8015	TCP	Console do UDP Gateway do UDP	httpd.exe	Externa	A porta de comunicação do HTTP/HTTPS padrão para se visitar o console do

					UDP e o gateway do UDP. **Observação:** é possível modificar a porta padrão de comunicação durante a instalação dos componentes de UDP.
8029	TCP	Console do UDP	tomcat9.exe	Interna	Porta padrão internamente usada pelo serviço de gerenciamento do console do UDP. **Observação:** não foi possível personalizar a porta e poderá ser ignorada na configuração do firewall. Se a porta 8029 estiver ocupada por outros programas, o programa de ins-

					talação do UDP atribuirá dinamicamente outra porta disponível.
8030	TCP	Console do UDP	tomcat9.exe	Interna	Porta padrão internamente usada pelo serviço de gerenciamento do console do UDP. **Observação:** não foi possível personalizar a porta e poderá ser ignorada na configuração do firewall. Se a porta 8030 estiver ocupada por outros programas, o programa de instalação do UDP atribuirá dinamicamente outra porta disponível.
18007	TCP	TOMCAT	tomcat9.exe	Interna	Internamente usado pelo serviço de

					gerenciamento do Tomcat. **Observação:** essa porta só pode ser alterada por meio da modificação dos arquivos de configuração do TOMCAT. Essa porta pode ser ignorada e pode ser ignorada na configuração do firewall.

RPS (Recovery Point Server - Servidor de Ponto de recuperação) do UDP

A tabela a seguir lista as portas usadas pelo RPS do Arcserve UDP:

Número da porta	Tipo de porta	Iniciado por	Processo de escuta	Porta interna/externa	Descrição
8014	TCP	UDP	httpd.exe	Externa	A porta de comunicação do HTTP/HTTPS padrão para se visitar o RPS do UDP e o agente do UDP. **Observações:** ▪ essa porta é a porta compartilhada padrão e a única porta que deve ser aberta quando você usar o RPS do UDP como o destino de replicação. Não abrir porta 5000-5060 usada por armazenamentos de dados com redução de redundância global ativada. ▪ é possível modificar a porta de comunicação padrão durante a instalação dos componentes do UDP.
8016	TCP	UDP	tomcat9.exe	Interna	Usado internamente pelos serviços web do RPS do UDP para a comunicação com o serviço de compartilhamento de porta do RPS do UDP no mesmo servidor. **Observação:** não foi possível personalizar a porta e poderá ser ignorada na configuração do firewall.
5000-5060	TCP	UDP	GDDServer.exe	Interna	Esse intervalo de portas está reservado para o serviço de repositório de dados de RPS do UDP. Um repositório de dados de redução de redundância de RPS do UDP usará 4 portas livres, já um repositório de dados de qualquer outro tipo usará 1 porta livre, ambos começando a partir da porta 5000. Isso é necessário quando o repositório de dados é processado para backup ou res-

					tauração. Se você usar o RPS como o destino de replicação, não é necessário para abri-lo na configuração do firewall. **Observação:** altere o seguinte para personalizar ao intervalo de portas no Registro: ■ HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\DataStore ▪ Nome da chave: PortRangeForGDD ▪ Tipo: Reg_SZ ▪ Valor padrão: 5000-5060 Somente o repositório de dados criado após as alterações de registro usará o intervalo de portas recentemente alterado.
18005	TCP	TOMCAT	tomcat9.exe	Interna	Para desligar o Tomcat utilizado pelo agente ou RPS do UDP. **Observação:** essa porta só pode ser alterada por meio da modificação dos arquivos de configuração do TOMCAT. Essa porta pode ser ignorada e pode ser ignorada na configuração do firewall
7788	TCP	UDP	Sync_util_d.exe	Interna	Porta padrão de comunicação HTTP/HTTPS para aceitar replicação em solicitações.
445	TCP			Externa	Usada pelo serviço SMB do sistema operacional Windows. A porta é usada quando o RPS hospeda o repositório de dados em um disco local. O repositório de dados expõe a pasta compartilhada como destino de backup para o agente do UDP fazer backup dos dados.

Agente do UDP Windows

A tabela a seguir lista as portas usadas pelo agente Arcserve UDP para Windows:

Número da porta	Tipo de porta	Iniciado por	Processo de escuta	Porta interna/externa	Descrição
8014	TCP	Agente do UDP Windows	tomcat9.exe	Externa	Porta de comunicação HTTP /HTTPS padrão para visitar RPS UDP e o agente UDP. **Observação:** é possível modificar a porta padrão de comunicação durante a instalação dos componentes de UDP.
18005	TCP	TOMCAT	tomcat9.exe	Interna	Para desligar o Tomcat utilizado pelo agente ou RPS do UDP. **Observação:** essa porta só pode ser alterada por meio da modificação dos arquivos de configuração do TOMCAT. Essa porta pode ser ignorada e pode ser ignorada na configuração do firewall.
4090	TCP	Agente do UDP Windows	HATransServer.exe	Externa	Para transferir dados para tarefas do Virtual Standby no modo de proxy. **Observação:** essa porta é necessária somente quando você especifica esse Agente Windows do UDP como Monitor do modo de espera virtual.
135	TCP			Externa	Porta de comunicação do serviço RPC no sis-

					tema operacional Windows. **Observação:** essa porta é necessária sempre que o console do UDP implanta remotamente o agente Windows do UDP para essa máquina do agente. Se o agente de UDP do Windows é instalado executando a instalação local, essa porta não é necessária.
445	TCP			Externa	Porta de comunicação do serviço SMB pata ativar a pasta compartilhada no sistema operacional Windows. **Observação:** essa porta é necessária sempre que o console do UDP implanta remotamente o agente Windows do UDP para essa máquina do agente. Se o agente de UDP do Windows é instalado executando a instalação local, essa porta não é necessária.

Componentes instalados no Linux

Esta seção fornece informações sobre as portas usadas no servidor de backup Linux e Nós do Linux protegidos pelo servidor de backup Linux remotamente.

Servidor de backup Linux

A tabela a seguir lista as portas usadas pelo servidor de backup Linux:

Número da porta	Tipo de porta	Iniciado por	Processo de escuta	Porta interna/externa	Descrição
67	UDP	UDP Linux	bootpd	Externa	Entrada, usada para o servidor de inicialização do PXE. Somente necessário se o usuário desejar usar o recurso de inicialização do PXE. **Observação:** esse número de porta não pode ser personalizado.
69	UDP	UDP Linux	tftpd	Externa	Entrada, usada para o servidor de inicialização do PXE. Somente necessário se o usuário desejar usar o recurso de inicialização do PXE. **Observação:** esse número de porta não pode ser personalizado.
8014	TCP	UDP Linux	java	Externa	Tanto de entrada quanto de saída. Porta de comunicação do HTTP/HTTPS padrão para se visitar o agente do UDP para Linux. **Observação:** é possível modificar a porta padrão de comunicação durante a instalação dos componentes de UDP.
8021	TCP	UDP Linux	cresvc	Externa	Entrada, usado para o serviço de backup.
18005	TCP	UDP Linux	java	Interna	Usado pelo Tomcat. Ignorar essa porta para a configuração do firewall. **Observação:** essa porta só pode ser alterada por meio da modificação dos arquivos

					de configuração do TOMCAT.
50000 ou 50000+	TCP	UDP Linux	ssh	Externa	Dependência de terceiros do UDP Linux. Necessária somente ao executar a BMR de migração do Linux da nuvem para o local. Uma porta disponível da porta 50000 é selecionada e usada. Por padrão, o UDP Linux abre a porta selecionada no sistema.
22	TCP	Serviço do SSH	sshd	Externa	Dependência de terceiros do UDP Linux. Padrão para o serviço de SSH; no entanto, é possível alterar essa porta. Essa porta é necessária para as comunicações de entrada e de saída.
8016	TCP	UDP Linux	d2ddss	Externa	Entrada, usada para o serviço de dados de VM ou BMR instantânea. Somente necessário se o usuário desejar usar o recurso de VM ou BMR instantânea.
111	TCP	Mapeador de porta	rpcbind	Externa	Dependência de terceiros do UDP Linux. Padrão para o mapeador de porta. Somente necessário durante a execução da VM instantânea do Linux a partir do ponto de recuperação de backup sem agente para o servidor vSphere ESX.
2049	TCP	Servidor NFS	nfsd	Externa	Dependência de terceiros do UDP Linux. Padrão para o servidor NFS. Somente necessário durante a execução da VM instantânea do Linux a partir do ponto de recuperação de backup sem agente para o servidor vSphere ESX.
Porta dinâmica	TCP	Serviço de montagem	rpc.mountd	Externa	Dependência de terceiros do

		do NFS			UDP Linux. Consulte a página principal do rpc.-mountd para saber como fazê-lo escutar a porta fixa. Somente necessário durante a execução da VM instantânea do Linux a partir do ponto de recuperação de backup sem agente para o servidor vSphere ESX.

Nós Linux protegidos remotamente pelo servidor de backup Linux

A tabela a seguir lista as portas usadas pelos nós Linux protegidos pelo Servidor de backup Linux remotamente:

Número da porta	Tipo de porta	Iniciado por	Processo de escuta	Porta interna/externa	Descrição
22	TCP	Serviço do SSH		Externa	Dependência de terceiros do UDP Linux. Padrão para o serviço de SSH; no entanto, é possível alterar essa porta. Essa porta é necessária para as comunicações de entrada e de saída.

Componentes instalados no hipervisor

Esta seção fornece informações sobre as portas usadas para host do Hyper-V:

Host do Hyper-V

A tabela a seguir lista as portas usadas pelo host do Hyper-V:

Número da porta	Tipo de port-a	Iniciado por	Processo de escuta	Interna/externa	Descrição
135	TCP			Externa	Usada pelo serviço WMI do sistema operacional Windows. O UDP usa a WMI para interagir com o host do Hyper-V em algumas situações.
445	TCP			Externa	Usada pelo serviço SMB do sistema operacional Windows. O UDP usa a SMB para interagir com o host do Hyper-V em algumas situações.
27000	TCP	Serviço CBT do UDP	cbt_ rep.exe	Externa	Usada pelo serviço CBT de backup com base no host UDP. Não é preciso registrar essa porta para a exceção do firewall porque o UDP registra essa porta automaticamente durante o backup. É necessário verificar se nenhum outro aplicativo está configurado com a mesma porta.
5895 ou 5986	TCP	Serviço WinRM		Externa	5895 para WinRM no protocolo HTTP, 5896 para WinRM no protocolo HTTPS. Apenas uma delas é necessária. Somente necessária durante a execução da VM instantânea do Linux no Hyper-V.
1024 ~ 65535	TCP			Externa	▪ Usado ao importar VMs do host do Hyper-V e/ou do agrupamento para o plano de backup. ▪ Por padrão, a tarefa de restauração de VM escolhe aleatoriamente uma porta disponível no inter-

					valo entre 1024 e 65535. Você pode especificar manualmente o intervalo pelos valores do registro definidos no host do Hyper-V. Para obter mais informações, consulte o link.

Como o processo de instalação afeta os sistemas operacionais

Os seguintes processos de instalação atualizam vários sistemas operacionais Windows:

- Instalação de arquivos binários não assinados
- Instalação de arquivos binários com versão incorreta do arquivo
- Instalação de arquivos binários sem SO no manifesto

Instalação de arquivos binários não assinados

Nome do arquivo binário	Origem	Nome do arquivo binário	Origem
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

Instalação de arquivos binários com versão incorreta do arquivo

Nome do arquivo binário	Origem	Nome do arquivo binário	Origem
AxShockwaveFlashObjects.dll	Adobe	libisccfg.dll	bind
ShockwaveFlashObjects.dll	Adobe	liblwres.dll	bind
openssl.exe	Apache	libxml2.dll	bind
UpdateData.exe	Licenciamento do 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		

Instalação de arquivos binários sem SO no manifesto

Nome do arquivo binário	Origem
openssl.exe	Apache
win _nsupdate.exe	bind
plink.exe	putty
sqlite3.exe	sqlite
vddkReporter.exe	VMware

Configuração do antivírus

O software de antivírus pode interferir na execução adequada do agente do Arcserve UDP (Windows) por meio do bloqueio temporário do acesso aos arquivos ou da quarentena ou exclusão de arquivos que são classificados incorretamente como suspeitos ou perigosos. É possível configurar um software antivírus para excluir arquivos ou pastas e evitar gastar tempo com a verificação de dados que não precisam ser protegidos.

A configuração adequada de seu software antivírus é necessária para excluir o destino do backup. Uma configuração correta permite evitar interferências nas operações de backup e restauração ou em quaisquer outros processos, como mesclagem e geração de catálogo.

Caminhos a serem excluídos da verificação do antivírus:

Verificação do antivírus para	Caminhos a serem excluídos
RPS	Pasta do repositório de dados Caminho de destino de dados Caminho de destino do índice Caminho de destino de hash
Agente do Windows não gerenciado pelo console	Destino do backup

Como instalar atualizações do Arcserve UDP

O processo para obter e instalar atualizações do Arcserve UDP tem duas partes, que envolvem verificar e fazer download da atualização e, em seguida, instalar a atualização.

Observação: todas as atualizações liberadas para o Arcserve UDP são cumulativas. Como resultado, cada atualização também incluirá todas as atualizações lançadas anteriormente para garantir que o computador esteja sempre atualizado. A caixa de diálogo **Ajuda sobre** exibe o nível de atualização instalado no computador. Se necessário, é possível usar essas informações para criar outro servidor com o mesmo nível de configuração/patch.

Execute as seguintes tarefas para instalar as atualizações do Arcserve UDP:

1. Analisar as considerações para a instalação de atualizações
2. Especificar Preferências de atualização
3. Verificar e instalar as atualizações
4. (Opcional) Instalar atualizações do Arcserve UDP no modo silencioso
5. Verifique se as atualizações foram instaladas com êxito

Analisar as considerações para a instalação de atualizações

Verifique as seguintes considerações antes de instalar as atualizações Arcserve UDP:

- Ao instalar uma atualização do Arcserve UDP ou uma atualização do Agente do Arcserve Unified Data Protection para Windows, é importante manter um desempenho ideal entre o Console, o RPS (Recovery Point Server - Servidor de Ponto de Recuperação) e os Agentes. Como resultado, quando a atualização é instalada em um ambiente que contém um console e um agente, você sempre deve instalar a atualização primeiro no console e, em seguida, no RPS e, finalmente, no agente. (Para o agente instalado no console ou no RPS, a atualização será instalada automaticamente nesse agente ao mesmo tempo).
- Se necessário, faça download das atualizações disponíveis do Arcserve diretamente em uma máquina cliente ou, primeiro, em um servidor de armazenamento temporário e, depois, em uma máquina cliente.
- Se necessário, use o nó da estação de trabalho como um servidor de armazenamento temporário para fazer download das atualizações do Arcserve UDP.
- Verifique se as configurações de preferência da Atualização estão definidas corretamente.
  - É possível instalar as atualizações por meio da interface de usuário ou no modo silencioso usando a linha de comando.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

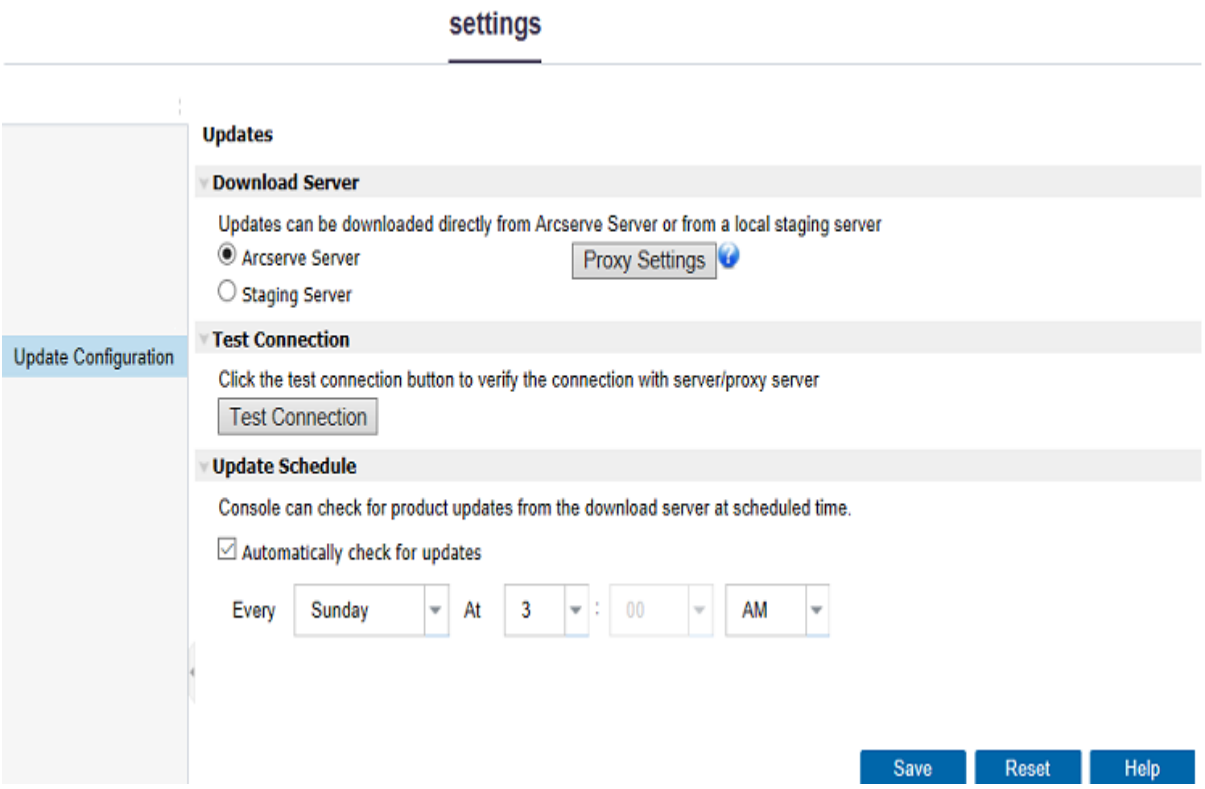
Especificar as preferências de atualizações

Usando o Arcserve UDP, é possível especificar as preferências de atualizações.

Siga estas etapas:

1. No Console do Arcserve UDP, clique na guia **Configurações**.
2. No painel à esquerda, clique em **Atualizar configuração**.

   A página **Atualizações** é exibida no painel direito.



3. Especifique as configurações de preferência das **Atualizações**.

   Servidor de download

   Especifica o servidor de origem ao qual seu servidor do Arcserve UDP se conectará e de onde deverá fazer download das atualizações disponíveis.

   - **Arcserve Servidor**

     Especifica que as atualizações são baixadas do servidor do Arcserve diretamente para o servidor local.

     Essa é a configuração padrão.

   - **Servidor de armazenamento temporário**

Especifica que as atualizações são baixadas do servidor de armazenamento temporário.

Observação: se necessário, você pode criar um servidor de armazenamento temporário. Para obter mais informações, consulte Como criar um servidor de armazenamento temporário.

Se você especificar mais de um servidor de armazenamento temporário, o primeiro servidor listado será designado como o servidor principal de armazenamento temporário. O Arcserve UDP tentará inicialmente se conectar ao servidor principal de armazenamento temporário. Se o primeiro servidor listado não estiver disponível, o próximo servidor listado se tornará o servidor de armazenamento temporário principal. A mesma sequência será seguida até que o último servidor listado se torne o servidor de armazenamento temporário principal. (A lista de servidores de armazenamento temporário está limitada ao máximo de 5 servidores).

- É possível usar os botões **Mover para cima** e **Mover para baixo** para alterar a sequência de servidores de armazenamento temporário.
- É possível usar o botão **Excluir** para remover um servidor desta listagem.
- É possível usar o botão **Adicionar servidor** para adicionar um novo servidor a esta listagem. Ao clicar no botão **Adicionar servidor**, a caixa de diálogo **Servidor de armazenamento temporário** é exibida, permitindo especificar o nome do servidor de armazenamento temporário adicionado.

Quando seleciona o servidor de armazenamento temporário como o servidor de download:

- Se o servidor de armazenamento temporário especificado tiver alguma atualização, o console do Arcserve UDP poderá obter atualizações desse servidor de armazenamento temporário.
- Se o servidor de armazenamento temporário especificado não tiver nenhuma atualização, o console do Arcserve UDP não poderá fazer o download das atualizações desse servidor de armazenamento temporário. O log exibirá a seguinte mensagem:

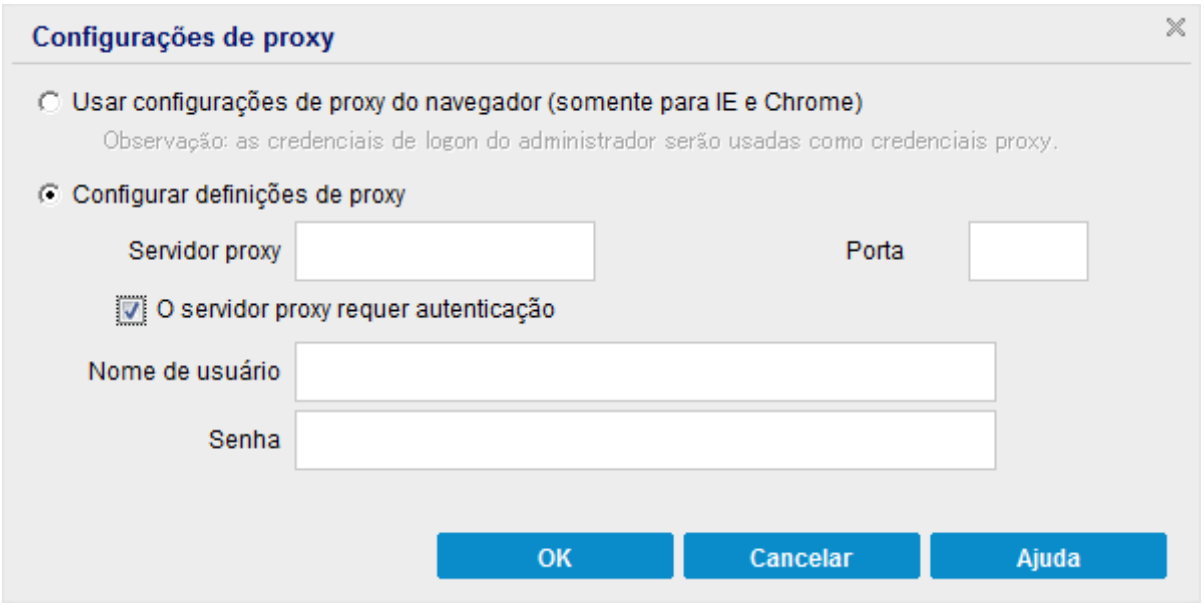
  Não há novas atualizações disponíveis.

- **Configurações de proxy**

  Observação: essa opção de **Servidor proxy** só é disponibilizada quando você seleciona o servidor da Arcserve como servidor de download.

  Selecione Configurações de proxy

Ao selecionar esta opção, a caixa de diálogo **Configurações de proxy** é aberta.



Usar configurações de proxy do navegador

Esta seleção é aplicável somente ao Windows Internet Explorer e Google Chrome.

Quando selecionada, direciona o Arcserve UDP para detectar automaticamente e usar as mesmas configurações de proxy aplicáveis ao navegador, com o objetivo de se conectar ao servidor do Arcserve para obter informações sobre atualizações do Arcserve UDP.

Definir configurações de proxy

Quando selecionada, permite que o servidor proxy especificado se conecte ao servidor do Arcserve para obter informações sobre atualizações do Arcserve UDP. Caso selecione esta opção, será necessário incluir também o endereço IP (ou nome do computador) do servidor proxy e o número da porta correspondente, usado pelo servidor proxy em conexões com a internet.

Além disso, você também pode especificar se o servidor proxy requer autenticação. Quando selecionado, especifica que as informações de autenticação (ID e senha do usuário) são obrigatórias para usar o servidor proxy.

Observação: o formato do nome de usuário deve corresponder a um nome de usuário de domínio totalmente qualificado na forma <nome de domínio>\<nome de usuário>.

Testar conexão

Permite que você teste as seguintes conexões e exiba uma mensagem de status quando concluído:

- Caso tenha selecionado o "Servidor do Arcserve" como o servidor de download, teste a conexão entre o computador e o servidor do Arcserve por meio do servidor proxy especificado.
- Se selecionou "Servidor de armazenamento temporário" como o servidor de download, testa a conexão entre o computador e o servidor de armazenamento temporário. O botão Testar conexão é usado para testar a disponibilidade de cada servidor de armazenamento temporário listado e um status correspondente é exibido no campo **Status de conexão**. Se nenhum dos servidores de armazenamento temporário configurados estiver disponível, a seguinte mensagem será exibida na parte superior do console do Arcserve UDP: Servidor de atualização indisponível.

  Observação: a conexão de teste é executada automaticamente quando você abre a página **Atualizar configuração** da guia **Configurações** no console do Arcserve UDP. Quando esse teste automático for executado, ele verificará o status da conexão mais recente do servidor de download configurado anteriormente (o servidor do Arcserve ou servidores de armazenamento temporário, aquele que estiver selecionado). Caso tenha configurado anteriormente mais de um servidor de armazenamento temporário, esse teste automático será executado em todos os servidores de armazenamento temporário para obter o status de conexão mais recente.

Programação de atualizações

Especifica quando verificar (e fazer download) novas atualizações do Arcserve UDP.

4. Clique em **Salvar**.

   As configurações das preferências sobre atualizações são salvas.

Como criar um servidor de preparo

O servidor de armazenamento temporário é um nó no qual o agente ou o console Arcserve UDP está instalado. O nó precisa concluir o download das atualizações do servidor de download Arcserve para funcionar como um servidor de armazenamento temporário para fornecer atualizações para outras pessoas.

Adição de um servidor de armazenamento temporário:

Você pode adicionar o servidor de armazenamento temporário em qualquer nó que atenda os dois requisitos a seguir:

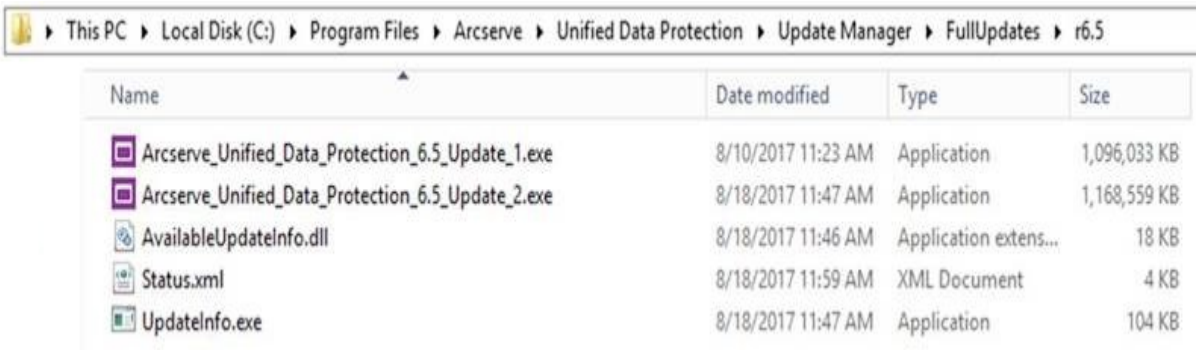
- O nó tem um agente do Arcserve UDP ou console do Arcserve UDP instalado.
  - O console do Arcserve UDP só pode fazer download das atualizações a partir do servidor de armazenamento temporário do console.
  - O agente do Arcserve UDP pode fazer download das atualizações a partir do servidor de armazenamento temporário do console ou do agente.
- O nó baixou com êxito as atualizações do servidor de download da Arcserve pelo menos uma vez.

Observação: outra configuração não é necessária se o servidor de armazenamento temporário de destino atender aos pré-requisitos.

Configurar a atualização do servidor de armazenamento temporário

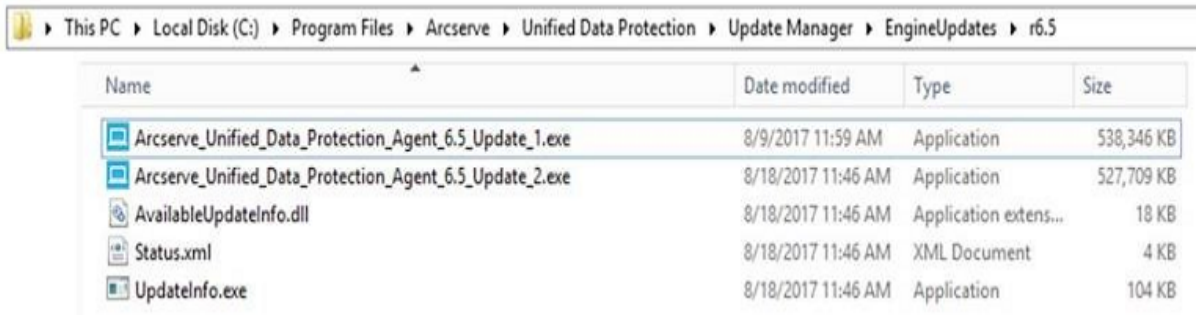
- Quando o servidor de armazenamento temporário é selecionado pelo console do Arcserve UDP instalado nesse nó, considere as seguintes observações:
  - Porta padrão: 8015
  - O console do Arcserve UDP pode obter atualizações deste servidor de armazenamento temporário
  - O agente do Arcserve UDP pode obter atualizações deste servidor de armazenamento temporário

  Observação: no diretório <UDP Installed path\Update Manager\FullUpdates> no servidor de armazenamento temporário de destino, verifique a versão de atualização mais recente disponível. Veja o exemplo abaixo.



- Quando o servidor de armazenamento temporário é selecionado pelo agente do Arcserve UDP instalado nesse nó, considere as seguintes observações:
  - Porta padrão: 8014
  - O console do Arcserve UDP não pode obter atualizações deste servidor de armazenamento temporário
  - O agente do Arcserve UDP pode obter atualizações deste servidor de armazenamento temporário

  Observação: no diretório <UDP Installed path\Update Manager\EngineUpdates> no servidor de armazenamento temporário de destino, verifique a versão de atualização mais recente disponível. Veja o exemplo abaixo.



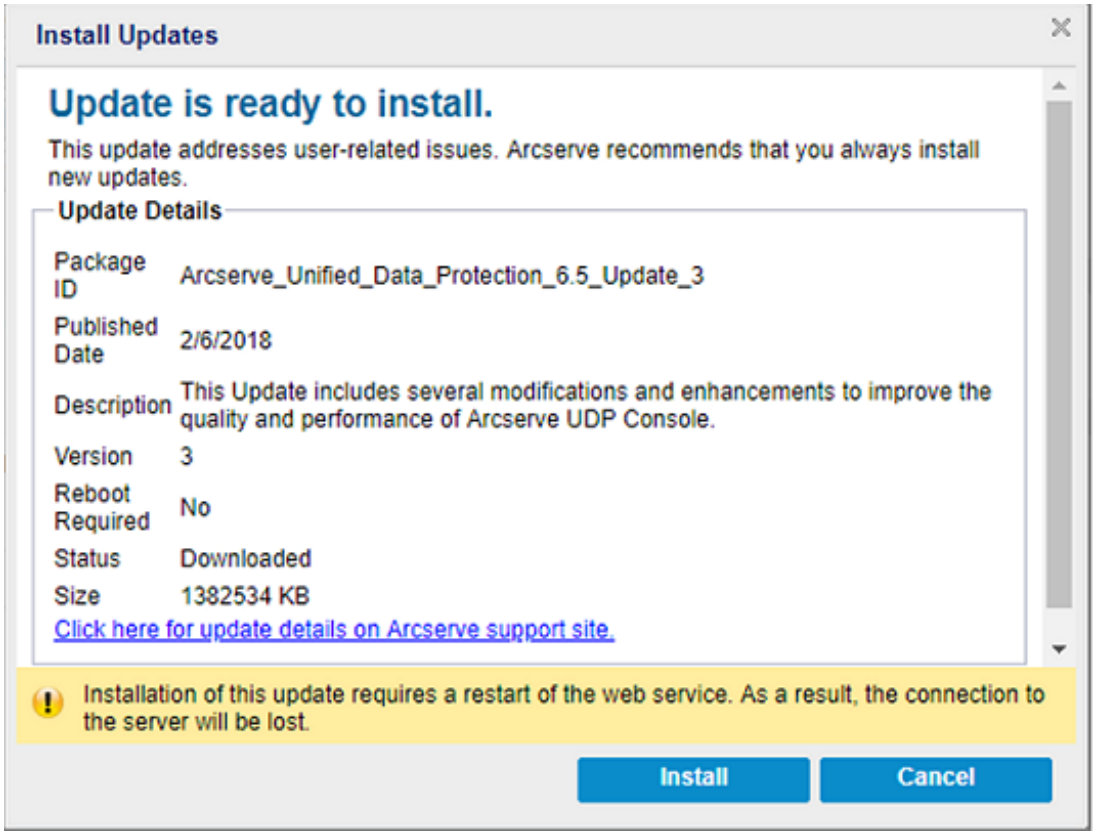
Verificar e instalar as atualizações

No Console da UDP, é possível determinar se novas atualizações estão disponíveis.

Siga estas etapas:

1. Clique em **Verificar se há atualizações** no menu suspenso **Ajuda.** Quando uma nova atualização estiver disponível, uma mensagem é exibida na parte superior. Além disso, a caixa de diálogo **Instalação da atualização** será exibida.
2. Se ativar a programação de atualizações e sempre que uma nova atualização estiver disponível, o download será feito automaticamente para o servidor da UDP. Um link **Nova atualização disponível** é exibido na barra superior para fornecer uma indicação visual de que uma nova atualização está pronta para ser instalada.
3. Clique no link **Nova atualização disponível** na barra superior.

   A caixa de diálogo **Instalar atualizações** é aberta para exibir as informações relacionadas à atualização disponível. A caixa de diálogo inclui informações como descrição, status de download, tamanho, requisito de reinicialização e um link para o servidor do Arcserve para obter mais detalhes sobre a atualização.



4. Clique em **Instalar**.

   A instalação das atualizações do Arcserve UDP é iniciada.

Atualizar agentes em nós remotos usando um gateway

O servidor e os nós remotos em um site interagem com o Console usando um gateway. Usando o Arcserve UDP, você pode detectar e implantar a versão mais recente do agente aos nós. Para atualizar ou instalar o Agente do Arcserve UDP em um nó no site, use Instalar/atualizar agente.

Siga estas etapas:

1. Clique na guia de **recursos** no Console.
2. No painel esquerdo **Navegação**, selecione um site na lista suspensa.
3. A página **Nós: Todos os nós** é exibida.
4. Selecione um ou mais nós.
5. No painel central, clique na lista suspensa **Ações** e, em seguida, clique em **Instalar/atualizar o agente**.

   Os detalhes de Instalar ou atualizar são exibidos no painel central.
6. Verifique os detalhes e clique em **OK**.

   O nó é instalado ou atualizado com a versão mais recente do agente do Arcserve UDP.

Atualizar o RPS no servidor remoto usando o gateway

O servidor e os nós remotos em um site interagem com o console usando um gateway. Usando o Arcserve UDP, é possível detectar e implantar a versão mais recente do componente RPS para servidores de ponto de recuperação. Depois de implantar o componente RPS, o servidor está pronto para armazenar as sessões de backup e servir como um servidor do ponto de recuperação. Para atualizar ou instalar o componente RPS do Arcserve UDP em servidores de um ponto de recuperação em um site, use instalar/atualizar servidor do ponto de recuperação.

Siga estas etapas:

1. Clique na guia de **recursos** no Console.
2. No painel esquerdo **Navegação**, selecione um site na lista suspensa.
3. Clique em **Servidores do ponto de recuperação**.

   A página **Destino:** a página do **Servidor de ponto de recuperação** é exibida.
4. Execute uma das seguintes ações:
   - Clique com o botão direito do mouse em um servidor de ponto de recuperação.
   - Selecione um servidor do ponto de recuperação e, no painel central, clique no menu suspenso **Ações**.

   Uma lista de opções é exibida.
5. Clique em **Instalar/atualizar o servidor de ponto de recuperação**.

   A página **Instalação e atualização** é exibida.
6. Modifique as configurações de implantação e clique em **OK** para implantar o servidor do ponto de recuperação para o nó selecionado.

   A implantação do servidor do ponto de recuperação é iniciada. É possível ver o andamento da implantação no painel direito.

(Opcional) Instalar atualizações do Arcserve UDP no modo silencioso

A instalação silenciosa de atualizações permite executar uma instalação autônoma e não requer nenhuma ação.

Siga estas etapas:

1. Inicie a instalação silenciosa da atualização do Arcserve UDP.

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

2. Configure a instalação silenciosa usando a sintaxe e os argumentos a seguir:

   UpdateExeFile

   Especifica para executar o pacote de arquivo executável.

   s

   Especifica para executar o pacote de arquivo executável usando o modo silencioso.

   v

   Especifica os argumentos adicionais para a instalação da atualização.

   Argumentos adicionais

   /s

   Especifica para executar a instalação de atualizações usando o modo silencioso.

   /AutoReboot

   Especifica a execução de uma reinicialização automática após a instalação da atualização. Se for necessária uma reinicialização para concluir a atualização, o computador será reiniciado automaticamente sem nenhuma notificação.

   ### Exemplos

   - Para instalar uma atualização usando o modo silencioso e reinicializar automaticamente após a conclusão, use o seguinte comando:

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

   - Para instalar uma atualização usando o modo silencioso e não reinicializar automaticamente após a conclusão, use o seguinte comando:

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

Verifique se as atualizações foram instaladas com êxito

No Console do Arcserve UDP, selecione **Ajuda**, clique em **Sobre** e, em seguida, verifique se a caixa de diálogo do Arcserve UDP exibe a versão mais atualizada.

Como desinstalar o Arcserve UDP

É possível desinstalar o Arcserve Unified Data Protection usando os seguintes métodos:

- **Desinstalação padrão**: use esse método para desinstalar usando o Painel de controle do Windows.
- **Desinstalação silenciosa**: use esse método para executar uma desinstalação autônoma usando a linha de comando do Windows.

Desinstalação padrão

É possível desinstalar os seguintes componentes.

- Console do Arcserve Unified Data Protection
- Servidor do ponto de recuperação do Arcserve Unified Data Protection
- Agente do Arcserve Unified Data Protection

Siga estas etapas:

1. Abra o Painel de Controle do Windows.
2. Clique em desinstalar um programa.

   A caixa de diálogo Desinstalar ou alterar um programa é aberta.
3. Selecione Arcserve Unified Data Protection e clique em Desinstalar.

   A caixa de diálogo Desinstalar aplicativo do Arcserve Unified Data Protection é exibida.
4. Selecione os componentes que deseja desinstalar e clique em Avançar.

   A caixa de diálogo **Mensagens** é exibida.
5. Clique em Avançar.

   A caixa de diálogo **Remover componentes** é exibida.
6. Clique em **Remover**.

   Os componentes selecionados são desinstalados do computador.

Desinstalação silenciosa

O processo de desinstalação silenciosa elimina a necessidade de interação do usuário durante a desinstalação.

Siga estas etapas:

1. Efetue logon no computador para desinstalar os componentes do Arcserve UDP.

   Observação: efetue logon no computador usando uma conta administrativa.

2. Abra a linha de comando do Windows e execute o seguinte comando que corresponde ao sistema operacional especificado:

   - **Sistema operacional x86:**

     Para desinstalar todos os componentes

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

     Para desinstalar os componentes selecionados

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

   - **Sistema operacional x64:**

     Para desinstalar todos os componentes

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

     Para desinstalar os componentes selecionados

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

   Os valores a seguir explicam os códigos de retorno:

   0 = a desinstalação foi realizada com êxito.

   3010 = a desinstalação foi realizada com êxito, mas é necessário reinicializar.

   Outros = falha na desinstalação.

   Utilização:

   A tabela abaixo define o código do produto que deve ser especificado para o componente do Arcserve Unified Data Protection que deseja desinstalar.

   Exemplo:

   A sintaxe a seguir permite desinstalar o servidor do ponto de recuperação do Arcserve Unified Data Protection no modo silencioso.

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

Componente	<Código do produto>
Agente do Arcserve Unified Data Protection (plataformas x86)	{CAAD8AEA-A455-4A9F-9B48-C3838976646A}
Agente do Arcserve Unified Data Protection (plataformas x64)	{CAAD1E08-FC33-462F-B5F8-DE9B765F2C1E}
Arcserve Unified Data Protection Servidor do ponto de recuperação	{CAAD8172-1858-4DC7-AE81-C887FA6AFB19}
Arcserve Unified Data Protection Console	{CAAD3E40-C804-4FF0-B1C0-26D534D438C0}
Arcserve Unified Data Protection Gateway	{FB95E75D-494F-4146-9B35-F867434B264A}

Depois que o comando for executado, os componentes do Arcserve UDP são desinstalados.

Remover componentes ignorados pelo programa de desinstalação

Importante:

1. o licenciamento da Arcserve é compartilhado por todos os produtos da Arcserve. Verifique se não há nenhum outro produto Arcserve instalado em seu computador; caso contrário, você poderá perder a licença de todos os produtos da Arcserve instalados no computador.
2. Se os componentes forem removidos, quaisquer programas instalados após o Agente do Arcserve Unified Data Protection para Windows e dependentes desses componentes poderão não funcionar corretamente.

   Se deseja remover manualmente esses componentes, execute as seguintes etapas:

   Remover o componente de licenciamento da Arcserve manualmente

1. Vá para o diretório *C:\Arquivos de programas (x86)\Arcserve\SharedComponents\CA_LIC*.
2. Localize o arquivo zip denominado *lic98_uninstaller.zip* e descompacte o arquivo para algum outro local (por exemplo: C:\temp).
3. Vá para o local onde os arquivos foram extraídos e localize dois arquivos de script que são denominados *rmlic.exe* e *rmlicense.bat*.
4. Clique em *rmlicense.bat* para executar o script que desinstala os componentes.
5. Exclua manualmente as seguintes pastas:
   - C:\Arquivos de programas (x86)\Arcserve
   - C:\Arquivos de programas\Arcserve
   - Pasta onde você extraiu o arquivo zip.
6. ArcserveRemova a chave do registro do componente de licenciamento da .
   - Para a plataforma x64: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Arcserve\License
   - Para a plataforma x86: HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\License

   Remover o Microsoft Visual C + + e o Microsoft SQL Server Express manualmente

1. Acesse o aplicativo padrão Adicionar ou remover programas localizado no Painel de controle do Windows (Painel de controle, Programas e Recursos, Remover Programas).

2. Selecione *Microsoft Visual C++ 2013 redistribuível (x86) - 12.0.30501* e clique em Desinstalar.
3. Selecione *Microsoft Visual C++ 2013 redistribuível (x64) - 12.0.30501* e clique em Desinstalar.
4. Selecione Microsoft SQL Server 2014 (64 bits) e clique em Desinstalar.
5. Para remover somente o banco de dados do Arcserve UDP, selecione "ARCSERVE_APP" e clique em Desinstalar.

Capítulo 4: Atualizar para o Arcserve UDP versão 8.0

Esta seção contém os seguintes tópicos:

Observação: para obter as práticas recomendadas sobre como proteger o servidor do Arcserve UDP, consulte Proteger o servidor do Arcserve UDP.

Versões com suporte para atualização

O Arcserve UDP 8.1 oferece compatibilidade com versões anteriores e atualizações, de acordo com as seguintes regras:

- O Arcserve UDP 8.1 oferece suporte à atualização do Arcserve UDP versão 8.0, 7.0, Atualização 2, 7.0, Atualização 1, 7.0, versão final e do Arcserve UDP versão 6.5, Atualização 4.

  Observações: antes de atualizar para o Arcserve UDP 8.1 a partir de outras versões anteriores, considere o seguinte:

  - No Arcserve UDP 6.5 com Atualização 3, Atualização 2, Atualização 1 ou versão final, primeiro atualize para o UDP 6.5, Atualização 4.
  - No Arcserve UDP versão 6.0, Atualização 3, para Windows, primeiro atualize para o Arcserve UDP versão 7.0.
  - No Arcserve UDP versão 6.0, Atualização 2, Atualização 1 ou versão final para Windows, primeiro atualize para o Arcserve UDP versão 6.5, Atualização 4.
  - No Arcserve UDP versão 6.0, Atualização 1, ou versão final para Linux, primeiro atualize para o Arcserve UDP versão 6.5, Atualização 4.
  - No Arcserve UDP versão 5.0, Atualização 4, primeiro atualize para o UDP 6.5, Atualização 4.
  - No Arcserve UDP 5.0 com Atualização 3, Atualização 2, Atualização 1, ou versão final, primeiro atualize para o UDP 6.0, Atualização 3 e, em seguida, atualize para o UDP 7.0.

- O Arcserve UDP 8.1 não oferece suporte à atualização do Arcserve D2D r16.5, do Arcserve Central Protection Management r16.5, do Arcserve Data Protection Console r16.5, do Arcserve Central Reporting r16.5 e do Arcserve Central Virtual Standby r16.5.

  Para obter mais informações, consulte Como atualizar a licença do Arcserve UDP.

Sequência de atualização do Arcserve Appliance

O Arcserve Versão 8.0 oferece suporte à atualização no UDP Appliance. A atualização pode envolver uma das sequências a seguir:

- Atualizar o Arcserve UDP
  - Atualizar o Arcserve Appliance que é executado como console e RPS do Arcserve UDP
  - Atualizar o Arcserve Appliance que é executado somente como RPS do Arcserve UDP
  - Atualizar etapas quando dois ou mais appliances do Arcserve são usados no ambiente
- Atualizar o agente para Linux do Arcserve no Arcserve UDP Appliance
- Atualizar o Arcserve Backup no Arcserve Appliance

Atualizar o appliance do Arcserve que é executado como console e RPS do Arcserve UDP

Atualize o appliance do Arcserve e siga a sequência de atualização descrita para atualizar o ambiente.

Atualizar o appliance do Arcserve que é executado somente como RPS do Arcserve UDP

Atualize o ambiente produtivo completo. Para obter mais informações, consulte a sequência de atualização.

Atualizar etapas quando dois ou mais appliances do Arcserve são usados no ambiente

Atualize o ambiente produtivo completo. Para obter mais informações, consulte a sequência de atualização.

Atualizar o agente do Arcserve para Linux no appliance do Arcserve UDP

1. Atualize o console do Arcserve UDP que gerencia o ambiente do servidor de backup Linux.
2. Atualize o servidor de backup Linux no appliance do Arcserve. Para obter detalhes, consulte a *Ajuda online do agente do Arcserve Unified Data Protection para Linux*.

Atualizar o Arcserve Backup no appliance do Arcserve

Consulte o *Guia de Implementação do Arcserve Backup* para realizar a atualização no appliance do Arcserve.

Diretiva suporte à compatibilidade com versões anteriores

Recomendamos atualizar todos os componentes para o Arcserve UDP 8.1 em todo o ambiente, para que os novos recursos do Arcserve UDP 8.1 possam ser explorados. Os planos de backup existentes não são afetados se a atualização não for concluída para todos os componentes ao mesmo tempo.

A compatibilidade com versões anteriores oferece suporte ao Arcserve UDP versão 8.0, 7.0, 7.0 Atualização 1, 7.0 Atualização 2 e ao Arcserve UDP 6.5 Atualização 4.

Esta seção contém os seguintes tópicos:

Diretiva de suporte à compatibilidade com versões anteriores do Arcserve UDP 8.0

Suporte à compatibilidade com versões anteriores entre diferentes consoles do UDP por meio da tarefa Replicar para um RPS gerenciado remotamente

Caso você esteja planejando executar a tarefa *Replicar para um RPS gerenciado remotamente*, é recomendável atualizar o console e o RPS no destino antes de atualizar o console/RPS/agente na origem.

- A replicação terá suporte se o RPS de origem tiver o UDP 8.1 e o RPS de destino ainda tiver o UDP versão 8.0, 7.0, 7.0 Atualização 1 e 7.0 Atualização 2.
- A replicação terá suporte se o RPS de origem tiver o UDP versão 8.0, 7.0, 7.0 Atualização 1 e 7.0 Atualização 2, e o RPS de destino tiver o UDP 8.1.
- Comportamentos de replicação:
  - Se você atualizar para o UDP 8.1 nos dois sites, será possível replicar do Cloud Hybrid para o local sem um IP público (novo comportamento do UDP).
  - Se você fizer a atualização para o UDP 8.1 apenas em um dos sites e o outro site usar uma versão com suporte do UDP, será possível replicar do Cloud Hybrid para o local usando o IP público.

Suporte à compatibilidade com versões anteriores do Windows RPS/Agente (ou proxy de backup sem agente)

- O console do Arcserve UDP 8.1 oferece suporte aos RPSs e agentes (ou proxies de backup sem agente) do UDP versão 8.0, 7.0, 7.0 Atualização 1 e 7.0 Atualização 2, para backup, caso o plano não seja alterado após uma atualização.

- O console do Arcserve UDP 8.1 e o RPS oferecem suporte a agentes (ou proxies de backup sem agente) do UDP versão 8.0, 7.0, 7.0 Atualização 1 e 7.0 Atualização 2, para backup, caso o plano não seja alterado após uma atualização.
- O console do Arcserve UDP 8.1 oferece suporte à implantação do plano existente sem alterações quando o RPS e os agentes (ou proxies de backup sem agente) ainda estão sendo executados no UDP versão 8.0, 7.0, 7.0 Atualização 1 e 7.0 Atualização 2. O agente não é atualizado automaticamente.
- O console do Arcserve UDP 8.1 oferece suporte a ações como pausar ou retomar o plano existente sem alterações quando o RPS e os agentes (ou proxies de backup sem agente) ainda estão sendo executados no UDP versão 8.0, 7.0, 7.0 Atualização 1 e 7.0 Atualização 2. O agente não é atualizado automaticamente.
- O console do Arcserve UDP 8.1 oferece suporte à criação de um novo plano ou à modificação do plano existente para configurar recursos herdados que já eram suportados na release anterior, quando o RPS e os agentes (ou proxies de backup sem agente) ainda estavam sendo executados no UDP versão 8.0, 7.0, 7.0 Atualização 1 e 7.0 Atualização 2. O agente não é atualizado automaticamente.
- O console do Arcserve UDP 8.1 oferece suporte à criação de um novo plano ou à modificação do plano existente para incluir os novos recursos do UDP 8.1 quando o RPS, o proxy ou o agente associado já tiver sido atualizado para a versão esperada.

  Por exemplo:

  - É possível especificar a rede para backup quando o console, o RPS, o proxy e o agente forem atualizados para o UDP 7.0, 7.0 Atualização 1, 7.0 Atualização 2, 8.0 ou 8.1.
- O console do Arcserve UDP 8.1 oferece suporte à atualização do nó quando o RPS e os agentes (ou proxies de backup sem agente) ainda estão sendo executados no UDP versão 8.0, 7.0, 7.0 Atualização 1 e 7.0 Atualização 2. O plano será implantado. O agente não é atualizado automaticamente.
- O console do Arcserve UDP 8.1 oferece suporte à adição de um servidor RPS na versão 8.0. Mas o RPS não é atualizado automaticamente para o Arcserve UDP versão 8.1 quando adicionado.
- O console do Arcserve UDP 8.1 oferece suporte à adição de uma versão anterior do agente (ou proxy de backup sem agente) sem atualizar o agente automaticamente.
- O console do Arcserve UDP 8.1 oferece suporte à adição de nós ao plano existente.

- A adição do nó limpo ao plano existente é suportada quando o RPS associado é atualizado para a versão 8.1. Caso contrário, o plano será salvo, mas sua implantação falhará.
- A adição do nó de versão anterior ao plano existente será suportada se a sua versão for semelhante à versão do RPS em execução. O agente não é atualizado automaticamente.
- A adição do nó do Arcserve UDP 8.1 ao plano existente é suportada quando o RPS associado é atualizado para o UDP 8.1.

- O gateway é atualizado automaticamente para coincidir com a versão do console do Arcserve UDP.
- Diretiva de compatibilidade com versões anteriores de replicação:
  - A replicação tem suporte quando o console é atualizado para o Arcserve UDP 8.1, mas todos RPSs associados ainda estão em execução no UDP 8.0, 7.0, 7.0 Atualização 1 e 7.0 Atualização 2.
    - A replicação tem suporte a partir do RPS de origem do Arcserve UDP 8.1 para o RPS de destino do UDP 8.0, 7.0, 7.0 Atualização 1 e 7.0 Atualização 2.
    - A replicação tem suporte a partir do RPS de origem do Arcserve UDP UDP 8.0, 7.0, 7.0 Atualização 1 e 7.0 Atualização 2 para o RPS de destino do UDP 8.1.
- Diretiva de compatibilidade com versões anteriores do modo de espera virtual:
  - A versão do monitor/proxy VSB deverá ser semelhante à versão do agente se o destino do backup for uma pasta compartilhada.
  - A versão do monitor/proxy VSB deverá ser semelhante à versão do RPS se o destino do backup for um RPS.
- Diretiva de compatibilidade com versões anteriores da máquina virtual instantânea:

  A versão do servidor de recuperação da VM instantânea deverá ser semelhante à versão do console do Arcserve UDP.

Diretiva de suporte à compatibilidade com versões anteriores para o Arcserve UDP versão 7.x

Suporte à compatibilidade com versões anteriores entre diferentes consoles do UDP por meio da tarefa Replicar para um RPS gerenciado remotamente

Caso você esteja planejando executar a tarefa *Replicar para um RPS gerenciado remotamente*, é recomendável atualizar o console e o RPS no destino antes de atualizar o console/RPS/agente na origem.

- A replicação terá suporte se o RPS de origem tiver o UDP 8.1 e o RPS de destino ainda tiver o UDP versão 7.0, 7.0 Atualização 1 e 7.0 Atualização 2.
- A replicação terá suporte se o RPS de origem tiver o UDP versão 7.0, 7.0 Atualização 1 e 7.0 Atualização 2, e o RPS de destino tiver o UDP 8.1.
- Comportamentos de replicação:
  - Se você atualizar para o UDP 8.1 nos dois sites, será possível replicar do Cloud Hybrid para o local sem um IP público (novo comportamento do UDP).
  - Se você fizer a atualização para o UDP 8.1 apenas em um dos sites e o outro site usar uma versão com suporte do UDP, será possível replicar do Cloud Hybrid para o local usando o IP público.

Suporte à compatibilidade com versões anteriores do Windows RPS/Agente (ou proxy de backup sem agente)

- O console do Arcserve UDP 8.1 oferece suporte aos RPSs e agentes (ou proxies de backup sem agente) do UDP versão 7.0, 7.0 Atualização 1 e 7.0 Atualização 2, para backup, caso o plano não seja alterado após uma atualização.
- O console do Arcserve UDP 8.1 e o RPS oferecem suporte a agentes (ou proxies de backup sem agente) do UDP versão 7.0, 7.0 Atualização 1 e 7.0 Atualização 2, para backup, caso o plano não seja alterado após uma atualização.
- O console do Arcserve UDP 8.1 oferece suporte à implantação do plano existente sem alterações quando o RPS e os agentes (ou proxies de backup sem agente) ainda estão sendo executados no UDP versão 7.0, 7.0 Atualização 1 e 7.0 Atualização 2. O agente não é atualizado automaticamente.
- O console do Arcserve UDP 8.1 oferece suporte a ações como pausar ou retomar o plano existente sem alterações quando o RPS e os agentes (ou proxies de backup sem agente) ainda estão sendo executados no UDP versão 7.0, 7.0 Atualização 1 e 7.0 Atualização 2. O agente não é atualizado automaticamente.

- O console do Arcserve UDP 8.1 oferece suporte à criação de um novo plano ou à modificação do plano existente para configurar recursos herdados que já eram suportados na release anterior, com o RPS e os agentes (ou proxies de backup sem agente) ainda sendo executados no UDP versão 7.0, 7.0 Atualização 1 e 7.0 Atualização 2. O agente não é atualizado automaticamente.
- O console do Arcserve UDP 8.1 oferece suporte à criação de um novo plano ou à modificação do plano existente para incluir os novos recursos do UDP 8.1 quando o RPS, o proxy ou o agente associado já tiver sido atualizado para a versão esperada.

  Por exemplo:

  - É possível especificar a rede para backup quando o console, o RPS, o proxy e o agente forem atualizados para o UDP 7.0, 7.0 Atualização 1, 7.0 Atualização 2, 8.0 ou 8.1.
- O console do Arcserve UDP 8.1 oferece suporte à atualização do nó quando o RPS e os agentes (ou proxies de backup sem agente) ainda estão sendo executados no UDP versão 7.0, 7.0 Atualização 1 e 7.0 Atualização 2. O plano será implantado. O agente não é atualizado automaticamente.
- O console do Arcserve UDP 8.1 oferece suporte à adição do UDP versão 7.0, 7.0 Atualização 1 e 7.0 Atualização 2 do servidor RPS. Mas o RPS não é atualizado automaticamente para o Arcserve UDP 8.1 quando adicionado.
- O console do Arcserve UDP 8.1 oferece suporte à adição de uma versão anterior do agente (ou proxy de backup sem agente) sem atualizar o agente automaticamente.
- O console do Arcserve UDP 8.1 oferece suporte à adição de nós ao plano existente.
  - A adição do nó limpo ao plano existente é suportada quando o RPS associado é atualizado para o UDP 8.1. Caso contrário, o plano será salvo, mas sua implantação falhará.
  - A adição do nó de versão anterior ao plano existente será suportada se a sua versão for semelhante à versão do RPS em execução. O agente não é atualizado automaticamente.
  - A adição do nó do Arcserve UDP 8.1 ao plano existente é suportada quando o RPS associado é atualizado para o UDP 8.1.
- O gateway é atualizado automaticamente para coincidir com a versão do console do Arcserve UDP.
- Diretiva de compatibilidade com versões anteriores de replicação:

- A replicação tem suporte quando o console é atualizado para o Arcserve UDP 8.1, mas todos RPSs associados ainda estão em execução no UDP 7.0, 7.0 Atualização 1 e 7.0 Atualização 2.
  - A replicação tem suporte do RPS de origem do Arcserve UDP 8.1 para o RPS de destino do UDP 7.0, 7.0 Atualização 1 e 7.0 Atualização 2.
  - A replicação tem suporte do RPS de origem do Arcserve UDP UDP 7.0, 7.0 Atualização 1 e 7.0 Atualização 2 para o RPS de destino do UDP 8.1.

- Diretiva de compatibilidade com versões anteriores do modo de espera virtual:
  - A versão do monitor/proxy VSB deverá ser semelhante à versão do agente se o destino do backup for uma pasta compartilhada.
  - A versão do monitor/proxy VSB deverá ser semelhante à versão do RPS se o destino do backup for um RPS.
- Diretiva de compatibilidade com versões anteriores da máquina virtual instantânea:

  A versão do servidor de recuperação da VM instantânea deverá ser semelhante à versão do console do Arcserve UDP.

Diretiva de suporte à compatibilidade com versões anteriores para Arcserve UDP versão 6.5, Atualização 4

Suporte à compatibilidade com versões anteriores entre diferentes consoles do UDP por meio da tarefa Replicar para um RPS gerenciado remotamente

Caso você esteja planejando executar a tarefa *Replicar para um RPS gerenciado remotamente*, é recomendável atualizar o console e o RPS no destino antes de atualizar o console/RPS/agente na origem.

- A replicação será suportada se o RPS de origem tiver o UDP 8.1 e o RPS de destino ainda estiver na versão 6.5, Atualização 4.
- A replicação será suportada se o RPS de origem estiver a versão 6.5, Atualização 4, e o RPS de destino for o UDP 8.1 e o patch P00001738 for aplicado. Se o RPS de origem estiver na versão 6.5, Atualização 1, 2 ou 3, atualize para a Atualização 4 primeiro e, em seguida, aplique o patch P00001738.

Suporte à compatibilidade com versões anteriores do Windows RPS/Agente (ou proxy de backup sem agente)

- O console do Arcserve UDP 8.1 oferece suporte aos RPSs e agentes (ou proxies de backup sem agente) da versão 6.5, Atualização 4, para backup, caso o plano não seja alterado após uma atualização.
- O RPS e o console do Arcserve UDP 8.1 oferecem suporte a agentes (ou proxies de backup sem agente) da versão 6.5, Atualização 4, para backup, caso o plano não seja alterado após uma atualização.
- O console do Arcserve UDP 8.1 oferece suporte à implantação do plano existente sem alterações quando o RPS e os agentes (ou proxies de backup sem agente) ainda estão sendo executados na versão 6.5, Atualização 4. O agente não é atualizado automaticamente.
- O console do Arcserve UDP 8.1 oferece suporte a ações como pausar ou retomar o plano existente sem alterações quando o RPS e os agentes (ou proxies de backup sem agente) ainda estão sendo executados na versão 6.5, Atualização 4. O agente não é atualizado automaticamente.
- O console do Arcserve UDP 8.1 oferece suporte à criação de um novo plano ou à modificação do plano existente para configurar recursos herdados que já eram suportados na release anterior, com o RPS e os agentes (ou proxies de

backup sem agente) ainda sendo executados na versão 6.5, Atualização 4. O agente não é atualizado automaticamente.

- O console do Arcserve UDP 8.1 oferece suporte à criação de um novo plano ou à modificação do plano existente para incluir os novos recursos do UDP 8.1 quando o RPS, o proxy ou o agente associado já tiver sido atualizado para a versão esperada.

  Por exemplo:

  - Especifique a rede para backup quando o console, o RPS, o proxy e o agente forem atualizados para a versão 7.0, Atualização 1, Atualização 2 ou UDP 8.1.

- O console do Arcserve UDP 8.1 oferece suporte à atualização do nó quando o RPS e os agentes (ou proxies de backup sem agente) ainda estão sendo executados na versão 6.5, Atualização 4. O plano será implantado. O agente não é atualizado automaticamente.
- O console do Arcserve UDP 8.1 oferece suporte à adição de um servidor RPS da versão 6.5, Atualização 4. Mas o RPS não é atualizado automaticamente para o Arcserve UDP 8.1 quando adicionado.
- O console do Arcserve UDP 8.1 oferece suporte à adição de uma versão anterior do agente (ou proxy de backup sem agente) sem atualizar o agente automaticamente.
- O console do Arcserve UDP 8.1 oferece suporte à adição de nós ao plano existente.

  - A adição do nó limpo ao plano existente é suportada quando o RPS associado é atualizado para o UDP 8.1. Caso contrário, o plano será salvo, mas sua implantação falhará.
  - A adição do nó de versão anterior ao plano existente será suportada se a sua versão for semelhante à versão do RPS em execução. O agente não é atualizado automaticamente.
  - A adição do nó do Arcserve UDP 8.1 ao plano existente é suportada quando o RPS associado é atualizado para o UDP 8.1.

- O gateway é atualizado automaticamente para coincidir com a versão do console do Arcserve UDP.
- Diretiva de compatibilidade com versões anteriores de replicação:

  - A replicação tem suporte quando o console é atualizado para o Arcserve UDP 8.1, mas todos os RPSs associados ainda estão em execução na versão 6.5, Atualização x.

        - A replicação tem suporte do RPS de origem do Arcserve UDP 6.5, Atualização x, para um RPS de destino da versão 6.5, Atualização 4.
        - A replicação tem suporte do RPS de origem do Arcserve UDP 6.5, Atualização 4, para o RPS de destino da versão 6.5, Atualização x.
    - A replicação tem suporte do RPS de origem do Arcserve UDP 6.5, Atualização x, para o RPS de destino do UDP 8.1.
    - A replicação tem suporte de um RPS de origem do Arcserve UDP 8.1 para um RPS de destino da versão 6.5, Atualização 4.
    - A replicação não tem suporte do RPS de origem do Arcserve UDP 8.1 para o RPS de destino da versão 6.5, Atualização 3, Atualização 2, Atualização 1 ou versão final.
- Diretiva de compatibilidade com versões anteriores do modo de espera virtual:
    - A versão do monitor/proxy VSB deverá ser semelhante à versão do agente se o destino do backup for uma pasta compartilhada.
    - A versão do monitor/proxy VSB deverá ser semelhante à versão do RPS se o destino do backup for um RPS.
- Diretiva de compatibilidade com versões anteriores da máquina virtual instantânea:

  A versão do servidor de recuperação da VM instantânea deverá ser semelhante à versão do console do Arcserve UDP.

Suporte à compatibilidade com versões anteriores para o servidor de backup Linux

Para o servidor de backup Linux 7.x e 6.5.x:

- O console do Arcserve UDP 8.1 oferece suporte às versões 6.5.x e 7.x do servidor de backup Linux quando os RPSs (Recovery Point Servers - Servidores de Ponto de Recuperação) possuem o Arcserve UDP 8.1. Todas as tarefas são executadas sem problemas, exceto o novo recurso ou aprimoramento no UDP 8.1.
- O console do Arcserve UDP 8.1 oferece suporte aos RPSs e às versões 6.5.x e 7.x do servidor de backup Linux. Todas as tarefas são executadas sem problemas, exceto o novo recurso ou aprimoramento na versão 8.1.
- Depois de atualizar o servidor de backup Linux para o Arcserve UDP 8.1, todos os recursos novos do UDP 8.1 terão suporte.

Sequência de atualização para o console do UDP, o RPS e o agente

Com base na diretiva de suporte à compatibilidade com versões anteriores, o planejamento da atualização na seguinte sequência ajuda a garantir um processo tranquilo:

1. Atualize o Console do Arcserve UDP.
2. Atualize o RPS do Arcserve UDP (local da recuperação de falhas).
3. Atualize o RPS do Arcserve UDP (datacenter).
4. Atualize o proxy sem agente do Arcserve UDP e alguns ou todos os agentes no datacenter.
5. Atualize o RPS do Arcserve UDP (local remoto).
6. Atualize o proxy sem agente do Arcserve UDP e alguns ou todos os agentes no local remoto.

   Observação: repita a etapa 5 e 6 para cada local remoto.

   Observações:

   - Caso a tarefa de replicação de MSP (Managed Service Provider – Provedor de Serviço Gerenciado) esteja configurada, primeiro, atualize o MSP no console ou RPS.
   - O gateway é atualizado automaticamente para a versão do console.
   - De acordo com a política de suporte de versões anteriores de replicação, sempre atualize o RPS de destino antes do RPS de origem.

Como atualizar para o Arcserve UDP 8.0 de uma release anterior

Atualizar uma instalação significa reinstalar recursos ou componentes para uma release mais recente. O processo de atualização permite manter a maioria de suas configurações atuais e migrar as informações armazenadas no banco de dados anterior do Arcserve UDP para o novo banco de dados do Arcserve UDP.

Considerações sobre a atualização

- Verifique se os requisitos de hardware do Arcserve UDP versão 8.0 são atendidos. Para obter mais informações, consulte *Informações do sistema* nas *Notas da Versão v8.0*.
- A versão usada de aplicativo, sistema operacional, hipervisor ou plataforma precisa ser suportada pelo Arcserve UDP 8.0. Para obter informações detalhadas, consulte a Matriz de compatibilidade.
- Antes de atualizar da versão 6.5.3 ou de versões anteriores com suporte, evite pausar um plano existente. Se o plano estiver pausado antes de uma atualização, não será possível retomar o plano até que todos os RPS relacionados sejam atualizados.
- Adquira a chave de produto do Arcserve UDP 8.0 e deixe-a à mão.
- Remova a versão anterior do utilitário autônomo Arcserve Exchange Granular Restore (AEGR) usado para o Arcserve UDP 5.0. Se esse utilitário for detectado, o Assistente de instalação solicitará a remoção dele.
- Os planos anteriores devem funcionar normalmente em todas as etapas de atualização descritas abaixo.

Siga estas etapas para fazer a atualização:

1. Para o MSP, atualize o console do Arcserve UDP anterior para o Arcserve UDP 8.0.

   Essa etapa só é necessária se a tarefa **Replicar de um RPS gerenciado remotamente** foi configurada na release anterior.

   Observações:

   - se o nó tiver somente o Console instalado, atualize o Console. Não é necessário interromper as tarefas em execução para atualizar o console.
   - Se o nó tiver o console e o RPS instalados, planeje a atualização do console para quando não houver tarefas em execução. Se necessário, interrompa o repositório de dados de RPS para cancelar as tarefas em execução antes de atualizar o Console.

- Para obter mais informações sobre como atualizar o Console, consulte Instalar o Arcserve Unified Data Protection usando o Assistente de instalação ou Instalar o Arcserve UDP usando o programa de instalação unificado.

2. Para MSP, atualize o RPS do Arcserve UDP anterior para o Arcserve UDP 8.0.

   Essa etapa só é necessária se a tarefa **Replicar de um RPS gerenciado remotamente** foi configurada na release anterior.

   Observações:

   - Planeje a atualização do RPS para quando não houver tarefas em execução. Se necessário, interrompa o repositório de dados de RPS para cancelar as tarefas em execução antes de atualizar o RPS.
   - Para obter mais informações sobre como atualizar o RPS, consulte Instalar/atualizar o servidor de ponto de recuperação.

3. Para cliente, atualize o console do Arcserve UDP anterior para o Arcserve UDP 8.0.

   Observações:

   - se o nó tiver somente o Console instalado, atualize o Console. Não é necessário interromper as tarefas em execução para atualizar o console.
   - Se o nó tiver o console e o RPS instalados e houver tarefas em execução no RPS, interrompa o repositório de dados do RPS para cancelar as tarefas em execução primeiro. Em seguida, atualize o console.
   - Para obter mais informações sobre como atualizar o Console, consulte Instalar o Arcserve Unified Data Protection usando o assistente de instalação ou Instalar o Arcserve UDP usando o programa de instalação unificado.

4. Para o cliente, atualize o antigo RPS de destino de replicação do Arcserve UDP para o Arcserve UDP 8.0.

   Observações:

   - O Arcserve UDP 8.0 oferece suporte à replicação a partir do RPS de origem do Arcserve UDP versão 6.5.x até o RPS de destino do Arcserve UDP 8.0. Quando o plano inclui várias tarefas de replicação, atualize o último destino de replicação RPS primeiro.
   - A replicação do RPS de origem do Arcserve UDP 8.0 para uma versão anterior do RPS de destino será suportada somente se o RPS de destino for do Arcserve UDP versão 6.5 Atualização 4.
   - Para obter mais informações sobre como atualizar o RPS, consulte Instalar/atualizar o servidor de ponto de recuperação.

5. Para o cliente, atualize o RPS de origem de replicação anterior para Arcserve UDP 8.0.

   Observação: para obter mais informações sobre como atualizar o RPS, consulte Instalar/atualizar o servidor de ponto de recuperação.

6. Para o cliente, atualize o proxy e agentes anteriores para o Arcserve UDP 8.0.

   Observações:

   - Para obter mais informações sobre como atualizar o proxy sem agente do Windows e o agente, consulte Implantar o agente em nós.
   - Para obter mais informações sobre como atualizar o servidor de backup do Linux, consulte Como atualizar o agente do Arcserve UDP (Linux).

7. Para o cliente, atualize o Monitor VSB ou o servidor de recuperação de VM instantânea anterior para o Arcserve UDP 8.0.

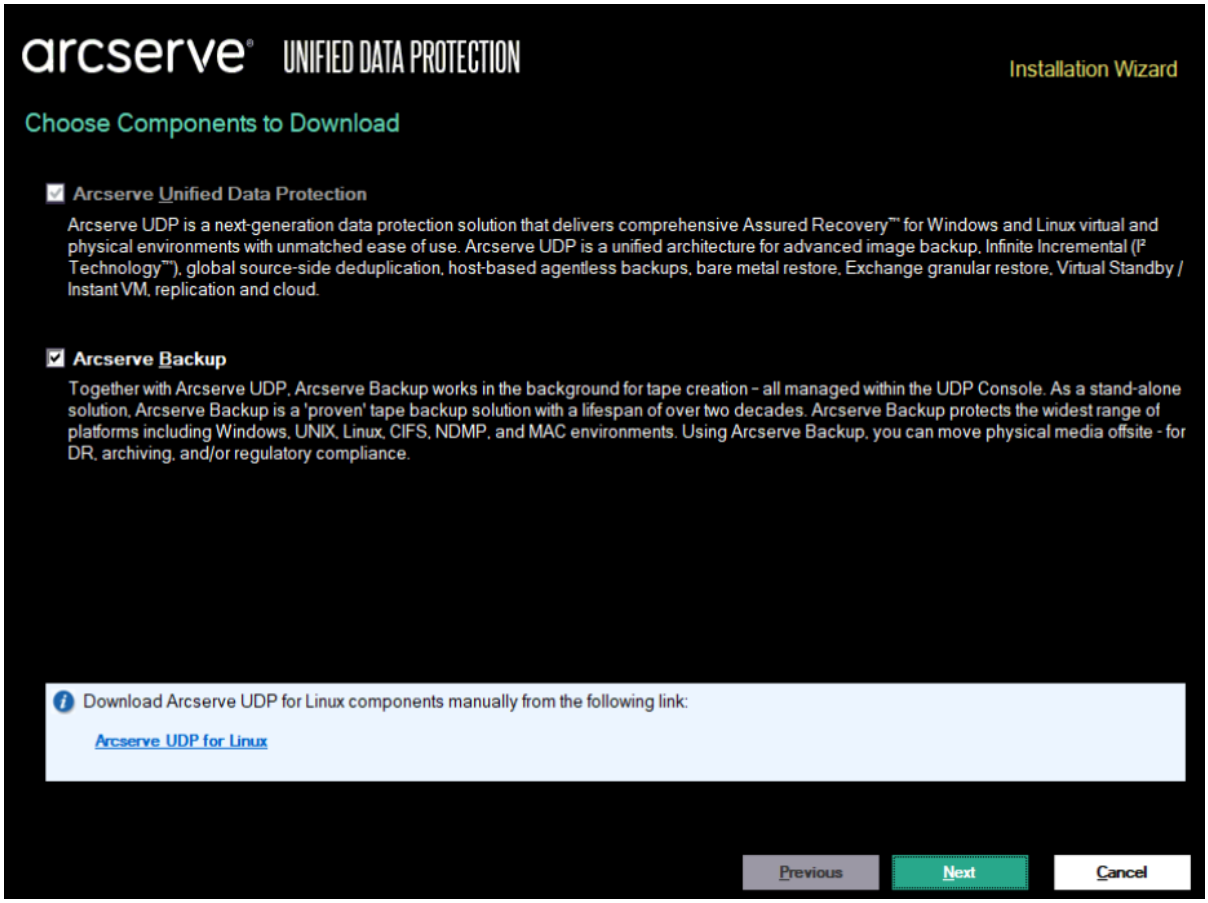
   Observação: para obter mais informações sobre como atualizar o Monitor VSB, consulte Instalar o Arcserve Unified Data Protection usando o assistente de instalação ou Instalar o Arcserve UDP usando o programa de instalação unificado.

Como atualizar para o Arcserve UDP 8.0 usando o único programa de instalação

Você pode atualizar o Arcserve UDP para a versão 8.0 usando o programa de instalação único. Verifique as versões com suporte antes de atualizar.

Siga estas etapas:

1. Faça download do ASDownloader.exe no link de download do Arcserve.
2. Execute o ASDownloader.exe, aceite o contrato de licença e clique em **Avançar**.
3. Clique em **Avançar** na tela **Introdução**.
4. Na tela **Escolha os componentes para download**, selecione os componentes dos quais você deseja fazer download.



Considerações para a seleção de componentes:

- Para atualizar a versão anterior do Arcserve UDP, selecione a opção **Arcserve Unified Data Protection**.

- Para atualizar a versão anterior do Arcserve Backup, selecione a opção do **Arcserve Backup**.

Observação: alguns componentes são selecionados automaticamente de acordo com a dependência quando você seleciona a opção **Arcserve Backup**. Se você não deseja instalar os componentes no mesmo computador, consulte Como atualizar para o Arcserve UDP 8.0 de uma release anterior e use o Assistente de instalação para atualizar apenas os componentes existentes. Nessa área, você também pode fazer download da configuração mais recente do Linux para o Arcserve UDP.

5. Depois de fazer download dos componentes, selecione o método de instalação para atualizar os componentes selecionados.

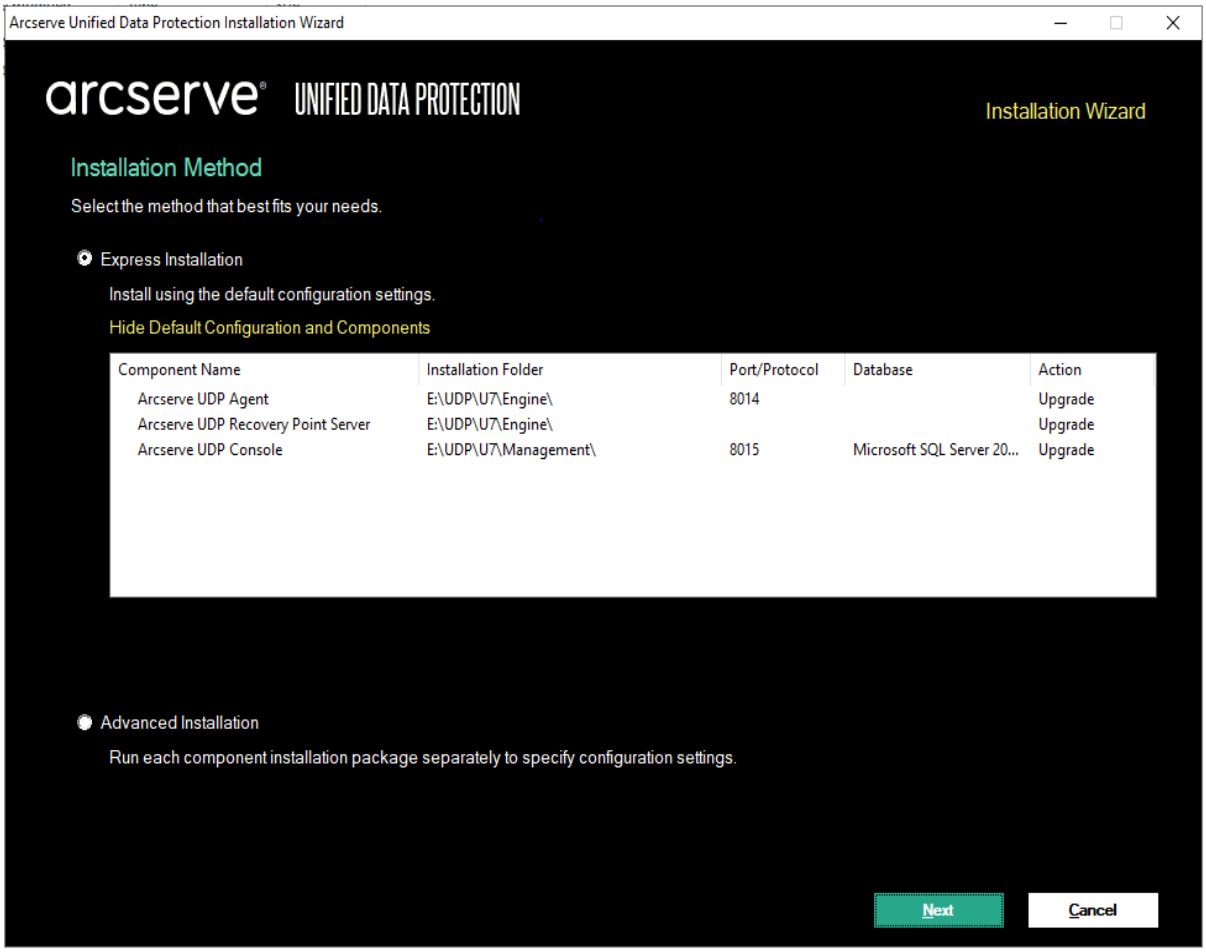
   Instalação expressa

   Recomendamos a instalação expressa quando você planeja instalar todos os componentes com sua configuração padrão no mesmo computador.

   Observações:

   - Verifique todos os pré-requisitos da atualização. Por exemplo, .Net 4.5.1 é obrigatório para o Arcserve Backup. Siga as instruções exibidas no programa de instalação até que todos os pré-requisitos sejam atendidos.
   - Consulte a Matriz de compatibilidade.
   - O método Instalação expressa instala os componentes de acordo com as configurações padrão, como: caminho, protocolo, porta e banco de dados. Quando você faz a atualização usando o método Instalação expressa, é usada

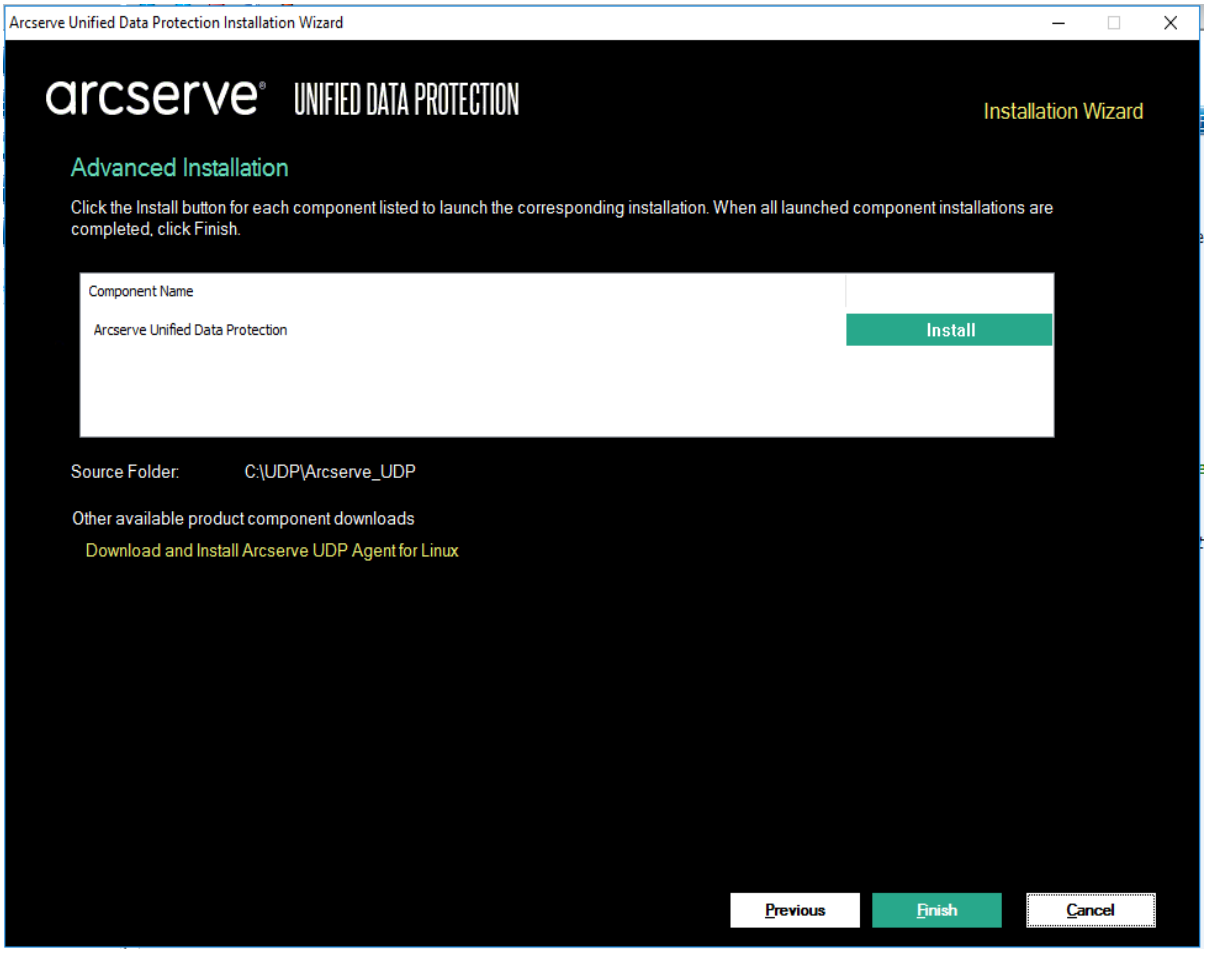
a configuração da release anterior.



Instalação avançada

Recomendamos a Instalação avançada para instalar ou atualizar cada componente separadamente na mesma máquina. Clique em **Instalar** para atualizar ou instalar cada componente separadamente.

Observação: para atualizar o Agente do Arcserve Unified Data Protection para Linux usando o programa de instalação unificado, faça download das imagens clicando nos links compartilhados no final do programa. Depois de copiar as imagens no servidor de backup Linux, siga as etapas mencionadas em *Como atualizar o agente do Arcserve UDP (Linux)* na Ajuda online do Agente para Linux.



O Arcserve UDP é atualizado com êxito usando o programa de instalação unificado.

Observação: para obter mais informações, consulte Como atualizar para o Arcserve UDP 8.0 de uma release anterior.

Como atualizar para o Arcserve UDP 8.0 ou Arcserve Backup 18.0 para ativar a cópia em fita

Esta seção fornece informações sobre como atualizar o Arcserve UDP ou o Arcserve Backup 18.0 da versão anterior do Arcserve UDP ou do Arcserve Backup para ativar a cópia em fita. O Arcserve UDP 8.0 apresenta integração com o Arcserve Backup 18.0 e permite copiar dados de backup para um destino de mídia em fita. É possível modificar um plano existente ou criar um plano com a tarefa **Copiar em fita** no console do Arcserve UDP.

Considerações sobre a atualização

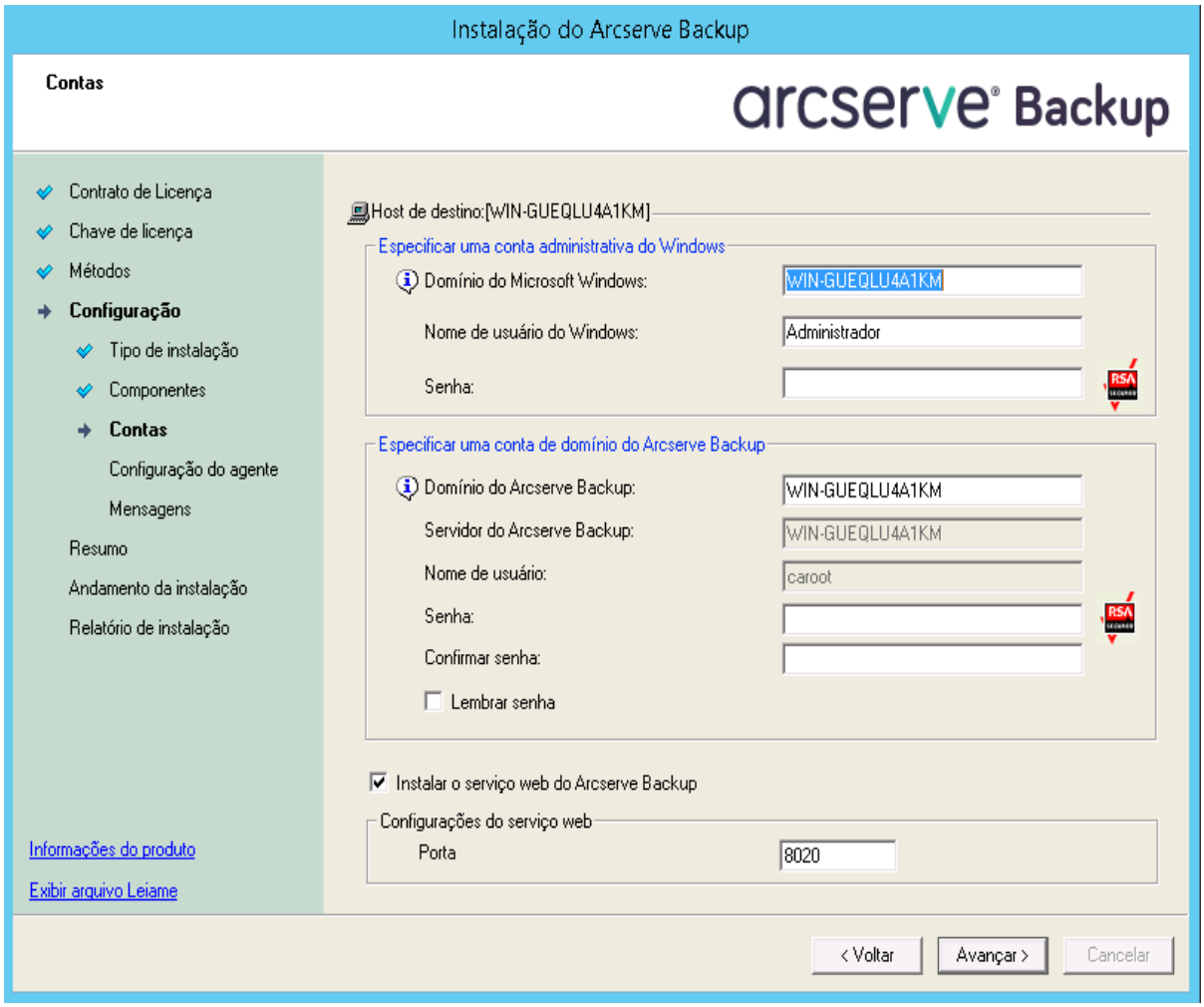
- Para garantir que o plano existente com a tarefa Copiar em fita seja executado sem problemas, atualize o Arcserve Backup para 18.0 antes de atualizar o Arcserve UDP para 8.0.
- Verifique os requisitos de hardware do Arcserve UDP 8.0. Para obter mais informações sobre os requisitos detalhados de hardware, consulte as *Informações do sistema* em *Notas da Versão 8.0*.
- A versão usada de aplicativo, sistema operacional, hipervisor ou plataforma precisa ser suportada pelo Arcserve UDP 8.0. Para obter informações detalhadas, consulte a Matriz de compatibilidade.
- Antes de atualizar o UDP 6.5.3 ou versões anteriores com suporte, evite pausar um plano existente. Se o plano for pausado antes da atualização, você não poderá retomá-lo até o RPS relacionado ser atualizado.
- Adquira a chave de produto do Arcserve UDP 8.0 e deixe-a à mão.
- Remova a versão anterior do utilitário autônomo Arcserve Exchange Granular Restore (AEGR) usado para o Arcserve UDP 5.0. Se esse utilitário for detectado, o Assistente de instalação solicitará a remoção dele.
- Os planos anteriores devem funcionar normalmente em todas as etapas de atualização descritas abaixo.

Consideração sobre Cópia em fita

- Prepare o servidor Arcserve Backup 18.0 instalando ou atualizando de qualquer caminho de atualização suportado anteriormente. O Arcserve Backup é necessário antes de configurar a tarefa **Copiar em fita** em um plano do Arcserve UDP.
- Verifique se você atendeu ao requisito do Arcserve Backup 18.0. Para obter mais informações, consulte a Matrix de compatibilidade.
- Adquira a chave do produto do Arcserve Backup 18.0 e a mantenha preparada.

Siga estas etapas para atualizar e ativar o recurso de Copiar em fita:

1. Atualize para o Arcserve Backup 18.0 de uma release anterior ou instale o Arcserve Backup 18.0 com a opção de instalação do **serviço web do Arcserve Backup** ativada.



Observação: para obter mais informações sobre a instalação e atualização do Arcserve Backup, consulte o *Guia de Implementação do Arcserve Backup 18.0*.

Ao concluir a atualização, realize as seguintes tarefas:

- Verifique se o mecanismo de tarefas foi iniciado no gerenciador do Arcserve Backup.
- No Console de serviços do Windows, verifique se **serviço web do Arcserve Backup** está no status em execução.

2. Atualize para o Arcserve UDP 8.0 a partir de uma release anterior.

Observação: para obter mais informações sobre como atualizar o produto, consulte Como atualizar para o Arcserve UDP 8.0 de uma release anterior.

3. Configure a tarefa **Copiar em fita** no console do Arcserve UDP para um plano já existente ou um novo plano.

   Observação: para obter mais informações sobre a configuração da tarefa Copiar em fita, consulte Como criar um plano de cópia em fita.

   O plano deve funcionar em todas as etapas.

Como migrar o console do Arcserve UDP de um servidor para outro

Para obter mais informações, clique em link.

Como fazer atualização de gateway para a mesma versão de seu Console registrado

O gateway do Arcserve UDP deve ser da mesma versão de seu Console registrado. Depois que o console do Arcserve UDP é atualizado, a versão de gateway relacionada é verificada quando o serviço inicia. Se a versão de gateway não corresponder à versão do Console, o Arcserve UDP acionará automaticamente uma atualização automática para os servidores de gateway.

Se o gateway não estiver disponível para a atualização automática, será possível atualizar manualmente o gateway mais tarde.

Siga estas etapas para atualizar manualmente o gateway:

1. Efetue logon no Console do Arcserve UDP.
2. Clique na guia **Recursos**, navegue até **Infraestrutura** e clique em **Sites**.
3. Selecione o site que você deseja atualizar.
4. Clique na lista suspensa **Ações** e, em seguida, clique em **Atualizar o gateway**.

   Uma caixa de diálogo de confirmação é exibida.
5. Clique em **Sim**.

   O gateway é atualizado com a versão mais recente do Gateway do Arcserve UDP.

Como executar a migração do console do Arcserve UDP

Você pode migrar um console do Arcserve UDP para outro console do Arcserve UDP usando *ConsoleMigration.exe*. No Arcserve UDP v6.5 Atualização 2 em diante, é possível migrar o console do Arcserve UDP entre dois consoles quaisquer do Arcserve UDP.

Use *ConsoleMigration.exe* para BackupDB e RecoverDB. A captura de tela a seguir mostra o uso de *ConsoleMigration.exe*:

Para realizar o processo de migração, siga estas etapas:

1. No antigo console do Arcserve UDP, faça backup do banco de dados do 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".
```

   A pasta *DB_Migration* é criada com êxito.

2. No novo console do Arcserve UDP, copie a pasta *DB_Migration* no seguinte caminho:

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

3. No novo console do Arcserve UDP, execute as etapas mencionadas na tela abaixo para recuperar o banco de dados do console do Arcserve 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".
```

   Observação: no console do Arcserve UDP, se houver qualquer outro site que não seja o site local, siga as etapas mencionadas no arquivo *NewRegistrationText.txt* para registrar o site novamente.

Você concluiu a migração do console do Arcserve UDP para o novo console do Arcserve UDP com êxito.

Você pode usar essa ferramenta para realizar a migração de console do console do Arcserve UDP conectado com o banco de dados SQL remoto. Após a conclusão da migração, o console do Arcserve UDP migrado estará configurado para conectar-se com o mesmo banco de dados SQL remoto.

Observação: no UDP v6.5 Atualização 2 e Atualização 3, quando você usa a ferramenta de migração do console para executar a migração entre dois consoles do Arcserve UDP, ambas a versões do console do Arcserve UDP e do banco de dados SQL devem ser consistentes nos dois sistemas do console do Arcserve UDP. Caso contrário, a migração do console falhará e uma mensagem de erro será exibida na linha de comando e nos arquivos de log no seguinte caminho:

<UDP_Home> \Management\BIN\Appliance\logs

No Arcserve UDP v6.5, Atualização 4, a opção ***-force*** foi introduzida no comando ***ConsoleMigration.exe*** para forçar a migração do arquivo do banco de dados de backup de recuperação para o console de destino nas seguintes condições:

1. Quando você deseja realizar a migração do console entre dois consoles, sendo que o console de origem usa o SQL Server Enterprise edition e o console de destino usa o SQL Server Express edition. Nesse caso, o tamanho mínimo necessário do banco de dados do console do UDP de origem é 4000 MB.
2. Quando você deseja realizar a migração de um console que usa uma versão avançada do banco de dados do SQL Server para um console que usa uma versão anterior do banco de dados do SQL Server. Por exemplo, ao fazer a migração de um console usando o SQL Server 2016 para um console usando o SQL Server 2014.

Capítulo 5: Explorar e configurar o Arcserve UDP

Esta seção contém os seguintes tópicos:

Efetuar logon no console do Arcserve UDP usando a autenticação multifator

O Arcserve UDP oferece suporte à autenticação multifator (MFA), que fornece uma camada adicional de segurança para todos os usuários. MFA é um processo de logon no qual o usuário é solicitado a fornecer uma forma adicional de identificação. Esse método de autenticação requer mais de um fator para verificar a identidade do usuário. Em geral, o processo de logon de MFA usa a autenticação de dois fatores, que permite dois fatores para a identificação do usuário.

O Arcserve UDP oferece suporte à autenticação de dois fatores. Ele permite o nome de usuário e a senha como a autenticação de primeiro fator. A autenticação de segundo fator usa uma das seguintes opções:

- **Senha de uso único com base em tempo (TOTP):** diferente do OTP tradicional que é enviado para um endereço de email ou SMS, um TOTP é gerado usando um aplicativo autenticador. O TOTP é válido por um curto período e é atualizado a cada 30 segundos.
- **OTP de email:** esse recurso é autenticado com um OTP que é enviado para o endereço de email registrado e o OTP é válido por 30 segundos. Ele é ativado somente quando você configura o endereço de email.

Esta seção contém os seguintes tópicos:

Verificar os pré-requisitos

Considere os seguintes pré-requisitos:

- Você deve ativar a MFA (Multi-factor Authentication - Autenticação multifator) para todos os usuários. Para obter mais informações sobre como ativar a MFA, consulte Configurando a autenticação multifator como usuário administrador.

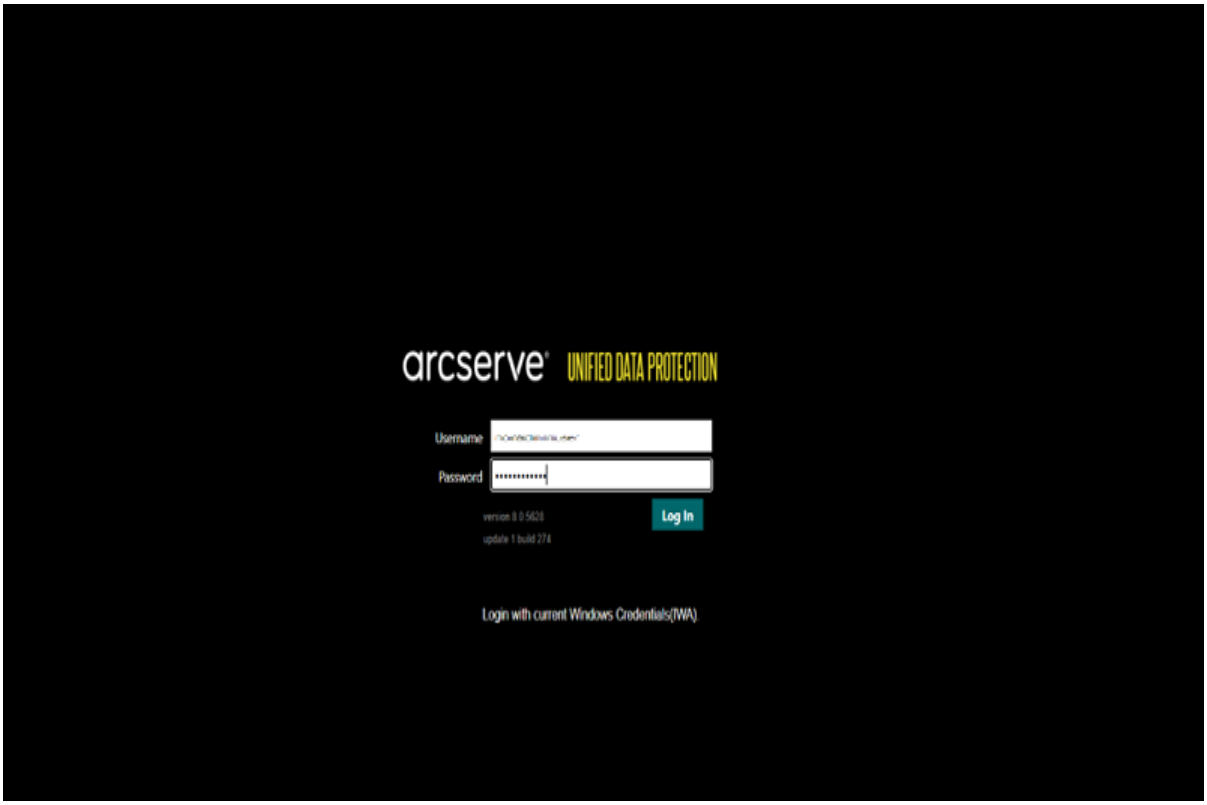
  Observação: somente os administradores podem ativar a autenticação multifator (MFA) para todos os usuários.
- Instale um aplicativo autenticador móvel no seu dispositivo móvel. Você pode encontrar os aplicativos autenticadores, como o Google Authenticator ou o Microsoft Authentication, na loja de aplicativos do seu dispositivo móvel.

Como efetuar logon no console do Arcserve UDP usando MFA

Esta seção fornece informações sobre como efetuar logon no console do Arcserve UDP usando MFA.

Siga estas etapas:

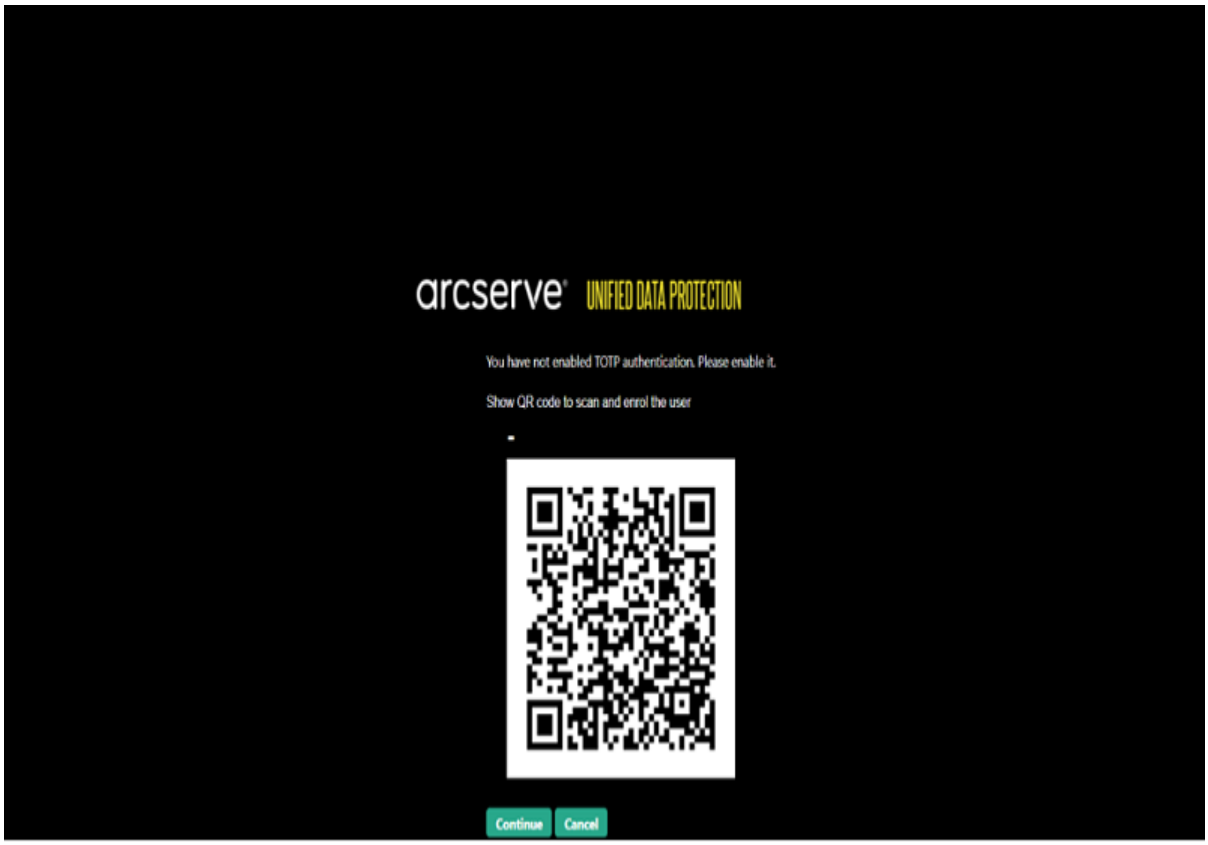
1. Vá para a página de logon do console do UDP.
2. Digite o nome de usuário e a senha, conforme necessário, e clique no botão **Efetuar logon**.



Na verificação bem-sucedida da autenticação de primeiro fator, a página de autenticação de segundo fator é exibida.

3. Se você não ativou a autenticação de TOTP, para ativá-la, faça o seguinte:
   a. Clique no link **Mostrar código QR para verificar e registrar o usuário**.

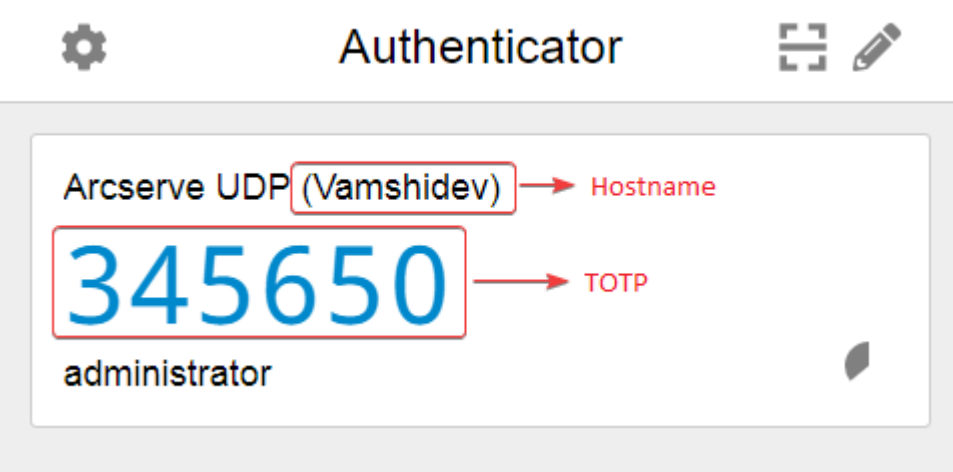
      A imagem do código QR é exibida.



b. Para gerar o TOTP, verifique a imagem do código QR usando um aplicativo autenticador.

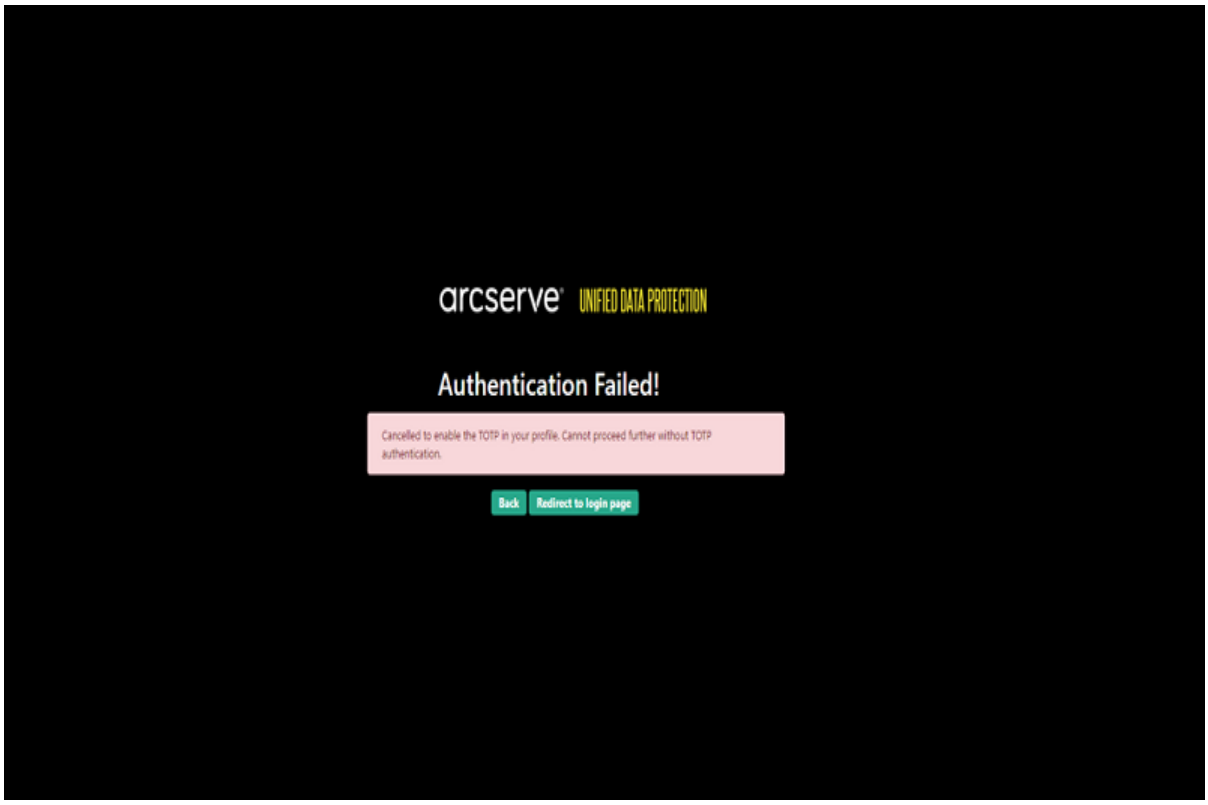
Observações:

- É possível usar qualquer um dos aplicativos autenticadores móveis, como o aplicativo autenticador do Google ou o aplicativo autenticador da Microsoft no seu dispositivo móvel. Como alternativa, você também pode usar a extensão do autenticador para o navegador Chrome.
- Ao usar um aplicativo autenticador para várias contas de usuário, o nome do host da conta do usuário diferencia os TOTPs. No aplicativo autenticador, é possível exibir o nome do host e o respectivo TOTP.



c. Clique no botão **Continuar**.

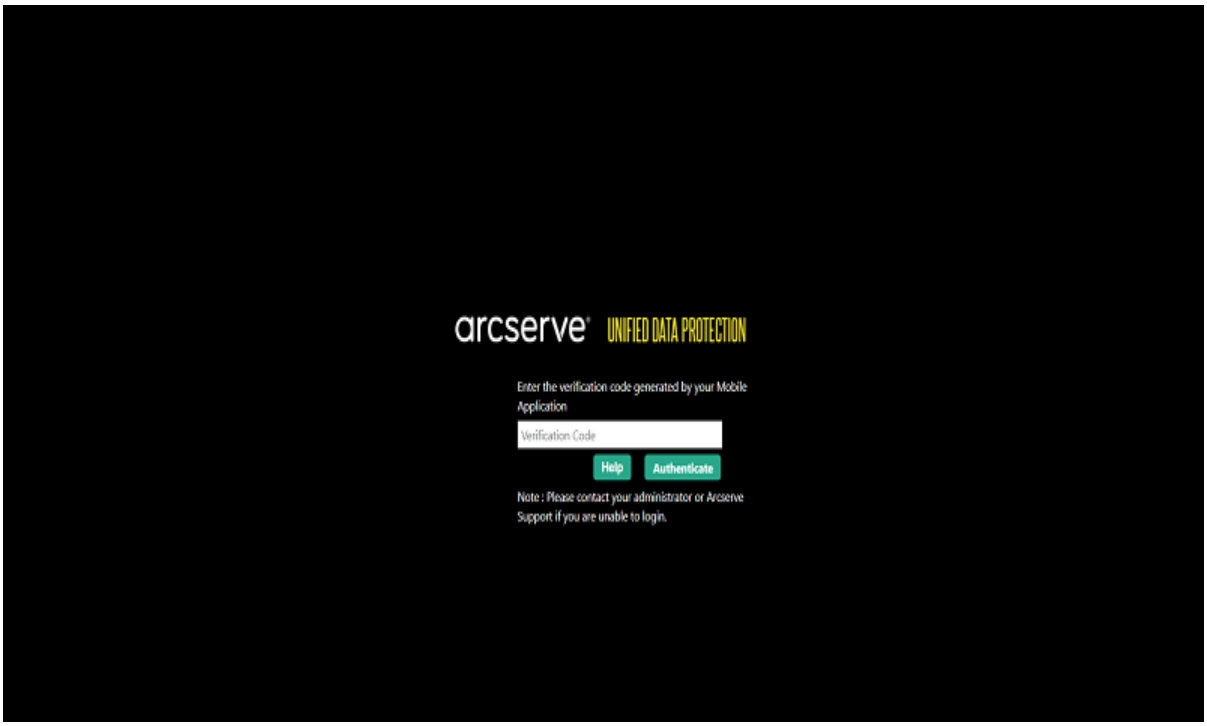
Se você clicar no botão **Cancelar**, a autenticação falhará.



Observação: se você já tiver ativado o fator de autenticação de TOTP, não será solicitado a executar a etapa 3.

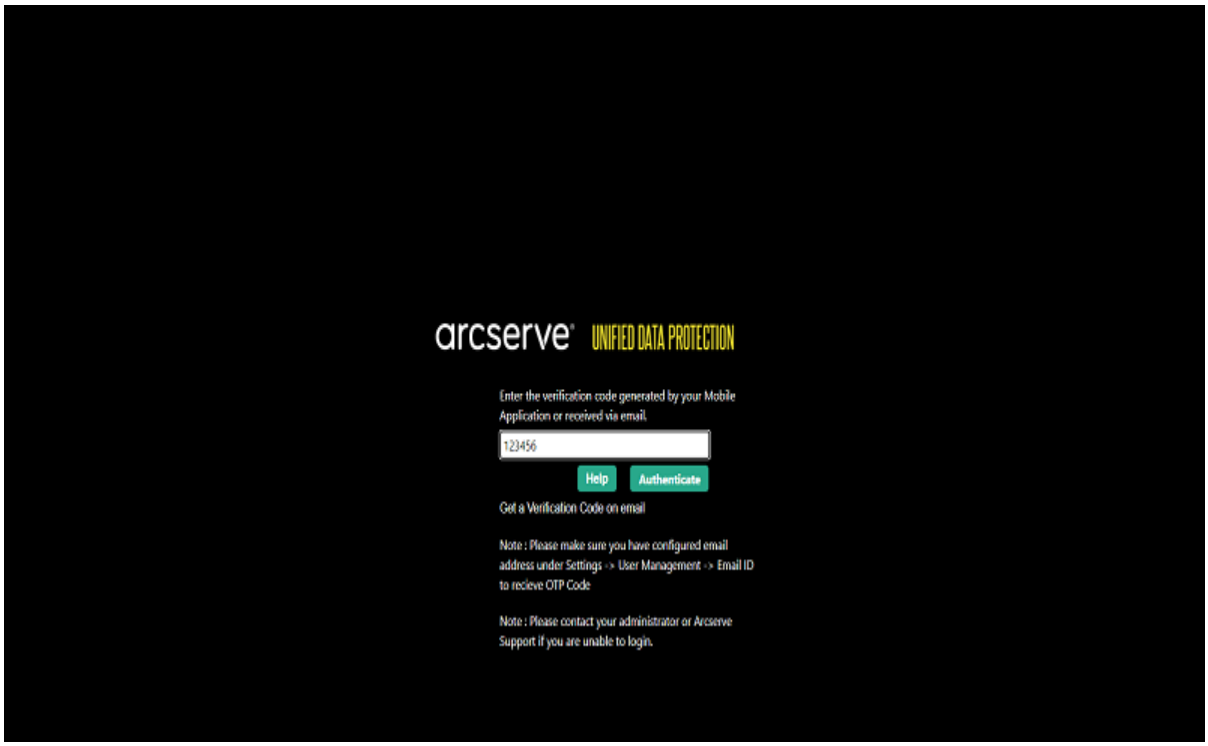
4. No campo Código de verificação, digite o TOTP.

Para o TOTP, abra o aplicativo autenticador móvel em seu dispositivo móvel ou a extensão do autenticador em seu navegador Chrome. O número é válido e atualizado a cada 30 segundos.



5. (Opcional) Se você não tiver TOTP, faça o seguinte:
   a. Clique no link **Obter um código de verificação no email**.

      O OTP de email temporário é enviado para seu endereço de email.



Observações:

- A opção OTP de email é acessada somente quando um usuário administrador ativa o OTP de email e define as configurações de email. Para obter mais informações, consulte Configurando a autenticação multifator como usuário administrador.
- Certifique-se de configurar o endereço de email em *Configurações* > *Gerenciamento de usuário* para receber o OTP de email.

b. No campo do código de verificação, digite o OTP de email.

6. Clique no botão **Autenticar**.

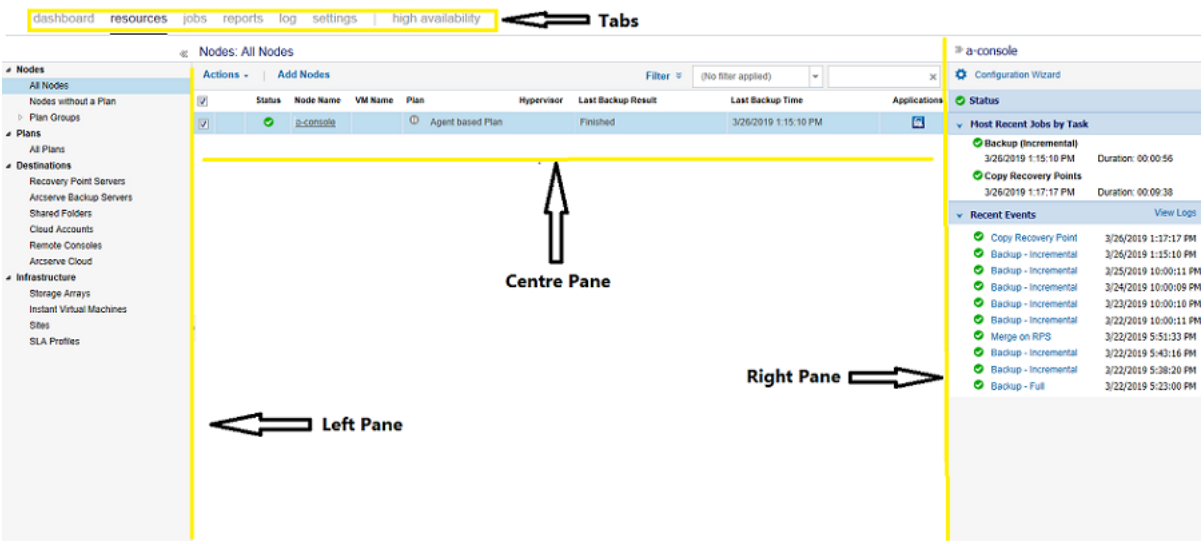
   Agora você efetuou logon com êxito no console do UDP.

Arcserve Unified Data Protection Interface do usuário

Antes de usar o Arcserve Unified Data Protection, familiarize-se com a interface de usuário. A interface do Arcserve Unified Data Protection permite realizar as seguintes tarefas:

- Gerenciar e monitorar tarefas
- Adicionar e gerenciar nós de origem
- Adicionar e gerenciar os servidores do ponto de recuperação de destino
- Gerenciar os planos para criar programações de backup
- Obter estatísticas de proteção de dados
- Exibir os logs de erro e de aviso
- Gerenciar e monitorar o ARCserve High Availability.
- Definir as configurações de proteção de dados
- Restaurar dados de backup

Navegando no Arcserve UDP



Guias

Permite que você acesse as diversas funções do Arcserve Unified Data Protection.

Painéis

Quando você navega para cada guia, a tela exibida é dividida nos seguintes painéis. Cada painel é usado para executar ações relacionadas.

Painel Esquerdo

Permite que você navegue para várias funções e operações. O resultado de cada clique é exibido no painel central.

Painel central

Permite executar a maioria das ações nesse painel, como adição, exclusão e modificação. Este painel exibe também o resultado e o status de cada atividade como, por exemplo, tarefas, planejamentos e relatórios. A maior parte das ações é realizada nesse painel. As informações exibidas nessa página são principalmente o resultado das opções selecionadas no painel esquerdo.

Painel à direita

Exibe um resumo dos itens selecionados no painel central. Por exemplo, na guia Tarefas, se tiver selecionado uma tarefa no painel central, será exibido no painel direito um resumo da tarefa, como monitor de tarefas (se houver uma tarefa em execução) e detalhes da tarefa, como o nome do nó de ori-

gem, a tarefa, o servidor do ponto de recuperação de destino e o repositório de dados de destino no painel direito.

Guias

A solução Arcserve Unified Data Protection fornece as seguintes guias para executar as funções de proteção de dados:

- Painel
- Recursos
- tarefas
- relatórios
- log
- configurações
- Alta disponibilidade

Painel

A guia **painel** permite que você exiba uma representação gráfica do último status da tarefa e armazenamento de dados dos últimos sete dias. Na guia **painel**, é possível executar as seguintes ações:

- Exiba a hora da última atualização. Clicar no ícone *Atualizar* exibe os dados mais recentes no painel.
- Clicar no gráfico de barras RTO abre diretamente a página Relatórios de RTO.
- Exiba o último status da tarefa dos nós ou planos de acordo com os filtros que você selecionar no gráfico **Último status da tarefa**.

Você pode exibir os gráficos para as seguintes opções na guia painel:

Último status da tarefa

Último status da tarefa refere-se ao último status da tarefa e oferece vários filtros para exibir o status. Com base na sua seleção da opção de filtro, você pode exibir o último status da tarefa. Por exemplo, selecione **Todos os nós** para ver o último status da tarefa de todos os nós ou selecione qualquer plano para ver o último status da tarefa dos nós protegidos por esse plano. Em seguida, filtre ainda mais com um tipo de tarefa específica. Ao selecionar **Todos os nós**, você pode ver o seguinte status:

- **Bem-sucedido** indica que o backup dos nós foi realizado com sucesso.
- **Falha** indica que o backup mais recente não foi obtido com sucesso.
- **Cancelado** indica que o backup mais recente foi interrompido.

- **Ausente** indica que o backup mais recente não foi executado como programado.
- **Não conectado** indica que o console do Arcserve UDP não pôde se conectar ao nó.
- **Incompleto** indica que a tarefa de restauração não foi concluída.

Quando clica em cada fatia (o status) do gráfico de pizza, a página **recursos** é aberta e os nós associado são exibidos. Por exemplo, se você clicar em **Bem-sucedido** no gráfico de pizza, a página **Recursos** será aberta. A página **recursos** exibe os nós que não têm qualquer plano. Além disso, o filtro **Bem-sucedido** está pré-selecionado na página **recursos**.

Tamanho dos dados brutos, restauráveis e reais: 7 dias

O gráfico refere-se ao armazenamento de dados brutos versus dados restauráveis versus dados reais dos últimos sete dias.

Tamanho dos dados restauráveis

Refere-se ao tamanho dos dados que podem ser restaurados a partir dos dados armazenados em todo o armazenamento de destino nesse dia. Independentemente do tipo de backup, backup completo ou backup incremental, todos os pontos de recuperação são usados para restaurar uma origem completa. Esse é o tamanho total de todos os tamanhos disponíveis da origem restaurada.

Por exemplo: se o tamanho dos dados brutos for 30 GB e, após a compactação e redução de redundância, o tamanho for 22 GB e o tamanho dos dados restauráveis for 30 GB para o primeiro backup completo, para uma alteração incremental de 4 GB, o tamanho dos dados restauráveis será 30 + 34 GB = 64 GB.

Tamanho do armazenamento de dados reais

Refere-se ao tamanho dos dados finais. Após a compactação dos dados brutos, da remoção de blocos de dados duplicados dos dados brutos e da adição de alguns metadados, os dados brutos se tornam os dados finais e são salvos no armazenamento de destino.

Tamanho dos dados brutos

Refere-se aos dados lidos na origem e transferidos para o destino.

Relatório de SLA para RTO e RPO

O Arcserve UDP apresenta o relatório de SLA (Service Level Agreement - Contrato de Nível de Serviço) para ajudar as organizações a gerar relatórios de conformidade relacionados ao RPO (Recovery Point Objective -

Objetivo do Ponto de Recuperação) e ao RTO (Recovery Time Objective - Objetivo do Tempo de Recuperação).

Relatório de RTO

o relatório de RTO do Arcserve UDP é um relatório de conformidade que mostra a comparação dos valores de Tempo de recuperação real e Objetivo de tempo de recuperação de todos os tipos de recuperação de tarefas executadas como Restauração do sistema de arquivos, Recuperação de VM, BMR, VM instantânea e Recuperação garantida. O gráfico de barras usa várias cores para exibir o status das tarefas. É possível detalhar mais ainda para ver o status de nível de nó filtrado por RTO atendido, não atendido, não testado e não definido.

Relatório de RPO

O relatório de RPO do Arcserve UDP exibe o número total de nós com pontos de recuperação disponíveis durante o período de tempo especificado no modo de exibição em barras, categorizados pelo tempo de vida dos pontos de recuperação mais recentes (15 minutos, última hora, 12 horas, último dia e assim por diante), tempo de vida dos pontos de recuperação mais antigos (30 dias e anterior) e distribuição mensal (janeiro a dezembro). É possível detalhar mais para ver o status de nível do nó da categoria selecionada.

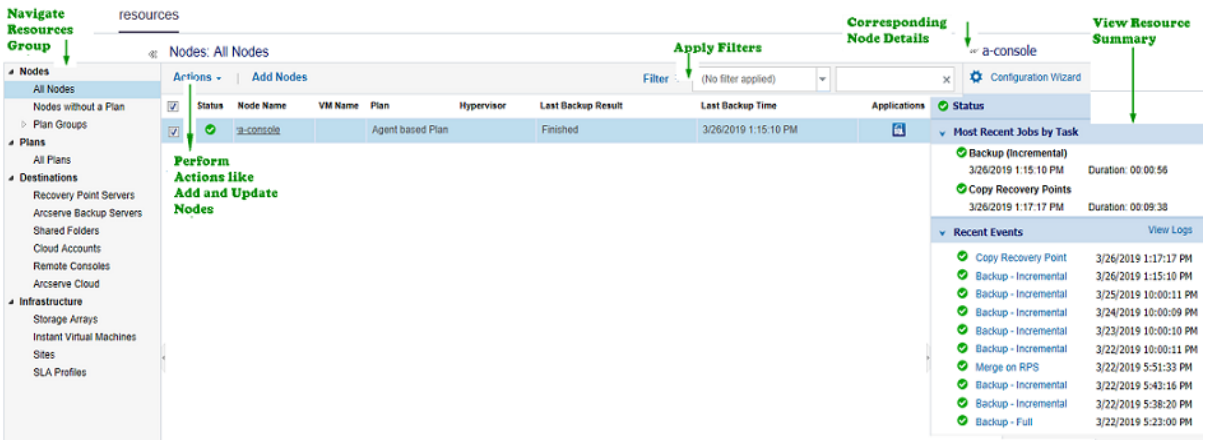
Observação: no painel, é possível exibir diretamente o relatório de RPO de um mês específico. O relatório é preenchido diretamente no painel do Arcserve UDP. Em Painel, se você clicar em um mês no gráfico de barras de RPO, será exibida a tela do relatório de RPO referente a esse mês na página RPO.

Recursos

A guia **recursos** permite gerenciar os recursos do Arcserve Unified Data Protection: nós, destinos, modo de espera virtual e planos. Use essa guia para adicionar recursos ao Arcserve Unified Data Protection, como nós que deseja proteger ou servidores do ponto de recuperação para backup. Você também usa essa guia para criar planos e tarefas de backup, tarefa em modo de espera virtual, e replicação. Na guia de recursos, é possível executar as seguintes opções:

- Gerenciamento de nós
- Gerenciamento de destino
- Gerenciamento de plano
- Gerenciamento de infraestrutura

Observação: apenas a guia **recursos** no console tem reconhecimento de sites. As outras guias no Console exibem dados consolidados de todos os sites. Para obter mais informações sobre Sites, consulte Como adicionar e gerenciar um site.



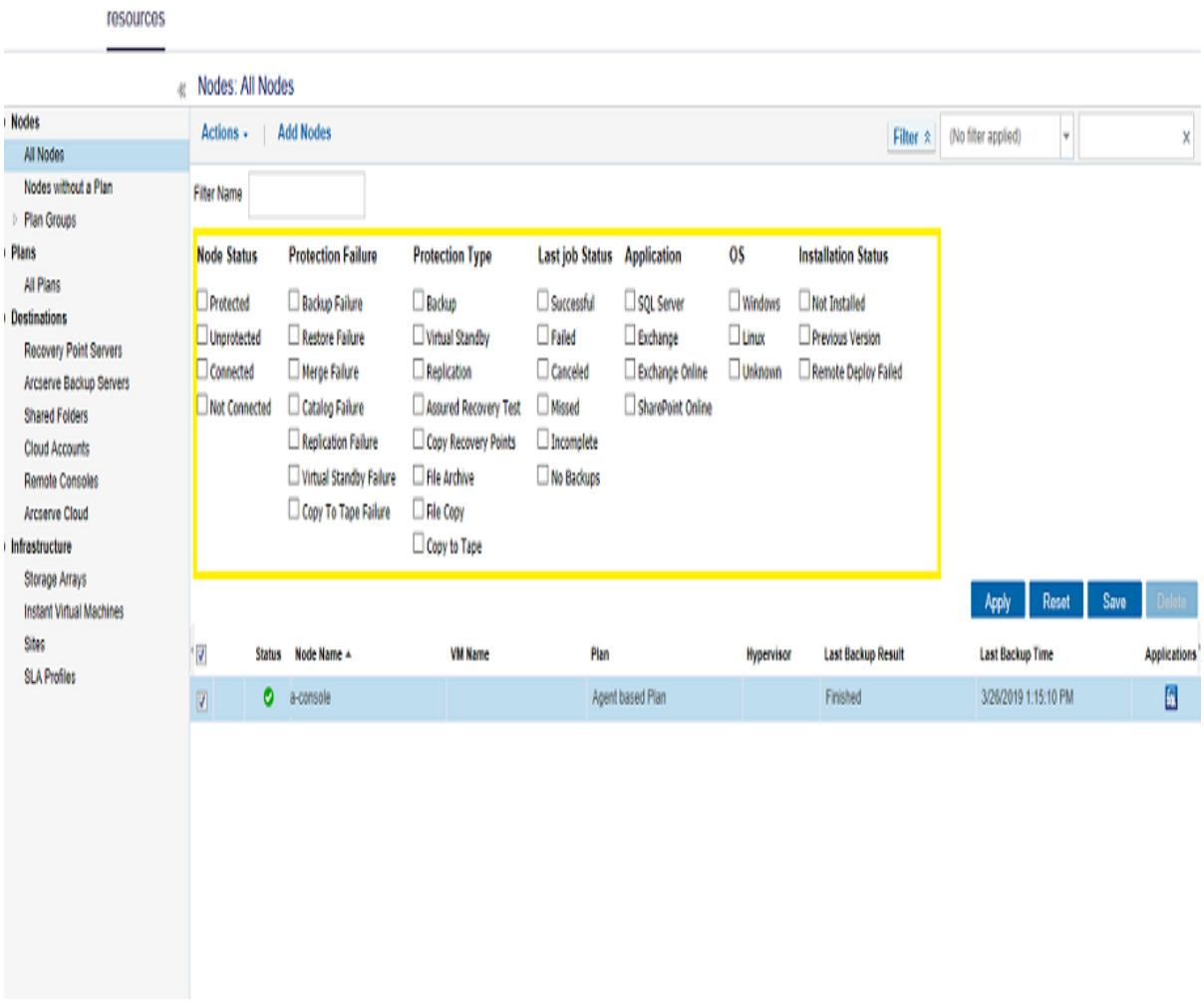
Gerenciamento de nós

A exibição de gerenciamento do nó permite que você gerencie todos os nós e aplique os filtros para refinar a pesquisa de nó. Quando seleciona o nó específico no painel central, será possível ver o status e os eventos recentes sobre o nó no painel direito. É possível aplicar diversos filtros no painel central. É possível criar grupos de nó no painel esquerdo para agrupar nós específicos.

Quando seleciona um nó no painel central, o status do nó e eventos recentes são exibidos no painel direito.

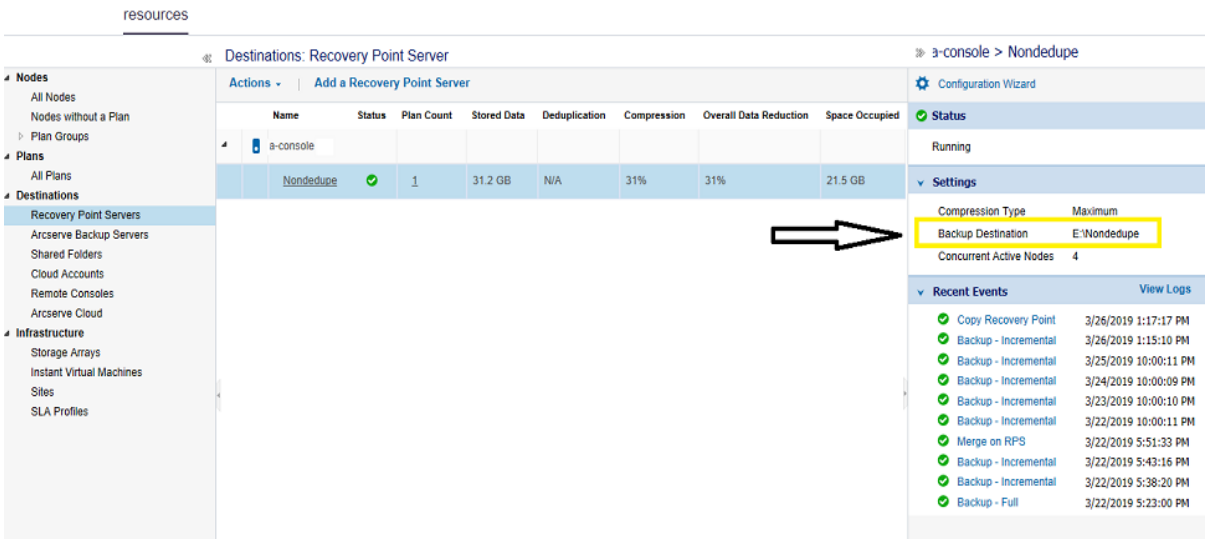
É possível executar operações nos nós clicando no menu suspenso Ações no painel central. Essas operações que podem ser executadas por meio de ações no painel central são aplicadas a todos os nós de origem. Essas operações, que podem ser executadas por meio de ações no painel à direita, são aplicadas somente ao nó selecionado no painel central.

Na guia Recursos, clique em **Todos os nós** sob Nó no painel à esquerda. Em seguida, no painel central, selecione um nó e clique em **Filtrar** para exibir as opções de gerenciamento de nós. Você pode marcar a caixa de seleção das opções desejadas e clicar em **Aplicar**.


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

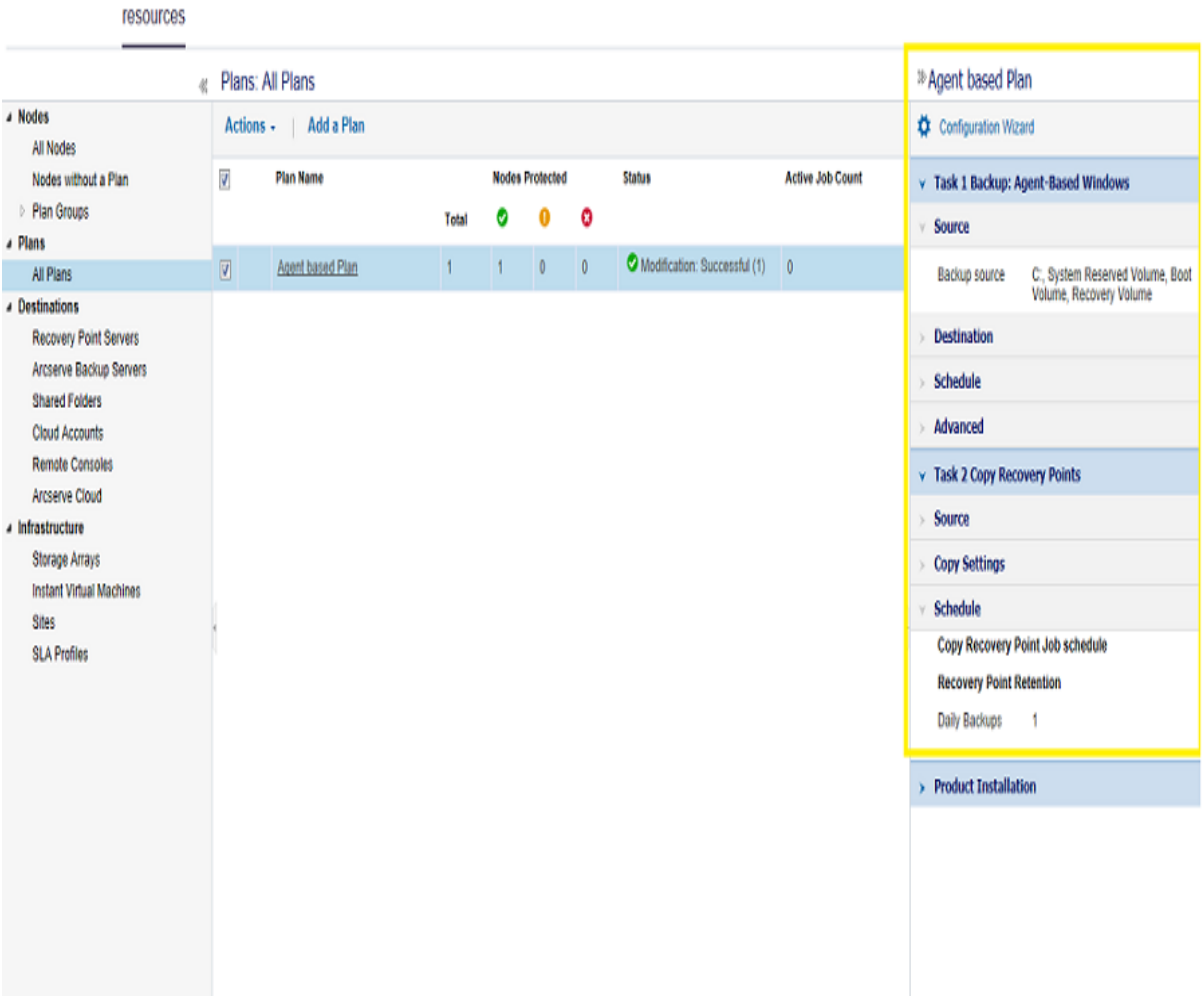
Gerenciamento de destino

A exibição de gerenciamento de destino permite gerenciar os servidores do ponto de recuperação de destino. Ao selecionar um servidor de painel central, seus eventos recentes são exibidos no painel direito. Quando seleciona um repositório de dados, o seu status e as configurações são exibidas no painel direito.



Gerenciamento de plano

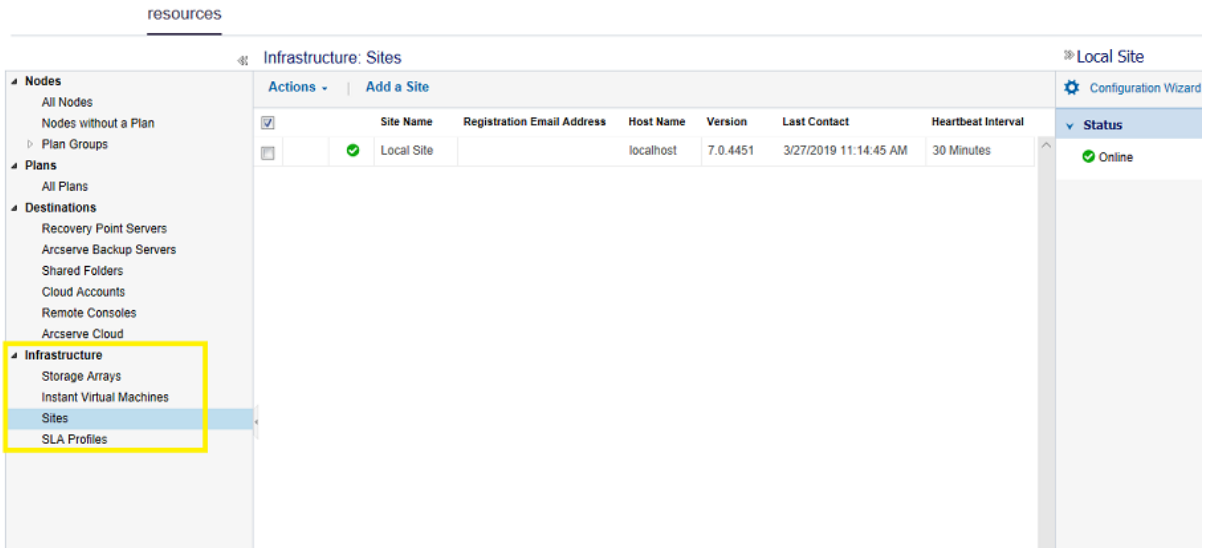
A exibição de gerenciamento do plano permite que você gerencie todos os seus planos. É possível criar, modificar, excluir, implantar, pausar e retomar planos nessa exibição. Os detalhes do plano são exibidos no painel direito. É possível clicar nos campos obrigatórios para exibir os detalhes e gerenciá-los.



Gerenciamento de infraestrutura

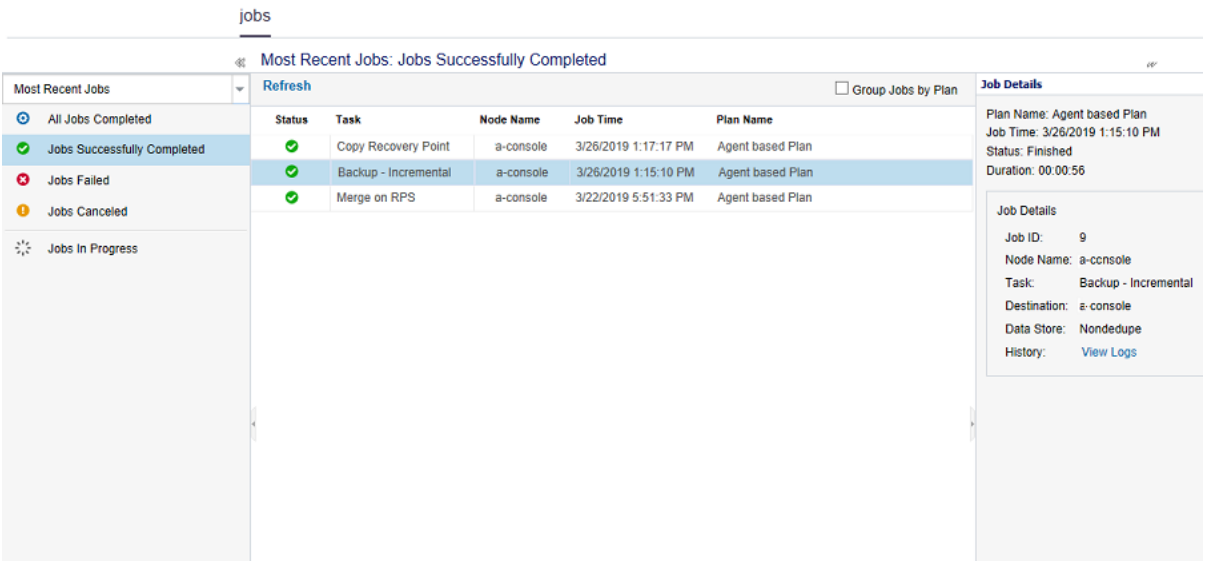
A exibição de gerenciamento da infraestrutura permite gerenciar matrizes de armazenamento, máquinas virtuais instantâneas e sites remotos.

Esta captura de tela mostra o painel de Gerenciamento de infraestrutura:



tarefas

A guia **tarefas** exibe o status das tarefas para um período específico. Use filtros para categorizar os resultados ou agrupar as tarefas por plano.

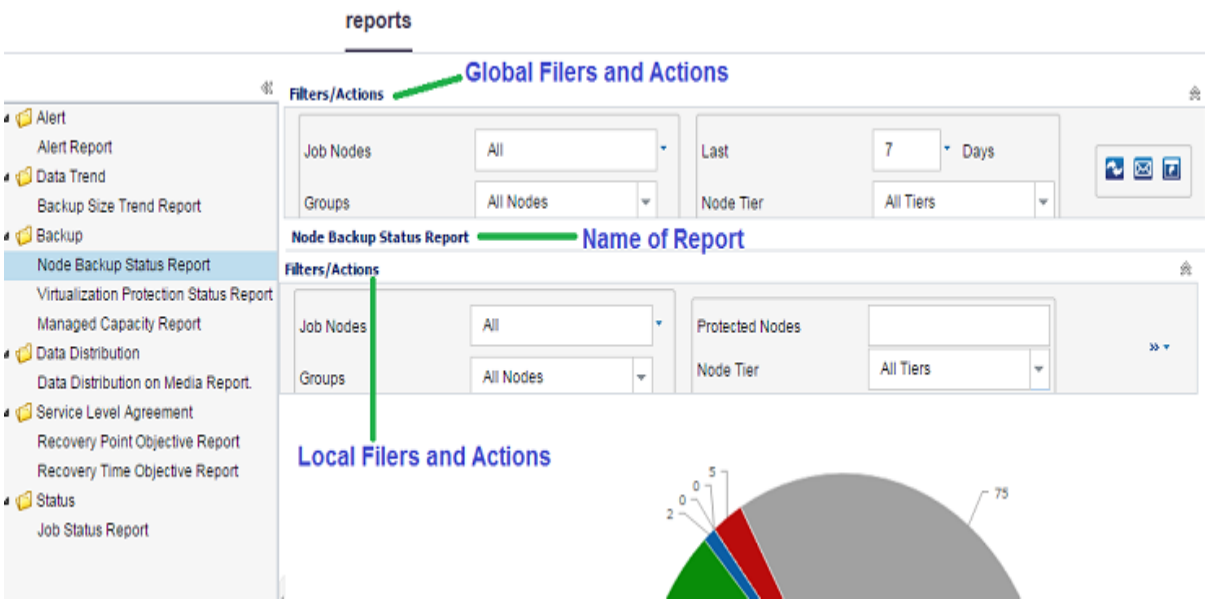


Quando há uma tarefa em andamento, o painel à direita exibe o monitor de tarefas que contém o andamento da tarefa. Clique em **Detalhes da tarefa** no painel direito para abrir o monitor de tarefas. É possível ver os monitores de tarefa apenas se a tarefa estiver em andamento.

Para cancelar uma tarefa, abra o monitor de tarefas e clique em **Cancelar**.

relatórios

A guia **Relatórios** exibe uma lista de relatórios que você pode gerar. É possível aplicar filtros em seus relatórios para obter relatórios específicos. Os relatórios são gerados em formatos CSV, PDF ou HTML. Para obter mais informações sobre esses relatórios, consulte Como gerar relatórios do Arcserve UDP.



log

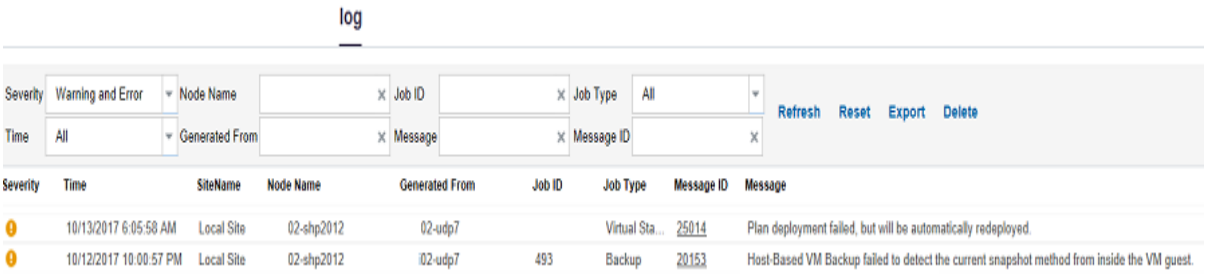
A guia **Logs** exibe todos os logs de atividades para os nós protegidos, servidores de destino, repositórios de dados e planos. É possível visualizar os logs e aplicar diversos filtros, como de gravidade, nó específico, logs gerados no computador, as IDs das tarefas e conteúdo de log.

A ID de mensagem fornece um hiperlink para acessar a documentação detalhada. Clique no hiperlink na coluna MessageID para exibir a descrição e uma solução para a mensagem.

Observação: os logs de atividades gerados pelo console e agente/servidor de backup Linux e a tarefa de Copiar em fita não têm a ID de mensagem.

É possível pesquisar os logs de atividade usando uma combinação dos filtros disponíveis ou uma das seguintes opções:

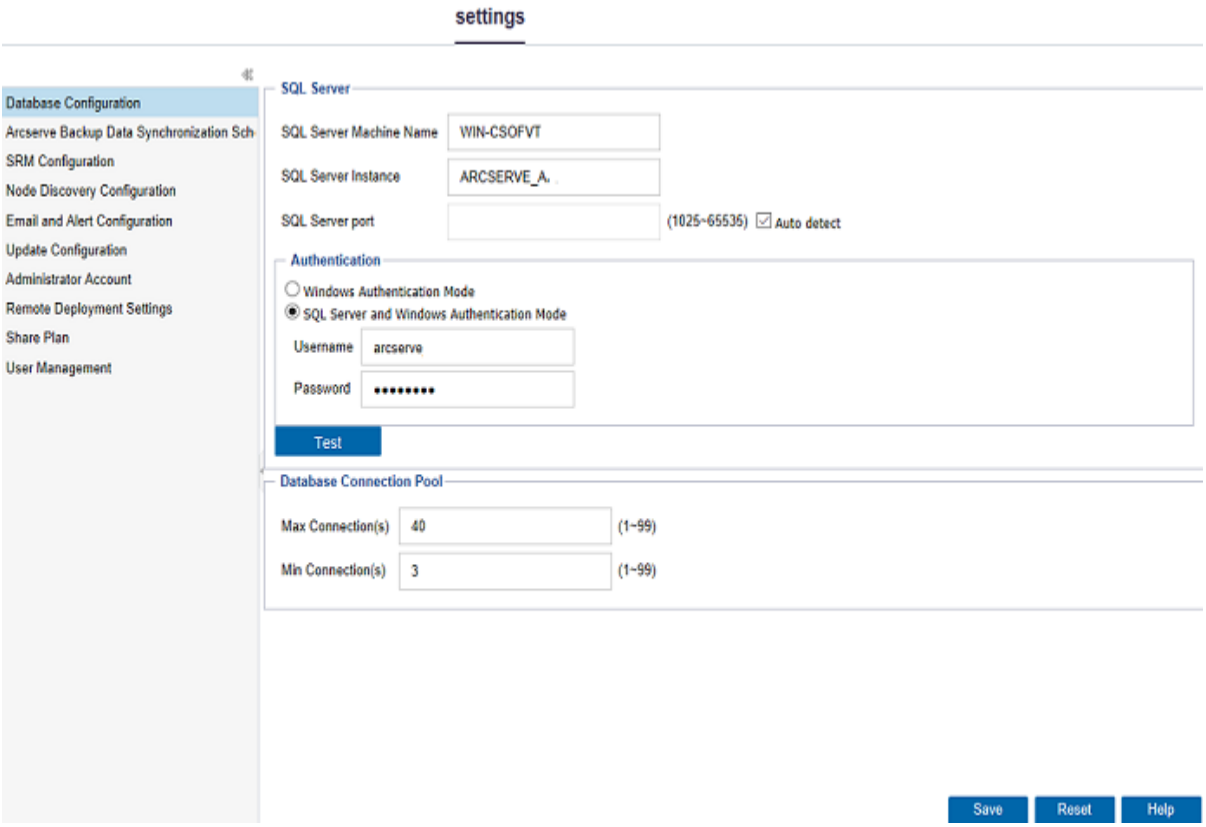
- Selecionar tipos de severidade para exibir todos os logs relacionados ao tipo selecionado.
- Insira outros detalhes (como Nome do nó e ID da tarefa) e clique em **Pesquisar**.
- **Atualizar:** exibe os últimos logs disponíveis de acordo com os filtros definidos.
- **Redefinir:** usa somente os filtros padrão e exibe apenas Aviso e erro para todos os tipos de tarefa.
- **Exportar:** faz download do log de tarefas atual como *.zip (ou seja, activitylog_export_2017_10_12_15_02_27_586.zip) para o diretório de downloads do sistema do Windows.
- **Excluir:** exclui todos os registros de log ou todos os registros de log anteriores à data específica.



configurações

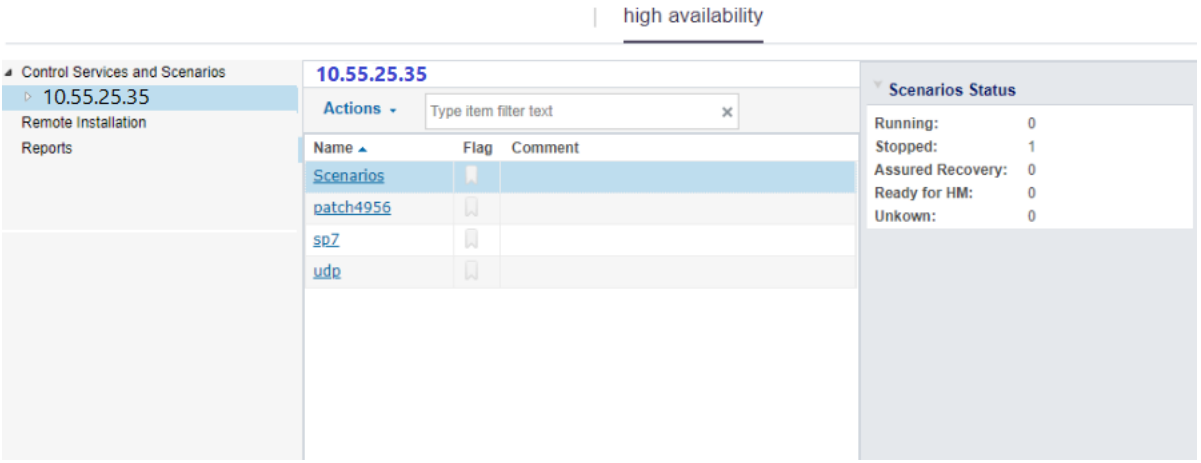
A guia **Configurações** permite definir certas preferências, como aquelas que o servidor de email usa, configurar a ID de usuário administrador e senha, e definir o caminho de implantação de nó padrão.

Para obter mais informações sobre a guia **configurações**, consulte Como configurar o Arcserve UDP.



Alta disponibilidade

A guia **alta disponibilidade** permite que você gerencie e controle as funções do Arcserve High Availability. Se for necessário, insira as credenciais na caixa de diálogo **Adicionar serviço de controle** e exiba os detalhes.

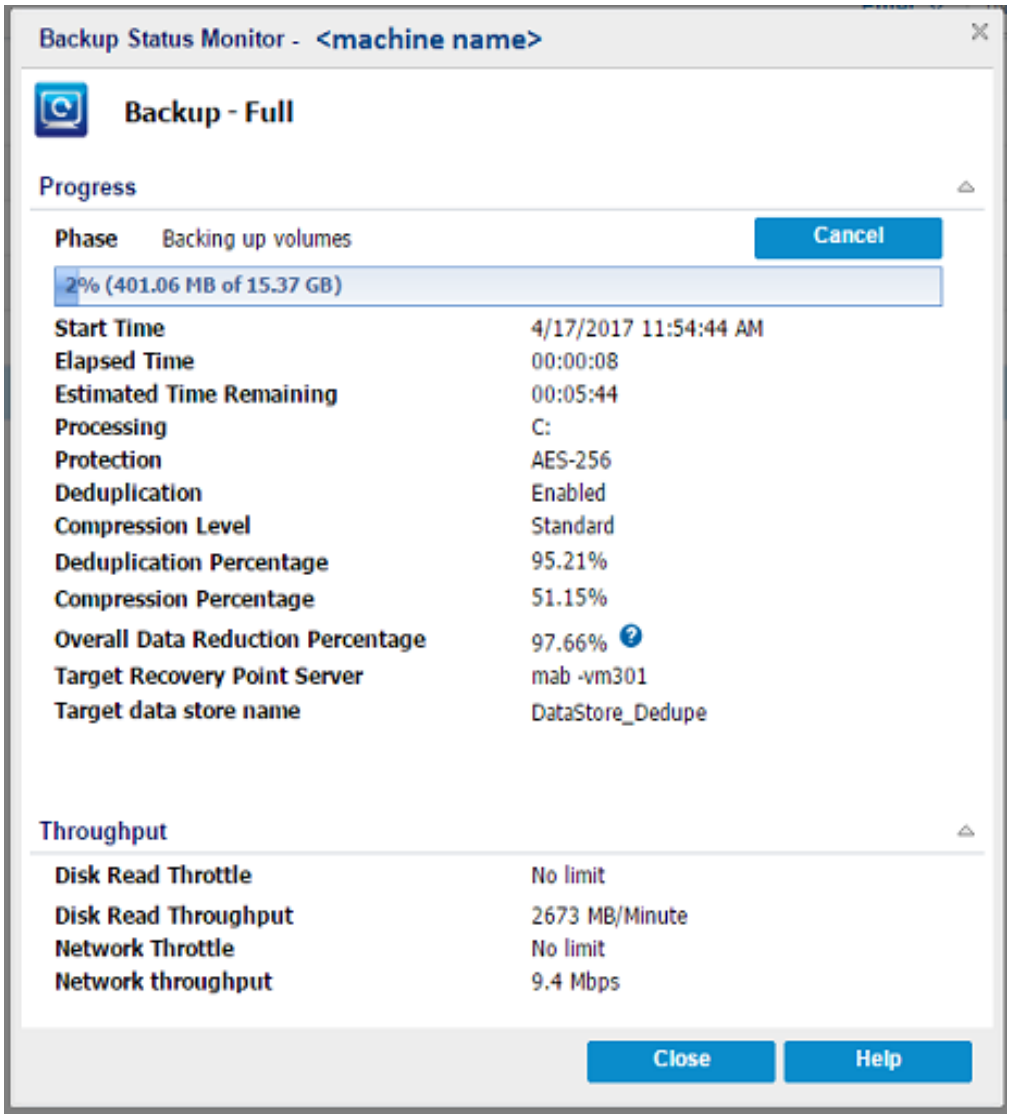


Caixa de diálogo Monitor de tarefas

A caixa de diálogo Monitor de tarefas permite exibir o status de uma tarefa. Quando uma tarefa está em execução, este painel se expande para exibir informações sobre eventos em andamento como o tempo restante estimado para concluir a tarefa, a porcentagem e o tamanho da tarefa já concluída, e o tamanho total da tarefa quando estiver concluída.

Quando uma tarefa estiver em execução, no painel direito, expanda **Eventos recentes** e clique no botão **Detalhes** para abrir os monitores de status e exibir informações mais detalhadas sobre a atual tarefa em execução.

É possível clicar no botão **Cancelar** para interromper a tarefa atual.



Como configurar o Arcserve UDP

Usando o Arcserve Unified Data Protection, é possível especificar as seguintes definições de configuração do Arcserve Unified Data Protection.

- Protocolo de comunicação do servidor
- Configurações de banco de dados
- Sincronização de dados do ARCserve Backup
- Configuração de SRM
- Configuração de detecção de nó
- Configuração de email e alerta
- Definir configurações de proxy
- Atualizar a configuração
- Conta de administrador
- Configurações da implantação remota
- Plano de compartilhamento
- Gerenciamento do usuário
- Configurar a duração do tempo limite do console

Configurar o protocolo de comunicação do servidor

A solução Arcserve Unified Data Protection usa o protocolo HTTP (Hypertext Transfer Protocol) para comunicação entre todos os seus componentes. Caso esteja preocupado com a segurança das senhas comunicadas entre esses componentes, é possível alterar o protocolo em uso para HTTPS (Hypertext Transfer Protocol Secure). Além disso, se você não precisar deste nível extra de segurança, é possível alterar o protocolo em uso para HTTP.

Observação: quando altera o protocolo para HTTPS, um aviso é exibido no navegador web. Esse comportamento ocorre devido a um certificado de segurança autoassinado que solicita que você ignore o aviso e continue ou adicione esse certificado ao navegador para evitar que o aviso seja exibido novamente.

Siga estas etapas:

1. Efetue logon no computador no qual o Console do Arcserve Unified Data Protection está instalado usando uma conta administrativa ou uma conta com privilégios administrativos.

   Observação: se você não efetuar logon usando uma conta administrativa ou uma conta com privilégios administrativos, deverá configurar a linha de comando a ser executada usando o privilégio Executar como administrador.

2. Abra a linha de comando do Windows.

3. Execute uma das seguintes tarefas:

   - Para alterar o protocolo de HTTP para HTTPS:

     Inicie a ferramenta de utilitário "changeToHttps.bat" no seguinte local padrão.

     Observação: o local da pasta BIN pode variar dependendo de onde você instalou o console do Arcserve Unified Data Protection.

     C:\Arquivos de programas\Arcserve\Unified Data Protection\Management\BIN

     Quando o protocolo for alterado com êxito, a seguinte mensagem será exibida:

     O protocolo de comunicação foi alterado para HTTPS.

   - Para alterar o protocolo de HTTPS para HTTP:

     Inicie a ferramenta de utilitário "changeToHttp.bat" no seguinte local padrão

     Observação: o local da pasta BIN pode variar dependendo de onde você instalou o console do Arcserve Unified Data Protection.

C:\Arquivos de programas\Arcserve\Unified Data Protection\Management\BIN

Quando o protocolo for alterado com êxito, a seguinte mensagem será exibida:

O protocolo de comunicação foi alterado para HTTP.

4. Reinicie o navegador e reconecte-se ao Console do Arcserve Unified Data Protection.

Observação: para atualizar o protocolo de comunicação usado pelo servidor de ponto de recuperação do Arcserve Unified Data Protection e o agente do Arcserve Unified Data Protection para se comunicar com o console do Arcserve Unified Data Protection, atualize o nó diretamente no console.

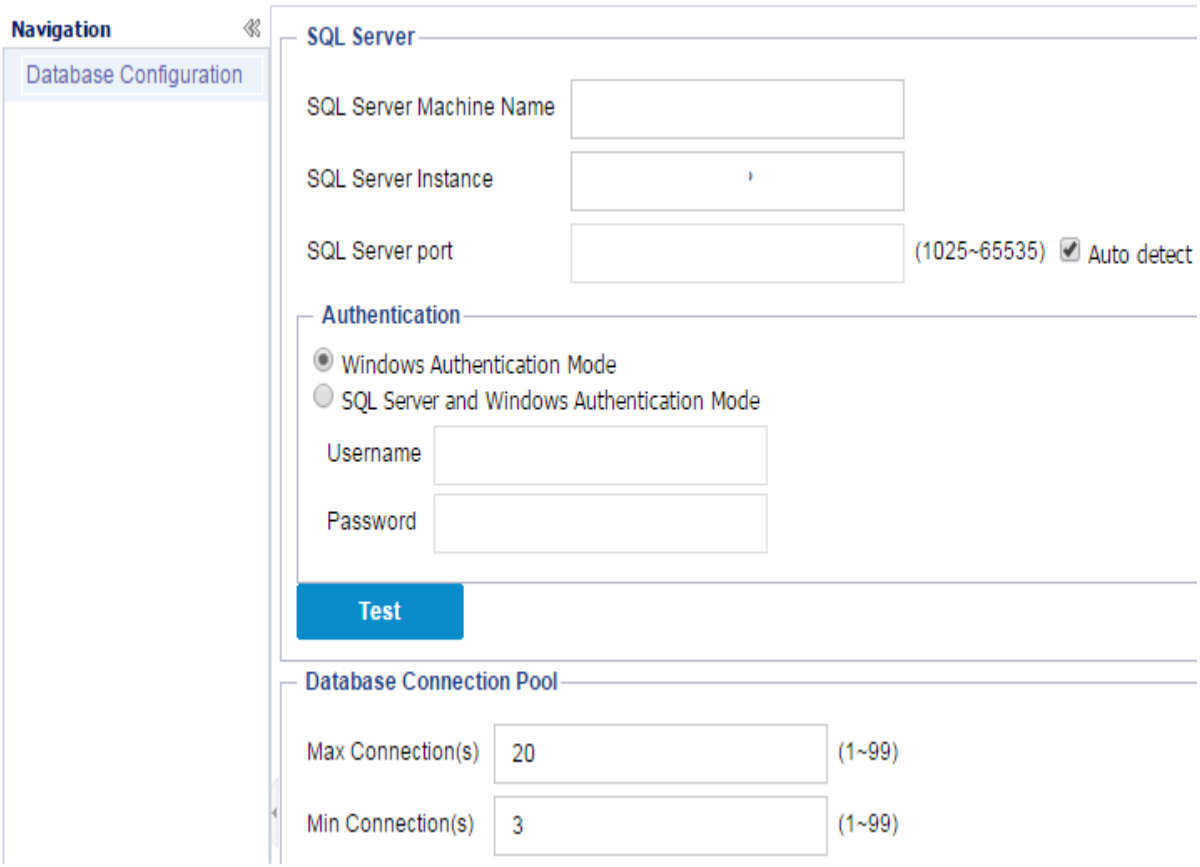
Configurar banco de dados

A página **Configuração do banco de dados** permite inserir detalhes sobre o banco de dados. A configuração do banco de dados exige detalhes sobre o SQL Server, o número de conexões e o modo de autenticação.

Observação: é possível recriar o banco de dados antes de configurar. Exclua o banco de dados do Arcserve Unified Data Protection usando o procedimento descrito em Recriar o banco de dados do Arcserve Unified Data Protection e, em seguida, configure o banco de dados.

Siga estas etapas:

1. No Console, clique na guia **Configurações**.
2. No painel à esquerda, clique em **Configuração do banco de dados**.



Para configurar, preencha os seguintes campos no painel de configuração e clique em **Salvar**.

Nome da máquina do SQL Server

Especifique o nome do servidor que hospeda a instância do SQL Server.

Instância do SQL Server

Especifique o nome da instância do SQL Server.

Porta do SQL Server

Especifique o número da porta para esta instância ou ative a opção **Detecção automática**. O intervalo de opções de número de porta é de 1025 a 65535.

Detecção automática

Marcar a caixa de seleção permite que o aplicativo encontre o número da porta.

Autenticação

Selecione um dos modos de autenticação entre as seguintes opções:

Modo de autenticação do Windows: modo padrão:

(Opcional) **Teste**: clique em Testar para verificar se o aplicativo pode se comunicar com a instância do Microsoft SQL Server.

Modo de autenticação do Windows e SQL Server:

Selecione a opção e preencha os campos Nome de usuário e Senha.

Valores do Pool de conexões do banco de dados

Para especificar o máximo e o mínimo de conexões, digite um valor entre 1 e 99.

A configuração do servidor de banco de dados foi definida.

Use a opção **Redefinir** para limpar todos os valores especificados e carregar os dados originais.

Recriar o banco de dados do Arcserve Unified Data Protection

Por vários motivos, você pode desejar recriar o banco de dados do Arcserve Unified Data Protection. Por exemplo, o banco de dados atual consome mais que 10 GB de dados. Para recriar o banco de dados, é necessário primeiro excluir o banco de dados existente do Arcserve Unified Data Protection e, em seguida, configurar um novo banco de dados a fim de substituir o banco de dados excluído. Ele se aplica aos bancos de dados do Microsoft SQL Server e Microsoft SQL Server Express Edition.

Importante: Ao excluir o banco de dados do Arcserve Unified Data Protection, todos os dados atuais serão perdidos.

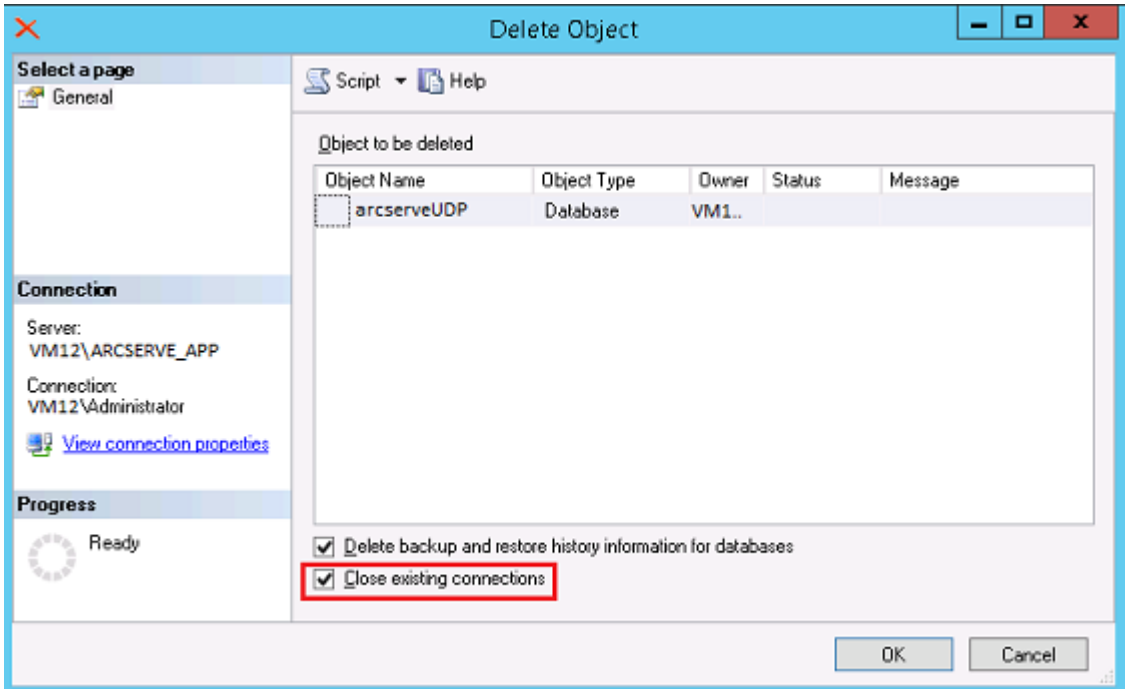
Para recriar o banco de dados do Arcserve Unified Data Protection

1. Abra o Microsoft SQL Server Management Studio Express e efetue logon na instância ARCSERVE_APP.

   Observação: se o Microsoft SQL Server Management Studio Express não estiver instalado no servidor do Arcserve Unified Data Protection, faça download do utilitário pelo Centro de Download da Microsoft.

2. Clique com o botão direito do mouse em arcserveUDP e escolha **Excluir** na lista de opções.

   A caixa de diálogo **Excluir objeto** é exibida.



3. Na caixa de diálogo **Excluir objeto**, clique nas opções **Fechar conexões existentes** e, em seguida, clique em **OK**.

   O banco de dados existente do Arcserve Unified Data Protection é excluído.

4. Configure o novo banco de dados. Para obter mais informações, consulte Configurar banco de dados.

   A solução Arcserve Unified Data Protection recria o banco de dados. O nome da instância do banco de dados é **ARCSERVE_APP**.

Configurar a sincronização de dados de backup do Arcserve

É possível configurar a **Programação de sincronização de dados de backup do Arcserve**.

Siga estas etapas:

1. No Console, clique na guia **Configurações**.
2. No painel à esquerda, clique em **Programação de sincronização de dados do Arcserve Backup**.
3. No painel direito, clique em **Ativar**.

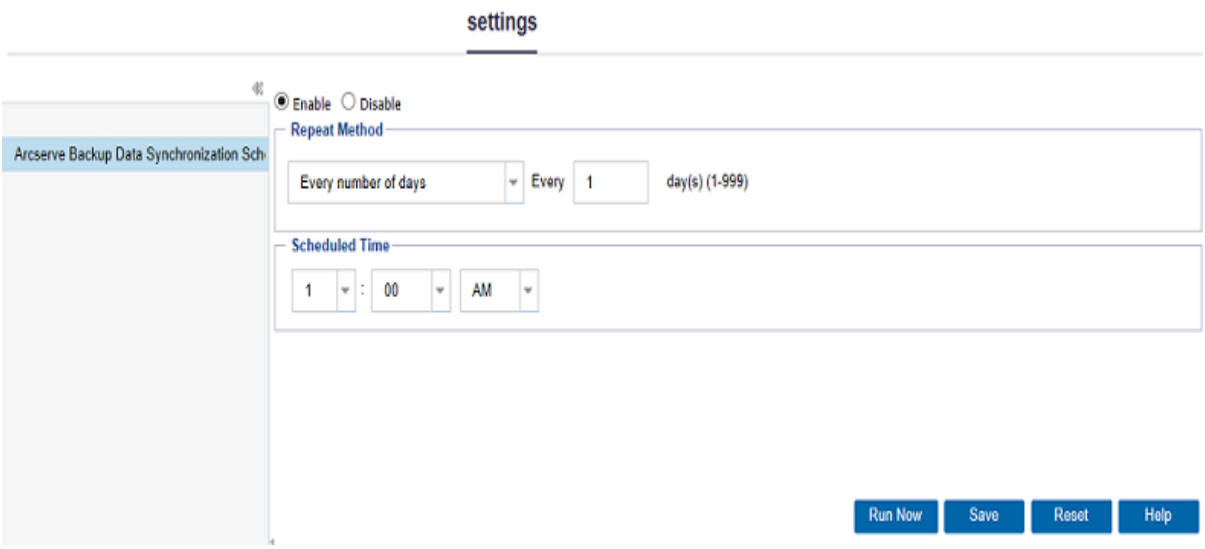
   Por padrão, a **Sincronização de dados do Arcserve Backup** está ativada.

   Observação: clicar em **Desativar** interrompe a programação.
4. Especifique os seguintes parâmetros para programar a Sincronização de dados do Arcserve Backup:
   - **Método de repetição**
   - **Hora programada**
5. Clique em **Salvar**.

   A programação da sincronização de dados do Arcserve Backup é aplicada.

   Observação: não clique em **Salvar** caso queira executar a sincronização imediatamente.
6. (Opcional) Para executar o processo imediatamente, clique em **Executar agora**.

   A caixa de diálogo **Nó** é exibida com a lista de nós disponíveis para sincronização.



7. Selecione os nós que deseja executar na sincronização e clique em **OK**.

Configurar o SRM

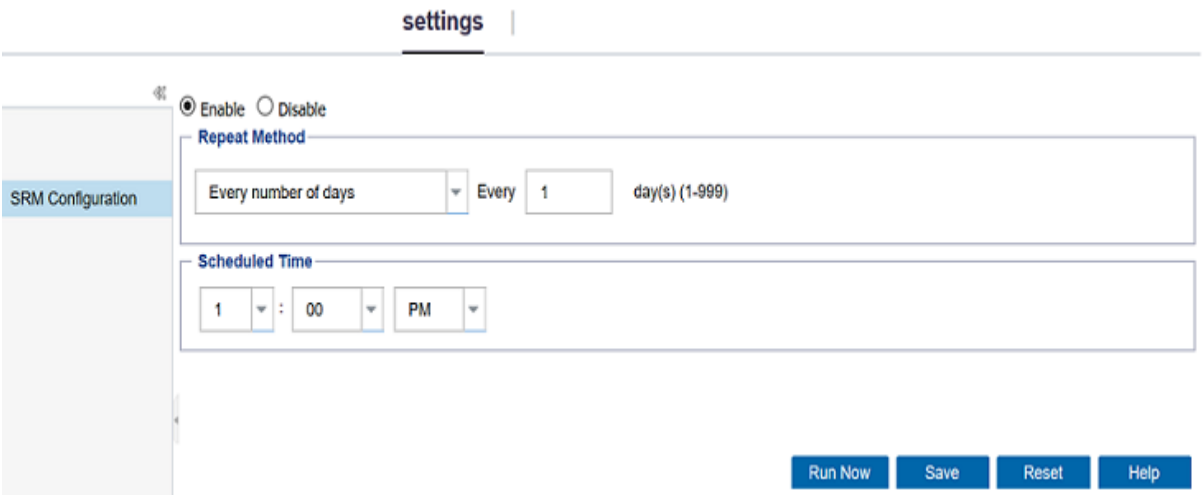
A página Configuração de SRM permite que você configure uma programação de SRM para os nós que definem quando e com que frequência coletar dados de SRM. SRM (Storage Resource Management) é a funcionalidade que coleta informações sobre os seguintes dados:

- Hardware, software e dados do aplicativo para implementações do Microsoft SQL Server e do Microsoft Exchange Server.
- Dados de PKI (Performance Key Indicators – Indicadores Principais de Desempenho) dos nós.

Siga estas etapas:

1. No Console, clique na guia **Configurações**.
2. No painel esquerdo, clique em **Configuração do SRM**.
3. No painel direito, clique em **Ativar**.

   Por padrão, a **Configuração de SRM** está ativada.



   Observação: clicar em **Desativar** interrompe a programação.

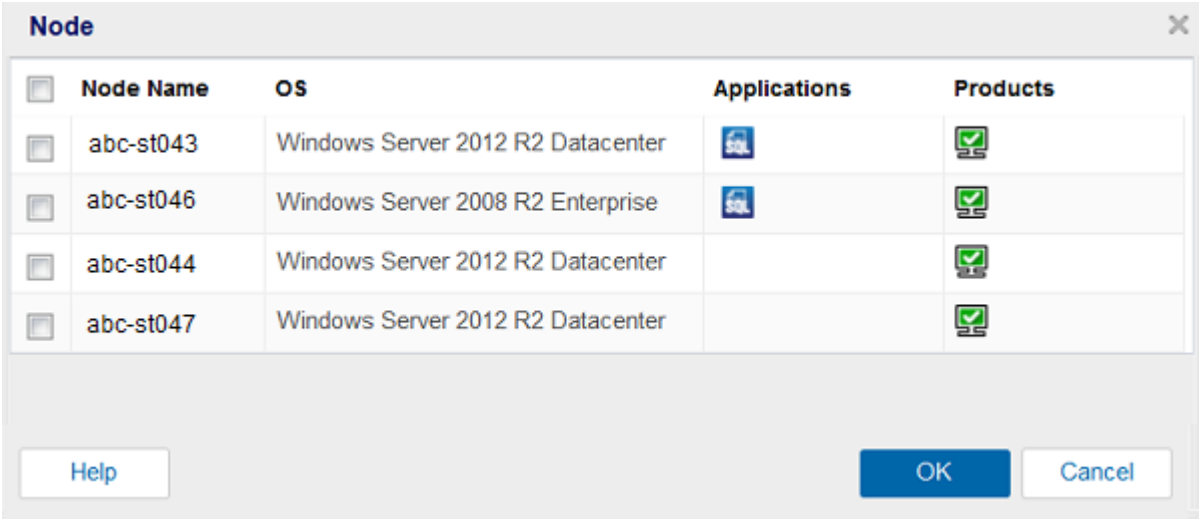
4. Especifique os seguintes parâmetros para programar o SRM:
   - **Método de repetição**
   - **Hora programada**
5. Clique em **Salvar**.

   A programação do SRM é aplicada.

   Observação: não clique em **Salvar**, caso deseje coletar dados de SRM imediatamente.

6. (Opcional) Para executar o processo imediatamente, clique em **Executar agora**.

   A caixa de diálogo **Nó** é exibida com a lista de nós disponíveis para sincronização.



7. Selecione os nós que deseja executar na sincronização e clique em **OK**.

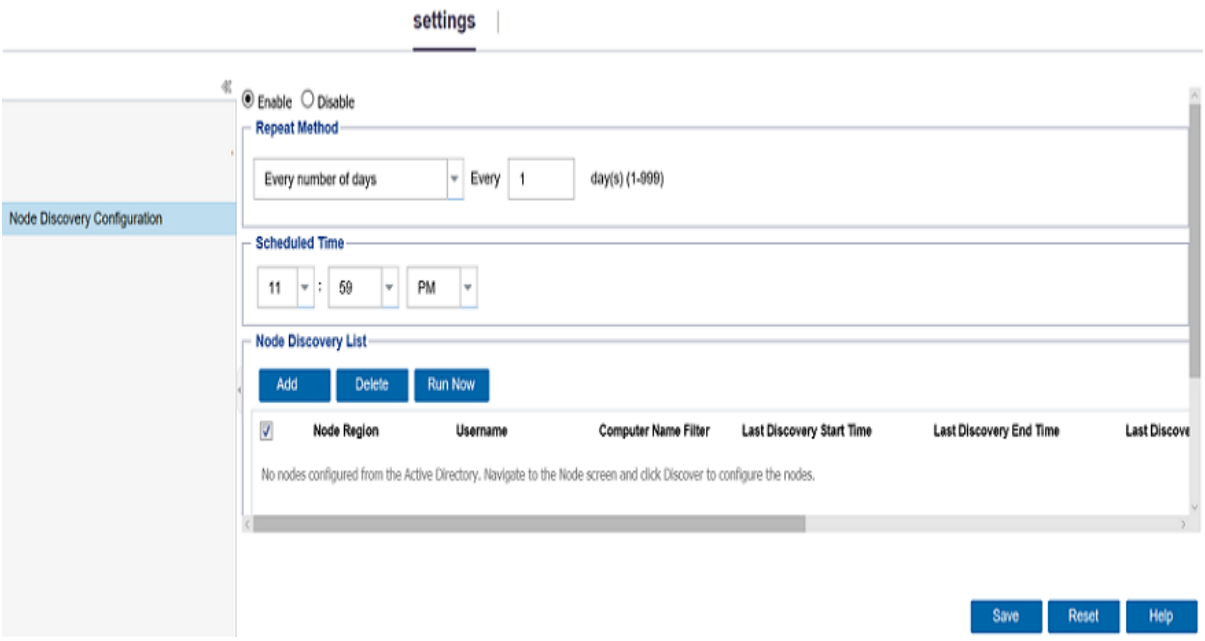
Configuração de detecção de nó

A página **Configuração de detecção de nó** permite configurar o Active Directory, o VMware vSphere e a programação de detecção do nó do Microsoft Hyper-V de forma repetitiva e em um horário agendado. Quando são detectados novos nós, é enviado um alerta por email ao administrador para ele adicionar manualmente esses nós. Por padrão, a **Configuração da detecção** está desativada.

Siga estas etapas:

1. No Console, clique na guia **Configurações**.
2. No painel à esquerda, clique em **Configuração de detecção de nó**.

   Para ativar a configuração, clique na opção **Ativar** para especificar o tipo de método de repetição desejado e um horário programado para que a detecção de nó seja iniciada.



É possível especificar os seguintes parâmetros para configurar a programação de detecção:

- **Cada quantidade de dias:** permite repetir este método no número de dias especificado. (Padrão)
- **Cada dia selecionado da semana:** permite repetir este método nos dias especificados. Segunda-feira, Terça-feira, Quarta-feira, Quinta-feira e Sexta-feira são o padrão para os dias da semana.
- **Cada dia selecionado do mês:** permite repetir este método no dia especificado do mês. 1 é a opção padrão para o dia do mês.

- **Hora programada:** permite especificar a hora em que a detecção é executada, conforme a programação de repetição.
- **Lista de detecções de nós>Adicionar:** selecionar de onde deseja adicionar nós. Em seguida, especifique as credenciais necessárias.

  Observação: como alternativa, clique em **Executar agora** para executar a detecção imediatamente.

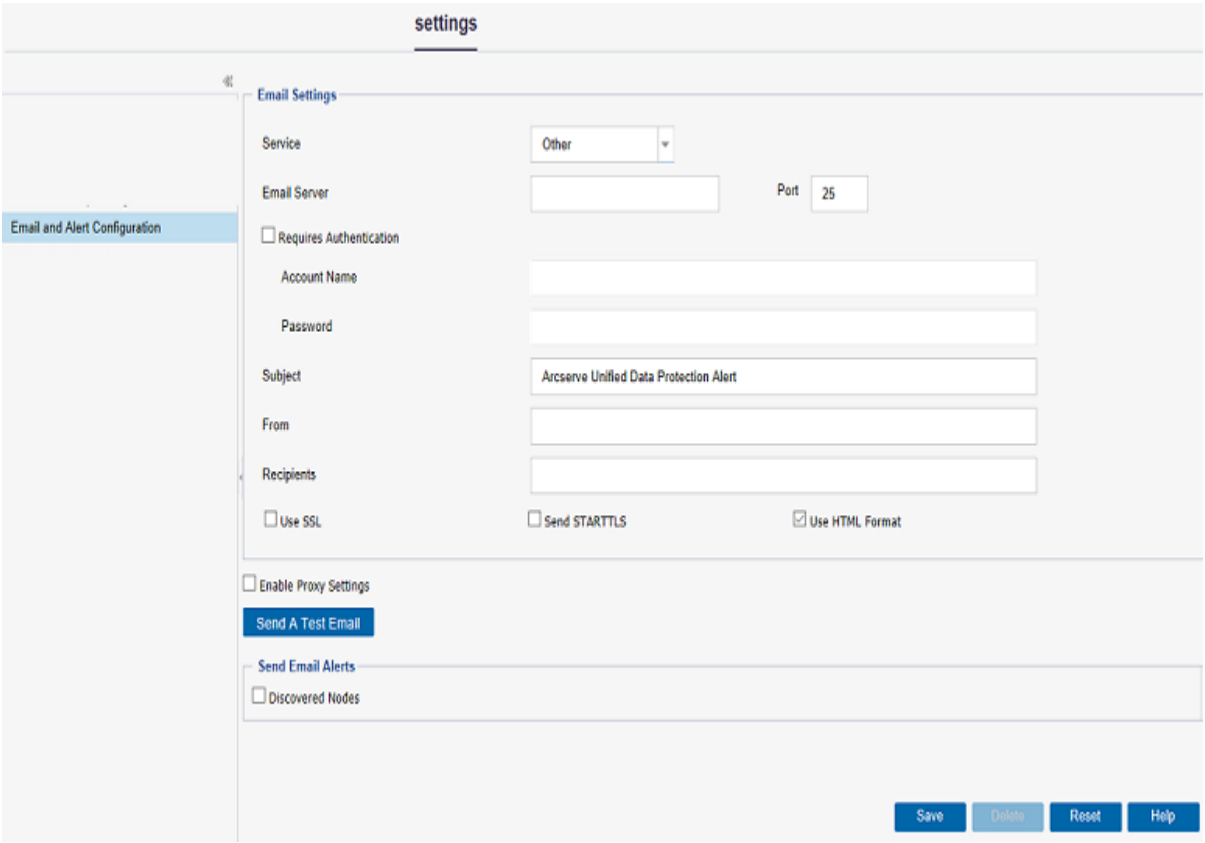
Configurar emails e alertas

A página **Configuração de alerta e email** permite fornecer definições de email e configurações de alertas por email.

Observação: como pré-requisito, instale o Microsoft .NET Framework (versão 2.0 ou superior) no computador em que você instalou o console para o recurso de exportação de gráfico de relatório, para exportar as imagens em um relatório com êxito.

Siga estas etapas:

1. No Console, clique na guia **Configurações**.
2. No painel à esquerda, clique em **Configuração de email e alerta**.
3. Insira detalhes para definir as configurações padrão.



Serviço

Selecione serviços de email a partir das opções disponíveis.

Servidor de email

Especifique o nome de host do servidor SMTP que deseja usar para enviar os alertas por email.

Porta

Especifique o número da porta relacionada ao servidor de email.

Requer autenticação

Marque a caixa de seleção para inserir as credenciais.

Usar SSL/Enviar STARTTLS/Usar formato HTML

Selecione a opção desejada para especificar os requisitos.

Ativar configurações de proxy

Marque a caixa de seleção para fornecer os detalhes do **Servidor proxy** e da Autenticação.

Email de teste

Clique nesse botão para verificar os detalhes inseridos na seção Configurações de email.

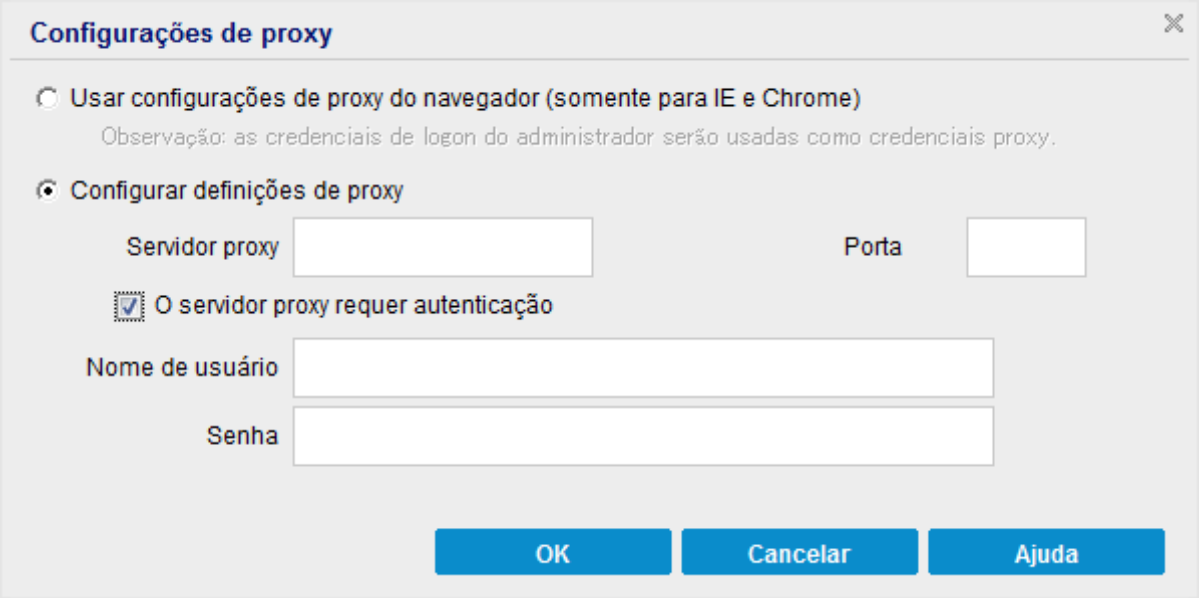
Enviar alertas por email

Selecione **Nós detectados** para configurar os nós do **Active Directory** que podem ser encontrados pela opção Detectar, disponível para os nós na guia **Recursos**.

Definir configurações de proxy

Selecione **Configurações de proxy** para especificar se deseja que o Arcserve UDP se comunique por meio do servidor proxy. Um servidor proxy age como um intermediário entre o seu servidor e o servidor Arcserve UDP para garantir a segurança, maior desempenho e controle administrativo. Ele serve como a conexão para o servidor Arcserve UDP a partir do qual o servidor de download obterá as atualizações.

Quando você seleciona o servidor da Arcserve como servidor de download, a caixa de diálogo **Configurações de proxy** é aberta.



- **Usar configurações de proxy do navegador**

  Esta seleção é aplicável somente ao Windows Internet Explorer e Google Chrome.

  Quando selecionada, direciona o Arcserve UDP para detectar automaticamente e usar as mesmas configurações de proxy aplicáveis ao navegador, com o objetivo de se conectar ao servidor do Arcserve para obter informações sobre atualizações do Arcserve UDP.

- **Definir configurações de proxy**

  Quando selecionada, permite que o servidor proxy especificado se conecte ao servidor do Arcserve para obter informações sobre atualizações do Arcserve UDP. Caso selecione esta opção, será necessário incluir também o endereço IP (ou nome do computador) do servidor proxy e o número da porta correspondente, usado pelo servidor proxy em conexões com a internet.

Além disso, você também pode especificar se o servidor proxy requer autenticação. Quando selecionado, especifica que as informações de autenticação (ID e senha do usuário) são obrigatórias para usar o servidor proxy.

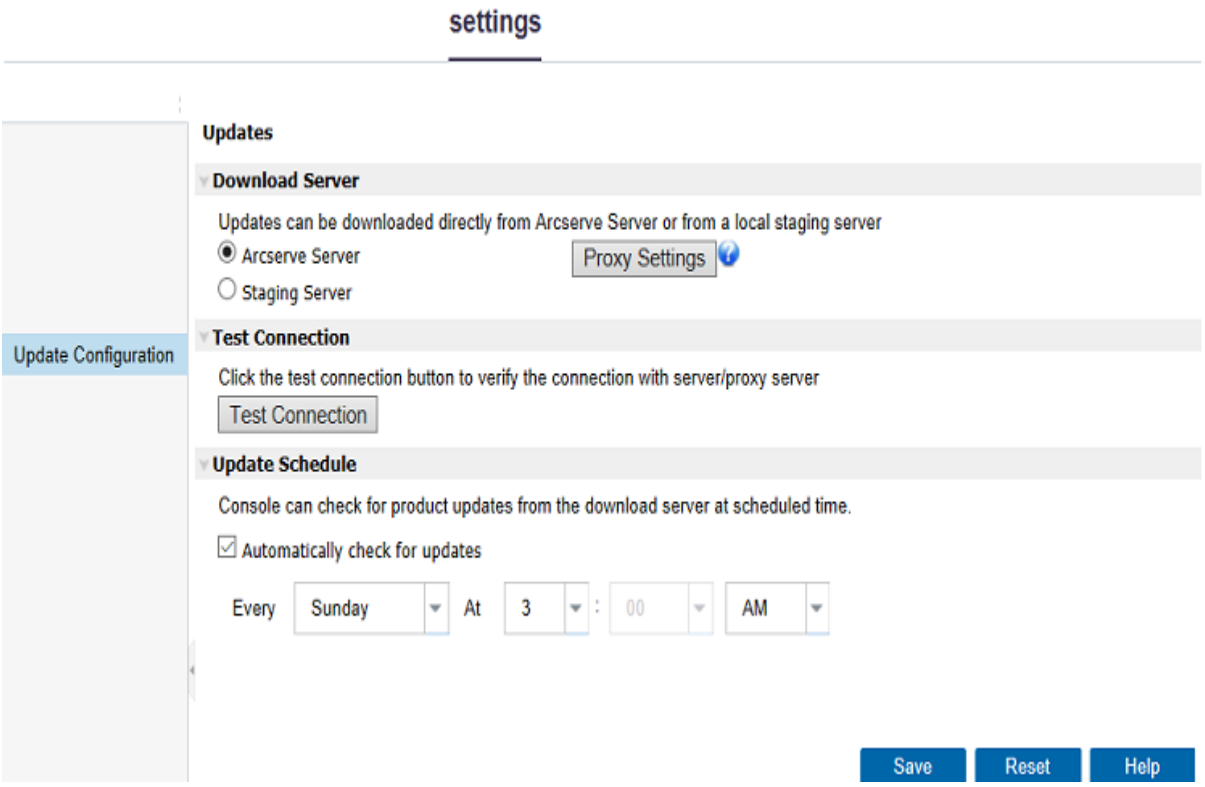
Observação: o formato do nome de usuário deve corresponder a um nome de usuário de domínio totalmente qualificado na forma <nome de domínio>\<nome de usuário>.

Atualizar a configuração

A página Atualizar configuração permite definir a programação do Servidor de download e Atualização para configurar atualizações. Você pode fornecer detalhes sobre as configurações de proxy do Servidor Arcserve ou do servidor de armazenamento temporário para o servidor de download.

Siga estas etapas:

1. No Console, clique na guia **Configurações**.
2. No painel à esquerda, clique em **Atualizar configuração**.



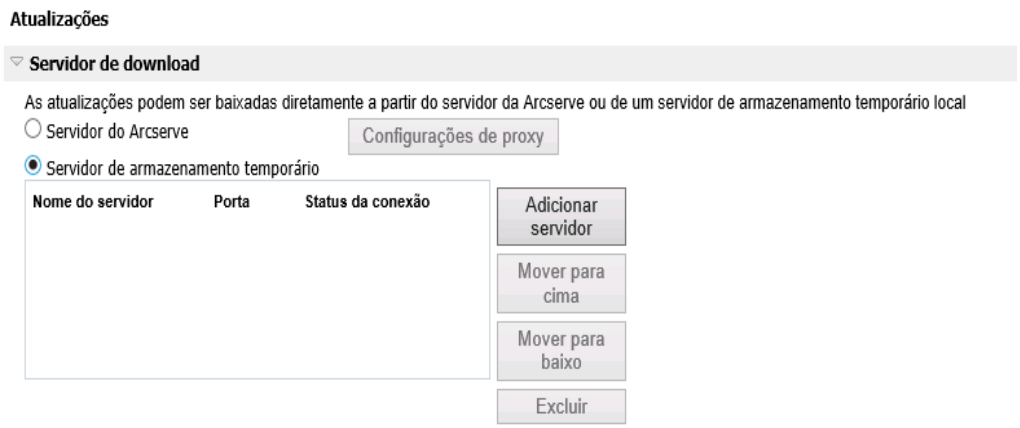
Forneça detalhes sobre o tipo de servidor de atualização e sobre a programação de atualização. O servidor de atualização é um Servidor Arcserve ou um servidor de armazenamento temporário.

3. Para o **servidor de download**, selecione uma das seguintes opções:
   - Para o **Servidor Arcserve**, clique em **Configurações de proxy** para concluir a configuração.
   - Para o **servidor de armazenamento temporário**, clique em **Adicionar servidor** para fornecer os detalhes do servidor de armazenamento temporário.

Para criar um servidor de armazenamento temporário, veja Como criar um servidor de armazenamento temporário.

Se o servidor de armazenamento temporário estiver protegido por um firewall, prepare um computador que possa acessar a internet, tenha o produto UDP instalado e receba as atualizações mais recentes do servidor da Arcserve. Em seguida, copie as pastas **EngineUpdates** e **FullUpdates** do local a seguir para o computador do servidor de armazenamento temporário:

<caminho de instalação do UDP>\ Arcserve\Unified Data Protection\Update Manager



Observações:

- Como o recurso Atualizar automaticamente não precisa de licença, não é necessário ativar a licença no servidor de armazenamento temporário.
- Para obter mais informações sobre as portas, consulte Portas de comunicação usadas pelo Arcserve UDP.

É possível adicionar vários servidores de armazenamento temporário.

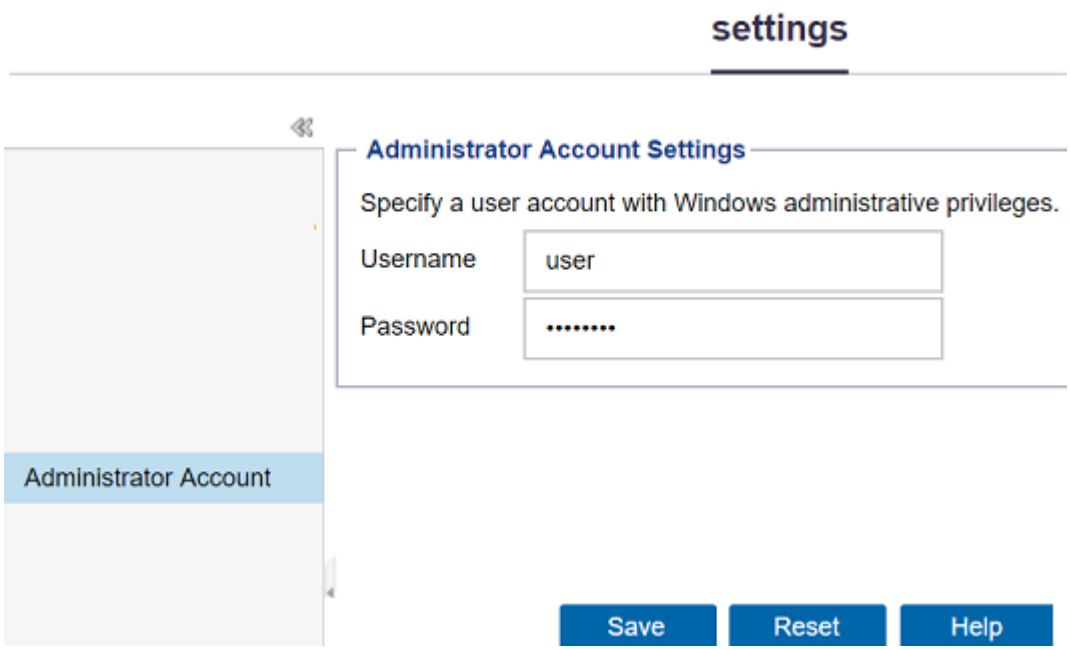
4. Clique em **Testar conexão** para verificar os detalhes do **Servidor de download**.
5. Forneça os detalhes da **programação de atualizações**.
6. Selecione a opção **Verificar atualizações automaticamente**.
7. Clique em **Salvar** para concluir atualização.

Configurar a conta de administrador

A página **Conta de administrador** permite criar uma conta de usuário fornecendo um **nome de usuário** e **senha**.

Siga estas etapas:

1. No Console, clique na guia **Configurações**.
2. No painel à esquerda, clique em **Conta de administrador**.



3. Forneça as credenciais da sua conta de administrador e clique em **Salvar**.

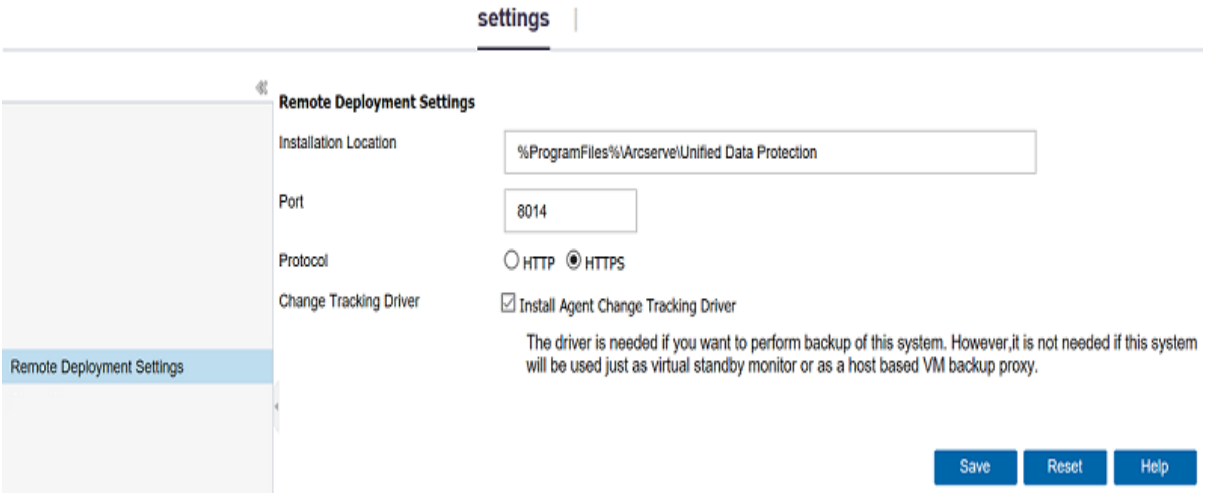
Configurações da implantação remota

A página **Configurações de implantação remota** permite especificar as configurações padrão para a instalação do Agente do Arcserve Unified Data Protection e do Servidor do ponto de recuperação do Arcserve Unified Data Protection. Especifique as configurações de instalação padrão para fornecer o local da instalação.

Forneça os detalhes sobre o **caminho de instalação**, **protocolo** e **porta** e clique em **Salvar**.

Siga estas etapas:

1. No Console, clique na guia **Configurações**.
2. No painel à esquerda, clique em **Configurações de implantação remota**.



3. Insira os detalhes conforme necessário e clique em **Salvar**.

Mapear o plano para a conta de usuário

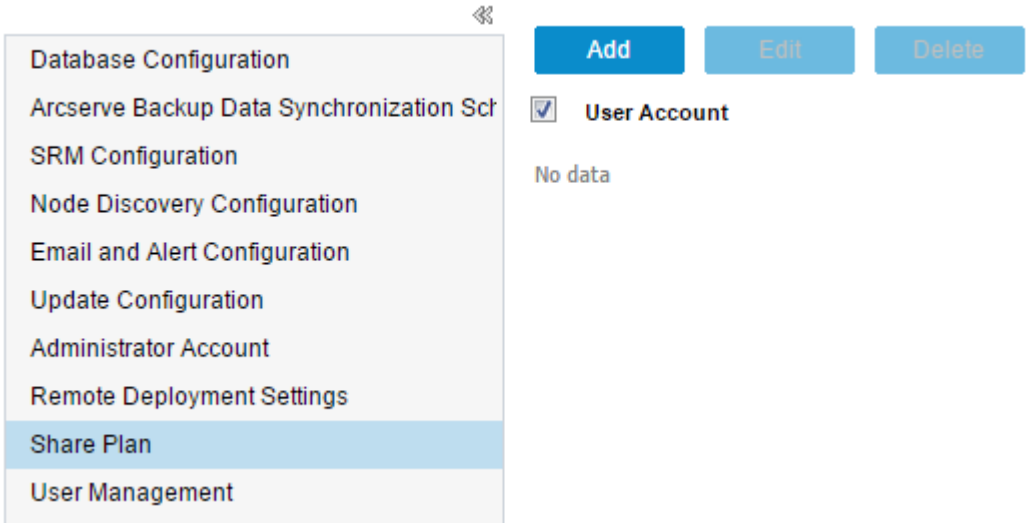
Administrador do destino

Você já criou uma conta de usuário e um plano para um console de origem. Para identificar e gerenciar dados replicados, atribua o plano à conta de usuário.

Observação: é possível atribuir mais de um plano a uma conta de usuário, mas duas contas diferentes não podem compartilhar um plano. No entanto, recomendamos atribuir um único plano a uma conta de usuário, para que você possa identificar e gerenciar facilmente os dados replicados.

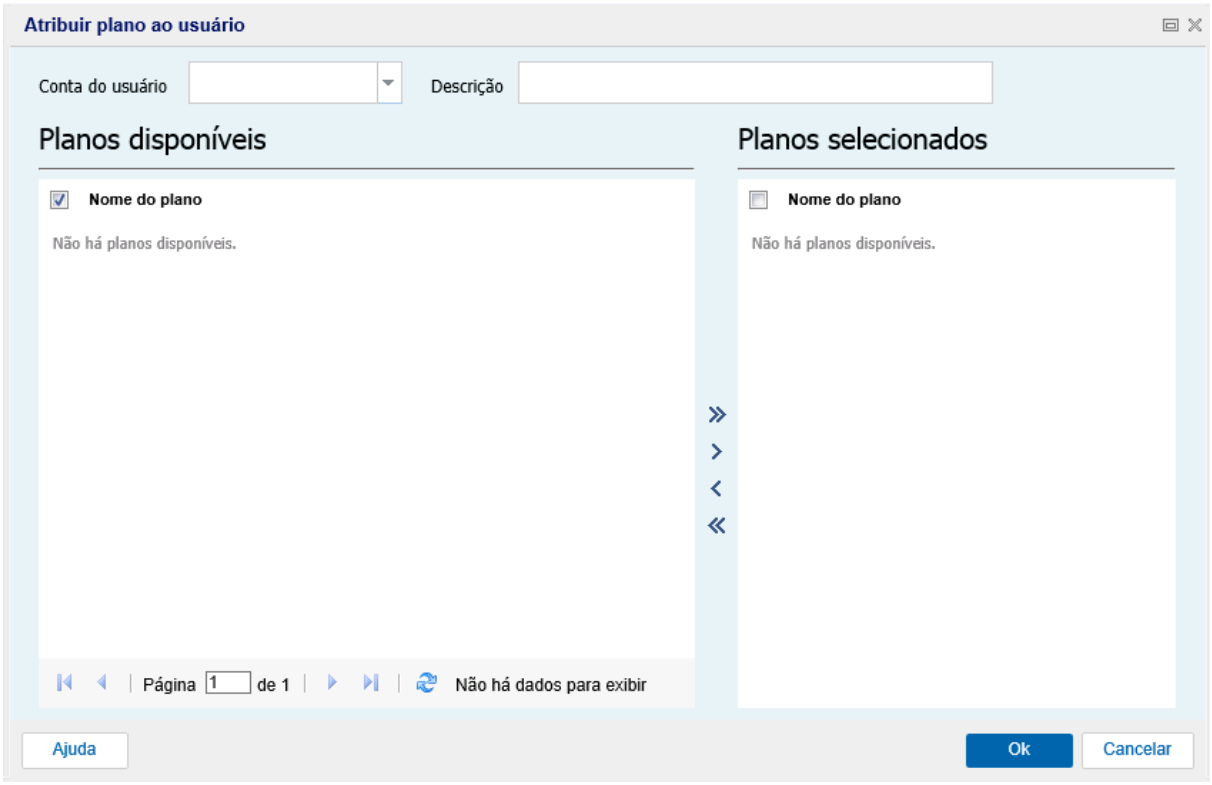
Siga estas etapas:

1. No Console, clique na guia **Configurações**.
2. No painel à esquerda, clique em **Plano de compartilhamento**.



3. No painel central, clique em **Adicionar**.

   A caixa de diálogo **Atribuir plano ao usuário** é exibida.



4. Selecione a **conta de usuário**.
5. Selecione um plano na coluna **Planos disponíveis**.

   Observação: se um plano já foi adicionado a um nome de usuário, ele não será exibido na coluna **Plano disponível**.
6. Clique em **Adicionar todos os planos** ou em **Adicionar planos selecionados** para adicionar os planos na coluna **Planos selecionados**.
7. Clique em **OK**.

   A caixa de diálogo **Atribuir plano ao usuário** é fechada. O nome de usuário e os planos associados são exibidos na página **Plano de compartilhamento**.

   A conta de usuário está mapeada para o plano criado para o console de origem.

   É possível usar a opção **Editar** para modificar a configuração do usuário ou **Excluir** para remover a conta de usuário da lista.

Gerenciamento do usuário

A página Gerenciamento de usuários permite fazer o seguinte:

- Efetuar logon no console de gerenciamento de usuários (console do serviço de identidade) a partir do console do Arcserve UDP. Para obter mais informações, consulte Iniciar o console de gerenciamento de usuários do Arcserve UDP.
- Ativar e configurar a autenticação multifator (MFA) para todos os usuários. Para obter mais informações, consulte Configurando a autenticação multifator.

Configurar a duração do tempo limite do console

Se o Console estiver inativo por um determinado período, você é desconectado automaticamente o Console. É possível alterar o valor de tempo limite padrão no arquivo ConsoleConfiguration.xml.

Siga estas etapas:

1. Faça logon no computador em que você instalou o Console.
2. Abra o arquivo ConsoleConfiguration.xml a partir do seguinte local:

   <UDP_Home>\Management\Configuration\ConsoleConfiguration.xml
3. Altere o valor de consoleUISessionTimeout.

   O valor está em segundos.

   Por exemplo:

   <consoleUISessionTimeout>3600</consoleUISessionTimeout> (o valor padrão é de 1 hora; valor em segundos)

   3600 indica que a duração do tempo limite do Console é de 3600 segundos.
4. Salve o arquivo ConsoleConfiguration.xml.

Como migrar pontos de recuperação do Arcserve r16.5 para Arcserve UDP

Importante: Se estiver replicando de uma pasta compartilhada para um repositório de dados selecionado no servidor de ponto de recuperação, consulte Como executar uma replicação de dados offline usando o início rápido do RPS .

Para migrar os pontos de recuperação do Arcserve r16.5 para o Arcserve UDP, execute as seguintes etapas:

1. Criar um repositório de dados para replicar os dados de um Arcserve r16.5
2. Replicar os dados do Arcserve r16.5 para o repositório de dados do UDP

Criar um repositório de dados para replicar os dados de um ponto de recuperação do Arcserve r16.5

Para replicar dados de um ponto de recuperação do Arcserve r16.5 D2D existente, primeiramente, é necessário criar um repositório de dados do console no qual os dados serão replicados.

Siga estas etapas:

1. Efetue logon no Console do Arcserve UDP.
2. Navegue para **Destinos**, **Servidor do ponto de recuperação**.
3. Selecione o servidor do ponto de recuperação.
4. Clique com o botão direito do mouse e selecione **Adicionar um armazenamento de dados**.
5. Digite os detalhes na página **Adicionar um repositório de dados**.
6. Salve o repositório de dados.

   O repositório de dados é criado.

Replicar os dados do Arcserve r16.5 para o repositório de dados do UDP

Depois de criar o repositório de dados, você pode replicar os dados do ponto de recuperação do Arcserve r16.5 usando Início rápido do RPS.

Siga estas etapas:

1. Clique em **Ações** e, em seguida, clique em **Início rápido do RPS**.

   O **Assistente do RPS Jumpstart** será exibido.

2. Selecionar de uma pasta compartilhada para um repositório de dados no servidor de ponto de recuperação selecionado.

3. Especificar a pasta compartilhada de origem.

   Os detalhes de ponto de recuperação serão exibidos.

   Observação: se a sessão e o repositório de dados de destino não estão criptografados, a senha da sessão é opcional. Se a sessão não estiver criptografada e o repositório de dados estiver criptografado, você deverá fornecer uma senha de sessão na página **Selecione o repositório de dados de destino**.

4. Clique em **Avançar**.

   A página **Selecione o repositório de dados de destino** é aberta. Se o repositório de dados de origem estiver criptografado, somente os repositórios de dados criptografados serão exibidos na lista suspensa.

5. (Opcional) Especifique a senha da sessão, se a sessão não tiver sido criptografada na Etapa 3.

6. Clique em **Avançar**.

7. Clique em **Concluir**.

   Os dados do ponto de recuperação do Arcserve r16.5 são replicados no repositório de dados do Arcserve UDP.

Configurar o assistente de configuração

Usando o Assistente de configuração, configure seu ambiente de proteção de dados assim que efetuar logon no console. Caso esteja usando o Arcserve UDP pela primeira vez, o Assistente de configuração é a melhor maneira de criar seu primeiro plano de backup. Ele cria planos para definir como proteger os dados. Um plano consiste em uma ou várias tarefas ao definir os parâmetros de origem, de destino, de programação e avançados. O Assistente de configuração é aberto com o primeiro logon no Console. Você pode ocultar a página de boas-vindas do assistente selecionando **Não mostrar esta página da próxima vez**.

É possível criar um plano para proteger os nós físicos como nós Windows e Linux, e máquinas virtuais como o VMware e o Hyper-V.

As etapas a seguir descrevem uma descrição genérica sobre como criar um plano com base em agente do Windows usando o assistente de configuração.

1. Efetue logon no Console.

   Se você estiver efetuando logon pela primeira vez, o assistente de configuração abre.

2. Se o assistente não abrir, clique na guia **recursos** e clique em **Assistente de configuração** no painel direito.

   A página de boas-vindas do assistente abre.

3. Clique em **Avançar**.

   A página **Criar um plano** abre.

4. Especifique o nome do plano.

5. Selecione um tipo de nó a ser protegido.

   Por exemplo, selecione **Backup: Windows com base em agente**.

6. Clique em **Avançar**.

   A página **Selecionar nós para proteger** abre. Os campos são opcionais na página **Adicionar nós para proteger**.

7. Selecione o método para adicionar nós a partir da lista suspensa.

   Os campos variam de acordo com sua seleção.

8. Forneça os detalhes do nó, clique em **Adicionar à lista** e clique em **Avançar**.

   A página **Destino do backup** é exibida.

9. Especifique o tipo de destino a partir da lista suspensa.

Os campos restantes na página **Destino de backup** variam de acordo com o tipo de destino. Também é possível ativar a senha da sessão.

Para criar um repositório de dados, consulte Adicionar um repositório de dados.

10. Especifique os detalhes de destino restantes e clique em **Avançar**.

    A página **Programação de backup** abre.

11. Especifique a programação de backup e clique em **Avançar**.

    A página **Confirmação do plano** abre.

12. Verifique o plano.

13. (Opcional) Clique em **Criar um plano**para adicionar outro plano.

14. Clique em **Avançar**

    A configuração do recurso foi concluída.

15. Clique em **Concluir**.

    O assistente fecha e um novo plano é criado.

    É possível ver o plano em **recursos Planos**, **Todos os planos**.

Capítulo 6: Trabalhando com os principais recursos do Arcserve UDP

Esta seção contém os seguintes tópicos:

Entendendo o recurso Nutanix no Arcserve UDP

Para explorar as funções disponíveis para o recurso Nutanix no Arcserve UDP, consulte How to Work With Nutanix Using Arcserve UDP.

Entendendo o recurso OneDrive no Arcserve UDP

Explore as funções disponíveis para o recurso OneDrive no Arcserve UDP.

- Gerenciar nós do OneDrive
- Como criar um plano de backup do Microsoft Office 365 OneDrive
- Como restaurar dados do OneDrive

Entendendo o recurso Exchange Online no Arcserve UDP

O Exchange Online é um aplicativo de email hospedado na nuvem da Microsoft. Para proteger os itens de email do Exchange Online (emails, itens de calendário, contatos etc.) no Microsoft Cloud, você precisa criar um plano no Arcserve UDP. Explore as funções disponíveis para o recurso Exchange Online em Arcserve UDP.

- Privilégios de usuário para o Exchange Online no Arcserve UDP
- Adicionar um nó do Microsoft Exchange Online
- Gerenciamento de nós do Exchange Online
- Adicionar o grupo e a função necessários à conta de backup do Exchange Online para executar backup e restauração
- Como criar um plano de backup do Exchange Online
- Como restaurar dados da caixa de correio do Exchange Online
- Aplicando práticas recomendadas

Entendendo o recurso de instantâneo de hardware no UDP

O Arcserve UDP tem o recurso de utilizar instantâneos de armazenamento de hardware para backup. Você pode especificar se deseja que um instantâneo de hardware seja gerado durante a criação de uma tarefa de backup. Se você selecionar o instantâneo de hardware, o Arcserve UDP primeiro tenta criar um instantâneo de hardware. Se o instantâneo de hardware falhar, o Arcserve UDP reverte automaticamente para o instantâneo de software sem uma falha na tarefa de backup.

- Como usar o instantâneo de hardware para backup
- Matriz de armazenamento suportada no Arcserve UDP
- Usar o instantâneo de hardware para o backup sem agente da VMware
- Usar o instantâneo de hardware para o backup sem agente do Hyper-V
- Usar o instantâneo de hardware para o backup com base em agente
- Verificar se o backup usou o instantâneo de hardware

Nimble

- Adicionar uma matriz de armazenamento
- Considerações sobre o armazenamento Nimble quando a autenticação CHAP está ativada
- Usar o instantâneo de hardware para o backup sem agente da VMware

HPE 3PAR storeserve

- Adicionar uma matriz de armazenamento
- Usar o instantâneo de hardware para o backup sem agente da VMware

NetApp

- Adicionar uma matriz de armazenamento
- Considerações sobre o suporte a iSCSI/FC do NetApp para VMware
- Condições aplicadas a instantâneos de hardware para NetApp NFS VMware
- Usar o instantâneo de hardware para o backup sem agente da VMware

Entendendo o recurso de nuvem no UDP

O recurso de nuvem do Arcserve UDP garante a proteção de dados na nuvem no caso de qualquer exclusão acidental. Usando os recursos de nuvem do Arcserve UDP, é possível copiar os arquivos especificados, pontos de recuperação, criar instâncias usando pontos de recuperação, criar VMs em modo de espera virtual na nuvem e assim por diante.

Exiba links para utilizar a nuvem no Arcserve UDP:

- Adicionar uma conta de nuvem
- Gerenciar nós para nuvem
  - Baixar o ponto de recuperação a partir da nuvem
  - Fazer upload do ponto de recuperação para a nuvem
  - Copiar ponto de recuperação para o disco local ou compartilhamento de rede
- Como configurar um RPS na nuvem
  - Especificar a configuração de nuvem para restauração a partir de um local de nuvem de cópia de arquivo
  - Especificar a configuração de nuvem para restauração a partir de um local de nuvem de arquivo morto
- Como fazer backup dos dados na nuvem
  - Como criar um modo de espera virtual para o plano do AWS EC2
  - Como criar e gerenciar uma máquina virtual instantânea no Amazon EC2
  - Como criar um plano de pontos de recuperação de cópia
- Nuvem para Linux
  - Instalar o Agente do Arcserve UDP (Linux) na nuvem da AWS
  - Como executar uma BMR (Bare Metal Recovery - Recuperação “bare metal”) para computadores Linux na nuvem AWS
  - Como executar uma BMR de migração em máquinas Linux do Amazon EC2 para um computador local
  - Como executar uma migração da IVM da nuvem para o local
- Plano de backup do Microsoft Office 365

- Como criar um plano de backup do Exchange Online
- Como restaurar dados da caixa de correio do Exchange Online
- Como criar um plano de backup do Microsoft Office 365 OneDrive
- Como restaurar dados do OneDrive
- Criar um plano de backup do SharePoint Online (Assistir ao vídeo)
- Como restaurar dados da coleção de sites do SharePoint Online

- Microsoft Azure
  - Como criar um modo de espera virtual para o plano do Microsoft Azure
  - Como criar e gerenciar uma máquina virtual instantânea no Microsoft Azure
- Solução de problemas
  - Como adicionar senha de criptografia em um destino criptografado existente
  - Configurar o registro para tarefa de cópia de ponto de recuperação
  - Congestionamento de largura de banda com tarefas de cópia do ponto de recuperação para a nuvem
  - Não é possível se conectar à nuvem

Entendendo o recurso do caminho UNC/NFS no UDP

O caminho UNC/NFS foi introduzido como um novo tipo de nó. Para usar o recurso, é possível consultar as seguintes seções:

- Privilégios de usuário para o caminho UNC/NFS no Arcserve UDP
- Como adicionar e gerenciar um caminho UNC/NFS
- Como criar um plano de backup de caminho UNC/NFS
- Como restaurar a partir de um caminho UNC/NFS

Entendendo o recurso SharePoint Online no UDP

O Arcserve UDP v6.5 Atualização 2 e superior oferece suporte ao trabalho com o ambiente do Microsoft SharePoint Online. Para usar o recurso, é possível consultar as seguintes seções:

- Pré-requisitos
- Adicionar um nó do SharePoint
- Gerenciar nós do SharePoint Online
- Criar um plano de backup do SharePoint Online
- Como restaurar dados da coleção de sites do SharePoint Online

Pré-requisitos

O Arcserve UDP 8.0 apresenta os seguintes pré-requisitos para funcionar com o ambiente do Microsoft SharePoint Online:

É necessário ter os privilégios de usuário apropriados para as funções do Arcserve UDP. Para obter mais informações, consulte Privilégios de usuário para o SharePoint Online no Arcserve UDP.

Capítulo 7: Usar a administração com base em função do Arcserve UDP

A administração com base em função (RBAC) permite que os administradores atribuam funções diferentes e a permissão para tipos diferentes de usuários para usar o Console do Arcserve UDP. Cada função pode ter suas próprias permissões. A função de superadministrador pode criar funções personalizadas e permissões para outros usuários do Console do Arcserve UDP.

Com RBAC, é possível atribuir nível variado de segurança para cada função.

Esta seção contém os seguintes tópicos:

Acessar o console de gerenciamento de usuários

A página Gerenciamento de usuários permite fazer o seguinte:

- Efetuar logon no console de gerenciamento de usuários (console do serviço de identidade) a partir do console do Arcserve UDP.
- Ativar e configurar a autenticação multifator (MFA) para todos os usuários.

Esta seção contém os seguintes tópicos:

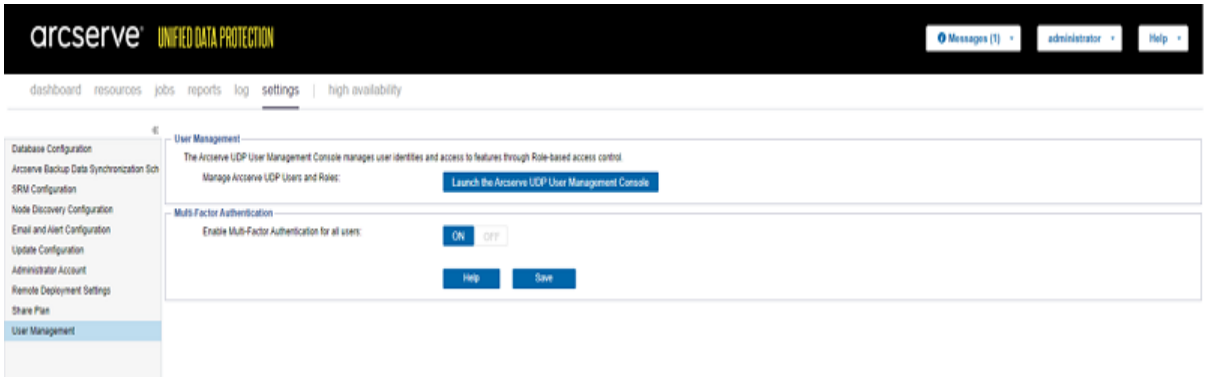
Iniciar o console de gerenciamento de usuários do Arcserve UDP

O Console de gerenciamento de usuários do Arcserve UDP gerencia as identidades dos usuários e controla o acesso aos recursos usando o controle de acesso com base em função. Esta seção fornece informações sobre como iniciar o console de gerenciamento de usuário do Arcserve UDP.

Siga estas etapas:

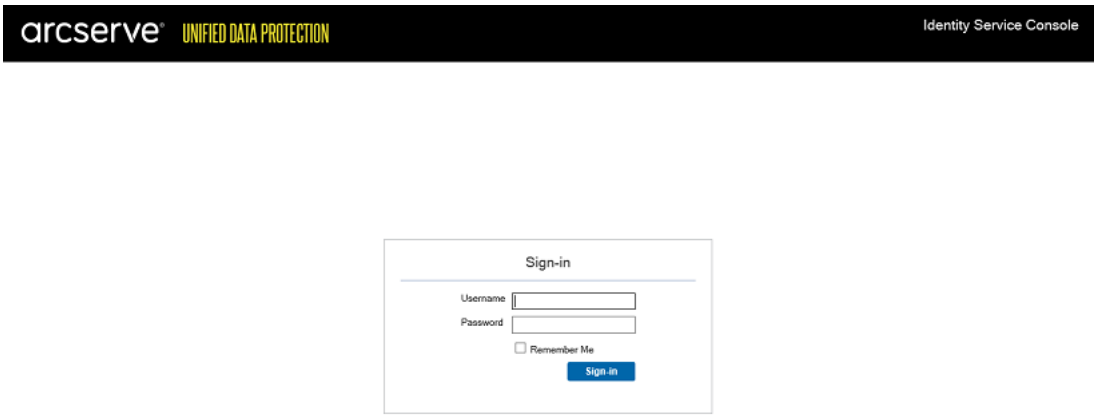
1. Efetue logon no Console do Arcserve UDP.
2. Vá para **configurações** > **Gerenciamento de usuários**.

   A página Gerenciamento de usuários é exibida no painel central.



3. Clique em **Abrir o console de gerenciamento de usuários do Arcserve UDP**.

   O Console do serviço de identidade é exibido em uma nova janela.



4. Especifique o nome de usuário e a senha e clique em **Conectar**.

   A página inicial do Console do serviço de identidade é exibida.

   Você acessou com êxito o Console de gerenciamento de usuários do Arcserve UDP.

   Como alternativa, você também pode efetuar logon no Console do serviço de identidade. Para efetuar logon, digite o endereço no seguinte formato na nova janela:

   http(ou https)://(endereço IP ou nome do host): (número da porta do console)/carbon

Configurando a autenticação multifator

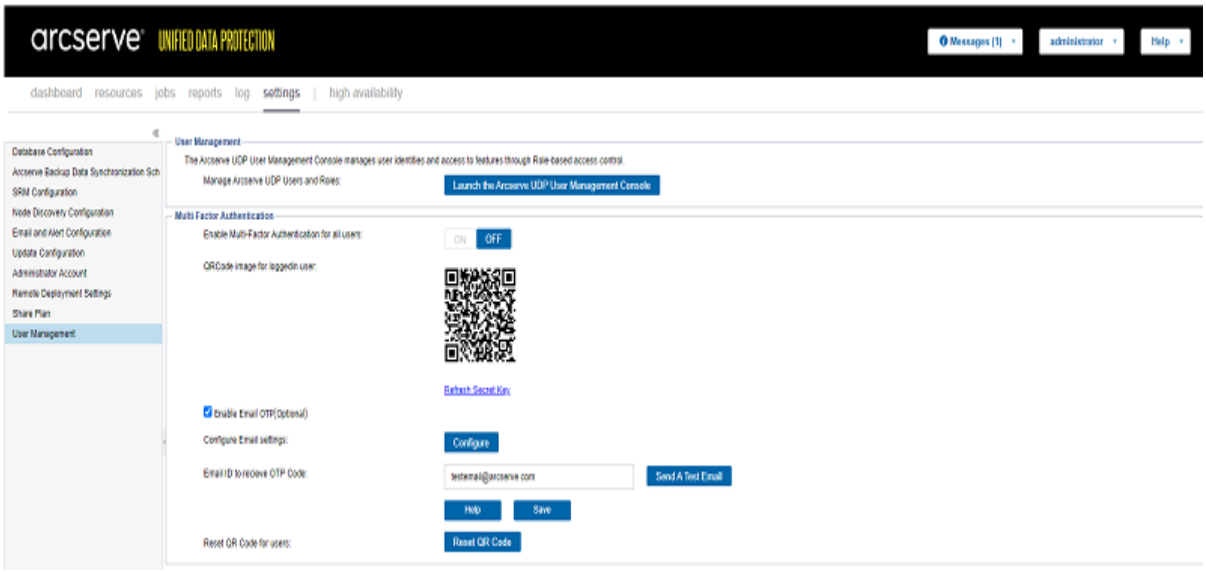
Esta seção contém os seguintes tópicos:

Configurando a autenticação multifator como usuário administrador

Esta seção fornece informações sobre como configurar a autenticação multifator para todos os usuários.

Siga estas etapas:

1. Efetue logon no console do Arcserve UDP usando credenciais de administrador.
2. Vá para **Configurações** > **Gerenciamento de usuários**.



3. Para ativar a autenticação multifator para todos os usuários, na seção Autenticação multifator, clique na configuração **ATIVAR**.

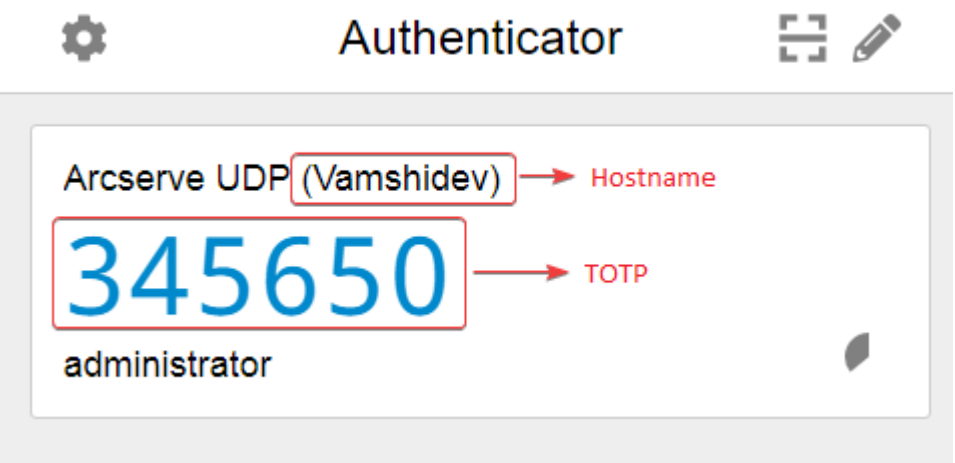
   A imagem do código QR para o usuário conectado é exibida.

   Observação: se desejar desativar a autenticação multifator para todos os usuários, clique na configuração **DESATIVAR**.

4. Para gerar o TOTP, verifique a imagem do código QR usando um aplicativo autenticador.

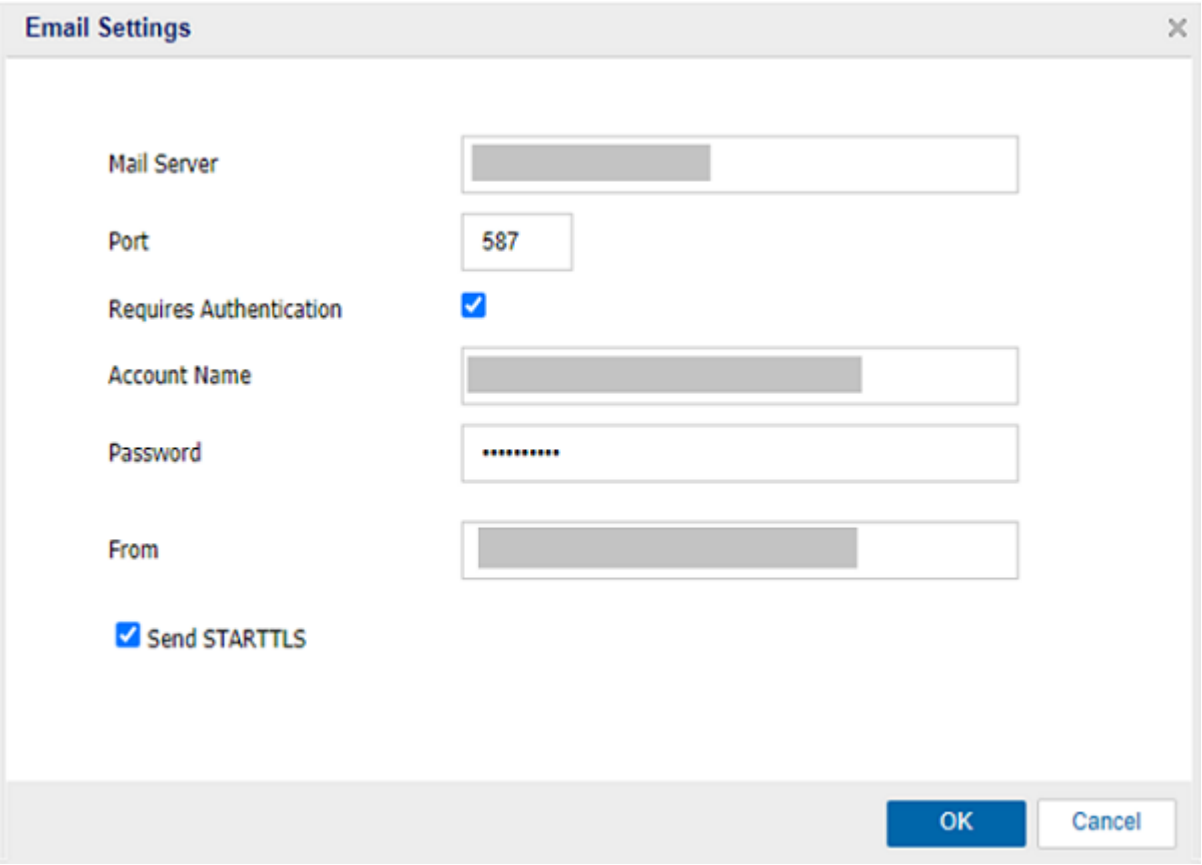
   Observações:

   - É possível usar qualquer um dos aplicativos autenticadores móveis, como o aplicativo autenticador do Google ou o aplicativo autenticador da Microsoft no seu dispositivo móvel. Como alternativa, você também pode usar a extensão do autenticador no navegador Chrome.
   - Para gerar um novo TOTP, sob a imagem do código QR, clique no link **Atualizar chave secreta**.
   - Ao usar um aplicativo autenticador para várias contas de usuário, o nome do host da conta do usuário diferencia os TOTPs. No aplicativo autenticador, é possível exibir o nome do host e o respectivo TOTP.



5. (Opcional) Se você deseja ativar a OTP de email, selecione **Ativar OTP de email (opcional)** e faça o seguinte:
   a. Para definir as configurações de email, clique no botão **Configurar**.

      A caixa de diálogo Configurações de email é exibida.



   b. Na caixa de diálogo Configurações de email, faça o seguinte e clique em **OK**:

- **Servidor de email:** digite o endereço do servidor de email.
- **Porta:** digite o número da porta do servidor de email.
- Se o servidor de email especificado exigir autenticação, marque a caixa de seleção **Requer autenticação**.
- **Nome da conta:** digite o nome de usuário ou endereço de email do servidor de email especificado.
- **Senha:** digite a senha para autenticação.
- **De:** digite o endereço de email do remetente conforme necessário.
- Se o servidor de email especificado exigir o comando do protocolo STARTLS, marque a caixa de seleção **Enviar STARTLS**.

c. Em *ID de email para receber o código de OTP*, digite um ou mais endereços de email.

Observação: é necessário fornecer um endereço de email para receber OTP durante o processo de logon. Se desejar fornecer vários endereços de email, use ponto-e-vírgula (;) para separá-los.

d. Para verificar se os endereços de email configurados estão recebendo OTP, clique em **Enviar um email de teste**.

6. Clique em **Salvar**.

   Uma caixa de diálogo de confirmação é exibida.

   Observação: a caixa de diálogo de confirmação é exibida para reiniciar o serviço de identidade somente quando você define, modifica ou remove as configurações de email.

7. Na caixa de diálogo Confirmar, para reiniciar o serviço de identidade, clique em **Sim**.

   Depois que o serviço de identidade for reiniciado, atualize o navegador. Isso é necessário para que as configurações de email sejam aplicadas.

Para redefinir o código QR, consulte Como redefinir o código QR.

Como redefinir o código QR

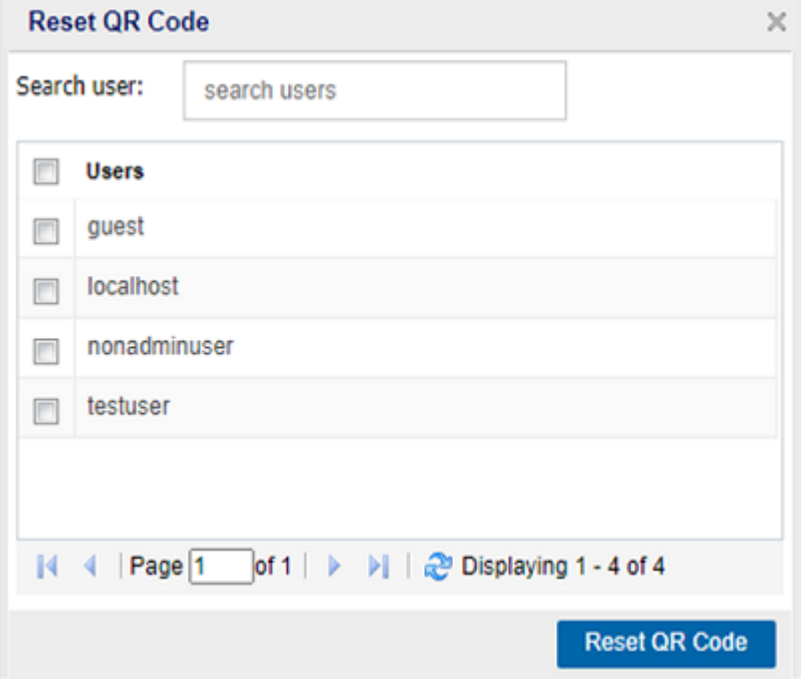
Esta seção fornece informações sobre como redefinir o código QR para os usuários.

Observação: um usuário administrador pode redefinir o código QR para todos os usuários, exceto para si mesmo.

Siga estas etapas:

1. Efetue logon no console do Arcserve UDP usando credenciais de administrador.
2. Vá para **Configurações** > **Gerenciamento de usuários**.
3. Em *Redefinir código QR para usuários*, clique no botão **Redefinir código QR**.

   A caixa de diálogo Redefinir código QR é exibida.



4. Na caixa de diálogo Redefinir código QR, na lista de usuários, selecione os usuários para os quais deseja redefinir o código QR e clique em **Redefinir código QR**.

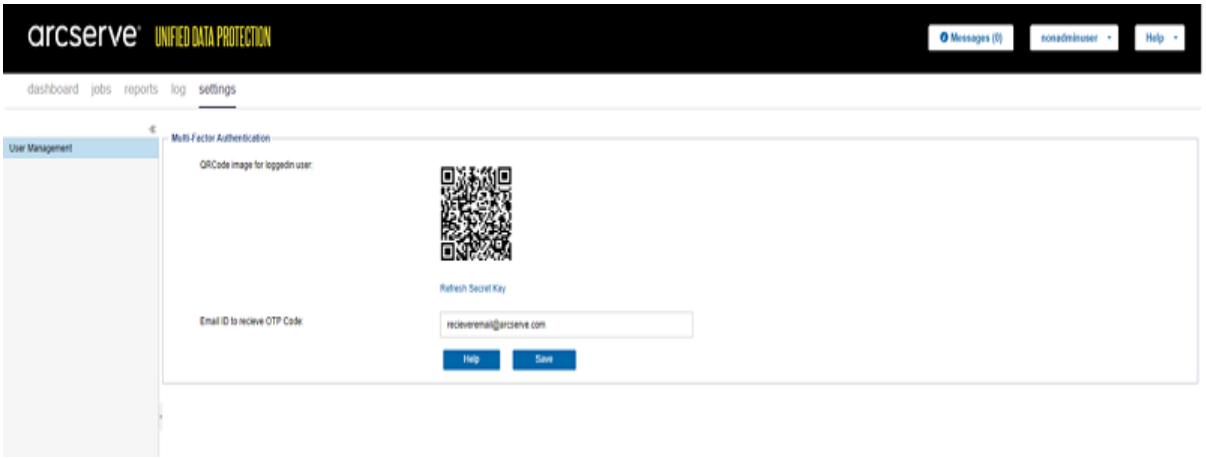
Observação: após redefinir o código QR, durante o próximo logon, os usuários selecionados devem ler o código QR novamente para um novo TOPT e fazer o registro novamente.

Configurando a autenticação multifator como um usuário não administrador

Esta seção fornece informações sobre como definir configurações de autenticação multifator para seu próprio perfil de usuário.

Siga estas etapas:

1. Efetue logon no console do Arcserve UDP usando credenciais que não sejam de administrador.
2. Vá para **Configurações** > **Gerenciamento de usuários**.



Observação: a página *Configurações> Gerenciamento de usuários* não está disponível para usuários que não têm permissão de Gerenciamento de usuários. No entanto, o administrador pode atribuir essa permissão a todos os usuários que não sejam administradores ou a outros usuários. Para obter mais informações, consulte Atribuir uma função pré-definida.

3. Para gerar um novo TOTP, sob a imagem do código QR, clique no link **Atualizar chave secreta**.
4. Em *ID de email para receber o código de OTP*, digite um ou mais endereços de email.

   Observação: é necessário fornecer um endereço de email para receber OTP durante o processo de logon. Se desejar fornecer vários endereços de email, use ponto-e-vírgula (;) para separá-los.

5. Clique em **Salvar**.

   As novas configurações são salvas.

Adicionar usuário, excluir usuários e alterar senha

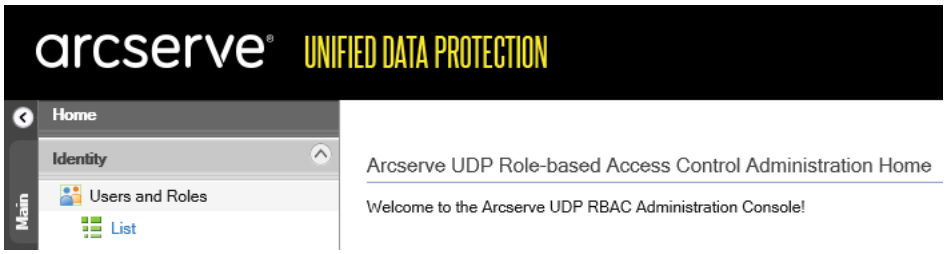
É possível adicionar ou excluir usuários locais ou de domínio no Controle de Usuário do Windows. A lista de gerenciamento de usuários no Console de serviço de identidade é atualizada imediatamente.

Use o Controle de Usuário do Windows para alterar a senha do usuário. Ao atualizar a senha de um usuário, o usuário deve efetuar logon no console de serviço de identidade usando a senha mais recente. A função do usuário é mantida.

Configurar o gerenciamento de usuário

É possível atribuir funções diferentes a usuários diferentes e fornecer permissões diferentes para diferentes funções. A configuração do gerenciamento de usuários ajuda você a executar as seguintes opções:

- Funções predefinidas
- Atribuir uma função pré-definida
- Exibir e cancelar uma função
- Adicionar uma nova função
- Pesquisar usuários e funções

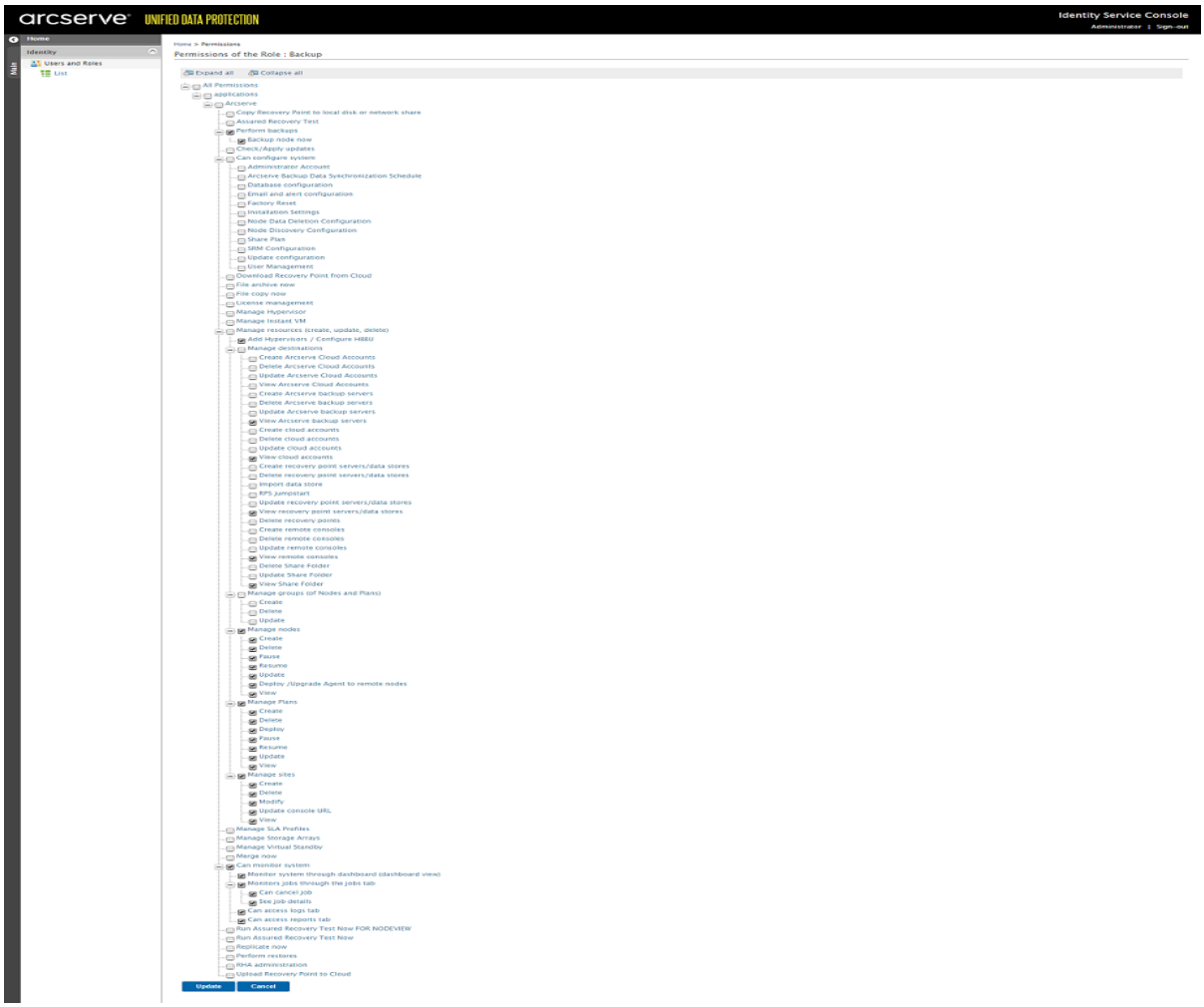


Funções predefinidas

O papel de uma função predefinida é fornecer uma referência para algumas definições de função típicas. Cada função tem um conjunto predefinido de permissões atribuídas.

Para a função de administrador, todas as opções da permissão são selecionadas. Uma função de administrador pode acessar todas as funções do Arcserve UDP.

Clique na permissão para a função de Backup e as seguintes permissões selecionadas são predefinidas:

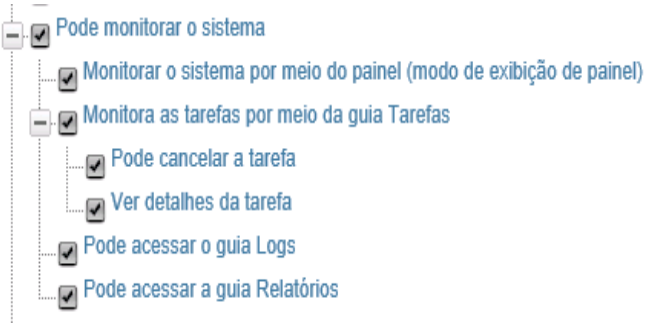

arcserve
UNIFIED DATA PROTECTION
Identity Service Console
Administrator | Sign-out
Home
Identity
Users and Roles
List
Main
Home > Permissions
Permissions of the Role : Backup
Expand all
Collapse all
All Permissions
applications
Arcserve
Copy Recovery Point to local disk or network share
Assured Recovery 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

As seguintes permissões estão predefinidas para a função de backup:

- Executar backup
- Exibir destino
- Gerenciamento de nós/plano/sites
- Função do sistema de monitoramento

A função de administrador permite flexibilidade completa para limpar as permissões selecionadas ou selecionar uma nova permissão. Quando você clicar em Atualizar, a permissão recém-adicionada torna-se a permissão padrão para a função de backup. Também é possível renomear a função.

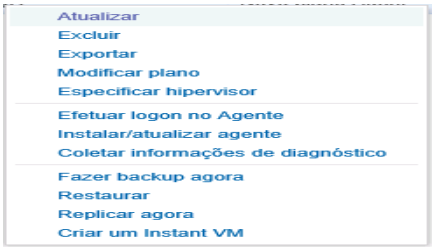
Para a função de Monitor são pré-selecionadas a permissão de monitor e log de tarefa do painel/permissão de relatório.



Para a função de restauração, as seguintes permissões são pré-selecionadas:

- Gerenciar a VM instantânea
- Exibir destino
- Exibir nó
- Exibir plano
- Gerenciar modo de espera virtual
- Monitorar tarefas
- Acessar logs
- Executar restauração

Se você atribuir a função de restauração a um usuário, ele poderá efetuar logon e terá a autoridade correspondente. Por exemplo, se um usuário tiver a função de restauração, em seguida, se for feito o backup de um nó com êxito, é possível criar uma VM instantânea ou Restaurar a fim de ir para a próxima atividade.



Para a função _Admin, a permissão de administração do RHA dá acesso à funcionalidade de alta disponibilidade.

Atribuir uma função pré-definida

Quando um superadministrador atribui uma função a um usuário, apenas esse usuário pode efetuar logon no console. O botão usuários exibe a lista de usuários completa, incluindo os usuários locais e usuários de domínio.

É possível atribuir a funções disponíveis (predefinidas) ou funções definidas pelo usuário para qualquer usuário local ou usuários de domínio.

Observação: apenas um superadministrador (um administrador que instala o Arcserve UDP) pode atribuir a função de administrador a outros usuários. Os administradores podem atribuir somente funções de não administrador para outros usuários.

Siga estas etapas:

1. Clique em **Usuários e funções** da página **Configurar**.

   Os usuários e funções são exibidos na página Gerenciamento de usuários.

2. Na página Gerenciamento de usuários, clique em **Usuários**.

   A lista de usuários é exibida.

3. Clique em **Atribuir funções** para um usuário.

   A página **lista de função de usuário** é aberta.

4. Selecione uma ou mais funções e clique em **Atualizar**.

   A função de usuário foi atualizada com êxito.

5. Clique em **Concluir** para ir para tela anterior.

   Você atribuiu com êxito uma função ao usuário.

Exibir e cancelar uma função

É possível exibir a função atual que está atribuída a um usuário. É possível cancelar uma função atribuída desmarcando a sua caixa de seleção.

Siga estas etapas:

1. Clique em **Usuários e funções** da página **Configurar**.

   Os usuários e funções são exibidos na página **Gerenciamento de usuários**.

2. Na página Gerenciamento de usuários, clique em Usuários.

   A lista de usuários é exibida.

3. Desmarque a caixa de seleção para cancelar uma função e clique em **Atualizar**.

   As funções são removidas do usuário.

   Observação: se não estiver atribuído a uma função, o usuário não conseguirá efetuar logon no console do Arcserve UDP.

4. Clique em **Concluir** para ir para a página anterior.

   Ela foi exibida com êxito e você cancelou uma função.

Adicionar uma nova função

Você pode criar uma função personalizada e selecionar a permissão para a função.

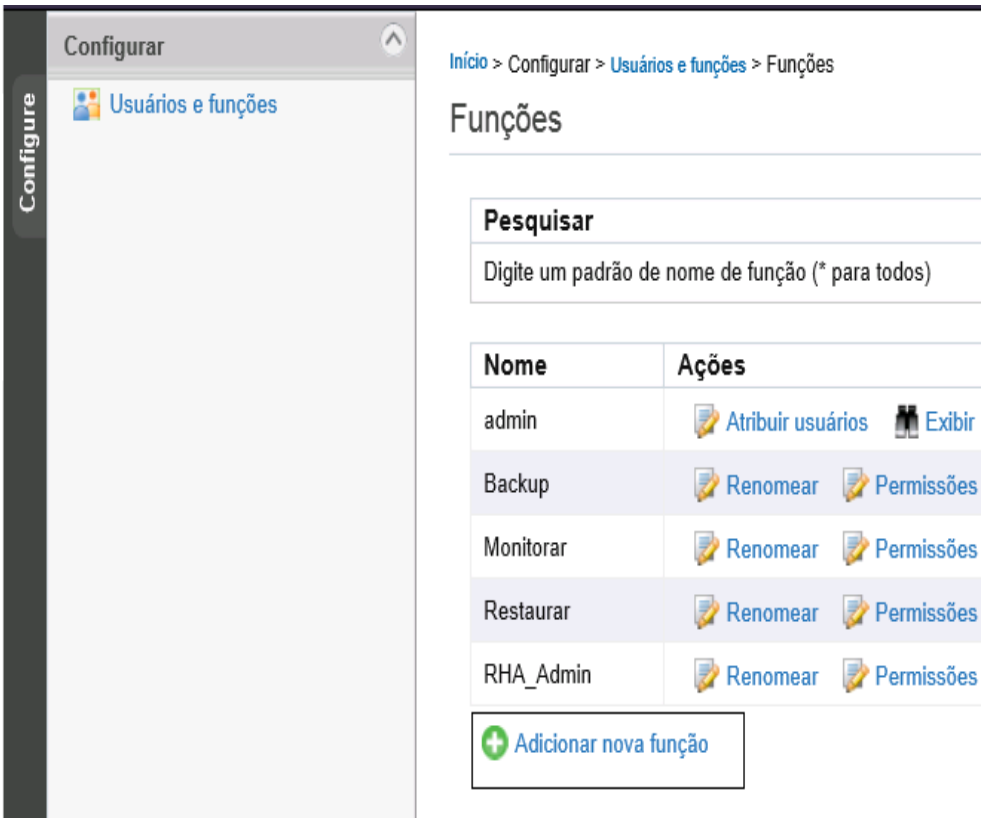
Siga estas etapas:

1. Clique em **Usuários e funções** da página **Configurar**.

   Os usuários e funções são exibidos na página **Gerenciamento de usuários**.

2. Clique em **Funções**.

   A página **Funções** é aberta e lista todas as funções disponíveis.



3. Clique em **Adicionar nova função**.

   A página **Adicionar função** é aberta.

4. Digite um nome da função e clique em **Avançar**.

   Observação: não use caracteres especiais como **~!@#$%^&*** no nome da função.

5. Marque as caixas de seleção de permissão necessárias e clique em **Avançar**.

6. Selecione os usuários dessa função.

7. Clique em **Concluir**.

   Uma nova função é criada e são atribuídas permissões para essa função.

Observação: algumas permissões funcionam apenas quando as permissões relacionadas também são selecionadas. Por exemplo, para configurar uma função a fim de gerenciar o modo de espera virtual, selecione a permissão de gerenciamento do modo de espera virtual e a permissão de exibição de nó para garantir o funcionamento normal da função.

Pesquisar usuários e funções

É possível filtrar os usuários e funções para localizar o usuário ou a função desejada. Digite * para procurar todos os usuários e funções.

Para pesquisar uma função, siga estas etapas:

1. Clique em **Usuários e funções** da página **Configurar**.

   Os usuários e funções são exibidos na página **Gerenciamento de usuários**.

2. Clique em **Funções**.

   A página **Funções** será aberta.

3. Especifique o padrão de nome de função e clique em **Pesquisar**.

   O resultado filtrado aparece.

Para pesquisar um usuário, siga estas etapas:

1. Clique em **Usuários e funções** da página **Configurar**.

   Os usuários e funções são exibidos na página **Gerenciamento de usuários**.

2. Clique em **Usuários**.

   A página **Usuários** é aberta.

3. Especifique o padrão de nome do usuário e clique em **Pesquisar**.

   O resultado filtrado aparece.

Integrar o Arcserve UDP ao Active Directory

O Arcserve UDP oferece suporte à integração do AD (Active Directory) usando grupos do Windows e do AD.

Esta seção contém os seguintes tópicos:

- Como integrar o Arcserve UDP 8.0 ao Active Directory usando grupos do Windows
- Como integrar o Arcserve UDP 8.0 ao Active Directory usando grupos do Active Directory

Como integrar o Arcserve UDP 8.0 ao Active Directory usando grupos do Windows

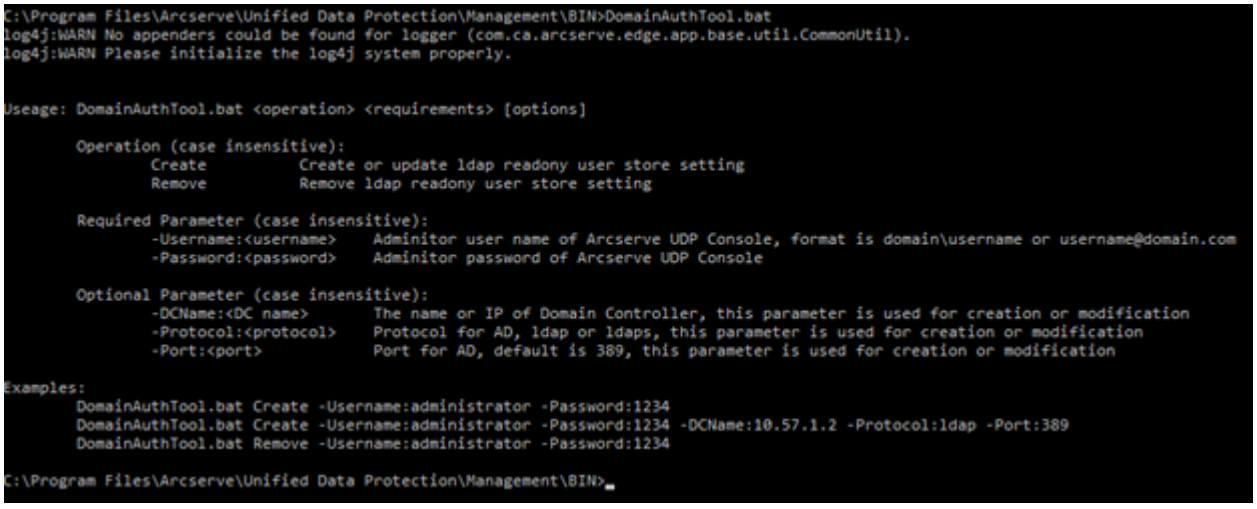
O recurso de administração com base em função (UDP-RBA) existente permite o gerenciamento de permissões do UDP com base nos grupos do Active Directory (AD). Na versão anterior do UDP-RBA, apenas contas de usuários individuais do AD eram suportadas. Agora, grupos do AD podem servir como funções do RBA.

O repositório de usuários secundário somente leitura do LDAP é automaticamente adicionado usando um utilitário.

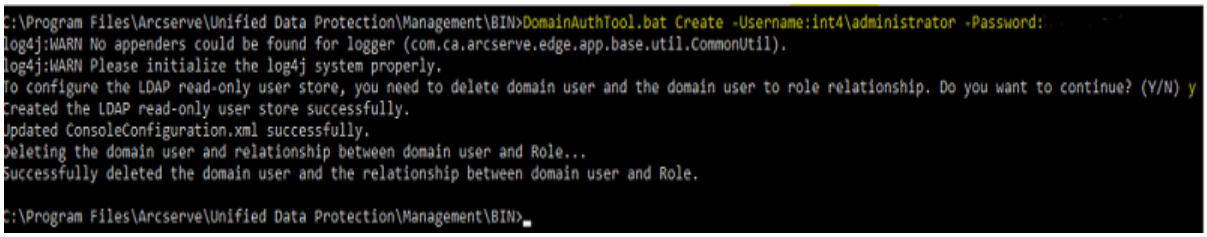
Siga estas etapas:

1. Inicie o prompt de comando e digite *C:\Program Files\Arcserve\Unified Data Protection\Management\BIN*.
2. Execute o utilitário *DomainAuthTool.bat*.

   As seguintes informações são exibidas na tela:



3. Crie um usuário secundário somente leitura do LDAP e modifique os parâmetros opcionais. Por exemplo, consulte o comando marcado em amarelo na captura de tela abaixo.



4. Atribua a função de usuário local.

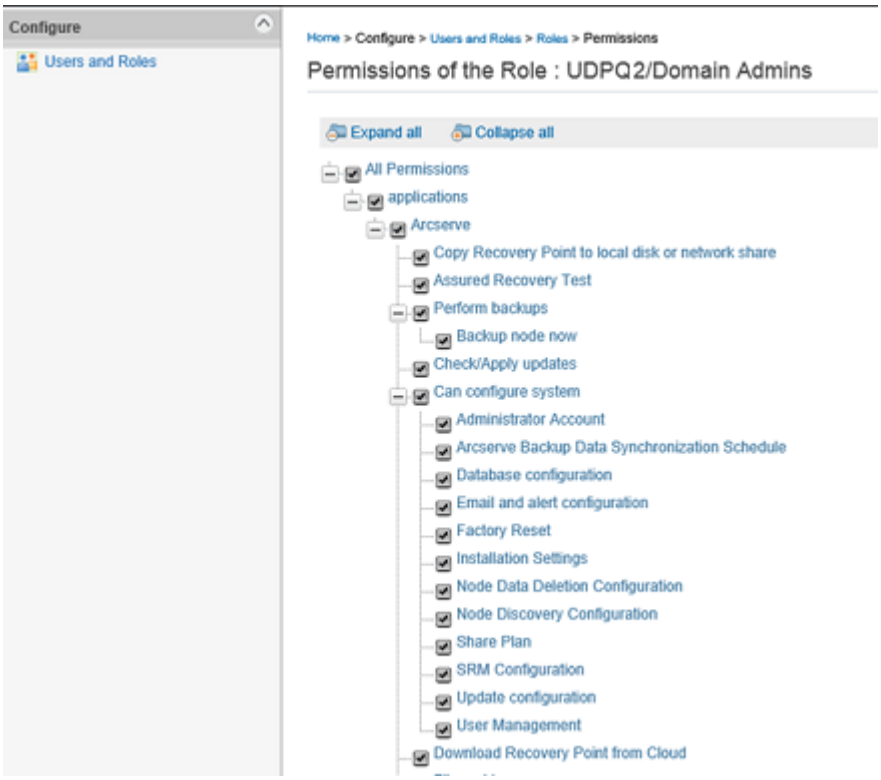
Para obter mais informações, consulte Atribuir uma função pré-definida.

5. Para atribuir uma permissão aos usuários de domínio somente leitura do LDAP, siga estas etapas:

   a. Junte-se ao grupo de Controlador de domínio.

   b. Atribua a permissão do Arcserve UDP ao grupo correspondente como mostrado na captura de tela abaixo.

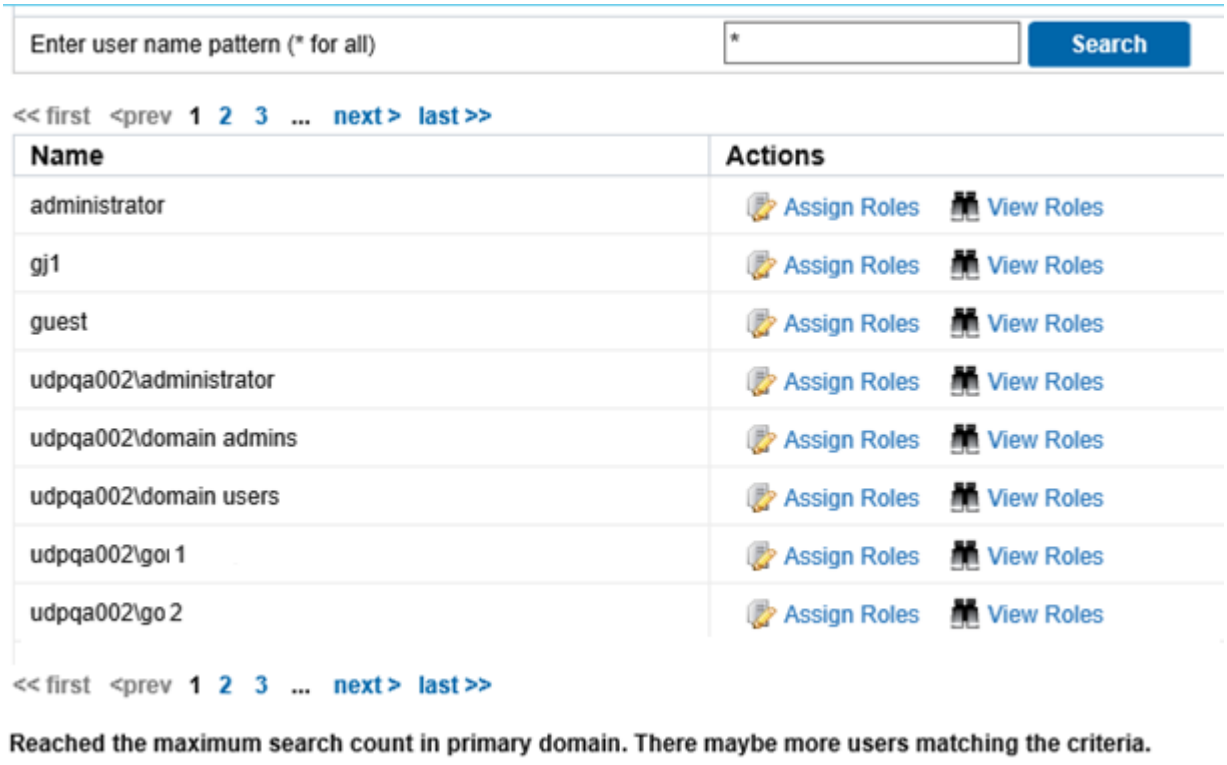
   Observação: não é possível atribuir a função padrão local diretamente aos usuários de domínio somente leitura.



   Agora, o usuário pode efetuar logon no console do Arcserve UDP com a permissão especificada.

6. (Opcional) Remova o repositório de usuários do LDAP usando o utilitário.

   Execute o utilitário para remover o repositório de usuários do LDAP. Em seguida, reinicie o serviço de gerenciamento que o usuário de domínio anterior será listado, como mostrado abaixo.


Enter user name pattern (* for all)
*
Search
<< first <prev 1 2 3 ... next > last >>
Name
Actions
administrator
Assign Roles
View Roles
gj1
Assign Roles
View Roles
guest
Assign Roles
View Roles
udpqa002\administrator
Assign Roles
View Roles
udpqa002\domain admins
Assign Roles
View Roles
udpqa002\domain users
Assign Roles
View Roles
udpqa002\go 1
Assign Roles
View Roles
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.

Como integrar o Arcserve UDP 8.0 ao Active Directory usando grupos do Active Directory

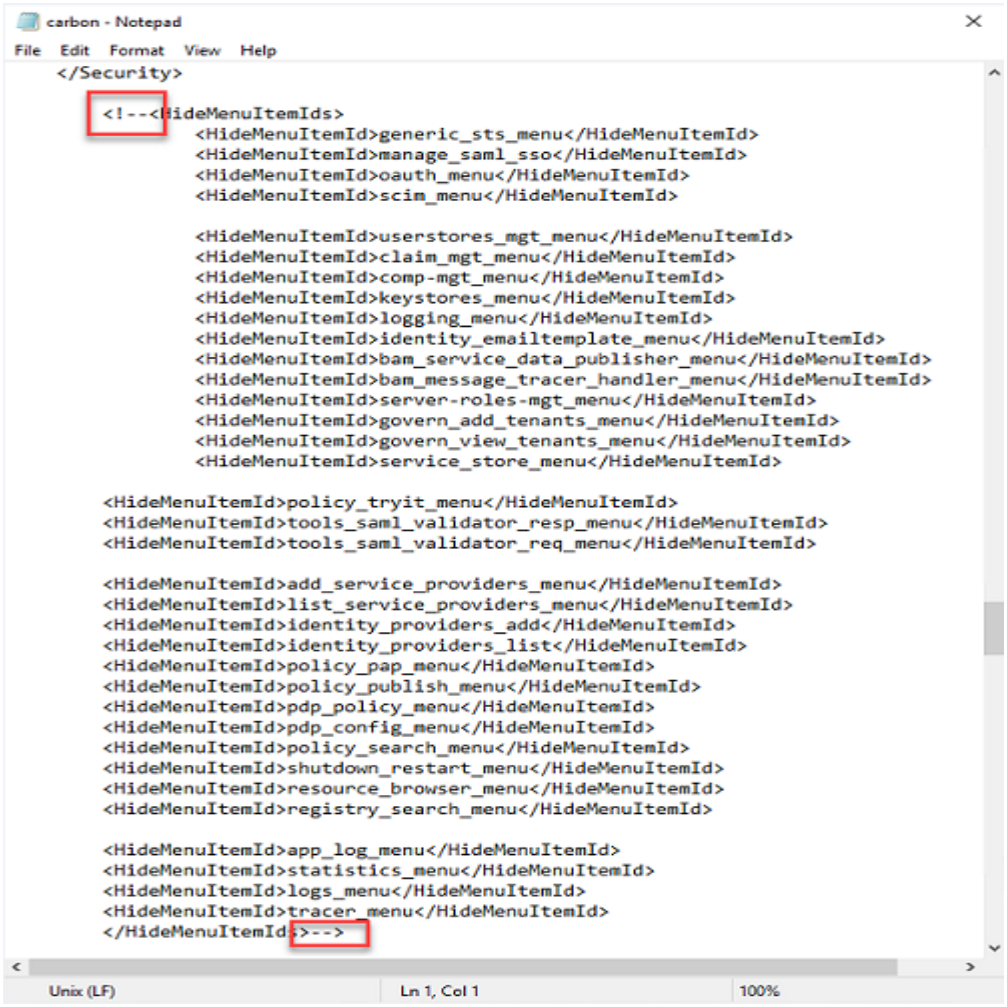
A administração com base em função do Arcserve UDP 8.0 possibilita a permissão no nível do usuário quando o recurso do AD (Active Directory) não é ativado por padrão. No entanto, a plataforma WSO2 Carbon no Arcserve UDP 8.0 não oferece suporte a grupos do AD que possuem repositório secundário de usuários. É possível ativar a extensão do Arcserve UDP 8.0 que configura grupos do AD como funções do Arcserve UDP e ajuda a atribuir permissões automaticamente para integrantes do grupo do AD.

Siga estas etapas:

1. Navegue até o seguinte caminho de instalação do Arcserve UDP e abra o arquivo *carbon.xml*:

   …\Arquivos de programas\Arcserve\Unified Data Protection\Management\IdentityServer\repository\conf\carbon.xml

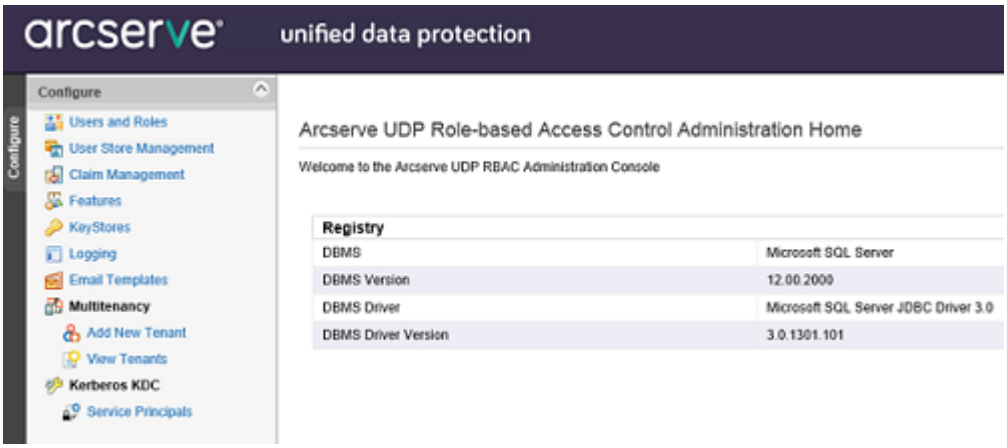
2. No arquivo *carbon.xml*, desative o conteúdo de HideMenuItemIds usando <!-- and -->, conforme exibido na captura de tela abaixo.



3. Salve o arquivo *carbon.xml* e reinicie o serviço de gerenciamento do Arcserve UDP.
4. Abra o console de gerenciamento de usuários por meio do link a seguir:

   https://localhost:8015/carbon

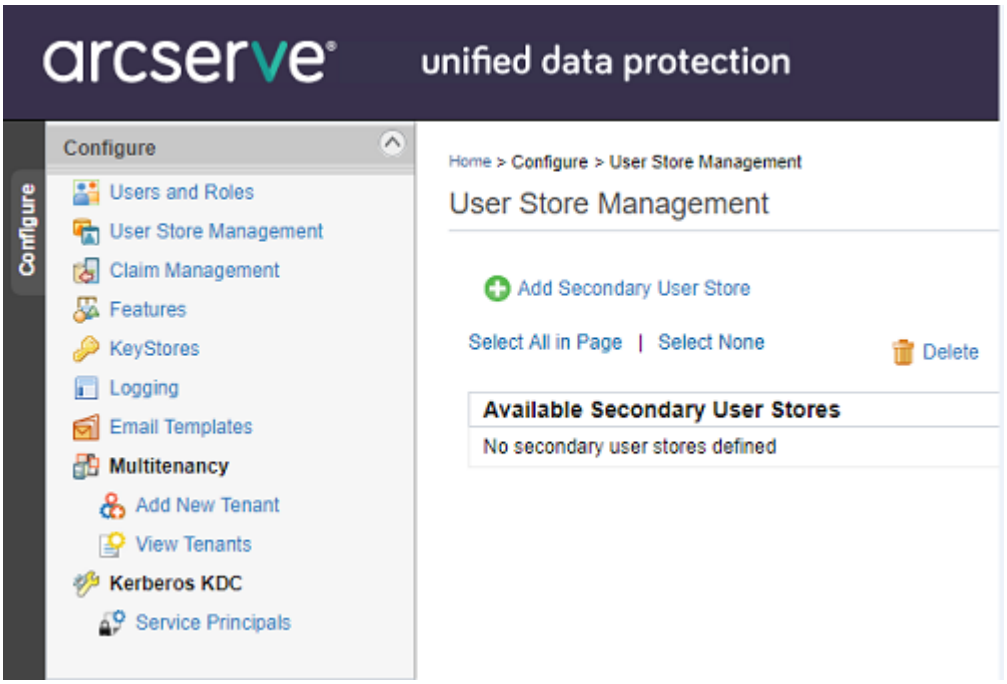
   A *Página inicial de administração do controle de acesso com base em função* do *Arcserve UDP* é exibida.



5. Clique na opção **Gerenciamento de repositório de usuários** disponível no painel esquerdo.

   A página **Gerenciamento de repositório de usuários** é exibida.

6. Clique em **Adicionar repositório de usuários secundário**.

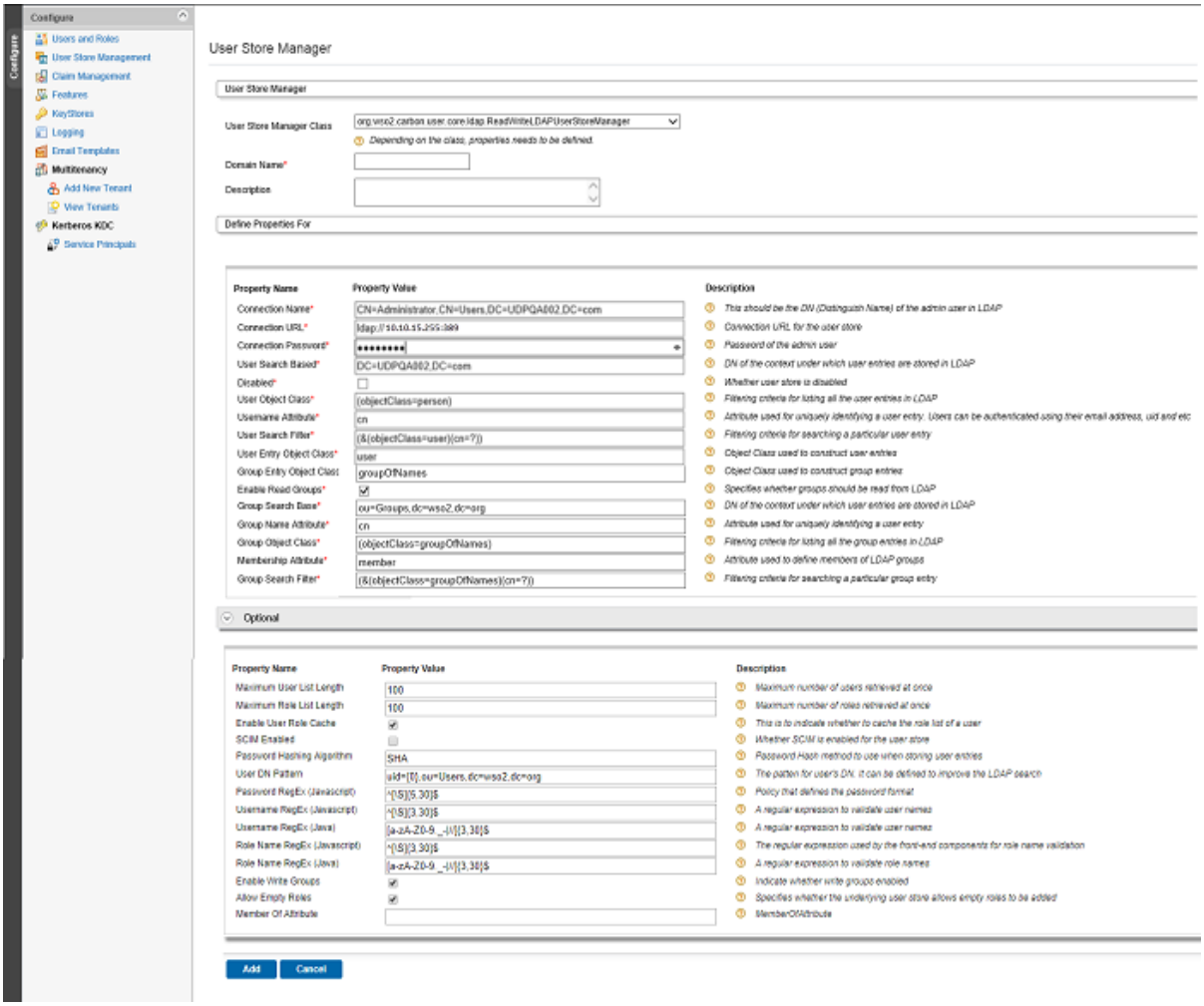


   A página **Gerenciador de repositório de usuários** é exibida.

7. Selecione a opção **Classe de gerenciador de repositório de usuários** desejada na lista suspensa e digite o nome de domínio no campo **Nome do domínio**.

8. Digite os detalhes nos campos, conforme necessário, dos grupos **Definir propriedades para** e **Opcional**.

A captura de tela a seguir é um exemplo da página Gerenciador de repositório de usuários após a inserção dos detalhes.



9. Clique em **Adicionar**.

   A caixa de diálogo **Gerenciamento de usuários do UDP** é exibida.

10. Clique em **OK**.

    A página Gerenciamento de repositório de usuários é exibida e mostra o repositório de usuários secundário adicionado.

Observação: se o repositório de usuários secundário não for exibido, atualize o navegador.

11. (Opcional) Clique na opção **Usuários e funções** no painel esquerdo para exibir a lista de usuários e funções.

    Observação: é necessário definir funções no domínio usando o AD.

12. Agora, execute as seguintes etapas para adicionar as permissões de função do UDP:

    a. Selecione um usuário ou grupo do AD .

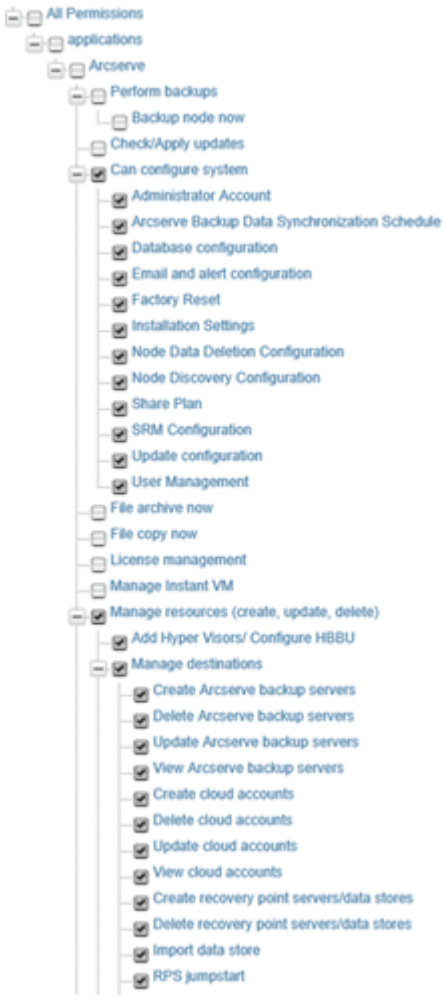
    b. Atribua uma função usando a lista de funções disponível.

    c. Clique em **Exibir funções**.

    A página **Lista de funções do usuário** é exibida.

    d. Clique em **Permissões**.

    A lista de permissões é exibida.



e. Selecione as permissões conforme necessário.

Agora, o usuário secundário pode efetuar logon no console do Arcserve UDP com as permissões atribuídas.

Acesso ao Arcserve UDP usando a autenticação integrada do Windows

Os usuários do Arcserve UDP agora também podem efetuar logon usando a IWA (Integrated Windows Authentication - Autenticação Integrada do Windows). A IWA facilita o logon com base em navegador. Após uma primeira autenticação, o IWA permite que o navegador da web salve as credenciais do usuário conectado pelo Windows. Você só precisa digitar o URL do aplicativo web protegido no navegador. O navegador e o servidor autenticam e conectam o usuário automaticamente.

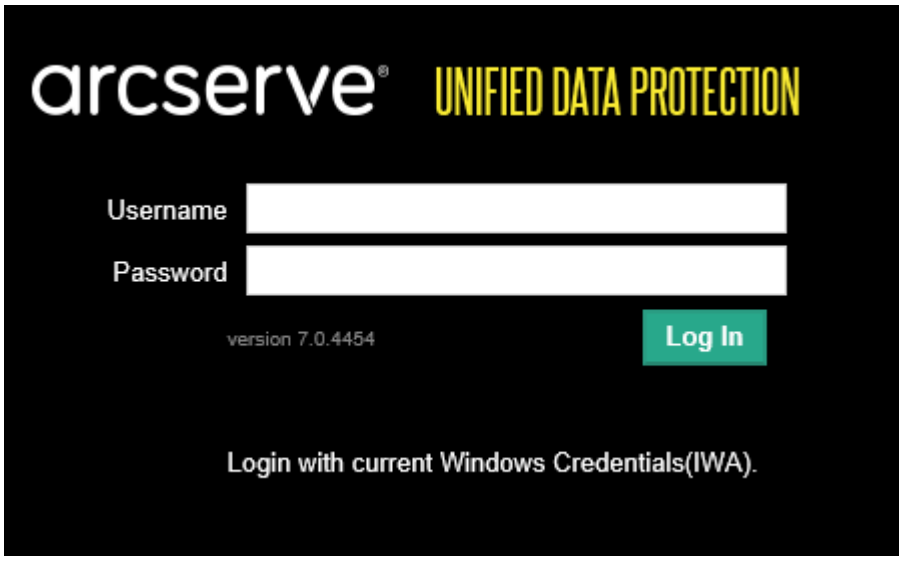
Observação: o console do Arcserve UDP não oferece suporte a IWA se a conexão de banco de dados do console usa o modo de autenticação do Windows. Para solucionar esse problema, consulte o link de solução de problemas.

Com a introdução do IWA, é possível usar o mesmo recurso e acessar o Arcserve UDP.

Siga estas etapas:

1. Abra a página de logon do console do Arcserve UDP.

   O link do IWA fica visível na página de logon.



2. Clique no link **Efetuar logon com as credenciais (IWA) atuais do Windows**.

   Você será redirecionado à página inicial.

   Para resolver qualquer problema, consulte Solução de problemas.

Solução de problemas da IWA (Integrated Windows Authentication - Autenticação Integrada do Windows)

Se o link da IWA não abrir a página do console, é possível usar as seguintes etapas de solução de problemas:

1. Verifique se você está usando a IWA no computador local em vez de no computador remoto.
2. Se você vir uma tela branca depois de clicar no link da IWA, verifique se o usuário está atribuído à função do seu console de administração do RBAC.

   Observação: caso a conexão de banco de dados do console use o Modo de Autenticação do Windows, clique neste link.
3. Caso enfrente algum problema durante o logon da IWA com o Firefox para abrir o URL do console, realize a configuração abaixo.

   Siga estas etapas:

   a. No campo Local do navegador, digite about:config.

   b. Clique em **Serei cuidadoso, prometo!** para seguir para a página about:config.

   c. Defina os valores de acordo com as seguintes opções, para que o navegador confie no dispositivo ProxySG e negocie a autenticação:

      network.automatic-ntlm-auth.trusted-uris, network.-negotiate.auth.delegation-uris, network.negotiate-auth.trusted-uris

      Para cada opção, execute as seguintes etapas:

      - Use a rolagem ou digite o nome da opção no campo Filtro para localizar a opção que deseja definir.
      - Clique duas vezes na opção para abrir a caixa de diálogo Digite o valor de sequência de caracteres.
      - Digite o URL virtual (para implantações transparentes).

        Se você tiver mais de um dispositivo ProxySG que solicitará credenciais de autenticação, separe as entradas com vírgulas. Por exemplo, se o URL aberto para o console for https://-localhost:8015, é possível digitar localhost como o valor de sequência de caracteres, ou https://10.57.60.9:8015 e, em seguida, digitar 10.57.60.9 como o valor de sequência de carac-

teres.

- Clique em **OK**.

4. Ao usar o Internet Explorer para abrir o console com a IWA na máquina remota que tem a mesma credencial do Windows da máquina local onde o UDP está instalado, pode ser preciso seguir estas etapas:
   a. Selecione Ferramentas > Opções da internet.
   b. Selecione a guia Segurança.
   c. Selecione a zona local de intranet e clique em Sites > **Avançado**.
   d. Digite o nome de domínio totalmente qualificado do appliance ProxySG (para implantações explícitas) ou o URL virtual (para implantações transparentes) no campo Adicionar este site à zona e clique em Adicionar > Fechar > OK.
   e. Selecione a guia Avançado e, em Segurança, marque a opção Ativar autenticação integrada do Windows caso ela ainda não esteja marcada.
   f. Clique em **OK** para salvar as alterações e fechar a caixa de diálogo Opções da internet.

O console do Arcserve UDP não oferece suporte a IWA se a conexão de banco de dados do Console usar o modo de autenticação do Windows

Para usar a IWA (Integrated Windows Authentication – Autenticação Integrada do Windows), é necessário alterar o modo de autenticação de Configuração do banco de dados do console para o modo de autenticação do Windows e do SQL Server.

Siga estas etapas:

1. Na ferramenta de gerenciamento do SQL Server, verifique se o banco de dados do console oferece suporte ao modo de autenticação do Windows e do SQL Server. Se não tiver suporte para banco de dados do console, alterne para o modo de autenticação do Windows e do SQL Server e reinicie o SQL Server.
2. Siga estas etapas para criar a conta do Arcserve UDP no SQL Server:
   a. Na pasta a seguir, clique com o botão direito do mouse em**DBAccountUpdate.bat** e, em seguida, clique na opção **Executar como administrador**:

      *<Pasta de Instalação do UDP>**Management**BIN*\

      A interface de comando é exibida.

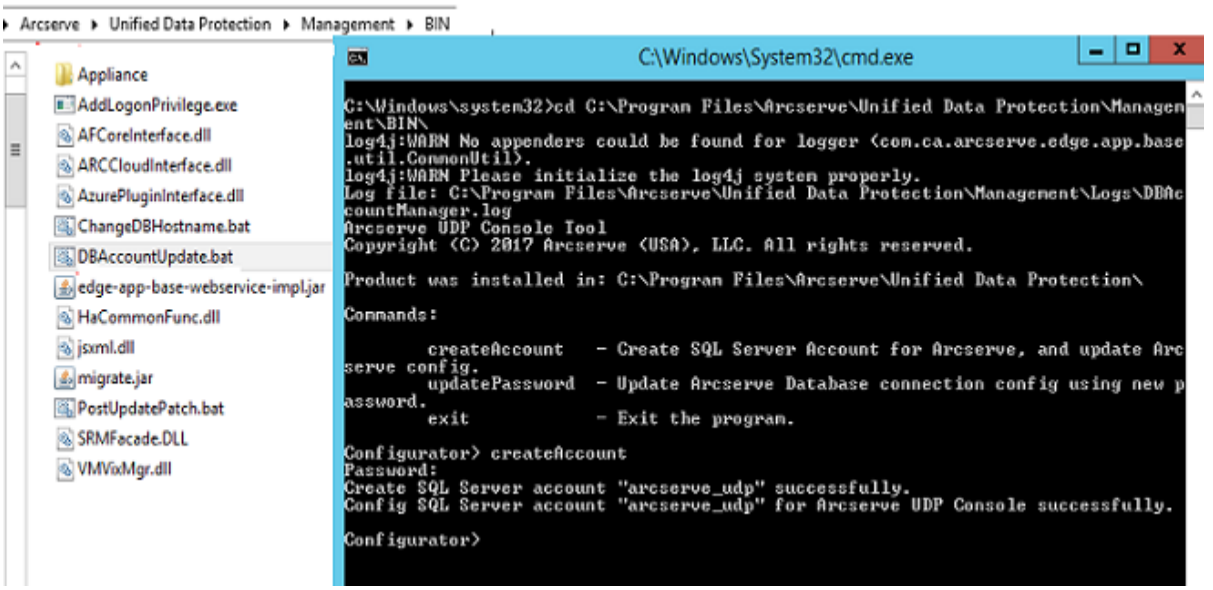
   b. Na interface de comando, digite *createAccount* e pressione Enter.

      A interface de linha de comando solicita que você forneça uma senha.

   c. Especifique a senha desejada para a conta *arcserve_udp* e pressione Enter.

      O console do Arcserve UDP cria a conta *arcserve_udp* do SQL Server.

   d. Digite *exit* para fechar a interface de linha de comando.



3. Reinicie o serviço de gerenciamento do Arcserve UDP.

Solução de problemas

Esta lista apresenta soluções para problemas que podem surgir no console de gerenciamento de usuários:

- **Sintoma**

  Falha ao efetuar logon no console de gerenciamento de usuários

  Solução

  Certifique-se de que você se conectou como administrador. Os usuários não administradores não têm permissão para acessar o Console de gerenciamento do usuário. Verifique se o nome de usuário e a senha estão corretos.

- **Sintoma**

  Falha de autenticação: o usuário não consegue efetuar logon no console

  Solução

  Verifique se o usuário está atribuído a alguma função. Se não estiver atribuído a uma função, o usuário não conseguirá efetuar logon no console do Arcserve UDP.

- **Sintoma**

  Tempo limite atingido para a página Console de gerenciamento de usuários

  Solução

  O tempo de retenção do logon para a página de gerenciamento de usuários é de 15 minutos. Se o Console não detectar nenhuma operação na página por 15 minutos, o usuário é automaticamente desconectado.

Capítulo 8: Adicionando e gerenciando nós de origem

Esta seção contém os seguintes tópicos:

Como adicionar nós no console

Um nó faz referência a um computador de origem físico ou virtual que você deseja proteger. É possível proteger um nó fazendo backup de dados para um destino. O Arcserve Unified Data Protection permite adicionar os seguintes tipos de nós:

- Windows
- Linux
- Máquinas virtuais nos servidores VMware ESX/vCenter e Microsoft Hyper-V

É possível adicionar nós especificando manualmente os detalhes do nó, detectando de um active directory ou importando de um arquivo e hipervisores.

Observação: também é possível adicionar nós durante a criação de um plano.

O que fazer a seguir?

- Verificar os pré-requisitos
- Adicionar nós
- Detectar nós
- Importar nós

Verificar os pré-requisitos

Antes de começar a adicionar um nó, complete as seguintes tarefas de pré-requisitos:

1. Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.
2. Efetue logon no Console.
3. Clique na guia **Recursos**.

   A página **Nós: todos os nós** é exibida.
4. No painel central, clique em **Adicionar nós**.

   A caixa de diálogo **Adicionar nós ao console do Arcserve UDP** é exibida.

   A caixa de diálogo fornece várias opções para adicionar um nó.

Adicionar nós

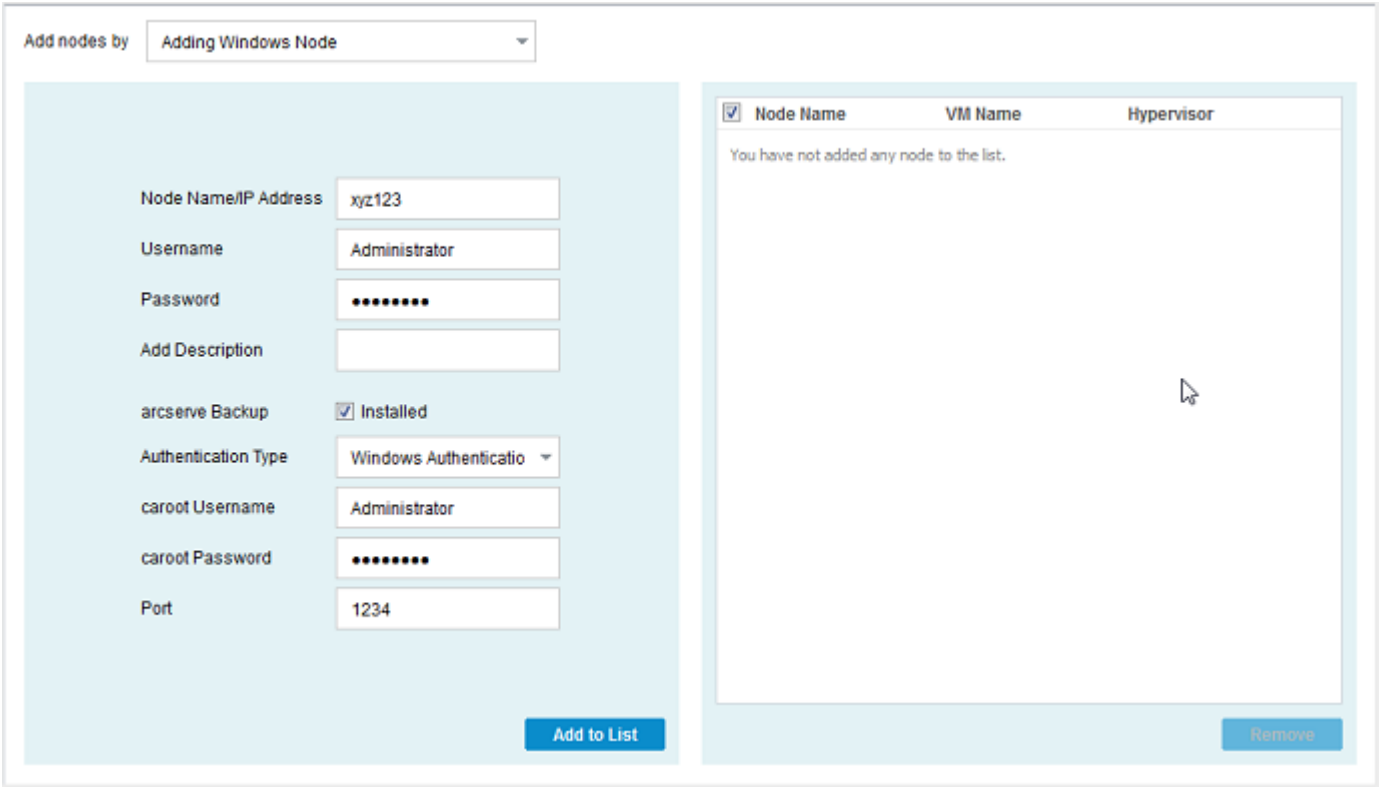
Quando você tiver o endereço IP, o nome de um nó ou de um conjunto de nós, é possível adicioná-lo ao console, especificando os detalhes manualmente. É possível adicionar os seguintes tipos de nós:

- **Windows:** os nós de origem Windows que você deseja proteger. Quando o nó de origem do Windows com porta SMB é bloqueado, o Agente do Arcserve UDP (Windows) é instalado nesse nó.
- **Linux:** os nós de origem Linux que você deseja proteger. O Agente do Arcserve Unified Data Protection para Linux está instalado no servidor de backup Linux e não nos nós de origem Linux.
- **Servidor de backup Linux:** o servidor Linux que gerencia os nós de origem Linux. O Agente do Arcserve Unified Data Protection para Linux está instalado neste servidor.

Siga estas etapas:

1. Na lista suspensa **Adicionar nós por**, selecione uma das seguintes opções:

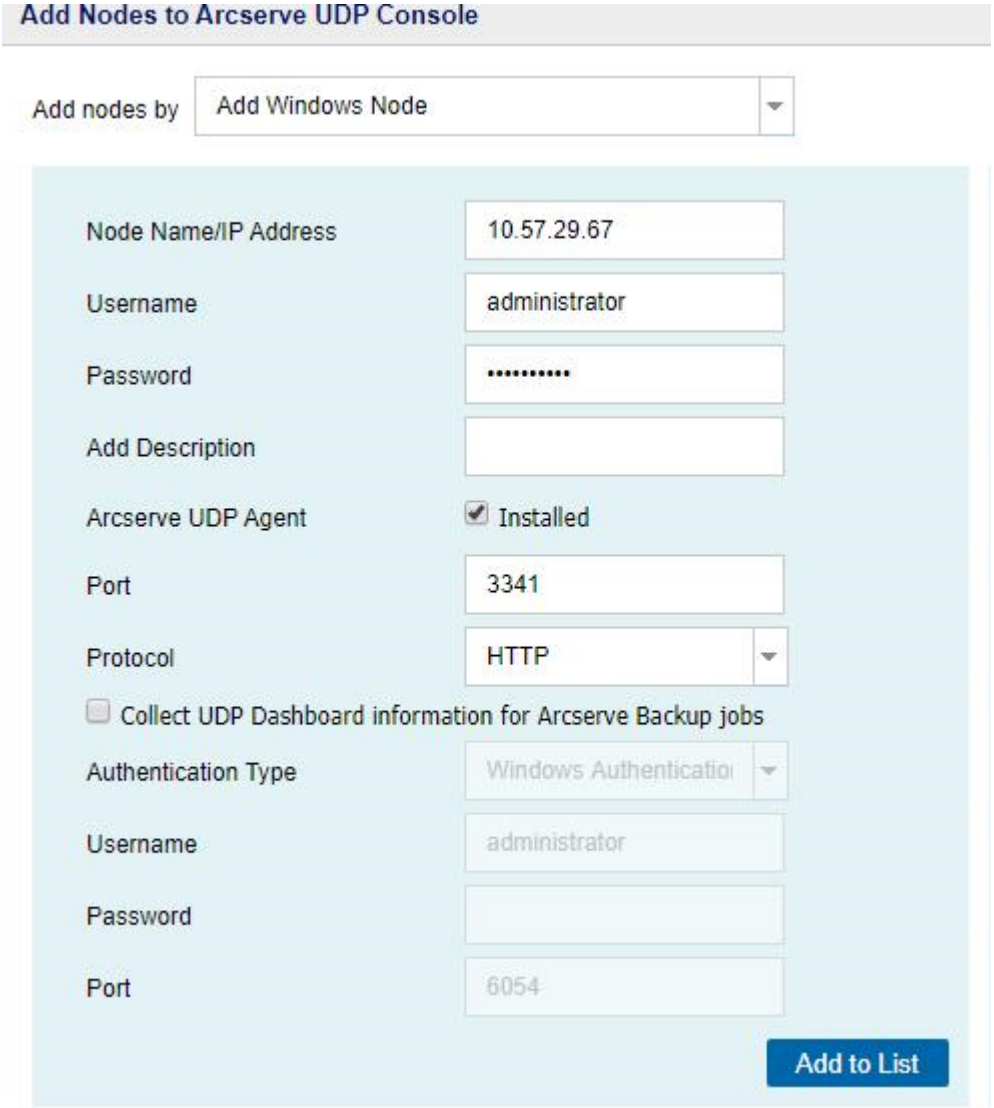
Adicionando nó do Windows



Observação: para ativar os detalhes do Arcserve Backup, selecione **Instalado**.

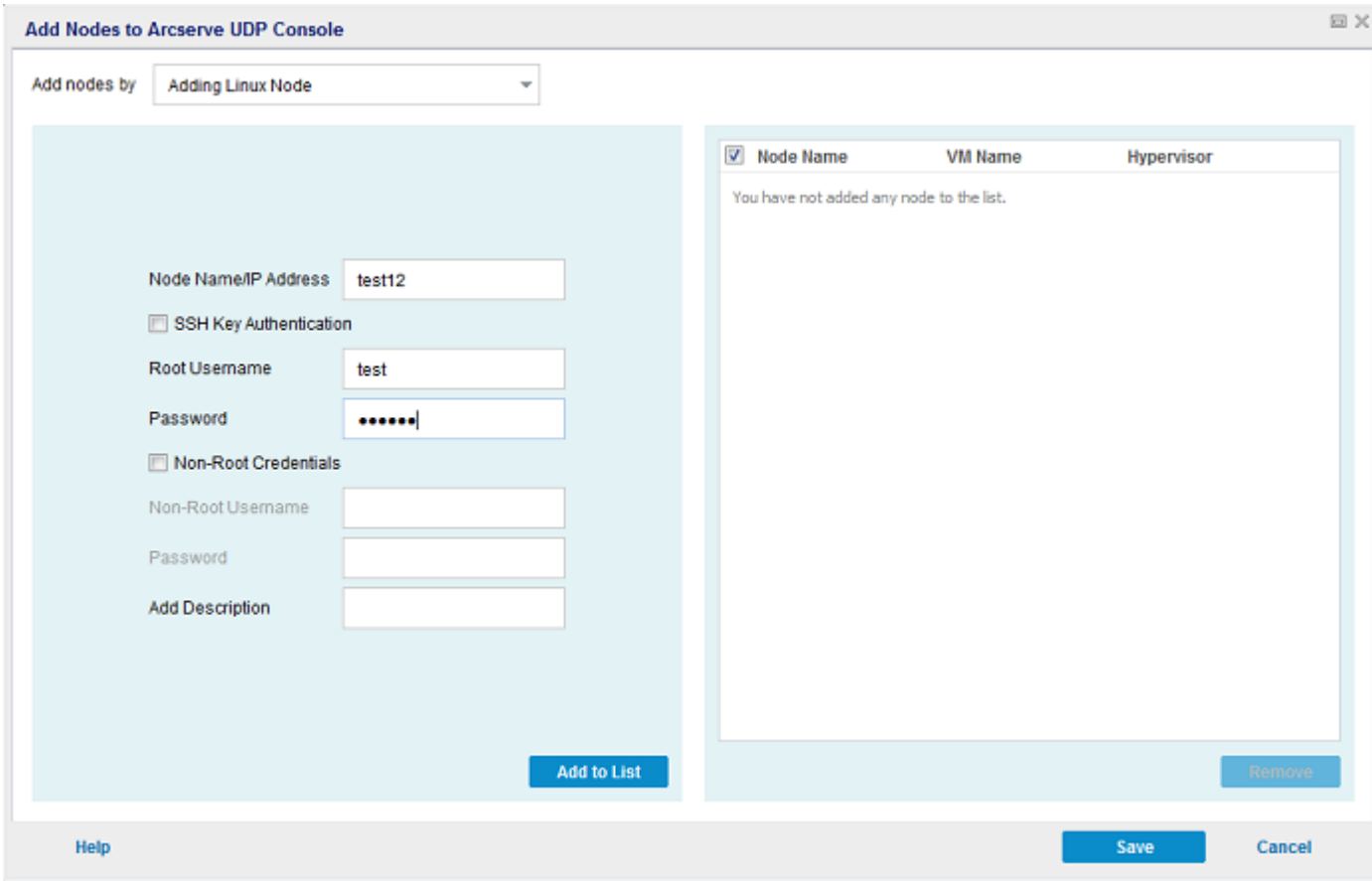
2. Para adicionar um nó bloqueado de porta SMB, vá para a lista suspensa **Adicionar nós por** e selecione uma das seguintes opções:

Adicionando nó do Windows



Observação: forneça os detalhes personalizados da porta e do protocolo e selecione instalado.

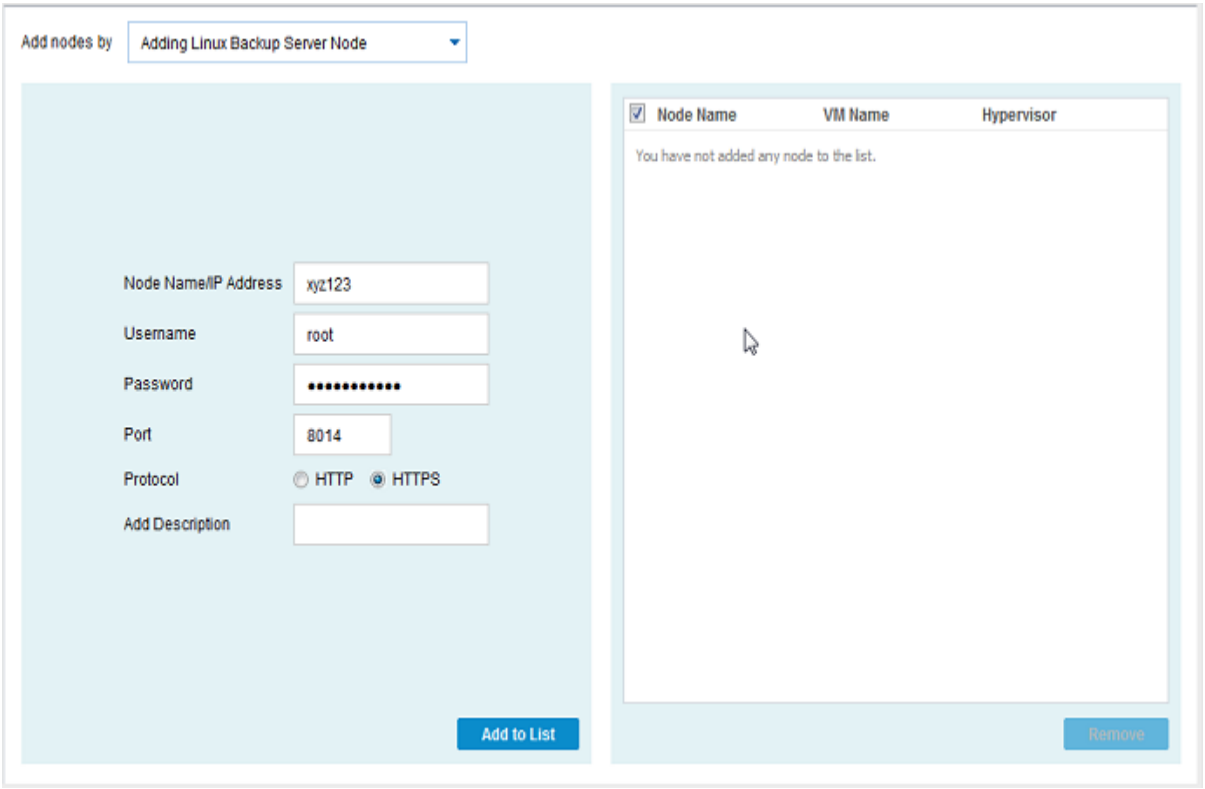
Adicionando nós Linux



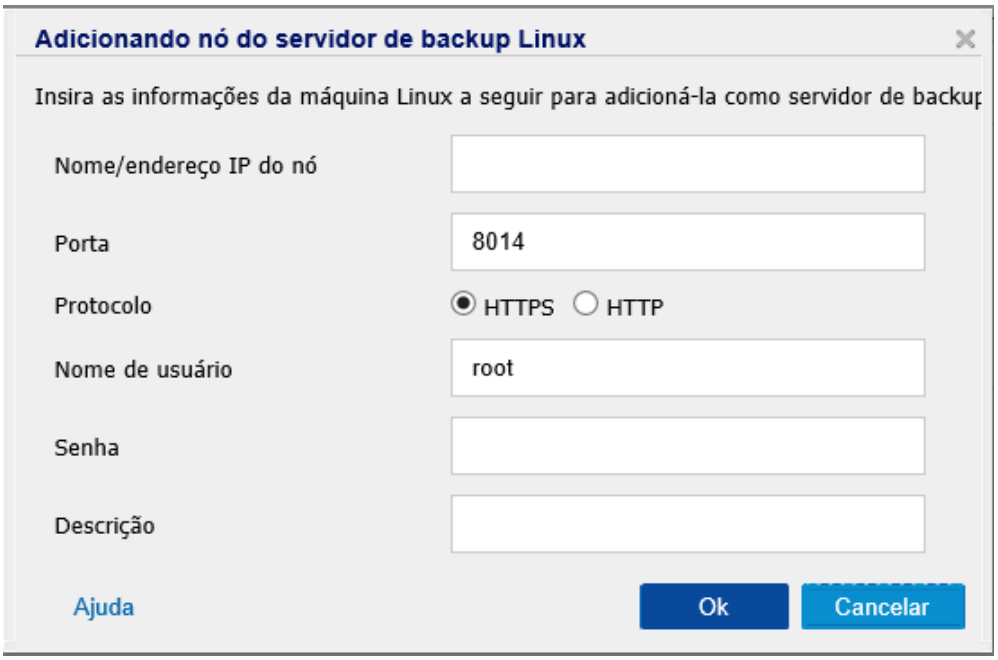
Observações:

- Para Linux, quando a opção **Autenticação da chave SSH** está selecionada, não é preciso digitar detalhes de senha, basta informar o nome de usuário. Para obter mais informações sobre como configurar a chave SSH, consulte o tópico Configurar a autenticação de chave pública e chave privada.
- Antes de adicionar um nó Linux, será necessário adicionar um **Servidor de backup Linux** que gerencie os nós Linux.
- No nó do Debian Linux, credenciais não raiz não são suportadas. Para adicionar o Debian Linux com um usuário que não é raiz, use sudoers. Para obter mais informações sobre como configurar o Sudo, consulte Configurar o sudo no Debian.
- Você só pode efetuar logon no servidor de backup Linux pelo console do Arcserve UDP ao executar uma restauração.

Adicionando nó do servidor de backup Linux



A caixa de diálogo a seguir aparece quando você adiciona o nó do servidor de backup Linux pela tarefa **Backup: Linux com base em agente**:



Os detalhes da opção selecionada são exibidos.

3. Digite os detalhes do nó e clique em **Adicionar à lista**.

O nó é adicionado ao painel direito. Para adicionar mais nós, siga as etapas novamente. Todos os nós adicionados são listados no painel direito.

4. (Opcional) Para remover os nós adicionados da lista do painel direito, selecione os nós e clique em **Remover**.
5. Selecione os nós a serem adicionados e clique em **Salvar**.

   Os nós são adicionados e exibidos na página **Nós: todos os nós**.

   Se o servidor de backup Linux estiver no ambiente NAT, siga estas etapas antes de adicionar os nós ao console do Arcserve UDP:

   1. Crie um arquivo *server.cfg* na seguinte pasta do servidor de backup Linux:

      /opt/Arcserve/d2dserver/configfiles/.
   2. Adicione a seguinte linha ao arquivo server.cfg:

      nat_enable=true
   3. Reinicie o agente do Linux usando a seguinte linha de comando:

      /opt/Arcserve/d2dserver/bin/d2dserver restart

   Observação: se este servidor de backup Linux já foi adicionado, atualize-o no console do UDP.

Detectar nós

Para adicionar nós que estão em um diretório ativo, é possível detectar primeiro os nós fornecendo os detalhes do diretório ativo e, em seguida, adicionando os nós ao Console.

Siga estas etapas:

1. Na lista suspensa **Adicionar nós por**, selecione **Detectando nós do Active Directory**.
2. Especifique as credenciais de usuário e clique em **Adicionar**.

   Nome de usuário

   Especifica o domínio e o nome de usuário no formato domínio\nome de usuário.

   Senha

   Especifica a senha do usuário.

   Filtragem pelo nome do computador

   Especifica o filtro para detectar os nomes do nó.

   Após a validação, o nome de usuário é adicionado à lista.
3. Selecione o nome de usuário adicionado e clique em **Procurar**.

   Uma detecção de nós com êxito resulta em uma caixa de diálogo **Confirmar** que pergunta se deseja adicionar os nós a partir do resultado da **Detecção**.

   Observação: o processo de detecção pode levar algum tempo, dependendo de fatores como a rede e o número de computadores na rede.
4. Clique em **Sim**.

   Os nós detectados são listados.
5. Selecione o nó, digite o nome de usuário e a senha e, em seguida, clique em **Aplicar**.

   Observação: quando você clicar em Aplicar, as credenciais serão verificadas. Você deve verificar cada nó antes de adicioná-lo à lista.

   As marcas de seleção verdes são exibidas para os nós verificados.
6. Clique em **Adicionar à lista**.

   O nó selecionado é listado no painel à direita.
7. Para adicionar os nós ao console, no painel à direita, selecione o nó e clique em **Sal-**

var. Para adicionar todos os nós, marque a caixa de seleção **Nome do nó**.

Os nós selecionados são adicionados e exibidos na página **Nós: todos os nós**.

Solução de problemas: o domínio especificado não existe ou não pôde ser contatado

Sintoma

Ao adicionar nós por detecção a partir de um Active Directory, recebo a seguinte mensagem de erro:

"O domínio especificado não existe ou não pôde ser contatado. Verifique se o Console do servidor pode acessar o controlador de domínio por meio da rede."

Solução

Primeiro, verifique a conexão entre o controlador de domínio e o Arcserve UDP. Se a conectividade estiver correta, use o comando a seguir com o argumento "dsgetdc" para verificar se o Windows pode localizar o controlador de domínio a partir do nome do domínio:

nltest.exe

Por exemplo, "nltest /dsgetdc:sample_domain", onde sample_domain é o nome do domínio.

Se houver falha no comando, poderá haver um problema de DNS em seu ambiente.

Observação: você deve executar o comando acima na máquina do UDP. Para obter mais detalhes, consulte o artigo da Microsoft.

Importar nós

O Arcserve Unified Data Protection permite adicionar vários nós físicos e virtuais usando o método de importação. Dependendo dos requisitos, é possível usar um dos seguintes métodos de importação:

- Importar nós de um arquivo CSV ou TXT
- Importar nós de um servidor vCenter/ESX
- Importar nós de um servidor Hyper-V

Importar nós de um servidor vCenter/ESX

Com esse método de importação, é possível importar nós da máquina virtual do servidor ESX ou vCenter. Essa opção listará todas as máquinas virtuais detectadas no servidor especificado, mesmo se já estiverem sendo gerenciadas no Arcserve Unified Data Protection.

Siga estas etapas:

1. Na lista suspensa **Adicionar nós por**, selecione **Importando do vCenter/ESX**.
2. Especifique os detalhes do servidor vCenter/ESX e clique em **Conectar**.

   A árvore do nó é exibida no painel à esquerda.

   Observação: o VMware Virtual Disk Development Kit (VDDK) 6.x.x é fornecido com o Arcserve UDP versão 7.0, mas o VDDK 6.x.x não oferece suporte a HTTP. Além disso, o vCenter e o ESX normalmente oferecem suporte à conexão HTTPS apenas por padrão. Selecione HTTPS, a menos que você substitua manualmente o VDDK 6.x.x integrado pelo VDDK de outra versão e configure manualmente o vCenter/ESX para permitir a conexão HTTP.
3. Expanda a árvore do nó.

   (Opcional) É possível digitar o nome do nó no campo de filtro para localizar o nó na árvore.
4. Selecione os nós que você deseja adicionar.

   Observação: o Arcserve UDP permite executar as seguintes opções:

   - Adicionar e proteger objetos de recipiente na infraestrutura do vSphere (como datacenter e pool de recursos).
   - Adicionar e proteger o modelo de VM e proteger a VM por qualificador.

   Mas, no momento, é possível executar essa ação apenas usando o Assistente de plano. Para obter detalhes, consulte *Adicionar nós do vCenter/ESX* no tópico Especificar a origem.
5. Marque a caixa de seleção **Fornecer credenciais para os nós selecionados** e forneça as credenciais do usuário.

   Observação: as credenciais do usuário são necessárias para funções como as de PFC (Pre-Flight Check - Verificação Prévia), de truncamento do log do aplicativo e para os comandos de backup anterior e posterior.
6. Clique em **Adicionar à lista**.

   Os nós selecionados são adicionados ao painel direito.

7. Selecione os nós e clique em **Salvar**.

   Os nós são adicionados e exibidos na página **Nós: todos os nós**.

Importar nós de um servidor Hyper-V

Com esse método de importação, é possível importar os nós da máquina virtual dos servidores Microsoft Hyper-V.

Siga estas etapas:

1. Na lista suspensa **Adicionar nós por**, selecione **Importando do vHyper-V**.
2. Preencha os campos a seguir e clique em **Conectar**.

   Hyper-V

   Especifica o endereço IP ou o nome do Hyper-V Server. Para importar máquinas virtuais que estão nos clusters do Hyper-V, especifique o nome de nó de cluster ou nome do host do Hyper-V.

   Nome de usuário

   Especifica o nome de usuário do Hyper-V com direitos de administrador.

   Observação: para os clusters do Hyper-V, use uma conta de domínio com privilégios administrativos do cluster. Para hosts autônomos do Hyper-V, recomenda-se usar uma conta de domínio.

   Senha

   Especifica a senha do nome de usuário.

   A solução Arcserve Unified Data Protection pesquisa e exibe uma árvore de nós no painel esquerdo.
3. Expanda a árvore do nó.

   (Opcional) É possível digitar o nome do nó no campo de filtro para localizar o nó na árvore.

   Observação: as máquinas virtuais configuradas como função de cluster são listadas logo abaixo do nome do nó do cluster na árvore. As máquinas virtuais que não fazem parte do cluster são listadas sob o nome do host de cada host individual do Hyper-V.
4. Selecione os nós que você deseja adicionar.
5. Marque a caixa de seleção **Fornecer credenciais para os nós selecionados** e forneça as credenciais do usuário.

   Observação: as credenciais do usuário são necessárias para funções como as de PFC (Pre-Flight Check - Verificação Prévia), de truncamento do log do aplicativo e para os comandos de backup anterior e posterior. Sem as credenciais do usuário, a PFC apresenta falha para os nós selecionados.
6. Clique em **Adicionar à lista**.

Os nós selecionados são adicionados ao painel direito.

7. Selecione os nós e clique em **Salvar**.

   Os nós são adicionados e exibidos na página **Nós: todos os nós**.

Importar máquina virtual usando a conta de administrador adicional

A conta de administrador adicional faz referência a essas contas que não são os administradores padrão. Essas contas também são conhecidas como contas administrativas não integradas. Para importar a máquina virtual de um host do Hyper-V, use a conta de administrador integrada do host do Hyper-V, uma conta de domínio que esteja no grupo de administradores locais do host do Hyper-V ou um usuário administrativo não integrado.

O usuário com a conta administrativa adicional pode usar os procedimentos explicados abaixo para desativar o acesso remoto do UAC.

Observações:

- Esse procedimento não é semelhante à desativação do UAC. Com ele, é possível desativar algumas das funções do UAC.
- Considerando que a tecnologia remota de WMI é usada para importação, verifique se a WMI não foi bloqueada pelo firewall.

Siga estas etapas:

1. Clique em Iniciar, digite regedit nos programas de pesquisa e nos campos dos arquivos e, em seguida, pressione Enter.

   O Editor do registro do Windows é exibido.

   Observação: talvez você precise fornecer credenciais administrativas para abrir o Editor do registro do Windows.

2. Localize e clique na chave de registro a seguir:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

3. No menu Editar, clique em Novo e, em seguida, clique em Valor DWORD (32 bits).
4. Especifique LocalAccountTokenFilterPolicy como o nome da nova entrada e pressione Enter.
5. Clique com o botão direito do mouse em LocalAccountTokenFilterPolicy e, em seguida, clique em Modificar.
6. Especifique 1 no campo de dados Valor e clique em OK.
7. Feche o Editor do Registro.

   Para obter mais informações sobre o comportamento do Windows, consulte a documentação da Microsoft.

Importar nós de um arquivo CSV ou TXT

Quando há vários nós físicos para adição, em vez de adicionar um nó de cada vez, você pode criar um arquivo CSV ou TXT usando o formato <NodeName>, <UserName>, <Password>. Posteriormente, é possível selecionar o arquivo CSV ou TXT e importá-lo para o console usando as opções de procura e upload.

Siga estas etapas:

1. Na lista suspensa **Ações**, selecione **Importar.**
2. Clique em **Procurar** para selecionar o arquivo salvo no formato CSV ou TXT.
3. Clique em **Carregar**.

   Os nós são adicionados e exibidos na página **Nós: todos os nós**.

Como gerenciar nós

Com o Arcserve UDP, é possível executar várias ações para gerenciar um nó, como atualizar o nó e o hipervisor, exportar nós, excluir e executar verificações prévias.

O que fazer a seguir?

- Verificar os pré-requisitos
- Atualizar as informações do hipervisor
- Especificar o hipervisor
- Atualizar informações da VM
- Atualizar nós
- Exportar nó
- Pausar nós
- Retomar nós
- Sincronizar dados
- Excluir nós do console
- Implantar o agente em nós
- Executar verificações prévias para as tarefas de backup

Verificar os pré-requisitos

Antes de começar a gerenciar os nós, conclua os seguintes pré-requisitos:

- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.
- Efetue logon no Console.
- Adicione um nó.

Atualizar informações do hipervisor

Após um nó de VM ser adicionado ao Arcserve Unified Data Protection, as informações relacionadas à conexão, como nome do host ou as credenciais do hipervisor da VM podem ser alteradas. Nesses casos, o Arcserve Unified Data Protection permite atualizar informações do hipervisor.

Siga estas etapas:

1. Clique na guia **Recursos**.
2. Clique com o botão direito do mouse no grupo de nós em **Grupos do vCenter/ESX** ou **Grupos do Hyper-V**.
3. Clique em **Atualizar vCenter/ESX** ou **Atualizar Hyper-V**.

   A caixa de diálogo **Atualizar vCenter/ESX** ou **Atualizar Hyper-V** é exibida.
4. Digite os novos detalhes na caixa de diálogo e clique em **OK**.

   A caixa de diálogo **Atualizar vCenter/ESX** ou **Atualizar Hyper-V** é fechada.

   As informações do hipervisor foram atualizadas com êxito.

Especificar o hipervisor

Especifique os detalhes do hipervisor para evitar o uso de licenças adicionais enquanto protege uma VM. Quando protege uma VM (Virtual Machine – Máquina Virtual) usando um plano de backup sem agente com base em host, a licença de host do hipervisor é usada para proteger a VM. Não é necessário instalar nenhum agente na VM. Em alguns casos, é possível optar por instalar o agente na VM e criar um plano de backup com base em agente para proteger a VM. Em tais casos, a VM usará outra licença, diferente da licença de host do hipervisor. Especifique os detalhes do hipervisor nesses casos que a VM usará a licença de host do hipervisor em vez de qualquer outra licença.

Exemplos descrevendo quando especificar as informações de hipervisor:

- Você tem um plano de backup sem agente com base em host para proteger as VMs do ESX ou Hyper-V Server. O plano usa a licença do hipervisor para proteger a VM. Agora, você instala o agente do UDP em uma VM do hipervisor especificado e cria um plano com base no agente para proteger a VM. Em geral, o plano usa a licença adicional para proteger a VM. Se especificar o hipervisor da VM, o plano usará a licença do hipervisor.
- Você tem um plano Linux com base em agente para proteger os nós de agente da VM Linux. Se especificar o hipervisor da VM, todas as VMs no mesmo hipervisor compartilharão a licença do hipervisor.

Considere as seguintes observações antes de especificar o hipervisor:

- Não é possível especificar o hipervisor para um nó físico.
- Não é possível especificar o hipervisor para um nó de VM importado do vCenter/ESX ou Hyper-V.
- É possível especificar o hipervisor para várias VMs desde que elas pertençam simultaneamente ao mesmo hipervisor.
- Verifique se as ferramentas do VMware ou o serviço de integração do Hyper-V mais recentes estão instalados e se a VM está ligada. Além disso, verifique se a WMI (Windows Management Instrumentation - Instrumentação de Gerenciamento do Windows) está na lista de exceções do firewall no nó do agente da VM.

Siga estas etapas:

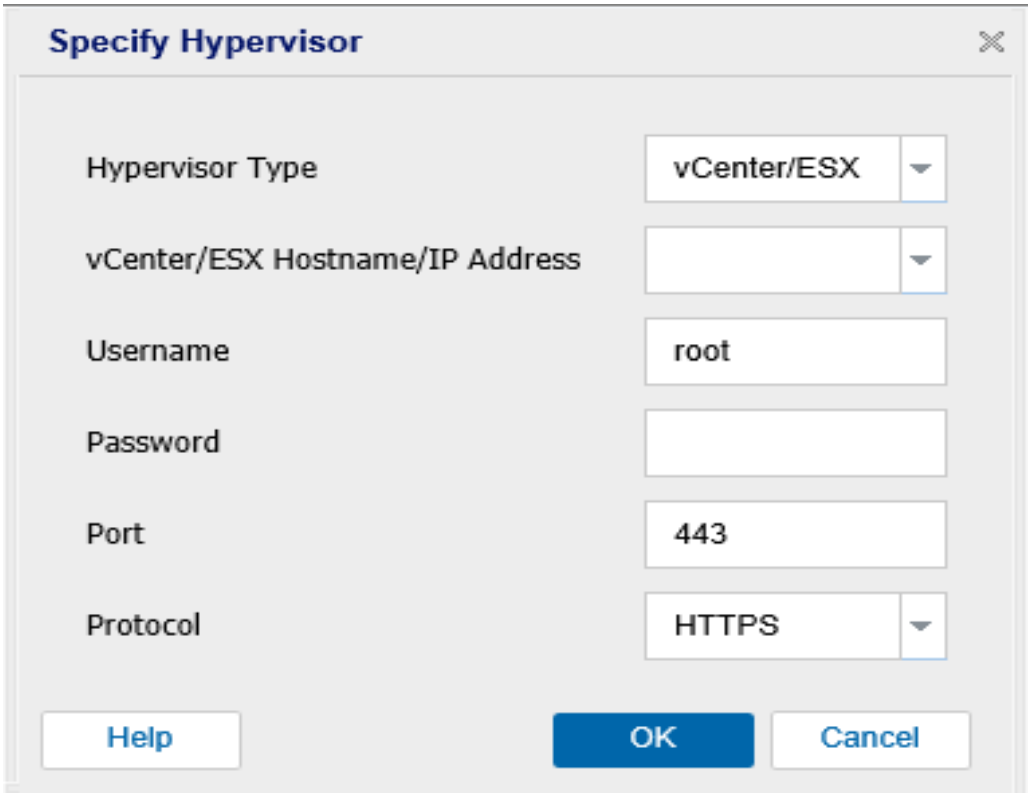
1. Clique na guia **Recursos**.
2. No painel esquerdo, navegue para **Nós** e clique em **Todos os nós**.

   A página **Nós: todos os nós** é exibida.

3. Execute uma das seguintes ações:
   - Clique com o botão direito do mouse no nome do nó.
   - Selecione o nome do nó e, no painel central, clique na lista suspensa **Ações**.

   Uma lista de opções é exibida.
4. Clique em **Especificar hipervisor**.

   A caixa de diálogo Especificar hipervisor é exibida. As opções em **Tipo de hipervisor** são: **Hyper-V**, **vCenter/ESX** e **Outro** (Xen, Kernel-based Virtual Machine, Red Hat Enterprise Virtualization).



5. Digite os detalhes do hipervisor e clique em **OK**.

   As informações do hipervisor são especificadas.

Atualizar informações da VM

O Arcserve Unified Data Protection permite atualizar algumas das propriedades dos nós de VM a partir dos seus hipervisores. É possível acionar a atualização manualmente ou automaticamente. As propriedades a seguir dos nós de VM são atualizadas e sincronizadas com suas respectivas máquinas virtuais no hipervisor:

- Nome do nó
- Nome da VM
- OS

Para acionar a atualização manualmente, use a opção **Atualizar informações da VM**.

Siga estas etapas:

1. Clique na guia **Recursos**.

   A página **Nós: Todos os nós** é exibida.

2. No painel central, clique na lista suspensa **Ações** e, em seguida, clique em **Atualizar informações da VM**.

   A caixa de diálogo **Atualizar informações da VM** é aberta.

3. Clique em **OK**.

   Você disparou uma detecção manual, que atualizará os nós da máquina virtual.

   O recurso de atualização automática é acionado automaticamente quando você executa as seguintes ações:

   - Abre a guia **Recurso** no console.
   - Envia um relatório programado.

   Observação: mesmo que você acione várias atualizações automáticas, apenas uma atualização automática é executada de cada vez. As atualizações automáticas restantes serão colocadas em uma fila.

Atualizar nós

É possível atualizar as informações relacionadas aos nós existentes. É possível atualizar o nó a qualquer momento. Algumas das situações em que é necessário atualizar um nó são as seguintes:

- Um novo produto foi instalado no nó após o nó ter sido registrado no Arcserve Unified Data Protection.
- O nome de usuário ou a senha do nó foi atualizado após o nó ter sido registrado no Arcserve Unified Data Protection.

Observação: se um nó atuar como servidor do ponto de recuperação e agente, e você alterar as credenciais ou o protocolo desse nó, atualize o nó na página **Destinos: servidor de ponto de recuperação**. O plano será implantado automaticamente no agente depois de atualizar o servidor do ponto de recuperação. Se atualizar o nó da página **Nós: todos os nós**, os planos envolvendo esses nós não serão implantados com êxito. Para implantar o plano, atualize novamente o nó na página **Destinos: servidor do ponto de recuperação**.

Siga estas etapas:

1. Clique na guia **Recursos**.

   A página **Nós: todos os nós** é exibida.

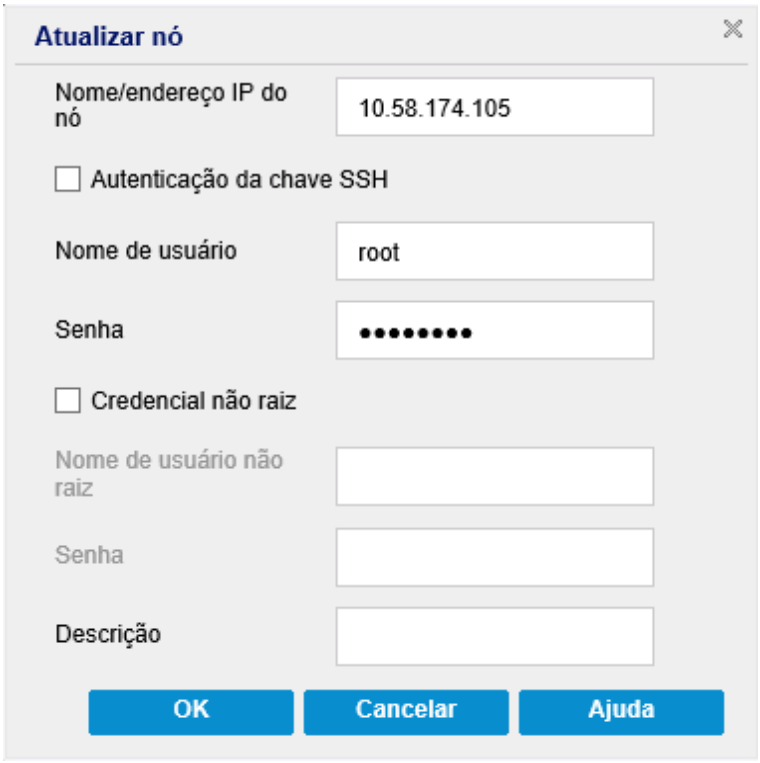
2. Execute uma das seguintes ações:

   - Clique com o botão direito do mouse no nome do nó.
   - Selecione o nome do nó e, no painel central, clique na lista suspensa **Ações**.

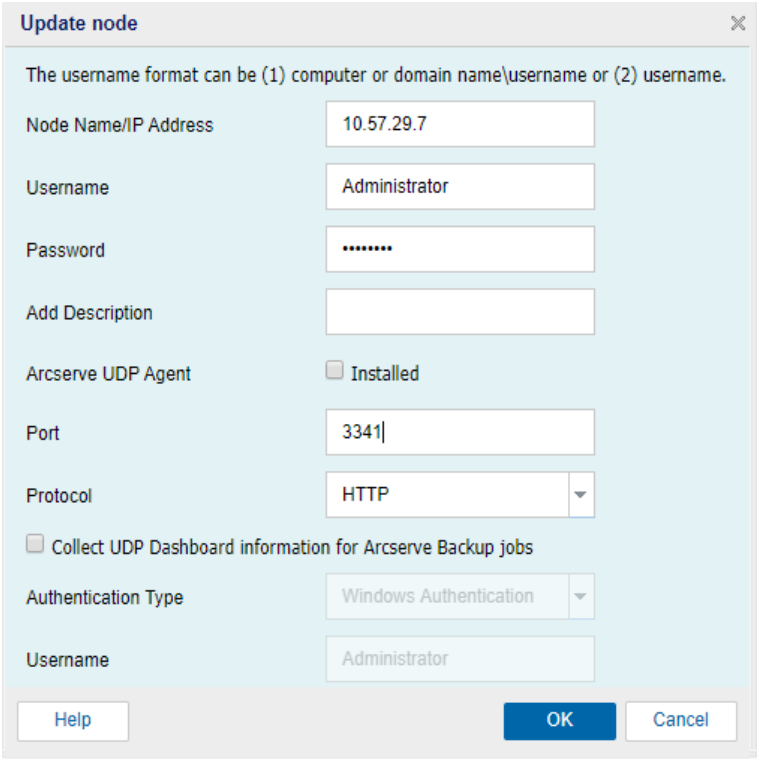
3. Clique em **Atualizar**.

   A caixa de diálogo **Atualizar nó** é exibida.

   A caixa de diálogo a seguir destina-se a nós do Linux:



A caixa de diálogo a seguir para o nó do Windows (quando a porta SMB está bloqueada) com uma porta personalizada é exibida:



4. Atualize os detalhes e clique em **OK**.

   As informações do nó são atualizadas.

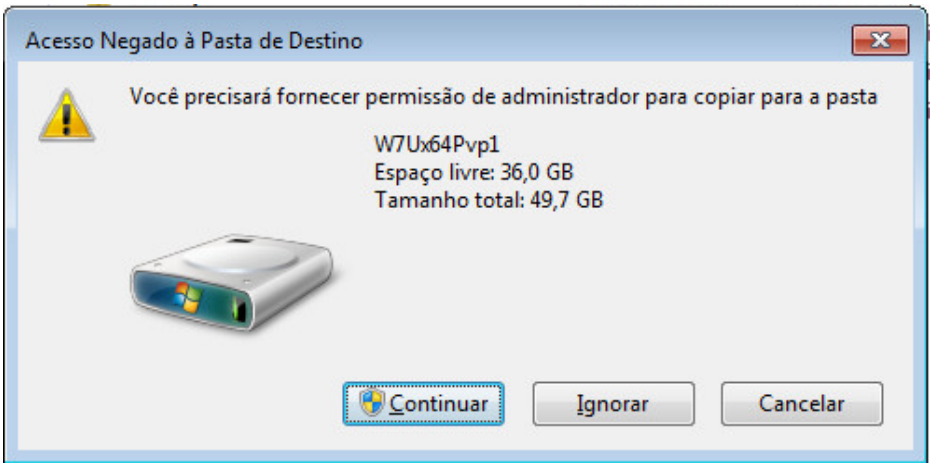
Atualizar nós usando uma conta administrativa adicional

Conta administrativa adicional refere-se às contas que não usam administradores padrão. Essas contas também são conhecidas como contas administrativas não integradas. As funções Atualizar nó e Verificação prévia (PFC) usam a conta especificada em Atualizar nó para se conectar a uma máquina virtual e executar as verificações relacionadas.

Observação: é necessário usar a conta de administrador interno ou a conta de administrador de domínio interno ao executar a função Atualizar nó. Se necessário, é possível usar a um administrador que não seja interno, mas antes de fazer isso, é preciso verificar se a conta usada tem as permissões de administrador.

Siga estas etapas:

1. Verifique se consegue acessar \\[nome de host da VM]\ADMIN$ usando a conta de administrador adicional de outro computador. Se tiver algum problema, verifique se "Compartilhamento de arquivos e impressoras" está bloqueado pelo firewall. Se as configurações do firewall forem boas, pode ser necessário desativar o acesso remoto de UAC. Para desativar o acesso remoto de UAC, consulte Importar máquina virtual usando a conta administrativa adicional.
2. Além da VMware, ao atualizar os nós, o Arcserve UDP instala automaticamente algumas ferramentas na VM para executar a PFC. Para verificar se a conta tem as permissões necessárias, faça o seguinte:
    a. Efetue logon na máquina virtual usando a conta de administrador que não seja interno.
    b. Copie um arquivo a partir do diretório C:\Windows para C:\ e certifique-se de que a seguinte mensagem não seja exibida:



c. Se você encontrar qualquer problema, é possível modificar as configurações de UAC. Para isso, desmarque a opção **Executar todos os administradores no modo de aprovação de administrador** na diretiva de segurança local alterando as configurações de UAC em secpol.msc -> Diretivas locais -> Opções de segurança. (Secpol.msc é editor da diretiva de segurança da Microsoft).

Observação: não tente desativar o UAC na caixa de diálogo Configurações de controle de conta do usuário, que é aberta no painel de controle.

Para obter mais informações sobre como alterar as definições de configuração do UAC, consulte a documentação correspondente da Microsoft.

3. Para VMs do Hyper-V, a conta de administrador adicional deve ter permissões semelhantes como mencionado na Importação da máquina virtual usando a conta administrativa adicional.

Exportar nó

É possível exportar os nós como um arquivo ZIP (.zip). Quando necessário, é possível importar o arquivo ZIP para manter os nós. Por exemplo, exportar nós antes de atualizações ou reinicializações ajuda a importar o mesmo conjunto de nós.

É possível exportar apenas os nós que possuem credenciais válidas e que são executados no sistema operacional Windows.

Siga estas etapas:

1. Clique na guia **Recursos**.

   A página **Nós: Todos os nós** é exibida.
2. Selecione o nó.
3. No painel central, clique na lista suspensa **Ações** e clique em **Exportar**.

   Uma caixa de diálogo é exibida solicitando sua ação no arquivo list.zip.
4. Clique em **Abrir** ou **Salvar**.

   A lista de nós é exportada.

Pausar nós

Usando o Arcserve UDP, é possível pausar apenas nós selecionados, em vez do plano inteiro. Agora, para impedir a execução de uma tarefa programada, não é necessário pausar e retomar o plano inteiro, o que interrompe todos os nós associados.

Importante: o recurso Pausar um nó só funciona se esse nó está associado a um plano do Windows com base em agente ou a um plano sem agente com base em host. Para outros planos, não é possível pausar um nó.

Siga estas etapas:

1. Clique na guia **Recursos**.

   A página **Nós: todos os nós** é exibida.

2. Selecione os nós desejados associados a um plano.

3. No painel central, clique na lista suspensa **Ações** e clique em **Pausar**.

   Uma caixa de diálogo de confirmação será exibida, indicando que somente tarefas manuais podem ser executadas para nós pausados

4. Clique em **Sim**.

   Os nós são pausados. Se algum nó não for pausado, será exibida uma mensagem explicando o motivo.

Retomar nós

Usando o Arcserve UDP, você pode retomar um nó pausado. Agora, em vez de pausar e retomar um plano, é possível pausar e retomar nós específicos associados a um plano.

Importante: pausar e retomar um recurso de nó funcionará somente se o nó estiver associado a um plano do Windows com base em agente ou a um plano sem agente com base em host. Para outros planos, não é possível pausar ou retomar um nó.

Siga estas etapas:

1. Clique na guia **Recursos**.

   A página **Nós: todos os nós** é exibida.

2. Selecione os nós pausados.

3. No painel central, clique na lista suspensa **Ações** e clique em **Retomar**.

   Uma caixa de diálogo é exibida solicitando a confirmação da ação.

4. Clique em **Sim**.

   O nó começa a ser executado novamente.

Sincronizar dados

A sincronização dos dados mantém os dados nos diferentes bancos de dados consistentes e atualizados.

Siga estas etapas:

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.

   A página **Nós: Todos os nós** é exibida.
3. (Nível de grupo) Selecione um dos grupos de nós que são exibidos no painel esquerdo e clique com o botão direito do mouse.
4. Clique em uma das seguintes opções:

   Observação: você pode exibir somente as opções que já adicionou para a sincronização com o Arcserve Unified Data Protection.

   - Sincronização completa do Arcserve Backup
   - Sincronização incremental do Arcserve Backup

   A caixa de diálogo **Informações** explica que o método de sincronização selecionado é enviado.

Excluir nós do console

Com o Arcserve Unified Data Protection, você tem a opção de excluir um nó. Se excluir os nós, os logs associados e os históricos de tarefas também serão excluídos. É possível adicionar o nó excluído mais tarde, se necessário.

Siga estas etapas:

1. Clique na guia **Recursos**.

   A página **Nós: Todos os nós** é exibida.

2. Selecione o nó que deseja excluir.
3. Execute uma das seguintes ações:
   - Clique com o botão direito do mouse no nome do nó.
   - Selecione o nome do nó e, no painel central, clique na lista suspensa **Ações**.
4. Clique em **Excluir**.

   A caixa de diálogo **Confirmação** é exibida.

5. Clique em **Sim**.

   O nó é excluído do console.

Implantar o agente em nós

Para atualizar ou instalar o Agente do Arcserve Unified Data Protection para um nó, use **Instalar/atualizar agente**. Se a máquina de destino tiver uma versão anterior do Agente do Arcserve Unified Data Protection, use a opção de atualização para obter a versão mais recente. Caso contrário, use a opção de instalação.

Observação: é possível implantar os Agentes do Arcserve Unified Data Protection em vários nós. De uma só vez, é possível executar apenas 16 tarefas de implantação. Se houver mais de 16 tarefas, outras tarefas permanecem no status pendente e são executadas somente quando algumas das 16 tarefas padrão implantadas estiverem concluídas. Para modificar a contagem de tarefas máximas, atualize a seguinte chave do registro:

deployMaxThreadCount

Siga estas etapas:

1. Clique na guia **Recursos**.

   A página **Nós: Todos os nós** é exibida.

2. Selecione um ou mais nós.

3. No painel central, clique na lista suspensa **Ações** e, em seguida, clique em **Instalar/atualizar o agente**.

   Os detalhes da instalação ou atualização são exibidos acima do nome do nó no painel central.

4. Verifique os detalhes.

5. Especifique a programação de instalação/atualização e clique em **OK**.

   O nó é instalado ou atualizado com a versão mais recente do Agente do Arcserve Unified Data Protection.

   Observação: você pode cancelar uma implantação de agente se ela tiver sido programada para uma ocasião futura. Para cancelar uma implementação do agente, selecione o agente e clique em **Ações, Cancelar implantação do agente**.

Executar verificações prévias para as tarefas de backup

A solução Arcserve Unified Data Protection oferece um utilitário chamado PFC (Pre-flight Check – Verificação Prévia), que permite fazer verificações vitais em nós específicos para detectar condições que podem ocasionar a falha das tarefas de backup. A PFC só é aplicável aos nós da máquina virtual que são importados do vCenter/ESX, do Hyper-V ou do Nutanix AHV. A PFC não funciona com o modelo de VM do VMware. A PFC é executada automaticamente quando você executa as seguintes ações:

- Importar máquinas virtuais de um sistema vCenter Server/ESX Server, Hyper-V ou Nutanix AHV.
- Permitir que uma tarefa de backup seja executada.

Outras referências:

- Soluções para itens da verificação prévia de VMs do VMware
- Soluções para itens da verificação prévia de VMs do Hyper-V
- Soluções para itens da verificação prévia de VMs do Nutanix AHV

Além disso, também é possível executar uma verificação prévia manualmente.

Siga estas etapas:

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.

   A página **Todos os nós: nó** é exibida no painel central.
3. Clique com o botão direito do mouse no nome de um nó e clique em **Verificação prévia**.

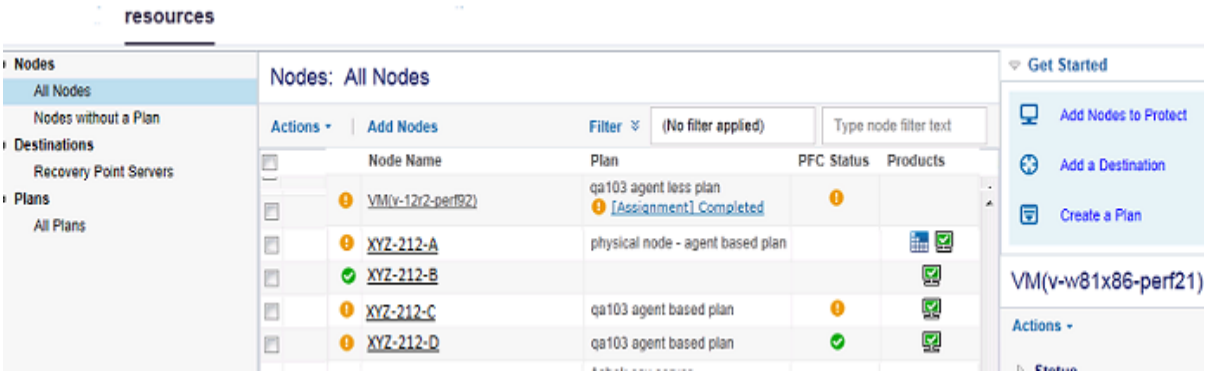
   Observação: também é possível executar a **Verificação prévia** usando uma das opções a seguir:

   - (Nível do nó) Clique nas caixas de seleção dos nós em que deseja executar a verificação prévia e, em seguida, clique em **Ações** e selecione **Verificação prévia**.
   - (Nível de grupo) Clique com o botão direito do mouse no grupo que contém os nós e clique em **Verificação prévia**.

   A mensagem a seguir é exibida: **iniciando a verificação prévia da máquina virtual.**
4. Vá para a coluna **Status do PFC** para exibir o status da Verificação prévia.

Observação: por padrão, a coluna Status do PFC não é visível na interface do usuário. É necessário ativar manualmente a coluna Status do PFC na interface do usuário.

Também é possível exibir o status de Verificação antecipada clicando em **Exibir Logs** no painel direito.



A tabela a seguir descreve as verificações executadas pela PFC para VMware VM:

Item	Descrição
CBT	Um recurso que rastreia os setores do disco localizados em uma máquina virtual que foi alterada. Isso ajuda a reduzir o tamanho dos backups. Este item verifica se o CBT está ativado.
VMware Tools	Este item verifica se as ferramentas de VMware estão instaladas em cada máquina virtual.
Discos	Este item verifica os discos da máquina virtual.
Estado da energia	Este item verifica se a máquina virtual está ligada.
Consistência dos dados	Este item verifica se o instantâneo consistente com o aplicativo pode ser executado para a VM.
ESX Server	Este item verifica se um servidor pode detectar a máquina virtual. A opção fica visível somente quando o nó não está disponível no ESX.

A tabela a seguir descreve as verificações executadas pela PFC para Hyper-V VM:

Item	Descrição
Credenciais do Hyper-V	O produto precisa implantar um utilitário de backup e o recurso Alterar rastreamento de bloco no Hyper-V Server por meio de sistemas de compartilhamento ADMIN$. A ação ajuda a verificar se o produto tem permissão necessária para o compartilhamento. A tarefa Backup/restauração falha se as credenciais do Hyper-V não estiverem corretas ou se o compartilhamento ADMIN$ foi fechado pelo administrador.
Serviços de integração	Este item verifica se os serviços de integração do Hyper-V estão instalados e ativados em cada máquina virtual. Sem os serviços de integração, o Arcserve

	Unified Data Protection não conseguirá concluir as ações a seguir: ▪ Executar comando anterior/posterior e ações de limpeza do log do aplicativo. ▪ Executar backup consistente com aplicativo. Os serviços de integração contém vários serviços. O Arcserve Unified Data Protection verifica o status dos dois serviços a seguir: ▪ Serviço de Troca de dados do Hyper-V: necessário para coletar informações da VM, executar comandos anteriores ou posteriores e ações de limpeza do log do aplicativo. ▪ Solicitante de Cópia de Sombra de Volume do Hyper-V: necessário backup consistente com aplicativo.
Estado da energia	Este item verifica se a máquina virtual está ligada. Um aviso de suspensão é exibido quando a VM estiver no status diferente de ligado e desliga, como o status Salvo. A solução Arcserve Unified Data Protection não consegue executar os comandos anterior/posterior e as ações de limpeza do log do aplicativo quando a VM não está no status Ativado. Além disso, o Arcserve Unified Data Protection não consegue executar o backup consistente com o aplicativo quando a VM está no status Suspenso.
Discos	Este item verifica se um disco não compatível está conectado à VM.
Consistência dos dados	Este item verifica se o instantâneo consistente com o aplicativo pode ser executado para a VM.

A tabela a seguir descreve as verificações executadas pela PFC para a VM do Nutanix AHV:

Item	Descrição
Estado da energia	Este item verifica se a máquina virtual está ligada.
Consistência dos dados	Este item verifica se o instantâneo consistente com o aplicativo pode ser executado para a VM.
Servidor do AHV	Este item verifica se um servidor pode detectar a máquina virtual. A opção fica visível somente quando o nó não está disponível no Nutanix AHV.

Soluções para itens da verificação prévia de VMs do VMware

Outras referências:

- Soluções para itens da verificação prévia de VMs do Hyper-V
- Soluções para itens da verificação prévia de VMs do Nutanix AHV

As tabelas a seguir descrevem as soluções para ajudá-lo a resolver erros e avisos dos resultados da anterior de VMS do VMware:

CBT

Status	Mensagem	Solução
Erro	Não é possível ativar o rastreamento do bloco alterado.	Se a máquina virtual não possuir a versão 7 ou superior do hardware, atualize a versão do hardware da máquina virtual ou crie um plano de backup com base em Agente no Arcserve Unified Data Protection e use o Agente do Arcserve Unified Data Protection para Windows para fazer backup da VM.
Aviso	O Rastreamento de Bloco Alterado é ativado com os instantâneos presentes. Um backup de disco completo será aplicado para as tarefas de backup completo e de verificação.	**Observação:** isso afeta apenas as tarefas de backup completo e de verificação. Para uma tarefa de backup Incremental, faz-se o backup apenas dos dados alterados. Para aplicar o backup de bloco usado para as tarefas de backup completo e de verificação, execute as seguintes etapas: 1. Exclua todos os instantâneos associados à máquina virtual. 2. Efetue logon no servidor proxy de backup. 3. Abra o editor de Registro e procure a seguinte chave: *HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\ARCserve Unified Data Protection\Engine\AFBackupDll\<VM-InstanceUUID>* **Observação:** substitua <VM-InstanceUUID> pelo valor UUID da máquina virtual em que o CBT estiver falhando. É possível encontrar o valor no URL da máquina virtual usada quando conectada ao Agente do Arcserve UDP (Windows). 4. Defina a chave do Registro como "full disk backupForFullBackup"=0. 5. Crie/defina o Registro como ResetCBT=1. 6. Envie a tarefa de backup.

VMware Tools

Status	Mensagem	Solução
Aviso	Desatualizado.	Instale a versão mais recente do VMware Tools.
Aviso	Não instalado ou não está em execução.	Instale a versão mais recente do VMware Tools e certifique-se de que a ferramenta está em execução.

Discos

Status	Mensagem	Solução
Erro	Instantâneos de VM não são suportados para a VM, pois ela tem um controlador SCSI configurado para configuração de compartilhamento de barramento.	Criar um plano de backup com base no Agente no Arcserve Unified Data Protection ou usar o Agente do Arcserve Unified Data Protection para Windows para fazer backup da VM.
Aviso	Não será feito backup do disco físico de RDM (Raw Device Mapping – Mapeamento de Dispositivo Simples).	Criar um plano de backup com base no Agente no Arcserve Unified Data Protection ou usar o Agente do Arcserve Unified Data Protection para Windows para fazer backup da VM.
Aviso	O disco virtual de RDM será armazenado em backup como um disco cheio.	Criar um plano de backup com base no Agente no Arcserve Unified Data Protection ou usar o Agente do Arcserve Unified Data Protection para Windows para fazer backup da VM.
Aviso	Não será feito backup do disco independente.	Criar um plano de backup com base no Agente no Arcserve Unified Data Protection ou usar o Agente do Arcserve Unified Data Protection para Windows para fazer backup da VM.
Aviso	Para tarefas de backup completo ou de verificação, faz-se o backup do disco no repositório de dados do NFS como um disco cheio.	**Observação:** isso afeta apenas as tarefas de backup completo e de verificação. Para uma tarefa de backup Incremental, faz-se o backup apenas dos dados alterados. Mova o disco virtual para um repositório de dados em um dispositivo de armazenamento de bloco ou crie um plano de backup com base em Agente no Arcserve Unified Data Protection ou use o Agente do Arcserve Unified Data Protection para Windows para fazer backup da VM.

Estado da energia

Status	Mensagem	Solução
Aviso	Desligado	Ligue a máquina virtual.
Aviso	Suspenso	Ligue a máquina virtual.

Consistência dos dados

Status	Mensagem	Solução

Aviso	O VMware não conta com suporte para encerramento em nível de aplicativo para uma VM que tem discos IDE.	Criar um plano de backup com base no Agente no Arcserve Unified Data Protection ou usar o Agente do Arcserve Unified Data Protection para Windows para fazer backup dos dados do Microsoft SQL Server e do Exchange Server.
Aviso	O VMware não conta com suporte para encerramento em nível de aplicativo para uma VM que tem discos SATA.	Criar um plano de backup com base no Agente no Arcserve Unified Data Protection ou usar o Agente do Arcserve Unified Data Protection para fazer backup dos dados do Microsoft SQL Server e do Exchange Server.
Aviso	VMware não oferece suporte a encerramento consistente com o aplicativo porque a versão do ESX Server é anterior à release 4.1.	Atualize o ESX Server para 4.1 ou superior, ou crie um plano de backup com base em Agente no Arcserve Unified Data Protection ou use o Agente do Arcserve Unified Data Protection para Windows para fazer backup dos dados do Microsoft SQL Server e do Exchange Server.
Aviso	VMware não oferece suporte a encerramento consistente com o aplicativo porque não há slots de SCSI suficientes disponíveis	Adicione um controlador SCSI à VM a partir do vSphere Web Client ou crie um plano de backup com base em agente no Arcserve Unified Data Protection ou use o Agente do Arcserve Unified Data Protection para Windows para fazer backup dos dados do Microsoft SQL Server e do Exchange Server.
Aviso	O VMware não conta com suporte a encerramento consistente com o aplicativo se o sistema operacional convidado tiver discos dinâmicos.	Criar um plano de backup com base no Agente no Arcserve Unified Data Protection ou usar o Agente do Arcserve Unified Data Protection para Windows para fazer backup dos dados do Microsoft SQL Server e do Exchange Server. **Observação:** o VMware não permite fechar para novas sessões o aplicativo em máquinas virtuais com o Windows Server 2008 e discos básicos ou dinâmicos.
Aviso	Não verificado porque o aplicativo não conseguiu acessar a máquina virtual. Certifique-se de que as credenciais do usuário estão cor-	Forneça as credenciais de administrador de domínio ou de administrador local integrado para efetuar

	retas e têm privilégios administrativos.	logon no sistema operacional convidado da máquina virtual. Além disso, verifique se o VMware Tools dentro da máquina virtual estão atualizados e em execução. Devido a uma limitação do VMware, o backup é compatível apenas com as VMs em execução em um ESX Server que possuem uma licença paga. Um backup não é suportado em servidores ESXi com uma licença gratuita. **Observação:** a verificação de consistência dos dados é suportada no Windows Server 2008 e posterior.
Aviso	Não foi possível verificar se o backup consistente de dados é possível porque a máquina virtual não está ligada.	Consulte a coluna Estado de energia
Aviso	O VMware não conta com suporte a encerramento consistente com o aplicativo se o sistema operacional convidado tiver espaços de armazenamento ativados. A recuperação no nível de arquivo é suportada apenas para os volumes que não têm espaços de armazenamento ativados. (A recuperação integral da VM oferece suporte para recuperação da VM).	Criar um plano de backup com base no Agente no Arcserve Unified Data Protection ou usar o Agente do Arcserve Unified Data Protection para Windows para fazer backup dos dados do Microsoft SQL Server e do Microsoft Exchange Server.

Como criar instantâneos consistentes com o aplicativo para VMware

Em alguns casos, o gravador de VSS da VMware não cria instantâneos consistentes com o aplicativo em algumas máquinas virtuais. Como resultado, os dados de backup podem não estar em um estado consistente com o aplicativo.

Verificar pré-requisitos:

Atenda aos seguintes pré-requisitos para criar instantâneos consistentes com o aplicativo:

- As ferramentas mais recentes do VMware devem estar instaladas e em execução dentro do sistema operacional convidado da VM. Além disso, verifique se o serviço provedor de instantâneo da VMware está instalado (não precisa estar em execução).
- A VM deve ser executada no ESXi 4.1 ou posterior.
- A VM deve usar apenas discos SCSI. A VM deve ter o mesmo número de slots SCSI livres correspondente ao número de discos.
- A interrupção consistente com aplicativo não é suportada para a VM que possui discos IDE ou SATA.
- Todos os volumes na VM são discos básicos e não há discos dinâmicos.
- O sistema operacional convidado da VM não tem espaço de armazenamento ativado.
- O parâmetro disk.EnableUUID da VM deve ser ativado. VMs criadas em 4.1 ou posterior têm esse parâmetro ativado por padrão. As seguintes configurações são executadas automaticamente por tarefa de backup para evitar inconsistência de dados e executar o backup consistente com o aplicativo. Se a tarefa de backup não puder ativar disk.EnableUUID devido a alguns motivos, configure o parâmetro manualmente usando o seguinte procedimento:
  - Se disk.EnableUUID existe e é FALSE, altere-o para TRUE.
  - Se disk.EnableUUID não existir, crie-o e defina-o como TRUE.
  - Se disk.EnableUUID existe e é TRUE, mantenha-o como está.

  Observação: para obter mais informações sobre como criar backups consistentes com o aplicativo, consulte o artigo sobre base de conhecimento da VMware.

Recursos afetado:

Se algum dos requisitos não for atendido, os dados da sessão permanecerão travados de maneira consistente. Como resultado, os seguintes recursos serão afetados:

- Os dados de backup que incluem dados do aplicativo de uma VM, como SQL, Exchange e SharePoint podem permanecer em um estado consistente de travamento.
- A tarefa de geração de catálogo pode falhar.

Soluções para itens da verificação prévia de VMs do Hyper-V

Outras referências:

- Soluções para itens da verificação prévia de VMs do VMware
- Soluções para itens da verificação prévia de VMs do Nutanix AHV

As tabelas a seguir descrevem as soluções para ajudá-lo a resolver erros e avisos dos resultados da verificação prévia de VMs do Hyper-V:

Credenciais do Hyper-V

Status	Mensagem	Solução
Erro	Falha ao acessar o compartilhamento ADMIN$ do servidor Hyper-V ou as devidas credenciais não existem.	■ Verificar se o servidor Hyper-V está em execução ■ Verifique se a rede do servidor Hyper-V é conectável. ■ Verifique se o compartilhamento ADMIN$ do Hyper-V Server está ativado. ■ Fornecer direitos de administrador do Hyper-V durante a importação de VM a partir dele.

Serviços de integração

Status	Mensagem	Solução
Aviso	Não instalado, em execução e operacional.	Instalar/atualizar/ativar os serviços de integração. **Observações:** ■ Para VM do Windows, se os serviços de integração estiverem instalados, verifique se os dois serviços seguintes necessários estão em execução na VM: serviço do Hyper-V Data Exchange e Solicitante de Cópia de Sombra de Volume do Hyper-V. Além disso, verifique se há erros de serviços do Hyper-V no log de eventos da VM. ■ Para Linux VM, verifique se os serviços de integração mais recentes estão instalados e os recursos de *Par Chave-Valor* e *backup da máquina virtual online* estão disponíveis na VM Linux específica. Para obter mais informações sobre os serviços inte-

		grados Linux na VM do Hyper-V, consulte o artigo de Microsoft KB.
Aviso	Não está respondendo.	Reiniciar os serviços de integração no sistema operacional convidado da VM.
Aviso	O serviço de integração dentro da máquina virtual é incompatível com o serviço de integração no servidor Hyper-V.	Crie um plano de backup com base em agente no Arcserve Unified Data Protection ou use o Agente do Arcserve Unified Data Protection para fazer backup da VM.
Aviso	Desatualizado.	Atualizar os serviços de integração.

Estado da energia

Status	Mensagem	Solução
Aviso	Desligado.	Ligue a máquina virtual.
Aviso	Suspenso.	Ligue a máquina virtual.

Discos

Status	Mensagem	Solução
Aviso	Não será feito backup do disco rígido vinculado à máquina virtual.	Crie um plano de backup com base em agente no Arcserve Unified Data Protection ou use o Agente do Arcserve Unified Data Protection para fazer backup da máquina virtual.
Aviso	Falha ao obter a máquina virtual pela UUID da instância.	Verifique se a máquina virtual está presente no servidor Hyper-V.

Consistência dos dados

Status	Mensagem	Solução
Aviso	Um instantâneo consistente com o aplicativo não é suportado. A máquina virtual tem um disco dinâmico.	Crie um plano de backup com base em agente no Arcserve Unified Data Protection ou use o Agente do Arcserve Unified Data Protection para fazer backup da máquina virtual.
Aviso	Um instantâneo consistente com o aplicativo não é suportado porque a VM tem espaços de armazenamento.	Criar um plano de backup com base em agente no Arcserve UDP ou usar o Agente do Arcserve UDP para fazer backup da máquina virtual.
Aviso	Um instantâneo consistente com o aplicativo não é suportado porque a VM tem um volume cujo armazenamento de cópia de sombra está localizado em outro volume.	Alterar a área de armazenamento de cópia de sombra do volume para o próprio volume. **Observação:** em uma VM no Hyper-V 2012 R2, se a última atualização da Microsoft for aplicada no host do Hyper-V, o instantâneo consistente com o aplicativo ainda será suportado nesses casos.

Aviso	Um instantâneo consistente com o aplicativo não é suportado. A máquina virtual tem diferentes sistemas de arquivos que não são NTFS/-referências.	Se quiser fazer backup da máquina virtual, mas ignorar outros sistemas de arquivos que não sejam NTFS/Refs, crie um plano de backup com base em agente no Arcserve Unified Data Protection ou use o Agente do Arcserve Unified Data Protection para fazer backup da máquina virtual. **Observação:** em uma VM no Hyper-V 2012 R2, se a última atualização da Microsoft for aplicada no host do Hyper-V, o instantâneo consistente com o aplicativo ainda será suportado nesses casos.
Aviso	Um instantâneo consistente com o aplicativo não é suportado. O recurso de instantâneo em escopo está ativado na máquina virtual.	Desative o ScopeSnapshot dentro da VM adicionando uma chave de registro DWORD, HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\\SystemRestore ScopeSnapshots com o valor 0.
Aviso	Um instantâneo consistente com o aplicativo não é suportado. O serviço de integração não está operacional (estado de Falha).	Consulte a coluna Serviços de integração.
Aviso	Não verificado devido à falha na obtenção da máquina virtual por UUID da instância.	Verifique se a máquina virtual está presente no servidor Hyper-V.
Aviso	Não verificado, pois a máquina virtual não está ligada.	Consulte a coluna Estado de energia.
Aviso	Um instantâneo consistente com o aplicativo não é suportado. Entretanto, ocorreu uma falha ao efetuar logon na máquina virtual para verificar o motivo.	Fornecer credenciais de administrador de domínio ou de administrador local integrado para efetuar logon no sistema operacional convidado da máquina virtual. Além disso, verificar se a máquina virtual tem conectividade de rede.
Aviso	Um instantâneo consistente com o aplicativo não é suportado por motivo desconhecido.	Para identificar o motivo de não ser possível obter um instantâneo consistente com o aplicativo, verifique os logs do evento. O log do evento está no seguinte local: Na VM: Visualizador de eventos > Logs do Windows > Aplicativo e sistema. No log, procure por erros provenientes do disco, do VSS e do VolSnap. No servidor Hyper-V: Visualizador de eventos > Logs do Windows > Logs de aplicativos e serviços > Microsoft > Windows > Hyper-V-*. No log, procure por erros da VM correspondente.

Como criar instantâneos consistentes com o aplicativo para Hyper-V

Em alguns casos, o gravador de VSS do Hyper-V não cria instantâneos consistentes com o aplicativo em algumas máquinas virtuais (VMs). Como resultado, os dados de backup podem não estar em um estado consistente com o aplicativo.

Verificar pré-requisitos:

Atenda aos seguintes pré-requisitos para criar instantâneos consistentes com o aplicativo:

- Na VM filho, o serviço de integração chamado Solicitante de Cópia de Sombra de Volume do Hyper-V está instalado e em execução.
- A VM filho deve estar no estado de execução.
- O Local do arquivo de Instantâneo da VM foi configurado para ser o mesmo volume no sistema operacional do host que dos arquivos VHD da VM.
- Todos os volumes na VM filho são discos básicos e não há discos dinâmicos.
- Todos os discos da VM filho devem usar um sistema de arquivos que ofereça suporte a instantâneos (por exemplo, NTFS).

Verificar considerações:

Atenda às considerações a seguir para criar instantâneos consistentes com o aplicativo:

- O serviço de integração instalado na VM filho deve ser compatível com o host do Hyper-V.
  - Por exemplo: o serviço de integração Windows 8.1/2012R2 dentro da VM não é compatível com o host Hyper-V do Windows 2008 R2.
- Para Windows 8, 2012 e posterior, e a VM executando execução no host Hyper-V do Windows 2008 R2, o recurso de instantâneo em escopo na VM deve ser desativado. Para desativar o recurso de instantâneo em escopo, siga estas etapas:
  1. Efetue logon na VM.
  2. Vá até o seguinte local:

     HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion
  3. Abra a chave SystemRestore.

     Observação: crie a chave se ela não existir.

4. Adicione o valor de registro DWORD de 32 bits chamado "ScopeSnapshots" e defina o valor como 0.

Recursos afetado:

Se alguns dos requisitos não forem atendidos, os dados da sessão permanecerão travados de maneira consistente. Como resultado, os seguintes recursos serão afetados:

- Os dados de backup que incluem dados do aplicativo de uma VM, como SQL, Exchange e SharePoint podem permanecer em um estado consistente de travamento.
- A tarefa de geração de catálogo pode falhar.

Soluções para itens da verificação prévia de VMs do Nutanix AHV

Outras referências:

- Soluções para itens da verificação prévia de VMs do VMware
- Soluções para itens da verificação prévia de VMs do Hyper-V

As tabelas a seguir descrevem soluções para ajudar você a resolver erros e avisos dos resultados da verificação prévia de VMs do Nutanix AHV:

NGT (Nutanix Guest Tools)

Status	Mensagem	Solução
Aviso	Não está em execução	Ative o Nutanix Guest Tools para a VM.
Aviso	Ativado	O Guest Tools está ativado, mas não está em execução. Instale o Guest Tools na VM.

Estado da energia

Status	Mensagem	Solução
Aviso	Desligado	Ligue a máquina virtual.
Aviso	Suspenso	Continue a máquina virtual.

Consistência dos dados

Status	Mensagem	Solução
Aviso	A Nutanix não oferece suporte ao encerramento consistente com o aplicativo para VMs com discos IDE.	Crie um plano de backup com base em agente no Arcserve UDP ou use o Agente (Windows) do Arcserve UDP para fazer backup dos dados do Microsoft SQL Server e Exchange Server.
Aviso	A Nutanix não oferece suporte ao encerramento consistente com o aplicativo para VMs com discos SATA.	Crie um plano de backup com base em agente no Arcserve UDP ou use o Agente do Arcserve UDP para fazer backup dos dados do Microsoft SQL Server e Exchange Server.
Aviso	A Nutanix não oferece suporte ao encerramento consistente com o aplicativo quando não há slots SCSI adequados disponíveis.	Crie um plano de backup com base em agente no Arcserve UDP ou use o Agente (Windows) do Arcserve UDP para fazer backup dos dados do Microsoft SQL Server e Exchange Server.
Aviso	Não verificado porque o aplicativo não conseguiu acessar a máquina virtual. Certifique-se de que as credenciais do usuário estão corretas e têm privilégios	Forneça as credenciais de administrador de domínio ou de administrador local integrado para efetuar logon no sistema operacional convidado da máquina virtual.

	administrativos.	
Aviso	Não foi possível verificar se o backup consistente de dados é possível porque a máquina virtual não está ligada.	Consulte a coluna Estado de energia.

Como adicionar e gerenciar um caminho UNC/NFS

O caminho UNC/NFS foi introduzido como um tipo de nó no Arcserve UDP. Diferentemente de outros nós, não é possível adicionar o nó do caminho UNC/NFS a partir da seção Todos os nós. Assim como o nó do Exchange Online, é possível adicionar o nó do caminho UNC/NFS somente ao criar um plano. Depois de adicionar, é possível gerenciar o nó do caminho UNC/NFS na seção Todos os nós para atualizar ou excluir.

O que fazer a seguir?

- Adicionar um caminho UNC/NFS
- Atualizar um caminho UNC/NFS
- Excluir um caminho UNC/NFS

Adicionar um caminho UNC/NFS

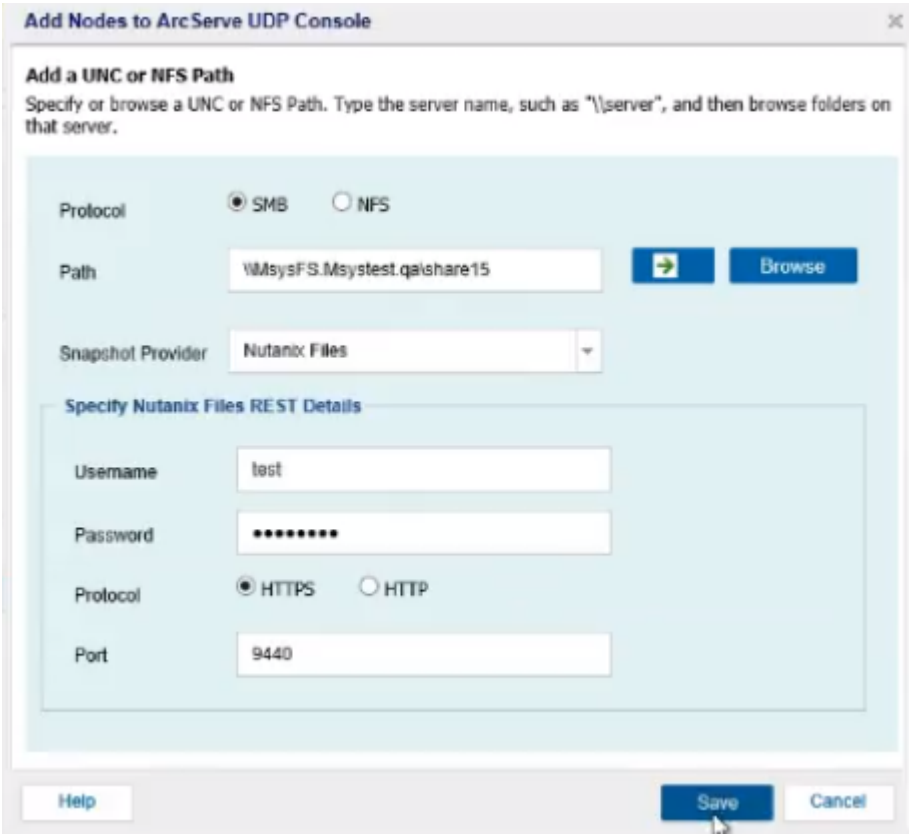
É possível adicionar um caminho UNC/NFS somente ao criar um plano de backup de caminho UNC/NFS. Ao criar o plano, na guia **Origem**, você poderá adicionar um nó de caminho UNC/NFS.

Siga estas etapas:

1. Na guia **Origem** do plano de backup de caminho UNC, clique na opção **Adicionar um caminho UNC ou NFS**.

   A caixa de diálogo Adicionar nós ao Console do Arcserve UDP será exibida.

2. Na página Adicionar um caminho UNC ou NFS, execute as seguintes etapas:



   a. Selecione **SMB** ou **NFS** como um protocolo.

      - Se você selecionar **SMB**, faça o seguinte:

        1. Digite o caminho UNC no seguinte formato:

           *Hostname**share*

           Observações:

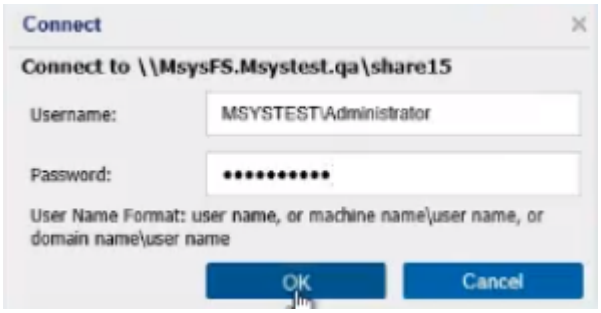
- Ao fornecer o compartilhamento de arquivos do Nutanix como origem para backup com arquivos do Nutanix como um provedor de instantâneos, os backups podem ser executados apenas no nível de compartilhamento, mas não no nível de subpasta.
- Para obter o caminho UNC, faça o seguinte:
  a. Selecione o compartilhamento recém-criado no painel central.
  b. Na coluna DETALHES DE COMPARTILHAMENTO/EXPORTAÇÃO, no painel Resumo, navegue até **Caminho de montagem** e copie o caminho de montagem.

     Se o caminho UNC for válido, uma seta para a direita e a opção Procurar serão ativadas.

2. Clique na seta à direita (>) para validar o caminho UNC.

   A caixa de diálogo Conectar é exibida.

3. Digite o nome do usuário e a senha, conforme necessário, e clique em **OK**.



   A caixa de diálogo Adicionar nós ao console do Arcserve UDP exibe o caminho UNC verificado.

- Se você selecionar NFS, faça o seguinte:

  1. Digite o caminho UNC no seguinte formato:

     *Hostname**share*

  2. Selecione a Codificação entre as opções disponíveis - ANSI, GB2312-80, KSC5601, BIG5, SHIFT-JIS, EUC-KR, EUC-TW, EUC-JP.

     O valor padrão é ANSI.

     Observação: durante o backup de uma pasta NFS compartilhada, todos os arquivos e todas as pastas com nomes que tiverem uma

codificação de idioma sem suporte serão ignorados ou seus nomes ficarão ilegíveis.

b. Na lista suspensa Provedor de instantâneo, selecione **Nutanix Files**.

c. Para a caixa Especificar detalhes de REST do Nutanix Files, especifique as seguintes credenciais:

Nome de usuário

Refere-se ao nome do usuário criado pelo usuário da API REST usando o Nutanix Prism.

Observação: para uma comunicação mais segura, selecione o protocolo HTTPS.

Senha

Refere-se à senha do nome de usuário.

Protocolo

Especifique o protocolo que deseja usar para a comunicação com o servidor de destino. As opções disponíveis são HTTP e HTTPS.

Porta

Refere-se ao número da porta. O valor da porta padrão é 9440 para acessar as chamadas de API REST e o Prism.

3. Clique em **Salvar**.

É possível atualizar ou excluir o nó do caminho UNC/NFS.

Atualizar um caminho UNC/NFS

É possível atualizar as informações relacionadas aos nós existentes. Ao modificar as credenciais do caminho UNC/NFS, será necessário atualizar o caminho UNC/NFS no Console.

Siga estas etapas:

1. Clique na guia **Recursos**.

   A página **Nós: todos os nós** é exibida.

2. No painel esquerdo, navegue até **Nós** e selecione **Caminhos UNC/NFS**.

   Os nós do caminho UNC/NFS existentes são exibidos no painel central.

3. No painel central, selecione um caminho UNC/NFS e clique em **Ações**.

   É exibida uma lista de opções.

4. Na lista, clique em **Atualizar**.

   A caixa de diálogo **Atualizar nó** é exibida.

5. Atualize os detalhes e clique em **OK**.

   As informações do nó são atualizadas.

Excluir um caminho UNC/NFS

É possível excluir um nó de caminho UNC/NFS existente na guia **Recursos**:

Siga estas etapas:

1. Clique na guia **Recursos**.

   A página **Nós: todos os nós** é exibida.

2. No painel esquerdo, navegue até **Nós** e selecione **Caminhos UNC/NFS**.

   Os nós do caminho UNC/NFS existentes são exibidos no painel central.

3. Selecione o caminho UNC/NFS desejado e clique em **Ações**.

   É exibida uma lista de opções.

4. Clique em **Excluir**.

   Uma janela de confirmação aparece.

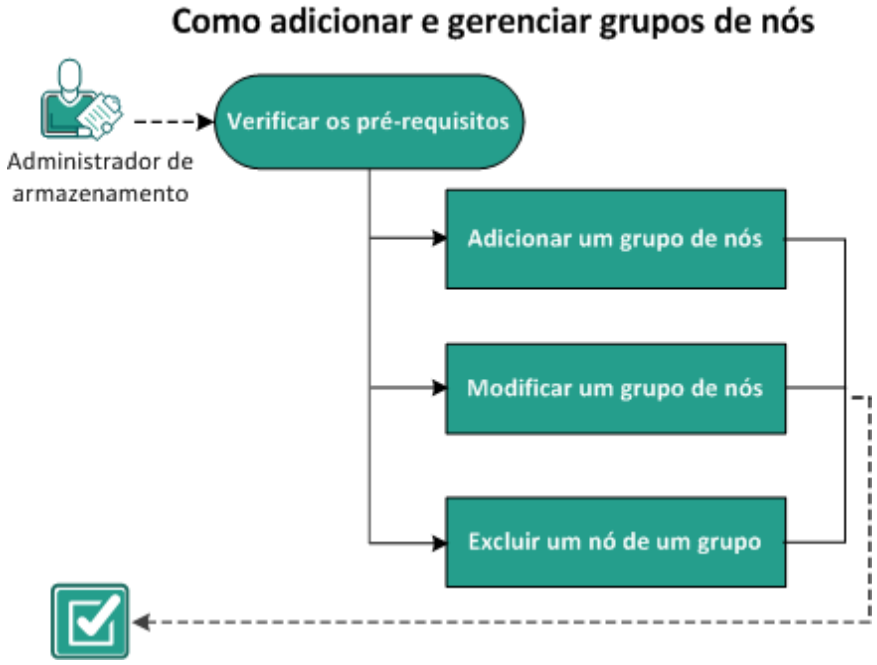
5. Clique em **OK**.

   O caminho UNC/NFS será excluído com êxito.

Como adicionar e gerenciar grupos de nós

Com o Arcserve Unified Data Protection, é possível adicionar vários nós a um grupo. É possível adicionar grupos de nós para gerenciar o seu ambiente de máquina virtual e físico.

O diagrama a seguir ilustra como adicionar e gerenciar os grupos de nós:



A solução Arcserve Unified Data Protection contém os seguintes grupos de nós:

- Grupos padrão:
  - **Todos os nós**: exibe todos os nós que são adicionados ao console.
  - **Nós sem um plano**: exibe os nós que não têm nenhum plano atribuído.

  Observação: não é possível modificar ou excluir os grupos de nós padrão.
- Grupos que são exibidos quando adiciona grupos filhos:
  - **Grupos de planos**: exibe a lista de planos criados por você. Selecione cada plano no grupo para exibir todos os nós associados a esse plano.
  - **Grupos personalizados**: exibe a lista de grupos de nós personalizados criados por você. Por exemplo, o grupo de nós que você criou clicando em **Ações**, **Grupo de nós**, **Adicionar** no painel central.
  - **Grupos do vCenter/ESX**: exibe os nós adicionados por você, usando a opção **Importando do vCenter/ESX**.
  - **Grupos de servidores de backup Linux**: exibe os nós do servidor de backup Linux.

- **Nós do Exchange Online**: exibe os nós do Exchange Online.
- **Caminhos UNC**: exibe os nós UNC.
- **Grupos de perfis de SLA**: exibe os nós relacionados a contrato de nível de serviço.
- **Grupos do Hyper-V**: exibe os nós adicionados por você usando a opção **Importando do Hyper-V**.
- **Grupos do painel global:** exibe o servidor principal de filial do Arcserve Backup sob o servidor do painel global. O grupo do painel global é exibido quando você adiciona um servidor do painel global do Arcserve Backup ao console e executa uma sincronização completa do Arcserve Backup para esse servidor.
- **Grupo de banco de dados Oracle:** exibe os nós do banco de dados Oracle.

O que fazer a seguir?

- Verificar os pré-requisitos
- Adicionar grupos de nós
- Modificar grupos de nós
- Excluir grupos de nós

Verificar os pré-requisitos

Antes de trabalhar com grupos de nós, conclua os seguintes pré-requisitos:

- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.
- Efetue logon no console.
- Adicione um nó.

Adicionar grupos de nós

Para gerenciar a lista de nós, é possível criar um grupo para os nós selecionados. Por exemplo, é possível agrupar nós por função de negócios ou por aplicativos instalados. Também é possível adicionar nós em quaisquer grupos personalizados mais tarde, depois de adicionar um grupo em branco.

Siga estas etapas:

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.

   A página **Nós: Todos os nós** é exibida.
3. No painel central, clique na lista suspensa **Ações**.
4. Clique em **Criar um grupo de nós**.

   A caixa de diálogo **Adicionar grupo** é aberta, exibindo todos os nós disponíveis.
5. Preencha as seguintes ações para adicionar nós ao grupo e clique em **OK**.
   - Selecione os nós que você deseja adicionar a um grupo.
   - Forneça um nome para o grupo.

     A caixa de diálogo **Informações** é exibida no painel direito para fornecer a mensagem informando que o grupo de nós foi criado.

   O grupo adicionado é colocado abaixo de **Grupos Personalizados** no painel esquerdo.

   Observação: as opções **Modificar** e **Excluir** são ativadas apenas quando você adiciona um grupo.

Modificar grupos de nós

Com o uso da solução Arcserve Unified Data Protection, é possível modificar os grupos de nós criados. É possível adicionar e remover nós do grupos de nós e alterar o nome do grupos de nós.

Siga estas etapas:

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.

   A página **Nós: Todos os nós** é exibida.
3. De **Grupos personalizado**s no painel à esquerda, selecione um grupo.

   Os detalhes do grupo selecionado são exibidas no painel central.
4. Clique na lista suspensa **Ações** e, em seguida, clique em **Editar esse grupo de nós**.

   A caixa de diálogo **Modificar grupo** é exibida.
5. Atualize os detalhes e clique em **OK**.

   O grupo do nó é atualizado.

Excluir grupos de nós

É possível excluir um grupo, se necessário. Quando você exclui um grupo que foi adicionado manualmente, as máquinas virtuais ou físicas não são removidas do Arcserve Unified Data Protection. No entanto, se excluir um grupo que foi criado automaticamente por uma detecção do ESX ou vCenter Server, o grupo e todas as máquinas virtuais serão excluídos do console.

Importante: Não é possível excluir os grupos de nós padrão.

Observação: o processo de exclusão dos grupos de nós não exclui os nós individuais do console.

Siga estas etapas:

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.

   A página **Nós: Todos os nós** é exibida.
3. Em **Grupos personalizados** no painel à esquerda, selecione o nome de um grupo.

   Os detalhes do grupo selecionado são exibidas no painel central.
4. Clique na lista suspensa **Ações** e, em seguida, clique em **Excluir esse grupo de nós**.

   A caixa de diálogo **Confirmar** é exibida.
5. Clique em **Sim**.

   A caixa de diálogo **Informações** é exibida no painel direito para fornecer a mensagem informando que o grupo de nós foi excluído.

Como gerenciar nós para a nuvem

Usando o Arcserve UDP, é possível executar várias ações para gerenciar um nó para a nuvem.

O que fazer a seguir?

- Baixar o ponto de recuperação a partir da nuvem
- Fazer upload do ponto de recuperação para a nuvem
- Copiar ponto de recuperação para o disco local ou compartilhamento de rede

Baixar o ponto de recuperação a partir da nuvem

Com esse recurso, é possível fazer download dos pontos de recuperação a partir da nuvem para o compartilhamento local ou de rede.

Siga estas etapas:

1. Clique na guia **Recursos**.

   A página **Nós: todos os nós** é exibida.

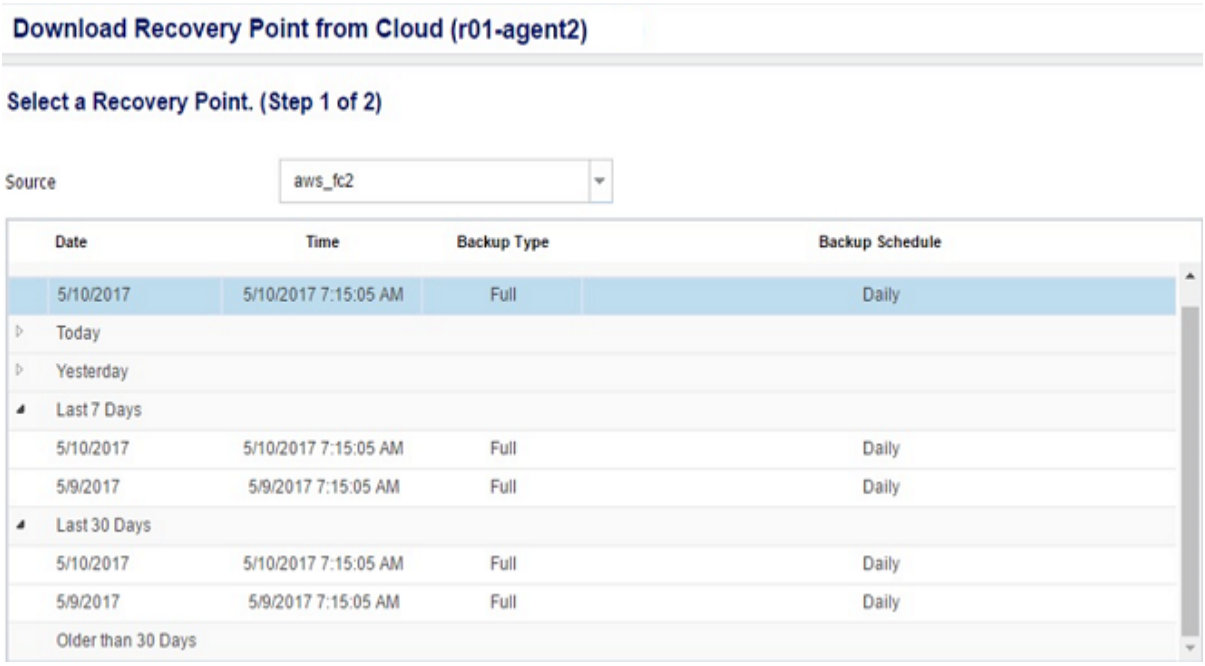
2. Execute uma das seguintes ações:

   - Clique com o botão direito do mouse no nome do nó.
   - Selecione o nome do nó e, no painel central, clique na lista suspensa **Ações**.

3. Clique em **Baixar o ponto de recuperação a partir da nuvem**.

   A página **Baixar o ponto de recuperação a partir da nuvem** é exibida.

   É possível fazer download do ponto de recuperação da nuvem em duas etapas.



4. Na etapa 1, para selecionar um ponto de recuperação, faça o seguinte e clique em **Avançar**.

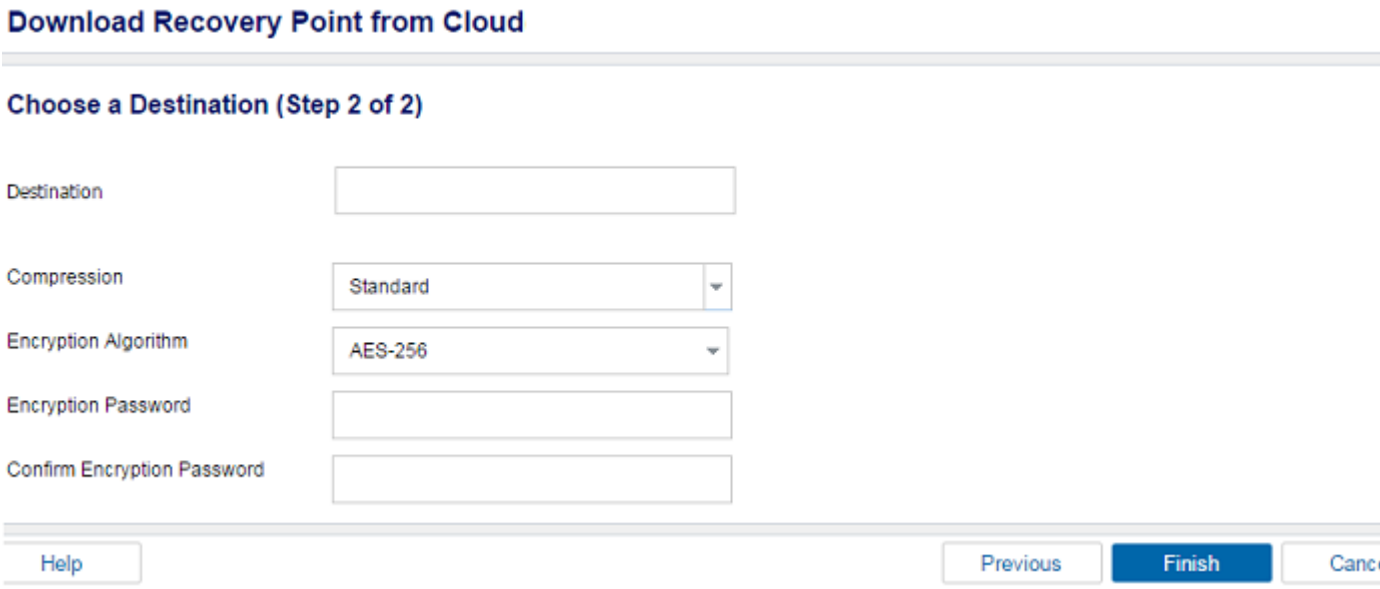
   a. Na lista suspensa Serviço de nuvem, selecione um serviço de nuvem.

   b. Na lista suspensa Armazenamento na nuvem, selecione um armazenamento na nuvem.

c. Na lista suspensa Nome do compartimento de memória, selecione um nome de compartimento de memória que contenha um ponto de recuperação.

   Os detalhes do ponto de recuperação são exibidos somente quando você configura uma tarefa CRP para o plano.

A tela Escolher um destino é exibida.



5. Na etapa 2, forneça os detalhes a seguir e clique em **Concluir**.

   a. Digite o **destino**.

      Observação: se tiver inserido um destino remoto que exige validação, ao clicar em **Concluir**, você verá a caixa de diálogo **Conectar**. Insira detalhes para validar o destino.

   b. Selecione o tipo de **Compactação.**

   c. Selecione o tipo de **Algoritmo de criptografia**.

   d. Digite a **Senha de criptografia** duas vezes.

O ponto de recuperação é obtido por download da nuvem.

Fazer upload do ponto de recuperação para a nuvem

Com esse recurso, é possível carregar pontos de recuperação de destinos de backup como compartilhamento RPS\local\remoto para a nuvem.

Importante: você precisa de um nó que tenha um plano de backup e uma sessão de backup qualificada para cópia de arquivo na nuvem.

Siga estas etapas:

1. Clique na guia **Recursos**.

   A página **Nós: todos os nós** é exibida.

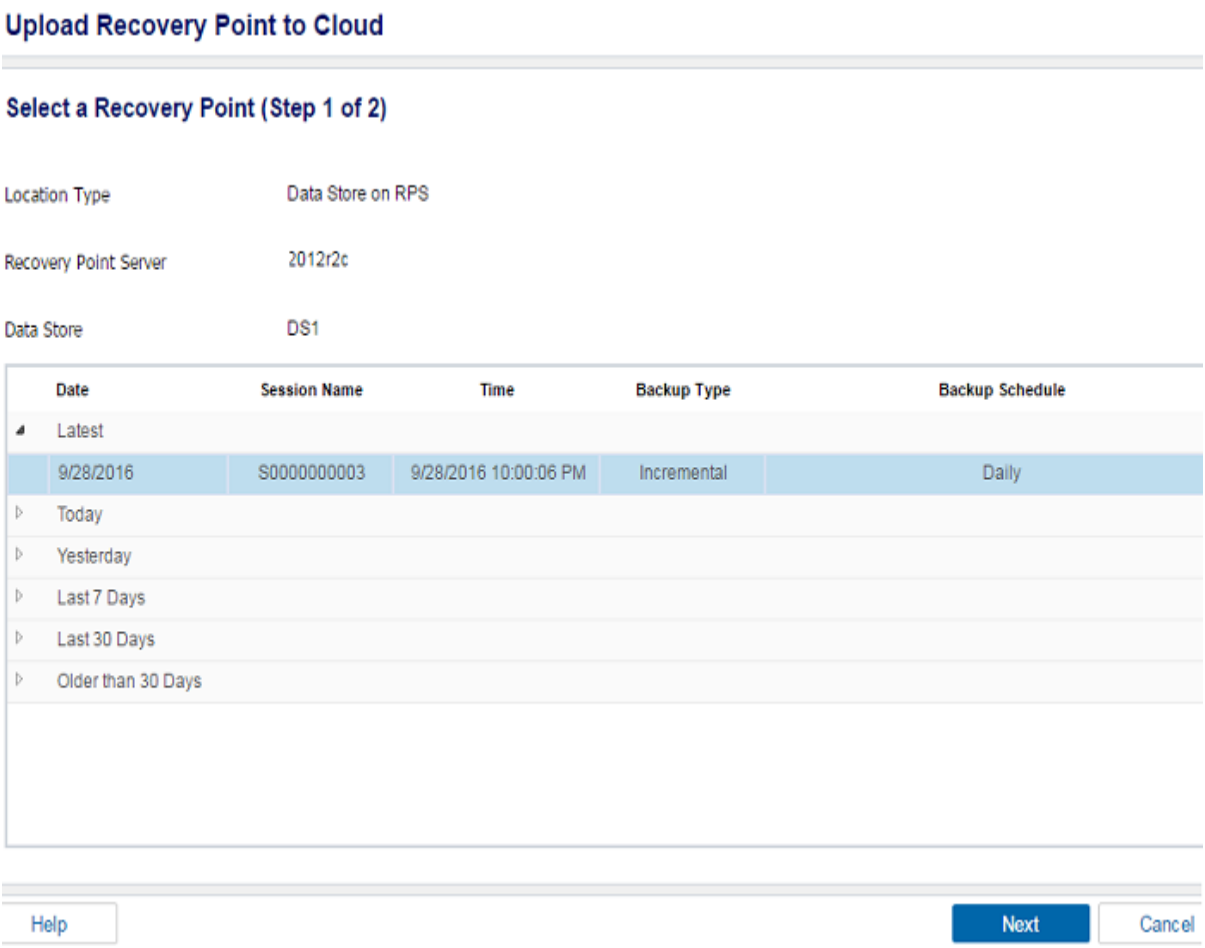
2. Execute uma das seguintes ações:

   - Clique com o botão direito do mouse no nome do nó.
   - Selecione o nome do nó e, no painel central, clique na lista suspensa **Ações**.

3. Clique em **Atualizar o ponto de recuperação para a nuvem**.

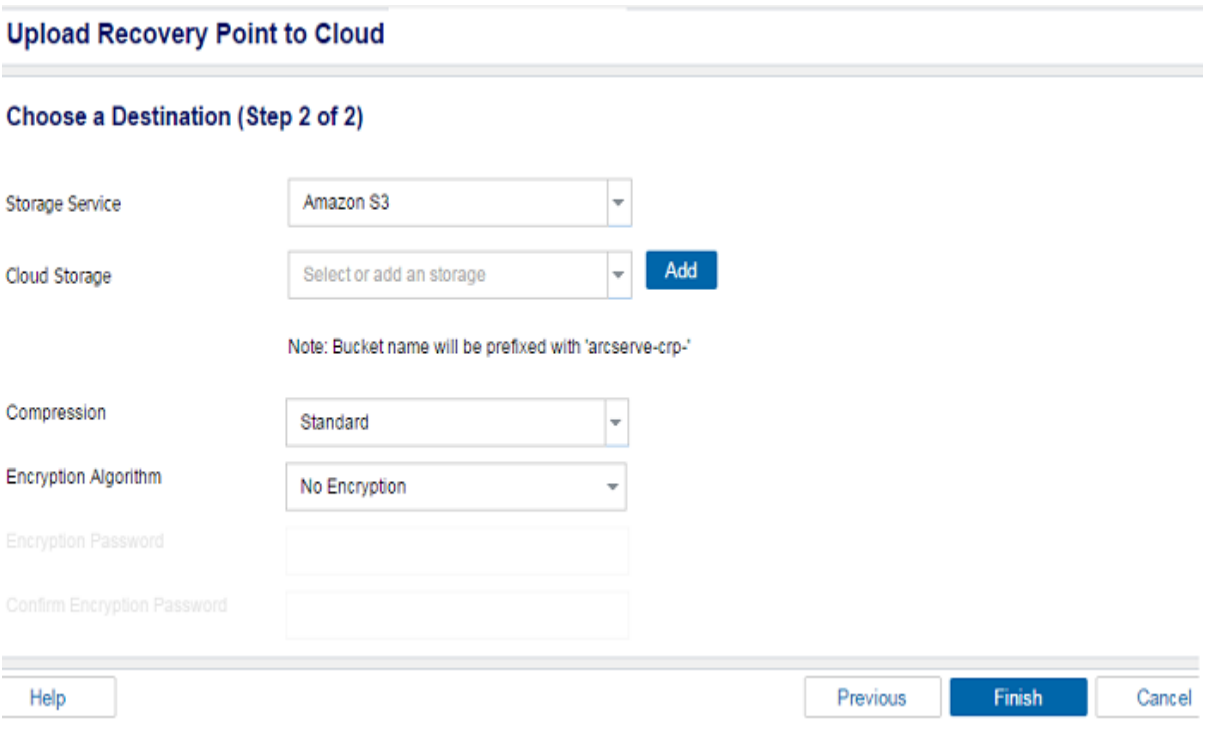
   A caixa de diálogo **Atualizar o ponto de recuperação para a nuvem** é aberta.

   Você pode carregar o ponto de recuperação na nuvem em duas etapas.



4. Na etapa 1, selecione um **Ponto de recuperação** e clique em **Avançar**.

   A próxima tela de upload é exibida.



5. Na etapa 2, forneça os detalhes a seguir e clique em **Concluir**.
   a. Selecione o **Serviço de armazenamento** na lista suspensa.
   b. Selecione o **Armazenamento na nuvem** na lista suspensa.

      Observação: se você ainda não adicionou uma conta de nuvem, clique em **Adicionar** para fazer isso.
   c. Selecione o tipo de compactação na lista suspensa.
   d. Selecione o tipo de **Algoritmo de criptografia**.
   e. Digite a **Senha de criptografia** duas vezes.

   Observação: um compartimento de memória/recipiente é criado com a convenção de nomenclatura *arcserve-{id-gerada-aleatoriamente}-<Nome do compartimento de memória>*. No entanto, cada tarefa *Fazer upload do ponto de recuperação para a nuvem* cria um novo compartimento de memória/recipiente com uma ID exclusiva *{id-gerada-aleatoriamente}*. Para obter o nome exato do compartimento de memória/recipiente, consulte o log de atividades da tarefa.

   O ponto de recuperação é carregado na nuvem.

Copiar ponto de recuperação para o disco local ou compartilhamento de rede

Com esse recurso, é possível copiar pontos de recuperação de destinos de backup como compartilhamento RPS\local\remoto para local ou remoto.

Importante: você precisa de um nó que tenha um plano de backup configurado e uma sessão de backup qualificada para copiar em compartilhamento local ou remoto.

Siga estas etapas:

1. Clique na guia **Recursos**.

   A página **Nós: todos os nós** é exibida.

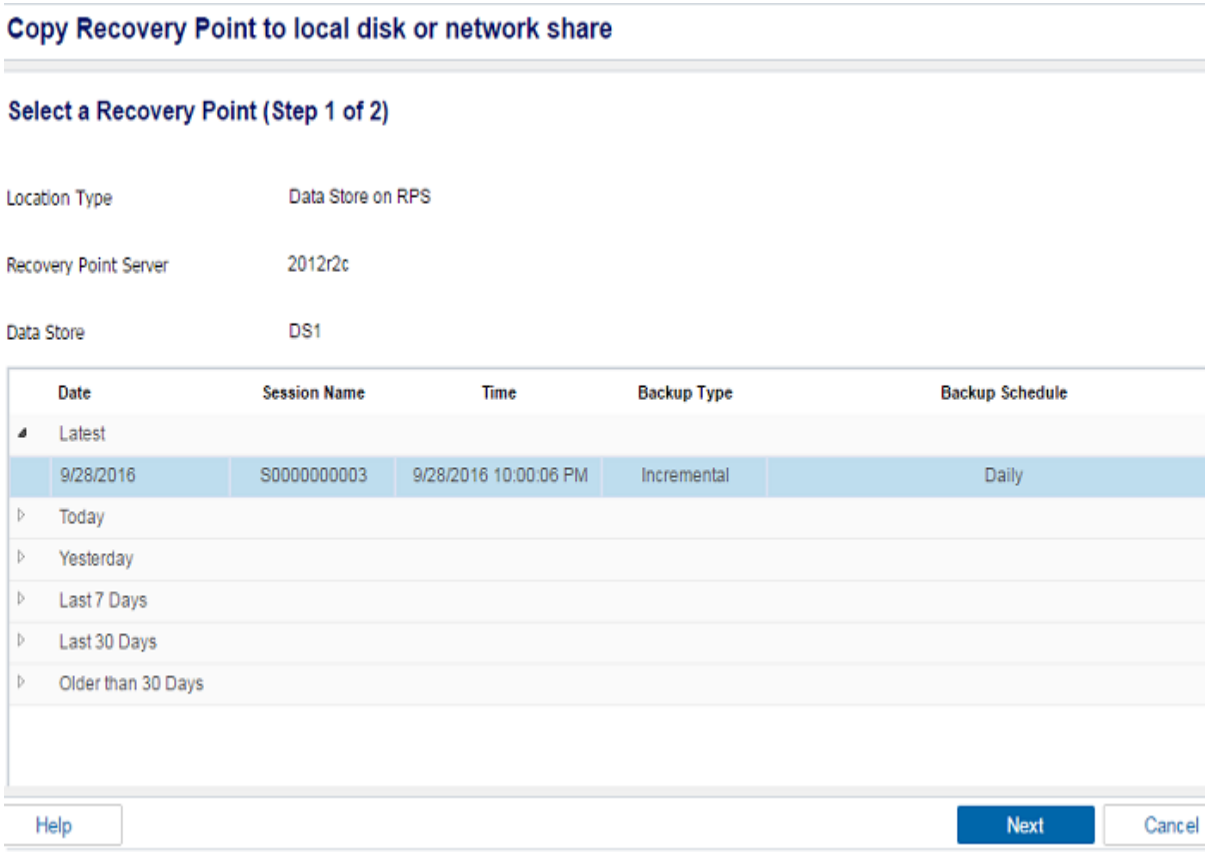
2. Execute uma das seguintes ações:

   - Clique com o botão direito do mouse no nome do nó.
   - Selecione o nome do nó e, no painel central, clique na lista suspensa **Ações**.

3. Clique em **Copiar o ponto de recuperação no compartilhamento de rede ou no disco local**.

   A caixa de diálogo **Copiar o ponto de recuperação no compartilhamento de rede ou no disco local** é aberta.

   É possível copiar o ponto de recuperação no compartilhamento de rede ou no disco local em duas etapas.



4. Na etapa 1, selecione um **Ponto de recuperação** e clique em **Avançar**.

   A próxima tela de cópia de ponto de recuperação é exibida.

5. Na etapa 2, forneça os detalhes a seguir e clique em **Concluir**.

a. Digite o **destino**.

   Observação: se tiver inserido um destino remoto que exige validação, ao clicar em **Concluir**, você verá a caixa de diálogo **Conectar**. Insira detalhes para validar o destino.

b. Selecione o tipo de **Compactação.**

c. Selecione o tipo de **Algoritmo de criptografia**.

d. Digite a **Senha de criptografia** duas vezes.

O ponto de recuperação é copiado da nuvem.

Adicionar uma matriz de armazenamento

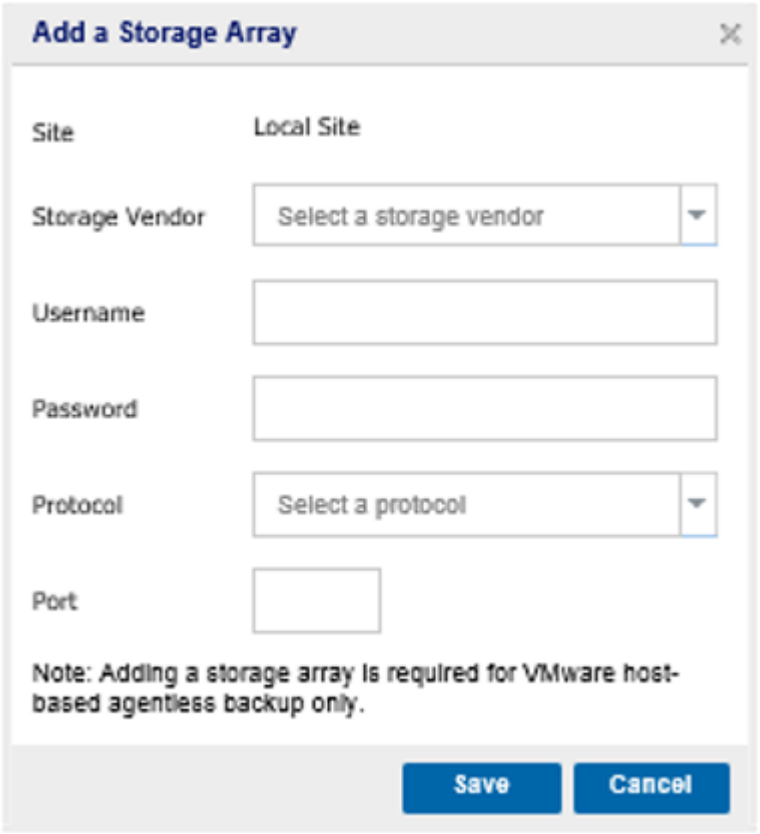
Se estiver usando instantâneos de hardware, você deve adicionar os detalhes da matriz de armazenamento ao console. Se você não adicionar a matriz de armazenamento e enviar uma tarefa de backup usando o instantâneo de hardware, a tarefa de backup primeiro procurará pelos detalhes da matriz de armazenamento no console. Quando a tarefa de backup não encontrar os detalhes da matriz de armazenamento, a tarefa usará um instantâneo de software para criar sessões de backup.

A adição de uma matriz de armazenamento é necessária somente para um backup sem agente com base em host da VMware.

Siga estas etapas:

1. No console, clique em **Recursos**.
2. Vá até **Infraestrutura** no painel esquerdo e clique em **Matrizes de armazenamento**.

   A caixa de diálogo **Adicionar uma matriz de armazenamento** abre.



   É possível adicionar um matriz de armazenamento para as seguintes opções:

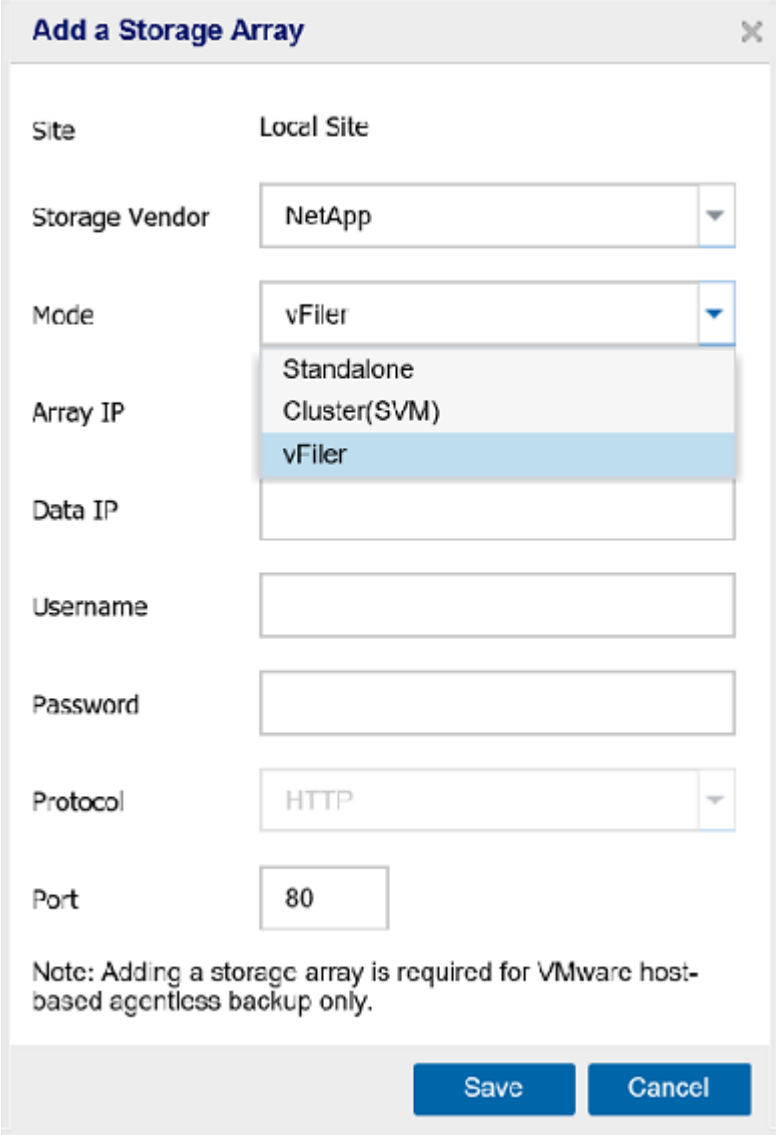
- NetApp
- HPE 3PAR
- Nimble

Adicionar uma matriz de armazenamento para o NetApp

Você pode adicionar uma matriz de armazenamento NetApp usando três opções.

Siga estas etapas:

1. Na caixa de diálogo **Adicionar uma matriz de armazenamento**, selecione NetApp no menu suspenso **Fornecedor de armazenamento**.



2. No Modo, selecione uma das seguintes opções para o tipo de matriz:

Autônomo

Especifica que a matriz de armazenamento é um dispositivo autônomo.

Agrupamento(SVM)

Especifica que a matriz de armazenamento pertence a um agrupamento de matrizes.

vFiler

Especifica que a matriz de armazenamento é um vFiler.

3. Forneça os detalhes a seguir para o tipo específico de matriz:

Instalação

Especifica o nome do site.

IP de matriz

Especifica o endereço IP da matriz. Para o modo 7, forneça o endereço IP que pode acessar a interface do iSCSI e o NFS. A VMware (ESXi) usa o endereço IP para acessar a matriz de armazenamento para operações de leitura e gravação. Para agrupamento e vFiler, forneça o endereço IP de gerenciamento da matriz de armazenamento ou o endereço IP de gerenciamento da SVM (Storage Virtual Machine – Máquina Virtual de Armazenamento).

Para localizar o endereço IP da matriz, consulte o tópico Localizar IP de dados e de matriz da matriz de armazenamento do SVM para o console do Arcserve UDP.

IP de dados

Especifica o IP de acesso a dados (interface lógica) da SVM (Storage Virtual Machine - Máquina Virtual de Armazenamento), em que as máquinas de destino (ESXi) podem acessar essa matriz de armazenamento para operações de leitura e de gravação. Essa opção aplica-se apenas para o Agrupamento e o vFiler. Se a máquina virtual de armazenamento oferece suporte apenas ao protocolo FC, digite NA.

Para localizar o endereço IP dos dados, consulte o tópico Localizar IP de dados e de matriz da matriz de armazenamento do SVM para o console do Arcserve UDP.

Nome de usuário

Especifica o nome do usuário para se conectar à matriz de armazenamento.

Senha

Especifica a senha do nome de usuário.

Protocolo

Especifica o protocolo para se conectar à matriz.

Porta

Especifica o número da porta da matriz.

Padrão: 443 (HTTPS), 80 (HTTP)

4. Clique em **Salvar**.

   A matriz de armazenamento é adicionada ao console.

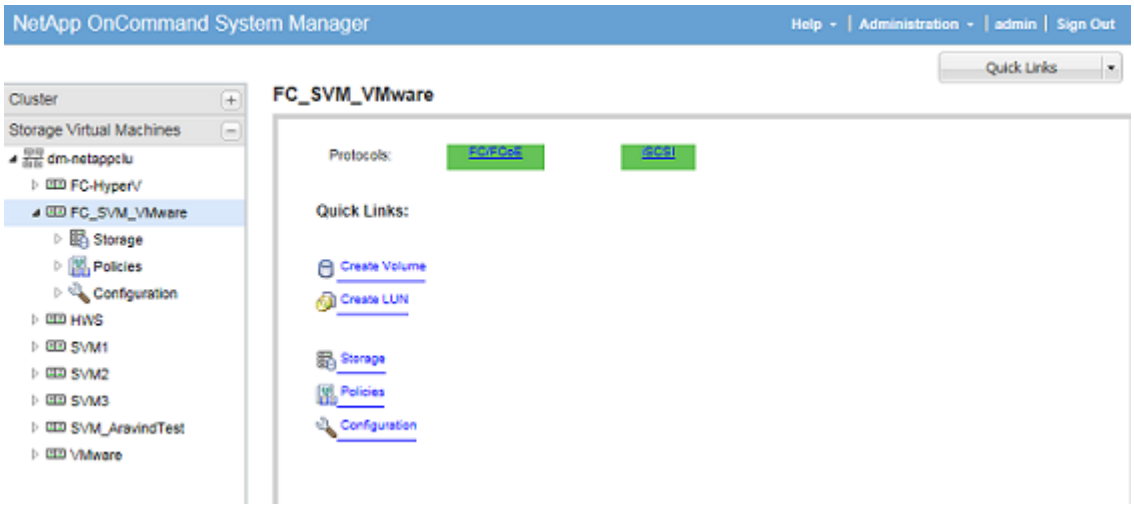
Localizar matriz e IP de dados da matriz de armazenamento do SVM para o console do Arcserve UDP

Esta seção descreve como localizar o IP de dados e de matriz quando a matriz de armazenamento do NetApp estiver em execução no modo de cDOT(agrupado).

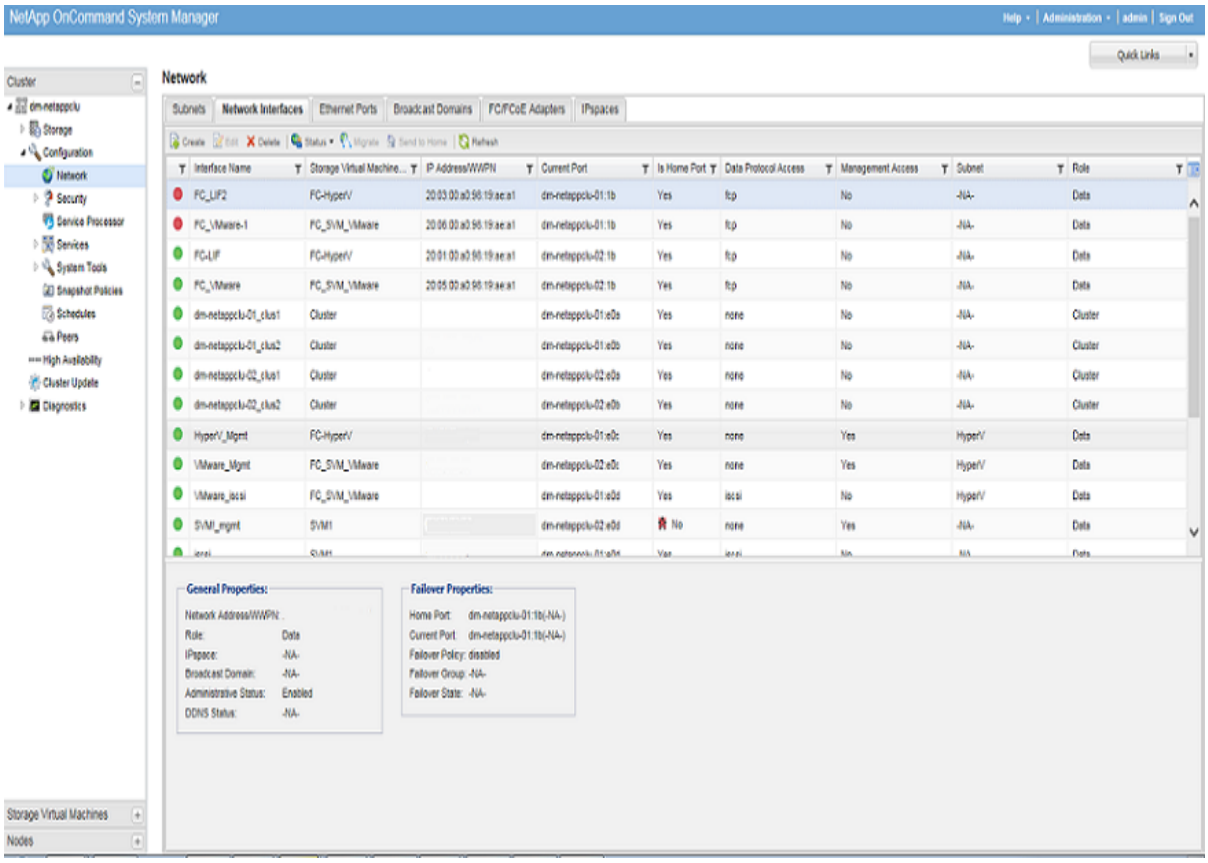
Observação: aplicável apenas ao agrupamento (SVM).

Siga estas etapas:

1. Efetue logon no gerenciador de sistema do NetApp e conecte-se ao agrupamento com credenciais válidas.
2. Identifique o SVM a ser adicionado ao console do Arcserve UDP.

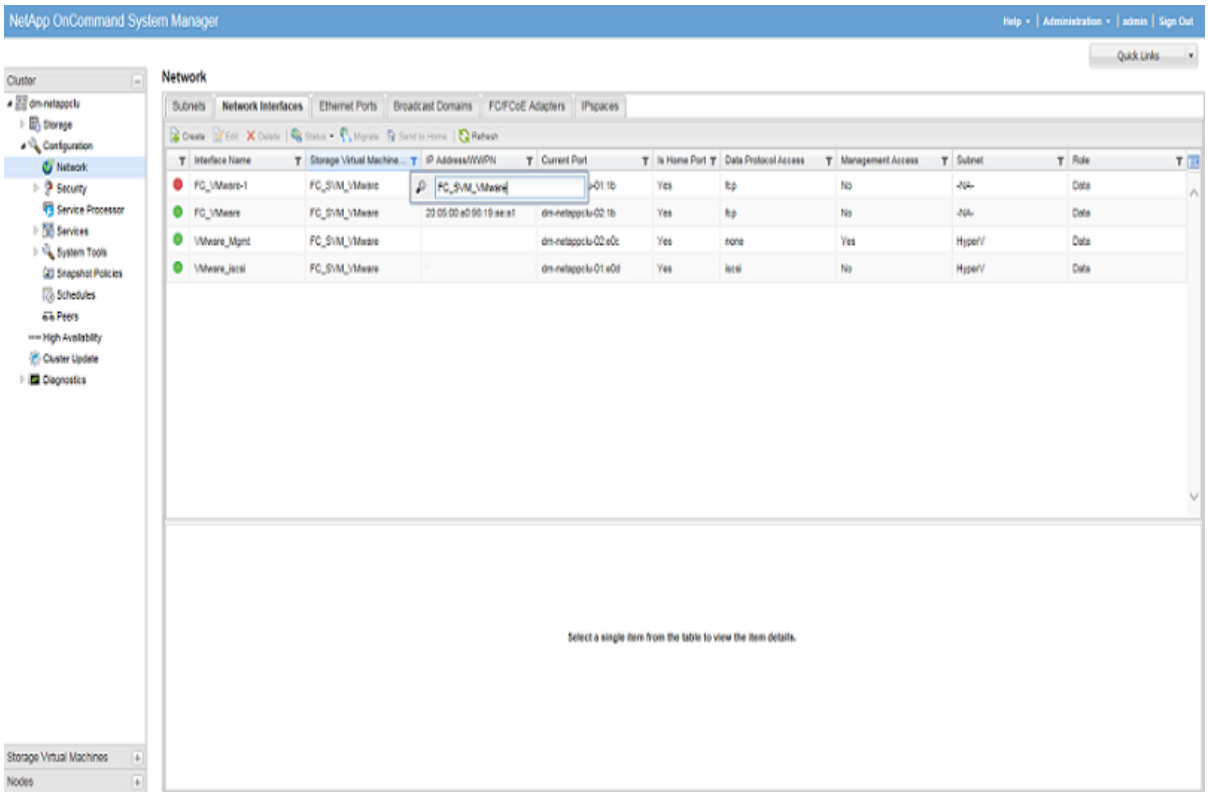


3. Altere a exibição para o cluster.
4. Em Agrupamento > Configuração, clique em Rede e abra Interfaces de rede.



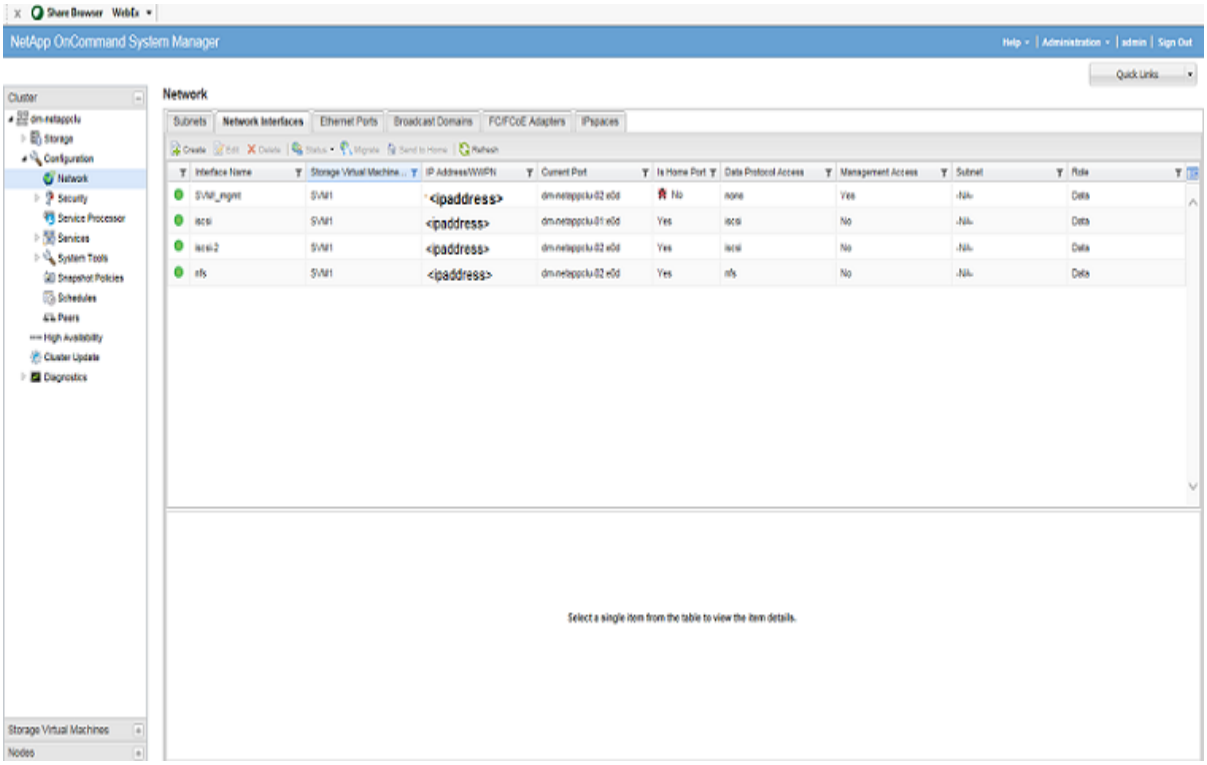
5.

6. Filtre a máquina virtual de armazenamento pelo SVM identificado.



7.

8. Descubra qual interface tem o endereço IP de acesso de gerenciamento e o endereço IP de acesso de protocolo de dados e forneça-os em Adicionar a matriz de armazenamento no Console do UDP.
    - Obter o endereço IP de acesso de gerenciamento:
        - Localize a Interface com a opção **Sim** sob a coluna **Acesso de gerenciamento**.
        - Na interface, selecione o endereço IP disponível em **Endereço IP/WWPN**.
    - Obtenha o endereço IP de acesso de protocolo de dados:
        - Localize a Interface com a opção **iSCSI** ou **NFS** sob a coluna **Protocolo de dados**.
        - Para a interface do ISCSI ou NFS, selecione o respectivo endereço IP disponível em **Endereço IP/WWPN.**



Observação: para iSCSI/NFS, o servidor ESXi deve usar o mesmo endereço IP de acesso de protocolo de dados usado para leitura e gravação na matriz de armazenamento do NetApp.

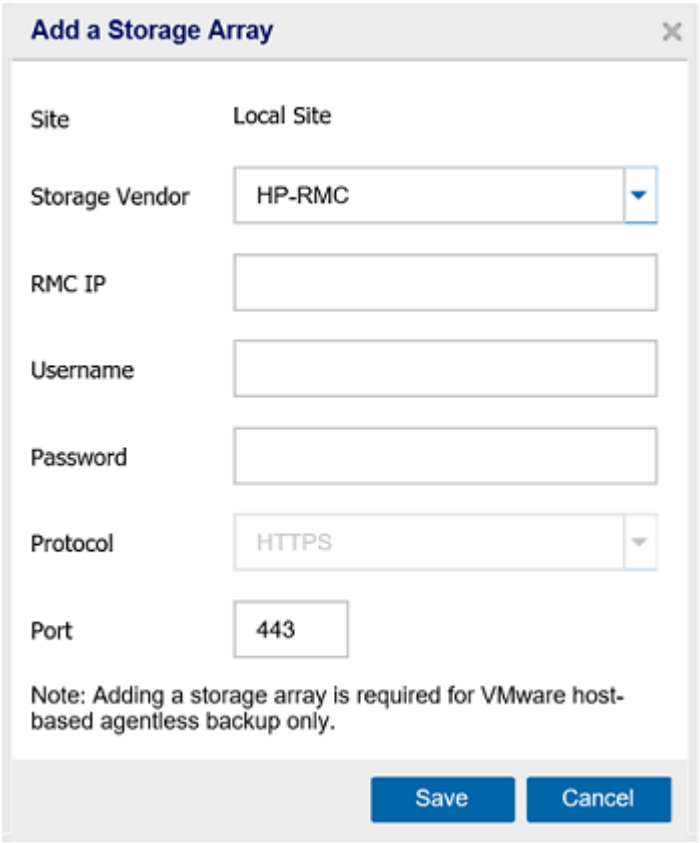
Adicionar detalhes do HPE RMC que gerencia a matriz de armazenamento de storeserve de HPE 3PAR

É possível adicionar detalhes do HPE RMC que gerencia uma matriz de storeserve de HPE 3PAR.

Importante: o storeserve de HPE 3PAR deve ser gerenciado pelo HP RMC.

Siga estas etapas:

1. na caixa de diálogo **Adicionar uma matriz de armazenamento**, selecione HP-RMC no menu suspenso **Fornecedor de armazenamento**.



2. Forneça os detalhes a seguir:

IP de RMC

Especifica o endereço IP de gerenciamento de HPE RMC.

Nome de usuário

Especifica o nome do usuário para se conectar à matriz de armazenamento.

Senha

Especifica a senha do nome de usuário.

Protocolo

Especifica o protocolo para se conectar à matriz.

Observação: só há suporte a HTTPS.

Porta

Especifica o número da porta da matriz.

Padrão: 443

3. Clique em **Salvar**.

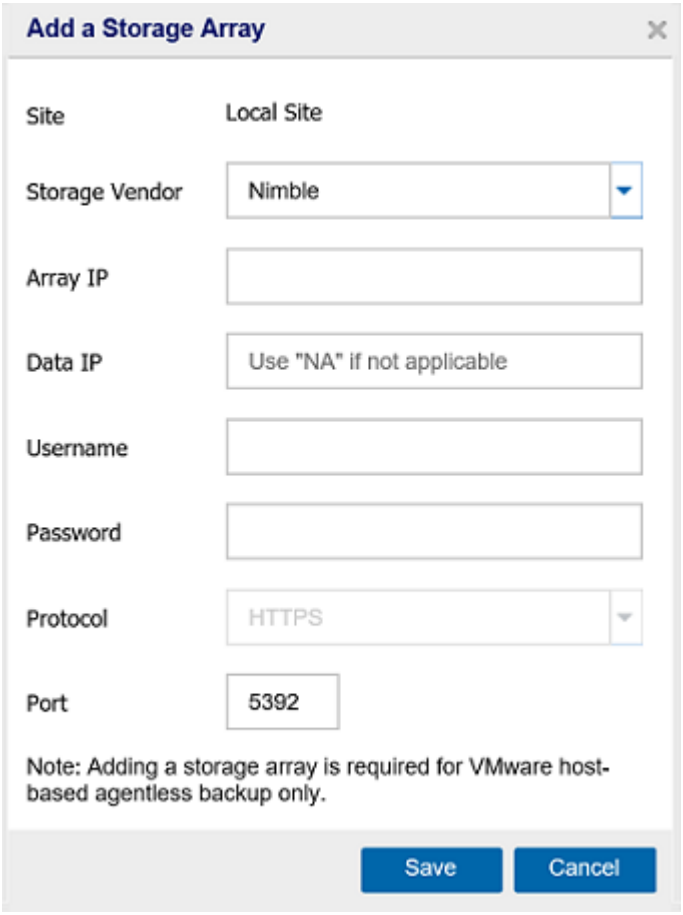
A matriz de armazenamento é adicionada ao console.

Adicionar uma matriz de armazenamento Nimble

É possível adicionar uma matriz de armazenamento Nimble.

Siga estas etapas:

1. Na caixa de diálogo **Adicionar uma matriz de armazenamento**, selecione Nimble no menu suspenso **Fornecedor de armazenamento**.



2. Forneça os detalhes a seguir para o tipo específico de matriz:

IP de matriz

Especifica o endereço IP da matriz. Digite o endereço IP de gerenciamento da matriz de armazenamento Nimble.

IP de dados

Especifica o IP de acesso a dados (interface lógica) da matriz de armazenamento Nimble, em que as máquinas de destino (ESXi) podem acessar essa matriz de armazenamento para operações de leitura e de gravação. Se a matriz de armazenamento Nimble oferece suporte apenas ao protocolo FC, digite NA.

Nome de usuário

Especifica o nome do usuário para se conectar à matriz de armazenamento.

Senha

Especifica a senha do nome de usuário.

Protocolo

Especifica o protocolo para se conectar à matriz.

Observação: só há suporte a HTTPS.

Porta

Especifica o número da porta da matriz.

Padrão: 5392

3. Clique em **Salvar**.

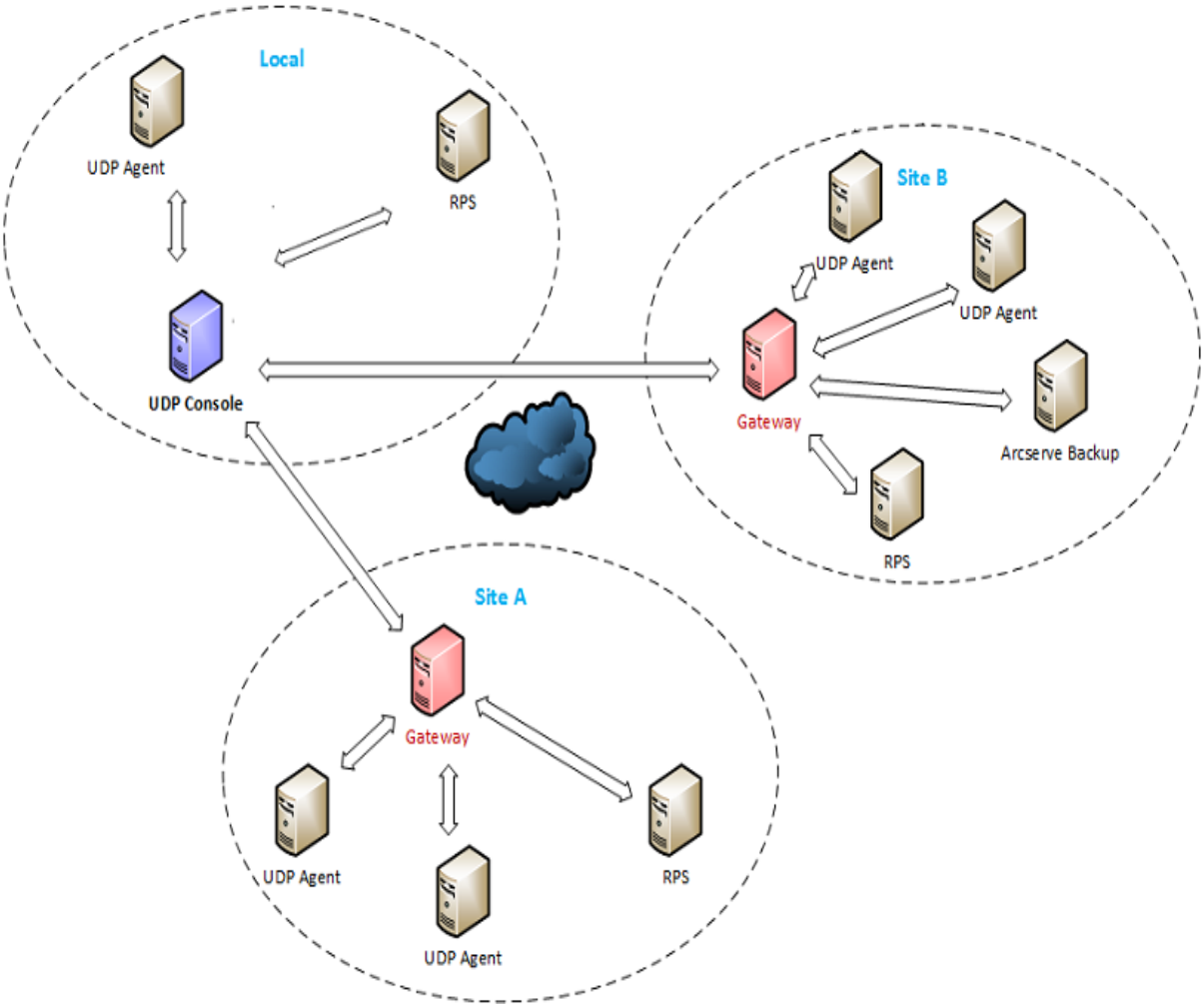
A matriz de armazenamento é adicionada ao console.

Como adicionar e gerenciar um site

O Console do Arcserve UDP pode gerenciar nós remotos e servidores de ponto de recuperação a partir de outra sub-rede em uma WAN. O servidor e os nós remotos em um site interagem com o console usando um gateway. O gateway é instalado nos sites. Embora diretamente o Console não possa conectar os nós remotos, o Arcserve UDP usa o gateway para estabelecer uma conexão entre os nós e o Console.

Importante: Se os pontos de recuperação estiverem em um local remoto, para restaurar dados, o Console deve se conectar ao site remoto usando uma conexão VPN.

O diagrama a seguir mostra a conexão entre o local e os sites.



Depois de adicionar um site, você pode modificar, atualizar ou excluir sites do console. Além disso, é possível gerenciar os nós remotos no Console.

Especificar o nome do site

A página Nome do site permite especificar um nome para o site e selecionar um intervalo de sinal de monitoramento. Esse nome de local é exibido no console.

Siga estas etapas:

1. Clique na guia **Recursos** no Console.
2. No painel à esquerda, navegue até **Infraestruturas** e clique em**Sites**.

   A página Infraestrutura: Sites é aberta no painel central.
3. Clique em **Adicionar um site**.

   O assistente **Adicionar um site** é aberto.
4. Forneça os seguintes detalhes na página do site:

   Nome do site

   Forneça um nome para o site.

   Intervalo de sinal de monitoramento

   Selecione um intervalo de tempo para o sinal de monitoramento na lista suspensa. Os sinais de monitoramento verificarão a conexão entre o console e o site no intervalo especificado.

   URL de conexão do console do UDP

   Especifica o URL do console remoto do UDP. O servidor de gateway conecta-se a esse URL.

   Lembre-se do URL de conexão do Console UDP

   Selecione essa caixa de seleção para lembrar o URL do Console.
5. Clique em **Avançar**.

   A página de instruções de instalação de Gateway de gerenciamento remoto do Arcserve é exibida.

   Você especificou o nome do site remoto.

Compartilhar instruções de registro

Compartilhar instruções de registro inclui as informações para o download e a instalação do gateway. As instruções de download são enviadas para o administrador remoto. O administrador remoto precisa usar as informações de download para o download e a instalação do gateway.

Siga estas etapas:

1. Copie as instruções e salve-o para sua referência.

   Se você não tiver configurado o email do Arcserve UDP, envie as instruções copiadas para o administrador remoto a partir de outro servidor de email.

2. Selecione **Enviar instruções usando o email do Arcserve UDP** e forneça o endereço de email do administrador remoto.

3. Clique em **Avançar**

   A página **Confirmação** será aberta.

   Você compartilhou as instruções de registro com êxito.

Verificar e adicionar o site

Verifique os detalhes antes de adicionar o site. Você pode clicar em **Voltar** para visitar páginas anteriores.

Siga estas etapas:

1. Verifique os detalhes na página de confirmação.

   Se necessário, você pode modificar as informações das páginas anteriores.

2. Clique em **Concluir**.

   O assistente é fechado.

   O site remoto é criado na página **Infraestrutura: sites**.

   Quando o administrador remoto instala o Gateway de Gerenciamento Remoto da Arcserve e fornece com êxito o código de autorização do gateway, aparece uma marca de seleção verde ao lado do nome do site no Console.

   Você adicionou um site com êxito.

Modificar o URL do Console

Quando você altera o URL do Console, o gateway deve ser registrado novamente para gerenciar o site no Console. O registro do gateway é executado pelo administrador remoto. Quando você atualiza o URL do Console, o Arcserve UDP envia um email para o administrador remoto com instruções detalhadas sobre como registrar o gateway do Console.

Siga estas etapas:

1. No console, clique em **Recursos**.
2. Vá para **Infraestrutura** no painel esquerdo e clique em **Sites**.

   A página **Infraestrutura: sites** é aberta no painel central.
3. Selecione o site e clique em **Ações**, **Atualizar URL do console**.

   A caixa de diálogo **Atualizar URL do console** é aberta.
4. Especifique o novo URL do console.
5. Clique em **Enviar**.

   Um email é enviado ao administrador remoto. Quando o administrador remoto atualiza o novo URL no servidor de gateway, o console exibe uma marca de seleção verde ao lado do site atualizado.

   Você modificou o URL do Console com êxito.

Modificar o site

É possível modificar o site para alterar qualquer um dos parâmetros do site adicionado. Por exemplo, é possível renomear o site ou alterar o intervalo do sinal de monitoramento.

Siga estas etapas:

1. No console, clique em **Recursos**.
2. Vá para **Infraestrutura** no painel esquerdo e clique em **Sites**.

   A página **Infraestrutura: Site** é exibida no painel central.
3. Selecione o local e clique em **Ações**, **Modificar**.

   O assistente **Modificar um site** é aberto.
4. Use **Anterior** e **Próxima** para visitar todas as páginas e modifique qualquer parâmetro.
5. Clique em **Concluir**.

   O assistente **Modificar um site** é fechado.

   Você modificou o site com êxito.

Excluir um site

É possível excluir um site que você não deseja gerenciar. Antes de excluir um site, todos os nós e filtros de detecção de nó relacionados a esse site devem ser excluídos primeiro.

Siga estas etapas:

1. No console, clique em **Recursos**.
2. Vá para **Infraestrutura** no painel esquerdo e clique em **Sites**.

   A página **Infraestrutura: Site** é exibida no painel central.
3. Selecione o site e clique em **Ações**, Excluir.

   A caixa de diálogo **Confirmar** é exibida.
4. Clique em **Sim**.

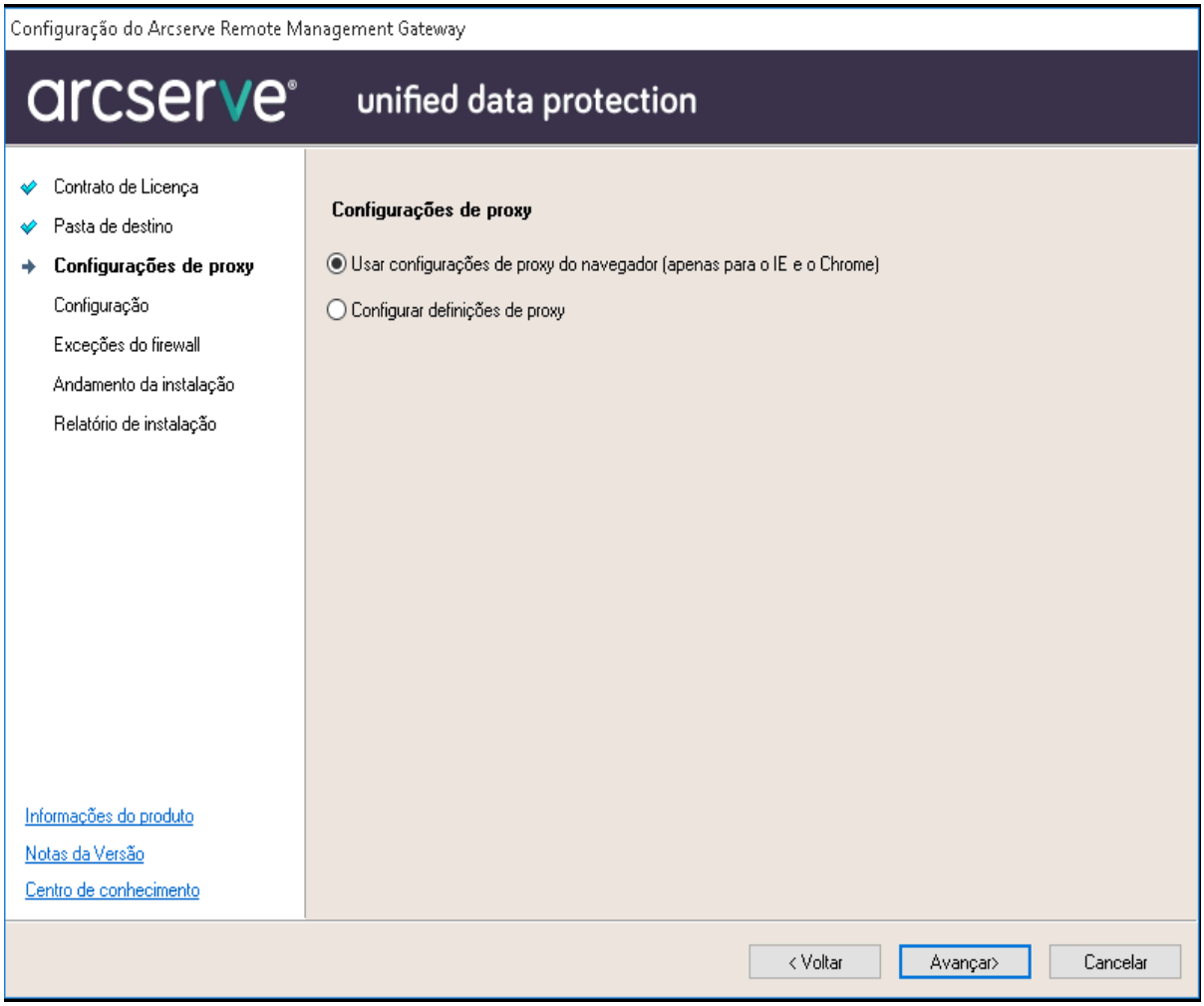
   O site é excluído.

Configurar um servidor proxy para o gateway

O Arcserve UDP oferece suporte à instalação de um servidor proxy no computador do gateway. O gateway usará esta configuração de proxy para comunicar-se com seu console registrado.

Siga estas etapas:

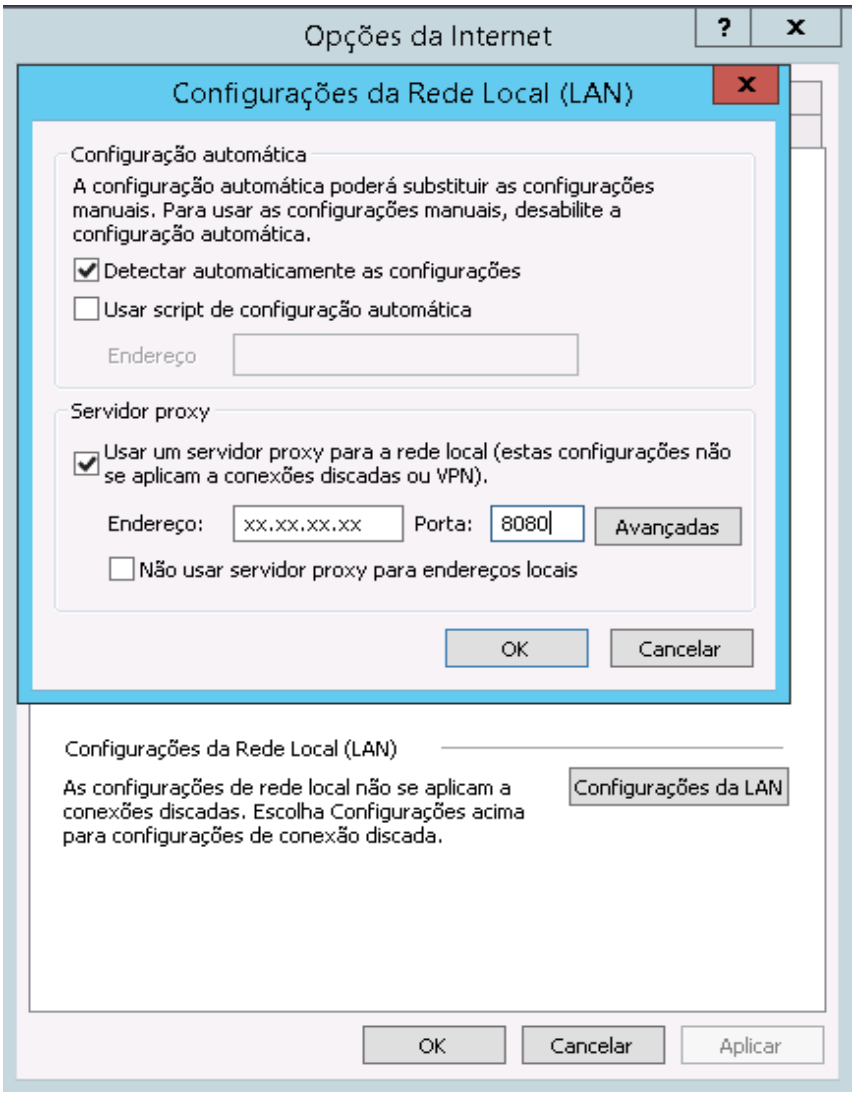
1. Abra o Assistente para configuração de Gateway do gerenciamento remoto do Arcserve.



2. Na caixa de diálogo Configurações do proxy, selecione uma das duas seguintes opções:

   Usar configurações de proxy do navegador (somente para IE e Chrome)

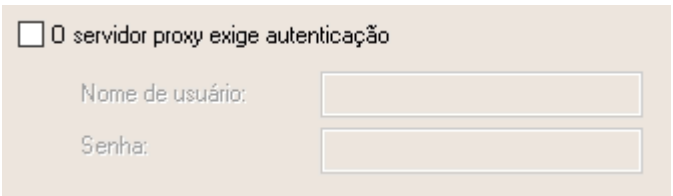
Especifica o uso das configurações de proxy do navegador. É necessário atualizar as configurações de proxy do navegador. Abra o navegador e clique em **Opções Conexão Configuração de LAN**.



Definir configurações de proxy

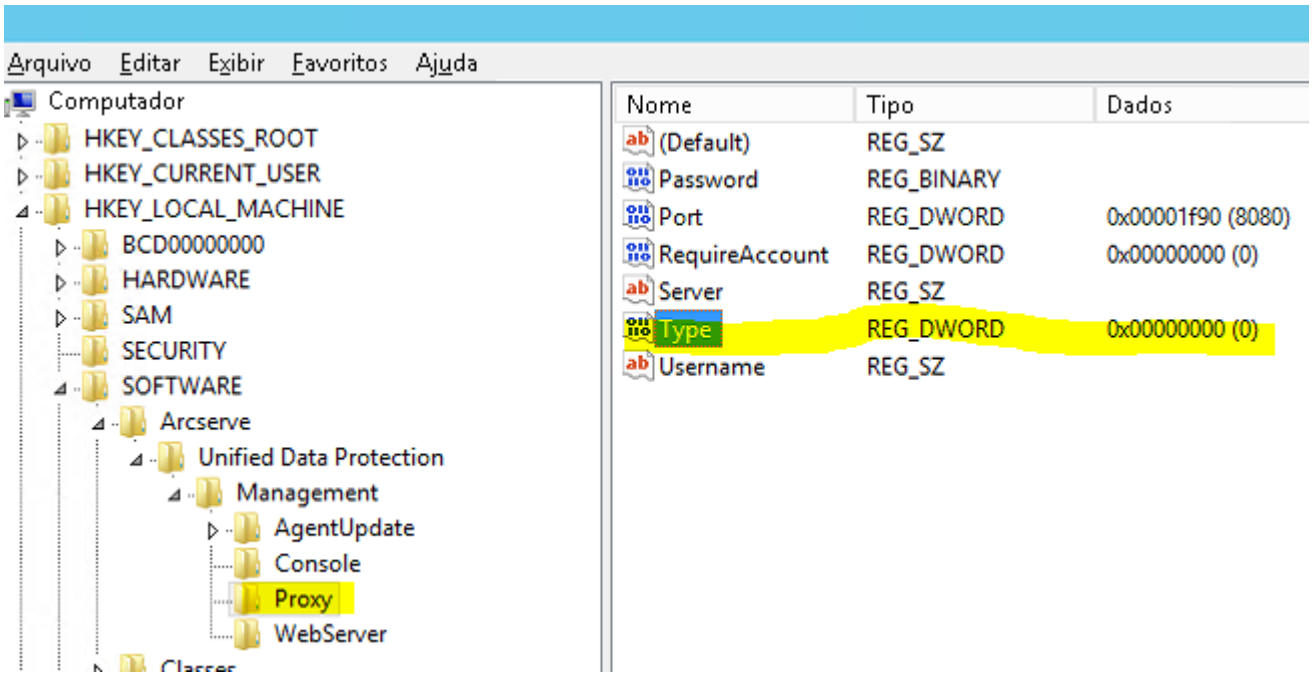
Especifica que você precisa fornecer os detalhes do servidor proxy na página do assistente.

3. Se o proxy não oferecer suporte a credenciais, desmarque a caixa de seleção de autenticação.



O servidor proxy é configurado para o gateway.

4. Para verificar a configuração de proxy, abra o regedit e vá para Proxy.



No campo Tipo, 0 indica as configurações do navegador e 1 indica outras configurações.

Observação: use o regedit para modificar as configurações de proxy, como: porta, endereço IP do servidor ou tipo.

Como gerenciar nós do Exchange Online

Não é possível adicionar os nós do Exchange Online diretamente à exibição de todos os nós. Após a adição ao plano de backup, o nó Exchange Online é adicionado à exibição de todos os nós.

É possível executar as seguintes tarefas:

1. Adicionar um nó do Microsoft Exchange Online
2. Atualizar um nó do Microsoft Exchange Online
3. Excluir um nó do Microsoft Exchange Online
4. Oferecer suporte a uma caixa de correio de pasta pública para a proteção do Exchange Online

Adicionar um nó do Microsoft Exchange Online

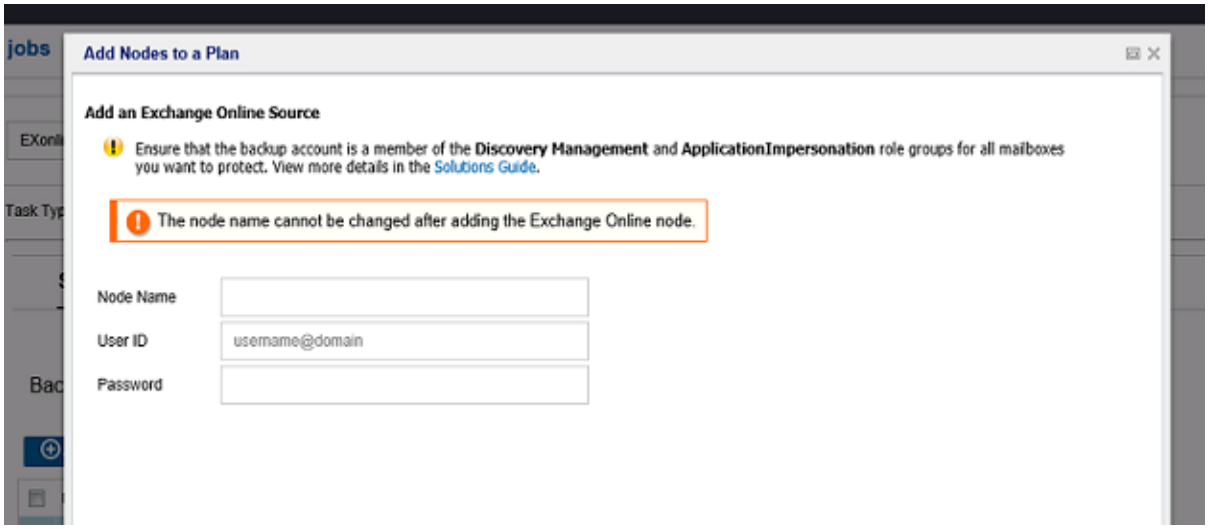
Observação: diferentemente de outros nós, não é possível adicionar o nó do Exchange Online na página Todos os nós. Os nós do Exchange Online são adicionados somente durante a criação ou modificação de um plano.

Para obter informações sobre como criar um plano, consulte Como criar um plano do Microsoft Exchange Online.

Siga estas etapas:

1. Digite o nome de usuário da conta de backup do Exchange Online que atenda aos pré-requisitos em Nome de usuário ou conta de usuário do nó do Exchange Online.

   Vários nós do Exchange Online podem usar a mesma conta de usuário (conta de serviço) do Exchange Online. Para adicionar um nó do Exchange por plano, especifique o nome do nó, o nome de usuário e a senha. Depois que o nó é criado, não é mais possível alterar o nome dele.



   Observação: a atualização/alteração da conta de usuário pode mudar o número de caixas de correio protegidas. Verifique se a conta de serviço nova/atualizada tem direitos de representação para as caixas de correio serem protegidas.

2. Digite a senha e clique em **Conectar**.
3. Selecione as contas do Exchange Online que você deseja proteger e clique na seta para a direita (>) a fim de movê-las para a lista protegida.

   Observação: marque a caixa de seleção referente à proteção de todas as origens do Exchange do Office 365 se deseja proteger todas as contas do Exchange Online em todas as páginas. Para adicionar à lista protegida todas as contas do Exchange Online listadas na página, clique na seta para a direita (>).

4. Clique em **Salvar**.

   Na opção Selecione as pastas a serem excluídas do backup, na guia Origem, você pode selecionar a(s) pasta(s) que você não deseja fazer backup.

   As contas selecionadas do Exchange Online são adicionadas.

Atualizar um nó do Microsoft Exchange Online

Ao modificar as credenciais do nó do Exchange Online, atualize esse nó no console.

Siga estas etapas:

1. Clique na guia de **recursos** no Console.
2. No painel à esquerda, navegue para **Nós** e clique em **Nós do Exchange Online**.

   Os nós do Exchange Online criados são exibidos no painel central.
3. Selecione o nó do Exchange Online e clique em **Ações**.
4. Clique em **Atualizar**.

   A caixa de diálogo **Atualizar nó** aparece.
5. Modifique os detalhes conforme desejado, e clique em **OK**.

   O nó do Exchange Online é atualizado.

Excluir um nó do Microsoft Exchange Online

Exclua os nós do Exchange Online que não são mais necessários.

Siga estas etapas:

1. Clique na guia de **recursos** no Console.
2. Vá até **Nós** e clique em **Nós do Exchange Online**.

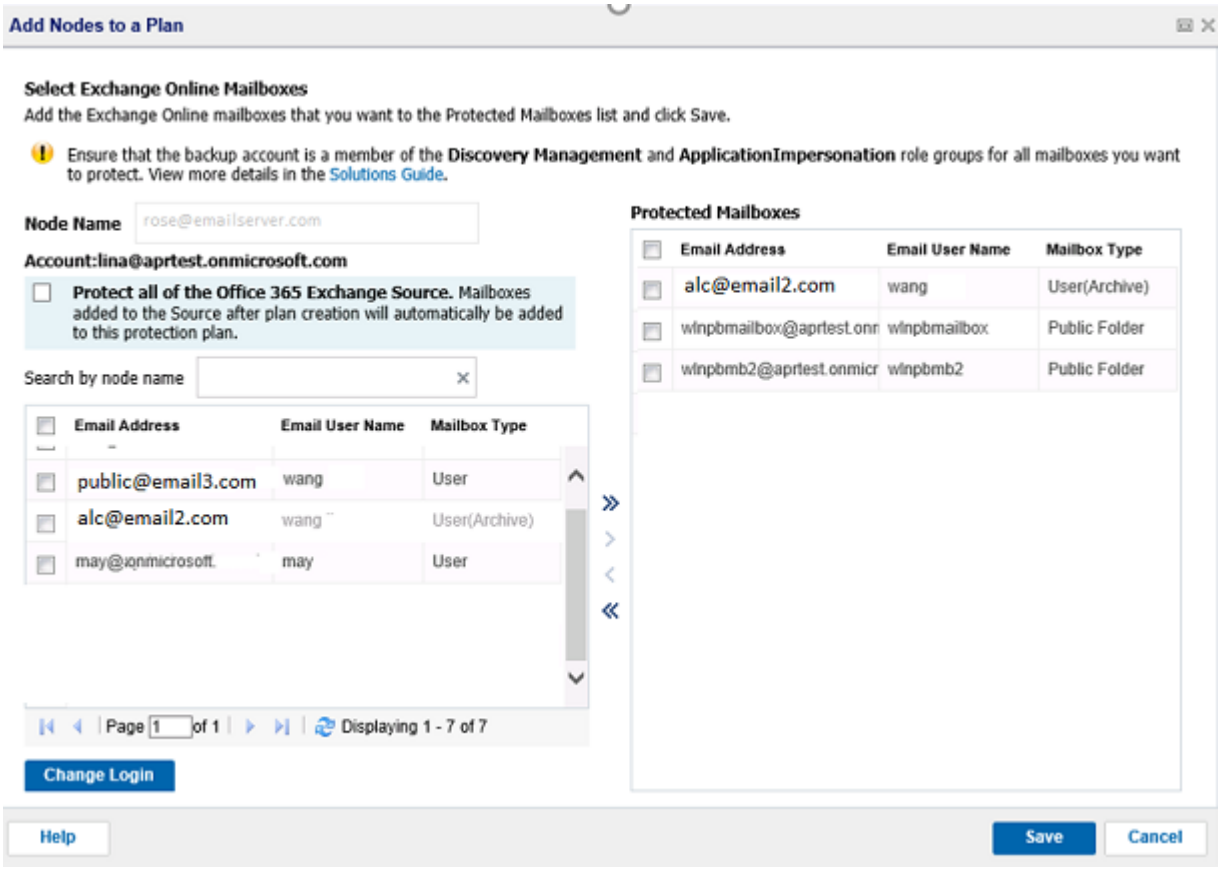
   Os nós do Exchange Online criados são exibidos no painel central.
3. Selecione o nó do Exchange Online e clique em **Ações**.
4. Clique em **Excluir**.

   Uma janela de confirmação aparece.
5. Clique em **OK**.

   O nó Exchange Online é excluído com êxito.

Oferecer suporte a uma caixa de correio de pasta pública para a proteção do Exchange Online

Ao adicionar o nó do Exchange Online, você pode ver a coluna Tipo de caixa de correio na janela **Adicionar nós a um plano**. A caixa de correio de pasta pública é exibida nessa janela e, na coluna, é exibido o tipo **Pasta pública**. Para proteger a pasta pública, adicione a caixa de correio pública correspondente a **Caixas de correio protegidas** e salve o plano.



Observação: clique no link 1 para obter mais informações sobre caixas de correio de pasta pública no Exchange Online e no link 2 para obter informações sobre permissões de pasta pública.

Como gerenciar nós do SharePoint Online

Não é possível adicionar os nós do SharePoint Online diretamente à exibição de todos os nós. Após a adição ao plano de backup, o nó do SharePoint Online é adicionado à exibição de todos os nós.

É possível executar as seguintes tarefas:

1. Adicionar um nó do SharePoint Online
2. Atualizar um nó do SharePoint Online
3. Excluir um nó do SharePoint Online

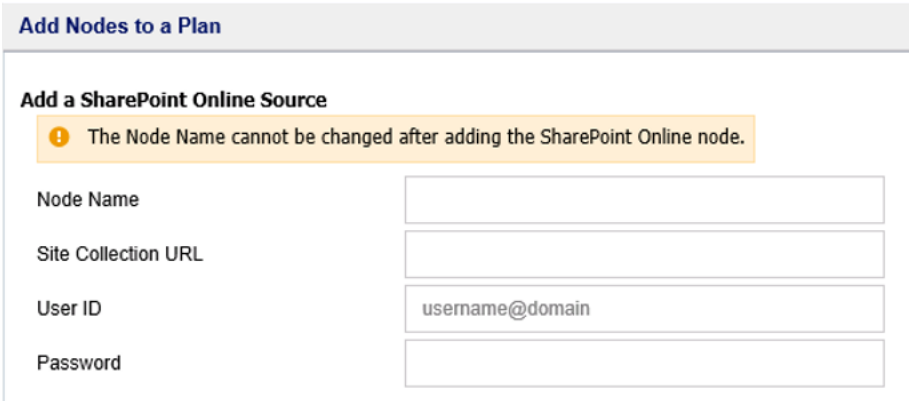
Adicionar um nó do SharePoint Online

Observação: diferentemente de outros nós, não é possível adicionar o nó do SharePoint Online na página Todos os nós. Um nó do SharePoint Online é adicionado somente em um plano durante a criação ou modificação de um plano.

Para obter informações sobre como criar um plano, consulte Como criar um plano do SharePoint Online.

Siga estas etapas:

1. Digite o nome de usuário do nó do SharePoint e digite o URL da coleção de sites, o nome de usuário e a senha do proprietário do site.



2. Digite a senha e clique em **Conectar**.
3. Selecione a lista/biblioteca ou os itens de lista do SharePoint a serem protegidos.
4. Clique em **Salvar**.

   As contas selecionadas do SharePoint Online são adicionadas.

Atualizar um nó do SharePoint Online

Ao modificar as credenciais do nó do SharePoint Online, atualize esse nó no console.

Siga estas etapas:

1. Clique na guia **Recursos** no Console.
2. No painel à esquerda, navegue para **Nós** e clique em **Nós do SharePoint Online**.

   Os nós do SharePoint Online criados são exibidos no painel central.
3. Selecione o nó do SharePoint Online e clique em **Ações**.
4. Clique em **Atualizar**.

   A caixa de diálogo **Atualizar nó** aparece.
5. Modifique os detalhes conforme desejado, e clique em **OK**.

   O nó do SharePoint Online é atualizado.

Excluir um nó do SharePoint Online

Exclua os nós do SharePoint Online que não são mais necessários.

Siga estas etapas:

1. Clique na guia **Recursos** no Console.
2. Vá até **Nós** e clique em **Nós do SharePoint Online**.

   Os nós do SharePoint Online criados são exibidos no painel central.
3. Selecione o nó do SharePoint Online e clique em **Ações**.
4. Clique em **Excluir**.

   Uma janela de confirmação aparece.
5. Clique em **OK**.

   O nó do SharePoint Online é excluído com êxito.

Como gerenciar o nó do OneDrive gere

Não é possível adicionar os nós do OneDrive diretamente à exibição de todos os nós. Após a adição ao plano de backup, o nó do OneDrive é diretamente adicionado à exibição de todos os nós.

É possível executar as seguintes tarefas:

1. Adicionar um nó do OneDrive
2. **Excluir o nó:** usando a opção Ações no nó do OneDrive, clique em **Excluir** e confirme no pop-up para excluir o nó do console.
3. **Exportar o nó:** usando a opção Ações no nó do OneDrive, clique em **Exportar** e receba o nó como um arquivo zip.
4. **Modificar o plano:** usando a opção Ações no nó do OneDrive, clique em **Modificar plano** para abrir o plano relacionado e atualizá-lo conforme o necessário.
5. **Efetuar logon no agente:** usando a opção Ações no nó do OneDrive, clique em **Efetuar logon no agente** para executar tarefas específicas do agente, como restaurar usando a opção de montagem de volume.
6. **Fazer backup agora:** usando a opção Ações no nó do OneDrive, clique em **Fazer backup agora** para executar um backup manual.
7. **Restaurar:** usando a opção Ações no nó do OneDrive, clique em **Restaurar** para efetuar logon no agente e executar uma restauração.
8. Baixar o ponto de recuperação a partir da nuvem

9. Atualizar o ponto de recuperação na nuvem
10. Copiar ponto de recuperação para o disco local ou compartilhamento de rede

Adicionar um nó do OneDrive

Observação: diferentemente de outros nós, não é possível adicionar o nó do OneDrive a partir da página Todos os nós. Um nó do OneDrive é adicionado a um plano apenas durante a criação ou modificação do plano.

Para obter informações sobre como adicionar o nó, consulte "Especificar a origem" Na página 1044 durante a criação do plano de backup do OneDrive.

Excluir um nó do OneDrive Online

Exclua todos os nós do OneDrive Online que não são mais necessários.

Siga estas etapas:

1. Clique em **Excluir** na opção **Ações** no nó do OneDrive.
2. Confirme no pop-up para excluir o nó do console.

   O nó do OneDrive Online é excluído com êxito.

Como gerenciar nós do grupo do banco de dados Oracle

Usando o Arcserve UDP, é possível executar várias ações para gerenciar os nós do banco de dados Oracle, como atualizar o nó, exportar o nó, executar a tarefa de backup, cancelar a tarefa de backup e excluir um nó.

Esta seção contém os seguintes tópicos:

Atualizar nó do banco de dados Oracle

É possível atualizar as informações relacionadas aos nós existentes. Ao modificar as credenciais dos nós do banco de dados Oracle, é necessário atualizar os nós do banco de dados Oracle no console.

Siga estas etapas:

1. Efetue logon no Console do Arcserve UDP.
2. Clique na guia **Recursos**.

   A página Nós: todos os nós é exibida.
3. Siga um destes procedimentos:

- No painel esquerdo, navegue até **Nós**, **Grupo de bancos de dados Oracle**, clique com o botão direito do mouse no nó que deseja atualizar e, em seguida, clique em **Atualizar**.
- No painel central, selecione o nó que deseja atualizar, clique na lista suspensa **Ações** e, em seguida, clique em **Atualizar**.

A caixa de diálogo Atualizar nó aparece.

5. Na caixa de diálogo Atualizar nó, modifique os detalhes conforme necessário e clique em **OK**.

   O nó do banco de dados Oracle é atualizado.

Exportar nó

É possível exportar os nós como um arquivo ZIP (.zip). Quando necessário, é possível importar o arquivo ZIP para manter os nós. Por exemplo, exportar nós antes de atualizações ou reinicializações ajuda a importar o mesmo conjunto de nós.

É possível exportar apenas os nós que possuem credenciais válidas e que são executados no sistema operacional Windows.

Siga estas etapas:

1. Efetue logon no Console do Arcserve UDP.
2. Clique na guia **Recursos**.

   A página Nós: todos os nós é exibida.
3. Siga um destes procedimentos:
   - No painel esquerdo, navegue até **Nós**, **Grupo de bancos de dados Oracle**, clique com o botão direito do mouse no nó que deseja exportar e, em seguida, clique em **Exportar**.
   - No painel central, selecione o nó que deseja exportar, clique na lista suspensa **Ações** e, em seguida, clique em **Exportar**.

   Uma caixa de diálogo é exibida solicitando sua ação no arquivo list.zip.
4. Clique em **Abrir** ou **Salvar**.

   A lista de nós é exportada.

Fazer backup do nó do banco de dados Oracle

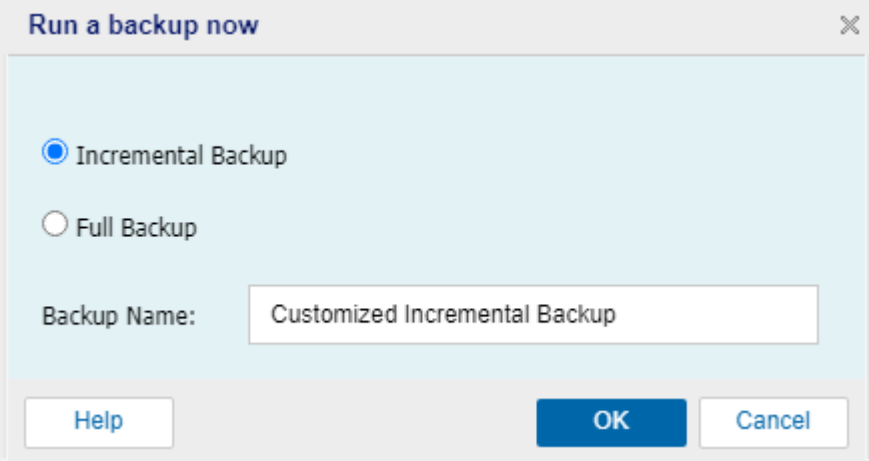
Em geral, os backups são executados automaticamente e controlados pelas configurações da programação. Além do backup programado, um backup manual fornece a opção de fazer backup dos nós de acordo com a necessidade.

Siga estas etapas:

1. Efetue logon no Console do Arcserve UDP.
2. Clique na guia **Recursos**.

   A página Nós: todos os nós é exibida.
3. Siga um destes procedimentos:
   - No painel esquerdo, navegue até **Nós**, **Grupo de bancos de dados Oracle**, clique com o botão direito do mouse no nó do qual deseja fazer backup e clique em **Fazer backup agora**.
   - No painel central, selecione o nó do qual deseja fazer backup, clique na lista suspensa **Ações** e, em seguida, clique em **Fazer backup agora**.

   A caixa de diálogo Fazer backup agora é exibida.
4. Na caixa de diálogo *Executar um backup agora*, selecione o tipo de backup que deseja executar e, em seguida, especifique o nome do backup, se necessário.



As opções disponíveis são:

Backup incremental

Inicia um backup incremental do computador inteiro. Um backup incremental realiza backup somente dos blocos que foram alterados desde o backup anterior.

Observação: se estiver executando um backup pela primeira vez, o backup completo será iniciado automaticamente, mesmo que você tenha selecionado a opção Backup incremental.

As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a execução de backups.

Backup completo

Inicia um backup completo do computador inteiro ou dos volumes selecionados.

Observação: se nenhum nome de backup for especificado, por padrão, ele será automaticamente nomeado como Backup completo ou incremental personalizado.

5. Clique em **OK**.

   A caixa de diálogo Informações do andamento é exibida.

6. Aguarde até que a tarefa de backup seja concluída e clique em **OK**.

   A tarefa de backup é realizada com êxito.

Cancelar a tarefa de backup dos nós do banco de dados Oracle

Após o início da tarefa de backup dos nós do banco de dados Oracle, é possível cancelar a tarefa de backup a qualquer momento. Quando você cancela a tarefa de backup, o backup é interrompido imediatamente.

Siga estas etapas:

1. Clique na guia **Recursos**.

   A página Nós: todos os nós é exibida.

3. Siga um destes procedimentos:

   - No painel esquerdo, navegue até **Nós**, **Grupo de bancos de dados Oracle**, clique com o botão direito do mouse no nó do qual deseja cancelar o backup e clique em **Cancelar**.
   - No painel central, selecione o nó cujo backup deseja cancelar, clique na lista suspensa **Ações** e, em seguida, clique em **Cancelar**.

   Uma mensagem de confirmação é exibida.

5. Clique em **Sim** para confirmar.

   A tarefa de backup é cancelada com êxito.

Excluir nós do banco de dados Oracle

Você pode excluir os nós do banco de dados Oracle dos quais não necessita mais. Se excluir os nós, os logs e os históricos de tarefas associados também serão excluídos. É possível adicionar o nó excluído mais tarde, se necessário.

Siga estas etapas:

1. Clique na guia **Recursos**.

   A página Nós: todos os nós é exibida.

3. Siga um destes procedimentos:

   - No painel esquerdo, navegue até **Nós**, **Grupo de bancos de dados Oracle**, clique com o botão direito do mouse no nó que deseja excluir e, em seguida, clique em **Excluir**.
   - No painel central, selecione o nó que deseja excluir, clique na lista suspensa **Ações** e, em seguida, clique em **Excluir**.

   Uma mensagem de confirmação é exibida.

5. Clique em **Sim** para confirmar.

   O nó é excluído com êxito do console.

Capítulo 9: Adicionando e gerenciando destinos

Esta seção contém os seguintes tópicos:

Como adicionar um destino

Um destino é um local onde você armazena os dados de backup. O Arcserve UDP permite adicionar vários tipos de destinos.

O que fazer a seguir:

1. Adicionar um destino usando o RPS
2. Adicionar servidores do Arcserve Backup
3. Adicionar um console remoto
4. Adicionar uma conta de nuvem
5. Adicionar uma conta de nuvem do Arcserve

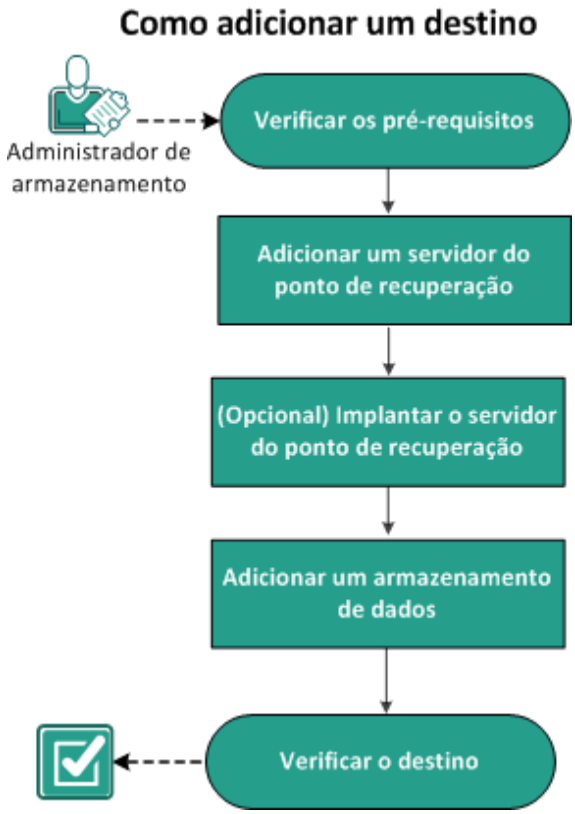
Como adicionar um destino

Para Arcserve UDP, é possível atribuir um RPS (Recovery Point Server – Servidor de Ponto de Recuperação) como um destino central. É possível armazenar dados de vários nós em um servidor de ponto de recuperação e, em seguida, recuperar os dados quando necessário. Adicionar um destino envolve principalmente duas etapas:

a. Adicionar um servidor de ponto de recuperação ao console.

b. Adicionar um repositório de dados ao servidor de ponto de recuperação.

O diagrama a seguir mostra como adicionar um destino:



O que fazer a seguir?

1. Verificar os pré-requisitos
2. Adicionar um servidor de ponto de recuperação
3. (Opcional) Implantar o servidor de ponto de recuperação
4. Adicionar um repositório de dados
5. Verificar o destino

Verificar os pré-requisitos

Antes de configurar um servidor de ponto de recuperação, conclua os seguintes pré-requisitos:

- Examine as Notas da Versão para obter uma descrição dos requisitos do sistema, os sistemas operacionais suportados e uma lista de problemas conhecidos nesta release do Arcserve Unified Data Protection.
- Verifique se você tem privilégios de administrador para instalar o Arcserve Unified Data Protection.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Adicionar um servidor do ponto de recuperação

A adição de um destino começa com a adição de um servidor de ponto de recuperação. Posteriormente, você adiciona repositório de dados ao RPS.

Siga estas etapas:

1. Faça logon no Arcserve Unified Data Protection e clique na guia **recursos**.
2. No painel à esquerda, navegue para **Destinos** e clique em **Servidores de ponto de recuperação**.

   A página **Destinos: servidores do ponto de recuperação** é exibida no painel central.
3. Clique em **Adicionar um servidor do ponto de recuperação**.

   A página **Adicionar um Servidor do ponto de recuperação** é exibida.
4. Digite os seguintes detalhes:

   Nome do nó/endereço IP

   Define o nome do nó do servidor de ponto de recuperação que você deseja adicionar ao console.

   Nome de usuário e senha

   Define o nome de usuário e a senha que ajudarão você a efetuar logon no nó.

   Observação: use um dos seguintes formatos de nome de usuário: nome do computador, nome do domínio/nome de usuário ou nome do usuário.

   Descrição

   (Opcional) Define quaisquer informações adicionais sobre o nó.
5. Preencha os campos a seguir para as **Configurações de instalação**:

   Observação: se o servidor já possuir o servidor de ponto de recuperação instalado, ignore estas configurações de instalação.

   Local de instalação

   Especifique o local onde deseja instalar o servidor do ponto de recuperação. É possível aceitar o caminho padrão ou especificar um caminho alternativo.

   Porta

   Especifica o número da porta que se conecta à interface de usuário com base na web.

   Padrão: 8014.

   Protocolo

Especifique o protocolo que deseja usar para a comunicação com o servidor de destino. As seleções disponíveis são HTTP e HTTPS.

Observação: para uma comunicação mais segura, selecione o protocolo HTTPS.

Driver de rastreamento de alterações

Especifique se deseja **Instalar o driver de rastreamento de alteração do agente.**

6. Programe a instalação ou atualização selecionando uma das opções em **Data e hora de início da instalação ou atualização**.

   Observação: se o servidor já possui o Servidor do ponto de recuperação instalado, ignore essas configurações.

7. Clique em **Salvar**.

   O andamento da implantação é exibido no painel direito. O servidor do ponto de recuperação é adicionado.

   Agora, o servidor do ponto de recuperação está implantado. É possível adicionar os repositórios de dados após o servidor de ponto de recuperação ser adicionado.

(Opcional) Implantar o servidor de ponto de recuperação

Usando o Arcserve Unified Data Protection, você pode detectar e implantar a versão mais recente do componente RPS em servidores de ponto de recuperação. Depois de implantar o componente RPS, o nó está pronto para armazenar as sessões de backup e servir como um servidor de ponto de recuperação.

Observação: os componentes de RPS são instalados com a instalação do Arcserve Unified Data Protection.

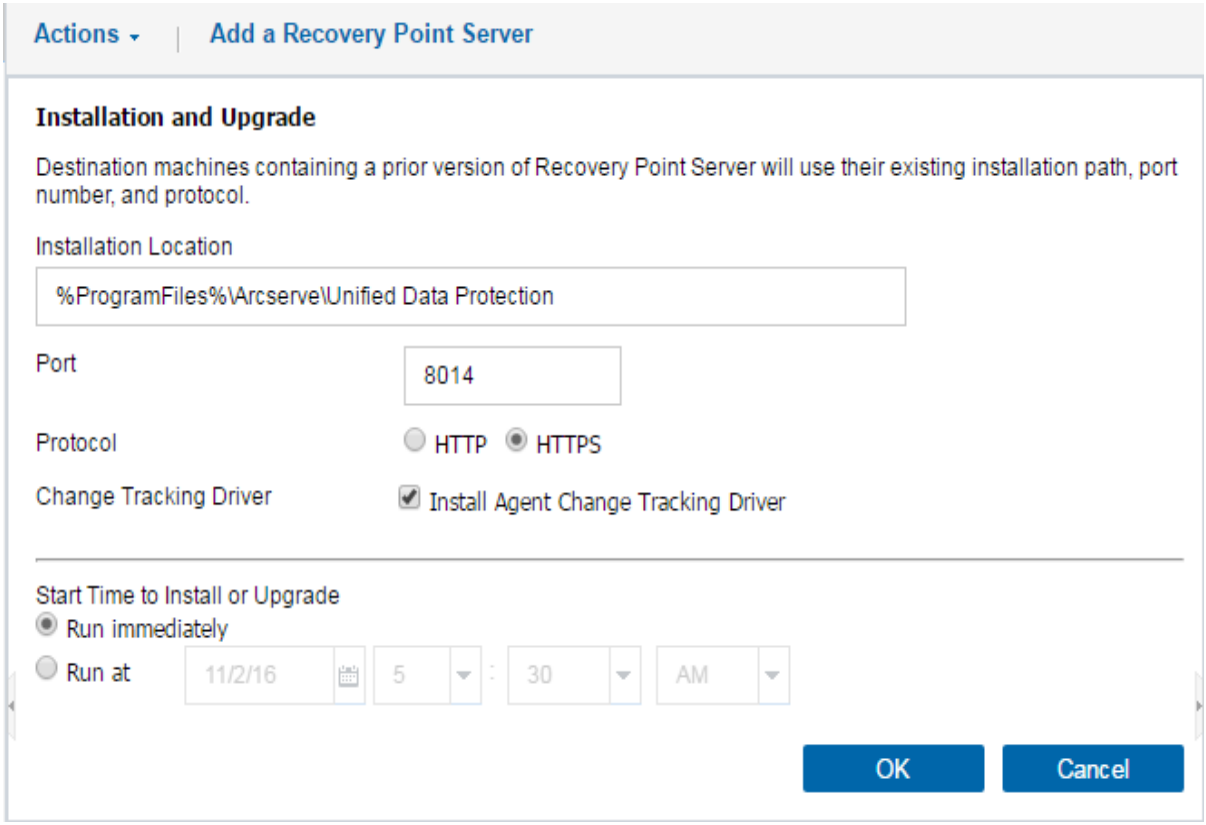
Siga estas etapas:

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Servidores do ponto de recuperação**.

   A página **Destino**: Servidor de ponto de recuperação é exibida.
3. Execute uma das seguintes ações:
   - Clique com o botão direito do mouse em um servidor de ponto de recuperação.
   - Selecione um servidor de ponto de recuperação e, no painel central, clique no menu suspenso **Ações**.

   Uma lista de opções é exibida.
4. Clique em **Instalar/atualizar o servidor de ponto de recuperação**.

   A página **Instalação e atualização** é exibida.



5. Modifique as configurações de implantação e clique em **OK** para implantar o servidor de ponto de recuperação para o nó selecionado.

   A implantação do servidor de ponto de recuperação é iniciada. É possível ver o andamento da implantação no painel direito.

Adicionar um repositório de dados

Para criar o destino, o servidor de ponto de recuperação precisa de repositórios de dados. O repositório de dados especifica onde os dados do backup serão armazenados. É possível adicionar vários repositórios de dados a um RPS.

Siga estas etapas:

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Servidores do ponto de recuperação**.

   A página **Destinos: servidores de ponto de recuperação** é exibida.
3. Execute uma das seguintes ações:
   - Clique com o botão direito do mouse em um servidor de ponto de recuperação.
   - Selecione um servidor de ponto de recuperação e, no painel central, clique no menu suspenso **Ações**.

   Uma lista de opções é exibida.
4. Clique em **Adicionar um repositório de dados.**

   A página **Criar repositório de dados** é exibida com o nome do servidor de ponto de recuperação especificado.
5. Especifique os campos a seguir e clique em **Salvar**.

   Servidor de ponto de recuperação

   Define o servidor de ponto de recuperação em que o repositório de dados foi criado. O servidor de ponto de recuperação já está adicionado por padrão.

   Nome do repositório de dados

   Define o nome do repositório de dados.

   Pasta do repositório de dados

   Define o local da pasta na qual o repositório de dados foi criado. Clique em Procurar para selecionar a pasta de destino.

   Observações:

   - Agora você pode ativar e exibir volumes ocultos. Para obter mais informações, consulte Como ativar e exibir volumes ocultos ao criar um repositório de dados.
   - para o repositório de dados de redução de redundância e de não redução de redundância, o caminho de destino deve ser uma pasta vazia.

Limite de nós ativos simultâneos

Especifica o número máximo de tarefas simultâneas no repositório de dados.

Valor padrão: 4

refere-se a um valor de 1 a 9999. O valor indica o número de tarefas que podem ser executadas simultaneamente. Se a execução de tarefas atender o número, outra tarefa será colocada na fila e apenas poderá ser iniciada apenas quando uma das tarefas em execução for concluída. A tarefa concluída pode significar uma tarefa concluída, cancelada ou com falha.

O número se aplica aos tipos de tarefas, mas não aos nós do servidor. Por exemplo, número 5 indica que cinco tarefas de backup estão em execução. Qualquer tarefa programada após as cinco tarefas de backup aguarda na fila, mas é possível enviar outra tarefa, como Catálogo do sistema de arquivos.

Se o valor for superior a 16 ou 32, sertão exibidas mensagens para avisar sobre a maior demanda no hardware.

Observação: limitar a quantidade afeta apenas a tarefa de saída de replicação e não a tarefa de entrada de replicação. Limitar a quantidade não afeta a restauração ou as tarefas de BMR. Essas tarefas não são colocadas em uma fila.

Ativar a redução de redundância

Especifica que a redução de redundância está ativada para o repositório de dados. O Arcserve UDP suporta dois tipos de redução de redundância: redução de redundância do lado da origem e a redução de redundância global. A redução de redundância do lado da origem impede que os blocos de dados duplicados se movam na rede de um determinado agente. A redução de redundância global elimina os dados duplicados em todos os computadores cliente com base no nível de agrupamento do volume.

Tamanho do bloco de redução de redundância

Define o tamanho do bloco de redução de redundância. As opções são: 4 KB, 8 KB, 16 KB, 32 KB e 64 KB. O tamanho do bloco de redução de redundância também afeta a estimativa da capacidade de redução de redundância. Por exemplo, se você alterar o valor padrão de 16 KB para 32 KB, as estimativas de capacidade de redução de redundância duplicarão. O aumento do tamanho de bloco de redução de redundância pode diminuir o percentual de redução de redundância.

Alocação de memória hash

Especifica a quantidade de memória física alocada para manter os hashes. Esse campo é preenchido previamente com um valor padrão. O valor padrão baseia-se no seguinte cálculo:

Se a memória física do RPS for menor do que 4 GB (ou igual a 4 GB), o valor padrão de **Alocação de memória hash** será idêntico para a memória física do RPS.

Se a memória física do RPS for maior do que 4 GB, o Arcserve UDP calcula a memória livre disponível no momento. Suponha que a memória livre disponível seja X GB no momento. O Arcserve UDP verifica também as seguintes condições:

- Se (X * 80%) > = 4 GB, o valor padrão de **Alocação de memória hash** é (X * 80%).
- Se (X * 80%) < 4 GB, o valor padrão de **Alocação de memória hash** é 4 GB.

Exemplo: considere que o RPS tem 32 GB de memória física. Suponhamos que o sistema operacional e outros aplicativos usem 4 GB de memória durante a criação do repositório de dados. Portanto, a memória livre disponível no momento é de 28 GB. Então, o valor padrão de **Alocação de memória hash** é 22.4 GB (22.4 GB = 28 GB * 80%).

O destino de hash está em uma SSD (Solid State Drive – Unidade de Estado Sólido)

Especifica se a pasta de hash está em uma unidade de estado sólido.

Observação: configure o destino de hash no SSD local se o destino de Hash que está em uma opção SSD (Solid State Drive - Unidade de Estado Sólido) estiver ativado

Destino de Dados

Define a pasta de destino de dados para salvar os blocos de dados reais exclusivo. Use o maior tamanho de disco para armazenar dados naquele que contém os blocos de dados originais de origem.

Observação: o caminho **Destino dos dados** deve ser uma pasta vazia.

Destino do índice

Define a pasta de destino do índice para armazenar os arquivos de índice. Escolha um disco diferente para melhorar o processamento de redução de redundância.

Observação: o caminho **Destino de índice** deve ser uma pasta vazia.

Destino de hash

Define o caminho para armazenar o banco de dados de hash. O Arcserve UDP usa o algoritmo SHA1 para gerar o hash para os dados de origem. Os valores de hash são gerenciados pelo banco de dados de hash. Selecionar uma SSD (Solid State Drive – Unidade de Estado Sólido) de alta velocidade

aumenta a capacidade de redução de redundância e exige uma alocação de memória menor. Para melhorar o desempenho de hash, é recomendável formatar o volume SSD como o sistema de arquivos NTFS com o tamanho do agrupamento do volume de 4KB.

Observação: o caminho de **Destino de hash** deve ser uma pasta vazia.

Observação: não é possível especificar o mesmo caminho para as quatro seguintes pastas: **Repositório de dados, Destino dos dados, Destino do índice** e **Destino de hash**.

Ativar compactação

Especifica se as configurações de compactação de dados estão ativadas.

Tipo de compactação

Especifica se é preciso usar o tipo de compactação padrão ou máxima.

A compactação geralmente é selecionada para reduzir o uso de espaço em disco, mas também tem um impacto inverso sobre a velocidade do backup, devido ao aumento no uso da CPU. Com base nos seus requisitos, é possível selecionar uma das três opções disponíveis.

Observação: para obter mais informações, consulte Tipo de compactação.

Ativar criptografia

Especifica se as configurações de criptografia estão ativadas. Ao selecionar essa opção, especifique e confirme a senha criptografada.

A criptografia de dados é a conversão de dados em uma forma ininteligível sem um mecanismo decodificador. A solução Arcserve Unified Data Protection usa algoritmos de criptografia AES (Advanced Encryption Standard – Padrão de criptografia avançada) seguros para atingir o máximo de segurança e privacidade dos seus dados. Os repositórios de dados podem ser usados com ou sem criptografia. Para criptografia, apenas AES-256 está disponível.

A senha não será obrigatória caso esteja tentando restaurar no computador em que o backup foi executado. No entanto, caso esteja tentando restaurar em um computador diferente, a senha será necessária. Por padrão, a senha é obrigatória apenas para o primeiro logon. Para informar a senha mesmo após o primeiro logon, o administrador precisará interromper manualmente o serviço Arcserve UDP Agent Explorer Extension.

Enviar um alerta por email quando um destino estiver se aproximando da capacidade máxima

A seleção dessa opção configura o repositório de dados para enviar um alerta por email. O RPS envia alertas por email aos destinatários quando a pasta de destino do repositório de dados está se aproximando da capacidade máxima.

Configurar email

Esse botão só é exibido quando você ativa a opção *Enviar um alerta por email quando um destino estiver se aproximando da capacidade máxima*. Ele ajuda você a fornecer a ID de email para o recebimento de alertas. Clique no botão **Configurar email** para carregar as configurações globais de alerta por email em Console > Configurações > Configuração de email e alerta. Se as configurações globais de email não estiverem disponíveis, quando você clicar no botão**Configurar email**, será aberta a caixa de diálogo**Configurações de email** para você definir os detalhes de email.

O repositório de dados é criado e é exibida no painel central. Clique no repositório de dados para visualizar os detalhes no painel direito.

Vários estados do repositório de dados

O repositório de dados exibe status diferentes dependendo da tarefa executada nele. Quando você seleciona um repositório de dados na guia **Recursos**, o status do repositório de dados é exibido no painel à direita.

- **Interrompido:**o repositório de dados está inativo. Não é possível enviar nenhuma tarefa nesse estado.
- **Iniciando:** o repositório de dados está sendo inicializado. Quando o repositório de dados está sendo iniciado, o andamento é exibido no console.
- **Em execução:**o repositório de dados está ativo. É possível enviar tarefas nesse estado.
- **Interrompendo:** o repositório de dados está sendo interrompido. Quando o repositório de dados está sendo interrompido, o andamento é exibido no Console.
- **Modificando:** o repositório de dados está sendo atualizado com os novos dados. Quando o repositório de dados está sendo modificado, o andamento é exibido no Console.
- **Excluindo:** o repositório de dados está sendo excluído. Quando o repositório de dados está sendo excluído, o andamento é exibido no Console.
- **Fora de serviço:** o repositório de dados não está funcionando corretamente. Não é possível enviar nenhuma tarefa nesse estado. Interrompa o repositório de dados e verifique a razão para esse comportamento. Os casos a seguir podem resultar no status Fora de serviço de um repositório de dados:
  - O destino de backup do repositório de dados não pode ser acessado.
  - As configurações no Registro ou no arquivo ou estão corrompidas.
  - O índice GDD ou a função de dados apresenta erros internos.
  - O índice GDD ou o processo de função de dados foi interrompido manualmente.
- **Restaurar somente:** no estado Restaurar somente, nenhuma tarefa que implica gravação de dados no repositório é executada. Tarefas como backup, tarefa de replicação (in), tarefa de início rápido (in), tarefa de migração de dados. Todas as outras tarefas são executadas, as quais precisam ler dados do repositório de dados. O status do repositório de dados muda para Somente restauração nas seguintes condições:

- quando o processo de função de hash é interrompido manualmente.
- Quando a memória hash atribuída/capacidade de volume do caminho de hash/índice/dados/destino de backup atinge o limite máximo.

Importante: quando o status do repositório de dados é Somente restaurar (estado de degradação) ou Fora de serviço (estado incorreto), o repositório de dados não funciona corretamente. Você deve interromper o repositório de dados e verificar a causa-raiz do status. Por exemplo, o problema pode estar no volume de redução de redundância de dados que atingiu seu limite máximo. Depois de resolver a causa-raiz, inicie o repositório de dados e envie a tarefa de backup novamente.

Verificar o destino

Após concluir todos os procedimentos envolvidos na adição de um RPS, verifique se o RPS foi adicionado com êxito.

Siga estas etapas:

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Servidores do ponto de recuperação**.

   A página **Destinos: Servidores de ponto de recuperação** é exibida.
3. Verifique os seguintes detalhes:
   - O RPS criado é exibido.
   - Os repositórios de dados são exibidos em RPS.

Adicionar servidores do Arcserve Backup

Adicione um servidor do Arcserve Backup para arquivar dados em uma fita. Quando você cria um plano para arquivar dados em um dispositivo de fita, é possível usar esse destino.

Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection e clique na guia **Recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Servidores do Arcserve Backup**.

   A página **Destinos: Servidores do Arcserve Backup** é exibida no painel central.
3. Clique em **Adicionar servidor do Arcserve Backup**.

   A página **Adicionar servidor do Arcserve Backup** é exibida.
4. Digite os seguintes detalhes:

   Nome do nó/endereço IP

   Especifica o nome do nó ou o endereço IP do servidor do Arcserve Backup.

   Tipo de autenticação

   Especifica o tipo de autenticação usado para se efetuar logon no servidor do Arcserve Backup. As duas opções a seguir estão disponíveis:

   Autenticação do Windows

   Especifica que a autenticação do Windows será usada para se efetuar logon no servidor do Arcserve Backup.

   Observação: o usuário do Windows deve ser registrado no Arcserve Backup primeiro usando o gerenciador de perfis de usuário do Arcserve Backup.

   Autenticação do Arcserve Backup

   Especifica que a autenticação do Arcserve Backup será usada para se efetuar logon no servidor do Arcserve Backup.

   Nome de usuário e senha

   Define o nome de usuário e sua senha para efetuar logon no nó.

   Observação: use um dos seguintes formatos para o nome de usuário: nome do computador, nome de domínio/nome de usuário ou nome de usuário.

   Porta

   Especifica o número da porta usada para se conectar ao servidor do Arcserve Backup.

Observação: o Arcserve UDP usa o número da porta para conectar-se aos servidores, ao servidor principal do Arcserve Backup e ao servidor integrante no domínio do Arcserve Backup.

5. Clique em **Salvar**.

   O servidor de backup do Arcserve é adicionado ao console.

   Depois de adicionar o servidor do Arcserve Backup no console, é possível navegar até **recursos, destino, servidores do Arcserve Backup** e verificar as informações detalhadas da mídia de fita.

Adicionar um console remoto

Adicione um console remoto para replicar pontos de recuperação para um servidor de ponto de recuperação gerenciado remotamente. Você pode usar o console remoto para criar um plano de replicação para enviar dados para o console de destino. Você também pode gerenciar o console remoto adicionado.

Siga estas etapas:

1. Faça logon no Arcserve Unified Data Protection e clique na guia **recursos**.
2. No painel esquerdo, navegue até **Destinos** e clique em **Console remoto**.

   A página **Destinos: console remoto** é exibida no painel central.
3. Clique em **Adicionar um console remoto**.

   A página **Adicionar um console remoto** é exibida.
4. Digite os seguintes detalhes:

   Console remoto

   Refere-se à URL da conta de console remoto que você deseja adicionar ao console.

   Nome de usuário

   Refere-se ao nome do usuário que ajuda a efetuar logon no console remoto.

   Observação: use um dos seguintes formatos de nome de usuário: nome do computador, nome do domínio/nome de usuário ou nome do usuário.

   Senha

   Refere-se à senha para o nome de usuário.

   Porta

   Refere-se ao número da porta que se conecta à interface do usuário com base na web.

   Padrão: 8015.

   Protocolo

   Especifique o protocolo que deseja usar para a comunicação com o servidor de destino. As seleções disponíveis são HTTP e HTTPS.

   Observação: para uma comunicação mais segura, selecione o protocolo HTTPS.

   Configurações de proxy

Especifica as configurações do servidor proxy. Marque a caixa de seleção **Conectar usando um servidor proxy** se desejar ativar esta opção. Caso selecione esta opção, será necessário incluir também o endereço IP (ou nome do computador) do servidor proxy e o número da porta correspondente, usado pelo servidor proxy em conexões com a internet. Pode-se também selecionar esta opção se o servidor proxy exigir autenticação. Será necessário fornecer as informações de autenticação correspondentes (nome de domínio/nome de usuário e senha) para usar o servidor proxy.

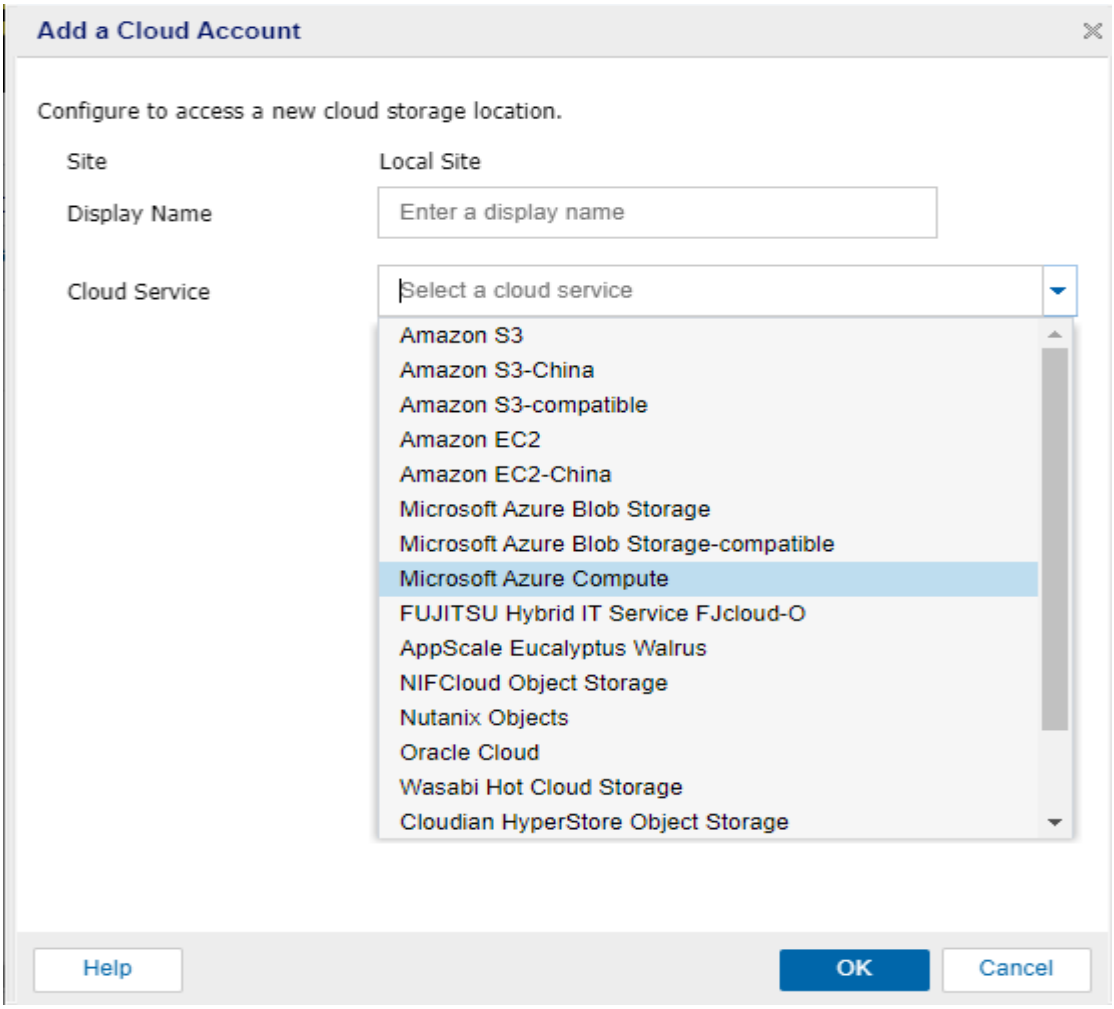
5. Clique em **OK**.

   Agora, o console remoto é adicionado.

Adicionar uma conta de nuvem

Adicione uma conta de nuvem para copiar arquivos ou pontos de recuperação em um armazenamento na nuvem. Você pode usar contas relacionadas ao criar tarefas ou um ou mais planos em Copiar ponto de recuperação/Cópia de arquivos/Arquivo morto/Modo de espera virtual para nuvem/Máquina virtual instantânea no Amazon EC2. Forneça um nome exclusivo de armazenamento e selecione o serviço de armazenamento necessário das várias opções exibidas na lista suspensa.

Observação: se você configurou a cópia de arquivo e o arquivo morto em versões do Arcserve UDP v6.0 ou versões anteriores e agora estiver atualizando para a versão mais recente do Arcserve UDP, para arquivo morto, o Arcserve UDP cria um novo compartimento de memória na nuvem com o sufixo **-fa**. A cópia de arquivo usa o mesmo compartimento de memória usado na versão anterior.



As opções de configuração para cada fornecedor da nuvem são semelhantes (com algumas terminologias distintas), e nenhuma diferença é descrita. Adicione uma conta de nuvem de sua escolha.

Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection e clique na guia **recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Contas da nuvem**.

   A página **Destinos: Contas da nuvem** é exibida no painel central.
3. Clique em **Adicionar uma conta de nuvem**.

   A página **Adicionar uma conta de nuvem** é exibida.
4. Em **Nome de exibição**, forneça um nome exclusivo.

   Nome de exibição especifica o nome do armazenamento na nuvem. Esse nome será adicionado ao console para identificar a conta da nuvem. Cada conta de nuvem deve ter um nome de exibição exclusivo.
5. Selecione a opção da lista suspensa **Serviço de nuvem**.

   Vários campos são exibidos para configuração.
6. Insira os detalhes nos campos a seguir para configurar e clique em **OK**:

   As opções de serviço de armazenamento disponíveis são Amazon S3, Compatível com o Amazon S3, Armazenamento de blobs do Microsoft Azure, Compatível com o armazenamento de blobs do Microsoft Azure, FUJITSU Hybrid IT Service FJcloud-O, AppScale Eucalyptus Walrus, Amazon EC2, Amazon EC2-China, Computação do Microsoft Azure, Nutanix Objects, Wasabi Hot Cloud Storage e Oracle Cloud.

   Observação: clique nos nomes de serviço de armazenamento para ver como adicionar uma conta de nuvem para o serviço de armazenamento.

   A opção de configuração varia de acordo com o serviço de armazenamento selecionado.

   A conta de nuvem de serviço de armazenamento selecionada é adicionada ao console do Arcserve UDP e exibida na tela **Destinos: contas de nuvem**. Por exemplo, as contas do Amazon S3 são exibidas abaixo.

O que fazer a seguir?

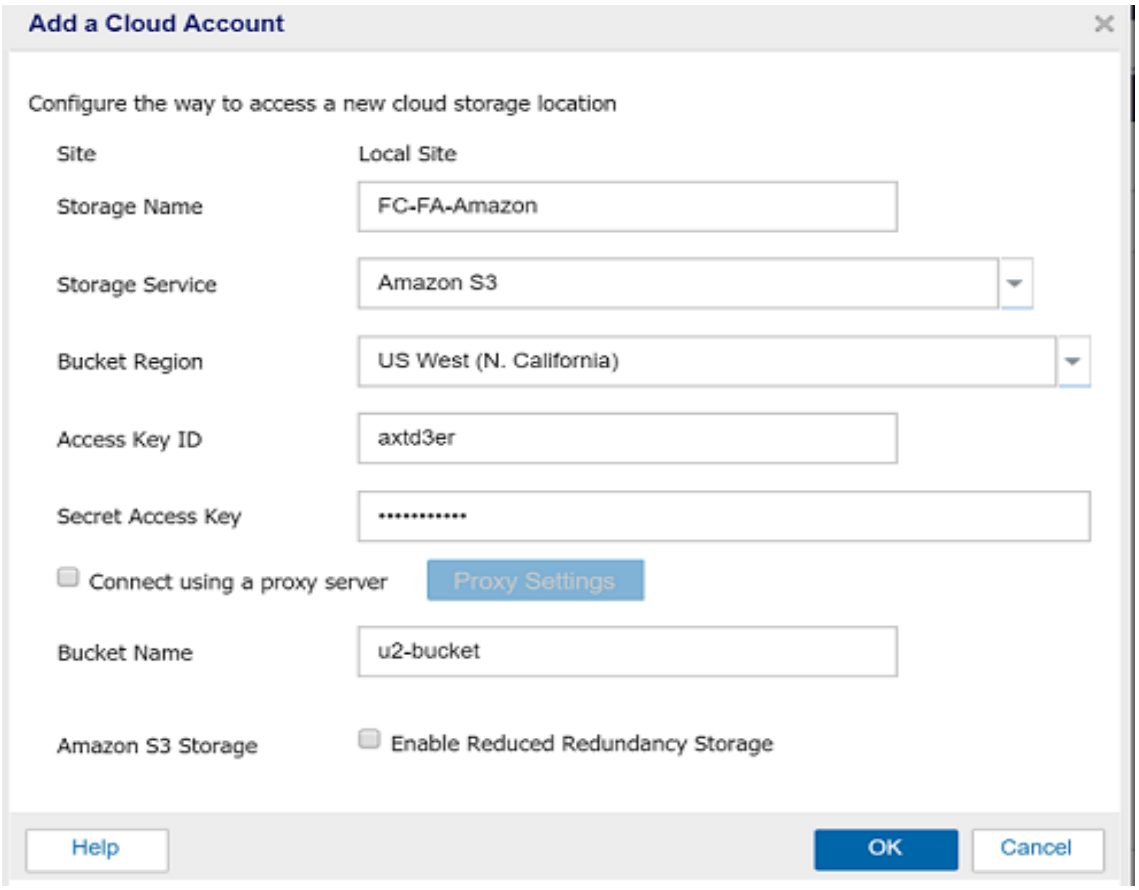
Adicione uma conta de nuvem para:

- Amazon S3
- Compatível com Amazon S3
- Armazenamento de blobs do Microsoft Azure
- Compatível com o armazenamento de blobs do Microsoft Azure
- FUJITSU Hybrid IT Service FJcloud-O
- AppScale Eucalyptus Walrus
- Amazon EC2
- Amazon EC2-China
- Computação do Microsoft Azure
- Nutanix Objects
- Wasabi Hot Cloud Storage
- Oracle Cloud

Adicionar uma conta de nuvem para Amazon S3

Adicione uma conta de nuvem Amazon S3 para copiar arquivos ou pontos de recuperação em um armazenamento na nuvem.

É possível usar essa conta durante a criação das tarefas Copiar ponto de recuperação/Cópia de arquivo/Arquivo morto.



Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection e clique na guia **recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Contas da nuvem**.

   A página **Destinos: Contas da nuvem** é exibida no painel central.
3. Clique em **Adicionar uma conta de nuvem**.

   A página **Adicionar uma conta de nuvem** é exibida.
4. Em **Nome de exibição**, forneça um nome exclusivo.

   Nome de exibição especifica o nome do armazenamento na nuvem. Esse nome será adicionado ao console para identificar a conta da nuvem. Cada conta de nuvem deve ter um nome de exibição exclusivo.

5. Selecione a opção da lista suspensa **Serviço de nuvem**.

   Vários campos são exibidos para configuração.

6. Insira os detalhes nos campos a seguir para configurar e clique em **OK**:

   Região de compartimento de memória

   Refere-se à região do compartimento de memória no Amazon.

   ID da chave de acesso

   Identifica o usuário que está solicitando acesso a este local.

   Chave de acesso confidencial

   Refere-se a uma senha que é usada para verificar a autenticidade da solicitação para acessar esse local porque sua chave de acesso não está criptografada.

   Importante: esta chave de acesso secreta é fundamental para manter a segurança de suas contas. É necessário manter as chaves e as credenciais da conta em um local seguro. Não incorpore a chave de acesso secreta em uma página da web ou em outro código-fonte de acesso público e não a transmita em canais não seguros.

   Configurações de proxy

   Especifica as configurações do servidor proxy. Marque a caixa de seleção **Conectar usando um servidor proxy** se desejar ativar esta opção. Caso selecione esta opção, será necessário incluir também o endereço IP (ou nome do computador) do servidor proxy e o número da porta correspondente, usado pelo servidor proxy em conexões com a internet. Pode-se também selecionar esta opção se o servidor proxy exigir autenticação. Será necessário fornecer as informações de autenticação correspondentes (nome de domínio/nome de usuário e senha) para usar o servidor proxy.

   Nome do compartimento de memória

   Todos os arquivos e as pastas movidos ou copiados para o fornecedor de nuvem são armazenados e organizados nos seus compartimentos de memória. Os compartimentos de memória são como um contêiner para os arquivos e são usados para agrupar e organizar objetos. Cada objeto armazenado no fornecedor da nuvem é colocado em um compartimento de memória.

   Ativar a redução de armazenamento de dados redundantes

   Para Amazon S3 apenas, esta opção permite ativar a RRS (Reduced Redundancy Storage). A RRS é uma opção de armazenamento no Amazon S3 que ajuda a reduzir os custos, armazenando dados reproduzíveis, não críticos em níveis de redundância mais baixos do que o armazenamento padrão do Amazon

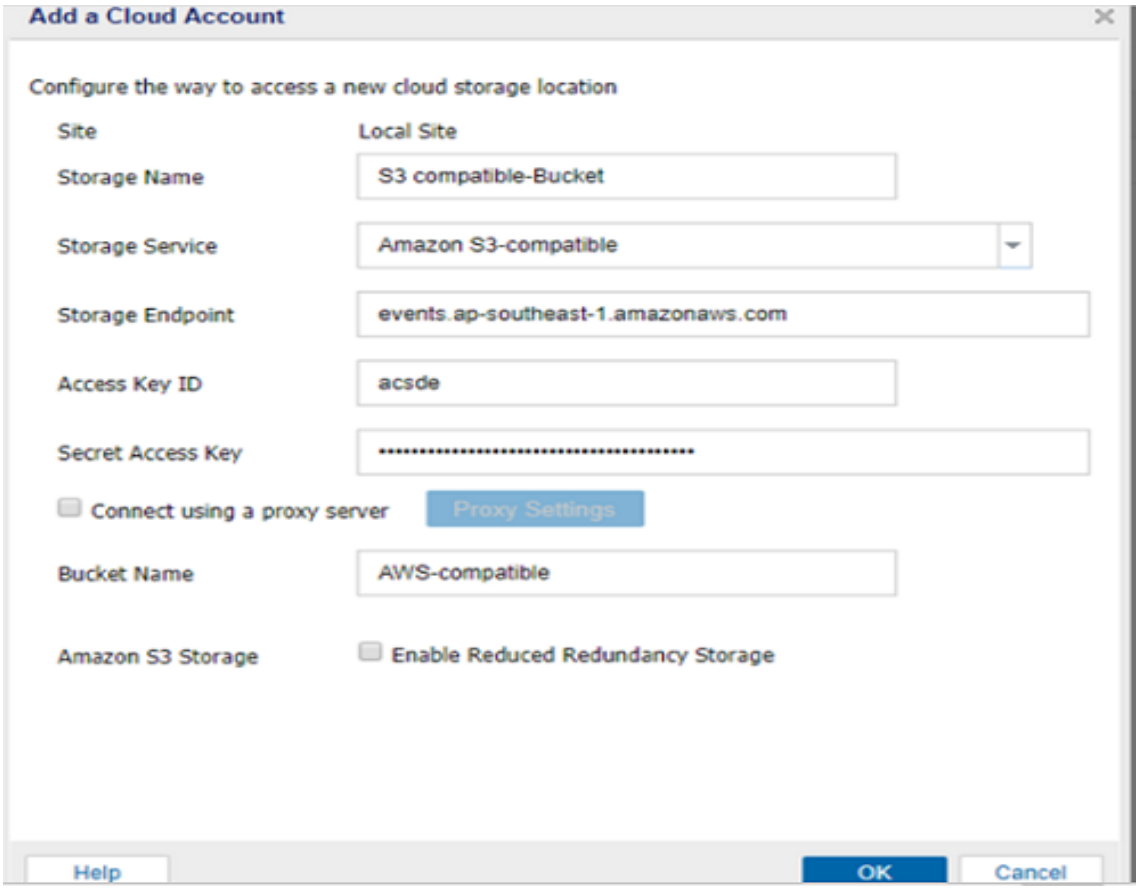
S3. As opções de armazenamento padrão e de redução de armazenamento de dados redundantes armazenam dados em vários recursos e dispositivos, mas com a RRS os dados são replicados menos vezes e o custo é menor. Deve-se esperar a mesma latência e taxa de transferência usando o armazenamento padrão ou RRS do Amazon S3. Por padrão, esta opção não está selecionada (o Amazon S3 usa a opção de armazenamento padrão).

A conta de nuvem é adicionada ao console.

Observação: se você configurou a cópia de arquivo e o arquivo morto em versões do Arcserve UDP v6.0 ou versões anteriores e agora estiver atualizando para a versão mais recente do Arcserve UDP, para arquivo morto, o Arcserve UDP cria um novo compartimento de memória na nuvem com o sufixo **-fa**. A cópia de arquivo usa o mesmo compartimento de memória usado na versão anterior.

Adicionar uma conta de nuvem compatível com Amazon S3

Adicione uma conta de nuvem compatível com Amazon S3 para copiar arquivos ou pontos de recuperação em um armazenamento na nuvem. É possível usar essa conta durante a criação das tarefas Copiar ponto de recuperação/Cópia de arquivo/Arquivo morto.



Observações:

- Para subfornecedores do S3/compatíveis com o S3, que usam o tipo de autenticação V3/V2 para obter a certificação do Arcserve CCI, ele funciona bem visto que o sinalizador de substituição de tipo Signatário padrão esteja definido como **Verdadeiro**. Entretanto, os subfornecedores usando a autenticação V4 precisam alterar o sinalizador para **Falso** no arquivo AmazonPlugin.properties e reiniciar os serviços.

  SIGNER_OVERRIDE=false

- Para oferecer suporte à nuvem HGST compatível com Amazon-S3, é necessário alterar o seguinte AmazonPlugin.property:

  SET_STORAGECLASS_HEADER=false

Essa propriedade ajuda a ignorar o cabeçalho do armazenamento. Como resultado, usando essa propriedade se você adicionar uma tarefa de Cópia de arquivo/Arquivamento de arquivo com o Amazon como o destino da nuvem, por padrão o cabeçalho de armazenamento é ignorado.

O arquivo AmazonPlugin.properties está no seguinte local:

C:\Arquivos de Programas\Arcserve\Unified Data Protection\Engine\BIN\CCI\Config

Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection e clique na guia **recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Contas da nuvem**.

   A página **Destinos: Contas da nuvem** é exibida no painel central.
3. Clique em **Adicionar uma conta de nuvem**.

   A página **Adicionar uma conta de nuvem** é exibida.
4. Em **Nome de exibição**, forneça um nome exclusivo.

   Nome de exibição especifica o nome do armazenamento na nuvem. Esse nome será adicionado ao console para identificar a conta da nuvem. Cada conta de nuvem deve ter um nome de exibição exclusivo.
5. Selecione a opção da lista suspensa **Serviço de nuvem**.

   Vários campos são exibidos para configuração.
6. Insira os detalhes nos campos a seguir para configurar e clique em **OK**:

   Ponto de extremidade do armazenamento

   Especifica o URL do serviço do fornecedor. Por exemplo, *http://[nome do servidor]:nº da porta*

   ID da chave de acesso

   Identifica o usuário que está solicitando acesso a este local.

   Chave de acesso confidencial

   Refere-se a uma senha que é usada para verificar a autenticidade da solicitação para acessar esse local porque sua chave de acesso não está criptografada.

   Importante: esta chave de acesso secreta é fundamental para manter a segurança de suas contas. É necessário manter as chaves e as credenciais da conta em um local seguro. Não incorpore a chave de acesso secreta em uma página da web ou em outro código-fonte de acesso público e não a transmita em canais não seguros.

Configurações de proxy

Especifica as configurações do servidor proxy. Marque a caixa de seleção **Conectar usando um servidor proxy** se desejar ativar esta opção. Caso selecione esta opção, será necessário incluir também o endereço IP (ou nome do computador) do servidor proxy e o número da porta correspondente, usado pelo servidor proxy em conexões com a internet. Pode-se também selecionar esta opção se o servidor proxy exigir autenticação. Será necessário fornecer as informações de autenticação correspondentes (nome de domínio/nome de usuário e senha) para usar o servidor proxy.

Nome do compartimento de memória

Todos os arquivos e as pastas movidos ou copiados para o fornecedor de nuvem são armazenados e organizados nos seus compartimentos de memória. Os compartimentos de memória são como um contêiner para os arquivos e são usados para agrupar e organizar objetos. Cada objeto armazenado no fornecedor da nuvem é colocado em um compartimento de memória.

Ativar a redução de armazenamento de dados redundantes

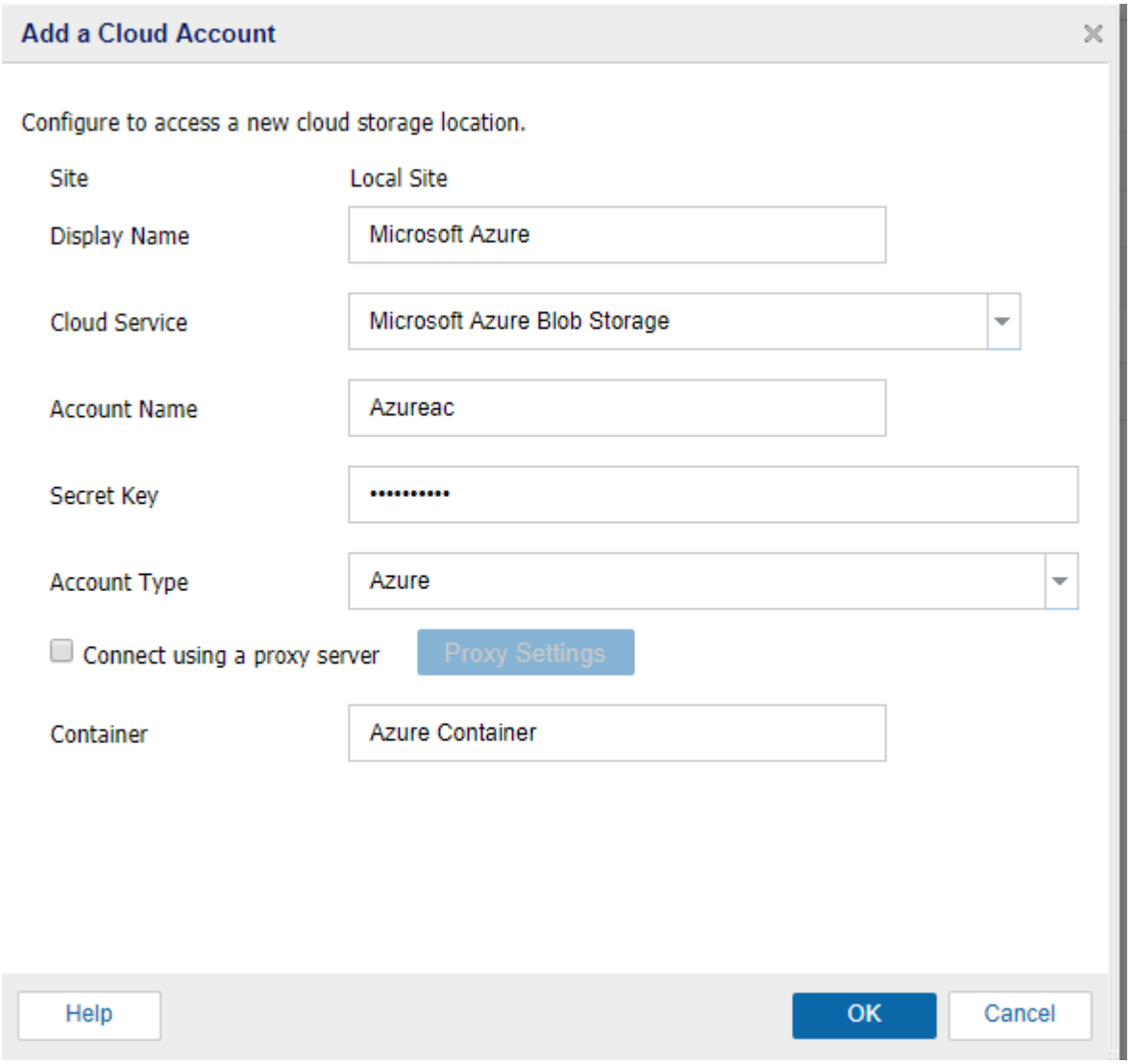
Para Amazon S3 apenas, esta opção permite ativar a RRS (Reduced Redundancy Storage). A RRS é uma opção de armazenamento no Amazon S3 que ajuda a reduzir os custos, armazenando dados reproduzíveis, não críticos em níveis de redundância mais baixos do que o armazenamento padrão do Amazon S3. As opções de armazenamento padrão e de redução de armazenamento de dados redundantes armazenam dados em vários recursos e dispositivos, mas com a RRS os dados são replicados menos vezes e o custo é menor. Deve-se esperar a mesma latência e taxa de transferência usando o armazenamento padrão ou RRS do Amazon S3. Por padrão, esta opção não está selecionada (o Amazon S3 usa a opção de armazenamento padrão).

A conta de nuvem é adicionada ao console.

Observação: se você configurou a cópia de arquivo e o arquivo morto em versões do Arcserve UDP v6.0 ou versões anteriores e agora estiver atualizando para a versão mais recente do Arcserve UDP, para arquivo morto, o Arcserve UDP cria um novo compartimento de memória na nuvem com o sufixo **-fa**. A cópia de arquivo usa o mesmo compartimento de memória usado na versão anterior.

Adicionar uma conta de nuvem para o armazenamento de blobs do Microsoft Azure

Adicione uma conta de nuvem do armazenamento de blobs do Microsoft Azure para copiar arquivos ou pontos de recuperação em um armazenamento na nuvem. É possível usar essa conta durante a criação das tarefas Copiar ponto de recuperação/Cópia de arquivo/Arquivo morto.



Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection e clique na guia **recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Contas da nuvem**.

   A página **Destinos: Contas da nuvem** é exibida no painel central.
3. Clique em **Adicionar uma conta de nuvem**.

A página **Adicionar uma conta de nuvem** é exibida.

4. Em **Nome de exibição**, forneça um nome exclusivo.

   Nome de exibição especifica o nome do armazenamento na nuvem. Esse nome será adicionado ao console para identificar a conta da nuvem. Cada conta de nuvem deve ter um nome de exibição exclusivo.

5. Selecione a opção da lista suspensa **Serviço de nuvem**.

   Vários campos são exibidos para configuração.

6. Insira os detalhes nos campos a seguir para configurar e clique em **OK**:

   Nome da conta

   Identifica o usuário que está solicitando acesso a este local.

   Chave secreta

   Refere-se a uma senha que é usada para verificar a autenticidade da solicitação para acessar esse local porque sua chave de acesso não está criptografada.

   Importante: Esta chave secreta é fundamental para manter a segurança de suas contas. É necessário manter as chaves e as credenciais da conta em um local seguro. Não incorpore a chave secreta em uma página da web ou em outro código-fonte publicamente acessível e não a transmita em canais não seguros.

   Configurações de proxy

   Especifica as configurações do servidor proxy. Marque a caixa de seleção **Conectar usando um servidor proxy** se desejar ativar esta opção. Caso selecione esta opção, será necessário incluir também o endereço IP (ou nome do computador) do servidor proxy e o número da porta correspondente, usado pelo servidor proxy em conexões com a internet. Pode-se também selecionar esta opção se o servidor proxy exigir autenticação. Será necessário fornecer as informações de autenticação correspondentes (nome de domínio/nome de usuário e senha) para usar o servidor proxy.

   Recipiente

   Todos os arquivos e as pastas movidos ou copiados para o fornecedor de nuvem são armazenados e organizados nos seus recipientes. Usando recipientes, é possível agrupar e organizar objetos juntos. Cada objeto armazenado no fornecedor da nuvem é colocado em um compartimento de memória.

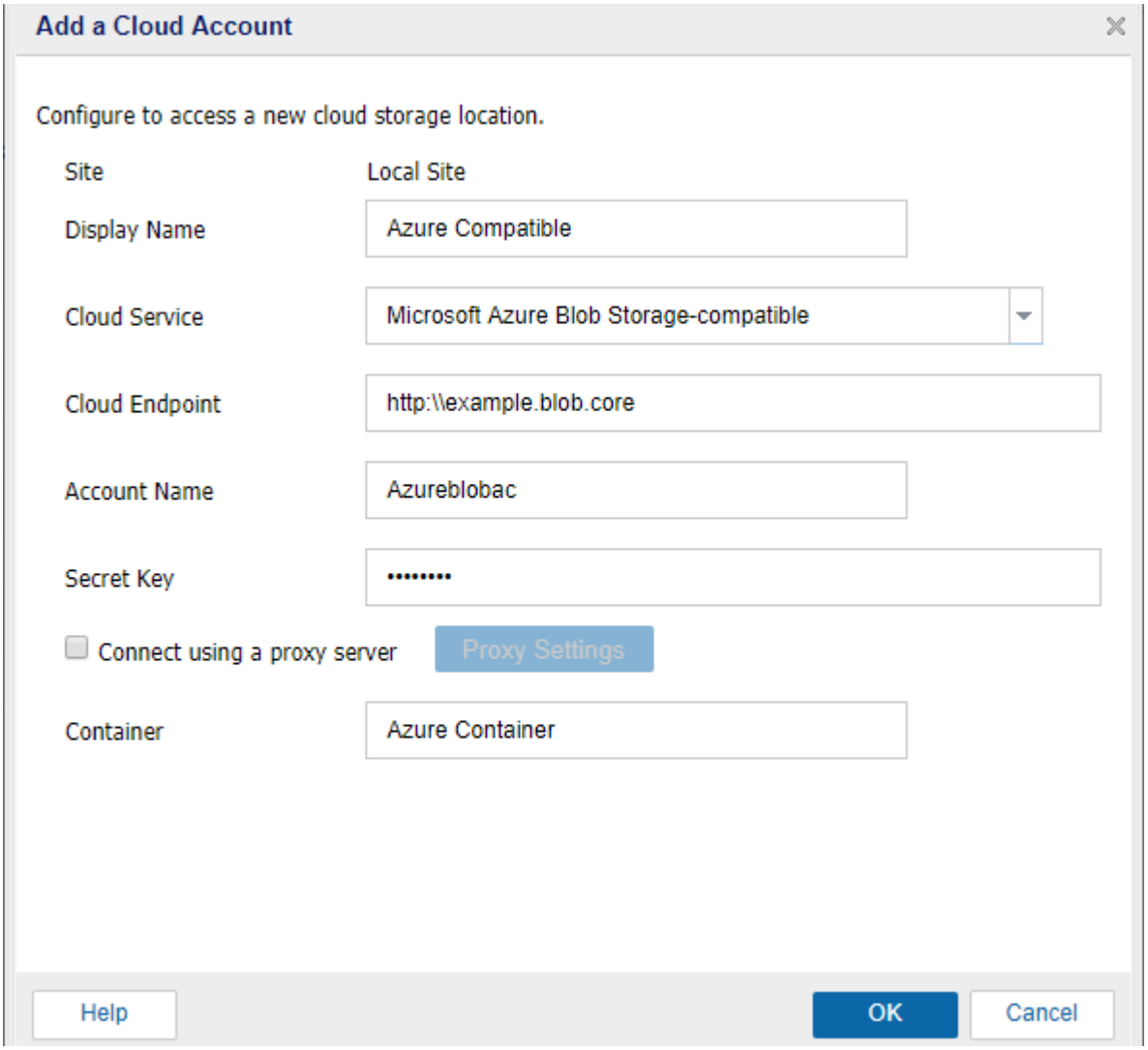
A conta de nuvem é adicionada ao console.

Observação: se você configurou a cópia de arquivo e o arquivo morto em versões do Arcserve UDP v6.0 ou versões anteriores e agora estiver atualizando para a

versão mais recente do Arcserve UDP, para arquivo morto, o Arcserve UDP cria um novo compartimento de memória na nuvem com o sufixo **-fa**. A cópia de arquivo usa o mesmo compartimento de memória usado na versão anterior.

Adicionar uma conta de nuvem compatível com o armazenamento de blobs do Microsoft Azure

Adicione uma conta de nuvem compatível com o armazenamento de blobs do Microsoft Azure para copiar arquivos ou pontos de recuperação em um armazenamento na nuvem. É possível usar essa conta durante a criação das tarefas Copiar ponto de recuperação/Cópia de arquivo/Arquivo morto.



Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection e clique na guia **recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Contas da nuvem**.

   A página **Destinos: Contas da nuvem** é exibida no painel central.
3. Clique em **Adicionar uma conta de nuvem**.

   A página **Adicionar uma conta de nuvem** é exibida.

4. Em **Nome de exibição**, forneça um nome exclusivo.

   Nome de exibição especifica o nome do armazenamento na nuvem. Esse nome será adicionado ao console para identificar a conta da nuvem. Cada conta de nuvem deve ter um nome de exibição exclusivo.

5. Selecione a opção da lista suspensa **Serviço de nuvem**.

   Vários campos são exibidos para configuração.

6. Insira os detalhes nos campos a seguir para configurar e clique em **OK**:

   Ponto de extremidade do armazenamento

   Especifica o URL do serviço do fornecedor. Por exemplo, *http://[nome do servidor]:nº da porta*

   Nome da conta

   Identifica o usuário que está solicitando acesso a este local.

   Chave secreta

   Refere-se a uma senha que é usada para verificar a autenticidade da solicitação para acessar esse local porque sua chave de acesso não está criptografada.

   Importante: Esta chave secreta é fundamental para manter a segurança de suas contas. É necessário manter as chaves e as credenciais da conta em um local seguro. Não incorpore a chave secreta em uma página da web ou em outro código-fonte publicamente acessível e não a transmita em canais não seguros.

   Configurações de proxy

   Especifica as configurações do servidor proxy. Marque a caixa de seleção **Conectar usando um servidor proxy** se desejar ativar esta opção. Caso selecione esta opção, será necessário incluir também o endereço IP (ou nome do computador) do servidor proxy e o número da porta correspondente, usado pelo servidor proxy em conexões com a internet. Pode-se também selecionar esta opção se o servidor proxy exigir autenticação. Será necessário fornecer as informações de autenticação correspondentes (nome de domínio/nome de usuário e senha) para usar o servidor proxy.

   Recipiente

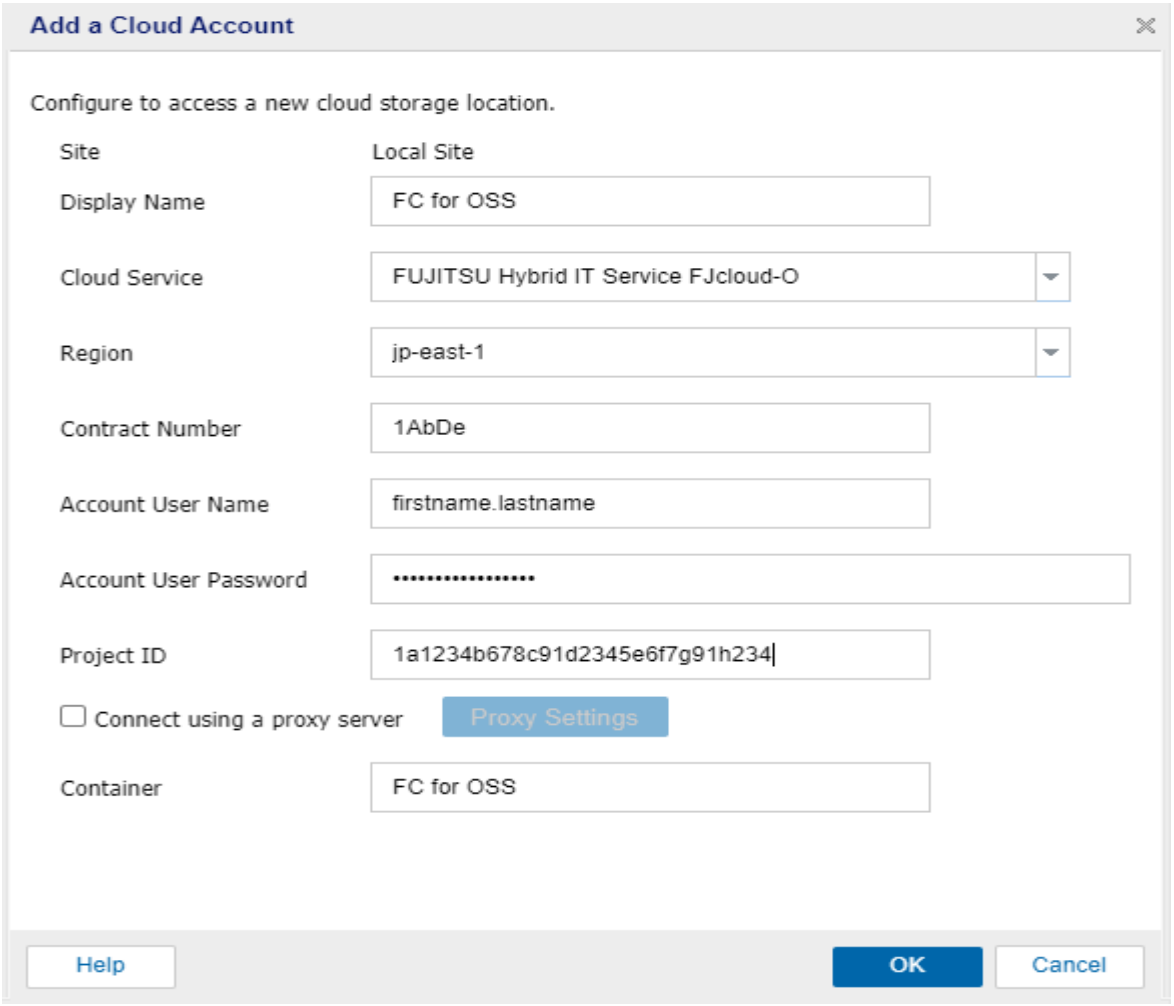
   Todos os arquivos e as pastas movidos ou copiados para o fornecedor de nuvem são armazenados e organizados nos seus recipientes. Usando recipientes, é possível agrupar e organizar objetos juntos. Cada objeto armazenado no fornecedor da nuvem é colocado em um compartimento de memória.

A conta de nuvem é adicionada ao console.

Observação: se você configurou a cópia de arquivo e o arquivo morto em versões do Arcserve UDP v6.0 ou versões anteriores e agora estiver atualizando para a versão mais recente do Arcserve UDP, para arquivo morto, o Arcserve UDP cria um novo compartimento de memória na nuvem com o sufixo **-fa**. A cópia de arquivo usa o mesmo compartimento de memória usado na versão anterior.

Adicionar uma conta de nuvem para FUJITSU Hybrid IT Service FJcloud-O

Adicione uma conta de nuvem do FUJITSU Hybrid IT Service FJcloud-O para copiar arquivos ou pontos de recuperação em um armazenamento na nuvem. É possível usar essa conta durante a criação de tarefas de cópia de arquivo ou de arquivo morto.



Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection e clique na guia **recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Contas da nuvem**.

   A página **Destinos: Contas da nuvem** é exibida no painel central.
3. Clique em **Adicionar uma conta de nuvem**.

   A página **Adicionar uma conta de nuvem** é exibida.

4. Em **Nome de exibição**, forneça um nome exclusivo.

   Nome de exibição especifica o nome do armazenamento na nuvem. Esse nome será adicionado ao console para identificar a conta da nuvem. Cada conta de nuvem deve ter um nome de exibição exclusivo.

5. Selecione a opção da lista suspensa **Serviço de nuvem**.

   Vários campos são exibidos para configuração.

6. Insira os detalhes nos campos a seguir para configurar e clique em **OK**:

   Região de compartimento de memória

   Refere-se à região do compartimento de memória no FUJITSU Hybrid IT Service FJcloud-O.

   Nome de usuário da conta

   Identifica o usuário que está solicitando acesso a este local.

   Senha do usuário da conta

   Refere-se a uma senha que é usada para verificar a autenticidade da solicitação para acessar esse local porque sua senha não está criptografada.

   Importante: Esta senha é fundamental para manter a segurança de suas contas. É necessário manter as chaves e as credenciais da conta em um local seguro. Não incorpore a senha em uma página da web ou em outro código-fonte publicamente acessível e não transmita a senha em canais não seguros.

   Configurações de proxy

   Especifica as configurações do servidor proxy. Marque a caixa de seleção **Conectar usando um servidor proxy** se desejar ativar esta opção. Caso selecione esta opção, será necessário incluir também o endereço IP (ou nome do computador) do servidor proxy e o número da porta correspondente, usado pelo servidor proxy em conexões com a internet. Pode-se também selecionar esta opção se o servidor proxy exigir autenticação. Será necessário fornecer as informações de autenticação correspondentes (nome de domínio/nome de usuário e senha) para usar o servidor proxy.

   Número do contrato

   Refere-se ao número do contrato que o FUJITSU Hybrid IT Service FJcloud-O fornece.

   ID do projeto

   Refere-à ID do projeto que o FUJITSU Hybrid IT Service FJcloud-O gera.

   Recipiente

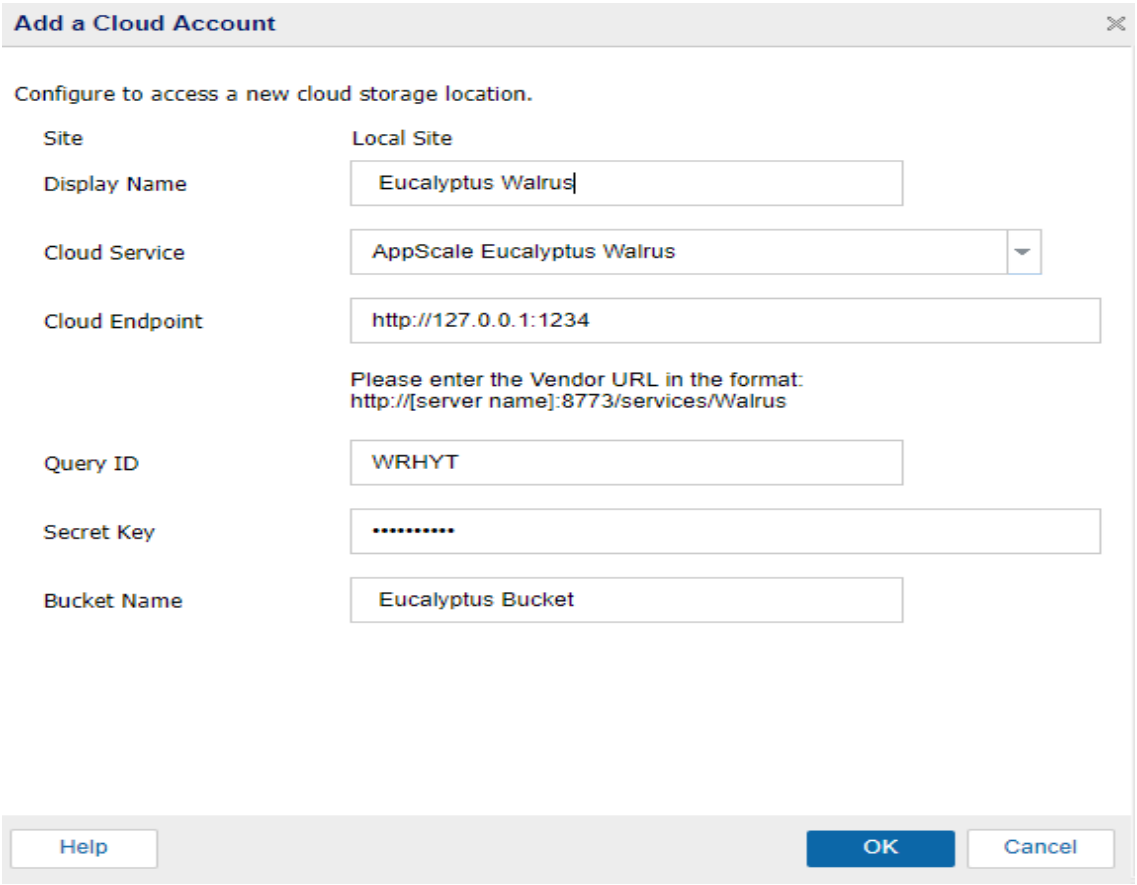
Todos os arquivos e as pastas movidos ou copiados para o fornecedor de nuvem são armazenados e organizados nos seus recipientes. Usando recipientes, é possível agrupar e organizar objetos juntos. Cada objeto armazenado no fornecedor da nuvem é colocado em um compartimento de memória.

A conta de nuvem é adicionada ao console.

Observação: se você configurou a cópia de arquivo e o arquivo morto em versões do Arcserve UDP v6.0 ou versões anteriores e agora estiver atualizando para a versão mais recente do Arcserve UDP, para arquivo morto, o Arcserve UDP cria um novo compartimento de memória na nuvem com o sufixo **-fa**. A cópia de arquivo usa o mesmo compartimento de memória usado na versão anterior.

Adicionar uma conta de nuvem para AppScale Eucalyptus Walrus

Adicione uma conta de nuvem do AppScale Eucalyptus Walrus para copiar arquivos ou pontos de recuperação em um armazenamento na nuvem. É possível usar essa conta durante a criação das tarefas Copiar ponto de recuperação/Cópia de arquivo/Arquivo morto.



Observação: se você estiver usando o AppScale Eucalyptus Walrus como seu fornecedor de nuvem de cópia de arquivo, não será possível copiar arquivos cujo comprimento total do caminho exceda 170 caracteres.

Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection e clique na guia **recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Contas da nuvem**.

   A página **Destinos: Contas da nuvem** é exibida no painel central.
3. Clique em **Adicionar uma conta de nuvem**.

   A página **Adicionar uma conta de nuvem** é exibida.
4. Em **Nome de exibição**, forneça um nome exclusivo.

Nome de exibição especifica o nome do armazenamento na nuvem. Esse nome será adicionado ao console para identificar a conta da nuvem. Cada conta de nuvem deve ter um nome de exibição exclusivo.

5. Selecione a opção da lista suspensa **Serviço de nuvem**.

   Vários campos são exibidos para configuração.

6. Insira os detalhes nos campos a seguir para configurar e clique em **OK**:

   Ponto de extremidade do armazenamento

   Especifica o URL do serviço do fornecedor. Por exemplo, *http://[nome do servidor]:nº da porta*

   ID da consulta

   Identifica o usuário que está solicitando acesso a este local.

   Chave secreta

   Refere-se a uma senha que é usada para verificar a autenticidade da solicitação para acessar esse local porque sua chave de acesso não está criptografada.

   Importante: Esta chave secreta é fundamental para manter a segurança de suas contas. É necessário manter as chaves e as credenciais da conta em um local seguro. Não incorpore a chave secreta em uma página da web ou em outro código-fonte publicamente acessível e não a transmita em canais não seguros.

   Nome do compartimento de memória

   Todos os arquivos e as pastas movidos ou copiados para o fornecedor de nuvem são armazenados e organizados nos seus compartimentos de memória. Os compartimentos de memória são como um contêiner para os arquivos e são usados para agrupar e organizar objetos. Cada objeto armazenado no fornecedor da nuvem é colocado em um compartimento de memória.

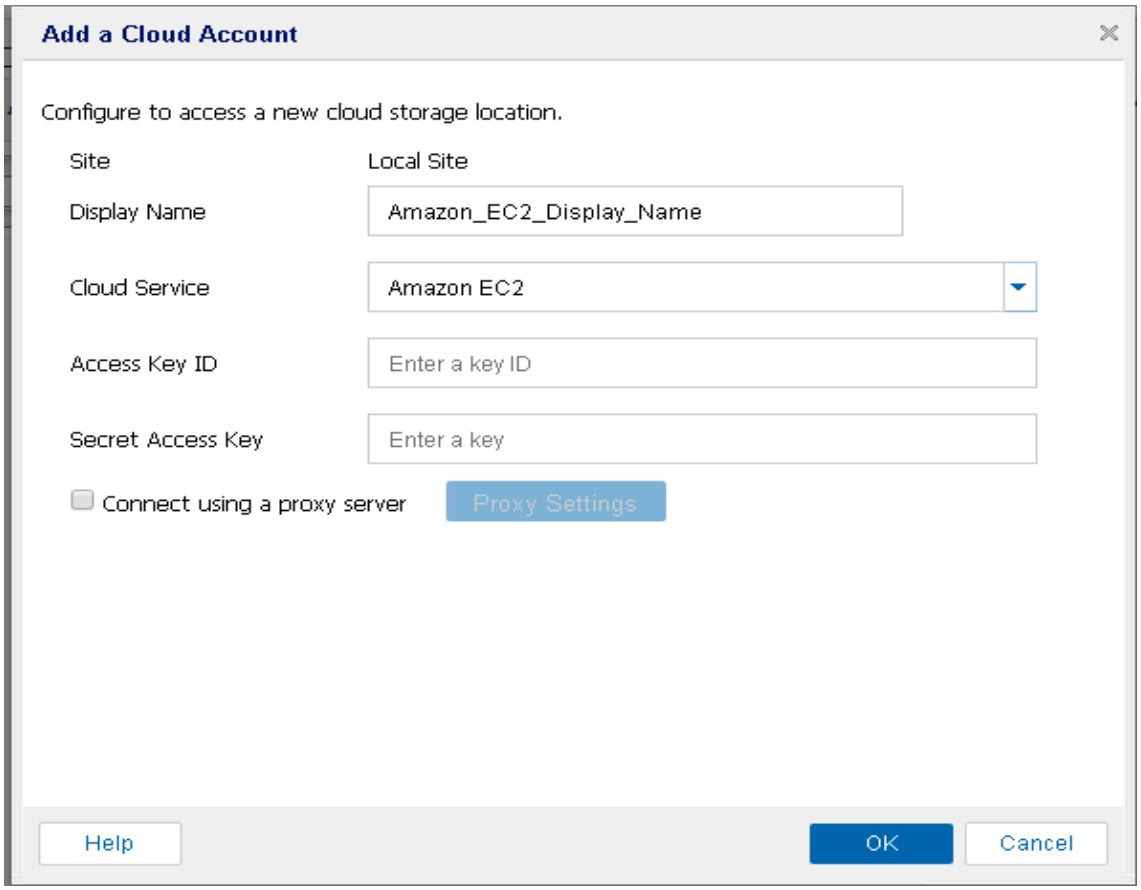
   A conta de nuvem é adicionada ao console.

   Observação: se você configurou a cópia de arquivo e o arquivo morto em versões do Arcserve UDP v6.0 ou versões anteriores e agora estiver atualizando para a versão mais recente do Arcserve UDP, para arquivo morto, o Arcserve UDP cria um novo compartimento de memória na nuvem com o sufixo **-fa**. A cópia de arquivo usa o mesmo compartimento de memória usado na versão anterior.

Adicionar uma conta de nuvem para Amazon EC2

Adicione uma conta de nuvem Amazon EC2 para copiar arquivos ou pontos de recuperação em um armazenamento na nuvem.

É possível usar esta conta ao criar tarefas para os planos de modo de espera virtual para nuvem ou máquina virtual instantânea no Amazon EC2.



Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection e clique na guia **recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Contas da nuvem**.

   A página **Destinos: Contas da nuvem** é exibida no painel central.
3. Clique em **Adicionar uma conta de nuvem**.

   A página **Adicionar uma conta de nuvem** é exibida.
4. Em **Nome de exibição**, forneça um nome exclusivo.

   Nome de exibição especifica o nome do armazenamento na nuvem. Esse nome será adicionado ao console para identificar a conta da nuvem. Cada conta de nuvem deve ter um nome de exibição exclusivo.

5. Selecione a opção da lista suspensa **Serviço de nuvem**.

   Vários campos são exibidos para configuração.

6. Insira os detalhes nos campos a seguir para configurar e clique em **OK**:

   ID da chave de acesso

   Identifica o usuário que está solicitando acesso a este local.

   Chave de acesso confidencial

   Refere-se a uma senha que é usada para verificar a autenticidade da solicitação para acessar esse local porque sua chave de acesso não está criptografada.

   Importante: esta chave de acesso secreta é fundamental para manter a segurança de suas contas. É necessário manter as chaves e as credenciais da conta em um local seguro. Não incorpore a chave de acesso secreta em uma página da web ou em outro código-fonte de acesso público e não a transmita em canais não seguros.

   Configurações de proxy

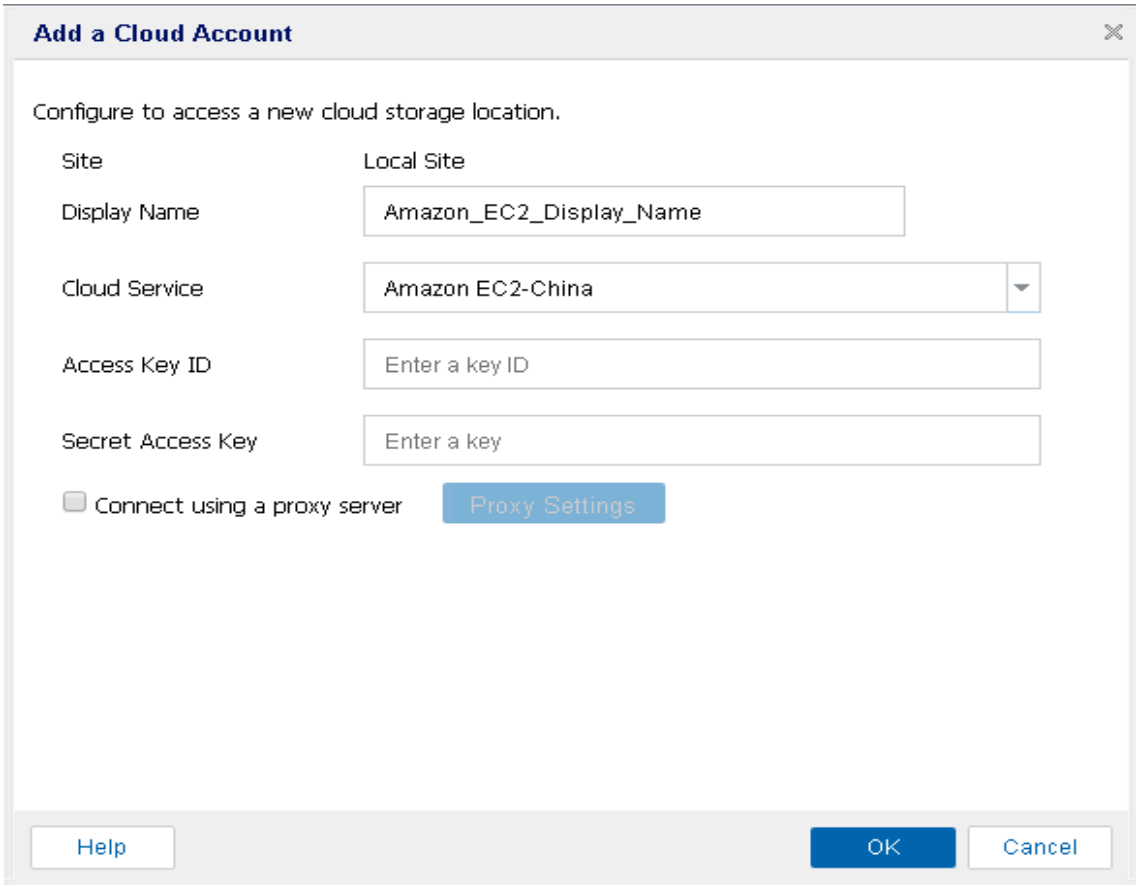
   Especifica as configurações do servidor proxy. Marque a caixa de seleção **Conectar usando um servidor proxy** se desejar ativar esta opção. Caso selecione esta opção, será necessário incluir também o endereço IP (ou nome do computador) do servidor proxy e o número da porta correspondente, usado pelo servidor proxy em conexões com a internet. Pode-se também selecionar esta opção se o servidor proxy exigir autenticação. Será necessário fornecer as informações de autenticação correspondentes (nome de domínio/nome de usuário e senha) para usar o servidor proxy.

   A conta de nuvem é adicionada ao console.

   Observação: se você configurou a cópia de arquivo e o arquivo morto em versões do Arcserve UDP v6.0 ou versões anteriores e agora estiver atualizando para a versão mais recente do Arcserve UDP, para arquivo morto, o Arcserve UDP cria um novo compartimento de memória na nuvem com o sufixo **-fa**. A cópia de arquivo usa o mesmo compartimento de memória usado na versão anterior.

Adicionar uma conta de nuvem para Amazon EC2-China

Adicione uma conta de nuvem Amazon EC2-China para copiar arquivos ou pontos de recuperação em um armazenamento na nuvem. É possível usar esta conta ao criar tarefas para os planos de modo de espera virtual para nuvem ou máquina virtual instantânea no Amazon EC2.



Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection e clique na guia **recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Contas da nuvem**.

   A página **Destinos: Contas da nuvem** é exibida no painel central.
3. Clique em **Adicionar uma conta de nuvem**.

   A página **Adicionar uma conta de nuvem** é exibida.
4. Em **Nome de exibição**, forneça um nome exclusivo.

Nome de exibição especifica o nome do armazenamento na nuvem. Esse nome será adicionado ao console para identificar a conta da nuvem. Cada conta de nuvem deve ter um nome de exibição exclusivo.

5. Selecione a opção da lista suspensa **Serviço de nuvem**.

   Vários campos são exibidos para configuração.

6. Insira os detalhes nos campos a seguir para configurar e clique em **OK**:

   ID da chave de acesso

   Identifica o usuário que está solicitando acesso a este local.

   Chave de acesso confidencial

   Refere-se a uma senha que é usada para verificar a autenticidade da solicitação para acessar esse local porque sua chave de acesso não está criptografada.

   Importante: esta chave de acesso secreta é fundamental para manter a segurança de suas contas. É necessário manter as chaves e as credenciais da conta em um local seguro. Não incorpore a chave de acesso secreta em uma página da web ou em outro código-fonte de acesso público e não a transmita em canais não seguros.

   Configurações de proxy

   Especifica as configurações do servidor proxy. Marque a caixa de seleção **Conectar usando um servidor proxy** se desejar ativar esta opção. Caso selecione esta opção, será necessário incluir também o endereço IP (ou nome do computador) do servidor proxy e o número da porta correspondente, usado pelo servidor proxy em conexões com a internet. Pode-se também selecionar esta opção se o servidor proxy exigir autenticação. Será necessário fornecer as informações de autenticação correspondentes (nome de domínio/nome de usuário e senha) para usar o servidor proxy.

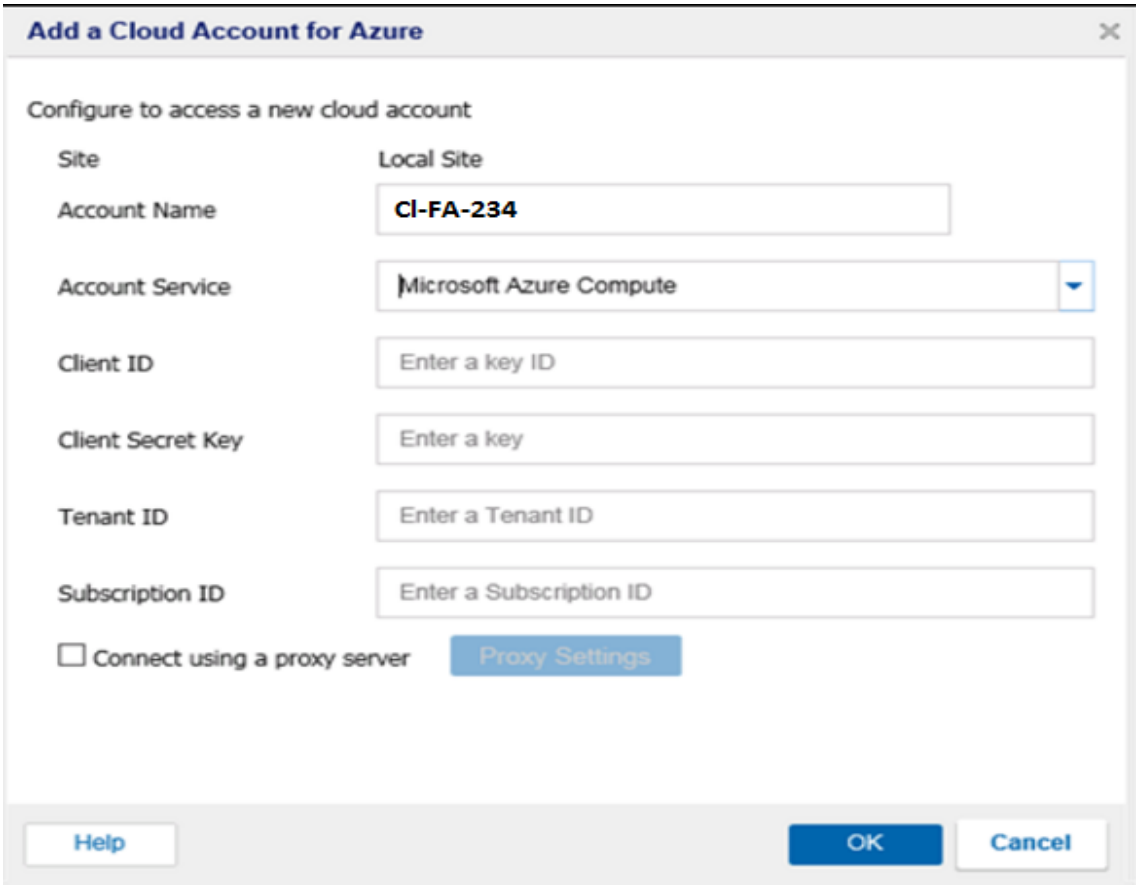
   A conta de nuvem é adicionada ao console.

   Observação: se você configurou a cópia de arquivo e o arquivo morto em versões do Arcserve UDP v6.0 ou versões anteriores e agora estiver atualizando para a versão mais recente do Arcserve UDP, para arquivo morto, o Arcserve UDP cria um novo compartimento de memória na nuvem com o sufixo **-fa**. A cópia de arquivo usa o mesmo compartimento de memória usado na versão anterior.

Adicionar uma conta de nuvem para Computação do Microsoft Azure

Adicione uma conta de nuvem da Computação do Microsoft Azure para copiar arquivos ou pontos de recuperação em um armazenamento na nuvem. É possível usar esta conta ao criar tarefas para os planos de modo de espera virtual para nuvem ou máquina virtual instantânea no Microsoft Azure.

Observação: para adicionar uma conta de nuvem para o Microsoft Azure, é necessário atender aos pré-requisitos. Para obter detalhes, consulte Pré-requisitos.



Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection e clique na guia **recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Contas da nuvem**.

   A página **Destinos: Contas da nuvem** é exibida no painel central.
3. Clique em **Adicionar uma conta de nuvem**.

   A página **Adicionar uma conta de nuvem** é exibida.
4. Para o **Nome da conta**, forneça um nome exclusivo.

O nome da conta especifica o nome do armazenamento na nuvem. Esse nome será adicionado ao console para identificar a conta da nuvem. Cada conta de nuvem deve ter um nome de armazenamento exclusivo.

5. Selecione a opção da lista suspensa **Conta de serviço**.

   Vários campos são exibidos para configuração.

6. Insira os detalhes nos campos a seguir para configurar e clique em **OK**:

   ID do cliente

   Refere-se à ID de aplicativo do aplicativo do Azure Active Directory. Copie sua ID de cliente preparada no editor de texto.

   Chave secreta do cliente

   Refere-se à chave de autenticação gerada para o aplicativo do Azure Active Directory que você digita como ID do cliente. Copie sua chave secreta de cliente preparada no editor de texto.

   Importante: Esta chave secreta é fundamental para manter a segurança de suas contas. É necessário manter as chaves e as credenciais da conta em um local seguro. Não incorpore a chave secreta em uma página da web ou em outro código-fonte publicamente acessível e não a transmita em canais não seguros.

   ID do locatário

   Refere-se à ID do Azure Active Directory na qual você criou o aplicativo do Azure Active Directory. Copie sua ID de locatário preparada no editor de texto.

   ID da assinatura

   Refere-se para um GUID (Globally Unique Identifier - Identificador Global Exclusivo) que identifica com exclusividade sua assinatura para usar os serviços do Azure. Copie sua ID de assinatura preparada no editor de texto.

   Configurações de proxy

   Especifica as configurações do servidor proxy. Selecione **Conectar usando um servidor proxy** para ativar essa opção. Caso selecione esta opção, será necessário incluir também o endereço IP (ou nome do computador) do servidor proxy e o número da porta correspondente, usado pelo servidor proxy em conexões com a internet. Pode-se também selecionar esta opção se o servidor proxy exigir autenticação. Será necessário fornecer as informações de autenticação correspondentes exigidas para usar o servidor proxy.

A conta de nuvem é adicionada ao console.

Pré-requisitos para adicionar uma conta de nuvem para o Microsoft Azure

Antes de criar uma conta de nuvem para o Microsoft Azure, você deve concluir as seguintes tarefas de pré-requisito obrigatórias na ordem fornecida:

1. Prepare os servidores a serem implantados como console do Arcserve UDP e o servidor de ponto de recuperação; esses servidores devem atender aos requisitos de sistema de cada componente.
2. Certifique-se de ter as permissões necessárias para criar um aplicativo no Azure Active Directory.

   Para obter instruções, consulte Verificar permissões do Azure Active Directory na documentação da Microsoft.
3. Crie um aplicativo do Azure Active Directory. Em um editor de texto (como o bloco de notas), copie a ID do aplicativo do aplicativo e o rótulo como ID do cliente.

   Para obter instruções, consulte Verificar permissões do Azure Active Directory na documentação da Microsoft.
4. Obtenha a ID do aplicativo e gere uma chave de autenticação para este aplicativo. Copie a cadeia de caracteres de chave de autenticação no editor de texto (como o bloco de notas) e rotule a cadeia de caracteres como chave secreta do cliente.

   Para obter instruções, consulte Obter chave de autenticação e ID do aplicativo na documentação da Microsoft.
5. Obtenha a ID do locatário, que é a ID do Azure Active Directory na qual você criou o aplicativo. Em um editor de texto (como o bloco de notas), copie a ID e rotule-a como ID do locatário.

   Para obter instruções, consulte Obter ID de locatário na documentação da Microsoft.
6. Execute as seguintes etapas para atribuir a função de colaborador para o aplicativo.
   a. No painel esquerdo do menu do Portal do Microsoft Azure, selecione **Assinaturas**.
   b. Selecione sua assinatura.
   c. Selecione a guia Controle de acesso (IAM).

d. Adicione o aplicativo.

e. Atribua a função de colaborador ao aplicativo.

Para obter detalhes, consulte Atribuir aplicativo à função na documentação da Microsoft.

7. Obtenha sua ID de assinatura do Azure.

Observação: a ID da assinatura é um GUID que identifica com exclusividade sua assinatura para usar os serviços do Azure.

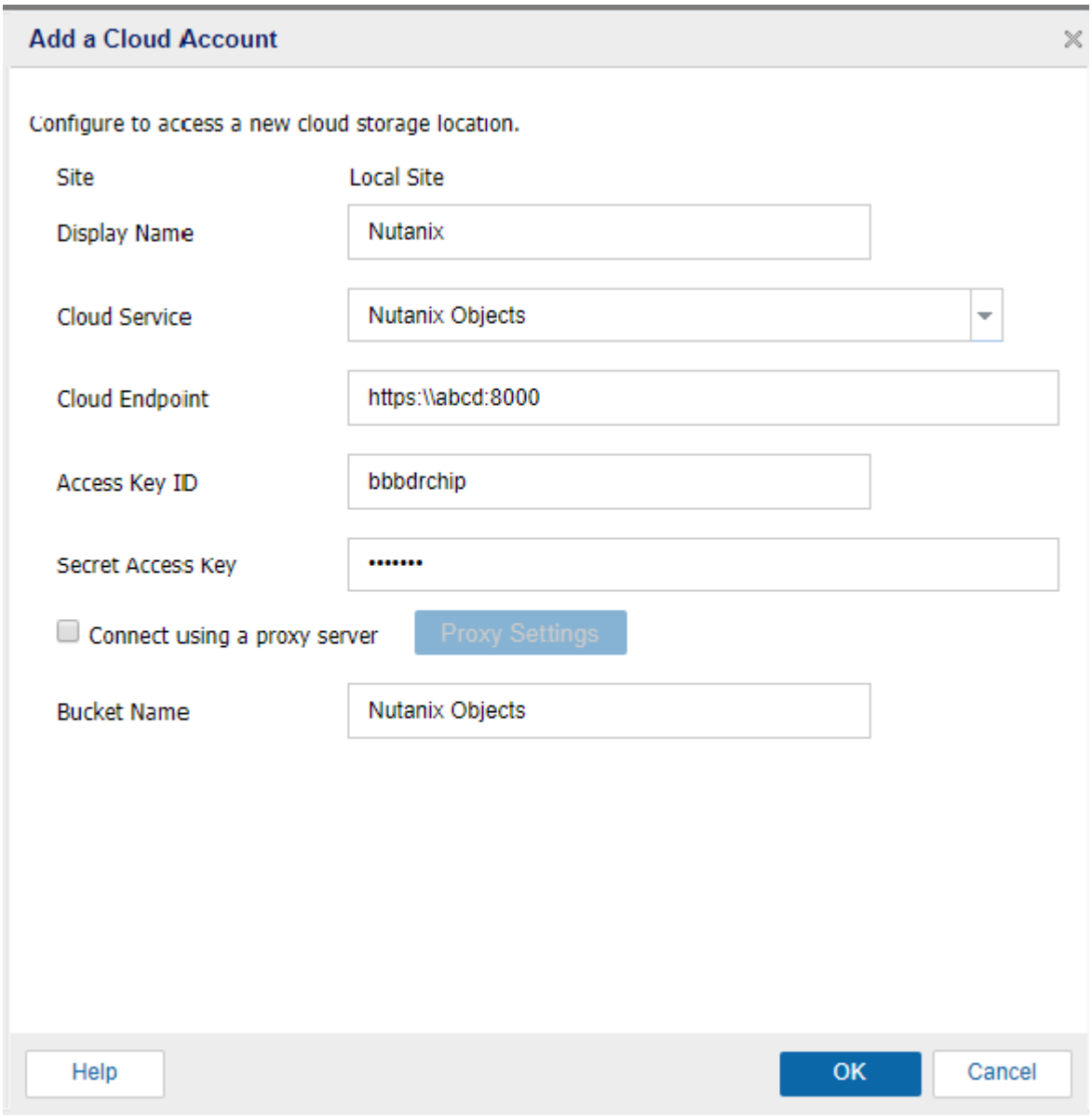
a. Faça logon no portal do Microsoft Azure.

b. No painel de navegação esquerdo, clique em Assinaturas.

A lista de suas assinaturas é exibida juntamente com a ID da assinatura.

Adicionar uma conta de nuvem para objetos Nutanix

Adicione uma conta de nuvem do Nutanix Objects para copiar arquivos ou pontos de recuperação em um armazenamento na nuvem. É possível usar essa conta durante a criação das tarefas Copiar ponto de recuperação/Cópia de arquivo/Arquivo morto.



Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection e clique na guia **recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Contas da nuvem**.

   A página **Destinos: Contas da nuvem** é exibida no painel central.
3. Clique em **Adicionar uma conta de nuvem**.

   A página **Adicionar uma conta de nuvem** é exibida.
4. Em **Nome de exibição**, forneça um nome exclusivo.

   Nome de exibição especifica o nome do armazenamento na nuvem. Esse nome será adicionado ao console para identificar a conta da nuvem. Cada conta de nuvem deve ter um nome de exibição exclusivo.
5. Selecione a opção da lista suspensa **Serviço de nuvem**.

Vários campos são exibidos para configuração.

6. Insira os detalhes nos campos a seguir para configurar e clique em **OK**:

Ponto de extremidade do armazenamento

Especifica o URL do serviço do fornecedor. Por exemplo, *http://[nome do servidor]:nº da porta*

ID da chave de acesso

Identifica o usuário que está solicitando acesso a este local.

Chave de acesso confidencial

Refere-se a uma senha que é usada para verificar a autenticidade da solicitação para acessar esse local porque sua chave de acesso não está criptografada.

Importante: esta chave de acesso secreta é fundamental para manter a segurança de suas contas. É necessário manter as chaves e as credenciais da conta em um local seguro. Não incorpore a chave de acesso secreta em uma página da web ou em outro código-fonte de acesso público e não a transmita em canais não seguros.

Configurações de proxy

Especifica as configurações do servidor proxy. Marque a caixa de seleção **Conectar usando um servidor proxy** se desejar ativar esta opção. Caso selecione esta opção, será necessário incluir também o endereço IP (ou nome do computador) do servidor proxy e o número da porta correspondente, usado pelo servidor proxy em conexões com a internet. Pode-se também selecionar esta opção se o servidor proxy exigir autenticação. Será necessário fornecer as informações de autenticação correspondentes (nome de domínio/nome de usuário e senha) para usar o servidor proxy.

Nome do compartimento de memória

Todos os arquivos e as pastas movidos ou copiados para o fornecedor de nuvem são armazenados e organizados nos seus compartimentos de memória. Os compartimentos de memória são como um contêiner para os arquivos e são usados para agrupar e organizar objetos. Cada objeto armazenado no fornecedor da nuvem é colocado em um compartimento de memória.

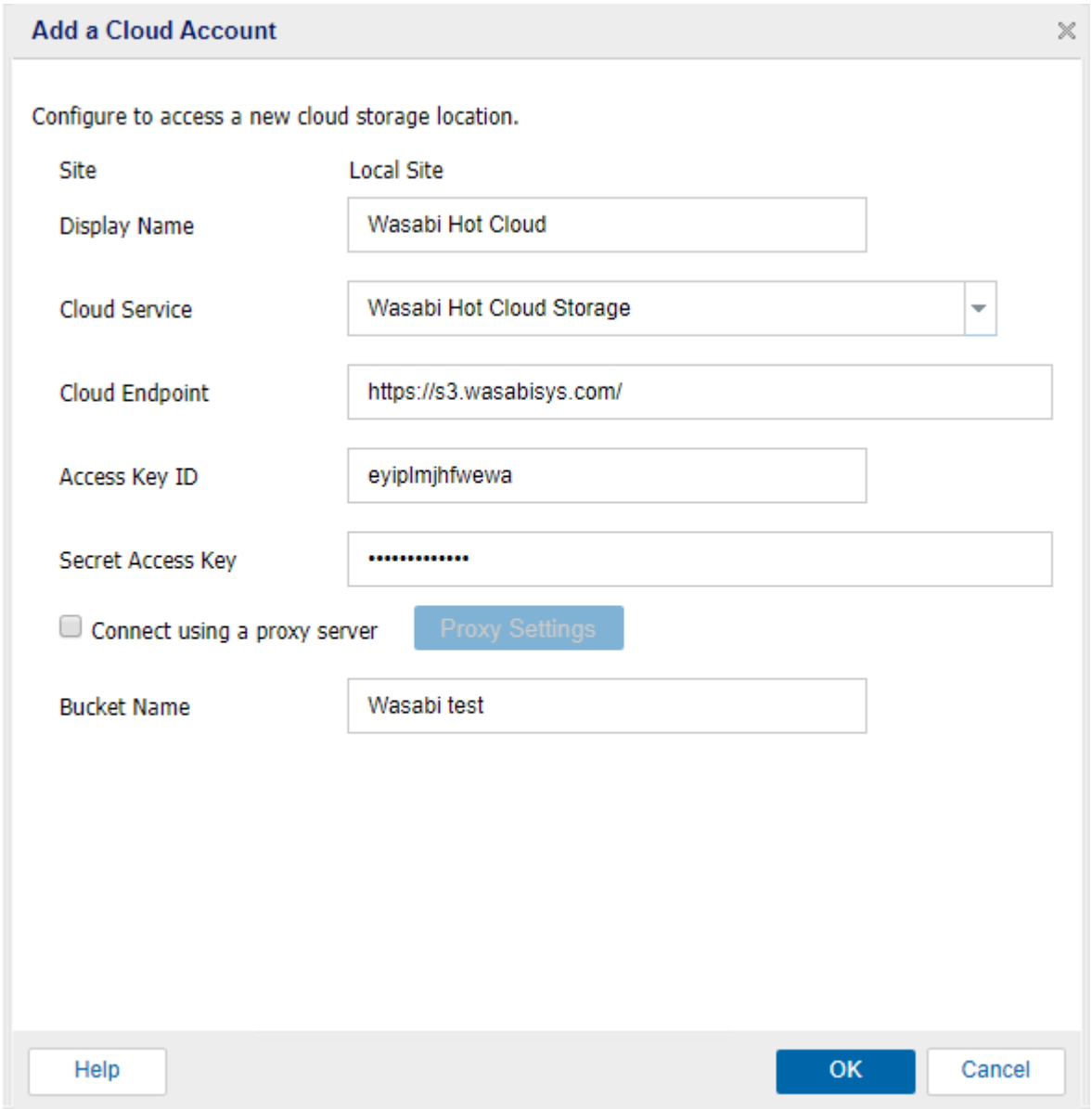
A conta de nuvem é adicionada ao console.

Observação: se você configurou a cópia de arquivo e o arquivo morto em versões do Arcserve UDP v6.0 ou versões anteriores e agora estiver atualizando para a versão mais recente do Arcserve UDP, para arquivo morto, o Arcserve UDP cria um

novo compartimento de memória na nuvem com o sufixo **-fa**. A cópia de arquivo usa o mesmo compartimento de memória usado na versão anterior.

Adicionar uma conta de nuvem para Wasabi Hot Cloud Storage

Adicione uma conta de nuvem do Wasabi Hot Cloud Storage para copiar arquivos ou pontos de recuperação em um armazenamento na nuvem. É possível usar essa conta durante a criação das tarefas Copiar ponto de recuperação/Cópia de arquivo/Arquivo morto.



Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection e clique na guia **recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Contas da nuvem**.

   A página **Destinos: Contas da nuvem** é exibida no painel central.
3. Clique em **Adicionar uma conta de nuvem**.

   A página **Adicionar uma conta de nuvem** é exibida.
4. Em **Nome de exibição**, forneça um nome exclusivo.

   Nome de exibição especifica o nome do armazenamento na nuvem. Esse nome será adicionado ao console para identificar a conta da nuvem. Cada conta de nuvem deve ter um nome de exibição exclusivo.
5. Selecione a opção da lista suspensa **Serviço de nuvem**.

   Vários campos são exibidos para configuração.
6. Insira os detalhes nos campos a seguir para configurar e clique em **OK**:

   Ponto de extremidade do armazenamento

   As três regiões a seguir são suportadas no Wasabi Hot Cloud Storage:

   - Para a região leste dos EUA: o ponto de extremidade é s3.wasabisys.com.
   - Para a região oeste dos EUA: o ponto de extremidade é s3.us-west-1.wasabisys.com
   - Para a região central da UE: o ponto de extremidade é s3.eu-central-1.wasabisys.com

   ID da chave de acesso

   Identifica o usuário que está solicitando acesso a este local.

   Chave de acesso confidencial

   Refere-se a uma senha que é usada para verificar a autenticidade da solicitação para acessar esse local porque sua chave de acesso não está criptografada.

   Importante: esta chave de acesso secreta é fundamental para manter a segurança de suas contas. É necessário manter as chaves e as credenciais da conta em um local seguro. Não incorpore a chave de acesso secreta em uma página da web ou em outro código-fonte de acesso público e não a transmita em canais não seguros.

   Configurações de proxy

   Especifica as configurações do servidor proxy. Marque a caixa de seleção **Conectar usando um servidor proxy** se desejar ativar esta opção. Caso selecione esta opção, será necessário incluir também o endereço IP (ou nome do

computador) do servidor proxy e o número da porta correspondente, usado pelo servidor proxy em conexões com a internet. Pode-se também selecionar esta opção se o servidor proxy exigir autenticação. Será necessário fornecer as informações de autenticação correspondentes (nome de domínio/nome de usuário e senha) para usar o servidor proxy.

Nome do compartimento de memória

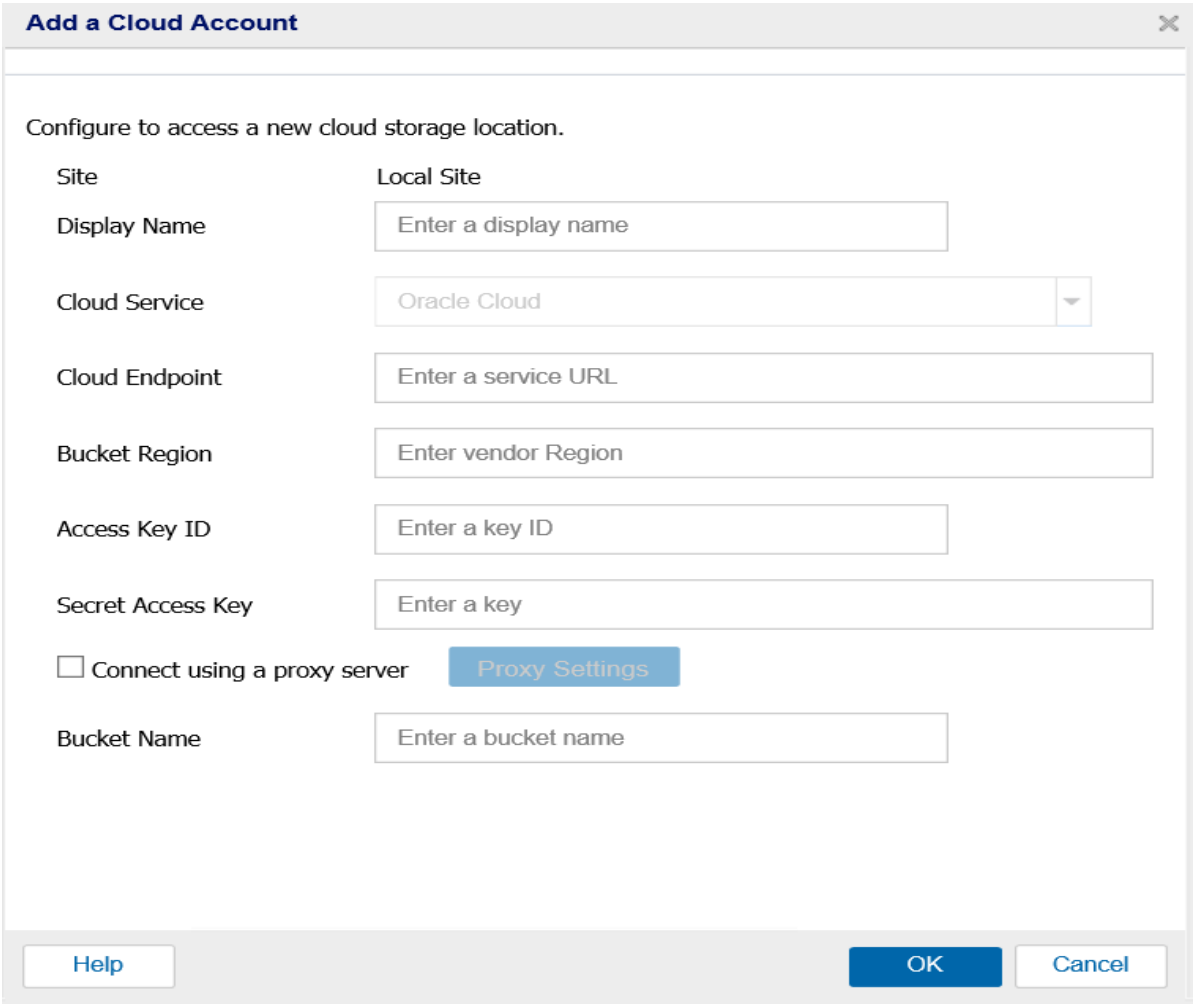
Todos os arquivos e as pastas movidos ou copiados para o fornecedor de nuvem são armazenados e organizados nos seus compartimentos de memória. Os compartimentos de memória são como um contêiner para os arquivos e são usados para agrupar e organizar objetos. Cada objeto armazenado no fornecedor da nuvem é colocado em um compartimento de memória.

A conta de nuvem é adicionada ao console.

Observação: se você configurou a cópia de arquivo e o arquivo morto em versões do Arcserve UDP v6.0 ou versões anteriores e agora estiver atualizando para a versão mais recente do Arcserve UDP, para arquivo morto, o Arcserve UDP cria um novo compartimento de memória na nuvem com o sufixo **-fa**. A cópia de arquivo usa o mesmo compartimento de memória usado na versão anterior.

Adicionar uma conta de nuvem para Oracle Cloud

Adicione uma conta de nuvem do Oracle para copiar arquivos ou pontos de recuperação em um armazenamento na nuvem. É possível usar essa conta durante a criação das tarefas Copiar ponto de recuperação/Cópia de arquivo/Arquivo morto.



Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection e clique na guia **recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Contas da nuvem**.

   A página **Destinos: Contas da nuvem** é exibida no painel central.
3. Clique em **Adicionar uma conta de nuvem**.

   A página **Adicionar uma conta de nuvem** é exibida.
4. Em **Nome de exibição**, forneça um nome exclusivo.

Nome de exibição especifica o nome do armazenamento na nuvem. Esse nome será adicionado ao console para identificar a conta da nuvem. Cada conta de nuvem deve ter um nome de exibição exclusivo.

5. Selecione a opção da lista suspensa **Serviço de nuvem**.

   Vários campos são exibidos para configuração.

6. Insira os detalhes nos campos a seguir para configurar e clique em **OK**:

   Ponto de extremidade de nuvem

   Especifica o URL do serviço do fornecedor. Por exemplo, *https://-namespace.compat.objectstorage.region.oraclecloud.com*

   Região de compartimento de memória

   Refere-se à região do compartimento de memória do fornecedor.

   ID da chave de acesso

   Identifica o usuário que está solicitando acesso a este local.

   Chave de acesso confidencial

   Refere-se a uma senha que é usada para verificar a autenticidade da solicitação para acessar esse local porque sua chave de acesso não está criptografada.

   Importante: esta chave de acesso secreta é fundamental para manter a segurança de suas contas. É necessário manter as chaves e as credenciais da conta em um local seguro. Não incorpore a chave de acesso secreta em uma página da web ou em outro código-fonte de acesso público e não a transmita em canais não seguros.

   Configurações de proxy

   Especifica as configurações do servidor proxy. Marque a caixa de seleção **Conectar usando um servidor proxy** se desejar ativar esta opção. Caso selecione esta opção, será necessário incluir também o endereço IP (ou nome do computador) do servidor proxy e o número da porta correspondente, usado pelo servidor proxy em conexões com a internet. Pode-se também selecionar esta opção se o servidor proxy exigir autenticação. Será necessário fornecer as informações de autenticação correspondentes (nome de domínio/nome de usuário e senha) para usar o servidor proxy.

   Nome do compartimento de memória

   Todos os arquivos e as pastas movidos ou copiados para o fornecedor de nuvem são armazenados e organizados nos seus compartimentos de memória. Os compartimentos de memória são como um contêiner para os arquivos e são usados

para agrupar e organizar objetos. Cada objeto armazenado no fornecedor da nuvem é colocado em um compartimento de memória.

A conta de nuvem é adicionada ao console.

Observação: se você configurou a cópia de arquivo e o arquivo morto em versões do Arcserve UDP v6.0 ou versões anteriores e agora estiver atualizando para a versão mais recente do Arcserve UDP, para arquivo morto, o Arcserve UDP cria um novo compartimento de memória na nuvem com o sufixo **-fa**. A cópia de arquivo usa o mesmo compartimento de memória usado na versão anterior.

Adicionar uma conta de nuvem do Arcserve

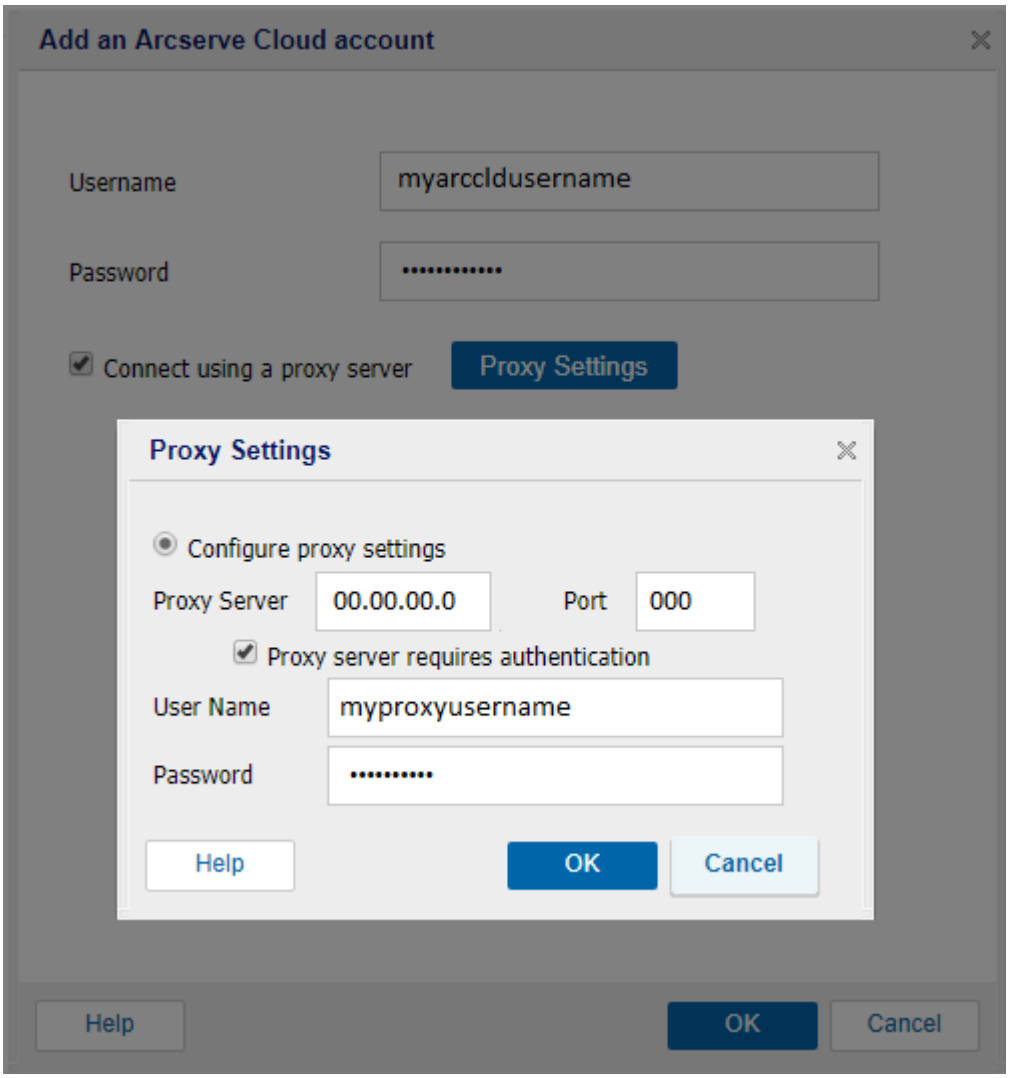
Adicione uma conta de nuvem do Arcserve para copiar arquivos ou pontos de recuperação em um armazenamento na nuvem do Arcserve.

Siga estas etapas:

1. Efetue logon no Arcserve UDP e clique na guia **Recursos**.
2. No painel à esquerda, vá até **Destinos** e clique em **Nuvem do Arcserve**.

   A tela Destinos: nuvem do Arcserve será exibida.
3. Clique em **Adicionar uma conta de nuvem do Arcserve**.

   A tela Adicionar uma conta de nuvem do Arcserve será exibida.



4. Digite os seguintes detalhes:

Nome de usuário

Especifica o nome de usuário da conta de nuvem do Arcserve que está registrada no Arcserve.

Senha

Especifica a senha do usuário correspondente da conta de nuvem do Arcserve que está registrada no Arcserve.

Conectar usando um servidor proxy

Selecione esta opção para se conectar à nuvem do Arcserve usando um servidor proxy que tenha conexão com a internet.

Configurações de proxy

Clique em Configurações de proxy se a opção Conectar usando um servidor proxy for selecionada.

A janela Configurações de proxy será exibida. Digite os detalhes a seguir e clique em **OK**.

Servidor proxy

Especifica o endereço IP do servidor proxy.

Porta

Especifica o número da porta que está aberta no servidor proxy.

O servidor proxy exige autenticação

Selecione esta opção se desejar que o acesso ao servidor proxy exija autenticação.

Nome de usuário

Especifica o nome de usuário que tem acesso ao servidor proxy.

Senha

Especifica a senha da conta do usuário correspondente que tem acesso ao servidor proxy.

5. Clique em **OK**.

   A conta de nuvem do Arcserve será adicionada com êxito.

Como gerenciar um repositório de dados

Depois de criar um repositório de dados, talvez seja necessário executar várias operações, como modificar, excluir, interromper e iniciar um repositório de dados.

Também é possível executar tarefas de mesclagem sob demanda para vários nós para criar mais espaço em um repositório de dados.

O que fazer a seguir?

- Verificar pré-requisitos
- Modificar um repositório de dados
- Excluir um repositório de dados do console
- Interromper um repositório de dados
- Iniciar um repositório de dados
- Monitorar a capacidade de espaço do repositório de dados
- Procurar pontos de recuperação em um repositório de dados
- Excluir os dados do nó de um repositório de dados
- Modificar o limite de nós ativos simultâneos para backup manual
- Executar uma tarefa de mesclagem manual ou por demanda
- Solução de problemas: como usar um repositório de dados quando a pasta de destino do backup está cheio

Verificar os pré-requisitos

Para gerenciar um repositório de dados, execute os seguintes pré-requisitos:

- Você já adicionou um repositório de dados.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Modificar um repositório de dados

É possível modificar um repositório de dados existente. No entanto, existem algumas restrições e não será possível modificar os seguintes detalhes de um repositório de dados:

- Detalhes da compactação
- De um repositório de dados sem redução de redundância para um repositório de dados de redução de redundância ou de um repositório de dados de redução de redundância para um repositório de dados sem redução de redundância.
- Opções de redução de redundância: Remover redundância de dados e Tamanho do bloco de redução de redundância.

Considerações antes da modificação de um repositório de dados:

- Se alterar o caminho do repositório de dados ou a senha de criptografia, todas as tarefas em execução nesse repositório de dados, incluindo as tarefas que aguardam na fila, serão canceladas. Qualquer alteração no nome do repositório de dados, tamanho da memória hash ou número de nós ativos simultâneos não afetará as tarefas em execução.
- Para repositórios de dados sem redução de redundância: para alterar o caminho do repositório de dados, mantenha a pasta de destino de backup vazia.
- Para repositórios de dados de redução de redundância: para alterar o caminho do repositório de dados, mantenha as seguintes pastas vazias:
  - Pasta de destino do backup
  - Destino de Dados
  - Destino do índice
  - Destino de hash
- As opções **Senha de criptografia** serão editáveis somente se tiver selecionado a opção **Criptografar dados** ao criar o repositório de dados.

Siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Destinos** e clique em **Servidores de ponto de recuperação**.

   A página **Destinos: Servidores do ponto de recuperação** exibe a lista de servidores de ponto de recuperação disponíveis.
3. Expanda um servidor do ponto de recuperação.

É possível ver a lista de repositórios de dados associados ao servidor do ponto de recuperação.

4. Execute uma das seguintes ações:
   - Clique com o botão direito do mouse no nome do repositório de dados.
   - Selecione o repositório de dados e, no painel central, clique no menu suspenso **Ações**.

   Uma lista de opções é exibida.
5. Clique em **Modificar**.

   A página **Modificar um repositório de dados** é exibida.
6. Atualize os campos necessários e clique em **Salvar**.

   Servidor de ponto de recuperação

   Define o servidor de ponto de recuperação em que o repositório de dados foi criado. O servidor de ponto de recuperação já está adicionado por padrão.

   Nome do repositório de dados

   Define o nome do repositório de dados.

   Pasta do repositório de dados

   Define o local da pasta na qual o repositório de dados foi criado. Clique em Procurar para selecionar a pasta de destino.

   Observações:

   - Agora você pode ativar e exibir volumes ocultos. Para obter mais informações, consulte Como ativar e exibir volumes ocultos ao criar um repositório de dados.
   - para o repositório de dados de redução de redundância e de não redução de redundância, o caminho de destino deve ser uma pasta vazia.

   Limite de nós ativos simultâneos

   Especifica o número máximo de tarefas simultâneas no repositório de dados.

   Valor padrão: 4

   refere-se a um valor de 1 a 9999. O valor indica o número de tarefas que podem ser executadas simultaneamente. Se a execução de tarefas atender o número, outra tarefa será colocada na fila e apenas poderá ser iniciada apenas quando uma das tarefas em execução for concluída. A tarefa concluída pode significar uma tarefa concluída, cancelada ou com falha.

   O número se aplica aos tipos de tarefas, mas não aos nós do servidor. Por exemplo, número 5 indica que cinco tarefas de backup estão em execução.

Qualquer tarefa programada após as cinco tarefas de backup aguarda na fila, mas é possível enviar outra tarefa, como Catálogo do sistema de arquivos.

Se o valor for superior a 16 ou 32, sertão exibidas mensagens para avisar sobre a maior demanda no hardware.

Observação: limitar a quantidade afeta apenas a tarefa de saída de replicação e não a tarefa de entrada de replicação. Limitar a quantidade não afeta a restauração ou as tarefas de BMR. Essas tarefas não são colocadas em uma fila.

Ativar a redução de redundância

Especifica que a redução de redundância está ativada para o repositório de dados. O Arcserve UDP suporta dois tipos de redução de redundância: redução de redundância do lado da origem e a redução de redundância global. A redução de redundância do lado da origem impede que os blocos de dados duplicados se movam na rede de um determinado agente. A redução de redundância global elimina os dados duplicados em todos os computadores cliente com base no nível de agrupamento do volume.

Tamanho do bloco de redução de redundância

Define o tamanho do bloco de redução de redundância. As opções são: 4 KB, 8 KB, 16 KB, 32 KB e 64 KB. O tamanho do bloco de redução de redundância também afeta a estimativa da capacidade de redução de redundância. Por exemplo, se você alterar o valor padrão de 16 KB para 32 KB, as estimativas de capacidade de redução de redundância duplicarão. O aumento do tamanho de bloco de redução de redundância pode diminuir o percentual de redução de redundância.

Alocação de memória hash

Especifica a quantidade de memória física alocada para manter os hashes. Esse campo é preenchido previamente com um valor padrão. O valor padrão baseia-se no seguinte cálculo:

Se a memória física do RPS for menor do que 4 GB (ou igual a 4 GB), o valor padrão de **Alocação de memória hash** será idêntico para a memória física do RPS.

Se a memória física do RPS for maior do que 4 GB, o Arcserve UDP calcula a memória livre disponível no momento. Suponha que a memória livre disponível seja X GB no momento. O Arcserve UDP verifica também as seguintes condições:

- Se (X * 80%) > = 4 GB, o valor padrão de **Alocação de memória hash** é (X * 80%).
- Se (X * 80%) < 4 GB, o valor padrão de **Alocação de memória hash** é 4 GB.

Exemplo: considere que o RPS tem 32 GB de memória física. Suponhamos que o sistema operacional e outros aplicativos usem 4 GB de memória durante a criação do repositório de dados. Portanto, a memória livre disponível no momento é de 28 GB. Então, o valor padrão de **Alocação de memória hash** é 22.4 GB (22.4 GB = 28 GB * 80%).

O destino de hash está em uma SSD (Solid State Drive – Unidade de Estado Sólido)

Especifica se a pasta de hash está em uma unidade de estado sólido.

Observação: configure o destino de hash no SSD local se o destino de Hash que está em uma opção SSD (Solid State Drive - Unidade de Estado Sólido) estiver ativado

Destino de Dados

Define a pasta de destino de dados para salvar os blocos de dados reais exclusivo. Use o maior tamanho de disco para armazenar dados naquele que contém os blocos de dados originais de origem.

Observação: o caminho **Destino dos dados** deve ser uma pasta vazia.

Destino do índice

Define a pasta de destino do índice para armazenar os arquivos de índice. Escolha um disco diferente para melhorar o processamento de redução de redundância.

Observação: o caminho **Destino de índice** deve ser uma pasta vazia.

Destino de hash

Define o caminho para armazenar o banco de dados de hash. O Arcserve UDP usa o algoritmo SHA1 para gerar o hash para os dados de origem. Os valores de hash são gerenciados pelo banco de dados de hash. Selecionar uma SSD (Solid State Drive – Unidade de Estado Sólido) de alta velocidade aumenta a capacidade de redução de redundância e exige uma alocação de memória menor. Para melhorar o desempenho de hash, é recomendável formatar o volume SSD como o sistema de arquivos NTFS com o tamanho do agrupamento do volume de 4KB.

Observação: o caminho de **Destino de hash** deve ser uma pasta vazia.

Observação: não é possível especificar o mesmo caminho para as quatro seguintes pastas: **Repositório de dados, Destino dos dados, Destino do índice** e **Destino de hash**.

Ativar compactação

Especifica se as configurações de compactação de dados estão ativadas.

Tipo de compactação

Especifica se é preciso usar o tipo de compactação padrão ou máxima.

A compactação geralmente é selecionada para reduzir o uso de espaço em disco, mas também tem um impacto inverso sobre a velocidade do backup, devido ao aumento no uso da CPU. Com base nos seus requisitos, é possível selecionar uma das três opções disponíveis.

Observação: para obter mais informações, consulte Tipo de compactação.

Ativar criptografia

Especifica se as configurações de criptografia estão ativadas. Ao selecionar essa opção, especifique e confirme a senha criptografada.

A criptografia de dados é a conversão de dados em uma forma ininteligível sem um mecanismo decodificador. A solução Arcserve Unified Data Protection usa algoritmos de criptografia AES (Advanced Encryption Standard – Padrão de criptografia avançada) seguros para atingir o máximo de segurança e privacidade dos seus dados. Os repositórios de dados podem ser usados com ou sem criptografia. Para criptografia, apenas AES-256 está disponível.

A senha não será obrigatória caso esteja tentando restaurar no computador em que o backup foi executado. No entanto, caso esteja tentando restaurar em um computador diferente, a senha será necessária. Por padrão, a senha é obrigatória apenas para o primeiro logon. Para informar a senha mesmo após o primeiro logon, o administrador precisará interromper manualmente o serviço Arcserve UDP Agent Explorer Extension.

Enviar um alerta por email quando um destino estiver se aproximando da capacidade máxima

A seleção dessa opção configura o repositório de dados para enviar um alerta por email. O RPS envia alertas por email aos destinatários quando a pasta de destino do repositório de dados está se aproximando da capacidade máxima.

Configurar email

Esse botão só é exibido quando você ativa a opção *Enviar um alerta por email quando um destino estiver se aproximando da capacidade máxima*. Ele ajuda você a fornecer a ID de email para o recebimento de alertas. Clique no botão **Configurar email** para carregar as configurações globais de alerta por email em Console > Configurações > Configuração de email e alerta. Se as configurações globais de email não estiverem disponíveis, quando você clicar no botão**Configurar email**, será aberta a caixa de diálogo**Configurações de email** para você definir os detalhes de email.

O repositório de dados é atualizado.

Modificar o Limite de repositório de dados

Este tópico traz informações sobre locais de registro de limite, nome de chave de limite e valores padrão, explica quando um erro de limite ou uma mensagem de aviso é exibida e demonstra como modificar o limite de um repositório de dados.

Os repositórios de dados têm uma configuração de limite de capacidade de espaço que ajuda a monitorar as informações de uso de espaço livre do destino deles. No repositório de dados de redução de redundância, os limites monitoram a memória alocada para o destino de hash e o espaço em disco alocado para a pasta de destino de backup, de destino de índice e de destino de dados. Para repositórios de dados sem redução de redundância, o limite monitora o espaço de armazenamento somente para a pasta de destino do backup. Os cinco itens dos monitores de limite têm dois tipos de valor:

- Limite de erro
- Limite de aviso

O valor de limite é salvo no registro do sistema. Você pode modificar o valor padrão manualmente.

Locais de registro de limites

1. Pasta do repositório de dados: [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\DataStore\XXXXXXX\CommStore]
2. Destino dos dados de redução de redundância:[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\DataStore\XXXXXXX\GDD\DataRole]
3. Memória e destino do hash de redução de redundância: [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\DataStore\XXXXXXX\GDD\HashRole]

   Observação: a função de hashing monitora a memória e o uso de disco. Caminho representa o uso do disco e Mem representa a memória.
4. Destino de índice da redução de redundância: [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\DataStore\XXXXXXX\GDD\IndexRole]

Nomes de chave de limite e valores padrão

Tipo de caminho	Tipo de limite	Nome da chave de registro	Valor padrão	Valor padrão (Antes da versão 6.5, atualização 1)

Pasta do repositório de dados	Aviso	WarnPathThreshold	0,05	0,03
	Erro	ErrorPathThreshold	2048	100
Caminho do índice de redução da redundância	Aviso	WarnPathThreshold	0,05	0,03
	Erro	ErrorPathThreshold	2048	100
Caminho do hash de redução de redundância	Aviso	WarnPathThreshold	0,05	0,03
	Erro	ErrorPathThreshold	2048	100
Caminho da função de dados de redução de redundância	Aviso	WarnPathThreshold	0,05	0,03
	Erro	ErrorPathThreshold	2048	100
Memória	Aviso	WarnMemThreshold	0,05	0,03
	Erro	ErrorMemThreshold	30	10

- Um valor inferior a 1 indica a porcentagem de espaço livre; por exemplo, 0,05 significa 5%. Se o espaço livre equivale a menos de 5% do tamanho do espaço total, é atingido o limite de aviso.
- Um valor superior ou igual a 1 indica o tamanho real de espaço livre; a unidade usada é MB. Por exemplo, o padrão 2048 significa 2.048 MB. Se o espaço livre é inferior a 2.048 MB, é atingido o limite de erro.

O valor padrão de limite é projetado para manter o desempenho ideal do repositório de dados. Você pode alterar os valores de limite. No entanto, não recomendamos que você altere esses valores, a menos que seja necessário mais espaço.

Siga as seguintes etapas para modificar o limite:

1. Navegue até o respectivo local do registro.
2. Altere manualmente o valor padrão de limite.

Modificar somente o destino de Hash

Quando um repositório de dados de redução de redundância for alterado, apenas o destino do caminho de hash pode ser alterado para uma pasta vazia. O Arcserve UDP gera novamente o caminho de hash para o novo repositório de dados. Esse processo é útil quando a pasta de hash está sem espaço e todas as tarefas foram canceladas. Você pode modificar o repositório de dados e fornecer uma nova pasta de destino de hash.

Como alternar os modos de destino de hash

Ao criar um repositório de dados de redução de redundância, você especifica se o destino de hash está em uma Unidade de estado sólido (modo SSD) ou na unidade de disco rígido (modo RAM). Se você configurar o disco rígido como o destino de hash, você precisará de mais memória para processar as chaves de hash. Como resultado, quando o tamanho do backup crescer, toda sua memória poderá ser esgotada. Nesse caso, você pode adicionar um SSD para fazer backup de mais dados. Da mesma forma, se tiver configurado um SSD como o destino de hash, você precisará de menos memória para processar as chaves de hash. No entanto, se estiver movendo para um computador com mais memória, talvez você deseje alternar para o modo de RAM para um processamento mais rápido de hash.

Para alternar o destino de um hash de RAM para SSD ou de SSD para uma RAM, o Arcserve UDP permite modificar um repositório de dados existente e alterar o modo, conforme necessário.

É possível modificar um repositório de dados existente, mesmo quando ele está em execução, mas o repositório de dados é reiniciado após você salvar a alteração.

Alterando de RAM para o modo SSD

Ao alternar da RAM para o modo SSD, você precisaria de menos memória. Portanto, o Arcserve UDP automaticamente diminui o valor mínimo de "Alocação de memória hash". No entanto, é possível alterar manualmente a alocação de memória hash. Neste caso, pode-se alterar as pastas de destino de hash para SSD. Quando você altera o destino de hash, o Arcserve UDP copia automaticamente os arquivos de hash para o novo local no SSD.

Alterando de SSD para o modo RAM

Ao alternar do SSD para o modo RAM, a RAM deve ser grande o suficiente para acomodar o repositório de dados hash atual. Por exemplo, antes da alteração, o repositório de dados criou 30 GB de arquivos hash em SSD. Agora, após a alteração, você deverá alocar, no mínimo, uma memória de 30 GB para os arquivos hash. Se a RAM não for suficiente, a alternância falhará. Nesse caso, o Arcserve UDP aumentará automaticamente os dois parâmetros a seguir:

- O valor mínimo de alocação de memória hash
- Alocação de memória hash

Isso assegura que o repositório de dados seja iniciado após a modificação.

Nesse caso, pode-se alterar as pastas de destino de hash para a unidade de disco rígido. Quando você altera o destino de hash, o Arcserve UDP copia automaticamente os arquivos de hash para o novo local na unidade de disco rígido.

Iniciar um repositório de dados

Caso você tenha interrompido um repositório de dados em execução para qualquer verificação de manutenção de rotina, é possível reiniciar o repositório de dados após a conclusão da verificação de manutenção. Quando você inicia o repositório de dados, as tarefas pendentes serão iniciadas no ponto em que foram interrompidas.

Observação: para iniciar um repositório de dados de redução de redundância, dependendo do tamanho do hash, os dados de hash demoram para serem carregados do disco rígido para a memória. No painel direito, o progresso do repositório de dados é exibido em porcentagem.

Siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Destinos** e clique em **Servidores de ponto de recuperação**.

   A página **Destinos: Servidores do ponto de recuperação** exibe a lista de servidores de ponto de recuperação disponíveis.
3. Expanda um servidor do ponto de recuperação.

   É possível ver a lista de repositórios de dados associados ao servidor do ponto de recuperação.
4. Execute uma das seguintes ações:
   - Clique com o botão direito do mouse no nome do repositório de dados.
   - Selecione o repositório de dados e, no painel central, clique no menu suspenso **Ações**.

   Uma lista de opções é exibida.
5. Clique em **Iniciar**.

   O painel direito exibe as informações de que o repositório de dados está sendo iniciado. O ícone de status do repositório de dados selecionado é alterado de **Interrompido** para **Em execução**.

Interromper um repositório de dados

Se você não quiser que um repositório de dados execute, use a opção de parado. Interromper o repositório de dados garante que nenhuma tarefa esteja em execução.

Observações:

- Se interromper um repositório de dados, todas as tarefas em execução, incluindo as tarefas em espera na fila, nesse repositório de dados serão canceladas.
- Se interromper um repositório de dados enquanto uma tarefa de replicação estiver em andamento, ao reiniciar o repositório de dados, a tarefa de replicação começará na mesma posição em que foi interrompida no repositório de dados.
- Se você interromper um repositório de dados enquanto uma tarefa de replicação (por exemplo, Tarefa-10) estiver em andamento e se, nesse período, mais duas tarefas de backup (por exemplo, Tarefa-11 e Tarefa-12) forem concluídas, ao reiniciar o repositório de dados, as tarefas de replicação serão concluídas na sequência (Tarefa-10, Tarefa-11, Tarefa-12 respectivamente).

Siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Destinos** e clique em **Servidores de ponto de recuperação**.

   A página **Destinos: Servidores do ponto de recuperação** exibe a lista de servidores de ponto de recuperação disponíveis.
3. Expanda um servidor do ponto de recuperação.

   É possível ver a lista de repositórios de dados associados ao servidor do ponto de recuperação.
4. Execute uma das seguintes ações:
   - Clique com o botão direito do mouse no nome do repositório de dados.
   - Selecione o repositório de dados e, no painel central, clique no menu suspenso **Ações**.

   Uma lista de opções é exibida.
5. Clique em **Parar**.

   A caixa de diálogo **Confirmar** é exibida.
6. Selecione **Sim** para parar.

O painel direito exibe as informações de que o repositório de dados está sendo parado.

O repositório de dados para e o ícone de status para o repositório de dados selecionado é alterado de **Em execução** para **Parado**.

Excluir um repositório de dados do console

Se não desejar mais usar um repositório de dados, será possível exclui-lo. Quando excluído, o repositório é removido do console. No entanto, o repositório de dados excluído existirá no servidor de ponto de recuperação.

Observações:

- É possível importar o repositório de dados excluído, se necessário.
- Para excluir um repositório de dados vinculado a planos, é preciso primeiro excluir o plano vinculado ao repositório de dados.

Siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Destinos** e clique em **Servidores de ponto de recuperação**.

   A página **Destinos: Servidores do ponto de recuperação** exibe a lista de servidores de ponto de recuperação disponíveis.
3. Expanda um servidor do ponto de recuperação.

   É possível ver a lista de repositórios de dados associados ao servidor do ponto de recuperação.
4. Execute uma das seguintes ações:
   - Clique com o botão direito do mouse no nome do repositório de dados.
   - Selecione o repositório de dados e, no painel central, clique no menu suspenso **Ações**.

   Uma lista de opções é exibida.
5. Clique em **Excluir**.

   A caixa de diálogo **Confirmação** é exibida.

   Observação: se o repositório de dados estiver vinculado a um plano, em vez da caixa de diálogo Confirmar, será exibida a caixa de diálogo **Aviso**.
6. Clique em **Sim**.

   O repositório de dados é removido.

Excluir os dados do nó de um repositório de dados

Como um administrador de armazenamento, é possível excluir dados de nós cujo backup foi feito a partir de um repositório de dados para liberar espaço e, de forma efetiva, gerenciar o espaço de armazenamento. O Arcserve UDP permite que você selecione os dados do nó em um repositório de dados e os exclua. É possível selecionar vários nós em um repositório de dados. Você pode excluir qualquer tipo de dados do nó, incluindo dados com redução de redundância e dados criptografados. O repositório de dados deve estar no estado de execução quando você iniciar essa tarefa, denominada tarefa de limpeza.

Observação: você poderá excluir somente quando o nó não estiver executando nenhuma tarefa (por exemplo, uma tarefa de backup/restauração/mesclagem).

Siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. Clique no repositório de dados que contém os dados do nós que deseja excluir.
3. A página **Resumo de pontos de recuperação** aparece.
4. Selecione o nó que deseja excluir.

   Aviso! Só selecione, não clique no nome do nó. Clicar no nome do nó redireciona para outra página na qual é possível executar a ação de exclusão.
5. Clique em **Ações**, **Excluir**.

   Observação: se você estiver usando o repositório de dados de redução de redundância, após a exclusão dos pontos de recuperação de um nó, o espaço em disco poderá não ser liberado imediatamente. O atraso ocorre porque para o repositório de dados de redução de redundância:

   - O processo de eliminação e recuperação em back-end é programado durante o tempo ocioso do repositório de dados.
   - Parte dos blocos de dados dos pontos de recuperação excluídos desse nó ainda pode ser usada pelo pontos de recuperação de outros nós.

     O volume de recuperação do espaço em disco depende do índice de redução de redundância do nó que você deseja excluir.
6. Confirme se deseja excluir os dados do nó.

   A tarefa de limpeza é iniciada e os dados do nó são excluídos da origem de dados. Você pode ver o status da tarefa de limpeza de logs e de **Eventos recentes**.

Monitorar a capacidade de espaço do repositório de dados

Os repositórios de dados do Arcserve UDP são criados no volume do RPS ou em discos compartilhados remotos. O mecanismo de monitoramento da capacidade de espaço do repositório de dados ajuda a acompanhar o uso da pasta de destino quando o destino está se aproximando da capacidade máxima. Quando o espaço livre na pasta de destino não é suficiente para executar o repositório de dados, pode ser enviado um alerta por email se a configuração de alertas por email do repositório de dados está ativada. Nesse caso, o log de atividades apresenta a saída. Durante esse período, o status dos repositórios de dados é alterado para Somente restaurar. Como resultado, as novas tarefas de backup/replicação são bloqueadas.

O monitoramento inclui as seguintes opções:

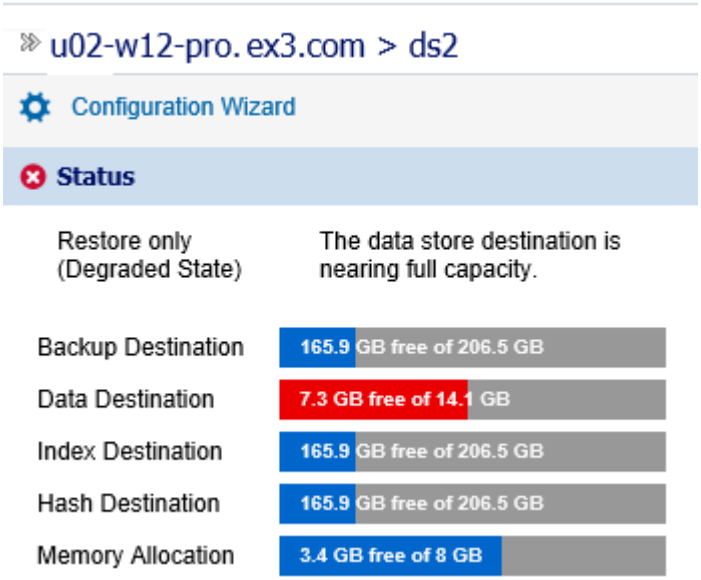
- Modificar o Limite de repositório de dados
- Usar limite de erro
- Usar limite de aviso
- Ativar alerta por email e compreender o formato de email

Usar limite de erro

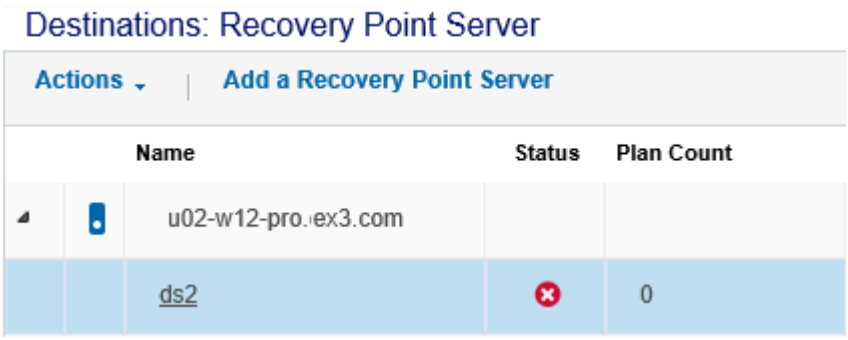
O limite de erro indica a ausência do espaço livre necessário para executar o repositório de dados. Além disso, alguns componentes de kernel podem não funcionar corretamente. Nesse caso, se não o repositório de dados não é interrompido de maneira manual, o status dele é alterado automaticamente para Restaurar somente.

Quando o espaço livre do repositório de dados atinge o limite de erro:

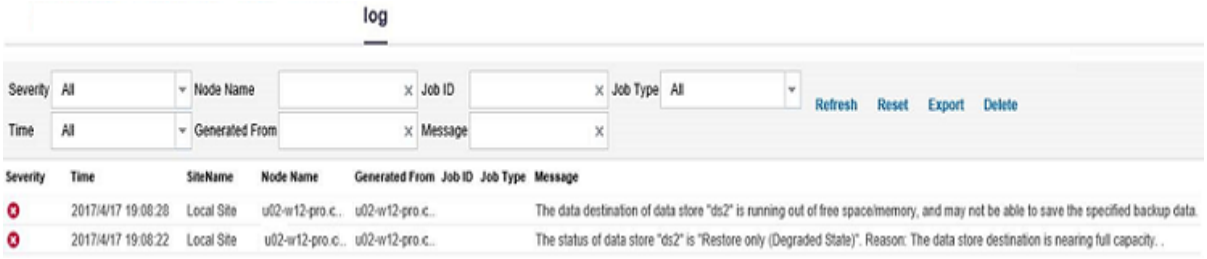
- O status do repositório de dados é alterado automaticamente para Restaurar somente (estado degradado). Enquanto o repositório estiver com esse status, nenhuma tarefa nova de backup/replicação poderá ser acionada para ele. Note, no entanto, que ainda é possível acionar tipos de tarefa que não geram novos dados. Por exemplo, tarefas de restauração e mesclagem.
- A barra de espaço do repositório de dados é exibida em vermelho.



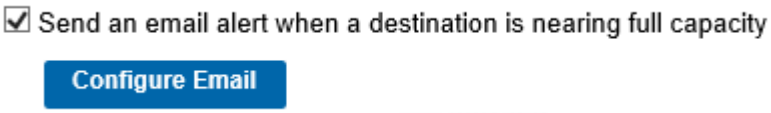
- O status do repositório de dados é mostrado com um ícone vermelho.



- Logs de atividades são exibidos para informá-lo que a pasta de destino do repositório de dados atingiu o nível de erro, ou seja, está sem espaço livre, e não é possível salvar novos dados de backup.



- Se o repositório de dados foi configurado para enviar alerta por email quando a pasta de destino está se aproximando da capacidade máxima, o RPS envia alertas por email aos destinatários.

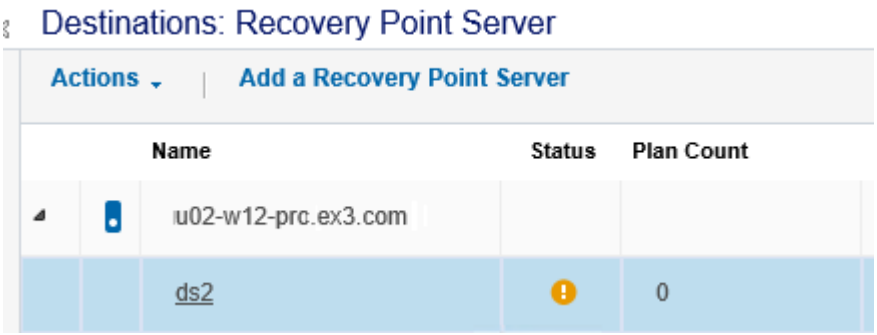


Usar limite de aviso

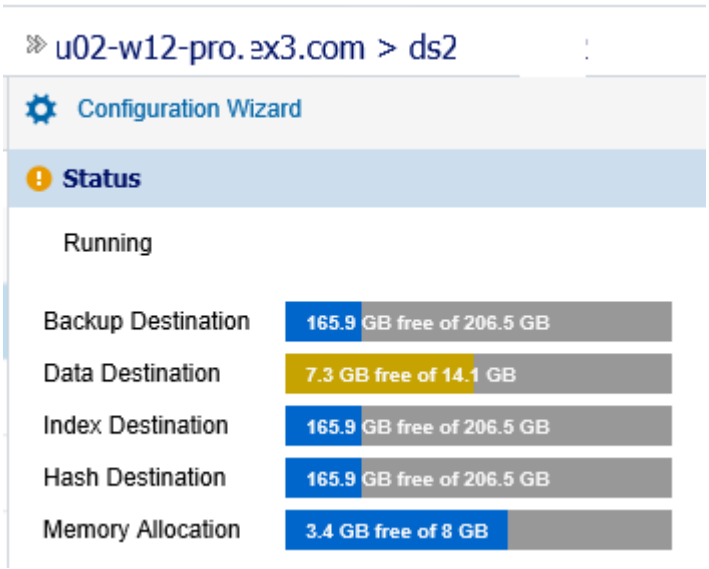
O limite de aviso indica que ainda há espaço livre no destino. No entanto, o espaço pode acabar rapidamente se chegarem novas tarefas de backup/replicação.

Quando o espaço livre do repositório de dados atinge o limite de aviso:

- O status original do repositório de dados é mantido. Por exemplo, o status Em execução.
- A programação de tarefa não é afetada.
- O status do repositório de dados é mostrado com um ponto de exclamação amarelo.



- A barra de espaço do repositório de dados é exibida em amarelo.



- Um log de atividades é exibido para informá-lo que a pasta de destino do repositório de dados está se aproximando da capacidade máxima, tendo já atingido o nível de aviso.

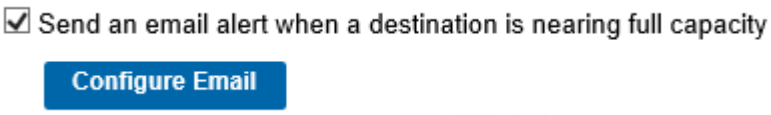
- Se o repositório de dados foi configurado para enviar alerta por email quando a pasta de destino está se aproximando da capacidade máxima, o RPS envia alertas por email aos destinatários.

Ativar alerta por email e compreender o formato de email

Quando o destino do repositório de dados está se aproximando da capacidade máxima ou o espaço livre da pasta de destino atinge o limite de aviso/erro, é enviado um alerta por email a destinatários especiais para notificá-los da situação. Para receber alertas por email, você precisa definir as configurações de email e ativar a opção de recebimento de alertas por email.

Para ativar a configuração, siga estas etapas:

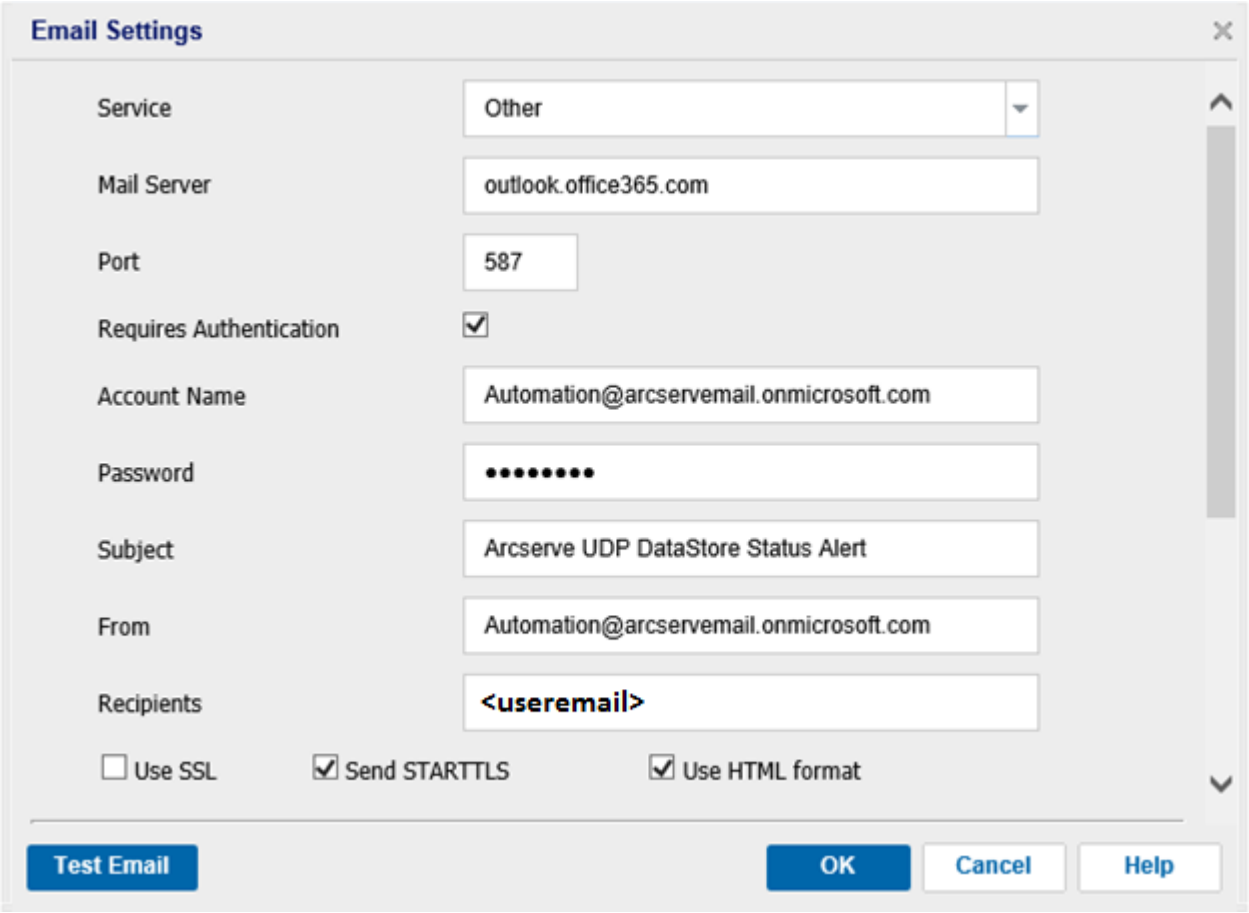
1. Marque a caixa de seleção de **Enviar um alerta por email quando um destino estiver se aproximando da capacidade máxima** ao adicionar/modificar/importar o repositório de dados.

   O botão Configurar email é exibido.

2. Clique em **Configurar email**.

   A caixa de diálogo Configurações de email é exibida.



3. Insira detalhes em Configurações de email e clique em **OK**.

   O email foi configurado para receber todos os alertas do repositório de dados.

   Observação: o botão **Email de teste** permite verificar se a ID de email dos destinatários está recebendo email. Recomendamos que você clique nesse botão antes de fechar a caixa de diálogo.

O alerta é enviado por email aos destinatários configurados quando:

- O espaço ocupado no caminho do repositório de dados atinge o limite de aviso.
- O espaço ocupado no caminho do repositório de dados atinge o limite de erro.
- É liberado espaço na pasta de destino do repositório de dados (por exemplo, depois de uma tarefa de mesclagem do repositório de dados ou da adição de espaço ao volume de destino) e o espaço ocupado fica abaixo do limite de aviso/erro.

Formato do alerta recebido no email

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.

Procurar pontos de recuperação em um repositório de dados

É possível usar a opção **Procurar pontos de recuperação** para exibir os detalhes relacionados aos pontos de recuperação e os planos associados a esse repositório de dados. Por exemplo, é possível exibir os detalhes relacionados às configurações do repositório de dados e aos eventos recentes.

Também é possível procurar os pontos de recuperação no modo de exibição Pastas compartilhadas.

Para excluir um nó de um repositório de dados, consulte Excluir os dados do nó de um repositório de dados.

Siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Destinos** e clique em **Servidores de ponto de recuperação**.

   A página **Destinos: Servidores do ponto de recuperação** exibe a lista de servidores de ponto de recuperação disponíveis.
3. Expanda um servidor do ponto de recuperação.

   É possível ver a lista de repositórios de dados associados ao servidor do ponto de recuperação.
4. Execute uma das seguintes ações:
   - Clique com o botão direito do mouse no nome do repositório de dados.
   - Selecione o repositório de dados e, no painel central, clique no menu suspenso **Ações**.

   Uma lista de opções é exibida.

   Observação: também é possível clicar no nome de um repositório de dados para procurá-lo.
5. Selecione **Procurar pontos de recuperação** entre as opções exibidas após selecionar um repositório de dados.

   A página do repositório de dados selecionado é exibida com o resumo com as informações sobre **pontos de recuperação.** Por exemplo, a página exibe informações relacionadas às **Configurações do repositório de dados** e aos **Eventos recentes**.
6. Para atualizar as informações sobre o plano ou repositório de dados, selecione o plano ou esse repositório de dados e clique em **Ações**, **Atualizar**.

7. Para restaurar, selecione Nó do agente, clique em **Ações** e **Restaurar**.

   É possível ver a caixa de diálogo **Restaurar** onde você escolheu a opção de restauração que deseja realizar para o repositório de dados.

Suporte a FQDN para um repositório de dados

Ao criar um repositório de dados em um disco local, o Arcserve UDP cria uma pasta compartilhada para repositório de dados, para que as tarefas em execução em outros servidores possam acessar os dados.

No Arcserve UDP Versão 5.0, a pasta foi compartilhada com o nome do host (por exemplo, <hostname>\sharename). Como resultado, quando o servidor remoto pôde acessar somente o RPS com FQDN (nome de domínio totalmente qualificado), não pôde acessar o RPS com o nome do host e as tarefas falharam.

Agora, a pasta de repositório de dados pode ser compartilhada com FQDN ou endereço IP. Isso permite que o servidor remoto acesse o repositório de dados.

Para conseguir isso, atualize o servidor de ponto de recuperação no Console para FQDN ou o endereço IP e crie um novo repositório de dados.

Observação: Para um banco de dados existente, interrompa o repositório de dados e importe-o novamente. É possível substituir o repositório de dados, em vez de excluí-lo. Em seguida, reimplante os planos que usam o repositório de dados.

Executar uma tarefa de mesclagem manual ou por demanda

Como administrador de armazenamento, você pode executar uma tarefa de mesclagem sob demanda e especificar o número de pontos de recuperação a serem retidos. Os valores podem ser diferentes das configurações do plano. A tarefa de mesclagem exclui as sessões de backup selecionadas de um repositório de dados para liberar espaço e efetivamente gerenciar o espaço de armazenamento. Você pode selecionar vários nós e executar a tarefa de mesclagem por demanda.

Observação: para a tarefa de mesclagem, quando uma tarefa de replicação estiver configurada e você executar uma tarefa de mesclagem por demanda do repositório de dados de origem, a tarefa não verifica se as sessões estão replicadas ou não. Como resultado, as sessões de mesclagem não podem ser replicadas para o repositório de dados de destino e você acaba replicando mais dados. Por exemplo, considere que há cinco sessões, s1, s2, s3, s4 e s5, respectivamente. s1 e s2 são replicadas. Agora, você executa uma tarefa de mesclagem sob demanda no lado de origem e retém duas sessões. s4 e s5 são retidas. s4 é uma sessão completa. Portanto, quando a próxima tarefa de replicação for iniciada, a tarefa precisa replicar uma sessão completa.

Siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, vá para **Destinos** e clique em **Servidores de ponto de recuperação**.
3. No painel central, clique no repositório de dados que contém os dados do nós que você deseja mesclar.

   A página **Resumo de pontos de recuperação** é exibida.
4. Selecione o nó que deseja mesclar.
5. Clique em **Ações Mesclar agora**.

   Observação: para mesclar vários nós de um repositório de dados, pressione a tecla Ctrl ou Shift e selecione os nós. Em seguida, clique em **Ação**, **Mesclar agora**.

   A caixa de diálogo **Executar uma mesclagem agora** é aberta.
6. Especifique a quantidade de pontos de recuperação que você deseja manter e clique em **OK**.

   A tarefa de mesclagem sob demanda é iniciada e os dados do nó são excluídos da origem de dados. Você pode ver o status da tarefa de mesclagem dos Eventos recentes e logs.

Modificar o limite de nós ativos simultâneos para backup manual

Para enviar backups manuais simultaneamente para vários nós, não controlados pela opção *Limite de nós ativos simultâneos*, adicione uma chave do registro no Servidor de ponto de recuperação. Os limites para nós ativos simultâneos são configurados na interface de usuário Repositório de dados.

Siga estas etapas:

1. Abra o Editor de registro do Windows. Para abrir, clique em **Iniciar**, digite *regedit* no campo Pesquisar programas e arquivos e, em seguida, pressione **Enter**.

   Observação: talvez você precise fornecer credenciais administrativas para abrir o Editor do registro do Windows.

2. Localize e clique na chave de registro a seguir:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

3. No menu Editar, clique em **Novo** e, em seguida, clique no **Valor DWORD (32 bits)))**.

   É possível ver a lista de repositórios de dados associados ao servidor do ponto de recuperação.

4. Especifique ManualJobsIgnoreConcurrentJobLimit como o nome para a nova entrada e, em seguida, pressione **Enter**.

5. Clique com o botão direito do mouse em ManualJobsIgnoreConcurrentJobLimit e em **Modificar**.

6. Especifique 1 no campo de dados **Valor** e, em seguida, clique em **OK**.

7. Feche o Editor do Registro.

   Observação: após ser ativada com 1, a chave do registro ManualJobsIgnoreConcurrentJobLimit funcionará para todos os repositórios de dados no servidor do RPS.

Solução de problemas: como usar um armazenamento de dados quando uma ou várias pastas estiverem cheias

Sintoma:

Como continuo a usar o armazenamento de dados quando uma das seguintes pastas estiver cheia:

- Destino de backup do repositório de dados
- Índice de redução de redundância
- Hash
- Dados

Solução:

Alterar o caminho de destino do backup

1. Interrompa o repositório de dados.
2. Modifique os planos que estão usando esse repositório de dados. Na guia Destino, aponte o destino para um repositório de dados diferente ou uma pasta compartilhada, marque a caixa de seleção **Pausar este plano** e **salve** o plano.
3. Exclua o repositório de dados.
4. Copie a pasta de destino do backup correspondente em um volume grande. Verifique se o tamanho e número de arquivos nas pastas de origem e destino são iguais.

   Observação: verifique se antes de copiar a pasta, repositório de dados foi interrompido. Durante a cópia, certifique-se de que todos os arquivos sejam copiados nas pastas de destino, sem pular qualquer arquivo.

   Aviso! Ignorar qualquer arquivo pode resultar em corrupção dos dados. Se o número ou o tamanho dos arquivos não coincidir entre as pastas de origem e destino, não prossiga para a próxima etapa.
5. Importe o repositório de dados. Especifique o novo caminho de dados/índice ao importar o repositório de dados.
6. No console do UDP, navegue até Recursos, Destinos, Servidores de ponto de recuperação.
7. Selecione o repositório de dados no servidor de ponto de recuperação.

8. No painel direito, em Configurações, verifique se o caminho de destino de dados/índice aponta para o local correto.

   Importante: ao executar as etapas mencionadas acima, NÃO inicie o repositório de dados até que a etapa 8 seja concluída.

9. Inicie o repositório de dados.
10. Modifique os planos que você pausou e os reconfigure para usar o repositório de dados importado (de acordo com o requisito). Desmarque a opção **Pausar este plano** e **salve** o plano.

    Observação: depois de importar o repositório de dados para vincular ao novo local e iniciar o repositório de dados, **NÃO retorne** ao caminho original. Essa ação pode causar a corrupção dos dados.

Alterar o caminho de destino do índice ou de dados

1. Interrompa o repositório de dados.
2. Copie a pasta correspondente (Dados/Índice de acordo com o requisito) em um volume grande. Verifique se o tamanho e o número de arquivos nas pastas de origem e destino são iguais.

   Observação: verifique se antes de copiar a pasta, repositório de dados foi interrompido. Durante a cópia, certifique-se de que todos os arquivos sejam copiados nas pastas de destino, sem pular qualquer arquivo.

   Aviso! Ignorar qualquer arquivo pode resultar em corrupção dos dados. Se o número ou o tamanho dos arquivos não coincidir entre as pastas de origem e destino, não prossiga para a próxima etapa.

3. Importe o repositório de dados. Especifique o novo caminho de dados/índice ao importar o repositório de dados.
4. No console do UDP, navegue até Recursos, Destinos, Servidores de ponto de recuperação.
5. Selecione o repositório de dados no servidor de ponto de recuperação.
6. No painel direito, em Configurações, verifique se o caminho de destino de dados/índice aponta para o local correto.

   Importante: ao executar as etapas mencionadas acima, NÃO inicie o repositório de dados até que a etapa 6 seja concluída.

7. Inicie o repositório de dados.

   Observação: depois de importar o repositório de dados para vincular ao novo local e iniciar o repositório de dados, **NÃO retorne** ao caminho original. Essa ação pode causar a corrupção dos dados.

Alterar caminho de destino de hash

Para obter detalhes, consulte Modificar somente o destino de hash.

Como gerenciar um servidor do ponto de recuperação

Com o Arcserve UDP, é possível executar várias operações no servidor de ponto de recuperação existente, como atualizar, excluir, importar e aprimorar.

O servidor de ponto de recuperação é exibido em **Nome** na página **Destinos: servidor de ponto de recuperação.** Clique na guia **Ações** ou o nome do servidor do ponto de recuperação na página **Destinos: servidor do ponto de recuperação** para receber todas as opções para gerenciar o servidor do ponto de recuperação.

O que fazer a seguir?

- Verificar os pré-requisitos
- Atualizar um servidor de ponto de recuperação
- Excluir um servidor de ponto de recuperação do console
- Importar um repositório de dados
- Instalar/atualizar o servidor de ponto de recuperação

Verificar os pré-requisitos

Para gerenciar um servidor do ponto de recuperação, conclua os seguintes pré-requisitos:

- Efetue logon no Console.
- Adicione um repositório do ponto de recuperação.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Atualizar um servidor de ponto de recuperação

Quando alterar as credenciais ou o protocolo do servidor de ponto de recuperação, será necessário atualizar o servidor de ponto de recuperação. Caso contrário, o servidor do ponto de recuperação falha ou não funciona corretamente.

Observação: se um nó atuar como servidor do ponto de recuperação e agente e você alterar as credenciais ou o protocolo desse nó, atualize-o na página **Destinos: Servidores de ponto de recuperação**. O plano será implantado automaticamente no agente depois de atualizar o servidor do ponto de recuperação. Se você atualizar o nó a partir da página **Nós: Todos os nós**, os planos que envolvem esses nós não serão implantados com êxito. Para implantar o plano, atualize novamente o nó na página **Destinos: Servidores de ponto de recuperação**.

Siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Destinos** e clique em **Servidores de ponto de recuperação**.

   A página **Destinos: Servidores de ponto de recuperação** é exibida.
3. Execute uma das seguintes ações:
   - Clique em um servidor do ponto de recuperação.
   - Selecione o servidor do ponto de recuperação e, no menu central, clique no menu suspenso **Ações**.
4. Clique em **Atualizar**.

   A caixa de diálogo **Atualizar nó** é exibida.
5. Modifique os detalhes conforme desejado, e clique em **OK**.

   O servidor de ponto de recuperação é atualizado.

Excluir um servidor de ponto de recuperação do Console

Para remover um servidor de ponto de recuperação do console, use a opção **Excluir**.

Observação: ao remover um servidor de ponto de recuperação, os repositórios de dados associados não são excluídos. Um servidor de ponto de recuperação usado em qualquer plano não pode ser excluído.

Siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Destinos** e clique em **Servidores de ponto de recuperação**.

   A página **Destinos: Servidores de ponto de recuperação** é exibida.
3. Execute uma das seguintes ações:
   - Clique em um servidor do ponto de recuperação.
   - Selecione o servidor do ponto de recuperação e, no menu central, clique no menu suspenso **Ações**.
4. Clique em **Excluir**.

   A caixa de diálogo **Confirmar** é exibida.
5. Clique em **Sim**.

   O servidor do ponto de recuperação é excluído.

Importar um repositório de dados

O recurso **Importar repositório de dados** permite adicionar um repositório de dados para o servidor do ponto de recuperação. É possível importar quaisquer repositórios de dados existentes para um servidor do ponto de recuperação. Os repositórios de dados que você excluiu anteriormente de um servidor do ponto de recuperação estão disponíveis para importar.

Observação: quando os dados de hash de um repositório de dados de redução de redundância forem perdidos ou danificados, ainda será possível importar o repositório de dados. Forneça uma pasta vazia como pasta de hash. O repositório de dados, em seguida, inicia o status **somente restauração** e uma mensagem de erro mostra que essa função de hash não está funcionando para a pasta vazia de hash. Usando esse método, você pode usar o repositório de dados apenas para tarefas de restauração. Reconstrua o hash se você deseja executar a tarefa de backup.

Siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Destinos** e clique em **Servidores de ponto de recuperação**.

   A página **Destinos: servidores de ponto de recuperação** é exibida.
3. Execute uma das seguintes ações:
   - Clique em um servidor do ponto de recuperação.
   - Selecione o servidor do ponto de recuperação e, no menu central, clique no menu suspenso **Ações**.
   - Para receber alertas por email, marque a caixa de seleção ao lado de *Enviar um alerta por email quando um destino estiver se aproximando da capacidade máxima*.

     Observação: se ainda não tiver configurado um email, clique em **Configurar email** para fazer isso.
4. Clique **Importar repositório de dados**.

   A página **Importar um repositório de dados** é exibida.
5. Selecione as opções a seguir e clique em **Avançar**:
   - **Procure** selecionar a **Pasta de destino do backup** a partir da qual você deseja importar o repositório de dados.
   - Digite a **senha criptografada**.

Observação: deixe em branco se o repositório de dados não foi criptografado.

Após a autenticação da **pasta de Destino do backup**, a página **Importar um repositório de dados** exibe os detalhes do repositório de dados.

6. Modifique os detalhes, se necessário, e clique em **Salvar**.

   Se copiou a pasta Destino de dados, Destino de índice e Destino de hash para o armazenamento de dados de redução de redundância, altere o caminho da pasta.

   Observação: não é possível ativar ou desativar a opção de criptografia para um repositório de dados existente.

   O repositório de dados é adicionado ao servidor do ponto de recuperação e exibido na caixa de diálogo **Destinos: servidores do ponto de recuperação**.

Instalar/atualizar o servidor de ponto de recuperação

Use a opção **Instalar/atualizar servidor do ponto de recuperação** pelos seguintes motivos:

- Quando ocorre uma falha na instalação.
- Quando desejar atualizar o produto.

Siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Destinos** e clique em **Servidores de ponto de recuperação**.

   A página **Destinos: Servidores de ponto de recuperação** é exibida.
3. Execute uma das seguintes ações:
   - Clique em um servidor do ponto de recuperação.
   - Selecione o servidor do ponto de recuperação e, no menu central, clique no menu suspenso **Ações**.
4. Clique em **Instalar/atualizar o servidor de ponto de recuperação**.

   Os detalhes do caminho de instalação são exibidos na mesma página, acima da lista do servidor do ponto de recuperação adicionado.
5. Atualize os detalhes conforme necessário.
6. Especifique a programação de instalação/atualização e clique em **OK**.

   A instalação ou a atualização é iniciada conforme a programação. É possível visualizar o progresso da instalação ou atualização no painel direito.

   Observação: é possível cancelar uma implantação de servidor de ponto de recuperação se ela tiver sido programada para uma ocasião futura. Para cancelar uma implantação do servidor de ponto de recuperação, selecione o agente e clique em Ações, Cancelar implantação de agente.

Como gerenciar servidores de backup do Arcserve

É possível gerenciar os servidores de backup do Arcserve a partir do console do Arcserve UDP. Também é possível atualizar e excluiro servidor de Backup do Arcserve do Console.

Atualizar um servidor de backup Arcserve

Quando as credenciais ou a porta do serviço web do Arcserve do servidor de backup do Arcserve é alterada, será necessário atualizá-la no Console.

Siga estas etapas:

1. Efetue logon no console e clique na guia **recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Servidores do Arcserve Backup**.

   A página **Destinos:** A página **Servidores de backup do Arcserve** é exibida no painel central.
3. Selecione um servidor de backup do Arcserve, com o botão direito e selecione **Atualizar**.

   A página **Atualizar um servidor de backup do Arcserve** é exibida.
4. Atualize os campos necessários e clique em **Salvar**.

   A página **Atualizar um servidor de backup do Arcserve** é fechada.

   Você atualizou com êxito o servidor de backup do Arcserve.

Excluir um servidor de backup Arcserve

Se você não precisar mais de um servidor de backup do Arcserve, é possível excluir esse servidor do Console. Antes de excluir um servidor de backup do Arcserve, certifique-se de que o servidor de Backup do Arcserve não esteja incluído em qualquer tarefa em um plano. Se o servidor estiver incluído em alguma tarefa, exclua a tarefa ou altere o destino de backup.

Siga estas etapas:

1. Efetue logon no console e clique na guia **recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Servidores do Arcserve Backup**.

   A página **Destinos:** A página **Servidores de backup do Arcserve** é exibida no painel central.
3. Selecione um servidor de backup do Arcserve, com o botão direito e selecione **Excluir**.

   A caixa de diálogo Confirmação é aberta.
4. Clique em **Sim**.

   O servidor de backup do Arcserve foi excluído com êxito do Console.

Como gerenciar a pasta compartilhada

É possível gerenciar as pastas compartilhadas no console do Arcserve UDP. Você também pode modificar e excluir a pasta compartilhada do console.

Modificar uma pasta compartilhada

O Arcserve UDP permite que modificar os detalhes de uma pasta compartilhada adicionada. Se as informações relacionadas à pasta compartilhada forem alteradas, será necessário modificar a pasta compartilhada adicionada no Arcserve UDP para os planos funcionarem.

Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection e clique na guia **recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Pastas compartilhadas**.

   A página **Destinos: pastas compartilhadas** exibe as pastas compartilhadas adicionadas no painel central.
3. Para gerenciar, clique com o botão direito em uma das pastas compartilhadas adicionadas ou selecione uma pasta compartilhada e clique em **Ações**.
4. Nas opções exibidas, clique em **Atualizar**.

   A caixa de diálogo **Atualizar** é exibida.
5. Modifique as informações e clique em **OK**.

   Agora, a pasta compartilhada é atualizada.

Excluir uma pasta compartilhada

O Arcserve UDP permite excluir uma pasta compartilhada adicionada.

Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection e clique na guia **recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Pastas compartilhadas**.

   A página **Destinos: pastas compartilhadas** exibe as pastas compartilhadas adicionadas no painel central.
3. Para gerenciar, clique com o botão direito em uma das pastas compartilhadas adicionadas ou selecione uma pasta compartilhada e clique em **Ações**.
4. Nas opções exibidas, clique em **Excluir**.

   Uma caixa de diálogo de **confirmação** ou **erro** é exibida.
5. Para a mensagem de confirmação, clique em **OK** para excluir.
6. (Opcional) Para a mensagem de erro, resolva o erro e tente excluir novamente.

   Agora, a pasta compartilhada é atualizada.

Como gerenciar um console remoto

Depois de criar um console remoto, talvez seja necessário realizar várias operações, como modificar, excluir ou testar a conexão.

O que fazer a seguir?

- Modificar um console remoto
- Excluir um console remoto
- Testar conexão do console remoto

Modificar um console remoto

O Arcserve UDP permite modificar os detalhes de um console remoto adicional. Se tiver alterado as informações de conexão para o console remoto, será necessário modificar a conta do console remoto adicionada em Arcserve UDP.

Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection e clique na guia **recursos**.
2. No painel esquerdo, navegue até **Destinos** e clique em **Console remoto**.

   A página **Destinos: console remoto** exibe o console remoto adicionado no painel central.
3. Para gerenciar, clique com o botão direito em um dos consoles remotos adicionados ou selecione um console remoto e clique em **Ações**.

   A página **Modificar um console remoto** é exibida.
4. Modifique as informações e clique em **OK**.

   Agora, o console remoto é atualizado.

Excluir um console remoto

O Arcserve UDP permite que você remova um console remoto quando necessário.

Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection e clique na guia **recursos**.
2. No painel esquerdo, navegue até **Destinos** e clique em **Console remoto**.

   A página **Destinos: console remoto** exibe o console remoto adicionado no painel central.
3. Para gerenciar, clique com o botão direito em um dos consoles remotos adicionados ou selecione um console remoto e clique em **Ações**.

   Uma mensagem de **confirmação** ou **erro** é exibida.

   Mensagem de confirmação

   Aparece quando o console remoto não é adicionado a um plano.

   Mensagem de erro

   Aparece quando o console remoto faz parte de um plano existente.
4. (Opcional) Quando aparecer a mensagem de erro:
   a. Clique em **OK** para fechar a mensagem de erro.
   b. Abra o plano ao qual o console remoto está associado.
   c. Exclua o plano relacionado ou modifique o plano para alterar o console remoto na guia destino do plano **Replicar para um RPS gerenciado remotamente**.

   Depois de remover o console remoto do plano, volte para a página do console remoto e tente excluir o console remoto novamente.
5. Na mensagem de confirmação, clique em **Sim**.

   Agora, o console remoto é removido.

Testar conexão do console remoto

O Arcserve UDP permite que você teste a conexão de um console remoto adicional. Uma conexão bem-sucedida para a conexão de console remoto é necessária para que o plano de replicação trabalhe enquanto a conta de console remoto é associada ao plano de trabalho.

A conexão de console remoto pode falhar por vários motivos:

- Quando as informações adicionadas para um destino de console remoto forem incorretas.
- Quando as informações de credencial, porta, protocolo ou proxy de console remoto forem alteradas, mas as mesmas informações não forem atualizadas no console do Arcserve UDP.
- Quando a conexão de rede quebrar entre esse console e o console remoto.
- Quando o serviço de gerenciamento do Arcserve UDP estiver interrompido no console remoto.

Você pode usar a opção de conexão de console remoto de teste para verificar se um console remoto está conectado e se as informações adicionadas à conta estão corretas.

Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection e clique na guia **recursos**.
2. No painel esquerdo, navegue até **Destinos** e clique em **Console remoto**.

   A página **Destinos: console remoto** exibe o console remoto adicionado no painel central.
3. Para gerenciar, clique com o botão direito em um dos consoles remotos adicionados ou selecione um console remoto e clique em **Ações**.

   Várias opções são exibidas.
4. Das várias opções exibidas, clique em **Testar conexão de console remoto**.

   Uma mensagem de **informações** será exibida se os detalhes do console remoto estiverem corretos.

   Uma mensagem de **erro** será exibida se os detalhes do console remoto estiverem incorretos. Forneça os detalhes corretos para corrigir a conexão e teste novamente.
5. (Opcional) Se for exibida uma mensagem de erro, corrija a conexão interrompida verificando um ou todos os seguintes motivos:

- As informações da conta estão corretas.
- A conexão de rede está estabelecida.
- O status do serviço de gerenciamento do Arcserve UDP no console remoto não está interrompido.

Agora, a conexão de console remoto é testada com êxito.

Capítulo 10: Criando planos para proteger os dados

Esta seção contém os seguintes tópicos:

Compreendendo o plano e as tarefas

Para proteger um nó, é necessário criar um plano com uma tarefa de backup. Um plano é um grupo de tarefas para gerenciar backup, replicação e criação de nós do modo de espera virtual. Um plano consiste em uma única ou em várias tarefas. As tarefas são um conjunto de atividades para definir a origem, destino, programação e parâmetros avançados.

É possível criar as seguintes tarefas:

Tarefas de backup

Permite criar uma tarefa de backup para proteger os nós da máquina virtual com base em host, Linux e Windows. Com base no tipo de nós que deseja proteger, use uma das seguintes tarefas:

Backup do Windows com base em agente

Define uma tarefa de backup para proteger os nós do Windows. Em um método de backup com base em agente, um componente de agente é usado para fazer backup dos dados. O agente é instalado no nó de origem.

Backup sem agente com base em host

Define uma tarefa de backup para proteger máquinas virtuais com base em host em um VMware vCenter/ESX Server ou Microsoft Hyper-V Server. Em um método de backup sem agente, não é preciso instalar um componente de agente no servidor ou na máquina virtual. No entanto, é preciso instalar o agente em um servidor proxy.

Linux com base em agente

Define uma tarefa de backup para proteger nós do Linux. O agente está instalado em um servidor de backup Linux e não nos nós de origem que deseja proteger.

Tarefa Replicar de um RPS remoto

Permite criar uma tarefa para receber dados de um servidor de ponto de recuperação remoto.

Tarefa de replicação

Permite criar uma tarefa para replicar dados de backup de um servidor de ponto de recuperação para outro servidor de ponto de recuperação.

Tarefa Modo de espera virtual

Permite criar uma tarefa para criar um nó no modo de espera virtual.

Tarefa Cópia de arquivo

Permite copiar arquivos selecionados do nó de origem e armazenar os arquivos copiados em uma pasta local ou compartilhada. Também é possível armazenar os arquivos em um armazenamento na nuvem.

Tarefa Copiar pontos de recuperação

Permite copiar os pontos de recuperação em uma pasta local, compartilhada ou na nuvem.

Tarefa Replicar para um RPS gerenciado remotamente

Permite criar uma tarefa para replicar ou enviar dados para um servidor de ponto de recuperação remoto.

Tarefa Arquivo morto

Permite copiar os pontos de recuperação para um compartilhamento de rede, armazenamento na nuvem ou volume em um nó protegido. Quando os pontos de recuperação são copiados no destino, os arquivos de origem são excluídos.

Tarefa Cópia em fita

Permite copiar os pontos de recuperação em uma fita com capacidade de recuperação granular diretamente a partir da fita.

Tarefa de recuperação garantida

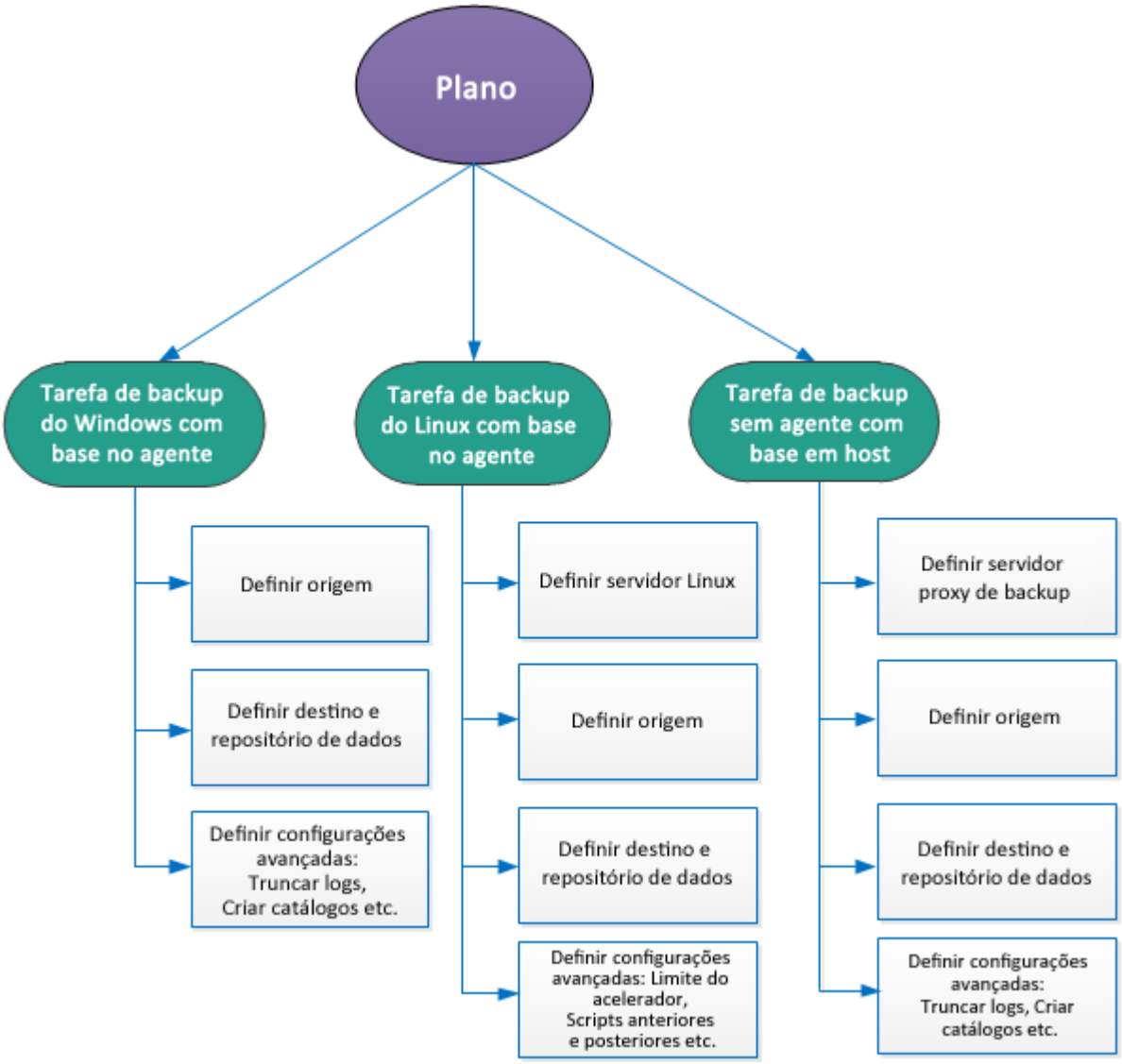
Permite verificar a acessibilidade e garantir a recuperação dos dados.

A tabela a seguir exibe a lista de tarefas de acompanhamento que podem ser adicionadas após a Tarefa 1:

Tarefa 1	Tarefas de acompanhamento
Backup: Windows com base em agente	■ Replicar ■ Modo de espera virtual ■ Copiar pontos de recuperação ■ Cópia de arquivo ■ Replicar para um RPS gerenciado remotamente ■ Arquivo morto ■ Copiar em fita ■ Teste de recuperação garantida
Backup: sem agente com base em host	■ Replicar ■ Modo de espera virtual ■ Copiar pontos de recuperação ■ Replicar para um RPS gerenciado remotamente ■ Copiar em fita

	■ Teste de recuperação garantida
Backup: Linux com base em agente	■ Replicar ■ Replicar para um RPS gerenciado remotamente ■ Copiar em fita ■ Teste de recuperação garantida
Replicar dados de um RPS remoto	■ Modo de espera virtual ■ Replicar ■ Teste de recuperação garantida
Backup: Office 365 Exchange Online	■ Replicar ■ Copiar pontos de recuperação ■ Replicar para um RPS gerenciado remotamente ■ Copiar em fita ■ Teste de recuperação garantida
Backup: Office 365 OneDrive	■ Replicar ■ Copiar pontos de recuperação ■ Replicar para um RPS gerenciado remotamente ■ Copiar em fita ■ Teste de recuperação garantida
Backup: Office 365 SharePoint Online	■ Replicar ■ Copiar pontos de recuperação ■ Replicar para um RPS gerenciado remotamente ■ Copiar em fita ■ Teste de recuperação garantida
Backup: Arquivos no caminho UNC ou NFS	■ Replicar ■ Copiar pontos de recuperação ■ Replicar para um RPS gerenciado remotamente ■ Copiar em fita ■ Teste de recuperação garantida

O diagrama a seguir ilustra como tarefas diferentes formam um plano de backup. O diagrama mostra também os parâmetros que podem ser definidos em cada tarefa.


Plano
Tarefa de backup do Windows com base no agente
Tarefa de backup do Linux com base no agente
Tarefa de backup sem agente com base em host
Definir origem
Definir destino e repositório de dados
Definir configurações avançadas: Truncar logs, Criar catálogos etc.
Definir servidor Linux
Definir origem
Definir destino e repositório de dados
Definir configurações avançadas: Limite do acelerador, Scripts anteriores e posteriores etc.
Definir servidor proxy de backup
Definir origem
Definir destino e repositório de dados
Definir configurações avançadas: Truncar logs, Criar catálogos etc.

Como criar um plano de backup do Windows

Para proteger os nós do Windows ou os nós agrupados, é necessário criar um plano. Um plano de nós do Windows consiste em uma tarefa de backup. Esta tarefa de backup permite especificar os nós que deseja proteger, o destino do backup e a programação de backup. O destino do backup é um servidor de ponto de recuperação onde você deseja armazenar os dados de backup. O destino também pode ser um destino local ou uma pasta compartilhada remota.

Também é possível fazer backup de um banco de dados Oracle. Antes de criar um plano para fazer backup de um banco de dados Oracle, verifique os seguintes pré-requisitos:

- Para fazer backup de um banco de dados Oracle

Para fazer backup de nós agrupados e discos compartilhados da Microsoft, verifique os seguintes pré-requisitos:

- Verificar os pré-requisitos para fazer backup dos nós agrupados e discos compartilhados da Microsoft

O que fazer a seguir?

1. Verificar os pré-requisitos e as considerações
2. Criar um plano de backup
3. (Opcional) Executar um backup manual
4. Verificar o backup

Verificar os pré-requisitos e as considerações

Estas tarefas de pré-requisito devem ser concluídas:

- A versão mais recente do agente do Arcserve UDP (Windows) está instalada.
- Efetue logon no Console.
- (Opcional) Criar um repositório de dados para armazenar os dados de backup.
- Revisar os pré-requisitos do banco de dados Oracle com o UDP Windows Agent.
- Verifique os pré-requisitos para fazer backup de nós agrupados e discos compartilhados.
- (Para backup de SQL quando o banco de dados está no modo completo) Verifique Como ativar os truncamentos de log quando o banco de dados SQL está no modo de recuperação completo.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Os pré-requisitos a seguir são para instantâneos de hardware:

- Instale um provedor de hardware VSS que oferece suporte ao instantâneo de hardware em agentes do Arcserve UDP. A configuração típica de um provedor de hardware VSS inclui:
  - Especificação de um servidor que controla o LUN.
  - Especificar as credenciais da matriz de disco para acessar a matriz de disco.

  Observação: para obter mais informações sobre como configurar o provedor de hardware VSS, entre em contato com o fornecedor do provedor de hardware.

Os pré-requisitos a seguir estão relacionados ao backup de rede específico:

- O agente do Windows e o RPS devem estar na mesma rede.
- O nó de proteção do Windows está programado.
- O RPS local com várias NICs está conectado.

Revisar os pré-requisitos do banco de dados Oracle com o UDP Windows Agent

Para fazer backup de um banco de dados Oracle com informações consistentes, certifique-se de que o modo ARCHIVELOG esteja ativado para arquivar os logs de Refazer.

Observação: o volume de dados deve incluir arquivos de dados Oracle, arquivos de controle, o arquivo de parâmetros do servidor e logs de repetição online. Os logs de repetição arquivados devem estar fisicamente localizados em um volume separado.

Siga estas etapas para verificar se o modo ARCHIVELOG está ativado:

a. Efetue logon no Oracle Server como usuário Oracle com privilégios de SYSDBA.

b. Digite o seguinte comando no prompt do SQL*Plus:

   ARCHIVE LOG LIST;

   As configurações de log arquivadas para a instância atual são exibidas.

c. Defina as seguintes configurações:

   Modo de log de banco de dados: modo de arquivamento

   Arquivamento automático: ativado

d. Iniciar o modo ARCHIVELOG.

   Observação: se o modo ARCHIVELOG não estiver ativado, inicie o modo ARCHIVELOG para fazer backup do banco de dados.

Siga estas etapas para iniciar o modo ARCHIVELOG:

a. Encerre o Oracle Server.

b. Execute as seguintes instruções no Oracle:

   CONNECT SYS/SYS_PASSWORD AS SYSDBA

   STARTUP MOUNT;

   ALTER DATABASE ARCHIVELOG;

   ALTER DATABASE OPEN;

   Por padrão, os logs de arquivo morto são gravados na área de recuperação em flash. Se não desejar gravar os logs de arquivo morto para a área de recuperação em flash, defina o parâmetro LOG_ARCHIVE_DEST_n para o local onde você deverá gravar logs de arquivos.

SQL>ALTER SYSTEM SET LOG_ARCHIVE_DEST_
1='LOCATION=e:\app\administrator\oradata\<oracle_database_name>\arch'
SCOPE= BOTH;

Sistema alterado.

SQL> ARCHIVE LOG LIST;

As configurações de log arquivadas para a instância atual são exibidas.

c. Defina as seguintes configurações:

Modo de log de banco de dados: modo de arquivamento

Arquivamento automático: ativado

Destino do arquivo: E:\app\oracle\oradata\<oracle_database_name>\arch

Sequência de log online mais antiga: 21

Sequência de log atual: 23

O serviço de gravador do Oracle VSS foi iniciado e está funcionando corretamente.

Observação: se o serviço Oracle VSS Writer não estiver em execução, o agente do Arcserve UDP (Windows) o iniciará automaticamente antes de fazer o instantâneo.

- O agente do Arcserve UDP (Windows) é instalado e um plano é programado.

  Certifique-se de ter selecionado os volumes que incluem todos os arquivos de dados Oracle, arquivo de parâmetros do servidor, arquivos de controle, logs de repetição arquivados e logs de repetição online para o backup.

- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Se desejar executar uma BMR para uma recuperação de falhas, verifique se você selecionou os volumes do sistema e os volumes que contêm todos os arquivos de instalação Oracle.

Verificar os pré-requisitos para fazer backup dos nós agrupados e discos compartilhados da Microsoft

Analise as seguintes etapas de pré-requisito ao fazer backup dos nós agrupados e discos compartilhados da Microsoft:

- Instale o agente do Arcserve UDP em todos os nós agrupados.
- Adicione todos os agentes ou nós ao mesmo plano de backup.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Observação: será feito backup dos discos compartilhados juntamente com o agente que possui os discos compartilhados. Se o disco compartilhado for movido do Nó A para o Nó B durante uma tolerância a falhas, para a próxima tarefa de backup no Nó B, será feito backup do disco como um disco completo, mesmo que a tarefa propriamente dita seja exibida como incremental. Após outra tolerância a falhas, se o disco compartilhado for movido de volta para o Nó A, mesmo assim será feito backup do disco como um disco completo, embora a tarefa propriamente dita seja exibida como incremental.

Como ativar os truncamentos de log quando o banco de dados SQL está no modo de recuperação completa

Sintoma

Quando o banco de dados está no modo Completo e um backup completo do banco de dados é executado, o log de truncamento do SQL não pode ser truncado.

Solução

Para resolver esse problema, adicione dois valores de registro para fazer com que o Arcserve UDP execute o comando BACKUP LOG para fazer backup do log de transações. Esse comando marcará espaço, que já foi gravado no arquivo de banco de dados, como reutilizável.

Siga estas etapas para adicionar o valor do registro:

1. Abra o editor de tabela do registro na máquina do agente usando o seguinte comando:

   ```
   regedit
   ```

2. Navegue até as chaves a seguir, de acordo com o backup com base em agente ou sem agente:

   No backup com base em agente para sistema operacional de 32 bits e 64 bits, navegue até a seguinte chave na máquina do agente:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   Ao usar uma versão anterior à Arcserve UDP v6.5, Atualização 2, para o backup sem agente, navegue até a chave a seguir. Crie o valor de tabela de registro na VM da qual você deseja fazer backup no servidor proxy. Se a chave de tabela do Registro não estiver disponível, crie o caminho completo da chave.

   - **Sistema operacional de 32 bits:**

     HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   - **Sistema operacional de 64 bits:**

     HKEY_LOCAL_MACHINE\SOFTWARE\WoW6432Node\Arcserve\Unified Data Protection\Engine\AFBackupDll

3. Crie os dois valores de registro seguintes e, para ambos, defina o valor como 1:

   - valor dword chamado BackupSQLLog4Purge
   - valor dword chamado ForceShrinkSQLLog

O valor do registro é adicionado.

A solução entrará em vigor quando ocorrer a próxima tarefa de limpeza.

Criar um plano de backup com uma tarefa de backup

Um plano de backup inclui uma tarefa de backup que executa um backup de um nó físico e armazena os dados em um destino especificado. Cada tarefa consiste em parâmetros que definem a origem, o destino, a programação e outros detalhes de backup.

Siga estas etapas:

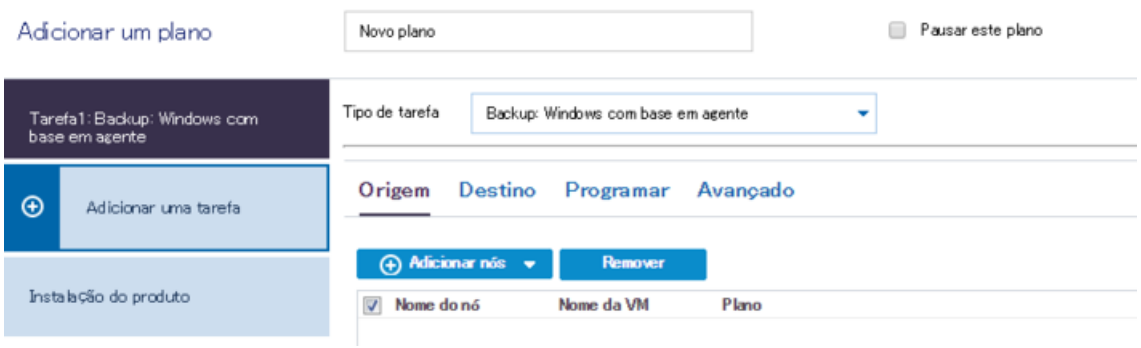
1. Efetue logon no Console do Arcserve UDP.
2. Navegue até **recursos** > **Planos** > **Todos os planos**.

   Se tiver criado os planos anteriores, esses planos serão exibidos no painel central.
3. No painel central, clique em **Adicionar um plano**.

   A opção Adicionar um plano é aberta.
4. Digite o nome do plano.
5. (Opcional) Selecione a caixa de seleção **Pausar este plano**.

   O plano não será executado até que você desmarque a caixa de seleção para retomar o plano.

   Observação: se um plano for pausado, nenhuma tarefa em andamento será pausada, mas todas as tarefas programadas correspondentes associadas a esse plano serão pausadas. No entanto, você pode executar uma tarefa manualmente. Por exemplo, você pode executar manualmente a tarefa de backup e a tarefa de replicação para um nó mesmo que o respectivo plano esteja pausado. Nesse caso, a tarefa seguinte da tarefa sob demanda (manual) não será executada. Por exemplo, há uma tarefa de replicação após uma tarefa de backup sob demanda, a tarefa de replicação não será executada para a tarefa de backup sob demanda. É necessário executar manualmente a tarefa de replicação. Quando você retomar o plano, as tarefas pendentes não são retomadas imediatamente. Depois de retomar o plano, as tarefas pendentes serão executadas no próximo horário programado.
6. Na lista suspensa Tipo de tarefa, selecione **Backup: Windows com base em agente**.



Agora especifique os detalhes de Origem, Destino, Programação e Avançado.

Especificar a origem

A página Origem permite especificar os nós de origem que deseja proteger. É possível selecionar mais de um nó em um plano. Caso não tenha adicionado nós para o console, você pode adicionar nós ao criar ou modificar um plano da página de origem. Também é possível salvar um plano sem adicionar nenhum nó de origem. O plano é implantado somente após você adicionar nós de origem.

Siga estas etapas:

1. Na guia Origem, clique em **Adicionar**.
2. Selecione uma das seguintes opções:

   Selecionar os nós a serem protegidos no Arcserve UDP

   Abre a caixa de diálogo Selecionar nós para proteger no Arcserve UDP. Selecione os nós na lista exibida. Selecione esta opção se você já tiver adicionado os nós para o console.

   Adicionar nó do Windows

   A caixa de diálogo Adicionar nós a um plano é exibida. Selecione esta opção se você não tiver adicionado os nós e desejar adicionar manualmente os nós para proteger.

   Detectar os nós do Active Directory

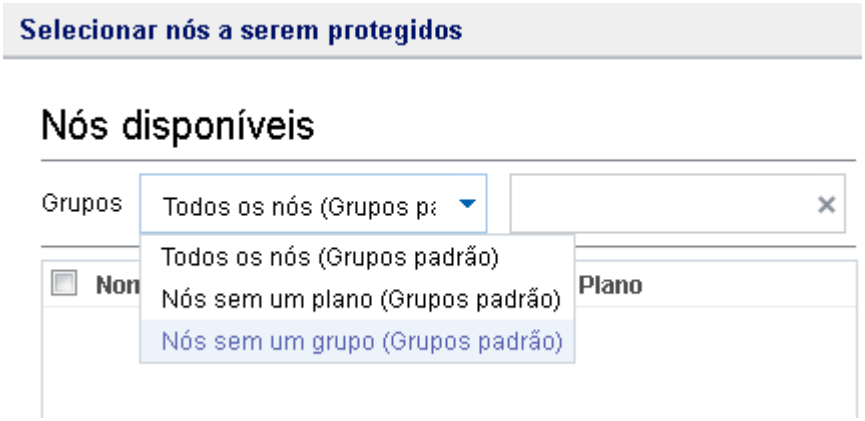
   Abra a caixa de diálogo Adicionar nós ao Console do Arcserve UDP. Selecione essa opção se desejar detectar e adicionar nós do Active Directory.
3. Se você selecionou a opção **Selecionar nós para proteger no Arcserve UDP**, na caixa de diálogo Selecionar nós para proteger, faça o seguinte:
   a. (Opcional) Selecione um filtro na lista suspensa Grupos para filtrar os nós. É possível digitar as palavras-chave para filtrar melhor seus nós.

      Os nós são exibidos na coluna Nós disponíveis.

   b. Selecione os nós na coluna Nós disponíveis e, em seguida, clique na seta simples à direita (>) ou na seta dupla à direita (>>) para mover os nós selecionados ou todos os nós, respectivamente, para a coluna Nós selecionados.

      Os nós são exibidos na coluna Nós selecionados.

   c. Clique em **OK** para fechar a caixa de diálogo.



4. Para escolher Tipo de proteção, selecione uma das seguintes opções:

   Fazer backup de todos os volumes

   Prepara um backup instantâneo de todos os volumes.

   Fazer backup dos volumes selecionados

   Prepara um instantâneo de backup do volume selecionado.

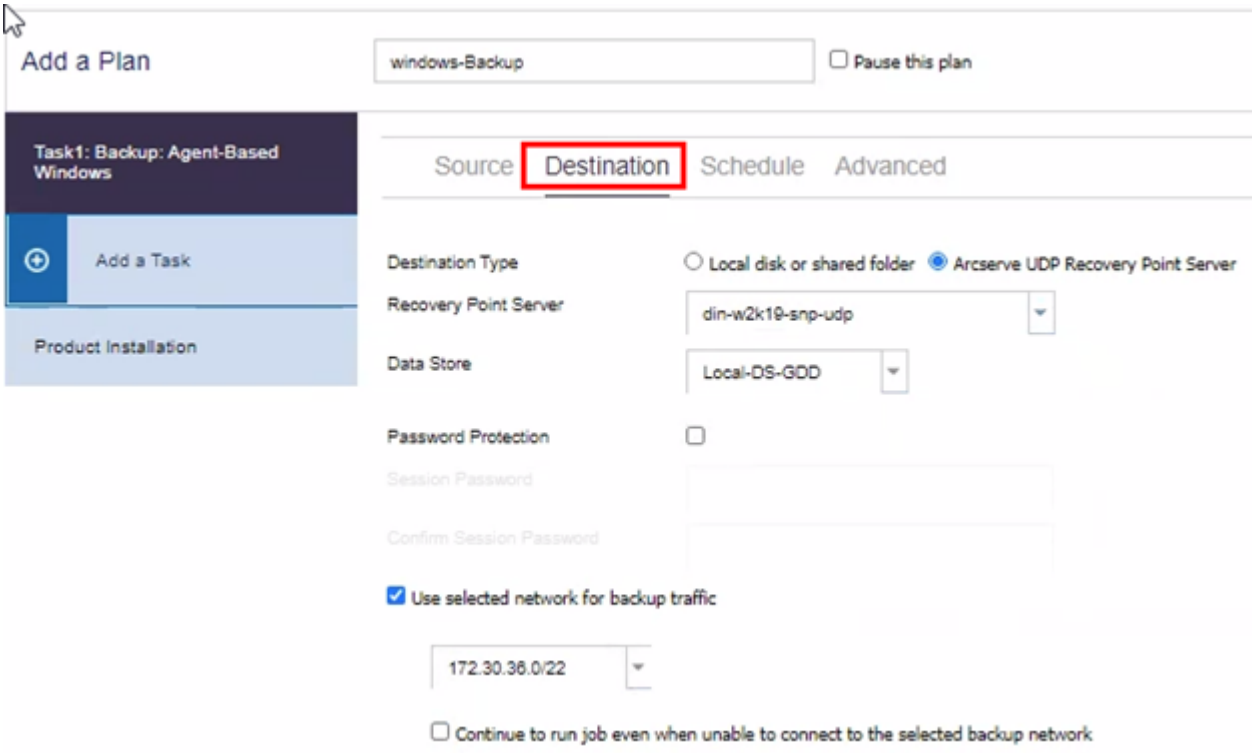
   A origem é especificada.

Especificar o destino

O destino é o local onde você armazena os dados de backup. É necessário, no mínimo, especificar o destino para salvar o plano.

Siga estas etapas:

1. Clique na guia **Destino**.



2. Selecione um dos seguintes tipos de destino:

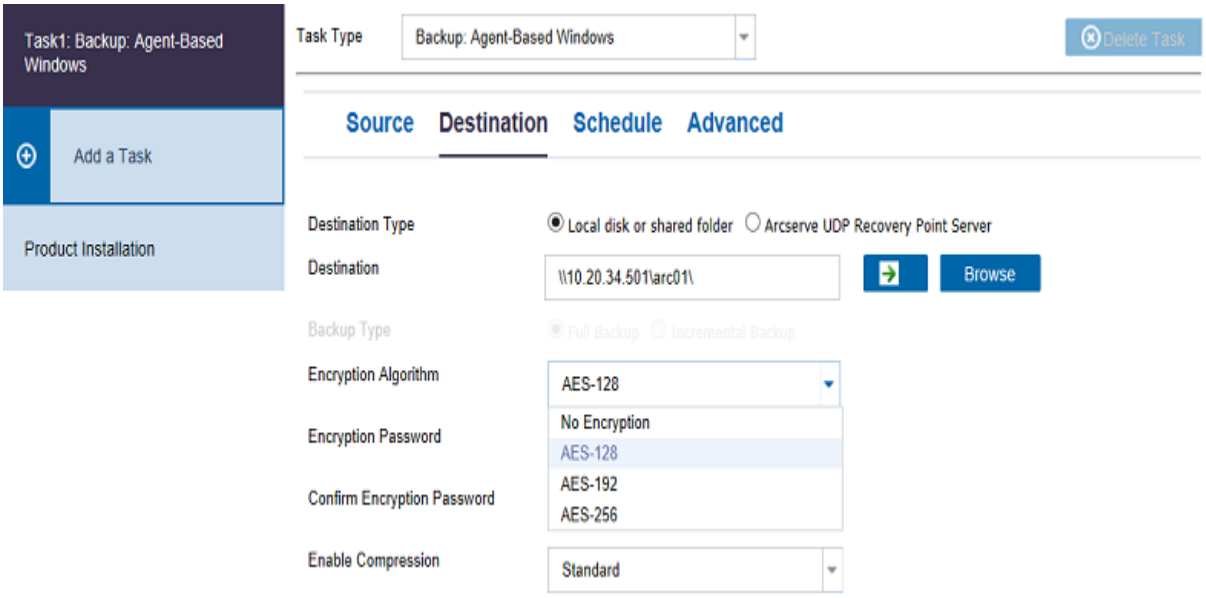
   Disco local ou uma pasta compartilhada

   Especifica que o destino do backup é um destino local ou uma pasta compartilhada. Se selecionar essa opção, será possível salvar os dados como pontos de recuperação ou conjuntos de recuperação. As opções de pontos de recuperação e de conjuntos de recuperação estão disponíveis na guia Programar.

   Servidor de ponto de recuperação do Arcserve UDP

   Especifica que o destino de backup é um servidor de ponto de recuperação. Se selecionar essa opção, os dados serão armazenados como pontos de recuperação. Não é possível armazenar dados como conjuntos de dados de recuperação.

3. Se você selecionar o **disco local ou a pasta compartilhada** como um tipo de destino, forneça os seguintes detalhes:



- Destino: forneça o caminho completo do destino local ou de rede. Para o destino de rede, especifique as credenciais com o acesso de gravação. Clique em **Procurar** para localizar o destino ou clique no ícone de seta para frente para testar a conexão e fornecer as credenciais para a pasta de destino fornecida.
- Algoritmo de criptografia: na lista de opções da lista suspensa, selecione o algoritmo de criptografia. Para obter mais informações, consulte Configurações de criptografia.
- (Opcional) Senha de criptografia: forneça uma senha de criptografia.
- Confirmar senha de criptografia: digite a senha de criptografia novamente para confirmar.
- Ativar compactação: selecione um tipo de compactação na lista suspensa. para obter mais informações, consulte Tipo de compactação.

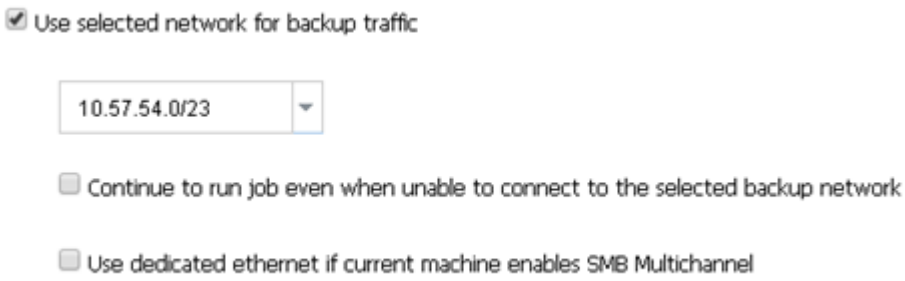
Observação: se armazenar os dados em um disco local ou em uma pasta compartilhada, não será possível replicar os dados para outro servidor de ponto de recuperação. A replicação é suportada apenas se armazenar os dados em um servidor de ponto de recuperação.

4. Se você selecionar o **Servidor de ponto de recuperação do Arcserve UDP** como um tipo de destino, faça o seguinte:

- Servidor de ponto de recuperação: na lista suspensa, selecione o RPS de destino.
- Repositório de dados: na lista suspensa, selecione o repositório de dados de destino.
- Proteção por senha: marque a caixa de seleção **Proteção por senha**, forneça a senha da sessão e digite a senha da sessão novamente para confirmar.

  Observação: a senha da sessão é opcional quando o destino de backup é um repositório de dados do RPS não criptografado..
- (Opcional) Marque a caixa de seleção **Usar a rede selecionada para o tráfego de backup** e siga estas etapas:

  a. Para ativar a comunicação entre o agente do Windows e o servidor de ponto de recuperação, na lista suspensa, selecione a rede CIDR.

  Observação: se a rede de backup selecionada não estiver acessível e para continuar a tarefa com a rede disponível ou com a rede padrão, clique na caixa de seleção **Continuar a executar a tarefa mesmo quando não for possível se conectar à rede de backup selecionada**.

  b. Para desativar o SMB Multichannel para que as transferências de dados sejam realizadas somente pela rede selecionada, marque a caixa de seleção **Usar ethernet dedicada se a máquina atual permitir o SMB Multichannel**.

  Observações:

  - Essa opção não está disponível por padrão. Para ativar essa opção, vá para o seguinte local da pasta: C:\Arquivos de programas\Arcserve\Unified Data Pro-

tec-
tion\Ma-
nagement\Configuration\ConsoleConfiguration.xml.
Em seguida, modifique o valor de *useDe-
dicatedEthernet* para True.

```
- <SpecifyNetwork>
    <useDedicatedEthernet>false</useDedicatedEthernet>
  </SpecifyNetwork>
```

A função Especificar rede fica desativada caso o repositório de dados seja remoto e utilize uma pasta compartilhada de rede como destino.

- Quando os serviços de gerenciamento do Arcserve UDP são reiniciados, o recurso SMB Multichannel é ativado.
- Por padrão, o recurso SMB Multichannel está ativado no Windows.

O destino é especificado.

Especificar a programação

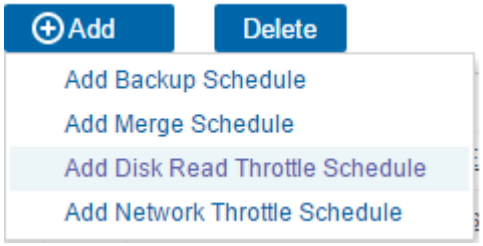
A página Programar permite definir uma programação para o backup e para que as funções Mesclar e Acelerar sejam repetidas em intervalos específicos. Após definir uma programação, as tarefas são executadas automaticamente de acordo com a programação. É possível adicionar várias programações e fornecer configurações de retenção.

Uma Programação de backup se refere a programação regular que é repetida várias vezes ao dia, com base no número de horas ou de minutos selecionado. Além da programação regular, uma programação de backup também fornece opções para adicionar programações diária, semanal e mensal.

Observação: para obter mais informações sobre as configurações de retenção e programação, consulte Entendendo a programação avançada e retenção.

Siga estas etapas:

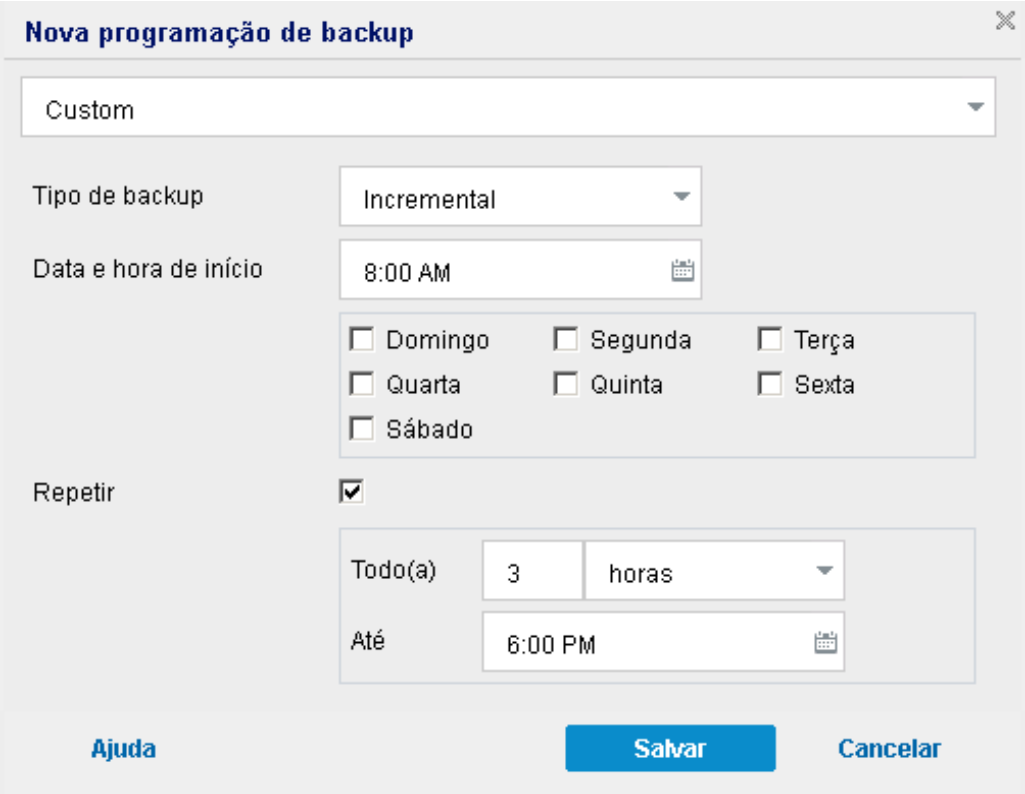
1. Adicione programações de backup, mesclagem, aceleração de leitura de disco e aceleração de rede.



Adicionar programação de backup

a. Clique em **Adicionar** e selecione **Adicionar programação de backups**.

   A caixa de diálogo **Nova programação de backup** é aberta.



b. Selecione uma das seguintes opções:

Personalizado

Especifica a programação de backup que se repete várias vezes por dia.

Diário

Especifica a programação de backup que ocorre uma vez por dia. Por padrão, todos os dias da semana estão selecionados para o backup diário. Se não desejar executar a tarefa de backup em um dia específico, desmarque a caixa de seleção correspondente àquele dia da semana.

Semanal

Especifica a programação de backup que ocorre uma vez por semana.

Mensal

Especifica a programação de backup que ocorre uma vez por mês.

c. Selecione o tipo de backup.

Completo

Especifica a programação de backups para backups completos. Conforme programado, o Arcserve UDP executa um backup completo de todos os blocos usados do computador de origem. Um backup completo em geral, consome tempo, dependendo do tamanho do backup.

Verificar

Especifica a programação de backups para backups de verificação.

A Arcserve UDP verifica se os dados protegidos são válidos e concluídos, executando uma verificação de confiabilidade da imagem de backup armazenada na origem do backup. Se necessário, a imagem será sincronizada novamente. Um backup de verificação examinará o backup mais recente de cada bloco e irá comparar o conteúdo e as informações com a origem. Esta comparação verifica se o backup mais recente dos blocos representa as informações correspondentes na origem. Se a imagem de backup de qualquer bloco não corresponder à origem (possivelmente devido a alterações no sistema desde o último backup), o Arcserve UDP atualizará (fará nova sincronização) o backup do bloco que não corresponder. Também é possível usar um backup de verificação (muito raramente) para obter a garantia de backup completo sem usar o espaço necessário para um backup completo.

Vantagens: produz uma pequena imagem de backup quando comparado ao backup completo, pois somente os blocos alterados (blocos que não coincidem com o último backup) são armazenados em backup.

Desvantagens: o tempo de backup é longo, pois todos os blocos de origem são comparados aos blocos do último backup.

Incremental

Especifica a programação de backups para backups incrementais.

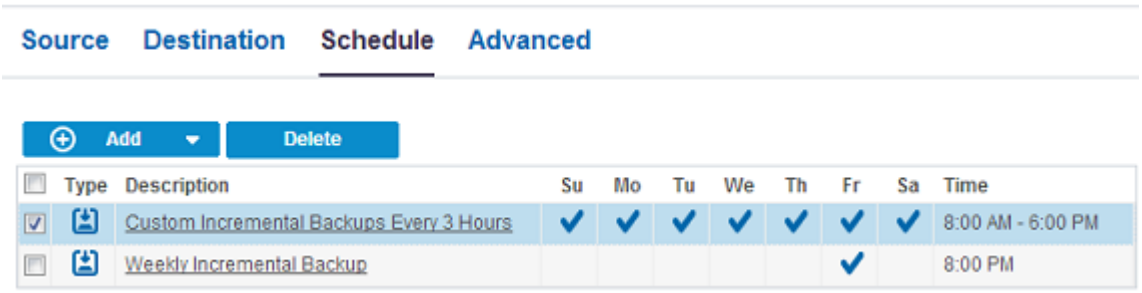
Conforme programado, o Arcserve UDP faz backup incremental apenas dos blocos que foram alterados após o último backup realizado com êxito. As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a executar um backup.

d. Especifique a hora de início do backup.

e. (Opcional) Marque a caixa de seleção de **Repetição** e especifique a programação a ser repetida.

f. Clique em **Salvar**.

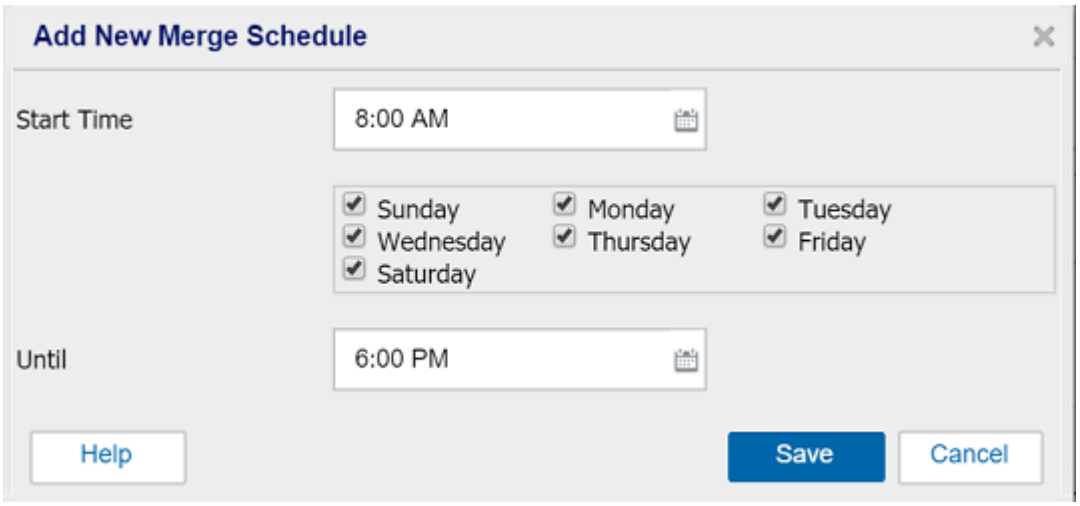
A programação de backup é especificada e aparece na página **Programar**.



Adicionar Programação de mesclagem

a. Clique em **Adicionar** e selecione **Adicionar programação de mesclagem**.

   A caixa de diálogo **Adicionar nova programação de mesclagem** é aberta.



b. Especifique a hora de início para iniciar a tarefa de mesclagem.

c. Especificar **Até** para especificar uma hora de término para a tarefa de mesclagem.

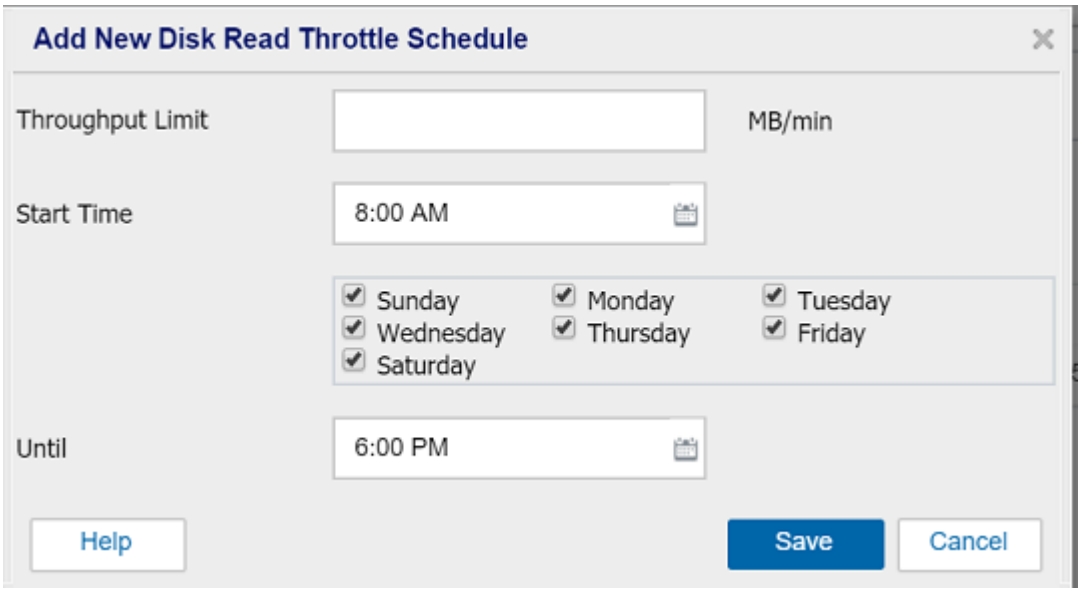
d. Clique em **Salvar**.

A programação de mesclagem é especificada e exibida na página de **Programação**.

Adicionar programação de acelerador de leitura de disco

a. Clique em **Adicionar** e selecione **Adicionar programação de acelerador de leitura de disco**.

   A caixa de diálogo **Adicionar nova programação de acelerador de leitura de disco** é aberta.



b. Especifique o limite de taxa de transferência em MB por minuto.

c. Especifique a hora de início para iniciar a tarefa de taxa de transferência de backup.

d. Especifique **Até** para especificar um horário de término para a tarefa de taxa de transferência.

e. Clique em **Salvar**.

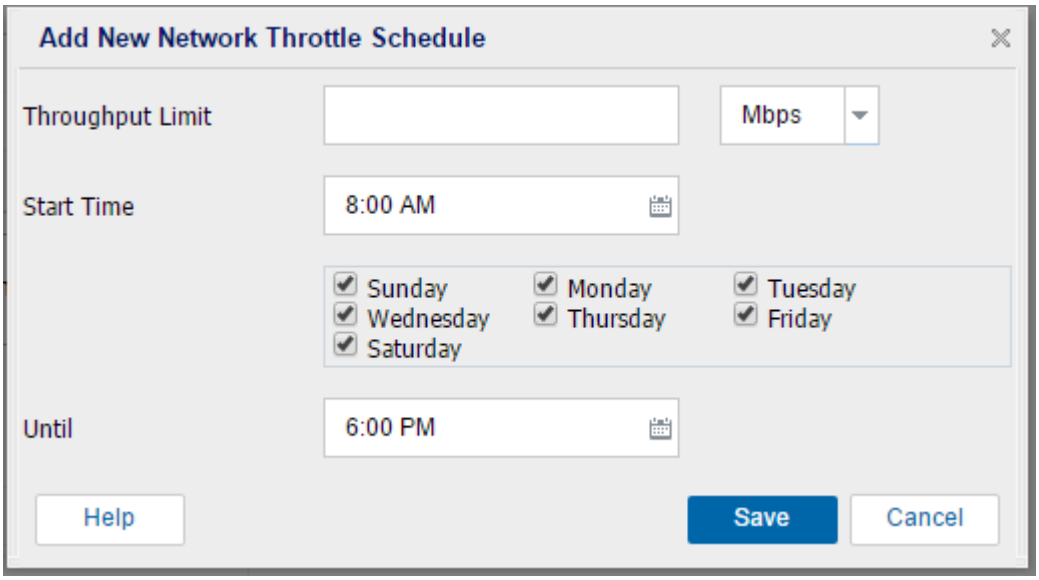
A Programação de acelerador de leitura de disco é especificada e aparece na página **Programação**.

Adicionar programação de acelerador de rede

Observação: a Programação de acelerador de rede é exibida apenas para backup com base em agente do Windows ao definir um repositório de dados com redução de redundância ativada como o destino para o plano.

a. Clique em **Adicionar** e selecione **Adicionar programação de acelerador de rede**.

   A caixa de diálogo **Adicionar nova programação de acelerador de rede** é aberta.



b. Especifique o limite de taxa de transferência em Mbps ou Kbps.

   Observação: o valor mínimo padrão é 500 Kbps. Para alterar o padrão valor, siga estas etapas:

   i. No caminho de registro SOFTWARE\Arcserve\Unified Data Protection\Management\Console, insira uma chave MinNetworkThrottleValueInKpbs, especifique o tipo como REG_SZ e defina um valor para ela.

   ii. Reinicie o serviço de gerenciamento do Arcserve UDP.

   iii. Modifique o plano ou crie outro plano.

   O valor personalizado entra em vigor.

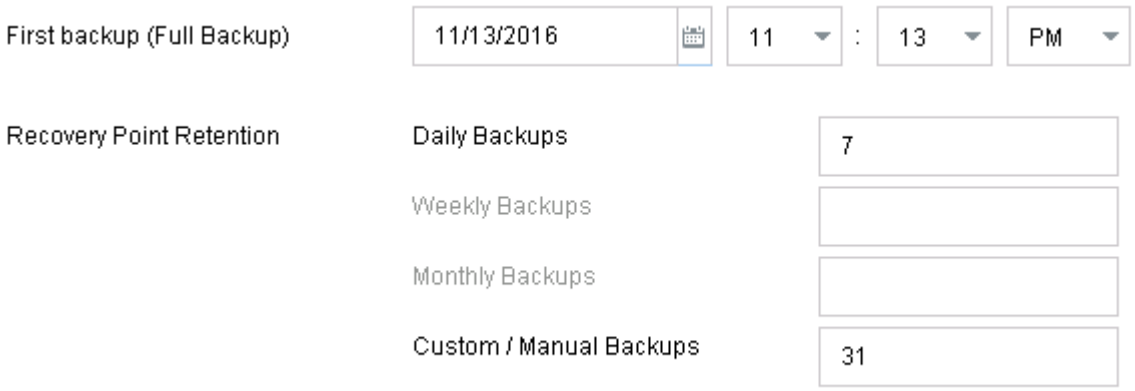
c. Especifique a hora de início para iniciar a tarefa de taxa de transferência de backup.

d. Especifique **Até** para especificar um horário de término para a tarefa de taxa de transferência.

e. Clique em **Salvar**.

A Programação de acelerador de rede é especificada e aparece na página **Programação**.

2. Especifique a hora de início do backup programado.



3. Especifique as configurações de retenção de pontos de recuperação para programação diária, semanal e mensal.

   Essas opções serão ativadas se tiver adicionado a programação de backup correspondente. Se você modificar as configurações de retenção desta página, as alterações serão refletidas na caixa de diálogo Programação de backup.

   A programação é especificada.

Noções básicas sobre a programação avançada e retenção

A opção de programação permite especificar uma programação personalizada, uma programação diária/semanal/mensal ou ambas. Na programação personalizada, é possível configurar a programação de backups para cada dia da semana ou adicionar até quatro programações de backup em cada dia. É possível escolher um dia específico da semana e criar uma janela para definir quando executar o backup e em que frequência.

Programação	Tarefa com suporte	Comentários
Backup	Tarefa de backup	Definir janelas de tempo para a execução de tarefas de backup.
Limitação de backup	Tarefa de backup	Definir janelas de tempo para controlar a velocidade de backup.
Mesclar	Tarefa de mesclagem	Definir quando executar tarefas de mesclagem.
Programação diária	Tarefa de backup	Definir quando executar tarefas do backup diário.
Programação semanal	Tarefa de backup	Definir quando executar tarefas do backup semanal.
Programação mensal	Tarefa de backup	Definir quando executar tarefas do backup mensal.

Também é possível especificar as configurações de retenção para os pontos de recuperação.

Observação: as configurações de retenção devem ser definidas em cada plano para controlar como os dados dos nós atribuídos a esse plano são retidos no repositório de dados de destino.

As programações para backups diários/semanais/mensais são independentes para a programação personalizada e umas das outras. É possível configurar para executar somente o backup diário, semanal ou mensal, sem configurar a Programação personalizada.

Programação de tarefas de backup

É possível adicionar quatro janelas de tempo por dia na programação do backup. Uma janela de tempo é válida das 00:00 às 23:59. Não é possível especificar uma janela de tempo das 18:00 às 6:00. Nesses casos, você deve especificar manualmente duas janelas de tempo diferentes.

Para cada janela de tempo, a hora de início é inclusiva e a hora de término é exclusiva. Por exemplo, você configurou para executar o backup incremental em intervalos de uma hora entre as 6:00 e as 9:00. O backup será iniciado às 6:00. Isso significa que o backup será executado às 6h00, 7h00 e 8h00, mas NÃO às 9h00.

Observação: se você deseja executar a tarefa de backup várias vezes até o fim do dia, defina a programação para até 0h00. Por exemplo, para executar a tarefa de backup a cada 15 minutos o dia inteiro, defina a programação como das 0h00 às 00h00, a cada 15 minutos.

Programação do acelerador de backup

A programação de aceleração do backup permite controlar a velocidade da taxa de transferência de backup o que, por sua vez, controla o uso de recursos (E/S de disco, CPU, largura de banda de rede) do servidor cujo backup está sendo feito. Isso é útil quando se não quiser afetar o desempenho do servidor durante o horário comercial. É possível adicionar quatro janelas de tempo por dia na sua programação de aceleração do backup. Para cada janela de tempo, é possível especificar um valor, em MB por minuto. Esse valor será usado para controlar a taxa de transferência do backup. Os valores válidos variam entre 1 MB/minutos a 99999 MB/minutos.

Se uma tarefa de backup estende seu tempo especificado, o limite de aceleração será ajustado de acordo com o tempo especificado. Por exemplo, você definiu o limite de aceleração de backup como 500 MB/minuto das 8:00 às 20:00 e 2500 MB/minuto das 20:00 às 22:00. Se uma tarefa de backup iniciar às 19h00 e for executada durante três horas, das 19h00 às 20h00 o limite de aceleração será de 500 MB/minuto e das 20h00 às 22h00, o limite de aceleração será 2500 MB/minuto.

Se não definir nenhuma programação do backup e programação da taxa de transferência do backup, o backup será executado o mais rápido possível.

Mesclar a programação

Permite mesclar pontos de recuperação com base na programação fornecida.

Considere os seguintes pontos para a tarefa de mesclagem:

- A qualquer momento apenas uma tarefa de mesclagem pode ser executada para um nó.
- Se uma tarefa de mesclagem iniciar, ela precisará ser concluída antes que a próxima tarefa de mesclagem seja iniciada. Isso significa que, se um ou mais conjuntos de pontos de recuperação forem mesclados, não será possível adicionar o

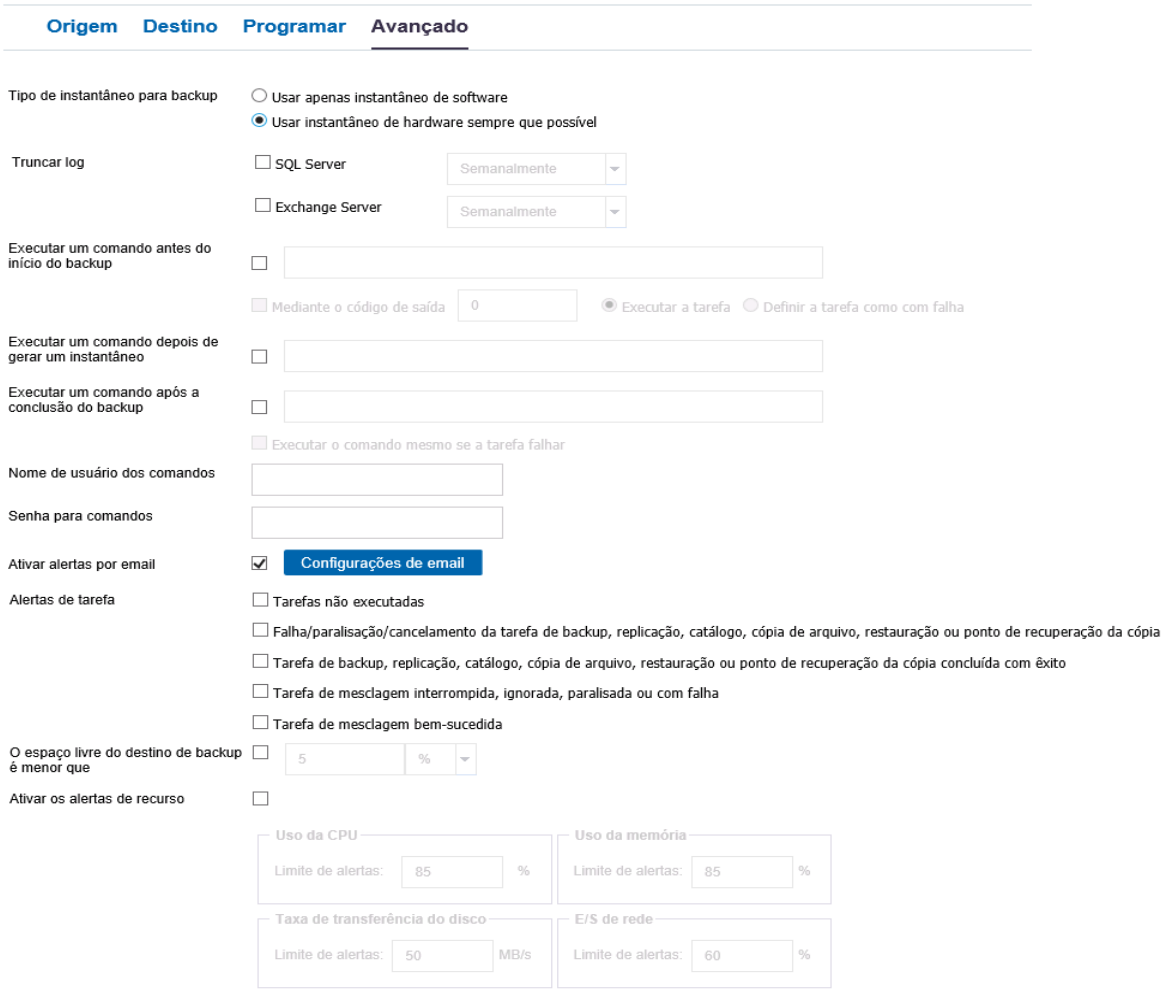
novo ponto de recuperação a este processo de mesclagem, até que o processo de mesclagem do conjunto atual de ponto de recuperação seja concluído.

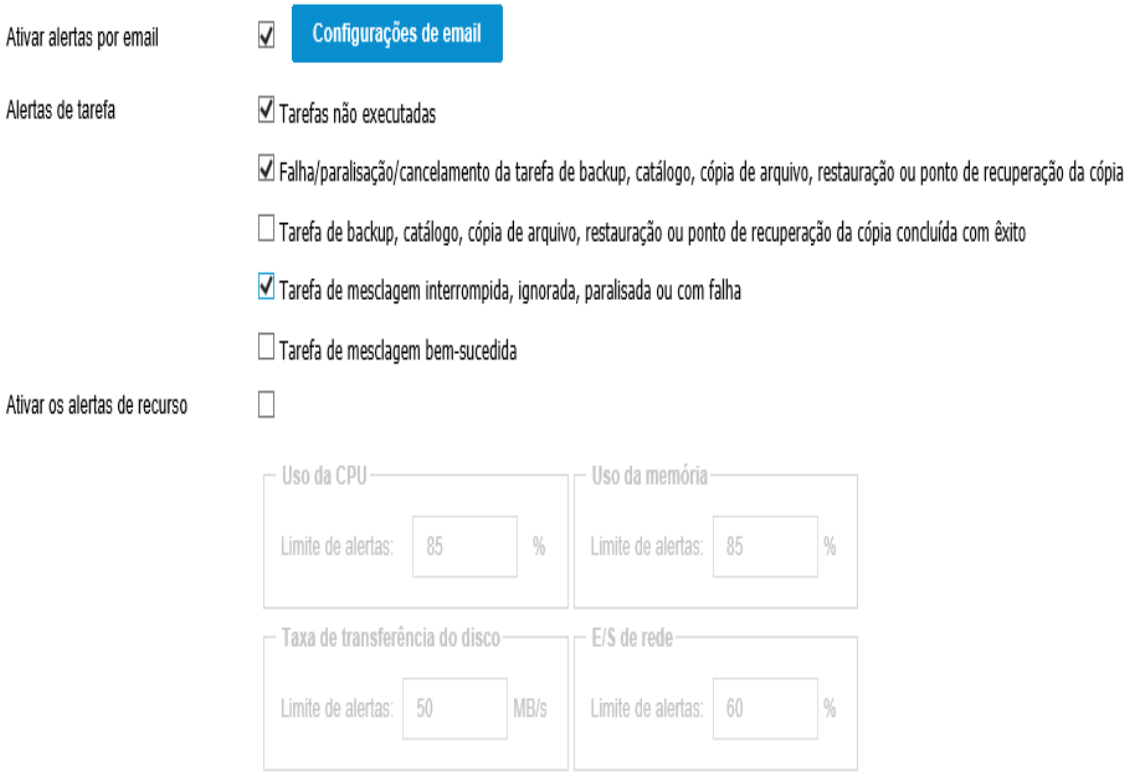
- Se uma tarefa de mesclagem estiver processando mais de um conjunto de pontos de recuperação (por exemplo, conjunto [1~4], conjunto [5~11] e conjunto [12~14]; são três conjuntos) o servidor de ponto de recuperação processará esses conjuntos, um por um.
- Se uma tarefa de mesclagem é retomada após um intervalo, a tarefa detectará em que ponto ela foi pausada e continuará a mesclagem a partir do ponto de pausa.

Especificar as configurações avançadas

A guia **Avançado** permite especificar algumas configurações avançadas para a tarefa de backup. As configurações avançadas incluem fornecer configurações de log de truncamento, a localização de quaisquer scripts e as configurações de email.

A imagem a seguir mostra a guia Avançado:


Origem
Destino
Programar
Avançado
Tipo de instantâneo para backup
Usar apenas instantâneo de software
Usar instantâneo de hardware sempre que possível
Truncar log
SQL Server
Semanalmente
Exchange Server
Semanalmente
Executar um comando antes do início do backup
Mediante o código de saída
0
Executar a tarefa
Definir a tarefa como com falha
Executar um comando depois de gerar um instantâneo
Executar um comando após a conclusão do backup
Executar o comando mesmo se a tarefa falhar
Nome de usuário dos comandos
Senha para comandos
Ativar alertas por email
Configurações de email
Alertas de tarefa
Tarefas não executadas
Falha/paralisação/cancelamento da tarefa de backup, replicação, catálogo, cópia de arquivo, restauração ou ponto de recuperação da cópia
Tarefa de backup, replicação, catálogo, cópia de arquivo, restauração ou ponto de recuperação da cópia concluída com êxito
Tarefa de mesclagem interrompida, ignorada, paralisada ou com falha
Tarefa de mesclagem bem-sucedida
O espaço livre do destino de backup é menor que
5
%
Ativar os alertas de recurso
Uso da CPU
Limite de alertas:
85
%
Uso da memória
Limite de alertas:
85
%
Taxa de transferência do disco
Limite de alertas:
50
MB/s
E/S de rede
Limite de alertas:
60
%



Siga estas etapas:

1. Especifique os seguintes detalhes.

   Tipo de instantâneo para backup

   Selecione uma das opções a seguir para o instantâneo de backup.

   Usar apenas instantâneo de software

   Especifica que o tipo de backup usa apenas o instantâneo do software. O Arcserve UDP não verificará se há instantâneos de hardware. O instantâneo de software utiliza menos recursos nas máquinas virtuais. É possível usar essa opção se o servidor tiver menos configurações e menor velocidade de processamento.

   Usar instantâneo de hardware sempre que possível

   Especifica que o tipo de backup primeiro verifica se há um instantâneo de hardware. Se todos os critérios forem atendidos, o tipo de backup usa o instantâneo de hardware.

   Observação: para obter mais informações sobre os critérios de instantâneo de hardware, consulte o pré-requisito.

   Truncar log

Permite especificar a programação para truncar logs para o SQL Server e o Exchange Server. É possível especificar a programação como **Diária**, **Semanal** ou **Mensal**.

Ativar a limpeza de logs em intervalos por hora para SQL por meio de uma chave de Registro

- Defina as configurações do plano. Marque a opção "SQL Server" na seção "Truncar Log" sob a guia "Avançado" e, em seguida, selecione "Diário".
- Defina a chave de Registro na máquina do SQL Server em que o agente do UDP está hospedado. "PurgeSqlLogPerHour" é o intervalo em horas para a limpeza de logs do SQL.

  Caminho: HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

  Nome do valor: PurgeSqlLogPerHour (indica o intervalo em horas para a limpeza de logs do SQL).

  Tipo de valor: REG_DWORD

Nome de usuário

Permite especificar o usuário que possui autorização para executar um script.

Senha

Permite especificar a senha do usuário que está autorizado a executar o script.

Executar um comando antes do início do backup

Permite a execução de um script antes de iniciar a tarefa de backup. Especifique o caminho completo onde o script está armazenado. Clique em **No código de saída** e especifique o código de saída para **Executar tarefa** ou **Tarefa com falha**. **Executar a tarefa** indica que a tarefa de backup continuará quando o script retornar o código de saída. **Tarefa com falha** indica que a tarefa de backup será interrompida quando o script retornar o código de saída.

Executar um comando após a criação de um instantâneo

Permite executar um script depois que o backup do instantâneo for gerado. Especifique o caminho completo onde o script está armazenado.

Para executar o script pós-instantâneo mesmo durante uma falha do instantâneo, selecione **Executar o comando mesmo quando o instantâneo falha**.

Executar um comando após a conclusão do backup

Permite executar um script depois que a tarefa de backup foi concluída. Especifique o caminho completo onde o script está armazenado.

Ativar alertas por email

Permite ativar alertas por email. É possível especificar configurações de email e os tipos de alertas que você deseja receber por email. Ao selecionar esta opção, as seguintes opções serão ativadas para a seleção.

Configurações de email

Permite configurar as definições de email. Clique em **Configurações de email** e configure o servidor de email e os detalhes do servidor proxy. Para obter mais informações sobre como definir as configurações de email, consulte Configurar email e alerta.

Alertas de tarefa

Permite que você selecione os tipos de emails da tarefa que deseja receber.

Ativar os alertas de recurso

Permite que você especifique um limite de uso da CPU, o uso da memória, a taxa de transferência de disco, E/S de rede. Você pode fornecer o valor em porcentagem. Você receberá um email quando o valor exceder o Limite de alerta.

2. Clique em **Salvar**.

Observação: quando você seleciona um nó como origem de backup ou proxy de backup, o Arcserve UDP verifica se o agente está instalado no nó e se é a versão mais recente. Em seguida, o Arcserve UDP exibe uma caixa de diálogo de verificação que lista todos os nós que possuem uma versão antiga do agente ou que não tem o agente instalado. Para instalar/atualizar o agente nesses nós, selecione o método de instalação e clique em Salvar.

As alterações são salvas e uma marca de seleção verde é exibida ao lado do nome da tarefa. A página do plano é fechada.

Observação: se precisar adicionar outra tarefa, deverá selecionar o plano na guia **Recursos** e modificar o plano. Para modificar o plano, clique no plano do painel central. O plano é exibido e será possível modificá-lo.

O plano de backup é criado e implantado automaticamente para o nó de origem. O backup é executado de acordo com a programação que você configurou na guia **Programar**. Também é possível fazer backup manual quando desejado.

(Opcional) Executar um backup manual

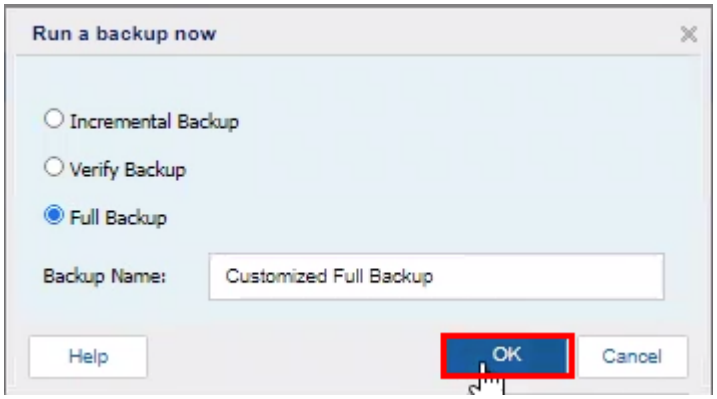
Em geral, os backups são executados automaticamente e controlados pelas configurações da programação. Além do backup programado, um backup manual fornece a opção de fazer backup dos nós de acordo com a necessidade. Por exemplo, se você repetir a programação para backups completos, incrementais e de verificação e desejar fazer grandes alterações em seu computador, deverá executar um backup manual imediato sem esperar até que ocorra o próximo backup programado.

Siga estas etapas:

1. Efetue logon no Console do Arcserve UDP.
2. Navegue até **recursos** > **Plano** > **Todos os planos**.

   A lista de todos os planos é exibida no painel central.
3. Clique com o botão direito do mouse no plano e selecione **Fazer backup agora**.

   A caixa de diálogo Fazer backup agora é exibida.
4. Na caixa de diálogo Executar um backup agora, selecione o tipo de backup que deseja executar e, em seguida, especifique o nome do backup, se necessário.



As opções disponíveis são:

Backup incremental

Inicia um backup incremental do computador inteiro. Um backup incremental realiza backup somente dos blocos que foram alterados desde o backup anterior.

Observação: se estiver executando um backup pela primeira vez, o backup completo será iniciado automaticamente, mesmo que você tenha selecionado a opção Backup incremental.

As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a execução de backups.

Verificar backup

Inicia um backup de verificação do computador, examinando o backup mais recente de cada bloco e comparando o conteúdo e as informações com a origem. Esta comparação verifica se o backup mais recente dos blocos representa as informações correspondentes na origem. Se a imagem de backup de algum bloco não corresponder à origem, o agente do Arcserve UDP (Windows) atualizará (ressincronizará) o backup do bloco divergente.

Vantagem: uma imagem de backup muito pequena é gerada quando comparada ao backup completo porque somente os blocos alterados (blocos que não correspondam ao último backup) são armazenados em backup.

Desvantagem: o tempo do backup fica lento porque todos os blocos do disco de origem são comparados aos blocos do último backup.

Backup completo

Inicia um backup completo do computador inteiro ou dos volumes selecionados.

Observações:

- se você adicionar um novo volume à origem do backup, será feito um backup completo do volume recém-adicionado, independentemente do método de backup geral selecionado.
- Se nenhum nome de backup for especificado, por padrão, ele será automaticamente nomeado como Backup completo/incremental/de verificação personalizado.

5. Clique em **OK**.

   A caixa de diálogo Informações do andamento é exibida.

6. Aguarde até que a tarefa de backup seja concluída e clique em **OK**.

7. Para monitorar as tarefas de backup, navegue até **tarefas** > **Tarefas em andamento**.

   Aguarde até a conclusão da tarefa de backup.

   Observação: apenas uma tarefa pode ser executada em uma hora. Se você tentar iniciar manualmente uma tarefa de backup quando outra tarefa estiver em execução no mesmo momento, uma mensagem de alerta será exibida informando

sobre a existência de outra tarefa em execução e solicitando uma nova tentativa mais tarde.

O backup manual é realizado com êxito.

Verificar o backup

Para verificar a tarefa de backup, confirme se você criou com êxito o plano de backup. Depois de verificar se o plano está criado com êxito, confirme se a tarefa de backup é executada conforme o programado. É possível verificar o status das tarefas de backup na guia **Tarefas**.

Siga estas etapas para verificar os planos:

1. Clique na guia **Recursos**.
2. No painel esquerdo, navegue para **Nós** e clique em **Todos os nós**.

   Uma lista de todos os nós é exibida no painel central.
3. Verifique se os planos são mapeados com nós.

Siga um destes métodos para verificar as tarefas de backup:

Método 1

1. Clique na guia **Tarefas**.
2. No painel à esquerda, clique em **Todas as tarefas concluídas**.

   O status de cada tarefa é incluído no painel central.
3. Verifique se a tarefa de backup é concluída com êxito.

   A tarefa de backup é verificada.

Método 2

1. Clique na guia **Tarefas**.
2. No painel esquerdo, clique em **Tarefas concluídas com êxito**.

   A lista de tarefas de backup concluídas é exibida no painel central.
3. Clique na tarefa que você deseja verificar.

   O painel direito é atualizado.
4. Em Detalhes da tarefa, clique no hiperlink **Exibir logs**.
5. Verifique se a tarefa de backup é concluída com êxito.

   A tarefa de backup é verificada.

Como criar um plano de backup do Nutanix

Para proteger os nós do Nutanix, é necessário criar um plano. Os nós do plano consistem em uma tarefa de backup. Esta tarefa de backup permite especificar os nós que deseja proteger, o destino do backup e a programação de backup. O destino do backup é um servidor de ponto de recuperação onde você deseja armazenar os dados de backup. O destino também pode ser um destino local ou uma pasta compartilhada remota.

Para explorar as funções disponíveis para o recurso Nutanix no Arcserve UDP, consulte How to Work With Nutanix Using Arcserve UDP.

Como criar um modo de espera virtual para o Nutanix AHV

Para proteger o modo de espera virtual no Nutanix AHV, consulte Protecting Virtual Standby on Nutanix AHV.

Como criar uma máquina virtual instantânea no Nutanix AHV

Para criar uma máquina virtual instantânea no Nutanix AHV, consulte Como criar uma máquina virtual instantânea no Nutanix AHV.

Como criar um plano de recuperação garantida e proteger o Nutanix AHV para o nó do Linux

Para criar um plano de recuperação garantida e proteger o Nutanix AHV para o nó do Linux, consulte Como criar um plano de recuperação garantida e proteger o Nutanix AHV para o nó do Linux.

Como fazer backup de volumes compartilhados do agrupamento

O Arcserve UDP oferece suporte ao backup de CSVs (Cluster Shared Volume - Volume Compartilhado do Agrupamento) a partir da versão 6.5 Atualização 4. Os volumes CSV são criados em espaços de armazenamento e são transparentes para o agente do Arcserve UDP (Windows). O CSV é sempre considerado para backup completo no nível do volume, independentemente do tipo de tarefa de backup (completo ou incremental). O backup de CSV protege os dados de todos os sistemas de arquivos populares, como NTFS, redução de redundância para NTFS, ReFS e CSVFS.

É possível criar um plano com base em agente ou atualizar um plano com base em agente existente no console do Arcserve UDP a fim de fazer backup de um CSV específico.

Siga estas etapas:

1. Selecione o volume compartilhado do agrupamento na máquina do agente. Para obter mais informações, consulte Modificar configurações da máquina do agente para fazer backup de volumes CSV.

Observação: também é possível executar a tarefa de backup na máquina do agente do Windows. Para obter mais informações, consulte a página sobre como executar backups a partir da máquina de agente do Windows.

2. Para executar o backup a partir do console do Arcserve UDP, vá até a guia **Recursos**.
3. No painel à esquerda, navegue para **Planos** e clique em **Todos os planos**.
4. No painel central, clique em **Adicionar um plano** e especifique um nome de plano.
5. Na lista suspensa **Tipo de tarefa**, selecione **Backup: Windows com base em agente**.
6. Na guia **Origem** do plano, marque a caixa de seleção de **Fazer backup de todos os volumes** como **Tipo de proteção**.
7. Especifique os detalhes avançados, de destino e de programação. Para obter mais informações, consulte Como criar um plano de backup do Windows.

   Agora, depois de salvar o plano, ao executar a tarefa de backup, será feito o backup do volume CSV especificado no agente do Windows.
8. Verifique o status das tarefas armazenadas em backup. Para obter mais informações, consulte Verificar o backup.

   Observações:

   - O log de atividades do nó do proprietário exibe o andamento da tarefa de backup e registra a mensagem de êxito após a conclusão do backup. O log de atividades do nó do membro (que não é o proprietário) exibe uma mensagem de aviso, conforme indicado abaixo, mas o status do backup aparece como bem-sucedido.

     Aviso: Falha ao buscar a localização física do volume compartilhado de agrupamento [C:\ClusterStorage\Volume1]. Esse volume será excluído do backup.

   - Se desejar excluir o volume CSV durante o backup, execute as seguintes etapas:

     a. No nó do agente do UDP, abra o Registro com o seguinte caminho:

        HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

     b. Crie um DWORD como 'BackupCSV'.

c. Defina o valor como 0.

   O volume CSV agora será excluído durante o backup.

Modificar configurações da máquina do agente para fazer backup de volumes CSV

Antes de executar seu primeiro backup, especifique as configurações de backup que serão aplicadas a cada tarefa de backup. Essas configurações podem ser mantidas para backup futuro ou podem ser modificadas a qualquer momento usando a página inicial do agente do Arcserve UDP (Windows).

Siga estas etapas:

1. Na página inicial do agente do Arcserve UDP (Windows), ou no monitor do agente do Arcserve UDP (Windows), clique em **Configurações**.

   A janela Configurações é aberta.

2. Clique na guia **Configurações de backup**.

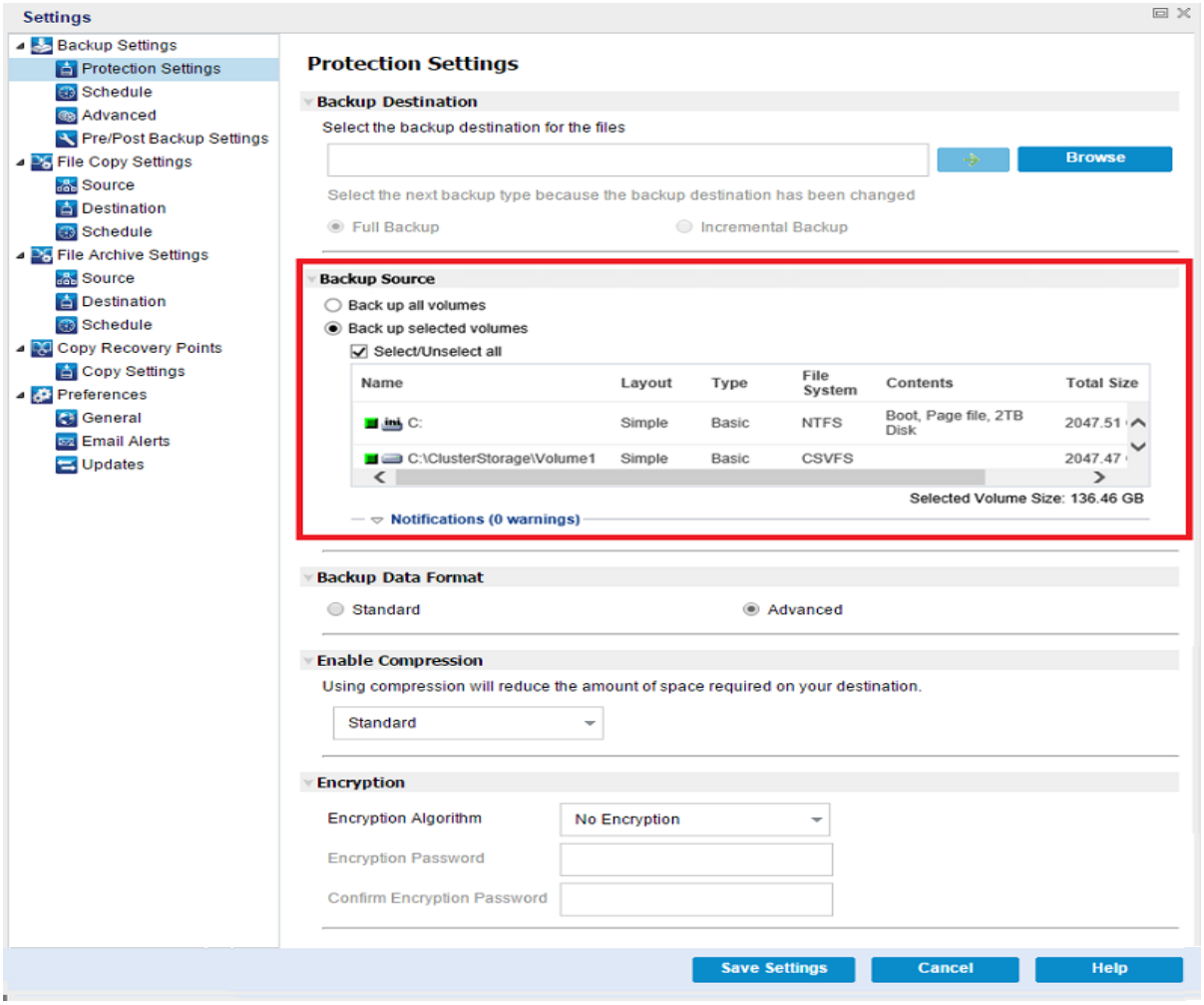
   A janela Configurações de backup é aberta.

3. Clique em Configurações de proteção.

4. A janela Configurações de proteção é aberta.

   Observações:

   - Se o agente do Arcserve UDP (Windows) estiver sendo gerenciado pelo console, nem todas as configurações estarão disponíveis e serão exibidas como informações somente leitura.
   - Quando o agente é gerenciado pelo console e não está protegido em um plano, todas as configurações estarão ainda disponíveis, exceto Preferência > Painel de atualizações.



5. No grupo **Origem do backup**, selecione **Fazer backup dos volumes selecionados**.

   A lista de volumes disponíveis na máquina do agente é exibida.

6. Selecione o volume CSV do qual você deseja fazer backup e clique em **Salvar configurações**.

   As configurações de proteção de backup são salvas.

Como fazer backup de volumes sem letra de unidade

No Arcserve UDP v6.5 Atualização 4, é possível proteger os volumes sem letra de unidade usando a opção **Volumes montados na pasta NTFS** em **Fazer backup dos volumes selecionados**. Antes de selecionar a opção **Volumes montados na pasta NTFS** no console do Arcserve UDP, você deve montar o volume da pasta NTFS. Você também pode personalizar ainda mais e fazer backup de apenas alguns volumes sem letra de unidade, em vez de fazer backup de todos eles.

Para obter mais informações, verifique o seguinte:

- Verificar pré-requisitos
- Montar volume sem letra de unidade na pasta NTFS
- Especificar volume sem letra de unidade no Registro

Verificar pré-requisitos

Revise o seguinte:

- Para que o repositório de dados esteja em execução nas reinicializações do RPS, ative a montagem automática no servidor de RPS. Você pode ativar a montagem automática usando o comando de montagem automática disk-part.

  Siga estas etapas:

  1. Abra um prompt de comando com privilégios elevados.
  2. No prompt de comando com privilégios elevados, faça o seguinte:
  3. Digite *diskpart* e pressione **Enter**.
  4. Digite *automount enable* e pressione **Enter**.
  5. Feche o prompt de comando com privilégios elevados.
  6. Para aplicar as alterações, reinicie o computador.

Montar volume sem letra de unidade na pasta NTFS

Você deve montar o volume sem letra de unidade na pasta NTFS para fazer backup do volume e do conteúdo do ponto de montagem.

Siga estas etapas:

1. No **Gerenciador de discos do Windows**, selecione um novo disco que não tenha uma letra de unidade atribuída a ele.
2. Nas opções exibidas ao clicar com o botão direito do mouse, clique em **Alterar letra de unidade e caminho**.

   A caixa de diálogo Adicionar letra de unidade ou caminho é aberta.
3. Clique em **Alterar**.

   A caixa de diálogo Alterar letra de unidade ou caminho é aberta.
4. Selecione **Montar na seguinte pasta NTFS vazia**, especifique o caminho a seguir e clique em **OK**.

   C:\MountPoint

O ponto de montagem é exibido no Windows Explorer. Você montou o volume sem letra de unidade com êxito.

Especificar volume sem letra de unidade no Registro

Você deve especificar o volume sem letra de unidade no Registro para proteger o volume e o conteúdo no ponto de montagem.

Siga estas etapas:

1. No **Gerenciador de discos do Windows**, selecione um novo disco que não tenha uma letra de unidade atribuída a ele.
2. Nas opções exibidas ao clicar com o botão direito do mouse, clique em **Propriedades**.

   A janela de propriedades do disco é aberta.
3. Na guia **Segurança**, copie o **Nome do objeto**.
4. Na máquina **Agente do Windows**, navegue até o respectivo **Nó do agente** e abra o **Registro**.

   A janela do Registro é aberta.
5. Navegue até o caminho abaixo e clique em **BackupVolumesWIthMountedVolumes**.

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   A caixa de diálogo Editar cadeia de caracteres múltipla é exibida.
6. No campo **Dados do valor**, adicione o nome do objeto copiado.
7. Clique em **OK**.

   O volume sem letra de unidade é especificado no registro.

   Quando você executar o backup do console do Arcserve UDP, somente os volumes especificados no Registro serão considerados para o backup.

Como fazer backup do volume selecionado

Este tópico descreve como fazer backup apenas dos volumes selecionados, em vez de executar um backup completo. Para fazer backup de um volume específico, é necessário marcar a caixa de seleção **Fazer backup dos volumes selecionados** da opção Origem durante a criação de um plano.

Siga estas etapas:

1. Ao criar ou modificar um plano, selecione a guia Origem.
2. Marque a caixa de seleção de Fazer backup dos volumes selecionados como tipo protegido.

   Vários campos serão exibidos para selecionar outras opções relacionadas ao volume.
3. Selecione uma ou várias unidades na lista de unidades.
4. Selecione uma ou várias opções na lista de volumes a seguir:

   Volume reservado do sistema

   Refere-se ao volume exigido ao inicializar o sistema operacional. Selecione essa opção se desejar executar uma BMR do nó de backup ou executar o backup de uma unidade específica.

   Volume de recuperação

   Refere-se ao volume necessário para o ambiente de recuperação do Windows. Selecione essa opção para fazer backup do volume de recuperação.

   Volume de inicialização

   Refere-se ao volume exigido ao inicializar o sistema operacional Windows. Selecione essa opção se desejar executar uma BMR do nó de backup ou executar o backup de uma unidade específica.

   Volumes montados na pasta NTFS

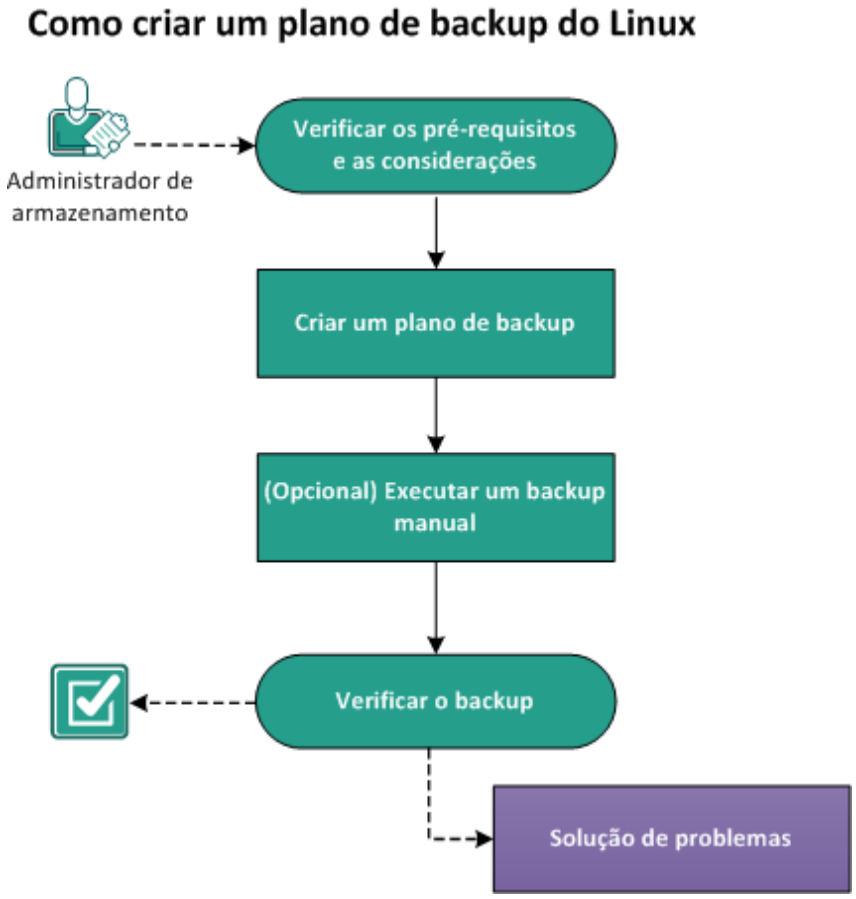
   Refere-se à opção de volumes montados na pasta NTFS. Selecione esta opção se for possível fazer backup de volumes sem letra de unidade. Antes de selecionar a opção no plano, é necessário montar o volume da pasta NTFS. Você também pode personalizar ainda mais e fazer backup de apenas alguns volumes sem letra de unidade, em vez de fazer backup de todos eles. Para obter mais informações, consulte Como fazer backup de volumes sem letra de unidade
5. Insira os detalhes nas outras guias do plano e salve o plano.

   Você especificou a unidade ou o volume. Será feito backup apenas do volume ou da unidade selecionada quando uma tarefa de backup for executada.

Como criar um plano de backup do Linux

Para proteger os nós do Linux, é necessário criar um plano. Um plano de backup de nós do Linux consiste em uma tarefa de backup. Esta tarefa de backup permite especificar os nós que deseja proteger, o destino do backup e a programação de backup. O destino de backup pode ser uma pasta de compartilhamento remota ou de destino local ou um repositório de dados em um servidor de ponto de recuperação.

O diagrama a seguir ilustra o processo para proteger os nós do Linux:



O que fazer a seguir?

1. Verificar os pré-requisitos e as considerações
2. Criar um plano de backup
3. (Opcional) Executar um backup manual
4. Verificar o backup
5. Solução de problemas

Verificar os pré-requisitos e as considerações

Preencha os seguintes pré-requisitos:

- Efetue logon no Console.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Criar um plano de backup

Um plano de backup inclui uma tarefa de backup que executa um backup do nó físico ou virtual e armazena os dados no destino especificado.

Siga estas etapas:

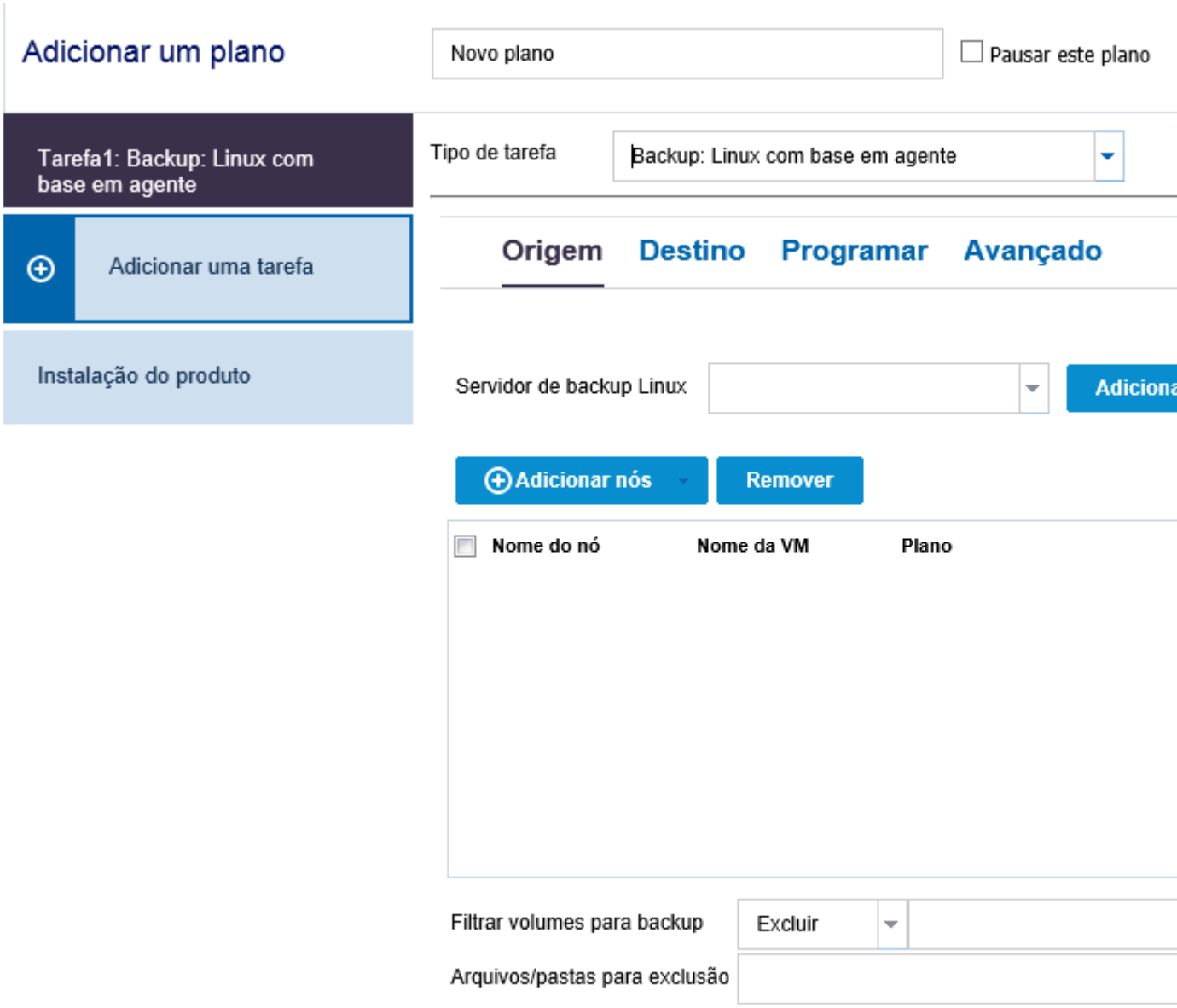
1. Efetue logon no Console do Arcserve UDP.
2. Navegue até a guia **recursos** > **Plano** > **Todos os planos**.

   Se tiver criado os planos anteriores, esses planos serão exibidos no painel central.
3. No painel central, clique em **Adicionar um plano**.

   A opção Adicionar um plano é aberta.
4. Digite o nome do plano.
5. (Opcional) Selecione a caixa de seleção **Pausar este plano**.

   O plano não será executado até que você desmarque a caixa de seleção para retomar o plano.

   Observação: se um plano for pausado, nenhuma tarefa em andamento será pausada, mas todas as tarefas programadas correspondentes associadas a esse plano serão pausadas. No entanto, você pode executar uma tarefa manualmente. Por exemplo, você pode executar manualmente a tarefa de backup e a tarefa de replicação para um nó mesmo que o respectivo plano esteja pausado. Nesse caso, a tarefa seguinte da tarefa sob demanda (manual) não será executada. Por exemplo, há uma tarefa de replicação após uma tarefa de backup sob demanda, a tarefa de replicação não será executada para a tarefa de backup sob demanda. É necessário executar manualmente a tarefa de replicação. Quando você retomar o plano, as tarefas pendentes não são retomadas imediatamente. Depois de retomar o plano, as tarefas pendentes serão executadas no próximo horário programado.
6. Na lista suspensa Tipo de tarefa, selecione **Backup: Linux com base em agente**.



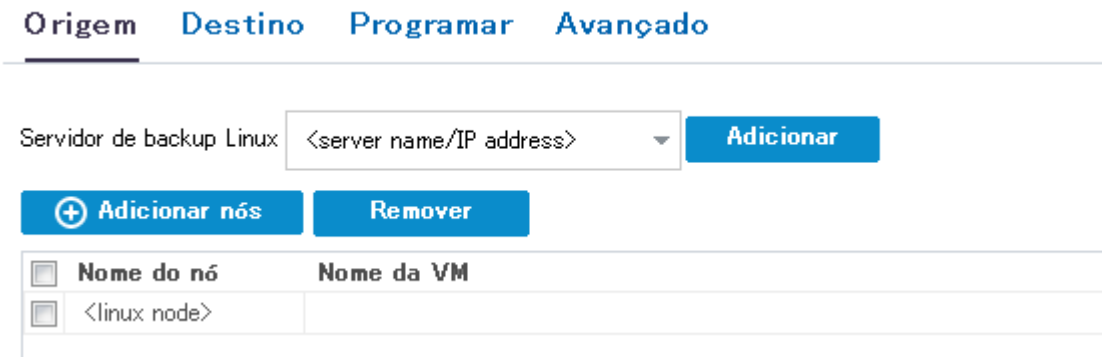
Agora especifique os detalhes de Origem, Destino, Programação e Avançado.

Especificar a origem

A página Origem permite especificar os nós de origem que deseja proteger. É possível selecionar mais de um nó em um plano. Caso não tenha adicionado nós no console, você pode adicionar nós da página de origem. É possível salvar um plano sem adicionar nós de origem, mas o plano não será implantado, a menos que você adicione todos os nós.

Siga estas etapas:

1. Clique na guia Origem.
2. Na lista suspensa Servidor de backup Linux, selecione o servidor de backup Linux.



3. (Opcional) Clique em **Adicionar** para adicionar um novo servidor de backup Linux à lista.
4. Clique em **++Adicionar** e selecione uma das seguintes opções:

   Selecionar os nós a serem protegidos no Arcserve UDP

   A caixa de diálogo Selecionar Nós para proteger é aberta. Selecione os nós na lista exibida. Selecione esta opção se você já tiver adicionado os nós para o console.

   Adicionar nó do Linux

   A caixa de diálogo Adicionar nós do Linux ao console do Arcserve UDP é exibida. Selecione esta opção se você não tiver adicionado os nós e desejar adicionar manualmente os nós para proteger.

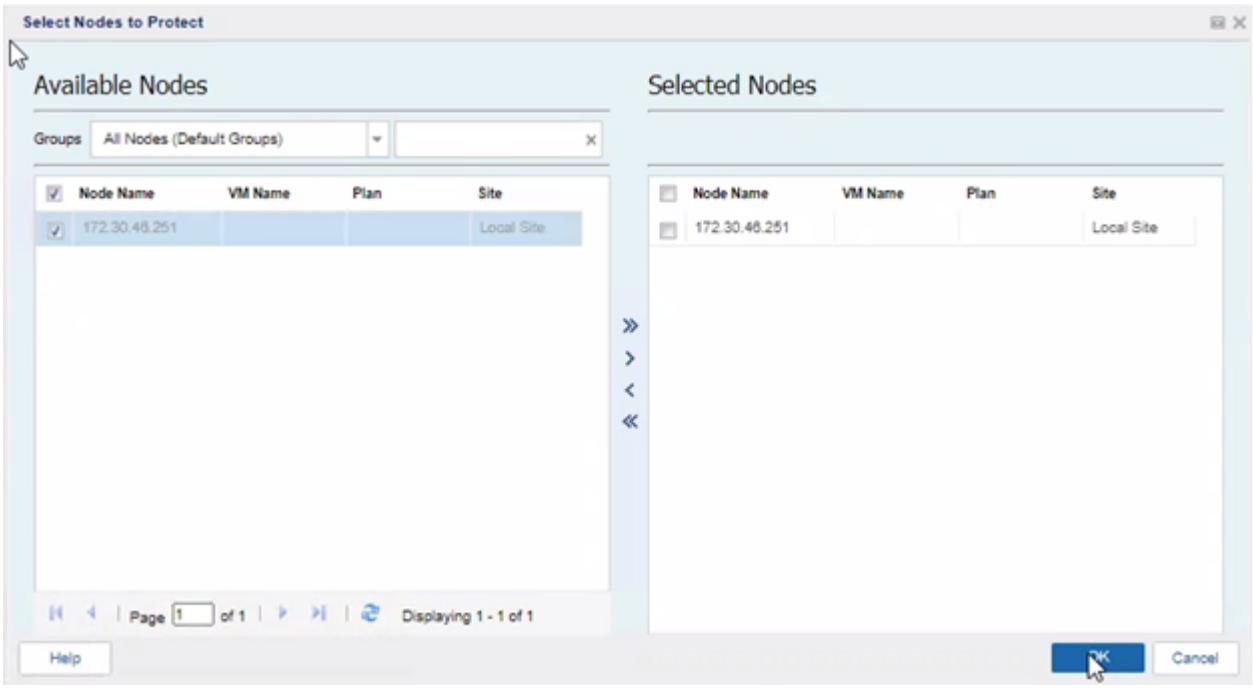
   Se selecionado, o nó do UDP Archiving é armazenado em backup pelo servidor de backup Linux instalado nesse próprio nó, mesmo se você seleciona outro servidor de backup Linux manualmente. Para o backup do nó ser feito por outro servidor de backup Linux, você pode adicionar esse nó como um nó Linux, em vez de adicioná-lo como um nó do UDP Archiving. Para obter mais informações, consulte Adicionar nós.
5. Na caixa de diálogo Selecionar nós para proteger, faça o seguinte:

a. (Opcional) Selecione um filtro na lista suspensa Grupos para filtrar os nós. É possível digitar as palavras-chave para filtrar melhor seus nós.

   Os nós são exibidos na coluna Nós disponíveis.

b. Selecione os nós na coluna Nós disponíveis, clique na seta para a direita e, em seguida, clique em **OK**.

   Os nós selecionados são exibidos na coluna Nós selecionados.



6. (Opcional) Forneça os detalhes para as seguintes opções:

   Filtrar volumes para backup

   Na lista suspensa, selecione **Incluir** ou **Excluir**. Incluir especifica que apenas os volumes especificados serão incluídos no backup. Não será feito backup de qualquer volume que não for especificado. Excluir especifica que os volumes serão excluídos do backup.

   Arquivos/pastas a serem excluídas

   Especifique os arquivos e as pastas que você não deseja incluir no backup para todos os nós listados. Se não desejar executar o backup de vários arquivos e várias pastas, separe cada arquivo e pasta usando um caractere de dois pontos (:). Forneça o caminho completo do arquivo e pasta que você deseja excluir.

7. Para a rede de backup designada, para selecionar a rede entre o LBS (Linux Backup Server - Servidor de backup Linux) e o nó do Linux, clique na caixa de seleção **Usar a rede selecionada para o tráfego de backup** e selecione a rede na lista suspensa.

Observação: se a rede de backup selecionada não estiver acessível e para continuar a tarefa com a rede disponível ou a rede padrão, clique na caixa de seleção **Continuar a executar a tarefa mesmo quando não for possível se conectar à rede de backup selecionada**.

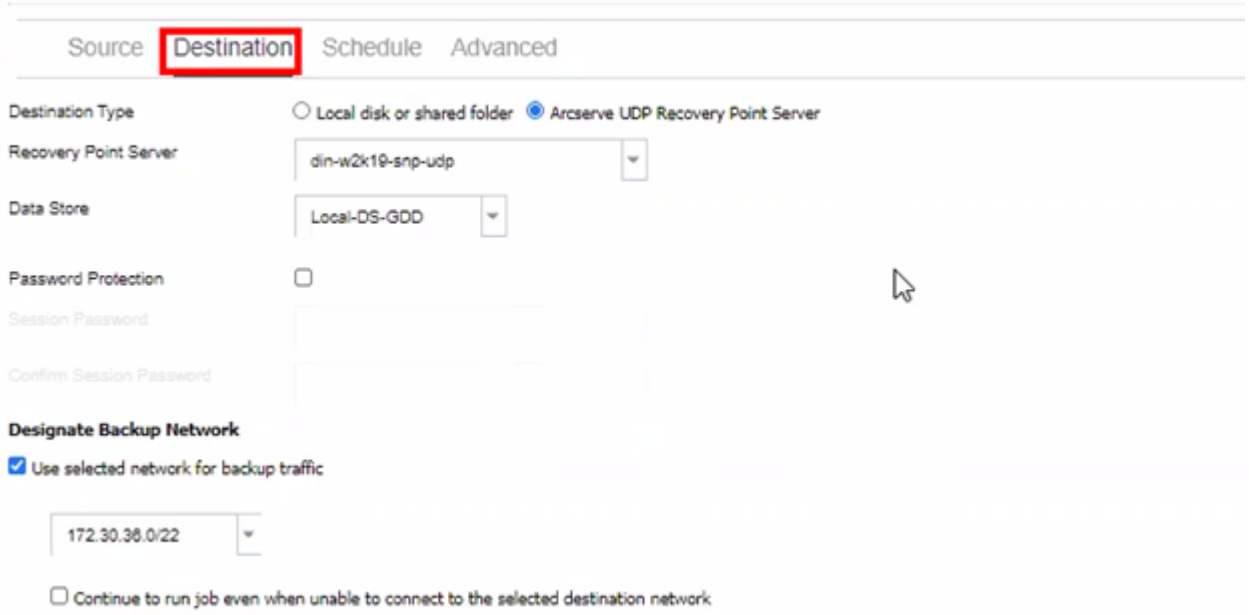
A origem é especificada.

Especificar o destino

O destino é o local onde você armazena os dados de backup. É necessário, no mínimo, especificar o destino para salvar o plano.

Siga estas etapas:

1. Clique na guia **Destino**.



2. Selecione um dos seguintes tipos de destino:

   Disco local ou uma pasta compartilhada

   Especifica que os dados de backup serão armazenados em um disco local ou em uma pasta compartilhada.

   Servidor de ponto de recuperação do Arcserve UDP

   Especifica que o destino de backup é um servidor de ponto de recuperação. Se selecionar essa opção, os dados serão armazenados como pontos de recuperação. Não é possível armazenar dados como conjuntos de dados de recuperação.

3. Se você selecionar o **disco local ou a pasta compartilhada** como um tipo de destino, forneça os seguintes detalhes:

   - Se tiver selecionado **Compartilhamento NFS**, digite os detalhes do destino de backup no seguinte formato:

     Endereço IP do compartilhamento de NFS:/caminho completo do local de armazenamento

- Clique no botão de seta para validar as informações do destino do backup.

  Se o destino do backup for inválido, uma mensagem de erro será exibida.

Observação: algumas versões do Domínio de dados do NAS não oferecem suporte ao mecanismo de bloqueio de arquivos do NFS. Como resultado, esse compartilhamento do NFS não pode ser usado como destino de backup. Para obter mais informações sobre esse problema, consulte Problemas de compatibilidade com o Agente do Arcserve Unified Data Protection para Linux.

- Se tiver selecionado **Compartilhamento CIFS**, digite os detalhes do destino de backup no seguinte formato:

  //nomehost/pasta_compartilhamento

  - Clique no botão de seta para validar as informações do destino do backup.

    Se o destino do backup for inválido, uma mensagem de erro será exibida.

  Observação: certifique-se de que o nome da pasta compartilhada não tenha espaços.

- Se você selecionou **Origem local**, siga estas etapas:

  a. Forneça o caminho do destino local.

     Por exemplo: /root

  b. Selecione um nível de compactação da lista suspensa Compactação para especificar um tipo de compactação a ser usado para o backup.

     As opções disponíveis para Compactação são:

     Compactação padrão

     Especifica um nível de compactação da lista suspensa Compactação para especificar um tipo de compactação a ser usado para o backup.

     Compactação máxima

     Especifica que essa opção proporciona maior uso da CPU (menor velocidade), mas também menos uso de espaço em disco para sua imagem de backup.

  c. Selecione um algoritmo na lista suspensa Algoritmo de criptografia e digite a senha de criptografia, se necessário.

d. Selecione o tipo de algoritmo de criptografia que deseja usar para os backups.

A criptografia de dados é a conversão de dados em uma forma ininteligível sem um mecanismo decodificador. A solução de proteção de dados do agente do Arcserve UDP (Linux) usa algoritmos de criptografia seguros AES (padrão de criptografia avançada) para atingir o máximo de segurança e privacidade dos dados especificados.

Para opções disponíveis de formatação de criptografia, consulte Configurações de criptografia.

- Um backup completo e todos os seus backups incrementais relacionados devem usar o mesmo algoritmo de criptografia.
- Se o algoritmo de criptografia para um backup incremental foi alterado, é necessário executar um backup completo.

Por exemplo, se você alterar o formato do algoritmo e, em seguida, executar um backup incremental, o tipo de backup é convertido automaticamente para um backup completo.

e. Quando um algoritmo de criptografia é selecionado, você deve fornecer (e confirmar) uma senha de criptografia.

- A senha de criptografia é limitada a um máximo de 23 caracteres.
- Um backup completo e todos os seus backups incrementais relacionados utilizam a mesma senha para criptografar dados.

- Se desejar fazer backup para o Amazon S3, faça o seguinte:

a. Selecione **Compartilhamento CIFS** e digite o armazenamento do Amazon S3 no seguinte formato

s3://Região S3/nome do compartimento de memória S3

b. Clique na seta e forneça as informações de acesso do Amazon S3.

4. Se você selecionar o **Servidor de ponto de recuperação do Arcserve UDP** como um tipo de destino, faça o seguinte:

- Servidor de ponto de recuperação: na lista suspensa, selecione o servidor de ponto de recuperação de destino.
- Repositório de dados: na lista suspensa, selecione o repositório de dados de destino.
- Proteção por senha: marque a caixa de seleção **Proteção por senha**, forneça a senha da sessão e digite a senha novamente para confirmar.

Observação: a senha da sessão é opcional quando o destino de backup é um repositório de dados do RPS não criptografado.

- Para a rede de backup designada, para selecionar a rede entre o LBS (Linux Backup Server - Servidor de backup Linux) e o RPS (Recovery Point Server - Servidor de ponto de recuperação), clique na caixa de seleção **Usar a rede selecionada para o tráfego de backup** e selecione a rede na lista suspensa.

  Observação: se a rede de backup selecionada não estiver acessível e para continuar a tarefa com a rede disponível ou com a rede padrão, clique na caixa de seleção **Continuar a executar a tarefa mesmo quando não for possível se conectar à rede de backup selecionada**.

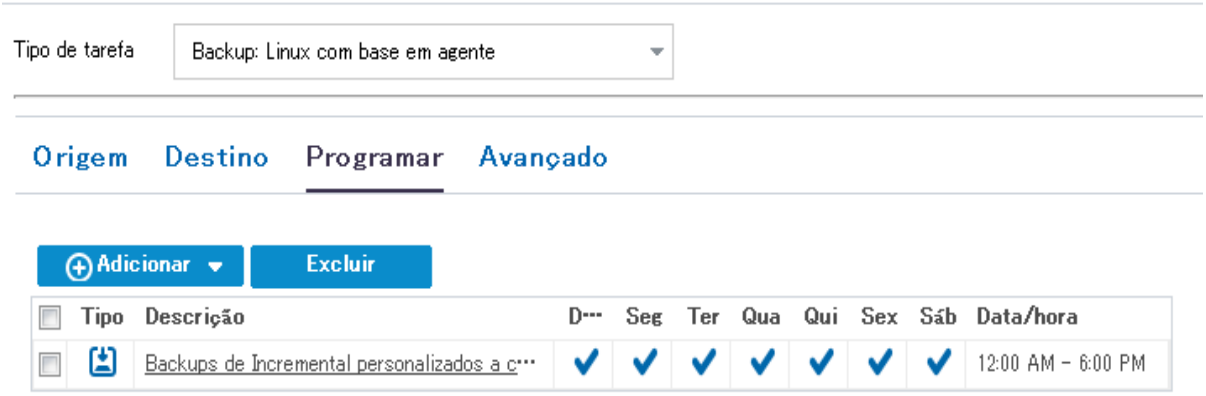
  Quando o destino do backup for um repositório de dados com redução de redundância, o tráfego ocorrerá diretamente entre a origem do Linux e o RPS, embora a opção Especificar a rede esteja configurada entre a origem do Linux e o LBS. No entanto, quando o destino do backup for um repositório de dados sem redução de redundância, o tráfego passará pelo LBS.

O destino é especificado.

Especificar a programação

A página Programação permite definir uma programação de backup para se repetir em intervalos específicos. Após definir uma programação, as tarefas são executadas automaticamente de acordo com a programação. É possível adicionar várias programações e fornecer configurações de retenção. Se o disco Local ou uma pasta compartilhada for o destino de backup, o valor padrão é um backup incremental personalizado a cada 22h00. Se o servidor RPS for o destino de backup, o valor padrão é um backup incremental diário a cada 22h00.

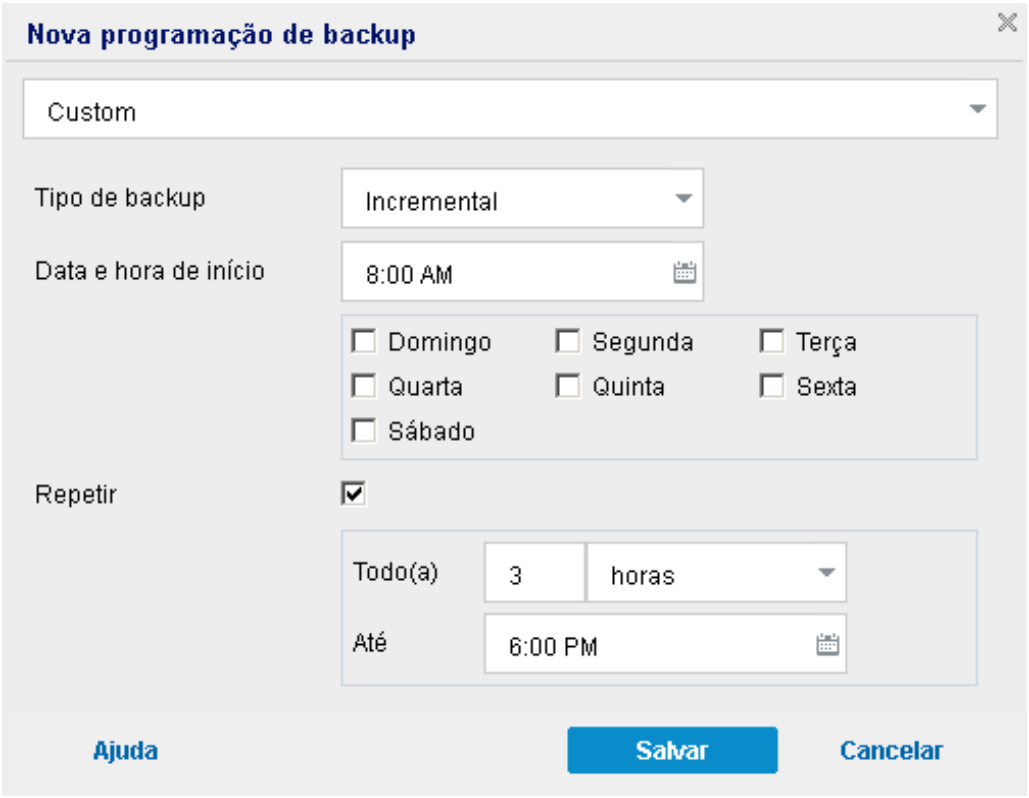
É possível editar ou excluir uma programação de tarefas de backup.



Siga estas etapas:

1. Clique na guia **Programar**.
2. Clique em **Adicionar** e selecione **Adicionar programação de backups**.

   A caixa de diálogo **Nova programação de backup** é aberta.



a. Selecione uma das seguintes opções:

Personalizado

Especifica a programação de backup que se repete várias vezes por dia.

Diário

Especifica a programação de backup que ocorre uma vez por dia. Por padrão, todos os dias da semana estão selecionados para o backup diário. Se não desejar executar a tarefa de backup em um dia específico, desmarque a caixa de seleção correspondente àquele dia da semana.

Semanal

Especifica a programação de backup que ocorre uma vez por semana.

Mensal

Especifica a programação de backup que ocorre uma vez por mês.

b. Selecione o tipo de backup.

Completo

Especifica a programação de backups para backups completos. Conforme programado, o Arcserve UDP executa um backup completo de todos os blocos usados do computador de origem. Um backup completo em geral, consome tempo, dependendo do tamanho do backup.

Verificar

Especifica a programação de backups para backups de verificação.

A Arcserve UDP verifica se os dados protegidos são válidos e concluídos, executando uma verificação de confiabilidade da imagem de backup armazenada na origem do backup. Se necessário, a imagem será sincronizada novamente. Um backup de verificação examinará o backup mais recente de cada bloco e irá comparar o conteúdo e as informações com a origem. Esta comparação verifica se o backup mais recente dos blocos representa as informações correspondentes na origem. Se a imagem de backup de qualquer bloco não corresponder à origem (possivelmente devido a alterações no sistema desde o último backup), o Arcserve UDP atualizará (fará nova sincronização) o backup do bloco que não corresponder. Também é possível usar um backup de verificação (muito raramente) para obter a garantia de backup completo sem usar o espaço necessário para um backup completo.

Vantagens: produz uma pequena imagem de backup quando comparado ao backup completo, pois somente os blocos alterados (blocos que não coincidem com o último backup) são armazenados em backup.

Desvantagens: o tempo de backup é longo, pois todos os blocos de origem são comparados aos blocos do último backup.

Incremental

Especifica a programação de backups para backups incrementais.

Conforme programado, o Arcserve UDP faz backup incremental apenas dos blocos que foram alterados desde o último backup realizado com êxito. As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a executar um backup.

c. Especifique a hora de início do backup.

d. (Opcional) Marque a caixa de seleção de **Repetição** e especifique a programação a ser repetida.

e. Clique em **Salvar**.

A programação de backup é especificada e é exibida na página de **Programação**.

3. Especifique as configurações de retenção se o destino for uma pasta compartilhada, ou de rede.

Observação: para obter mais informações sobre os conjuntos de recuperação, consulte Noções básicas sobre os conjuntos de recuperação.

Especifique o número de conjuntos de recuperação a ser retido

Especifica o número de conjuntos de recuperação retidos.

Iniciar um novo conjunto de recuperação a cada:

Dia da semana selecionado

Especifica o dia da semana selecionado para iniciar um novo conjunto de recuperação.

Dia do mês selecionado

Especifica o dia do mês selecionado para iniciar um novo conjunto de recuperação. Especifique de 1 a 31 ou o último dia do mês.

Observação: o servidor de backup Linux verifica o número de conjuntos de recuperação no armazenamento de backup configurado a cada 15 minutos e exclui qualquer conjunto de recuperação extra do local de armazenamento de backup.

4. Se você tiver selecionado o servidor de ponto de recuperação da Arcserve como o destino, siga estas etapas adicionais.

Adicionar Programação de mesclagem

a. Clique em **Adicionar** e selecione **Adicionar programação de mesclagem**.

A caixa de diálogo **Adicionar nova programação de mesclagem** é aberta.

b. Especifique a hora de início para iniciar a tarefa de mesclagem.

c. Especificar **Até** para especificar uma hora de término para a tarefa de mesclagem.

d. Clique em **Salvar**.

A programação de mesclagem é especificada e exibida na página de **Programação**.

Adicionar programação de acelerador

a. Clique em **Adicionar** e selecione **Adicionar programação de acelerador.**

A caixa de diálogo Adicionar nova programação do acelerador é aberta.

b. Especifique o limite de taxa de transferência em MB por minuto.

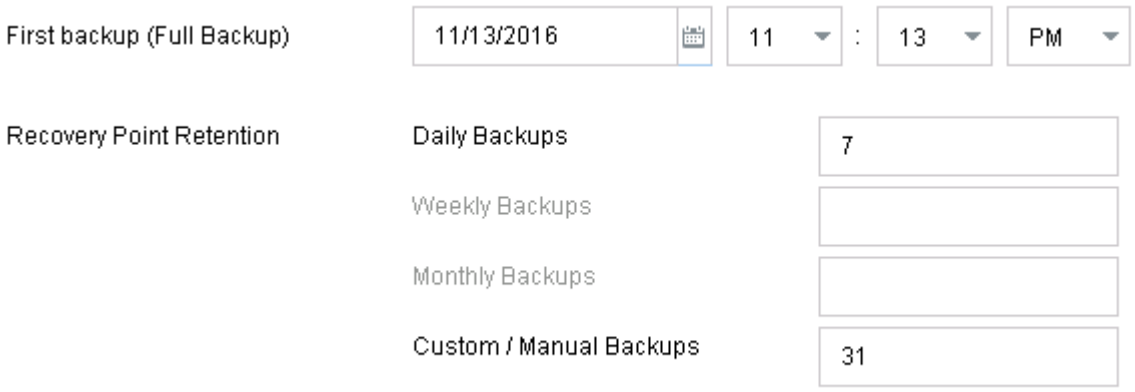
c. Especifique a hora de início para iniciar a tarefa de taxa de transferência de backup.

d. Especifique **Até** para especificar um horário de término para a tarefa de taxa de transferência.

e. Clique em **Salvar**.

A Programação de acelerador é especificada e exibida na página **Programar**.

5. Especifique a hora de início do backup programado.



6. Especifique as configurações de retenção de pontos de recuperação para programação diária, semanal e mensal.

   Essas opções serão ativadas se tiver adicionado a programação de backup correspondente. Se você modificar as configurações de retenção desta página, as alterações serão refletidas na caixa de diálogo Programação de backup.

   A programação de backup está especificada.

Noções básicas sobre os conjuntos de recuperação

Um conjunto de recuperação é uma configuração de armazenamento em que um grupo de pontos de recuperação obtidos em backup por período determinado é armazenado como um único conjunto. Um conjunto de recuperação é uma série de backups, iniciando com um backup completo e seguido de alguns backups incrementais, de verificação ou completos. É possível especificar o número de conjuntos de recuperação a reter.

As **Definições do conjunto de recuperação** garantem a manutenção periódica dos conjuntos de recuperação. Quando o limite especificado é excedido, o conjunto de recuperação mais antigo é excluído. Os valores a seguir definem os conjuntos de recuperação padrão, mínimo e máximo no Agente do Arcserve Unified Data Protection para Linux:

Padrão: 2

Mínimo: 1

Número máximo de conjuntos de recuperação: 100

Observação: se desejar excluir um conjunto de recuperação para economizar espaço de armazenamento de backup, reduza o número de conjuntos retidos e o servidor de backup excluirá automaticamente o conjunto de recuperação mais antigo. Não tente excluir o conjunto de recuperação manualmente.

Conjunto de exemplo 1:

- Completo
- Incremental
- Incremental
- Verificar
- Incremental

Conjunto de exemplo 2:

- Completo
- Incremental
- Completo
- Incremental

Um backup completo é necessário para iniciar um novo conjunto de recuperação. O backup que inicia o conjunto será convertido automaticamente em um backup completo, mesmo que não haja nenhum backup completo configurado ou programado para ser executado nesse momento. Depois que a configuração do

conjunto de recuperação for alterada (por exemplo, alterando o ponto de partida do conjunto de recuperação, do primeiro backup de segunda-feira para o primeiro backup de quinta-feira), o ponto de partida dos conjuntos de recuperação existentes não será alterado.

Observação: um conjunto de recuperação incompleto não é contado ao calcular um conjunto de recuperação existente. Um conjunto de recuperação é considerado concluído somente quando o backup inicial do próximo conjunto de recuperação é criado.

Exemplo 1 - Reter 1 conjunto de recuperação:

- Especifique o número de conjuntos de recuperação a serem retidos como 1.

  O servidor de backup sempre mantém dois conjuntos para manter um conjunto completo antes de iniciar o próximo conjunto de recuperação.

Exemplo 2 - Reter 2 conjuntos de recuperação:

- Especifique o número de conjuntos de recuperação a serem retidos como 2.

  O servidor de backup excluirá o primeiro conjunto de recuperação quando o quarto estiver pronto para iniciar a recuperação. Isso garante que, quando o primeiro backup for excluído e o quarto estiver sendo iniciado, você ainda tenha dois conjuntos de recuperação (conjunto de recuperação 2 e conjunto de recuperação 3) disponíveis no disco.

  Observação: mesmo que você opte por reter apenas um conjunto de recuperação, precisará de espaço para, pelo menos, dois backups completos.

Exemplo 3 - Reter 3 conjuntos de recuperação:

- A hora de início do backup é às 6h00 de 20 de agosto de 2012.
- Um backup incremental é executado a cada 12 horas.
- Um novo conjunto de recuperação começa na sexta-feira. Por padrão, a primeira tarefa de backup na sexta-feira será o início do novo conjunto de recuperação.
- Você deseja reter 3 conjuntos de recuperação.

  Com a configuração acima, um backup incremental será executado às 6h00 e outro às 18h00, diariamente. O primeiro conjunto de recuperação é criado quando o primeiro backup (deve ser um backup completo) é realizado. Em seguida, o primeiro backup completo é marcado como o backup inicial do conjunto de recuperação. Quando o backup programado para as 6:00 de sexta-feira for executado, ele será convertido em um backup completo e será marcado como o backup inicial do conjunto de recuperação.

Observação: Se você deseja executar a tarefa de backup várias vezes até o fim do dia, defina a programação para até 0h00. Por exemplo, para executar a tarefa de backup a cada 15 minutos o dia inteiro, defina a programação como das 0h00 às 00h00, a cada 15 minutos.

Especificar as configurações avançadas

Usando a guia Avançado, especifique algumas configurações adicionais para a tarefa de backup, incluindo a taxa de transferência de backup e as configurações de script anterior e posterior.

Siga estas etapas:

1. Clique na guia **Avançado**.
2. Especifique o valor Acelerar backup.

   Aplicável apenas quando o destino do backup for uma pasta local ou compartilhada.

   Você pode especificar a velocidade máxima (MB/min) em que os backups são gravados. É possível restringir a velocidade de backup para reduzir a utilização da CPU ou da rede. No entanto, ao limitar a velocidade de backup, isso terá um efeito negativo na janela de backup. À medida que se reduz a velocidade máxima do backup, aumenta-se seu tempo de execução.

   Observação: por padrão, a opção Acelerar backup não está ativada e a velocidade de backup não é controlada.
3. Especifique as suas configurações pré-backup e pós-backup nas **Configurações de script anterior e posterior**.

   Esses scripts executam os comandos de script para as ações a serem realizadas antes do início da tarefa e/ou após a conclusão da tarefa.

   Observação: os campos Configurações de script anterior e posterior serão preenchidos apenas se já tiver criado um arquivo de script e o tiver colocado no seguinte local do servidor de backup Linux:

   /opt/Arcserve/d2dserver/usr/prepost

   Observação: para obter mais informações sobre como criar scripts anteriores e posteriores, consulte o tópico *Gerenciar scripts anteriores e posteriores para automação*.
4. Clique em Ativar alertas por email para especificar as configurações de email e selecionar os alertas de tarefa.

   Aplicável apenas quando o destino de backup for o servidor de ponto de recuperação do Arcserve.
5. Clique em **Salvar**.

   As alterações são salvas.

O plano de backup é criado e implantado automaticamente para o nó de origem. O backup é executado de acordo com a programação que você configurou na guia **Programar.** Também é possível fazer backup manual quando desejado.

Agora, é possível adicionar as seguintes tarefas ao plano:

- Replicar
- Replicar para um RPS gerenciado remotamente
- Copiar em fita

(Opcional) Gerenciar scripts anteriores e posteriores para automação

Os scripts anteriores e posteriores permitem executar sua própria lógica de negócios em estágios específicos de uma tarefa em execução. É possível especificar quando executar seus scripts em **Configurações de scripts anteriores/posteriores** do **Assistente de backup** e do **Assistente de restauração** no console. Dependendo da sua programação, é possível executar os scripts no servidor de backup.

O gerenciamento dos scripts anteriores e posteriores é um processo em duas etapas, que consiste em criar os scripts anteriores e posteriores e em colocar o script na pasta prepost.

Criar scripts anteriores e posteriores

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Crie um arquivo de script usando as variáveis de ambiente em sua linguagem de scripts de preferência.

   Variáveis de ambiente de script anterior e posterior

   Para criar seu script, use as seguintes variáveis de ambiente:

   D2D_JOBNAME

   Identifica o nome da tarefa.

   D2D_JOBID

   Identifica a ID da tarefa. A ID da tarefa é um número fornecido para a tarefa durante a execução da tarefa. Se você executar novamente a mesma tarefa, receberá um novo número de tarefa.

   D2D_TARGETNODE

   Identifica o nó cujo backup está sendo feito ou restaurado.

   D2D_JOBTYPE

   Identifica o tipo da tarefa em execução. Os valores a seguir identificam a variável D2D_JOBTYPE:

   backup.full

   Identifica a tarefa como um backup completo.

   backup.incremental

   Identifica a tarefa como um backup incremental.

backup.verify

Identifica a tarefa como um backup de verificação.

restore.bmr

Identifica a tarefa como uma BMR (Bare-Metal Recovery – Recuperação Bare Metal). Esta é uma tarefa de restauração.

restore.file

Identifica a tarefa como uma restauração em nível de arquivo. Esta é uma tarefa de restauração.

D2D_SESSIONLOCATION

Identifica o local onde os pontos de recuperação estão armazenados.

D2D_PREPOST_OUTPUT

Identifica um arquivo temporário. O conteúdo da primeira linha do arquivo temporário é exibido no log de atividades.

D2D_JOBSTAGE

Identifica o estágio da tarefa. Os valores a seguir identificam a variável D2D_JOBSTAGE:

pre-job-server

Identifica o script que é executado no servidor de backup antes do início da tarefa.

post-job-server

Identifica o script que é executado no servidor de backup após a conclusão da tarefa.

pre-job-target

Identifica o script que é executado no computador de destino antes do início da tarefa.

post-job-target

Identifica o script que é executado no computador de destino após a conclusão da tarefa.

pre-snapshot

Identifica o script que é executado no computador de destino antes de capturar o instantâneo.

post-snapshot

Identifica o script que é executado no computador de destino depois de capturar o instantâneo.

D2D_TARGETVOLUME

Identifica o volume cujo backup foi feito durante uma tarefa de backup. Essa variável é aplicável a scripts de instantâneo anteriores e posteriores para uma tarefa de backup.

D2D_JOBRESULT

Identifica o resultado de um script de tarefa posterior. Os valores a seguir identificam a variável D2D_JOBRESULT:

success

Identifica o resultado realizado com êxito.

fail

Identifica o resultado realizado sem êxito.

D2DSVR_HOME

Identifica a pasta onde o servidor de backup está instalado. Essa variável é aplicável a scripts que são executados no servidor de backup.

O script é criado.

Observação: para todos os scripts, um valor de retorno zero indica êxito e um valor de retorno diferente de zero indica falha.

Colocar o script na pasta Prepost e verificar

Todos os scripts anteriores e posteriores de um servidor de backup são gerenciados na pasta prepost no seguinte local:

/opt/Arcserve/d2dserver/usr/prepost

Siga estas etapas:

1. Coloque o arquivo no seguinte local do servidor de backup:

   /opt/Arcserve/d2dserver/usr/prepost
2. Forneça a permissão de execução para o arquivo de script.
3. Efetue logon na interface da web do Agente do Arcserve Unified Data Protection para Linux.
4. Abra o **Assistente de backup** ou o **Assistente de restauração** e navegue até à guia **Avançado**.
5. Selecione o arquivo de script na lista suspensa **Configurações de scripts anteriores/posteriores** e, em seguida, envie a tarefa.

6. Clique em **Log de atividades** e verifique se o script é executado para a tarefa de backup especificada.

   O script é executado.

   Os scripts anteriores e posteriores são criados com êxito e colocados na pasta pre-post.

(Opcional) Executar um backup manual

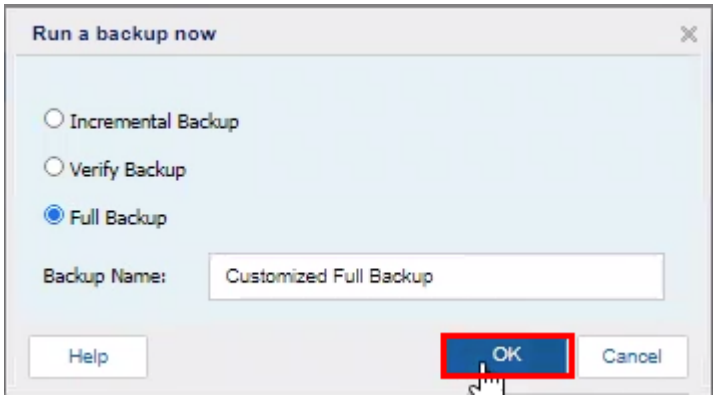
Em geral, os backups são executados automaticamente e controlados pelas configurações da programação. Além do backup programado, um backup manual fornece a opção de fazer backup dos nós de acordo com a necessidade. Por exemplo, se você repetir a programação para backups completos, incrementais e de verificação e desejar fazer grandes alterações em seu computador, deverá executar um backup manual imediato sem esperar até que ocorra o próximo backup programado.

Siga estas etapas:

1. Efetue logon no Console do Arcserve UDP.
2. Navegue até **recursos** > **Plano** > **Todos os planos**.

   A lista de todos os planos é exibida no painel central.
3. Clique com o botão direito do mouse no plano e selecione **Fazer backup agora**.

   A caixa de diálogo Fazer backup agora é exibida.
4. Na caixa de diálogo Executar um backup agora, selecione o tipo de backup que deseja executar e, em seguida, especifique o nome do backup, se necessário.



As opções disponíveis são:

Backup incremental

Inicia um backup incremental do computador inteiro. Um backup incremental realiza backup somente dos blocos que foram alterados desde o backup anterior.

Observação: se estiver executando um backup pela primeira vez, o backup completo será iniciado automaticamente, mesmo que você tenha selecionado a opção Backup incremental.

As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a execução de backups.

Verificar backup

Inicia um backup de verificação do computador, examinando o backup mais recente de cada bloco e comparando o conteúdo e as informações com a origem. Esta comparação verifica se o backup mais recente dos blocos representa as informações correspondentes na origem. Se a imagem de backup de algum bloco não corresponder à origem, o agente do Arcserve UDP (Windows) atualizará (ressincronizará) o backup do bloco divergente.

Vantagem: uma imagem de backup muito pequena é gerada quando comparada ao backup completo porque somente os blocos alterados (blocos que não correspondam ao último backup) são armazenados em backup.

Desvantagem: o tempo do backup fica lento porque todos os blocos do disco de origem são comparados aos blocos do último backup.

Backup completo

Inicia um backup completo do computador inteiro ou dos volumes selecionados.

Observações:

- se você adicionar um novo volume à origem do backup, será feito um backup completo do volume recém-adicionado, independentemente do método de backup geral selecionado.
- Se nenhum nome de backup for especificado, por padrão, ele será automaticamente nomeado como Backup completo/incremental/de verificação personalizado.

5. Clique em **OK**.

   A caixa de diálogo Informações do andamento é exibida.

6. Aguarde até que a tarefa de backup seja concluída e clique em **OK**.

7. Para monitorar as tarefas de backup, navegue até **tarefas** > **Tarefas em andamento**.

   Aguarde até a conclusão da tarefa de backup.

   Observação: apenas uma tarefa pode ser executada em uma hora. Se você tentar iniciar manualmente uma tarefa de backup quando outra tarefa estiver em execução no mesmo momento, uma mensagem de alerta será exibida informando

sobre a existência de outra tarefa em execução e solicitando uma nova tentativa mais tarde.

O backup manual é realizado com êxito.

Verificar o backup

Para verificar o backup, confirme se você criou com êxito o plano de backup. Depois de verificar se o plano está criado com êxito, confirme se a tarefa de backup é executada conforme o programado. É possível verificar o status das tarefas de backup na guia Tarefas.

Siga estas etapas: para verificar os planos

1. Clique na guia **Recursos**.
2. No painel esquerdo, navegue para **Nós** e clique em **Todos os nós**.

   Uma lista de todos os nós é exibida no painel central.
3. Verifique se os planos são mapeados com nós.

Siga um desses métodos para verificar as tarefas de backup

Método 1

1. Clique na guia **Tarefas**.
2. No painel à esquerda, clique em **Todas as tarefas**.

   O status de cada tarefa é incluído no painel central.
3. Verifique se a tarefa de backup é concluída com êxito.

   A tarefa de backup é verificada.

Método 2

1. No console do Arcserve UDP, navegue até a guia **tarefas** > **Tarefas concluídas com êxito**.

   A lista de tarefas de backup concluídas é exibida no painel central.
2. Clique na tarefa de replicação inversa concluída. O painel direito é atualizado.
3. Em Detalhes da tarefa, clique no hiperlink **Exibir logs**.
4. Verifique se a tarefa de backup é concluída com êxito.

   A tarefa de backup é verificada.

A tarefa de backup é verificada.

Solução de problemas

O status de tarefas, histórico de tarefas e o log de atividades não são visíveis

O status de tarefas, histórico de tarefas e o log de atividades não são visíveis

Sintoma

Eu não consigo ver o status de tarefas, o histórico da tarefa e o log de atividades no Console do Arcserve UDP.

Solução

O servidor de backup Linux não pode estabelecer conexão com Arcserve UDP usando o nome do host.

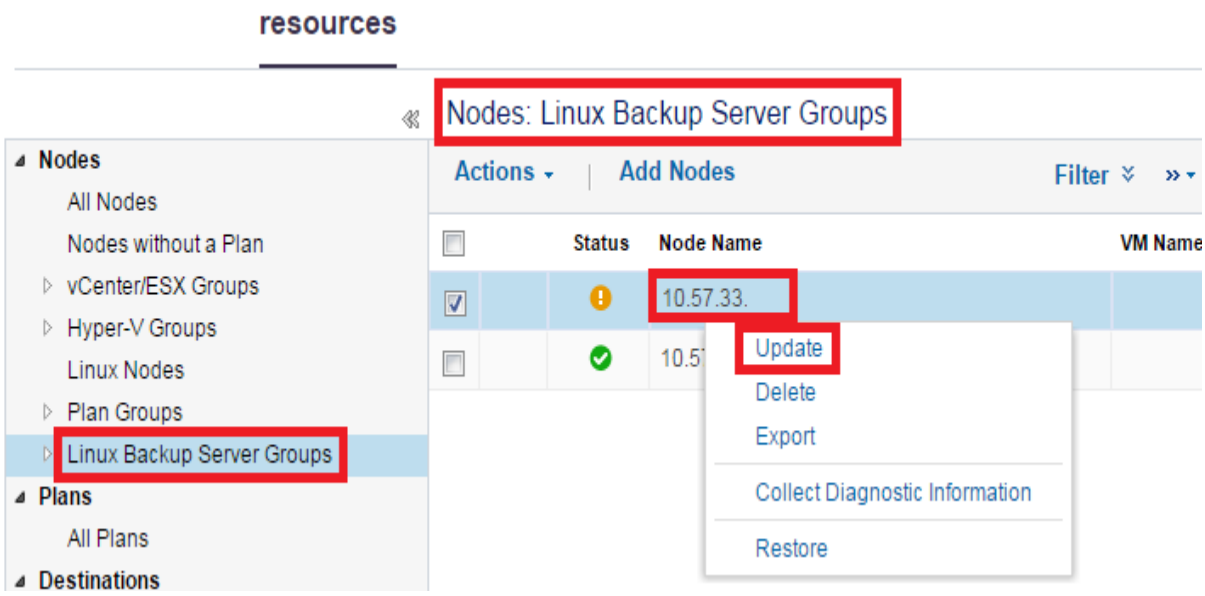
Siga estas etapas:

1. Crie o arquivo server_ip.ini no seguinte local do Arcserve UDP:

   "UDP installation path"\Management\Configuration\server_ip.ini

2. Digite o endereço IP o Arcserve UDP nesse arquivo.
3. Efetue logon no console do Arcserve UDP e atualize o servidor de backup Linux, bem como os nós Linux.

   Observação: o servidor de backup Linux pode ser atualizado apenas nos Grupos de servidores de backup Linux, onde todos os servidores de backup Linux estão listados.



O status de tarefas, o histórico de tarefas e o log de atividades são visíveis.

Como criar um plano de backup de máquina virtual com base em host

Para proteger os nós da máquina virtual com base em host, é necessário criar um plano de backup com base em host. Um plano de backup para os nós da máquina virtual com base em host consiste em uma tarefa de backup. Esta tarefa de backup permite especificar os nós que deseja proteger, o destino do backup e a programação do backup. O destino do backup pode ser um local de destino ou uma pasta compartilhada remota, ou o servidor de ponto de recuperação onde você deseja armazenar os dados de backup.

Você também pode fazer backup de bancos de dados Oracle, SQL e Exchange Servers. Para fazer backup dos bancos de dados Oracle, certifique-se dos pré-requisitos específicos. Para fazer backup do SQL Server e do Exchange Server não existem pré-requisitos. Verifique os pré-requisitos a seguir para executar um backup consistente do aplicativo de um banco de dados Oracle:

- Pré-requisito para criar um backup consistente do aplicativo de um banco de dados Oracle

O diagrama a seguir ilustra o processo para proteger os nós da máquina virtual com base em host.

O que fazer a seguir?

1. Verificar os pré-requisitos e as considerações
2. Criar um plano de backup com base em host
3. (Opcional) Executar um backup manual
4. Verificar o plano
5. Solução de problemas

Verificar os pré-requisitos e as considerações

Os seguintes pré-requisitos devem ser concluídos:

- Efetue logon no Console.
- Prepare um servidor proxy de backup com base em host no qual o Agente do Arcserve Unified Data Protection para Windows esteja instalado.
- Para executar as funções, como verificação prévia, comandos de execução anterior/posterior ou limpeza do log do aplicativo, atualize a máquina virtual na exibição de lista de nós do console do Arcserve UDP com uma das seguintes credenciais para a máquina virtual convidada:
  - Credenciais de usuário administrador integradas.
  - Credenciais de usuário administrador de domínio integradas.
  - Para obter outras credenciais de administrador, desative o UAC (User Account Control – Controle de Conta de Usuário) na máquina virtual convidada.
- Para que seja possível executar uma restauração em nível de banco de dados (para Exchange e SQL Server) ou a restauração em nível granular (Exchange) após um backup, é preciso atender aos seguintes pré-requisitos:
  - A VM deve suportar o backup consistente do aplicativo. Para obter mais informações sobre backup consistente com o aplicativo, consulte Como criar instantâneos consistentes com o aplicativo para VMware ou Como criar instantâneos consistentes com o aplicativo para Hyper-V.
  - Para VM da VMware, o método de encerramento de instantâneo do **VMware Tools** deve ser usado no plano de backup.
  - Para a VM do Hyper-V, o Arcserve UDP precisa implantar automaticamente um utilitário no sistema operacional convidado da VM para reunir os metadados do aplicativo durante um backup. O sistema operacional convidado da VM deve ser acessado a partir do servidor proxy de backup ou do host do Hyper-V usando uma rede. Ao mesmo tempo, o nó da VM deve ser atualizado com as devidas credenciais administrativas na exibição de lista de nó do console do Arcserve UDP. Por algum motivo, se o sistema operacional convidado da VM não puder ser acessado tanto a partir do servidor proxy de backup e quanto do host do Hyper-V, siga estas etapas para instalar manualmente o utilitário no sistema operacional convidado da VM:

a. Efetue logon no servidor proxy de backup e vá até seguinte pasta:

   <Arcserve UDP installation path>\Engine\BIN (Example, C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN)

b. Localize o arquivo executável **VMICService_32.exe** ou **VMICService_64.exe**.

c. Copie o arquivo executável em qualquer pasta dentro do sistema operacional convidado da VM. (Para um sistema operacional de 32 bits, copie **VMICService_32.exe**, caso contrário, copie **VMICService_64.exe**).

   Por exemplo, você pode criar uma imagem ISO, incluindo esse arquivo executável e montá-lo no dispositivo DVD da VM.

d. Efetue logon no sistema operacional convidado da VM e execute **VMICService_32.exe -install** ou **VMICService_64.exe -install**.

- Instale o componente do servidor e crie repositórios de dados se deseja armazenar os dados de backup no servidor de ponto de recuperação.
- Verifique os pré-requisitos para fazer backup de um banco de dados Oracle.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Os pré-requisitos a seguir são para instantâneos de hardware:

Para o Hyper-V

- Instale um provedor de hardware VSS nos servidores do Hyper-V e para oferecer suporte ao instantâneo transportável, instale o provedor de hardware VSS no servidor proxy de backup. A configuração típica de um provedor de hardware VSS inclui:
  - Especificação de um servidor que controla o LUN.
  - Especificar as credenciais da matriz de disco para acessar a matriz de disco.

  Para obter mais informações sobre como configurar o provedor de hardware VSS, entre em contato com o fornecedor do provedor de hardware.
- O servidor Hyper-V e o servidor proxy devem ter uma versão de sistema operacional semelhante.
- Se o servidor Hyper-V pertencer a um agrupamento, o servidor proxy não deverá fazer parte do cluster do Hyper-V.
- Desinstale o CBT do UDP de "Programas e recursos" no painel de controle do host do Hyper-V.

Para o VMware

- O Arcserve UDP oferece suporte a LUNs NetApp iSCSI e NetApp NFS.
- Para criar um instantâneo de hardware para a VMware, adicione a matriz de armazenamento ao console. Para obter mais informações sobre a adição de uma matriz de armazenamento, consulte o tópico Adicionar uma matriz de armazenamento.
- Para usar o instantâneo de hardware, a licença Flexclone é obrigatória para as matrizes de armazenamento do NetApp com dados ONTAP operando no modo de 7 e no modo de agrupamento.

Considerações ao fazer backup da VM:

- **Como a desfragmentação do volume pode afetar a continuação dos backups**

  A desfragmentação do volume com a ferramenta nativa do Windows afeta o tamanho dos backups em nível de bloco, pois o Arcserve UDP continuará a fazer backup de todos os blocos alterados de forma incremental. Isso significa que os blocos alternados durante a desfragmentação serão incluídos no backup, mesmo se nenhum dado foi alterado nos arquivos. Como resultado, o tamanho do backup aumenta. Esse comportamento é esperado.

- **Como proteger máquinas virtuais no Hyper-V 2016 usando o Windows Resilient Change Tracking**

  Para proteger VMs no Hyper-V 2016, é recomendável utilizar o Windows RCT (Resilient Change Tracking) para backups incrementais. O Arcserve UDP usará automaticamente o Windows RCT (Resilient Change Tracking) ao fazer backup de máquinas virtuais com configuração na versão 8.0 ou superior que são executadas no host/agrupamento do Hyper-V 2016. Se o Hyper-V for atualizado de uma versão anterior, atualize a configuração da máquina virtual usando também a documentação da Microsoft. Ao concluir a atualização de todas as máquinas virtuais protegidas pelo Arcserve UDP, é recomendável desinstalar o serviço CBT do Arcserve UDP do host do Hyper-V.

Considerações para o backup de rede específico:

- O hipervisor, o agente do Windows e o RPS devem estar na mesma rede.
- Se o ESXi for adicionado com um **nome de host** ao vCenter, a seleção da rede de backup deverá ser a rede padrão do ESXi.

  Observação: a rede padrão é a rede que é resolvida pelo DNS.
- Se o ESXi for adicionado com o IP ao vCenter, a seleção da rede de backup deverá ser a mesma rede que o ESXi usa para se conectar ao vCenter.

Cenário nº	Tem o vCenter	O que é usado para adicionar ao vCenter	Poderia usar a rede de backup?	A solução alternativa de arquivo DNS/de host funciona?
1	Não	N/D	Sim	N/D
2	Sim	O nome de host do ESXi – o IP de produção do nome de host foi resolvido	Não	Sim. Atualize o arquivo DNS ou hosts no servidor proxy.
3	Sim	Nome de host do ESXi – o IP da rede de backup do nome de host foi resolvido	Sim	N/D
4	Sim	IP de produção do ESXi	Não	Não
5	Sim	IP da rede de backup do ESXi	Sim	N/D

Verificar os pré-requisitos para executar backup consistente do aplicativo para o banco de dados Oracle

Para fazer backup de um banco de dados Oracle com informações consistentes, certifique-se de que o modo ARCHIVELOG esteja ativado para arquivar os logs de Refazer.

Observação: o volume de dados deve incluir arquivos de dados Oracle, arquivos de controle, o arquivo de parâmetros do servidor e logs de repetição online. Os logs de repetição arquivados devem estar fisicamente localizados em um volume separado.

Siga estas etapas para verificar se o modo ARCHIVELOG está ativado:

a. Efetue logon no Oracle Server como usuário Oracle com privilégios de SYSDBA.

b. Digite o seguinte comando no prompt do SQL*Plus:

   ARCHIVE LOG LIST;

   As configurações de log arquivadas para a instância atual são exibidas.

c. Defina as seguintes configurações:

   Modo de log de banco de dados: modo de arquivamento

   Arquivamento automático: ativado

d. Iniciar o modo ARCHIVELOG.

   Observação: se o modo ARCHIVELOG não estiver ativado, inicie o modo ARCHIVELOG para fazer backup do banco de dados.

Siga estas etapas para iniciar o modo ARCHIVELOG:

a. Encerre o Oracle Server.

b. Execute as seguintes instruções no Oracle:

   CONNECT SYS/SYS_PASSWORD AS SYSDBA

   STARTUP MOUNT;

   ALTER DATABASE ARCHIVELOG;

   ALTER DATABASE OPEN;

   Por padrão, os logs de arquivo morto são gravados na área de recuperação em flash. Se não desejar gravar os logs de arquivo morto para a área de recuperação em flash, defina o parâmetro LOG_ARCHIVE_DEST_n para o local onde você deverá gravar logs de arquivos.

SQL>ALTER SYSTEM SET LOG_ARCHIVE_DEST_
1='LOCATION=e:\app\administrator\oradata\<oracle_database_name>\arch'
SCOPE= BOTH;

Sistema alterado.

SQL> ARCHIVE LOG LIST;

As configurações de log arquivadas para a instância atual são exibidas.

c. Defina as seguintes configurações:

Modo de log de banco de dados: modo de arquivamento

Arquivamento automático: ativado

Destino do arquivo: E:\app\oracle\oradata\<oracle_database_name>\arch

Sequência de log online mais antiga: 21

Sequência de log atual: 23

O serviço de gravador do Oracle VSS foi iniciado e está funcionando corretamente.

Criar um plano de backup com base em host

Um plano de backup inclui uma tarefa de backup que executa um backup da máquina virtual e armazena os dados no destino especificado. Cada tarefa consiste em parâmetros que definem a origem, o destino, a programação e outros detalhes de backup.

Siga estas etapas:

1. Clique na guia **recursos** no Console.
2. No painel à esquerda, navegue para **Planos** e clique em **Todos os planos**.

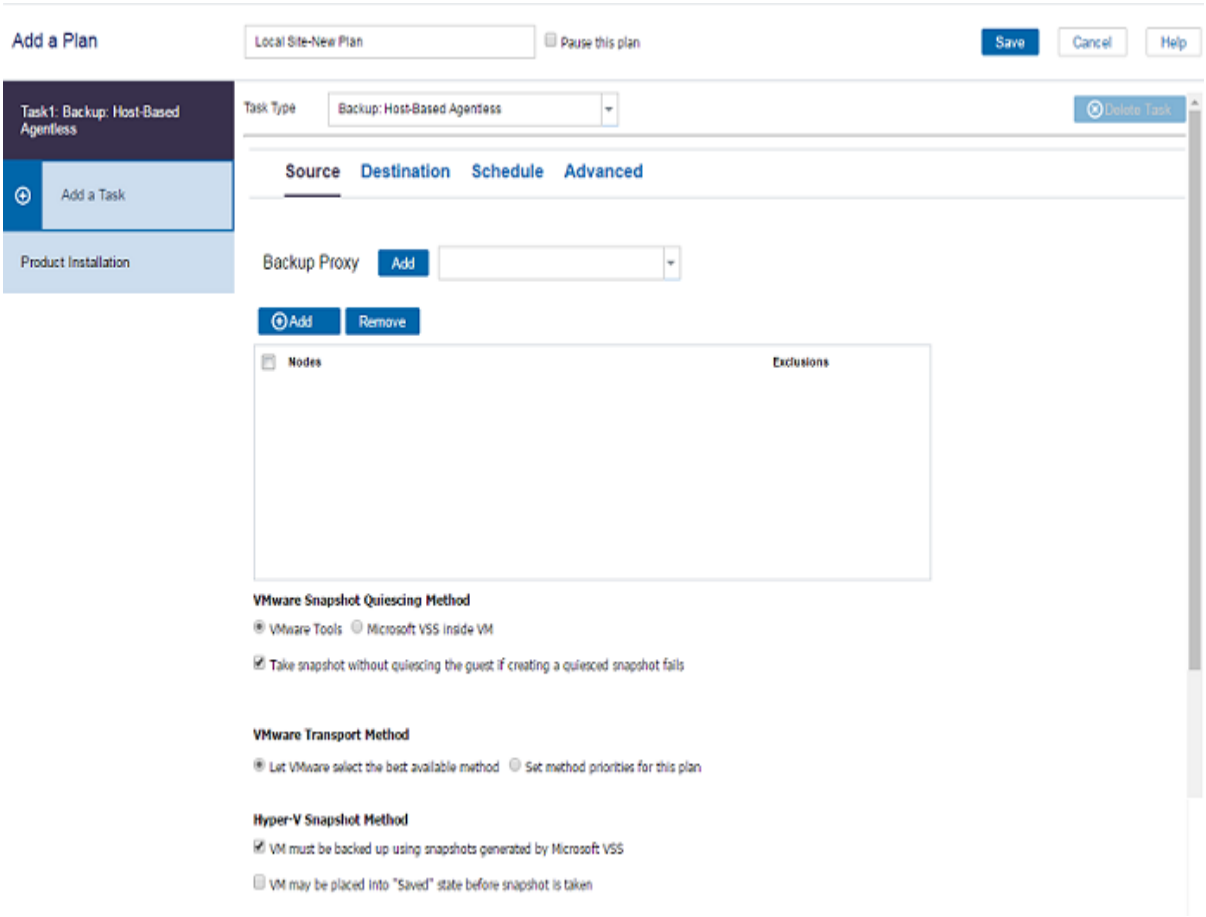
   Se tiver criado os planos anteriores, esses planos serão exibidos no painel central.
3. No painel central, clique em **Adicionar um plano**.

   Adicionar um plano é exibido.
4. Digite o nome do plano.
5. (Opcional) Marque a caixa de seleção **Pausar este plano**.

   O plano não será executado até que você desmarque a caixa de seleção para retomar o plano.

   Observação: se um plano for pausado, nenhuma tarefa em andamento será pausada, mas todas as tarefas programadas correspondentes associadas a esse plano serão pausadas. No entanto, você pode executar uma tarefa manualmente. Por exemplo, você pode executar manualmente a tarefa de backup e a tarefa de replicação para um nó mesmo que o respectivo plano esteja pausado. Nesse caso, a tarefa seguinte da tarefa sob demanda (manual) não será executada. Por exemplo, há uma tarefa de replicação após uma tarefa de backup sob demanda, a tarefa de replicação não será executada para a tarefa de backup sob demanda. É necessário executar manualmente a tarefa de replicação. Quando você retomar o plano, as tarefas pendentes não são retomadas imediatamente. Depois de retomar o plano, as tarefas pendentes serão executadas no próximo horário programado.
6. Na lista suspensa **Tipo de tarefa**, selecione **Backup, com base em host sem**

agente.



Agora especifique os detalhes de Origem, Destino, Programação e Avançado.

Especificar a origem

A página Origem permite especificar os nós de origem que deseja proteger. É possível selecionar mais de um nó em um plano. Caso não tenha adicionado nós para o console, você pode adicionar nós ao criar ou modificar um plano da página de origem. É possível salvar um plano sem adicionar nenhum nó de origem. O plano é implantado somente após você adicionar nós de origem.

Siga estas etapas:

1. Clique na guia **Origem** e adicione um servidor proxy de backup.

   O servidor proxy é um nó no qual você instala o Agente do Arcserve Unified Data Protection para Windows. Se o agente não estiver instalado nesse servidor proxy, depois, quando você salvar o plano, o agente será implantado no servidor proxy. A configuração da implantação de agente está na tarefa de instalação do agente no plano.

   - Se o proxy de backup já foi adicionado, selecione o proxy de backup na lista suspensa.

   - Se o proxy de backup não foi adicionado, clique em **Adicionar**.

     A caixa de diálogo **Adicionando servidor proxy de backup sem agente com base em host** é aberta.

     Especifique os detalhes do servidor proxy e clique em **OK**.

   Não é necessário adicionar o número da porta e o protocolo. O número da porta e o protocolo são configurados na guia **configurações** do console.

   Observação: quando você modifica um plano alterando o proxy de backup, mas os nós incluídos no plano têm tarefas em execução, a implantação do plano falha. Siga estas etapas para alterar o proxy de um plano:

a. Pause o plano.

b. Aguarde até que todos os nós no plano concluam as tarefas de backup em execução. (Ou, é possível cancelar as tarefas em execução).

c. Altere o proxy do plano e salve-o.

d. Retome o plano.

2. Clique em **Adicionar nós** para selecionar uma das opções a seguir e adicionar os nós dos quais você deseja fazer backup:

Selecionar nós a serem protegidos

Selecione a caixa de diálogo **Selecionar nós a serem protegidos** e será possível selecionar os nós na lista exibida. Selecione esta opção se você já tiver adicionado os nós para o console.

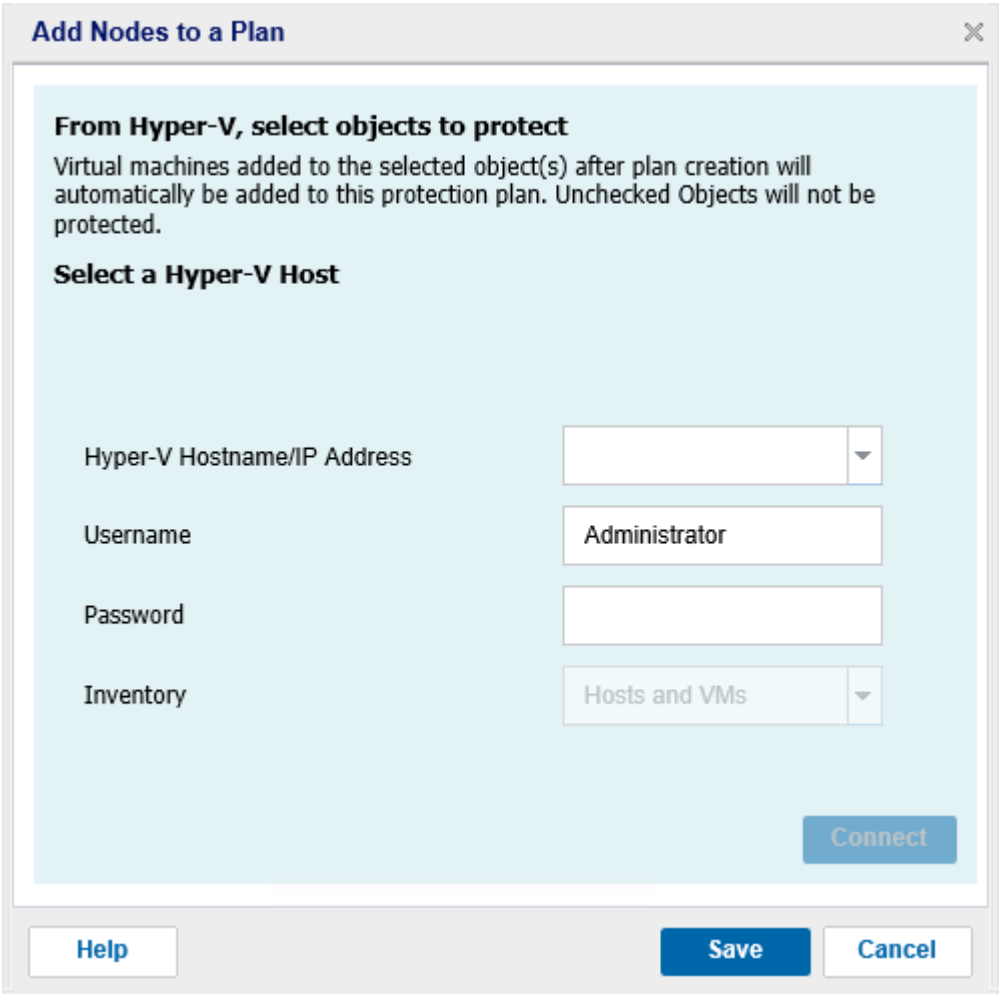
Adicionar nós a partir de um Hyper-V

Abra a caixa de diálogo **Adicionar nós ao console do Arcserve UDP**. Você pode adicionar nós individuais de VM ou objetos de recipiente VM (inclusive o agrupamento do Hyper-V, o host do Hyper-V, o local de armazenamento) em um plano. Depois de adicionar um objeto de recipiente de VM ao plano, o plano protege automaticamente todas as VMs atribuídas. Quando uma nova VM é criada sob o objeto de recipiente da VM ou movida para o objeto de recipiente da VM de outro lugar, Arcserve UDP protege a VM sem intervenção manual. Se a VM é excluída do objeto do recipiente da VM (ou movida para fora do objeto de recipiente da VM), Arcserve UDP para de proteger a VM.

Para adicionar um objeto de recipiente da VM a um plano, siga estas etapas:

a. Especifique os detalhes do servidor Hyper-V, selecione como você deseja procurar as VMs na lista suspensa Inventário (hosts e VMs, armazenamentos e VMs) e clique em Conectar.

Uma árvore de hierarquia do Hyper-V aparece.

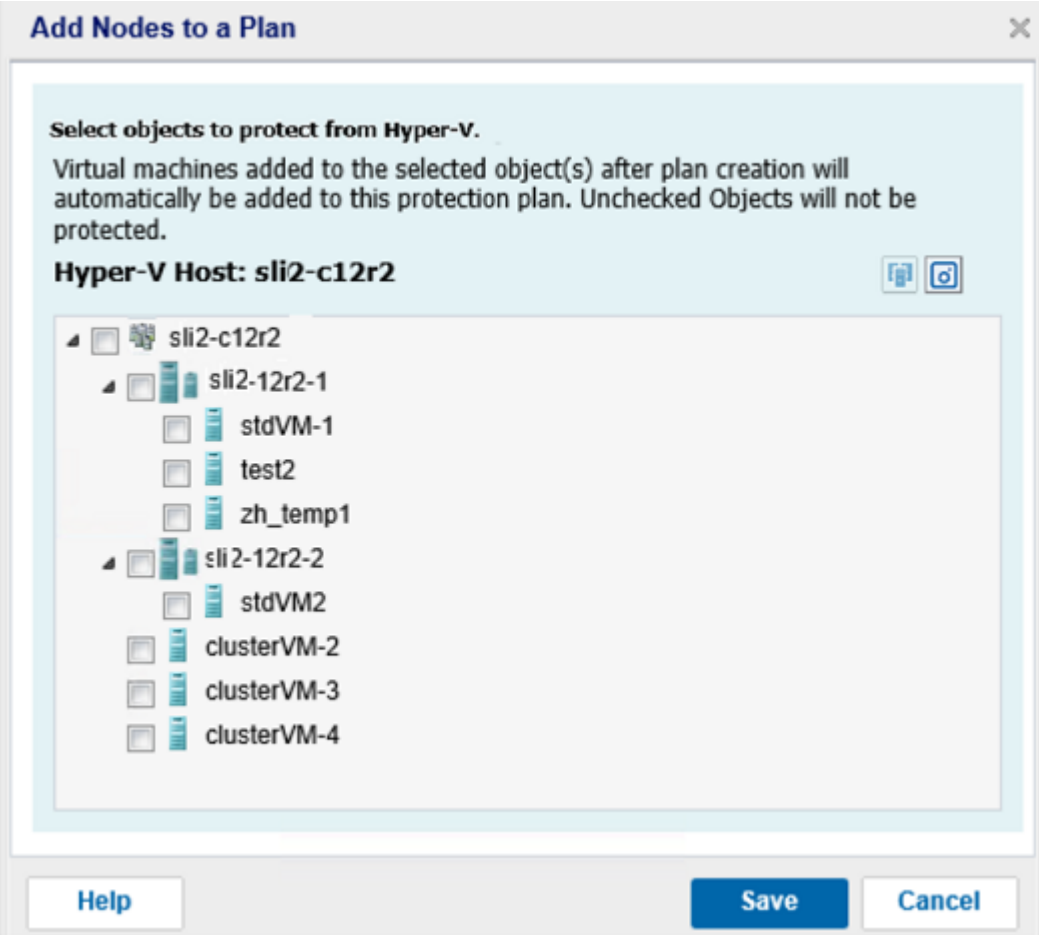


b. Expanda a árvore de hierarquia do Hyper-V para realizar as seguintes opções:

Observação: dependendo da seleção na lista suspensa Inventário, diferentes exibições das árvores de hierarquia são exibidos: hosts e VMs ou armazenamentos e VMs. Para alternar entre as diferentes exibições de árvore clique nos botões no canto superior direito da árvore.

i. **Adicionar uma VM individual**

Selecione a caixa de seleção da VM que você deseja adicionar a partir da lista e clique em **Salvar**.



ii. **Adicionar um objeto de recipiente de VM**

Selecione a caixa de seleção do objeto de recipiente da VM que você deseja adicionar a partir da lista e clique em Salvar. Ao selecionar o objeto de recipiente de VM para proteger, também é possível limpar a seleção de uma VM filha ou de um objeto de recipiente de VM filha disponível abaixo do objeto. Como resultado, a VM filha ou o objeto de recipiente da VM filha é excluído da proteção.

Observação: o Arcserve UDP usa o nome de host/agrupamento do Hyper-V, o nome do volume ou o nome do compartilhamento SMB para identificar exclusivamente o objeto do recipiente na lista do Hyper-V. Como resultado, é possível adicionar o mesmo objeto de recipiente de VM aos planos mais de uma vez.

Por exemplo, você pode adicionar um host do Hyper-V pelo nome do host e usar o endereço IP para adicionar o mesmo host do Hyper-V novamente. Outro exemplo é adicionar um compartilhamento SMB, que usa o nome do host da máquina host, ou adicionar o mesmo compartilhamento SMB, que usa o endereço IP do computador host.

Importante: Arcserve UDP não oferece suporte para adicionar o mesmo objeto de recipiente a um plano duas vezes para evitar comportamentos imprevisíveis.

Adicionar nós do vCenter/ESX

Abra a caixa de diálogo **Adicionar nós ao console do Arcserve UDP**. É possível adicionar nós de VM individuais, modelos de VM ou objetos de recipiente de VM a um plano. Depois de adicionar um objeto de recipiente de VM ao plano, o plano protege automaticamente todas as VMs atribuídas. Quando uma nova VM é criada sob o objeto de recipiente da VM ou movida para o objeto de recipiente da VM de outro lugar, o Arcserve UDP protege a VM sem intervenção manual. Se a VM é excluída do objeto do recipiente da VM ou movida para fora do objeto de recipiente da VM, o Arcserve UDP para de proteger a VM.

Observação: além dos objetos de recipiente da VM que existem no vSphere, o Arcserve UDP também considera o qualificador e a categoria de qualificador como um objeto de recipiente da VM, para que eles sejam adicionados ao plano de backup sem agente. Nesse caso, todas as VMs e os modelos atribuídos com o determinado qualificador serão automaticamente protegidos. Além disso, se um objeto de recipiente da VM de nível superior for atribuído com um qualificador, será considerado que todas as VMs desse objeto de recipiente da VM têm o mesmo qualificador na prática. Por exemplo, atribuir um qualificador a um pool de recursos automaticamente fornece o mesmo qualificador às VMs desse pool, mesmo que na verdade elas não tenham um qualificador atribuído no vCenter. Além disso, a proteção automática por qualificador tem suporte apenas para vCenter 6.0 e 6.5.

Para adicionar um objeto de recipiente da VM a um plano, siga estas etapas:

a. Especifique os detalhes do servidor vCenter/ESX, selecione como você deseja procurar as VMs na caixa de listagem suspensa Inventário (Hosts e agrupamentos, VMs e modelos, VMs e qualificadores) e clique em **Conectar**.

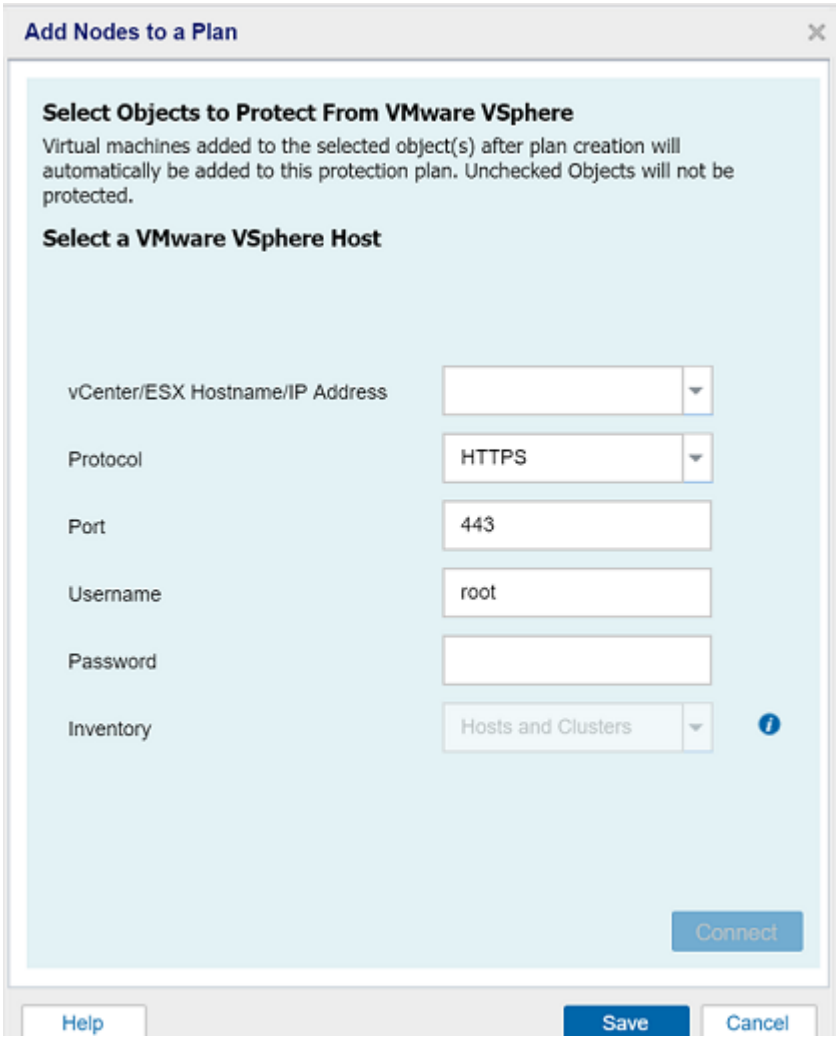
   Uma árvore de hierarquia vSphere aparece.

   Observação: considere o seguinte:

   - O VMware Virtual Disk Development Kit (VDDK) 6.x.x é fornecido com o Arcserve UDP 7.0, mas o VDDK 6.x.x não oferece suporte a HTTP. Além disso, o vCenter e o ESX oferecem suporte à

conexão HTTPS apenas por padrão.

- Selecione o **Protocolo** HTTPS se você quiser substituir manualmente o VDDK 6.x.x integrado por outra versão do VDDK e configurar manualmente o vCenter/ESX para permitir a conexão HTTP.

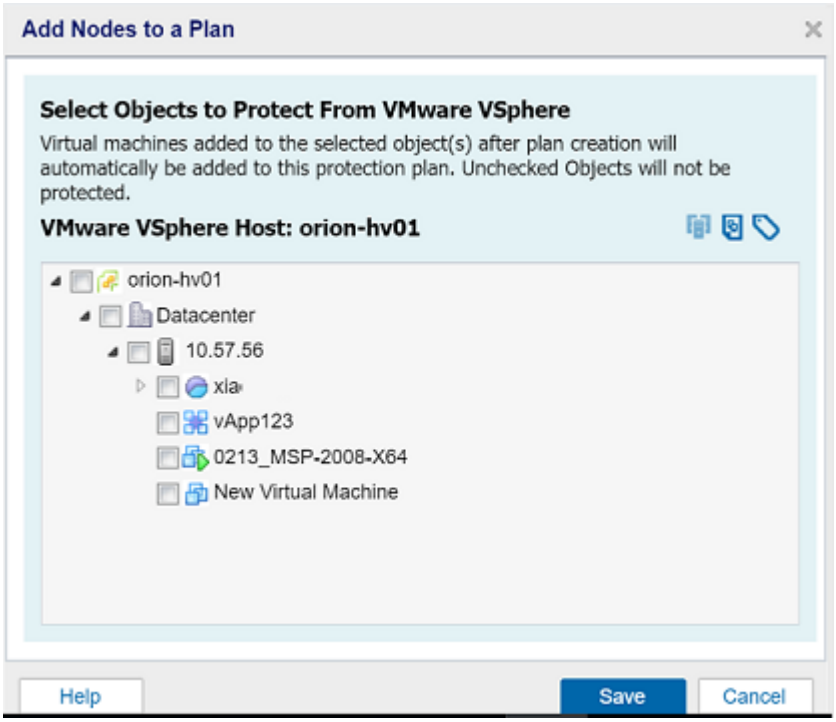


b. Expanda a lista do vSphere para adicionar o seguinte:

Observação: dependendo do que está selecionado na lista suspensa Inventário, haverá exibições diferentes da árvore de hierarquia: Hosts e agrupamentos, VMs e modelos, VMs e qualificadores. É possível alternar entre as diferentes exibições de árvore clicando nos botões no canto superior direito da árvore.

i. **Adicionar uma VM individual**

Selecione a caixa de seleção da VM que você deseja adicionar a partir da lista e clique em **Salvar**.



ii. **Adicionar um objeto de recipiente de VM**

Selecione a caixa de seleção do recipiente que você deseja adicionar a partir da lista e clique em **Salvar**. Enquanto você seleciona o recipiente a ser protegido, você também pode desmarcar a seleção de uma VM filha ou objeto de recipiente da VM filha que está sob ele. Como resultado, a VM filha ou o objeto de recipiente da VM filha é excluído da proteção.

Observação: o Arcserve UDP usa o nome do vCenter/ESX e a ID do vSphere MoRef (ID de referência de objeto gerenciado) para identificar exclusivamente o objeto de recipiente da VM na lista do **vSphere**. Isso permite que você adicione o mesmo objeto de recipiente da VM ao plano mais de uma vez.

Por exemplo:

a. adicione um objeto de recipiente da VM a um vCenter conectando-se ao vCenter usando o nome do host e, em seguida, adicione o objeto de recipiente da VM novamente conectando-se usando o endereço IP do vCenter.

b. Adicione um objeto de recipiente da VM a um vCenter e, em seguida, adicione-o novamente a partir do host ESX diretamente.

Importante: o Arcserve UDP não oferece suporte à adição do mesmo objeto de recipiente da VM a um plano duas vezes, pois isso pode causar comportamentos imprevisíveis.

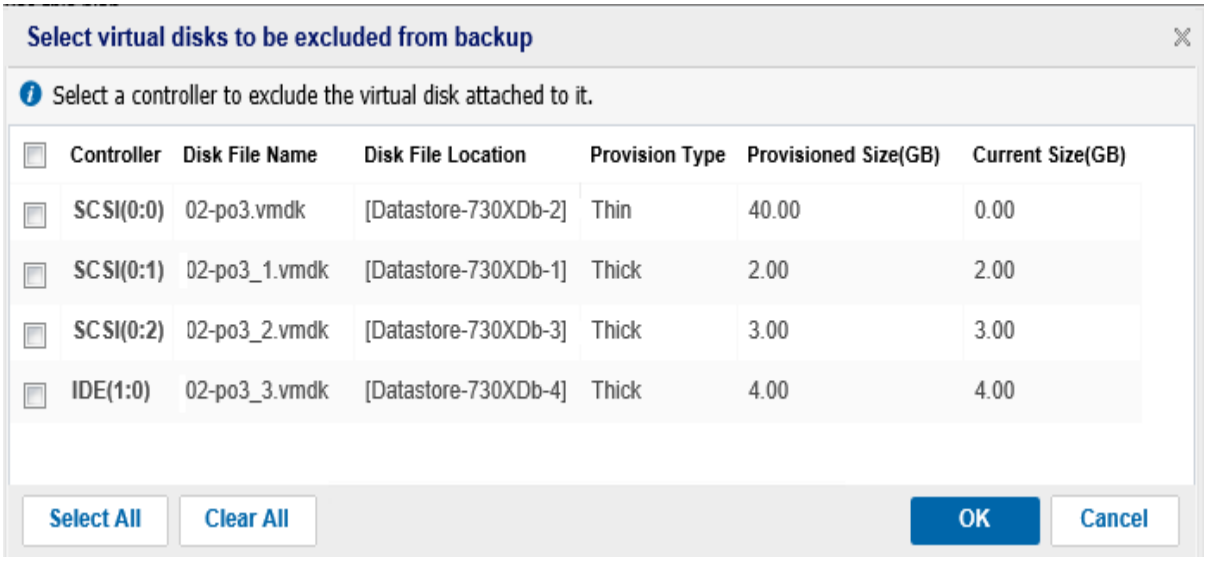
3. (Opcional) Selecione o disco virtual que você pode excluir da tarefa de backup.

   Por padrão, a tarefa de backup sem agente faz o backup da VM inteira, incluindo todos os seus discos virtuais. Porém, você pode especificar um ou mais discos virtuais que são ignorados durante o backup.

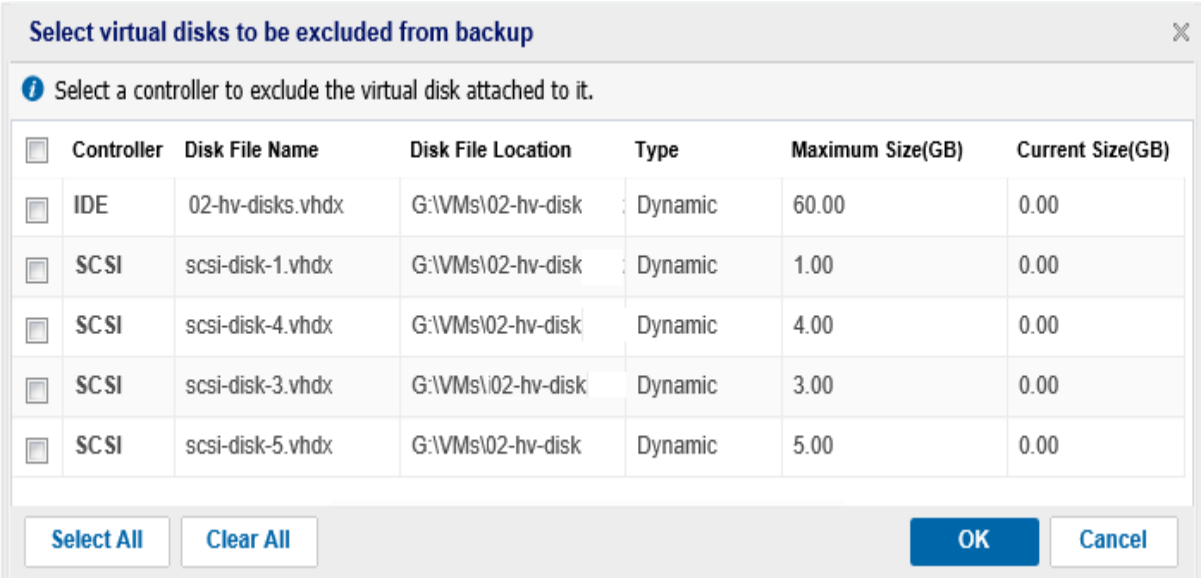
   a. Depois de adicionar um nó da VM no plano, clique no botão Configurar disponível no lado direito do nó.

      Uma caixa de diálogo é exibida.

      Caixa de diálogo para a VM do VMware



      Caixa de diálogo para a VM do Hyper-V



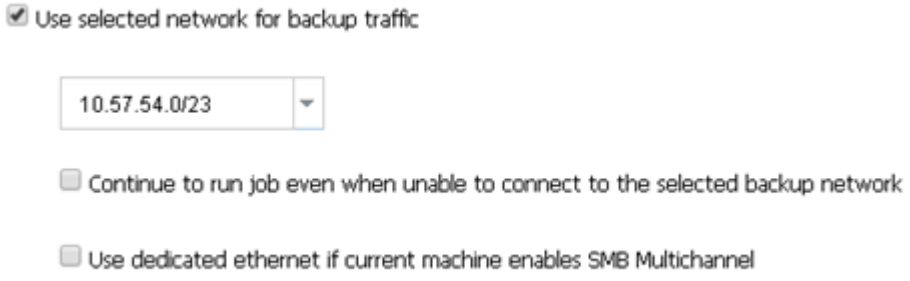
b. Marque a caixa de seleção para o disco virtual que você deseja excluir do backup e clique em **OK** para salvar.

Observações:

- O disco virtual foi excluído pelo controlador em vez do nome do arquivo de disco virtual.
- Se o disco virtual que contém o volume de sistema do sistema operacional convidado for excluído pelo backup, a VM restaurada não poderá inicializar.
- Se a VM tiver um aplicativo (SQL Server ou Exchange) instalado e nenhum disco virtual foi excluído pelo backup, a restauração no nível de banco de dados não será permitida.

4. (Opcional) Marque a caixa de seleção **Usar rede selecionada para o tráfego de backup** e siga estas etapas:

a. Para ativar a comunicação entre o proxy do Windows e o servidor do hipervisor, selecione a rede CIDR no menu suspenso.



b. Se desejar que a tarefa de backup continue mesmo que a rede selecionada não esteja disponível entre o servidor proxy e o hipervisor, marque a caixa de seleção

Continuar a executar a tarefa mesmo que não seja possível conectar-se à rede de backup selecionada.

c. Para definir a restrição no SMB Multichannel para que as transferências de dados sejam realizadas somente pela rede selecionada, marque a caixa de seleção **Usar ethernet dedicada se a máquina atual permitir o SMB Multichannel**.

Observações:

- Essa opção não está disponível por padrão. Para ativar essa opção, vá para o seguinte local da pasta: C:\Arquivos de programas\Arcserve\Unified Data Protection\Management\Configuration\ConsoleConfiguration.xml. Em seguida, modifique o valor de useDedicatedEthernet para True.

```
- <SpecifyNetwork>
    <useDedicatedEthernet>false</useDedicatedEthernet>
  </SpecifyNetwork>
```

- Por padrão, o recurso SMB Multichannel está ativado no Windows.

5. Especifique as configurações de rede para o backup de VM do Hyper-V de backup com base em host:

Configuração do registro: SMBSpecifiedIONetwork

Localização: HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll ou HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\VMInstUUID

Tipo: valor com múltiplas strings

Nome do valor: SMBSpecifiedIONetwork

Dados do valor: string no formulário CIDR (IP/maskBitCount)

Exemplo: 192.168.10.0/24

Se os discos da VM do Hyper-V/agrupamento do Hyper-V estiverem residindo no compartilhamento do SMB, o usuário também poderá definir outra rede a ser usada para transferência de dados entre o servidor SMB e o computador proxy.

Observação: o mapeamento entre o IP especificado e o nome de host do servidor SMB deve ser registrado no domínio.

6. (Opcional) Selecione um dos seguintes métodos de interrupção do VMware. Estas opções são aplicáveis ao VMware somente.

VMware Tools

Indica que o Arcserve UDP usa as ferramentas do VMware para interromper a máquina virtual. Se tiver usado a opção **Microsoft VSS dentro da VM** na tarefa de backup anterior, a primeira tarefa de backup subsequente com essa opção exigirá as credenciais para acessar a máquina virtual. Isso ocorre porque o Arcserve UDP remove as ferramentas necessárias da VM. Além disso, as ferramentas do VMware precisam ser instaladas e atualizadas para a data da VM.

VSS da Microsoft dentro da VM

Indica que o Arcserve UDP usa o VSS da Microsoft no sistema operacional convidado para interromper a máquina virtual. É aplicável somente a máquinas virtuais com sistema operacional convidado Windows. As ferramentas do VMware devem ser instaladas no sistema operacional convidado e atualizadas. Quando usa essa opção, a máquina virtual deve ser ligada e deve estar atualizada com as credenciais de administrador incorporadas. Para obter mais informações sobre como atualizar um nó, consulte Atualizar nós.

Observação: o instantâneo fornecido pela VMware usando essa opção pode não ser consistente com o aplicativo. Em outras palavras, o backup gerado usando essa opção pode não ser um backup consistente com o aplicativo. A solução alternativa é usar o método de encerramento de instantâneo do VMware Tools, juntamente com a desativação dos gravadores VSS *Gravador do serviço da MSSearch* e *Gravador de otimização de cópia de sombra* no sistema operacional convidado da VM antes de esse problema ser corrigido.

Capturar instantâneo sem quiescência de convidado se o instantâneo de quiescência falhar

Indica que, quando a tarefa de backup falha ao criar o instantâneo com a opção de quiescência, o Arcserve UDP continua a tarefa de backup ao obter um instantâneo sem encerrar a máquina virtual.

Observações:

- a opção **VSS da Microsoft dentro da VM** não oferece suporte para a restauração de nível de banco de dados e nível granular do aplicativo.
- Nenhum dos métodos de interrupção é aplicável quando a máquina virtual está desligada. Se uma tarefa de backup for iniciada quando a máquina virtual estiver desligada, a tarefa de backup ignora ambos os métodos de fechamento.
- Para ambos os métodos de interrupção, se a tarefa de backup não puder continuar por qualquer motivo (por exemplo, credenciais incorretas), o Arcserve UDP falhará na tarefa de backup. Para obter mais informações sobre a falha da tarefa de backup, consulte o tópico Solução de problemas.

7. (Opcional) Selecione um dos métodos de transporte do VMware. Estas opções são aplicáveis para VMware.

   Permitir que o VMware selecione o melhor método disponível

   Indica que o VMware seleciona a opção de transferência de dados. Você não precisa definir manualmente qualquer opção de transferência de dados.

   Definir as prioridades do método para este plano

   Indica que é possível selecionar a opção de transferência de dados e definir a prioridade para cada opção. Use o botão de seta para priorizar o modo de transporte.

   - Modo de transporte HOTADD
   - Modo de transporte NBD
   - Modo de transporte NBDSSL
   - Modo de transporte SAN

   Observação: se você tiver especificado o modo de transporte no console e na chave de registro e, em seguida, o conjunto de prioridades do console substitui o conjunto de prioridades na chave do Registro. Para obter mais informações sobre como definir a prioridade usando a chave de registro, consulte Definir um modo de transporte para restauração e backup sem agente com base em host.

8. (Opcional) Selecione o método de instantâneo do Hyper-V. Essas opções são aplicáveis ao Hyper-V somente.

   O backup da VM deve ser efetuado usando instantâneos gerados pelo método VSS da Microsoft

   Indica que o Arcserve UDP usa os métodos de instantâneos nativos da Microsoft – online e offline para a tarefa de backup. Essa é a opção padrão. Quando esta caixa de seleção não está marcada e nenhum dos métodos (online e offline) da Microsoft está disponível, a tarefa de backup usará o método do Arcserve UDP para fazer o backup da máquina virtual.

   Se o método offline da Microsoft for usado para o backup e for necessário que a máquina virtual esteja em um estado salvo, marque também a caixa de seleção **A VM pode ser colocada no estado Salvo antes de obter o instantâneo**. Se não marcar essa caixa de seleção, a tarefa de backup falhará.

   O backup online é o método de backup recomendado, porque ele oferece suporte ao backup consistente de aplicativos sem o tempo de inatividade da máquina virtual. A máquina virtual fica acessível durante o backup. O método de backup online deve satisfazer alguns pré-requisitos, tais como os serviços de integração devem ser instalados e devem estar em execução. Se

qualquer um dos pré-requisitos não for satisfeito, apenas o método de backup offline será usado.

O método de backup offline da Microsoft tem duas abordagens – abordagem de estado salvo e de ponto de verificação. Se o host do Hyper-V tiver o sistema operacional Windows 2012R2 com KB 2919355 ou posterior, a abordagem de ponto de verificação será usada; caso contrário, a abordagem de estado salvo será usada.

A principal diferença entre essas duas abordagens é que a abordagem de estado salvo requer que a máquina virtual fique inacessível por um curto período. A máquina virtual deve ser colocada em um estado salvo por alguns minutos, enquanto é obtido o instantâneo.

Além dos métodos de instantâneos nativos da Microsoft, o Arcserve UDP tem seu próprio método de instantâneos que pode ser usado quando os métodos de instantâneos nativos da Microsoft não estão disponíveis.

Observação: tanto o método offline da Microsoft quanto o método do Arcserve UDP são métodos de backup consistentes nas falhas. Nenhum dos métodos pode garantir a integridade dos dados. A principal diferença entre os métodos é que o método offline da Microsoft pode ser comparado ao estado que a VM tinha ao ter sido desligada abruptamente e o método do Arcserve UDP pode ser comparado ao estado que o host Hyper-V tinha quando foi desligado abruptamente.

A VM pode ser colocada no estado Salvo antes de obter o instantâneo

Indica que a máquina virtual é colocada no estado Salvo, se necessário, antes de obter o instantâneo do VSS. Selecione essa opção quando a máquina virtual não oferecer suporte ao backup online. Se a máquina virtual oferecer suporte ao backup online, mesmo se ativar essa opção, a máquina virtual não será colocada no estado Salvo.

A origem é especificada.

Definir um modo de transporte no registro para backup e restauração sem agente com base em host

É possível definir o modo de transporte (dados de transferência) para o agente de UDP como proxy que executa tarefas de backup sem gente com base em host ou de restauração para máquinas virtuais que residem em um servidor VMware ESX. Por padrão, o backup sem agente com base em host e a restauração usam um modo que permite a otimização do desempenho do backup sem agente com base no host e restauração (aumentar a velocidade) na transferência de dados. No entanto, quando você deseja especificar um modo de transporte específico para backup e restauração, é necessário configurar a chave de registro descrita neste tópico.

Observação: para o backup, o modo de transporte definido no plano tem precedência sobre o que é definido no Registro.

O Host-Based VM Backup pode executar backups usando os seguintes modos de transporte:

- Modo de transporte HOTADD
- Modo de transporte NBD
- Modo de transporte NBDSSL
- Modo de transporte SAN

Observe as seguintes considerações:

- Esta tarefa de configuração é opcional. Por padrão, o Host-Based VM Backup executa backups usando um modo de transporte que otimiza o desempenho da operação de backup.
- Ao configurar essa chave de registro para usar um modo de transporte específico e se o modo não estiver disponível, o backup da VM com base em host usará um modo de transporte padrão disponível para a operação de backup.
- É possível definir o modo de transporte para todas as VMs que são usadas para o backup usando o servidor proxy (nível de proxy) ou definindo um determinada VM (nível da VM). Se configurar o servidor proxy e a VM, o registro de nível da VM terá precedência sobre o nível de registro do proxy.

Siga estas etapas para definir o modo de transporte no nível do servidor proxy (aplicável para backup e restauração):

1. Efetue logon no servidor proxy de backup do Agente do Arcserve Unified Data Protection para Windows.
2. Abra o editor de registro do Windows e procure a seguinte chave de registro:

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine]

3. Clique com o botão direito em VDDKEnforceTransport e clique em Modificar no menu pop-up para abrir a caixa de diálogo Editar cadeia de caracteres.
4. No campo Dados de valor, especifique o modo de transporte que você deseja usar durante a tarefa de backup. Especifique um ou mais dos seguintes valores separados por ":". (Por exemplo, nbd ou san:nbd:nbdssl:)

   hotadd

   Modo de transporte HOTADD

   nbd

   Modo de transporte NBD

   nbdssl

   Modo de transporte NBDSSL

   san

   Modo de transporte SAN
5. Clique em OK para aplicar o valor e fechar a caixa de diálogo Editar sequência.

   O modo de transporte é definido e usado na próxima vez que a tarefa for executada.

   Observação: para restaurar VMDK (Virtual Machine Disks – Discos de Máquina Virtual) finos, o modo de transporte não avançado (modo de transporte LAN) é usado por padrão. Para ativar o modo de transporte avançado para VMDK finos, atualize a chave do registro, conforme mostrado no exemplo a seguir:

   a. Abra o editor de registro do Windows e procure a seguinte chave de registro:

      ```
      [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified
      Data Protection\Engine]
      ```

   b. Crie uma chave denominada AFRestoreDll.

   c. Crie um valor de sequência de caracteres denominado EnforceTransportForRecovery na chave AFRestoreDll.

   d. Especifique o modo de transporte que deseja usar durante a tarefa de recuperação. (Por exemplo: "san:nbd:nbdssl")

      Exemplo

      [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFRestoreDll]

      "EnforceTransportForRecovery"="san:hotadd:nbd:nbdssl"

   Siga estas etapas para definir o modo de transporte no nível da VM (somente aplicável para backup):

1. Efetue logon no servidor proxy de backup do Agente do Arcserve Unified Data Protection para Windows para as máquinas virtuais.
2. Abra o editor de registro do Windows e procure a seguinte chave de registro:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\{VM-InstanceUUID}
3. Clique com o botão direito do mouse em VM-InstanceUUID e selecione Novo.
4. Clique em Valor da sequência no menu pop-up.
5. Nomeie o novo valor da sequência de caracteres, como a seguir.

   EnforceTransport
6. Clique com o botão direito em EnforceTransport e clique em Modificar no menu pop-up para abrir a caixa de diálogo Editar sequência.
7. No campo Dados de valor, especifique o modo de transporte que você deseja usar durante a tarefa de backup. Especifique um dos seguintes valores:

   hotadd

   Modo de transporte HOTADD

   nbd

   Modo de transporte NBD

   nbdssl

   Modo de transporte NBDSSL

   san

   Modo de transporte SAN
8. Clique em OK para aplicar o valor e fechar a caixa de diálogo Editar sequência.

   O modo de transporte é definido e usado na próxima vez que a tarefa for executada.

Especificar o destino

O destino é o local onde você armazena os dados de backup. É necessário, no mínimo, especificar o destino para salvar o plano.

Siga estas etapas:

1. Selecione um dos seguintes **Tipos de destino**:

   Disco local ou uma pasta compartilhada

   Especifica que o destino de backup é um destino local ou uma pasta compartilhada. Se selecionar essa opção, será possível salvar os dados como pontos de recuperação ou conjuntos de recuperação. As opções de pontos de recuperação e de conjuntos de recuperação estão disponíveis na guia **Programar**.

   Servidor de ponto de recuperação do Arcserve UDP

   Especifica que o destino de backup é um servidor de ponto de recuperação. Se selecionar essa opção, os dados serão armazenados como pontos de recuperação. Não é possível armazenar dados como conjuntos de dados de recuperação.

2. Se tiver selecionado **Servidor de ponto de recuperação do Arcserve UDP**, forneça os seguintes detalhes:

   a. Selecione um servidor de ponto de recuperação.

   b. Selecione um repositório de dados. A lista exibe todos os repositórios de dados que são criados no servidor de ponto de recuperação especificado.

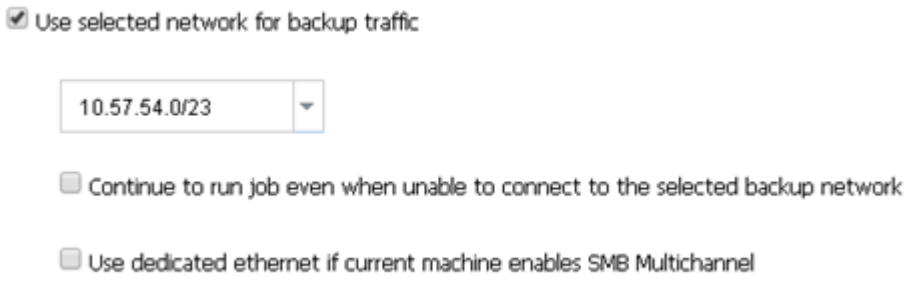
   c. Forneça uma senha da sessão.

   Observação: a senha da sessão é opcional quando o destino de backup é um repositório de dados do RPS não criptografado.

   d. Confirme a senha da sessão.

   e. (Opcional) Marque a caixa de seleção **Usar rede selecionada para o tráfego de backup** e siga estas etapas:

      1. Para ativar a comunicação entre o proxy do Windows e o servidor de ponto de recuperação, selecione a rede CIDR no menu suspenso.



2. Se você desejar que a tarefa de backup continue mesmo que a rede selecionada não esteja disponível entre o servidor proxy e o servidor de ponto de recuperação, marque a caixa de seleção **Continuar a executar a tarefa mesmo que não seja possível conectar-se à rede de backup selecionada**.
3. Para desativar o SMB Multichannel para que as transferências de dados sejam realizadas somente pela rede selecionada, marque a caixa de seleção **Usar ethernet dedicada se a máquina atual permitir o SMB Multichannel**.

Observações:

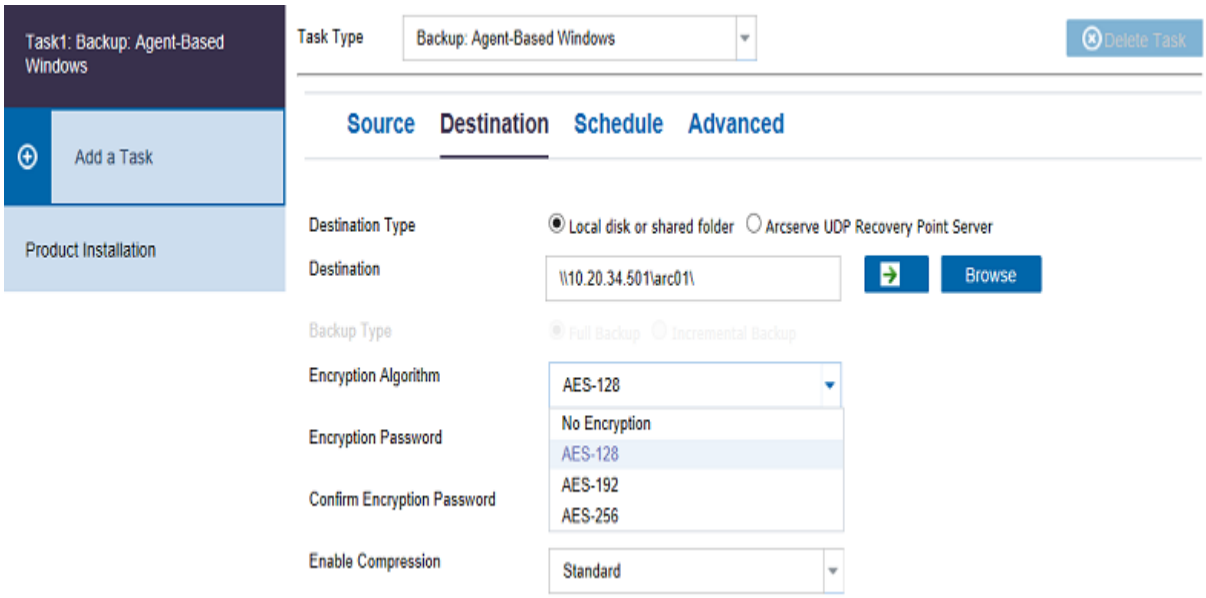
- Essa opção não está disponível por padrão. Para ativar essa opção, vá para o seguinte local da pasta: C:\Arquivos de programas\Arcserve\Unified Data Protection\Management\Configuration\ConsoleConfiguration.xml. Em seguida, modifique o valor de *useDedicatedEthernet* para True.

```
- <SpecifyNetwork>
    <useDedicatedEthernet>false</useDedicatedEthernet>
  </SpecifyNetwork>
```

  A função Especificar rede fica desativada caso o repositório de dados seja remoto e utilize uma pasta compartilhada de rede como destino.

- Por padrão, o recurso SMB Multichannel está ativado no Windows.

3. Se tiver selecionado **Disco local ou pasta compartilhada**, forneça os seguintes detalhes:



a. Forneça o caminho completo do destino local ou de rede. Para o destino de rede, especifique as credenciais com o acesso de gravação. Você pode clicar em Procurar para localizar o destino ou clicar no ícone de seta para frente para testar a conexão e fornecer as credenciais para a pasta de destino fornecida.

b. Na lista de opções da lista suspensa, selecione o algoritmo de criptografia. Para obter mais informações, consulte Configurações de criptografia.

c. Como opção, forneça uma senha de criptografia.

d. Digite a senha de criptografia novamente para confirmar.

e. Selecione um tipo de compactação. para obter mais informações, consulte Tipo de compactação.

Observação: se armazenar os dados em um disco local ou em uma pasta compartilhada, não será possível replicar os dados para outro servidor de ponto de recuperação. A replicação é suportada apenas se armazenar os dados em um servidor de ponto de recuperação.

O destino é especificado.

Especificar a programação

A página Programar permite definir uma programação para o backup e para que as funções Mesclar e Acelerar sejam repetidas em intervalos específicos. Após definir uma programação, as tarefas são executadas automaticamente de acordo com a programação. É possível adicionar várias programações e fornecer configurações de retenção.

Uma Programação de backup se refere a programação regular que é repetida várias vezes ao dia, com base no número de horas ou minutos que selecionar. Além da programação regular, uma programação de backup também fornece opções para adicionar programações diária, semanal e mensal.

Observação: para obter mais informações sobre as configurações de retenção e programação, consulte Entendendo a programação avançada e retenção.

Siga estas etapas:

1. (Opcional) Selecione a opção para gerenciar os pontos de recuperação. Essa opção será visível somente se tiver selecionado o local ou a pasta compartilhada como o destino do backup.

   Reter por pontos de recuperação

   Os dados de backup são armazenadas como pontos de recuperação.

   Reter por conjuntos de recuperação

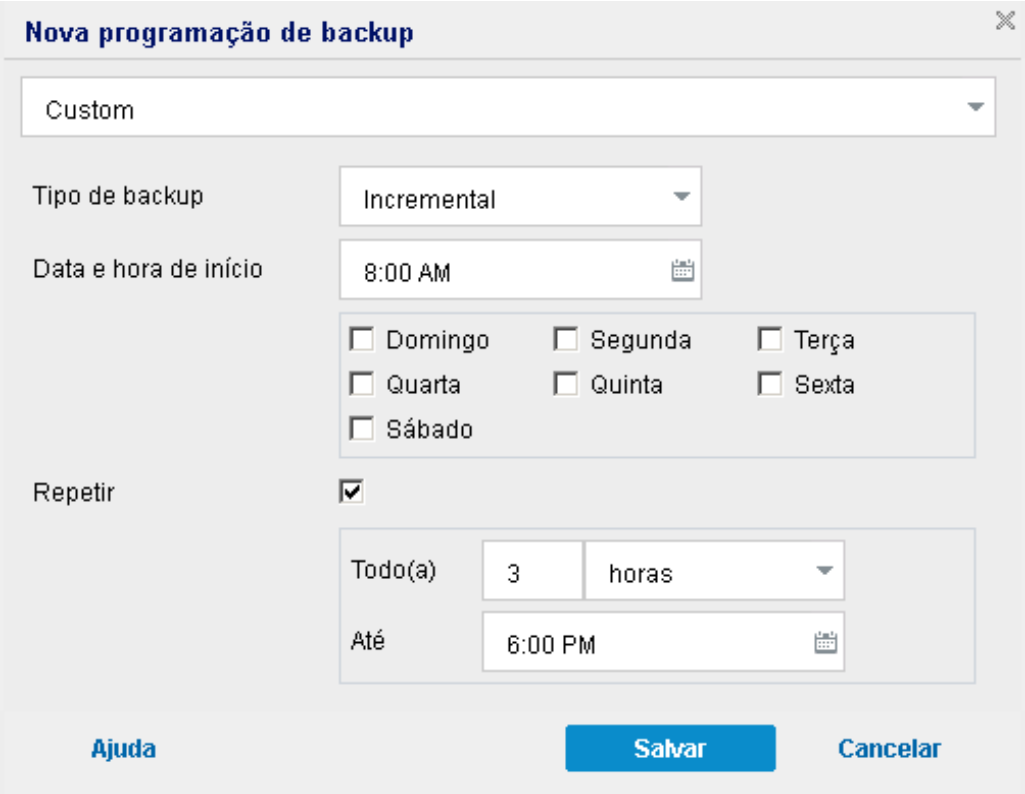
   Os dados de backup são armazenadas como conjuntos de recuperação.

2. Adicionar programações de backup, mesclagem e acelerador.

   Adicionar programação de backup

   a. Clique em **Adicionar** e selecione **Adicionar programação de backups**.

      A caixa de diálogo **Nova programação de backup** é aberta.



b. Selecione uma das seguintes opções:

Personalizado

Especifica a programação de backup que se repete várias vezes por dia.

Diário

Especifica a programação de backup que ocorre uma vez por dia. Por padrão, todos os dias da semana estão selecionados para o backup diário. Se não desejar executar a tarefa de backup em um dia específico, desmarque a caixa de seleção correspondente àquele dia da semana.

Semanal

Especifica a programação de backup que ocorre uma vez por semana.

Mensal

Especifica a programação de backup que ocorre uma vez por mês.

c. Selecione o tipo de backup.

Completo

Especifica a programação de backups para backups completos. Conforme programado, o Arcserve UDP executa um backup completo de todos os blocos usados do computador de origem. Um backup completo em geral, consome tempo, dependendo do tamanho do backup.

Verificar

Especifica a programação de backups para backups de verificação.

Conforme programado, o Arcserve UDP verificará se os dados protegidos são válidos e íntegros executando uma verificação de confiabilidade da imagem de backup armazenada na origem do backup. Se necessário, a imagem será sincronizada novamente. Um backup de verificação examinará o backup mais recente de cada bloco e irá comparar o conteúdo e as informações com a origem. Esta comparação verifica se o backup mais recente dos blocos representa as informações correspondentes na origem. Se a imagem de backup de qualquer bloco não corresponder à origem (possivelmente devido a alterações no sistema desde o último backup), o Arcserve UDP atualizará (fará nova sincronização) o backup do bloco que não corresponder. É possível também usar um backup de verificação (muito raramente) para obter a garantia de backup completo sem usar o espaço necessário para um backup completo.

Vantagens: produz uma pequena imagem de backup quando comparado ao backup completo, pois somente os blocos alterados (blocos que não coincidem com o último backup) são armazenados em backup.

Desvantagens: o tempo de backup é longo, pois todos os blocos de origem são comparados aos blocos do último backup.

Incremental

Especifica a programação de backups para backups incrementais.

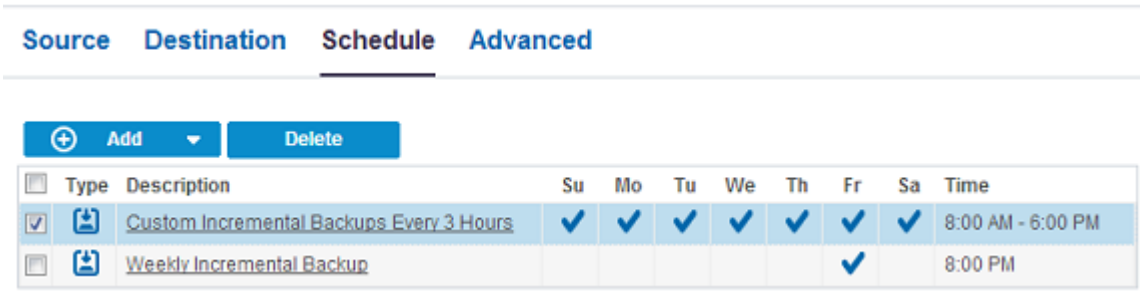
Conforme programado, o Arcserve UDP faz backup incremental apenas dos blocos que foram alterados desde o último backup realizado com êxito. As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a execução de backups e você deve usá-la por padrão.

d. Especifique a hora de início do backup.

e. (Opcional) Marque a caixa de seleção de **Repetição** e especifique a programação a ser repetida.

f. Clique em **Salvar**.

A programação de backup é especificada e é exibida na página de **Programação**.



Adicionar Programação de mesclagem

a. Clique em **Adicionar** e selecione **Adicionar programação de mesclagem**.

b. A caixa de diálogo **Adicionar nova programação de mesclagem** é aberta.

c. Especifique a hora de início para iniciar a tarefa de mesclagem.

d. Especificar **Até** para especificar uma hora de término para a tarefa de mesclagem.

e. Clique em **Salvar**.

A programação de mesclagem é especificada e é exibida na página de **Programação**.

Adicionar programação de acelerador

a. Clique em **Adicionar** e selecione **Adicionar programação de acelerador.**

b. A caixa de diálogo Adicionar nova programação do acelerador é aberta.

c. Especifique o limite de taxa de transferência em MB por minuto.

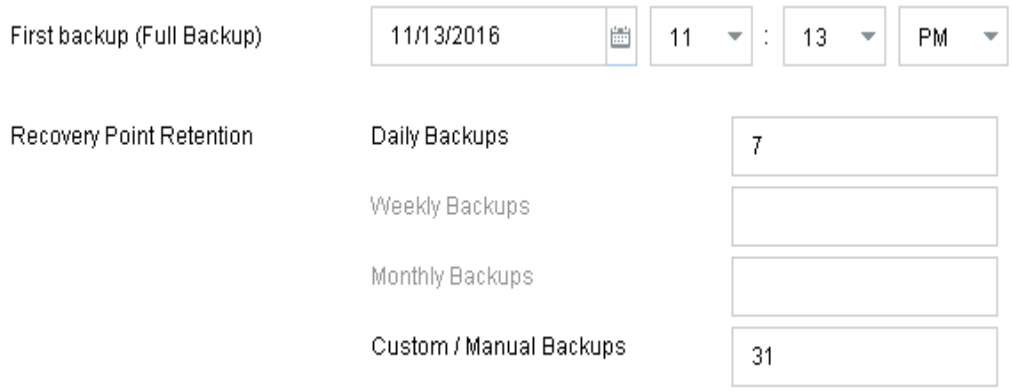
d. Especifique a hora de início para iniciar a tarefa de taxa de transferência de backup.

e. Especifique **Até** para especificar um horário de término para a tarefa de taxa de transferência.

f. Clique em **Salvar**.

A programação de taxa de transferência é especificada e é exibida na página de **Programação**.

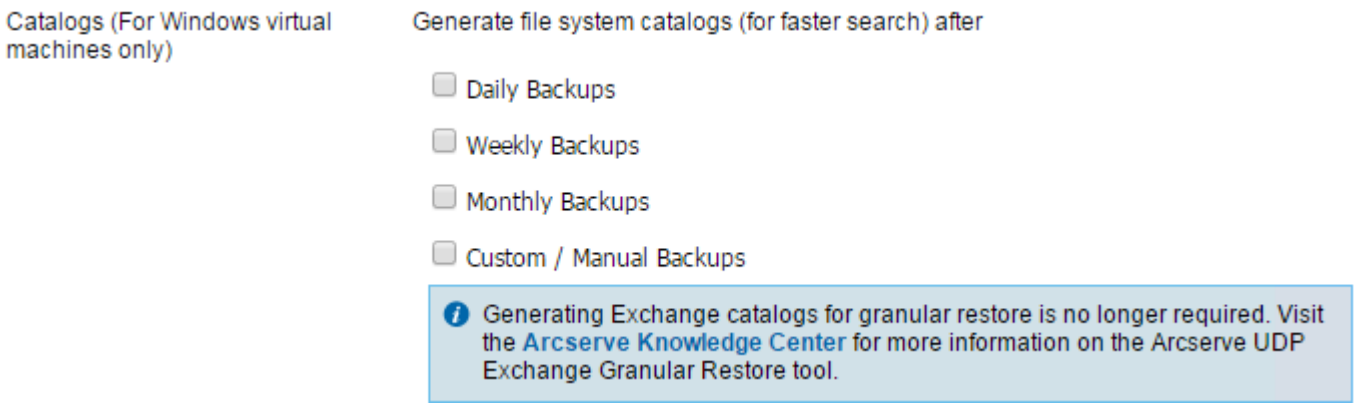
3. Especifique a hora de início do backup programado.



4. Especifique as configurações de retenção de pontos de recuperação para programação diária, semanal e mensal.

   Essas opções serão ativadas se tiver adicionado a programação de backup correspondente. Se você modificar as configurações de retenção desta página, as alterações serão refletidas na caixa de diálogo Programação de backup.

5. Especifique os detalhes de catálogo.



   Os catálogos permitem gerar o catálogo do sistema de arquivos. O catálogo do sistema de arquivos é necessário para agilizar e facilitar a pesquisa. Os catálogos estão ativados de acordo com o tipo de backup que você especificou.

   A programação é especificada.

Noções básicas sobre a programação avançada e retenção

A opção de programação permite especificar uma programação personalizada, uma programação diária/semanal/mensal ou ambas. Na programação personalizada, é possível configurar a programação de backups para cada dia da semana ou adicionar até quatro programações de backup em cada dia. É possível escolher um dia específico da semana e criar uma janela para definir quando executar o backup e em que frequência.

Programação	Tarefa com suporte	Comentários
Backup	Tarefa de backup	Definir janelas de tempo para a execução de tarefas de backup.
Limitação de backup	Tarefa de backup	Definir janelas de tempo para controlar a velocidade de backup.
Mesclar	Tarefa de mesclagem	Definir quando executar tarefas de mesclagem.
Programação diária	Tarefa de backup	Definir quando executar tarefas do backup diário.
Programação semanal	Tarefa de backup	Definir quando executar tarefas do backup semanal.
Programação mensal	Tarefa de backup	Definir quando executar tarefas do backup mensal.

Também é possível especificar as configurações de retenção para os pontos de recuperação.

Observação: as configurações de retenção devem ser definidas em cada plano para controlar como os dados dos nós atribuídos a esse plano são retidos no repositório de dados de destino.

As programações para backups diários/semanais/mensais são independentes para a programação personalizada e umas das outras. É possível configurar para executar somente o backup diário, semanal ou mensal, sem configurar a Programação personalizada.

Programação de tarefas de backup

É possível adicionar quatro janelas de tempo por dia na programação do backup. Uma janela de tempo é válida das 00:00 às 23:59. Não é possível especificar uma janela de tempo das 18:00 às 6:00. Nesses casos, você deve especificar manualmente duas janelas de tempo diferentes.

Para cada janela de tempo, a hora de início é inclusiva e a hora de término é exclusiva. Por exemplo, você configurou para executar o backup incremental em intervalos de uma hora entre as 6:00 e as 9:00. O backup será iniciado às 6:00. Isso significa que o backup será executado às 6h00, 7h00 e 8h00, mas NÃO às 9h00.

Observação: se você deseja executar a tarefa de backup várias vezes até o fim do dia, defina a programação para até 0h00. Por exemplo, para executar a tarefa de backup a cada 15 minutos o dia inteiro, defina a programação como das 0h00 às 00h00, a cada 15 minutos.

Programação do acelerador de backup

A programação de aceleração do backup permite controlar a velocidade da taxa de transferência de backup o que, por sua vez, controla o uso de recursos (E/S de disco, CPU, largura de banda de rede) do servidor cujo backup está sendo feito. Isso é útil quando se não quiser afetar o desempenho do servidor durante o horário comercial. É possível adicionar quatro janelas de tempo por dia na sua programação de aceleração do backup. Para cada janela de tempo, é possível especificar um valor, em MB por minuto. Esse valor será usado para controlar a taxa de transferência do backup. Os valores válidos variam entre 1 MB/minutos a 99999 MB/minutos.

Se uma tarefa de backup estende seu tempo especificado, o limite de aceleração será ajustado de acordo com o tempo especificado. Por exemplo, você definiu o limite de aceleração de backup como 500 MB/minuto das 8:00 às 20:00 e 2500 MB/minuto das 20:00 às 22:00. Se uma tarefa de backup iniciar às 19h00 e for executada durante três horas, das 19h00 às 20h00 o limite de aceleração será de 500 MB/minuto e das 20h00 às 22h00, o limite de aceleração será 2500 MB/minuto.

Se não definir nenhuma programação do backup e programação da taxa de transferência do backup, o backup será executado o mais rápido possível.

Mesclar a programação

Permite mesclar pontos de recuperação com base na programação fornecida.

Considere os seguintes pontos para a tarefa de mesclagem:

- A qualquer momento apenas uma tarefa de mesclagem pode ser executada para um nó.
- Se uma tarefa de mesclagem iniciar, ela precisará ser concluída antes que a próxima tarefa de mesclagem seja iniciada. Isso significa que, se um ou mais conjuntos de pontos de recuperação forem mesclados, não será possível adicionar o

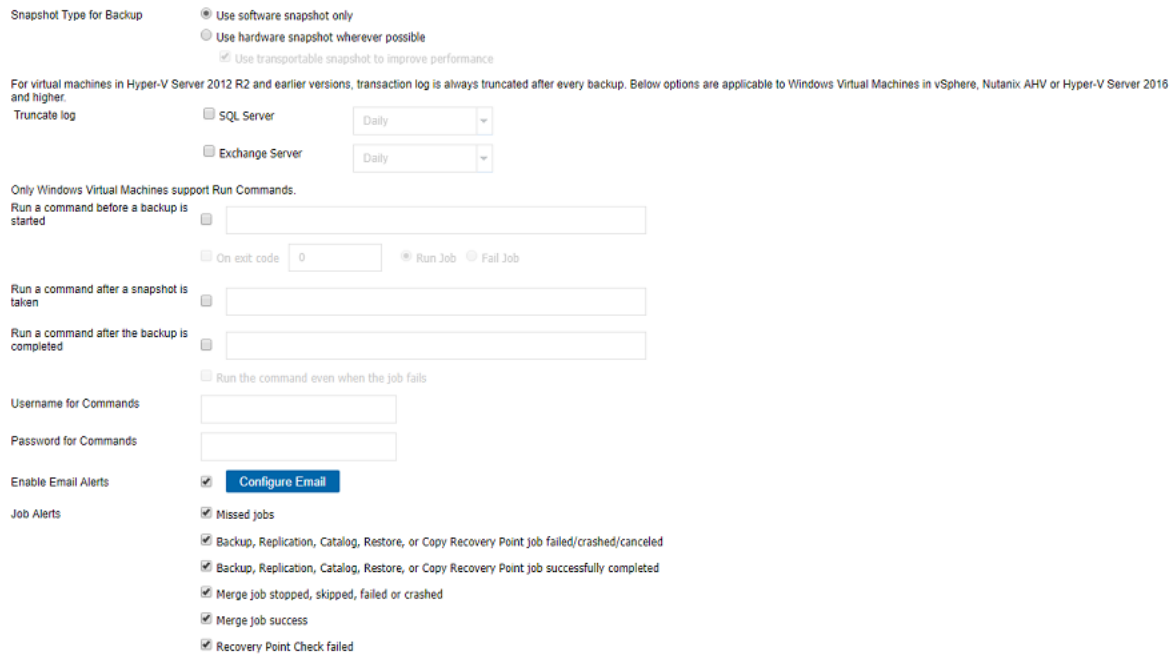
novo ponto de recuperação a este processo de mesclagem, até que o processo de mesclagem do conjunto atual de ponto de recuperação seja concluído.

- Se uma tarefa de mesclagem estiver processando mais de um conjunto de pontos de recuperação (por exemplo, conjunto [1~4], conjunto [5~11] e conjunto [12~14]; são três conjuntos) o servidor de ponto de recuperação processará esses conjuntos, um por um.
- Se uma tarefa de mesclagem é retomada após um intervalo, a tarefa detectará em que ponto ela foi pausada e continuará a mesclagem a partir do ponto de pausa.

Especificar as configurações avançadas

A guia **Avançado** permite especificar algumas configurações avançadas para a tarefa de backup. As configurações avançadas incluem fornecer o tipo de instantâneo para backup, as configurações de log de truncamento, a localização de todos os scripts e as configurações de email. Verifique os pré-requisitos antes de selecionar o tipo de instantâneo de hardware.

A imagem a seguir mostra a guia Avançado:



Siga estas etapas:

1. Especifique os seguintes detalhes.

   Tipo de instantâneo para backup

   Selecione uma das opções a seguir para o instantâneo de backup.

   Usar apenas instantâneo de software

   Especifica que o tipo de backup usa apenas o instantâneo do software. O Arcserve UDP não verificará se há instantâneos de hardware. O instantâneo de software utiliza menos recursos nas máquinas virtuais. É possível usar essa opção se o servidor tiver menos configurações e menor velocidade de processamento.

   Usar instantâneo de hardware sempre que possível

Especifica que o tipo de backup primeiro verifica se há um instantâneo de hardware. Se todos os critérios forem atendidos, o tipo de backup usa o instantâneo de hardware.

Observação: para obter mais informações sobre os critérios de instantâneo de hardware, consulte o pré-requisito.

Para o Hyper-V, o Arcserve UDP usa o provedor de hardware para obter um instantâneo VSS dos volumes no host do Hyper-V e importa o instantâneo de hardware para o servidor proxy. O servidor proxy deve ter um provedor de hardware adequado instalado. Para o VMware, o Arcserve UDP cria um instantâneo de software do vSphere por um curto período e, em seguida, cria um instantâneo de hardware. Esse instantâneo de hardware é montado no VMware ESX Server e o instantâneo de software é excluído. Em seguida, o Arcserve UDP usa o conteúdo no instantâneo de hardware para fazer backup dos arquivos relacionados à VM.

Usar instantâneo transportável para melhorar o desempenho

Especifica que o instantâneo de hardware usa um instantâneo transportável. Um instantâneo transportável aumenta a taxa de transferência de backup. Essa opção aplica-se apenas a servidores Hyper-V.

Truncar log

Permite especificar a programação para truncar logs para o SQL Server e o Exchange Server. É possível especificar a programação como **Diária**, **Semanal** ou **Mensal**. Isso é aplicável somente para VMware.

Executar um comando antes do início do backup

Permite a execução de um script antes de iniciar a tarefa de backup. Especifique o caminho em que o script está armazenado dentro do sistema operacional convidado da máquina virtual. Clique em **No código de saída** e especifique o código de saída para **Executar tarefa** ou **Tarefa com falha**. **Executar a tarefa** indica que a tarefa de backup continuará quando o script retornar o código de saída. **Tarefa com falha** indica que a tarefa de backup será interrompida quando o script retornar o código de saída. Isso é aplicável somente para VM do Windows.

Observações (também aplicáveis aos comandos Depois de gerar um instantâneo e Após a conclusão do backup):

- Sugerimos a especificação do caminho completo do comando/script. Por exemplo, use C:\Windows\System32\Ping.exe, em vez de apenas Ping.exe.
- Para evitar o problema de que a tarefa de backup trava porque comando/script suspende, por padrão o comando/script será encerrado se a sua

conclusão não for realizada em 3 minutos. Se você desejar alterar a configuração de tempo limite padrão, siga estas etapas no servidor proxy ou nível da VM:

No nível do servidor proxy (aplicável a todas as tarefas de backup em execução no servidor proxy)

a. Abra a chave do registro no seguinte local:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

b. Adicione um valor DWORD com o nome PrePostCMDTimeoutInMinute e especifique seu valor com tempo limite em minutos.

No nível da VM

a. Abra a chave do registro no seguinte local:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<vm instance uuid>]

b. Adicione um valor DWORD com o nome PrePostCMDTimeoutInMinute e especifique seu valor com tempo limite em minutos.

   Observação: se você adicionar ao registro um valor no nível de VM e outro no nível proxy, a configuração do registro no nível de VM terá prioridade sobre a configuração no nível de proxy.

Executar um comando depois de gerar um instantâneo

Permite executar um script depois que o backup do instantâneo for gerado. Especifique o caminho em que o script está armazenado dentro do sistema operacional convidado da máquina virtual. Isso é aplicável somente para VM do Windows.

Executar um comando após a conclusão do backup

Permite executar um script depois que a tarefa de backup foi concluída. Especifique o caminho em que o script está armazenado dentro do sistema operacional convidado da máquina virtual. Isso é aplicável somente para VM do Windows.

Executar um comando, mesmo quando a tarefa falhar

Se essa caixa de seleção for selecionada, o script especificado em "Executar um comando após a conclusão do backup" é executado mesmo quando a tarefa de backup falha. Caso contrário, aquele script é executado somente quando a tarefa de backup é concluída com êxito.

Nome de usuário para comandos

Permite especificar o nome de usuário para executar os comandos.

Senha para comandos

Permite especificar a senha para executar os comandos.

Ativar alertas por email

Permite ativar alertas por email. É possível especificar configurações de email e os tipos de alertas que você deseja receber por email. Ao selecionar esta opção, as seguintes opções serão ativadas para a seleção.

Configurações de email

Permite configurar as definições de email. Clique em **Configurações de email** e configure o servidor de email e os detalhes do servidor proxy.

Alertas de tarefa

Permite selecionar os tipos de emails de alerta de tarefas que deseja receber.

2. Clique em **Salvar**.

As atualizações são salvas, e uma marca de seleção verde é exibida ao lado do nome da tarefa. A página do plano é fechada.

Observação:

- Caso precise adicionar outra tarefa, selecione o plano na guia Recursos e modifique-o. Para modificar o plano, clique no plano do painel central. O plano é exibido e será possível modificá-lo.
- Quando você seleciona um nó que não tem o agente do Arcserve UDP instalado, como o proxy de backup, o console do UDP implanta um agente nesse nó automaticamente após o salvamento do plano.

O plano de backup com base em host sem agente para a máquina virtual é criado. O backup é executado de acordo com a programação que você configurou na guia **Programar.** Também é possível fazer backup manual quando desejado.

Executar o comando de script e truncamento do log com a conta de administrador adicional

A conta de administrador adicional faz referência a essas contas que não são administradores padrão. As próximas duas contas são envolvidas quando você executa os comandos ou scripts:

1. Conta definida por atualização de nó
2. Conta definida na guia Avançado de um plano

As máquinas virtuais VMware e Hyper-V têm condições separadas para usar as contas de administrador adicionais.

Máquinas virtuais do VMware

Se ambas as contas forem definidas, use a primeira conta para efetuar logon na máquina virtual (o SDK do vSphere é usado para se comunicar com a máquina virtual, de modo que o acesso à rede não é necessário entre o servidor proxy e a máquina virtual). Em seguida, use a segunda conta para executar o comando ou script na máquina virtual.

Se alguma das contas não estiver definida, use a conta disponível para efetuar logon na máquina virtual e executar o comando ou o script.

É recomendável usar a conta de administrador padrão ou a conta de administrador de domínio padrão para ambas as contas.

Se usar qualquer conta de administrador adicional (conta de administrador que não seja interno), o procedimento é diferente.

Siga estas etapas:

1. Para efetuar logon na máquina virtual usando a conta de administrador adicionada, siga a etapa no tópico Atualizar nó para certificar-se de que a conta tenha as permissões necessárias.
2. Para executar o comando ou o script usando a conta de administrador adicional, verifique se a conta tem a permissão necessária. Efetue logon na máquina virtual de convidado usando a conta de administrador adicional, execute o comando ou script e confirme se o comando ou o script pode ser concluído com êxito.

Máquinas virtuais do Hyper-V

Você precisa de apenas uma conta para máquinas virtuais do Hyper-V. Se ambas as contas forem definidas, use a segunda conta (definida na guia Avançado de um plano) para se conectar à máquina virtual e executar o comando ou o script. A WMI (Windows Management Instrumentation - Instrumentação de Gerenciamento

do Windows) é usada para se comunicar com a máquina virtual, para que o acesso à rede seja necessário entre o servidor proxy e a máquina virtual.

Se alguma das contas não estiver definida, use a conta de administrador disponível para se conectar à máquina virtual e executar o comando ou o script.

Siga estas etapas:

1. Acesse a máquina virtual com a WMI remota. Verifique se possui as permissões necessárias com a conta de administrador adicional. Consulte o tópico Atualizar nó para obter os requisitos da conta.
2. Para executar o comando ou o script usando a conta de administrador adicional, verifique se a conta tem a permissão necessária. Efetue logon na máquina virtual de convidado usando a conta de administrador adicional, execute o comando ou script e confirme se o comando ou o script pode ser concluído com êxito.

   Além disso, verifique se a WMI é permitida pelo firewall na VM convidada. Se não estiver ativada, siga estas etapas:

1. Efetue logon na VM convidada.
2. Abra o painel de controle.
3. Abra o Windows Firewall.
4. Clique em Permitir um aplicativo ou recurso através do Firewall do Windows.
5. Ative a WMI.
6. Clique em OK.

Definir um limite para a quantidade de backups simultâneos

É possível definir um limite para a quantidade de tarefas de backup executadas simultaneamente. Este recurso permite otimizar o desempenho do servidor proxy de backup da máquina virtual com base em host em seu ambiente de backup. Por padrão, o Backup de VM com base em host pode executar até quatro tarefas de backup da VM do VMware, dez tarefas de backup da VM do Hyper-V e quatro tarefas de backup da VM do Nutanix AHV simultaneamente. Em ambientes com várias máquinas virtuais associadas a um servidor proxy, uma grande quantidade de backups simultâneos pode ter um efeito adverso no desempenho da rede e do backup.

Observação: quando a quantidade de tarefas simultâneas exceder o limite definido, as tarefas que excederem o limite entrarão em uma fila de tarefas.

Observação: se o número máximo de tarefas simultâneas de backup do VMware exceder o limite de conexão do ESX Serve, pode ocorrer falha na comunicação entre o ESX Server e o proxy de backup e o sistema de arquivos do repositório de dados do ESX Server pode permanecer bloqueado. Nesses casos, reinicie o ESX Server ou migre a máquina virtual bloqueada para outro repositório de dados para desbloquear a VM. Para obter mais detalhes, consulte o documento de VMware (VMware KB: 1022543).

Siga estas etapas:

1. Efetue logon no sistema proxy da máquina virtual do Arcserve UDP.
2. Abra o editor de registro do Windows e procure a seguinte chave de registro:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine
   ```

3. Localize as seguintes chaves:

   ```
   VMwareMaxJobNum
   ```

   ```
   HyperVMaxJobNum
   ```

   ```
   AHVMaxJobNum
   ```

   Observação: ambas as chaves já foram criadas e o valor padrão é 4 e 10, respectivamente.

4. Clique com o botão direito do mouse em VMMaxJobNum, HyperVMaxJobNum ou AHVMaxJobNum e clique em Modificar no menu pop-up.

   A caixa de diálogo Editar Cadeia de Caracteres é aberta.

5. No campo Dados do valor, especifique a quantidade de tarefas de backup que deseja executar simultaneamente.
   - **Limite mínimo**--1
   - **Limite máximo**--nenhum
   - **Padrão**--10 para o Hyper-V e 4 para o VMware e o Nutanix AHV
6. Clique em OK.

   O limite é definido.

   O limite de tarefas de backup simultâneas é definido.

(Opcional) Executar um backup manual

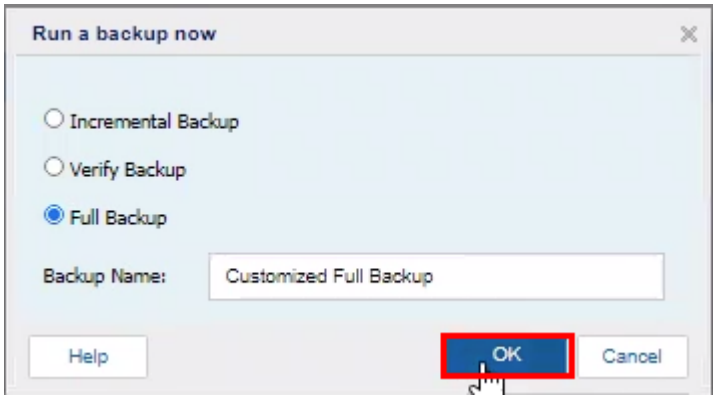
Em geral, os backups são executados automaticamente e controlados pelas configurações da programação. Além do backup programado, um backup manual fornece a opção de fazer backup dos nós de acordo com a necessidade. Por exemplo, se você repetir a programação para backups completos, incrementais e de verificação e desejar fazer grandes alterações em seu computador, deverá executar um backup manual imediato sem esperar até que ocorra o próximo backup programado.

Siga estas etapas:

1. Efetue logon no Console do Arcserve UDP.
2. Navegue até **recursos** > **Plano** > **Todos os planos**.

   A lista de todos os planos é exibida no painel central.
3. Clique com o botão direito do mouse no plano e selecione **Fazer backup agora**.

   A caixa de diálogo Fazer backup agora é exibida.
4. Na caixa de diálogo Executar um backup agora, selecione o tipo de backup que deseja executar e, em seguida, especifique o nome do backup, se necessário.



As opções disponíveis são:

Backup incremental

Inicia um backup incremental do computador inteiro. Um backup incremental realiza backup somente dos blocos que foram alterados desde o backup anterior.

Observação: se estiver executando um backup pela primeira vez, o backup completo será iniciado automaticamente, mesmo que você tenha selecionado a opção Backup incremental.

As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a execução de backups.

Verificar backup

Inicia um backup de verificação do computador, examinando o backup mais recente de cada bloco e comparando o conteúdo e as informações com a origem. Esta comparação verifica se o backup mais recente dos blocos representa as informações correspondentes na origem. Se a imagem de backup de algum bloco não corresponder à origem, o agente do Arcserve UDP (Windows) atualizará (ressincronizará) o backup do bloco divergente.

Vantagem: uma imagem de backup muito pequena é gerada quando comparada ao backup completo porque somente os blocos alterados (blocos que não correspondam ao último backup) são armazenados em backup.

Desvantagem: o tempo do backup fica lento porque todos os blocos do disco de origem são comparados aos blocos do último backup.

Backup completo

Inicia um backup completo do computador inteiro ou dos volumes selecionados.

Observações:

- se você adicionar um novo volume à origem do backup, será feito um backup completo do volume recém-adicionado, independentemente do método de backup geral selecionado.
- Se nenhum nome de backup for especificado, por padrão, ele será automaticamente nomeado como Backup completo/incremental/de verificação personalizado.

5. Clique em **OK**.

   A caixa de diálogo Informações do andamento é exibida.

6. Aguarde até que a tarefa de backup seja concluída e clique em **OK**.

7. Para monitorar as tarefas de backup, navegue até **tarefas** > **Tarefas em andamento**.

   Aguarde até a conclusão da tarefa de backup.

   Observação: apenas uma tarefa pode ser executada em uma hora. Se você tentar iniciar manualmente uma tarefa de backup quando outra tarefa estiver em execução no mesmo momento, uma mensagem de alerta será exibida informando

sobre a existência de outra tarefa em execução e solicitando uma nova tentativa mais tarde.

O backup manual é realizado com êxito.

Observação: também é possível acionar um backup manual. Clique com o botão direito do mouse em um plano e selecione **Fazer backup agora** nas opções. Nesse caso, se o plano proteger objetos de recipiente do vSphere, o UDP acionará o backup de todas as VMs disponíveis no recipiente.

Verificar o plano

Para verificar o backup, confirme se você criou com êxito o plano de backup. Depois de verificar se o plano está criado com êxito, confirme se a tarefa de backup é executada conforme o programado. É possível verificar o status das tarefas de backup na guia tarefas.

Siga estas etapas: para verificar os planos

1. Clique na guia Recursos.
2. No painel à esquerda, navegue para Nós e clique em Todos os nós.

   Uma lista de todos os nós é exibida no painel central.
3. Verifique se os planos são mapeados com nós.

Siga estas etapas: para verificar tarefas de backup

1. Clique na guia tarefas.
2. No painel à esquerda, clique em Todas as tarefas.

   O status de cada tarefa é incluído no painel central.
3. Verifique se a tarefa de backup é concluída com êxito.

   A tarefa de backup é verificada.

Como criar um modo de espera virtual para o plano do AWS EC2

O modo de espera virtual converte os pontos de recuperação em formatos da máquina virtual na nuvem especificada e prepara um instantâneo para facilitar a recuperação de seus dados quando necessário. Este recurso oferece a capacidade com alta disponibilidade também e garante que a máquina virtual pode assumir o controle imediatamente quando o computador de origem falhar. A máquina virtual em modo de espera é criada pela conversão dos pontos de recuperação no formato da máquina virtual do Amazon AWS EC2.

Observação: a tarefa de modo de espera virtual é executada apenas se a tarefa de backup criar um instantâneo do ponto de recuperação válido. Se a tarefa de backup falhar, a tarefa no modo de espera virtual será ignorada.

O que fazer a seguir?

1. Verificar os pré-requisitos e as considerações
2. Criar um plano com uma tarefa de backup
3. Adicionar ao plano uma tarefa de modo de espera virtual para EC2
4. (Opcional) Executar a tarefa no modo de espera virtual para EC2 manualmente
5. Pause e retome a tarefa do modo de espera virtual
6. Verificar o plano
7. Encerrar os recursos do EC2

Verificar os pré-requisitos e as considerações

Verifique se concluiu os seguintes pré-requisitos:

- Efetue logon no Console.
- Instale o componente do servidor e crie repositórios de dados, caso deseje armazenar os dados de backup no servidor de ponto de recuperação.
- Você tem um ponto de recuperação válido para criar uma máquina no modo de espera virtual. Os pontos de recuperação podem ser provenientes de uma das seguintes tarefas:
  - Backup, Windows com base em agente
  - Backup, sem agente com base em host
  - Replicar
  - Replique de um servidor de ponto de recuperação remoto
- Fazer backup da máquina completa para ativar a tarefa Modo de espera virtual. Não é possível criar uma tarefa Modo de espera virtual se o backup não for um backup completo.
- Instale o volume do sistema no primeiro disco. Verifique se o volume do sistema e o volume de inicialização do computador de origem estão no mesmo disco.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.
- Defina a configuração do grupo de segurança no EC2 para abrir as portas relacionadas para acesso de entrada, incluindo TCP 8014 e TCP 4091.
- Verifique se a conta do AWS Amazon pode acessar o AWS S3 e o AWS EC2. O Arcserve UDP não fornece a conta.
- É necessário instalar o volume do sistema no primeiro disco. Verifique se o volume do sistema e o volume de inicialização do computador de origem estão no mesmo disco.
- Permissões de API AWS específicas são necessárias para que usuários do Amazon IAM obtenham controle e interação com as APIs AWS do VSB para EC2. Para obter detalhes, consulte Como configurar permissões granulares do IAM para usuários IAM com VSB para EC2.

Considerações:

- a tarefa Modo de espera virtual para EC2 NÃO oferece suporte à inicialização do computador de origem a partir do firmware UEFI devido à limitação do Amazon AWS EC2.
- O .NET framework 4.5 é necessário no computador de origem para se instalar o driver do Amazon PV para a tarefa Modo de espera virtual para EC2.
- O volume de inicialização e do sistema no nó de origem no plano VSB para EC2 deve estar no primeiro disco devido à limitação do AWS.
- A personalização da configuração de TCP/IP não pode ser aplicada à primeira interface de rede na instância do EC2 devido à limitação do AWS.
- A atribuição de endereço IP elástico só está disponível para a primeira interface de rede na instância do EC2.
- A personalização da configuração de TCP/IP só é aplicável para o cenário quando a VPN ou o acesso direto é configurado entre o site principal e a rede do AWS. Caso contrário, a personalização faz com que a instância do EC2 fique inacessível.
- Não é possível modificar a opção Ativar/desativar IP público da atribuição automática para os nós existentes no plano, e a atualização afeta somente os nós novos adicionados ao plano.
- Você deve instalar o PowerShell versão 3.0 ou superior na máquina de origem antes de configurar o VSB para EC2 para os seguintes tipos de instância:

  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 e z1d

Configurar permissões granulares do IAM para usuários do IAM com VSB para EC2

Esta seção explica as etapas e a diretiva de permissão da API necessárias para o Agente do Arcserve UDP instalado no proxy de nuvem VSB no Amazon EC2 Web Services. As permissões ajudam a executar as ações necessárias para a transferência de dados e o modo de espera virtual na nuvem do AWS EC2.

Usando o procedimento, você pode ajudar um usuário do Amazon IAM a obter controle e interação com a API do AWS. A diretiva de permissões não é aplicada somente ao usuário diretamente, mas também a uma função e grupo na interface de segurança do IAM no Amazon Web Services.

Siga estas etapas:

1. Efetue logon no Amazon Web Services como administrador.
2. Selecione Minhas credenciais de segurança, clique em **Usuários** no lado esquerdo e clique no botão**Criar novos usuários.**
3. Digite o nome de usuário desejado.

   Observação: verifique se a opção para **Gerar uma chave de acesso para cada usuário** está selecionada.
4. Clique no botão **Criar**.
5. Clique em **Fazer download das credenciais**.

   As credenciais contém a chave de acesso e o segredo necessários posteriormente no Console do UDP.
6. Na exibição de usuários, selecione o usuário na lista de usuários e, em seguida, clique na guia de permissões disponível na parte inferior.
7. Na opção de diretiva personalizada, crie uma diretiva personalizada inline para o usuário.
8. Digite um nome para a diretiva e cole o seguinte conteúdo no documento de diretiva.

```
{
"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",
        "Ação": [
            "s3:CreateBucket",
            "s3:DeleteBucket",
            "s3:DeleteObject",
            "s3:GetObject",
            "s3:ListBucket",
            "s3:PutObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "*"
        ]
    },
    {
        "Sid": "Stmt1477883239716",
        "Action": [
            "iam:GetUser"
        ],
        "Effect": "Allow",
```

```
        "Resource": [
            "*"
        ]
    }
    ]
    }
```

9. Clique em **Aplicar diretiva**.
10. No console do UDP, use a chave de acesso do usuário do IAM e a chave de acesso de segurança para criar o plano VSB para EC2.

Criar um plano com uma tarefa de backup

Um plano inclui tipos diferentes de tarefas que você deseja executar. Para criar a máquina no modo de espera virtual, crie um plano que inclui uma tarefa de backup e uma tarefa no modo de espera virtual. Uma tarefa de backup executa um backup dos nós de origem e armazena os dados para o destino especificado. Esses dados de backup são usados pelo recurso no modo de espera virtual, que os converte em um formato da máquina virtual.

É possível criar uma máquina no modo de espera virtual a partir de um backup do Windows com base em agente, backup com base em host sem agente. Também é possível criar uma máquina no modo de espera virtual a partir de dados que são replicados com a tarefa **Replicar**. O procedimento indicado a seguir é um exemplo para criar backup do Windows com base em agente.

Observações:

- para obter mais informações sobre o backup sem agente e com base em host, consulte Como criar um plano de backup da máquina virtual com base em host.
- Para obter mais informações sobre a replicação de dados de backup, consulte Como replicar dados entre repositórios de dados gerenciados de um console do UDP e gerenciados a partir de diferentes consoles do UDP.
- Modo de espera virtual para EC2 NÃO oferece suporte à inicialização do computador de origem do firmware UEFI devido às limitações do Amazon AWS EC2.

Siga estas etapas:

1. Clique na guia **Recursos** no Console.
2. No painel à esquerda, navegue para **Planos** e clique em **Todos os planos**.

   Se tiver criado os planos anteriores, esses planos serão exibidos no painel central.
3. No painel central, clique em **Adicionar um plano**.

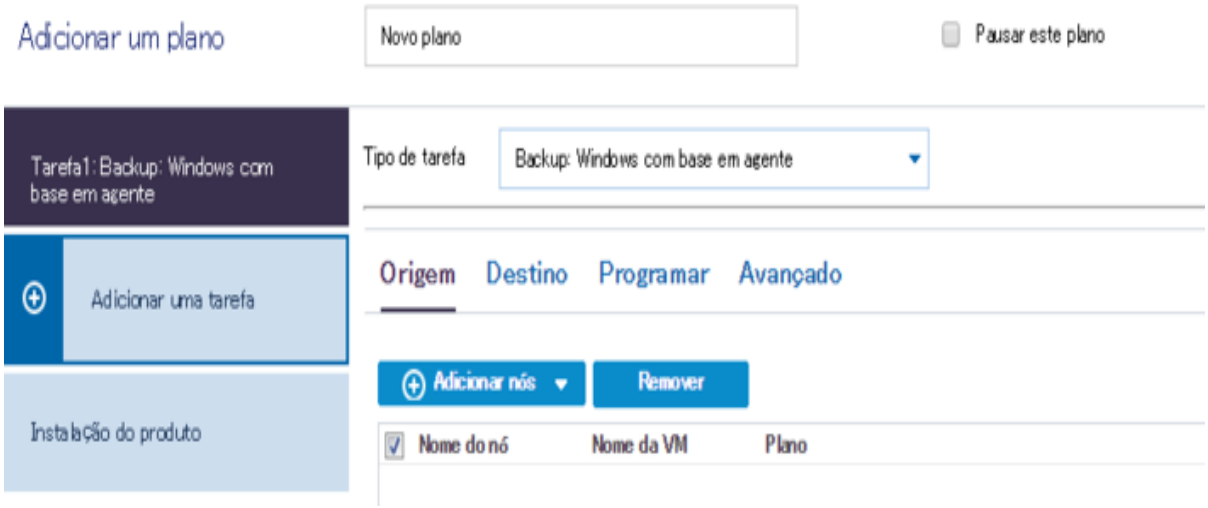
   Adicionar um plano é exibido.
4. Digite o nome do plano.
5. (Opcional) Marque a caixa de seleção **Pausar este plano**.

   O plano não será executado até que você desmarque a caixa de seleção para retomar o plano.

   Observação: se um plano for pausado, nenhuma tarefa em andamento será

pausada, mas todas as tarefas programadas correspondentes associadas a esse plano serão pausadas. No entanto, você pode executar uma tarefa manualmente. Por exemplo, você pode executar manualmente a tarefa de backup e a tarefa de replicação para um nó mesmo que o respectivo plano esteja pausado. Nesse caso, a tarefa seguinte da tarefa sob demanda (manual) não será executada. Por exemplo, há uma tarefa de replicação após uma tarefa de backup sob demanda, a tarefa de replicação não será executada para a tarefa de backup sob demanda. É necessário executar manualmente a tarefa de replicação. Quando você retomar o plano, as tarefas pendentes não são retomadas imediatamente. Depois de retomar o plano, as tarefas pendentes serão executadas no próximo horário programado.

6. Na lista suspensa **Tipo de tarefa**, selecione **Backup, Windows com base em agente**.



Agora, especifique os detalhes de Origem, Destino, Programação e Avançado.

Especificar a origem

A página Origem permite especificar os nós de origem que deseja proteger. É possível selecionar mais de um nó em um plano. Caso não tenha adicionado nós para o console, você pode adicionar nós ao criar ou modificar um plano da página de origem. Também é possível salvar um plano sem adicionar nenhum nó de origem. O plano é implantado somente após você adicionar nós de origem.

Siga estas etapas:

1. Na guia Origem, clique em **Adicionar**.
2. Selecione uma das seguintes opções:

   Selecionar os nós a serem protegidos no Arcserve UDP

   Abre a caixa de diálogo Selecionar nós para proteger no Arcserve UDP. Selecione os nós na lista exibida. Selecione esta opção se você já tiver adicionado os nós para o console.

   Adicionar nó do Windows

   A caixa de diálogo Adicionar nós a um plano é exibida. Selecione esta opção se você não tiver adicionado os nós e desejar adicionar manualmente os nós para proteger.

   Detectar os nós do Active Directory

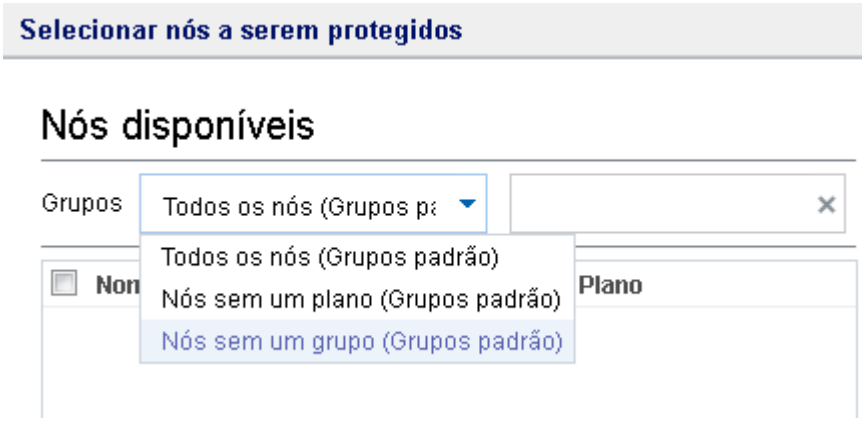
   Abra a caixa de diálogo Adicionar nós ao Console do Arcserve UDP. Selecione essa opção se desejar detectar e adicionar nós do Active Directory.
3. Se você selecionou a opção **Selecionar nós para proteger no Arcserve UDP**, na caixa de diálogo Selecionar nós para proteger, faça o seguinte:
   a. (Opcional) Selecione um filtro na lista suspensa Grupos para filtrar os nós. É possível digitar as palavras-chave para filtrar melhor seus nós.

      Os nós são exibidos na coluna Nós disponíveis.

   b. Selecione os nós na coluna Nós disponíveis e, em seguida, clique na seta simples à direita (>) ou na seta dupla à direita (>>) para mover os nós selecionados ou todos os nós, respectivamente, para a coluna Nós selecionados.

      Os nós são exibidos na coluna Nós selecionados.

   c. Clique em **OK** para fechar a caixa de diálogo.



4. Para escolher Tipo de proteção, selecione uma das seguintes opções:

   Fazer backup de todos os volumes

   Prepara um backup instantâneo de todos os volumes.

   Fazer backup dos volumes selecionados

   Prepara um instantâneo de backup do volume selecionado.

   A origem é especificada.

Especificar o destino

O destino é o local onde você armazena os dados de backup. É necessário, no mínimo, especificar o destino para salvar o plano.

Siga estas etapas:

1. Selecione um dos seguintes **Tipos de destino**:

   Disco local ou uma pasta compartilhada

   Especifica que o destino de backup é um destino local ou uma pasta compartilhada. Se selecionar essa opção, será possível salvar os dados como pontos de recuperação ou conjuntos de recuperação. As opções de pontos de recuperação e de conjuntos de recuperação estão disponíveis na guia **Programar**.

   Servidor de ponto de recuperação do Arcserve UDP

   Especifica que o destino de backup é um servidor do ponto de recuperação. Se selecionar essa opção, os dados serão armazenados como pontos de recuperação. Não é possível armazenar dados como conjuntos de dados de recuperação.

2. Se tiver selecionado **Servidor do ponto de recuperação do Arcserve UDP**, forneça os seguintes detalhes:
   a. Selecione um servidor do ponto de recuperação
   b. Selecione um repositório de dados. A lista exibe todos os repositórios de dados que são criados no servidor do ponto de recuperação especificado.
   c. Forneça uma senha da sessão.
   d. Confirme a senha da sessão.
3. Se tiver selecionado **Disco local ou pasta compartilhada**, forneça os seguintes detalhes:
   a. Forneça o caminho completo do destino local ou de rede. Para o destino de rede, especifique as credenciais com o acesso de gravação.
   b. Selecione o algoritmo de criptografia. Para obter mais informações, consulte Configurações de criptografia.
   c. Como opção, forneça uma senha de criptografia.
   d. Confirme a senha de criptografia.
   e. Selecione um tipo de compactação. para obter mais informações, consulte Tipo de compactação.

Observação: se armazenar os dados em um disco local ou em uma pasta compartilhada, não será possível replicar os dados para outro servidor do ponto de recuperação. A replicação é suportada apenas se armazenar os dados em um servidor do ponto de recuperação.

O destino é especificado.

Especificar a programação

A página Programar permite definir uma programação para o backup e para que as funções Mesclar e Acelerar sejam repetidas em intervalos específicos. Após definir uma programação, as tarefas são executadas automaticamente de acordo com a programação. É possível adicionar várias programações e fornecer configurações de retenção.

Uma Programação de backup se refere a programação regular que é repetida várias vezes ao dia, com base no número de horas ou de minutos selecionado. Além da programação regular, uma programação de backup também fornece opções para adicionar programações diária, semanal e mensal.

Observação: para obter mais informações sobre as configurações de retenção e programação, consulte Entendendo a programação avançada e retenção.

Siga estas etapas:

1. (Opcional) Selecione a opção para gerenciar os pontos de recuperação. Essa opção será visível somente se tiver selecionado o local ou a pasta compartilhada como o destino do backup.

   Reter por pontos de recuperação

   Os dados de backup são armazenadas como pontos de recuperação.

   Reter por conjuntos de recuperação

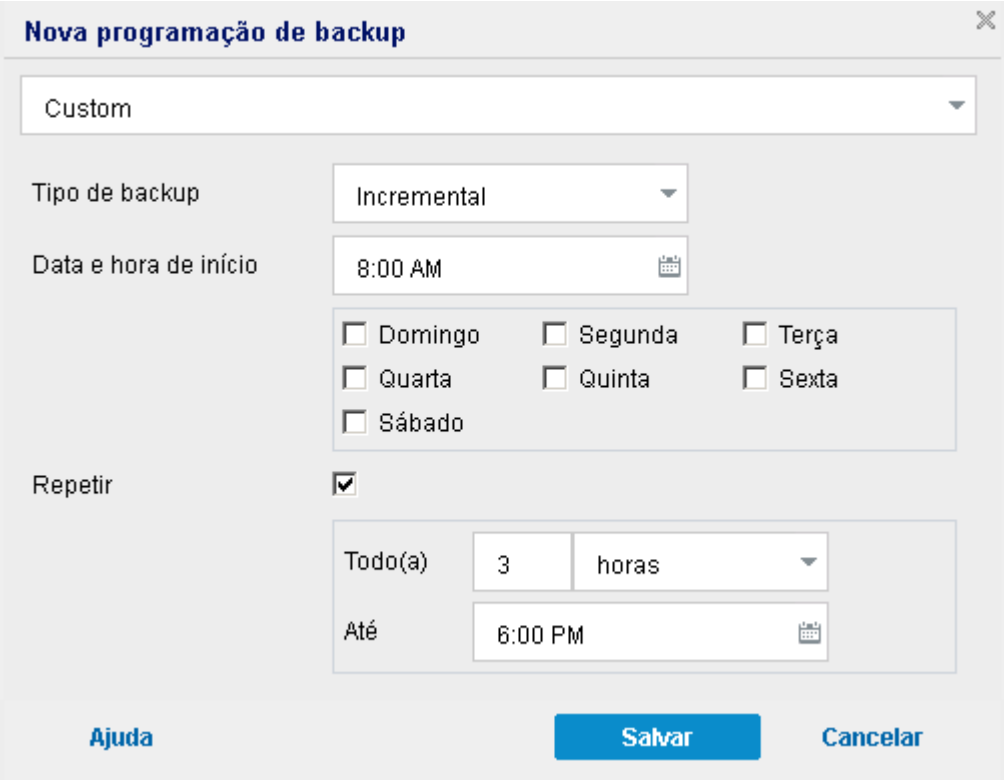
   Os dados de backup são armazenadas como conjuntos de recuperação.

2. Adicionar programações de backup, mesclagem e acelerador.

   Adicionar programação de backup

   a. Clique em **Adicionar** e selecione **Adicionar programação de backups**.

      A caixa de diálogo **Nova programação de backup** é aberta.



b. Selecione uma das seguintes opções:

Personalizado

Especifica a programação de backup que se repete várias vezes por dia.

Diário

Especifica a programação de backup que ocorre uma vez por dia. Por padrão, todos os dias da semana estão selecionados para o backup diário. Se não desejar executar a tarefa de backup em um dia específico, desmarque a caixa de seleção correspondente àquele dia da semana.

Semanal

Especifica a programação de backup que ocorre uma vez por semana.

Mensal

Especifica a programação de backup que ocorre uma vez por mês.

c. Selecione o tipo de backup.

Completo

Especifica a programação de backups para backups completos. Conforme programado, o Arcserve UDP executa um backup completo de todos os blocos usados do computador de origem. Um backup completo em geral, consome tempo, dependendo do tamanho do backup.

Verificar

Especifica a programação de backups para backups de verificação.

A Arcserve UDP verifica se os dados protegidos são válidos e concluídos, executando uma verificação de confiabilidade da imagem de backup armazenada na origem do backup. Se necessário, a imagem será sincronizada novamente. Um backup de verificação examinará o backup mais recente de cada bloco e irá comparar o conteúdo e as informações com a origem. Esta comparação verifica se o backup mais recente dos blocos representa as informações correspondentes na origem. Se a imagem de backup de qualquer bloco não corresponder à origem (possivelmente devido a alterações no sistema desde o último backup), o Arcserve UDP atualizará (fará nova sincronização) o backup do bloco que não corresponder. Também é possível usar um backup de verificação (muito raramente) para obter a garantia de backup completo sem usar o espaço necessário para um backup completo.

Vantagens: produz uma pequena imagem de backup quando comparado ao backup completo, pois somente os blocos alterados (blocos que não coincidem com o último backup) são armazenados em backup.

Desvantagens: o tempo de backup é longo, pois todos os blocos de origem são comparados aos blocos do último backup.

Incremental

Especifica a programação de backups para backups incrementais.

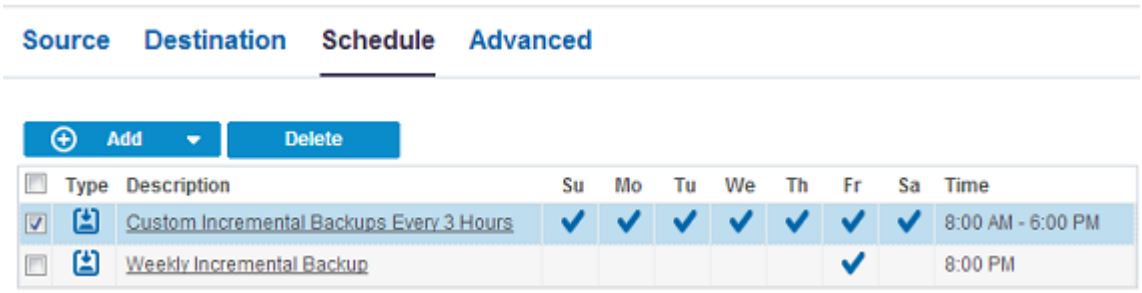
Conforme programado, o Arcserve UDP faz backup incremental apenas dos blocos que foram alterados desde o último backup realizado com êxito. As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a executar um backup.

d. Especifique a hora de início do backup.

e. (Opcional) Marque a caixa de seleção de **Repetição** e especifique a programação a ser repetida.

f. Clique em **Salvar**.

A programação de backup é especificada e exibida na página de **Programação**.



Adicionar Programação de mesclagem

a. Clique em Adicionar e selecione Adicionar programação de mesclagem.

   A caixa de diálogo **Adicionar nova programação de mesclagem** é aberta.

b. Especifique a hora de início para iniciar a tarefa de mesclagem.

c. Especificar **Até** para especificar uma hora de término para a tarefa de mesclagem.

d. Clique em **Salvar**.

   A programação de mesclagem é especificada e exibida na página **Programar**.

Adicionar programação de acelerador

a. Clique em **Adicionar** e selecione **Adicionar programação de acelerador.**

   A caixa de diálogo Adicionar nova programação do acelerador é aberta.

b. Especifique o limite de taxa de transferência em MB por minuto.

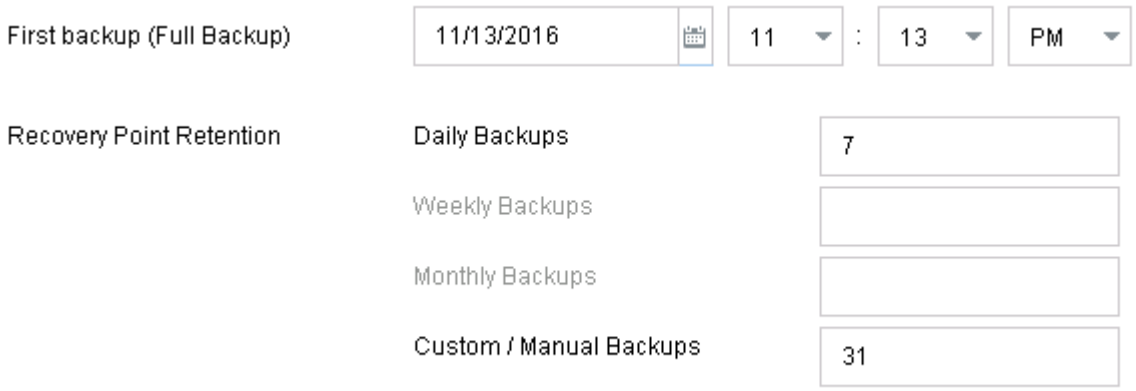
c. Especifique a hora de início para iniciar a tarefa de taxa de transferência de backup.

d. Especifique **Até** para especificar um horário de término para a tarefa de taxa de transferência.

e. Clique em **Salvar**.

   A Programação de acelerador é especificada e exibida na página **Programar**.

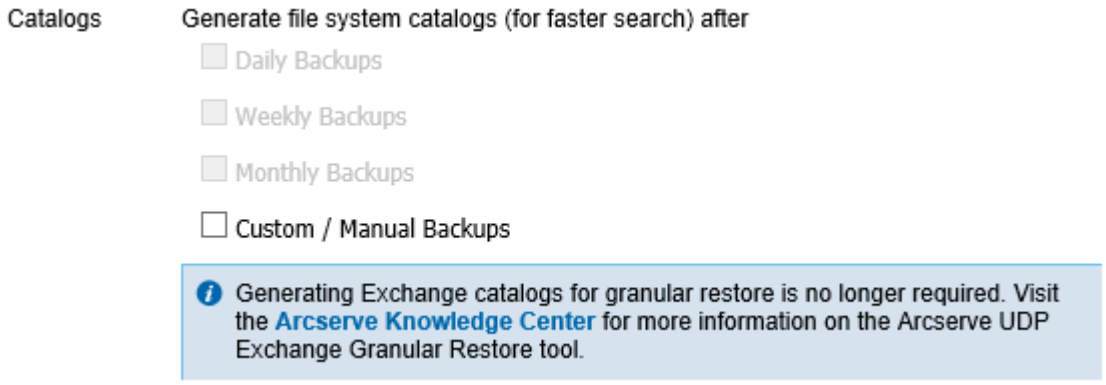
3. Especifique a hora de início do backup programado.



4. Especifique as configurações de retenção de pontos de recuperação para programação diária, semanal e mensal.

   Essas opções serão ativadas se tiver adicionado a programação de backup correspondente. Se você modificar as configurações de retenção desta página, as alterações serão refletidas na caixa de diálogo Programação de backup.

5. Especifique os detalhes de catálogo.



   Os catálogos permitem gerar o catálogo do sistema de arquivos. O catálogo do sistema de arquivos é necessário para agilizar e melhorar a pesquisa. Se marcar as caixas de seleção do catálogo, os catálogos serão ativados de acordo com o tipo de backup que você especificou. Desmarque a caixa de seleção para desativar a geração do catálogo.

   A programação é especificada.

Noções básicas sobre a programação avançada e retenção

A opção de programação permite especificar uma programação personalizada, uma programação diária/semanal/mensal ou ambas. Na programação personalizada, é possível configurar a programação de backups para cada dia da semana ou adicionar até quatro programações de backup em cada dia. É possível escolher um dia específico da semana e criar uma janela para definir quando executar o backup e em que frequência.

Programação	Tarefa com suporte	Comentários
Backup	Tarefa de backup	Definir janelas de tempo para a execução de tarefas de backup.
Limitação de backup	Tarefa de backup	Definir janelas de tempo para controlar a velocidade de backup.
Mesclar	Tarefa de mesclagem	Definir quando executar tarefas de mesclagem.
Programação diária	Tarefa de backup	Definir quando executar tarefas do backup diário.
Programação semanal	Tarefa de backup	Definir quando executar tarefas do backup semanal.
Programação mensal	Tarefa de backup	Definir quando executar tarefas do backup mensal.

Também é possível especificar as configurações de retenção para os pontos de recuperação.

Observação: as configurações de retenção devem ser definidas em cada plano para controlar como os dados dos nós atribuídos a esse plano são retidos no repositório de dados de destino.

As programações para backups diários/semanais/mensais são independentes para a programação personalizada e umas das outras. É possível configurar para executar somente o backup diário, semanal ou mensal, sem configurar a Programação personalizada.

Programação de tarefas de backup

É possível adicionar quatro janelas de tempo por dia na programação do backup. Uma janela de tempo é válida das 00:00 às 23:59. Não é possível especificar uma janela de tempo das 18:00 às 6:00. Nesses casos, você deve especificar manualmente duas janelas de tempo diferentes.

Para cada janela de tempo, a hora de início é inclusiva e a hora de término é exclusiva. Por exemplo, você configurou para executar o backup incremental em intervalos de uma hora entre as 6:00 e as 9:00. O backup será iniciado às 6:00. Isso significa que o backup será executado às 6h00, 7h00 e 8h00, mas NÃO às 9h00.

Observação: se você deseja executar a tarefa de backup várias vezes até o fim do dia, defina a programação para até 0h00. Por exemplo, para executar a tarefa de backup a cada 15 minutos o dia inteiro, defina a programação como das 0h00 às 00h00, a cada 15 minutos.

Programação do acelerador de backup

A programação de aceleração do backup permite controlar a velocidade da taxa de transferência de backup o que, por sua vez, controla o uso de recursos (E/S de disco, CPU, largura de banda de rede) do servidor cujo backup está sendo feito. Isso é útil quando se não quiser afetar o desempenho do servidor durante o horário comercial. É possível adicionar quatro janelas de tempo por dia na sua programação de aceleração do backup. Para cada janela de tempo, é possível especificar um valor, em MB por minuto. Esse valor será usado para controlar a taxa de transferência do backup. Os valores válidos variam entre 1 MB/minutos a 99999 MB/minutos.

Se uma tarefa de backup estende seu tempo especificado, o limite de aceleração será ajustado de acordo com o tempo especificado. Por exemplo, você definiu o limite de aceleração de backup como 500 MB/minuto das 8:00 às 20:00 e 2500 MB/minuto das 20:00 às 22:00. Se uma tarefa de backup iniciar às 19h00 e for executada durante três horas, das 19h00 às 20h00 o limite de aceleração será de 500 MB/minuto e das 20h00 às 22h00, o limite de aceleração será 2500 MB/minuto.

Se não definir nenhuma programação do backup e programação da taxa de transferência do backup, o backup será executado o mais rápido possível.

Mesclar a programação

Permite mesclar pontos de recuperação com base na programação fornecida.

Considere os seguintes pontos para a tarefa de mesclagem:

- A qualquer momento apenas uma tarefa de mesclagem pode ser executada para um nó.
- Se uma tarefa de mesclagem iniciar, ela precisará ser concluída antes que a próxima tarefa de mesclagem seja iniciada. Isso significa que, se um ou mais conjuntos de pontos de recuperação forem mesclados, não será possível adicionar o

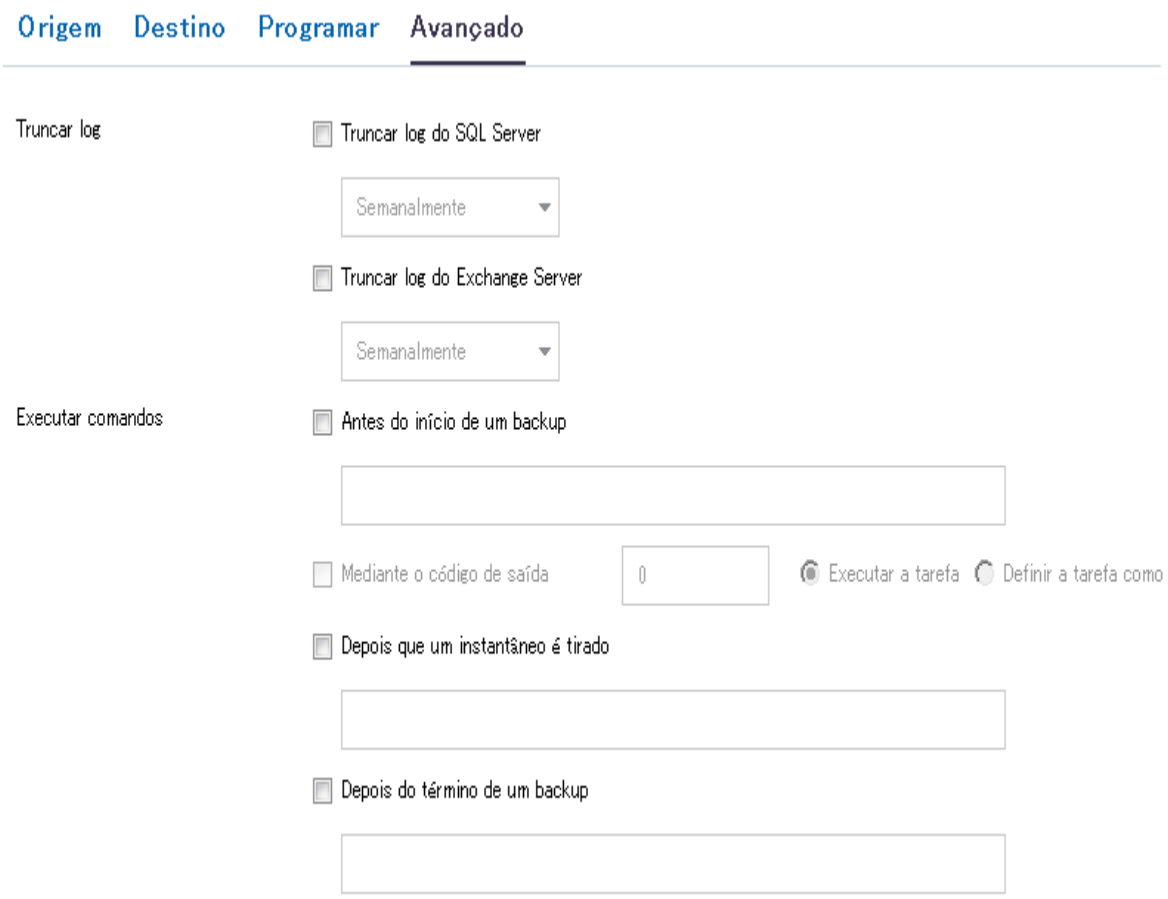
novo ponto de recuperação a este processo de mesclagem, até que o processo de mesclagem do conjunto atual de ponto de recuperação seja concluído.

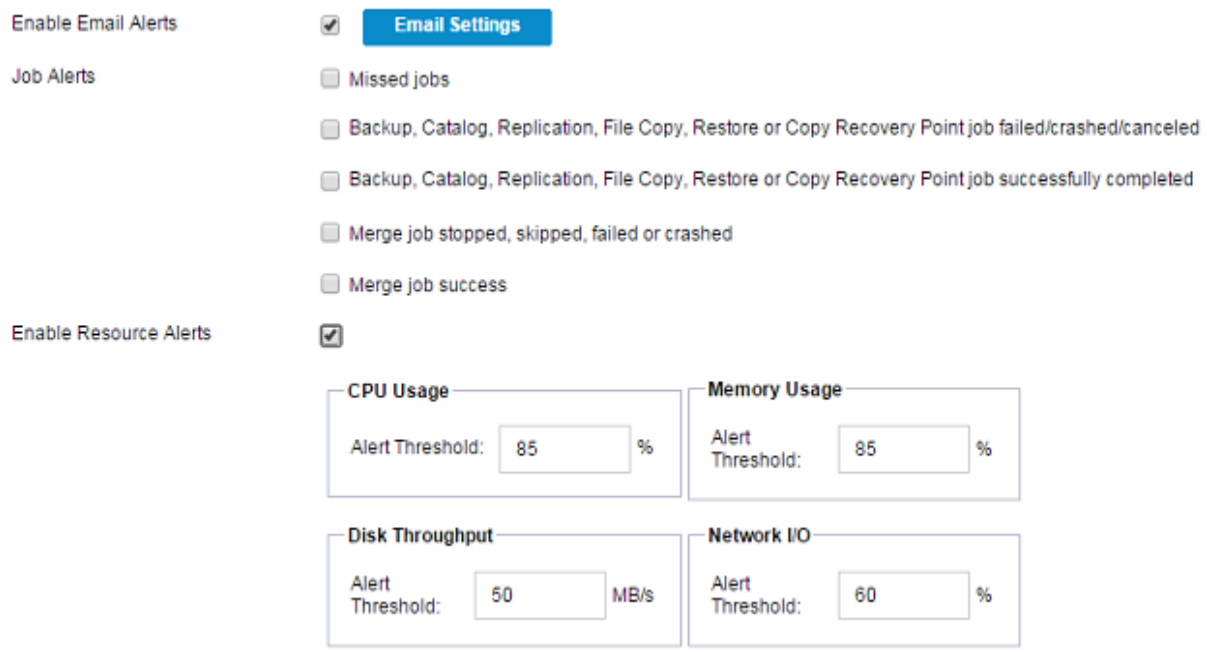
- Se uma tarefa de mesclagem estiver processando mais de um conjunto de pontos de recuperação (por exemplo, conjunto [1~4], conjunto [5~11] e conjunto [12~14]; são três conjuntos) o servidor de ponto de recuperação processará esses conjuntos, um por um.
- Se uma tarefa de mesclagem é retomada após um intervalo, a tarefa detectará em que ponto ela foi pausada e continuará a mesclagem a partir do ponto de pausa.

Especificar as configurações avançadas

A guia **Avançado** permite especificar algumas configurações avançadas para a tarefa de backup. As configurações avançadas incluem fornecer configurações de log de truncamento, a localização de quaisquer scripts e as configurações de email.

A imagem a seguir mostra a guia Avançado:





Siga estas etapas:

1. Especifique os seguintes detalhes.

Truncar log

Permite especificar a programação para truncar logs para o SQL Server e o Exchange Server. É possível especificar a programação como **Diária**, **Semanal** ou **Mensal**.

Nome de usuário

Permite especificar o usuário que possui autorização para executar um script.

Senha

Permite especificar a senha do usuário que está autorizado a executar o script.

Executar um comando antes do início do backup

Permite a execução de um script antes de iniciar a tarefa de backup. Especifique o caminho onde o script está armazenado. Clique em **No código de saída** e especifique o código de saída para **Executar tarefa** ou **Tarefa com falha**. **Executar a tarefa** indica que a tarefa de backup continuará quando o script retornar o código de saída. **Tarefa com falha** indica que a tarefa de backup será interrompida quando o script retornar o código de saída.

Executar um comando após a criação de um instantâneo

Permite executar um script depois que o backup do instantâneo for gerado. Especifique o caminho onde o script está armazenado.

Executar um comando após a conclusão do backup

Permite executar um script depois que a tarefa de backup foi concluída. Especifique o caminho onde o script está armazenado.

Ativar alertas por email

Permite ativar alertas por email. É possível especificar configurações de email e os tipos de alertas que você deseja receber por email. Ao selecionar esta opção, as seguintes opções serão ativadas para a seleção.

Configurações de email

Permite configurar as definições de email. Clique em **Configurações de email** e configure o servidor de email e os detalhes do servidor proxy.

Alertas de tarefa

Permite que você selecione os tipos de emails da tarefa que deseja receber.

Ativar os alertas de recurso

Permite que você especifique um limite de uso da CPU, o uso da memória, a taxa de transferência de disco, E/S de rede. Você pode fornecer o valor em porcentagem. Você receberá um email quando o valor exceder o Limite de alerta.

2. Clique em **Salvar**.

Observação: quando você seleciona um nó como origem de backup ou proxy de backup, o Arcserve UDP verifica se o agente está instalado no nó e se é a versão mais recente. Em seguida, o Arcserve UDP exibe uma caixa de diálogo de verificação que lista todos os nós que possuem uma versão antiga do agente ou que não tem o agente instalado. Para instalar/atualizar o agente nesses nós, selecione o método de instalação e clique em Salvar.

As alterações são salvas e uma marca de seleção verde é exibida ao lado do nome da tarefa. A página do plano é fechada.

Observação: se precisar adicionar outra tarefa, deverá selecionar o plano na guia **Recursos** e modificar o plano. Para modificar o plano, clique no plano do painel central. O plano é exibido e será possível modificá-lo.

O plano de backup é criado e implantado automaticamente para o nó de origem. O backup é executado de acordo com a programação que você configurou na guia **Programar.** Também é possível fazer backup manual quando desejado.

Adicionar ao plano uma tarefa de modo de espera virtual para EC2

Criar uma tarefa no modo de espera virtual para EC2 para que os dados de backup sejam convertidos em um formato da máquina virtual e a máquina virtual seja criada.

Observações:

- O modo de espera virtual para EC2 não oferece suporte ao início automático da máquina virtual.
- se você pausar o plano, a tarefa Modo de espera virtual não será iniciada. Ao se retomar o plano novamente, a tarefa do modo de espera virtual não é retomada automaticamente. É necessário executar manualmente outra tarefa de backup para iniciar a tarefa do modo de espera virtual. Além disso, se o plano for pausado, a opção Pausar/Retomar o modo de espera virtual não estará disponível. Se não desejar que a máquina virtual inicie automaticamente após o plano ser pausado, pause manualmente o sinal de monitoramento dos nós.

Siga estas etapas:

1. Clique em **Adicionar uma tarefa** no painel esquerdo.

   Uma nova tarefa será adicionada ao painel esquerdo.

2. No menu suspenso, selecione **Tipo de tarefa** do **Modo de espera virtual.**

   A tarefa em Modo de espera virtual é adicionada.

3. Na guia **Origem**, selecione uma origem para a tarefa do modo de espera virtual.
4. Clique na guia **Servidor de Virtualização**.
5. Selecione EC2 como o tipo de virtualização e digite os detalhes.

   Tipo de virtualização – EC2

   Nome da conta

   Selecione a conta AWS Amazon existente para acessar o AWS EC2. Também é possível adicionar uma nova conta clicando em **Adicionar**. Para obter mais informações, consulte Adicionar uma conta de nuvem para Amazon EC2.

   Região EC2

   Selecione a região do EC2 na qual se encontra o proxy de nuvem. O Arcserve UDP oferece suporte a todas as regiões globais do EC2 e a região da China do EC2.

Observação: a conta especificada deve ser uma conta administrativa ou uma conta com privilégios administrativos no EC2.

Proxy na nuvem VSB

Especifique uma instância do EC2 na região selecionada como o proxy de nuvem.

Observação: a instância do EC2 deve ter o agente do Arcserve UDP instalado.

Nome de usuário e senha

Especifica as credenciais para se efetuar logon no proxy de nuvem do VSB.

Protocolo

Especifique HTTP ou HTTPS como o protocolo que você deseja usar para comunicação entre o Agente do Arcserve Unified Data Protection de origem e o proxy de nuvem do VSB.

Porta

Especifique a porta que deseja usar para a transferência de dados entre o servidor de origem e o proxy de nuvem de VSB.

Observação: como o proxy de nuvem é usado para a transferência de dados, as portas relacionadas devem ser ativadas para o acesso à entrada no grupo de segurança do AWS EC2, incluindo TCP 8014 e 4091.

6. Clique na guia **Máquina Virtual** e digite os detalhes da configuração Básica, da configuração de Armazenamento na nuvem e da configuração de Redes.

   Amazon AWS EC2

   Aplique as seguintes opções de máquina virtual ao Amazon AWS EC2:

   Prefixo do nome da VM

   Especifique o prefixo que deseja adicionar ao nome de exibição da máquina virtual no AWS EC2.

   Valor padrão: UDPVM_

   Instantâneos do ponto de recuperação

   Especifique o número de instantâneos dos pontos de recuperação (pontos de recuperação) para a máquina no modo de espera virtual. O número máximo de instantâneos dos pontos de recuperação é 29 para o AWS EC2.

   Combine todas as sessões não convertidas em um único instantâneo do ponto de recuperação

Especifique se deseja combinar todas as sessões não convertidas em um único instantâneo do ponto de recuperação quando a próxima tarefa do VSB programada ocorrer.

Padrão: Selecionado

Tipo de instância

O Amazon EC2 fornece uma ampla seleção de tipos de instância otimizados de acordo com diferentes usos. As instâncias são servidores virtuais que podem executar aplicativos. Elas têm combinações de CPU, memória, armazenamento e capacidade de rede variáveis e fornecem a flexibilidade para escolher o conjunto adequado de recursos para os aplicativos. Para obter mais informações sobre os tipos de instância, e como elas atendem às suas necessidades de computação, veja este link.

Tipos de volume EBS

Os volumes de Finalidade Geral (SSD) podem disparar para 3000 IOPS e fornecer uma linha de base consistente de 3 IOPS/GiB. Os volumes de IOPs (SSD) provisionados podem transmitir até 20000 IOPS e são os melhores para instâncias otimizadas a EBS. Os volumes magnéticos, anteriormente conhecidos como volumes padrão, enviam 100 IOPS em média e podem disparar para centenas de IOPS. Para obter mais informações sobre os tipos de volume de EBS, veja este link.

Rede

Permite definir o VPC, as sub-redes, as NICs e o grupo de segurança para a máquina virtual no modo de espera virtual no AWS EC2.

Observação: quando o IP público de atribuição automática está ativado, devido à limitação do AWS EC2, apenas uma NIC é mapeada para o AWS EC2, e as outras são descartadas.

O mesmo número de adaptadores de rede como origem no último backup

Selecione essa opção para definir como mapear a NIC virtual para a rede no EC2. Especifique essa opção quando a máquina virtual contiver NICs virtuais e uma rede virtual.

Observação: essas configurações só podem ser definidas quando o IP público de atribuição automática está desativado.

7. Clique em **Salvar**.

As alterações são salvas e a tarefa no modo de espera virtual é automaticamente implantada no servidor do modo de espera virtual.

Você criou com êxito e implantou o plano no modo de espera virtual.

Adicionar a transferência de dados à programação de limitação na nuvem

A programação do acelerador permite controlar a velocidade da taxa de transferência de dados para a nuvem o que, por sua vez, controla o uso de recursos (largura de banda de rede) do servidor que está sendo transferido para a nuvem. Isso é útil quando se não quiser afetar o desempenho do servidor durante o horário comercial. É possível adicionar quatro janelas de tempo por dia à programação de limitação da transferência de dados para a nuvem. Para cada janela de tempo, é possível especificar um valor, em Mbps/Kbps por minuto. Esse valor será usado para controlar a taxa de transferência para a nuvem. Valores válidos variam entre 1 Mbps/Kbps a 99999 Mbps/Kbps.

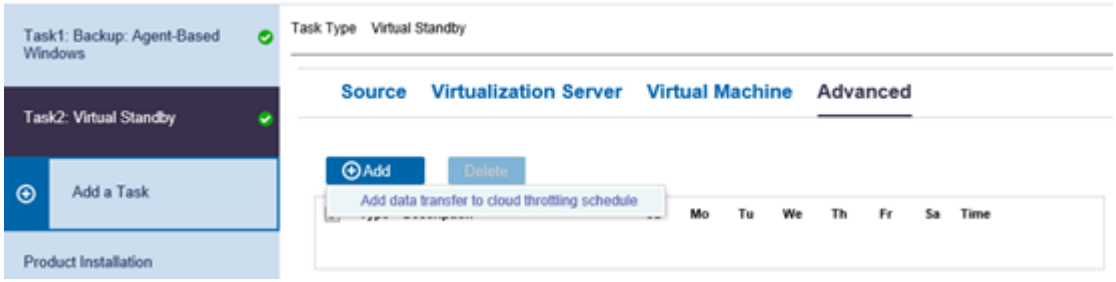
Se a tarefa de transferência de dados estender seu tempo especificado, o limite do acelerador será ajustado de acordo com a janela de tempo especificada. Por exemplo, você definiu o limite do acelerador da transferência de dados como 500 Mbps das 8:00 às 20:00 e 2500 Mbps das 20:00 às 22:00. Se uma tarefa de transferência de dados iniciar às 19h00 e for executada durante três horas, das 19h00 às 20h00 o limite do acelerador será de 500 Mbps e das 20h00 às 22h00, o limite do acelerador será 2500 Mbps.

Se houver mais de um nó de origem na tarefa de backup com o modo de espera virtual na nuvem, eles dividirão o limite do acelerador igualmente. Por exemplo, você definiu o limite do acelerador da transferência de dados como 500 Mbps e há dois nós de origem no plano. Quando eles transferirem dados para a nuvem ao mesmo tempo, o limite do acelerador será 250 Mbps para cada nó. Depois de concluída a tarefa de transferência de dados de um nó, o limite do acelerador do outro nó em execução será alterado para 500 Mbps.

Se não for definida nenhuma programação de limitação, a tarefa de transferência de dados para a nuvem será executada o mais rápido possível.

Siga estas etapas:

1. Clique em Adicionar e selecione Adicionar a transferência de dados à programação de limitação na nuvem.



A caixa de diálogo Adicionar nova programação do acelerador é aberta.

2. Especifique o limite de taxa de transferência em Mbps/Kbps.

   A página Configuração de rede da máquina virtual no modo de espera – <nome do nó> é exibida.

3. Especifique a hora de início para iniciar a tarefa de taxa de transferência de backup.
4. Especifique Até para especificar um horário de término para a tarefa de taxa de transferência.
5. Clique em Salvar.

   A Programação de acelerador é especificada e exibida na página Programar.

Configurar a rede da VM no modo de espera

É possível acionar a VM no modo de espera no AWS EC2 com configurações de rede personalizadas. É possível definir as seguintes configurações de rede na VM no modo de espera:

- Especifique a rede virtual e a NIC (Network Interface Card – Placa de Interface de Rede), e as configurações TCP/IP de cada adaptador de rede na guia **Configurações do adaptador de rede**.
- Atualize os servidores DNS para redirecionar clientes do computador de origem para as máquinas virtuais no modo de espera virtual com base nas configurações TCP/IP na guia **Configurações de atualização de DNS**.

Siga estas etapas:

1. Na guia **Recursos**, navegue até o grupo de nós do **Modo de espera virtual**.

   Os nós no Modo de espera virtual são exibidos no painel central.

2. No painel central, selecione o nó e clique em **Configuração de rede da máquina virtual no modo de espera**.

   A página Configuração de rede da máquina virtual no modo de espera – <nome do nó> é exibida.

3. Na guia **Configurações do adaptador de rede**, selecione a rede virtual na lista **Máquina virtual em modo de espera – Rede virtual**.
4. Selecione a subrede na lista suspensa.
5. Selecione o endereço IP elástico na lista **IP Elástico**.
6. Selecione **Personalizar as configurações de TCP/IP**.
7. Clique no botão **Adicionar endereço** e adicione **endereços IP**, **Endereços de gateway**, **Endereços DNS** e **endereços WINS**.

   Observação: se você adicionar **endereços DNS**, deverá configurar os servidores DNS na guia **Configurações de atualização do DNS**.

8. Clique em **Salvar**.

   A página Configuração de rede da máquina virtual no modo de espera – <nome do nó> é fechada.

   É configurada a rede da máquina virtual no modo de espera.

(Opcional) Executar a tarefa no modo de espera virtual para EC2 manualmente

Para executar manualmente uma tarefa no modo de espera virtual, você deverá primeiro executar um backup manual. A tarefa Modo de espera virtual para EC2 está associada a uma tarefa de backup. Se um plano incluir uma tarefa de backup e uma tarefa Modo de espera virtual para EC2, quando você executar a tarefa de backup manualmente, a tarefa do modo de espera virtual executará automaticamente após a conclusão da tarefa de backup.

Siga estas etapas:

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.

   Caso você tenha adicionado algum planos, esse plano será exibido no painel central.
3. Selecione os nós que deseja fazer backup e que tenha um plano atribuído a ele.
4. No painel central, clique em **Ações**, **Fazer backup agora**.

   A caixa de diálogo **Fazer backup agora** é exibida.
5. Selecione o tipo de backup e forneça um nome para a tarefa de backup.
6. Clique em **OK**.

   A tarefa de backup é executada.

   A tarefa Modo de espera virtual para EC2 é executada imediatamente após a tarefa de backup ser concluída.

   A tarefa no modo de espera virtual para EC2 é executada manualmente.

Pausar e retomar a tarefa do modo de espera virtual

A conversão virtual é o processo em que o recurso do modo de espera virtual converte pontos de recuperação do Arcserve Unified Data Protection de nós de origem em formatos da máquina virtual, denominados instantâneos do ponto de recuperação. No caso de um servidor de origem falhar, o recurso de Modo de espera virtual usa os instantâneos de pontos de recuperação para ligar uma máquina virtual no nó de origem.

Como prática recomendada, permita que o processo de conversão virtual opere continuamente. No entanto, se deseja pausar o processo de conversão virtual nos servidores no modo de espera virtual local ou remoto temporariamente, pode fazê-lo no Console. Depois de corrigir os problemas no nó de origem, você pode continuar o processo de conversão virtual.

Quando você faz uma pausa nas tarefas do Modo de espera virtual (tarefas de conversão), a operação de pausa não pausa a tarefa de conversão que está em andamento no momento. A operação de pausa aplica-se somente à tarefa que está aguardando para ser executada no final da próxima tarefa de backup. Como resultado, a próxima tarefa de conversão não é iniciada até que você retome explicitamente a tarefa de conversão (pausada).

Se continuar o modo de espera virtual dos nós e se houver várias sessões de backup sem instantâneo do ponto de recuperação, será exibida uma caixa de diálogo para selecionar a opção de cópia inteligente. Se clicar em Sim, a tarefa em modo de espera virtual poderá converter a sessão combinada em um único instantâneo do ponto de recuperação. Se clicar em Não, a tarefa em modo de espera virtual poderá converter cada sessão individualmente

Observação: como alternativa, é possível pausar e retomar tarefas do Modo de espera virtual diretamente nos nós. Para obter mais informações, consulte o tópico Pausar e retomar tarefas do Virtual Standby nos nós.

Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection.
2. Clique na guia **Recursos**.
3. No painel à esquerda, vá até o **Modo de espera virtual** e clique em **Todos os nós**.

   Se você tiver adicionado alguns nós, os nós serão exibidos no painel central.
4. Selecione o nó que deseja pausar ou retomar.

5. No painel central, clique em **Ações**, **Modo de espera virtual**, **Pausar** ou **Retomar**.

   A função do modo de espera virtual para o nó selecionado é pausada ou retomada.

Verificar o plano

Para verificar seu recurso no modo de espera virtual, verifique se você criou com êxito o plano no modo de espera virtual. Depois de verificar se o plano está criado com êxito, confirme se a tarefa de backup está executando conforme o programado. Depois que a tarefa de backup for concluída com êxito, a tarefa em modo de espera virtual será executada. É possível verificar o status da tarefa de backup e da tarefa no modo de espera virtual na guia **tarefas**.

Siga estas etapas para verificar os planos:

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.

   Uma lista de todos os nós é exibida no painel central.
3. Verifique se os planos são mapeados com nós.

Siga estas etapas para verificar as tarefas no modo de espera virtual:

1. Clique na guia **tarefas**.
2. No painel à esquerda, clique em **Todas as tarefas**.

   O status de cada tarefa é incluído no painel central.
3. Verifique se a tarefa de backup e a tarefa no modo de espera virtual foi bem-sucedida.

   O plano para modo de espera virtual é verificado com êxito.

   O computador no modo de espera virtual é criado.

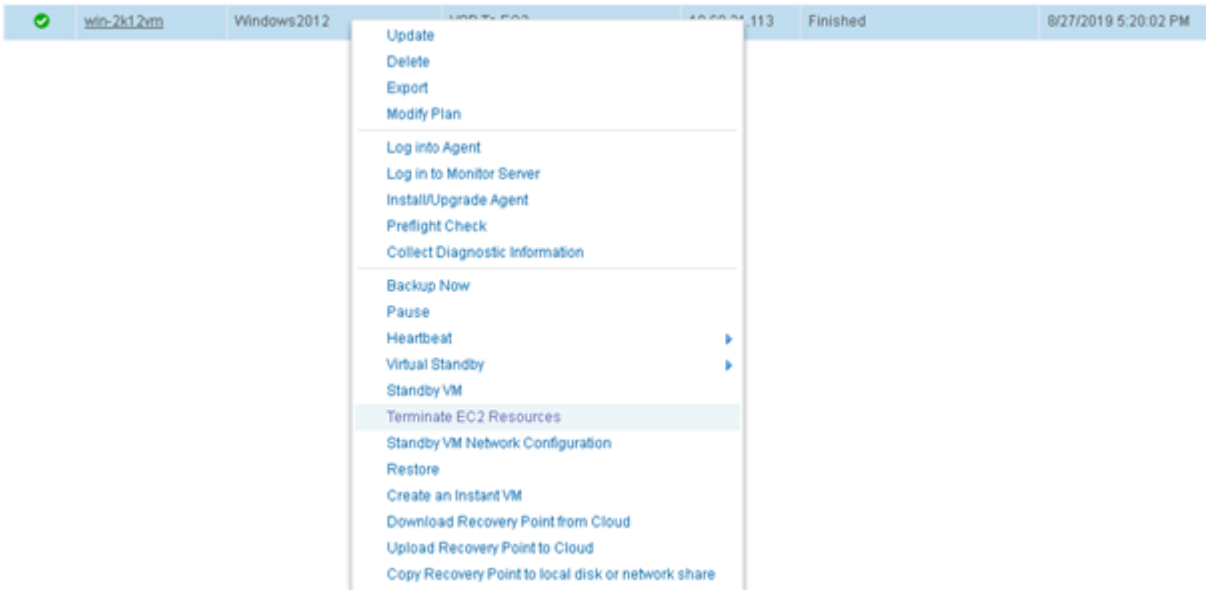
Encerrar os recursos do EC2

Siga estas etapas:

1. Clique na guia **Recursos**.
2. No painel esquerdo, navegue para **Nós** e clique em **Todos os nós**.

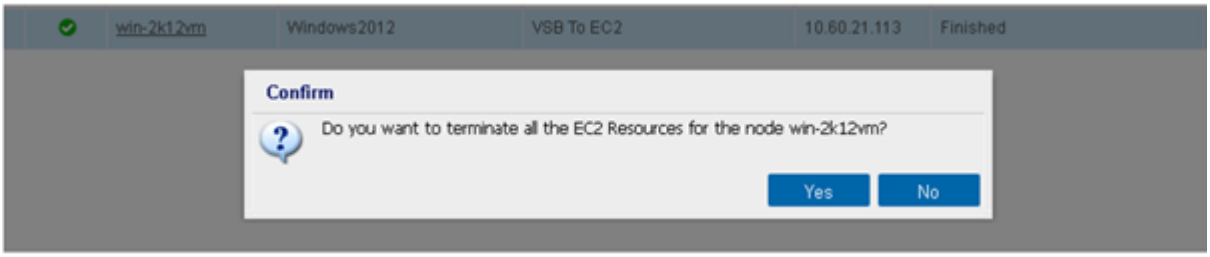
   Todos os nós são exibidos no painel central.
3. Clique com o botão direito do mouse em um nó e selecione Encerrar os recursos do EC2.

   A caixa de diálogo Confirmação é exibida.



4. Clique em **Sim** para limpar os recursos da nuvem do AWS que são gerados a partir do modo de espera virtual para a tarefa do EC2. Clique em **Não** para interromper o processo de encerramento.

   Observação: se um nó não apresentar nenhuma tarefa bem-sucedida do VSB para o EC2, esse nó não terá a opção Encerrar os recursos do EC2.



Como criar um modo de espera virtual para o plano do Microsoft Azure

O modo de espera virtual converte os pontos de recuperação em formatos da máquina virtual e prepara um instantâneo para facilitar a recuperação de seus dados quando necessário. Este recurso oferece a capacidade com alta disponibilidade também e garante que a máquina virtual pode assumir o controle imediatamente quando o computador de origem falhar. A máquina virtual em modo de espera é criada pela conversão dos pontos de recuperação no formato da máquina virtual da Microsoft.

Observação: a tarefa de modo de espera virtual é executada apenas se a tarefa de backup criar um instantâneo do ponto de recuperação válido. Se a tarefa de backup falhar, a tarefa no modo de espera virtual será ignorada.

O que fazer a seguir?

1. Verificar os pré-requisitos e as considerações
2. Criar um plano com uma tarefa de backup
3. Adicionar um modo de espera virtual à tarefa do Azure
4. (Opcional) Execute a tarefa no modo de espera virtual manualmente
5. Pause e retome o sinal de monitoramento
6. Pause e retome a tarefa do modo de espera virtual
7. Verificar o plano

Verificar os pré-requisitos e as considerações

Verifique se concluiu os seguintes pré-requisitos:

- Efetue logon no Console.
- Instale o componente do servidor e crie repositórios de dados, caso deseje armazenar os dados de backup no servidor do ponto de recuperação.
- Você tem um ponto de recuperação válido para criar uma máquina no modo de espera virtual. Os pontos de recuperação podem ser provenientes de uma das seguintes tarefas:
  - Backup, Windows com base em agente
  - Backup, sem agente com base em host
  - Replicar
  - Replique de um servidor do ponto de recuperação remoto
- Verifique se os pré-requisitos para adicionar uma conta de nuvem no Microsoft Azure são atendidos. Para obter mais informações, consulte Pré-requisitos para adicionar uma conta de nuvem no Microsoft Azure.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Criar um plano com uma tarefa de backup

Um plano inclui tipos diferentes de tarefas que você deseja executar. Para criar a máquina no modo de espera virtual, crie um plano que inclui uma tarefa de backup e uma tarefa no modo de espera virtual. Uma tarefa de backup executa um backup dos nós de origem e armazena os dados para o destino especificado. Esses dados de backup são usados pelo recurso no modo de espera virtual, que os converte em um formato da máquina virtual.

Para obter mais informações, consulte Criar um plano com uma tarefa de backup.

Adicione uma Tarefa no modo de espera virtual ao plano

Crie um modo de espera virtual na tarefa do Azure para que os dados de backup sejam convertidos em um formato da máquina virtual e a máquina virtual seja criada. O recurso modo de espera virtual também monitora o sinal de monitoramento do nó de origem de modo que, quando o nó de origem estiver desativado, a máquina virtual imediatamente assume o controle como nó de origem.

Observações:

- O modo de espera virtual não pode ligar automaticamente os instantâneos de ponto de recuperação criados a partir nós de máquina virtual com base em host, nós replicados a partir de um servidor de ponto de recuperação remoto e a origem da tarefa do modo de espera virtual é aquela replicada em um site diferente. É preciso ativar instantâneos do ponto de recuperação manualmente para esses nós.
- se você pausar o plano, a tarefa Modo de espera virtual não será iniciada. Ao retomar o plano novamente, a tarefa do modo de espera virtual não é retomada automaticamente. É necessário executar manualmente outra tarefa de backup para iniciar a tarefa do modo de espera virtual. Além disso, se o plano for pausado, a opção Pausar/Retomar o modo de espera virtual não estará disponível. Se não desejar que a máquina virtual inicie automaticamente após o plano ser pausado, é necessário pausar manualmente o sinal de monitoramento dos nós.

Siga estas etapas:

1. Clique em **Adicionar uma tarefa** no painel esquerdo.

   Uma nova tarefa será adicionada ao painel esquerdo.

2. No menu suspenso, selecione **Tipo de tarefa** do **Modo de espera virtual.**

   A tarefa em Modo de espera virtual é adicionada.

3. Na guia **Origem**, selecione uma origem para a tarefa do modo de espera virtual.
4. Clique na guia **Servidor de virtualização** e digite os detalhes e o servidor de monitoramento e do servidor de virtualização.

   Tipo de virtualização - Azure

   Tipo de virtualização

   Especifique o Azure como o tipo de virtualização.

Nome da conta

Selecione uma conta existente do Azure. Também é possível adicionar uma nova conta clicando em **Adicionar**.

Para obter mais informações, consulte Como adicionar uma conta de nuvem.

Grupo de recursos

Especifique um grupo de recursos. Você deve ter um grupo de recursos no Azure.

Para obter instruções, consulte Grupo de recursos no Azure na documentação da Microsoft.

Região

Selecione a região do Azure onde deseja que sua VM no modo de espera seja localizada. Para obter mais informações sobre a região, consulte Regiões no Azure.

Monitor

Especifique o nome do host do servidor que monitora o status do servidor de origem.

Observações:

- Você pode usar qualquer computador físico ou máquina virtual como servidor do monitor.
- Não é possível usar o servidor de origem de backup como servidor do monitor.
- A configuração do servidor do monitor não será necessária se os nós forem replicados a partir de um servidor de ponto de recuperação remoto ou se a origem da tarefa no modo de espera virtual for replicada para um site diferente.
- A configuração do servidor do monitor não será necessária se a fonte do modo de espera virtual for a tarefa replicada e o servidor RPS de destino de replicação estiver no Azure.

Nome de usuário

Especifique o nome de usuário para efetuar logon no sistema de monitoramento.

Senha

Especifique uma senha para o nome de usuário para efetuar logon no sistema de monitoramento.

Protocolo

Especifique HTTP ou HTTPS como o protocolo que você deseja usar para comunicação entre o Arcserve Unified Data Protection e o servidor de monitoramento.

Porta

Especifique a porta que deseja usar para a transferência de dados entre o Arcserve Unified Data Protection e o servidor de monitoramento.

5. Clique na guia **Máquina virtual** e insira os detalhes para as Configurações básicas da VM, Repositório de dados da VM para VMware, Caminho da VM para Hyper-V e Rede da VM.

Prefixo do nome da VM

Especifique o prefixo que deseja adicionar ao nome de exibição da máquina virtual no Azure.

Valor padrão: UDPVM_

Instantâneos do ponto de recuperação

Especifique o número de instantâneos dos pontos de recuperação (pontos de recuperação) para a máquina virtual no modo de espera. O número máximo de instantâneos do ponto de recuperação é 29 para o Azure.

Valor padrão: 5

Combine todas as sessões não convertidas em um único instantâneo do ponto de recuperação

Especifique se deseja combinar todas as sessões não convertidas em um único instantâneo do ponto de recuperação quando a próxima tarefa do VSB programada ocorrer.

Padrão: Selecionado

Tamanho da máquina virtual

O Microsoft Azure fornece uma ampla seleção de tamanho da máquina virtual otimizada para atender aos diferentes casos de uso. Eles têm várias combinações de CPU, memória, armazenamento e capacidade de rede. Para obter mais informações sobre o tamanho da máquina virtual e como eles atendem às suas necessidades de computação, consulte Tamanhos para máquina virtual Windows no Azure.

Nome da conta de armazenamento

Selecione um nome de conta de armazenamento. Você deve ter um nome da conta de armazenamento no Azure. Para o tipo de conta de armazenamento,

selecione Storage (finalidade geral v1) ou StorageV2 (finalidade geral v2). Para obter mais informações, consulte Conta de armazenamento no Azure na documentação da Microsoft.

Rede virtual

Selecione uma rede virtual. Você deve ter uma rede virtual no Azure. Para obter mais informações, consulte Rede virtual no Azure na documentação da Microsoft.

Sub-rede

Selecione uma sub-rede de acordo com a rede virtual selecionada. Você deve ter uma sub-rede no Azure. Para obter mais informações, consulte Sub-rede no Azure na documentação da Microsoft.

Grupo de segurança de rede

Selecione um grupo de segurança de rede. Você deve ter um grupo de segurança de rede no Azure. Configure as regras de grupo de segurança para abrir as portas relacionadas, incluindo 3389 para área de trabalho remota, 8014, 8015 para comunicação do Arcserve UDP. Para obter instruções, consulte Grupo de segurança de rede na documentação da Microsoft.

Ativar IP público da atribuição automática

Quando o IP público da atribuição automática estiver ativado, o IP público será atribuído à VM no modo de espera automaticamente quando ela for iniciada no Azure.

6. Clique na guia **Avançado** e forneça os seguintes detalhes:

Iniciar a máquina virtual automaticamente

Especifique se deseja iniciar a máquina virtual automaticamente.

Observação: essa opção não está disponível para os nós de máquina virtual com base em host e nós replicados a partir de um servidor de ponto de recuperação remota e a origem da tarefa no modo de espera virtual é aquela replicada para um local diferente. A fonte do Modo de espera virtual é a tarefa de replicação e o servidor RPS de destino de replicação dentro do Azure.

Timeout

Especifique o tempo que o servidor de monitoramento deve aguardar por um sinal de monitoramento antes de ligar o instantâneo do ponto de recuperação.

Frequência

Especifique a frequência com que o servidor de origem fará a comunicação dos sinais de monitoramento para o servidor de monitoramento.

Exemplo: o valor de tempo limite especificado é 60. O valor de frequência especificado é 10. O servidor de origem comunicará sinais de monitoramento em intervalos de 10 segundos. Se o servidor de monitoramento não detectar um sinal de monitoramento em 60 segundos do último sinal detectado, ele ligará a máquina virtual usando o instantâneo do ponto de recuperação mais recente.

Personalizar parâmetros da tarefa

Você pode personalizar os parâmetros da tarefa para as seguintes opções:

- *Número de segmentos sendo carregados para cada tarefa*: valor padrão: 4
- *Tamanho do buffer de cada segmento*: valor padrão: 4096 KB

Ativar alertas por email

Permite receber alertas por email de acordo com as configurações que você fornecer. Quando essa opção for selecionada, outras categorias de alertas por email são ativadas para a seleção.

- **Sinal de monitoramento faltando para a máquina de origem** – o modo de espera virtual envia notificações de alerta quando o servidor de monitoramento não detecta um sinal de monitoramento no servidor de origem.

  Observação: para nós de Replicar a partir de um servidor de ponto de recuperação remoto ou se a origem da tarefa do modo de espera virtual for aquela que é replicada para um site diferente, essa opção não estará disponível.

- **VM ligada para a máquina de origem configurada para ser ligada automaticamente** – o modo de espera virtual envia notificações de alerta quando ele liga uma máquina virtual que foi configurada para ligar automaticamente quando um sinal de monitoramento não é detectado.

  Observação: para nós de Replicar a partir de um servidor de ponto de recuperação remoto ou se a origem da tarefa do modo de espera virtual for aquela que é replicada para um site diferente, essa opção não estará disponível. Essa opção também não está disponível para os nós da máquina virtual com base em host.

- **VM ativada para máquina de origem configurada para ligar manualmente** – o modo de espera virtual envia notificações de alerta quando ativa uma máquina virtual manualmente.

- **Erros/falhas/paralisação no modo de espera virtual** – o modo de espera virtual envia notificações de alerta quando detecta um erro que ocorreu durante o processo de conversão.

- **Operação do modo de espera virtual realizada com êxito** – o modo de espera virtual envia notificações de alerta quando detecta que uma máquina virtual foi ligada com êxito.
- **O modo de espera virtual não foi iniciado com êxito a partir do instantâneo do ponto de recuperação** – o modo de espera virtual envia notificações de alerta quando detecta que uma máquina virtual não foi ligada automaticamente e a opção de início automático da recuperação de substituição da máquina virtual é especificada.

7. Clique em **Salvar**.

   As alterações são salvas e a tarefa no modo de espera virtual é automaticamente implantada no servidor do modo de espera virtual.

   Observação: quando a tarefa no modo de espera virtual estiver concluída, o volume da máquina virtual no modo de espera será criado. A máquina virtual no modo de espera será criada apenas depois que a máquina virtual for ativada no Arcserve UDP.

   Você criou com êxito e implantou o modo de espera virtual no plano do Azure.

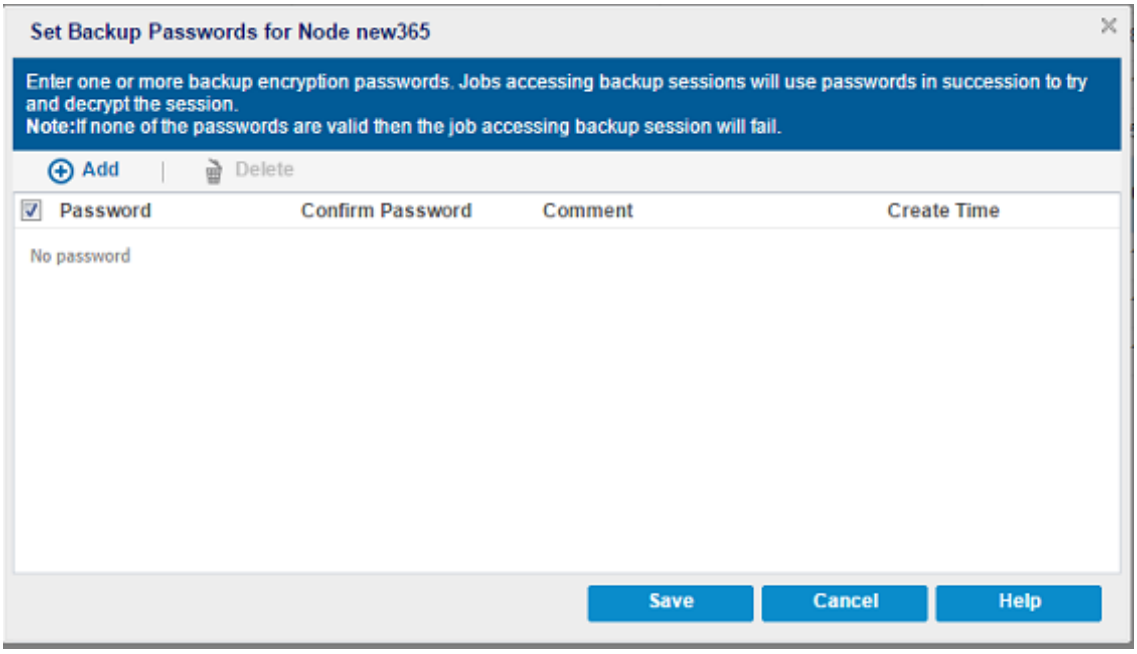
Definir senhas de backup para um ou mais nós

Para garantir que o conversor possa converter os pontos de recuperação replicados, o modo de espera virtual permite especificar senhas de backup para os dados que o conversor pode usar para converter os dados.

Siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.
3. No painel central, clique com o botão direito do mouse no nó e clique em **Definir senhas de backup**.

   A caixa de diálogo **Definir senhas de backup para o nó** será exibida.

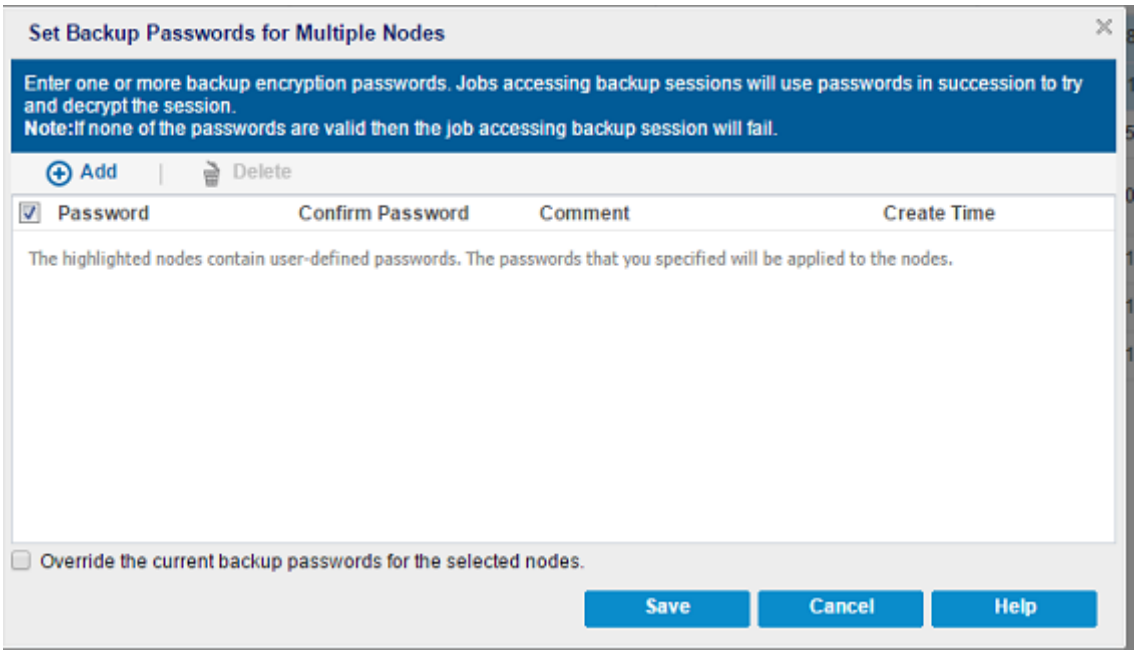


4. Execute as seguintes tarefas para um ou mais nós, na caixa de diálogo **Definir senhas de backup**:

   Adicionar – clique em **Adicionar** para adicionar uma ou mais senhas de backup aos nós selecionados.

   Excluir – clique em **Excluir** para excluir uma ou mais senhas de backup dos nós selecionados.

   Observação: é possível substituir as senhas de backup atuais de vários nós marcando a caixa de seleção **Substituir as senhas de backup atuais** dos nós selecionados.



5. Clique em **Salvar**.

   A caixa de diálogo é fechada, e as senhas de backup são definidas para os nós remotos selecionados.

(Opcional) Execute a tarefa no modo de espera virtual manualmente

Para executar manualmente uma tarefa no modo de espera virtual, você deverá primeiro executar um backup manual. A tarefa no modo de espera virtual está associada a uma tarefa de backup. Se um plano incluir uma tarefa de backup e uma tarefa no modo de espera virtual e você executar a tarefa de backup manualmente, a tarefa do modo de espera virtual será executada automaticamente após a conclusão da tarefa de backup.

Siga estas etapas:

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.

   Exibe os planos que você adicionou.
3. Selecione os nós dos quais deseja fazer backup. O nó selecionado deve ter atribuído um plano.
4. No painel central, clique em **Ações**, **Fazer backup agora**.

   A caixa de diálogo **Fazer backup agora** é exibida.
5. Selecione o tipo de backup e forneça um nome para a tarefa de backup.
6. Clique em **OK**.

   A tarefa de backup é executada.

   A tarefa no modo de espera virtual é executada imediatamente após a tarefa de backup ser concluída.

   A tarefa no modo de espera virtual é executada manualmente.

Pausar e retomar sinal de monitoramento

A solução Arcserve Unified Data Protection permite pausar e retomar os sinais de monitoramento detectados pelo servidor de monitoramento. O sinal de monitoramento é o processo em que o servidor de origem e o servidor de monitoramento se comunicam sobre a integridade do servidor de origem. Se o servidor de monitoramento não detectar um sinal de monitoramento após um determinado período de espera, o recurso do Modo de espera virtual configura a máquina virtual para funcionar como o nó de origem.

Exemplos: quando pausar ou retomar sinais de monitoramento

Os exemplos a seguir descrevem quando pausar e retomar sinais de monitoramento:

- Pause o sinal de monitoramento quando quiser colocar offline um nó (servidor de origem) para manutenção.
- Retome o sinal de monitoramento após as tarefas de manutenção serem concluídas e o nó (servidor de origem) estar online.

Esteja ciente do seguinte:

- É possível pausar e retomar os sinais de monitoramento no nível de grupo ou no nível de nó individual.
- Você pode pausar e retomar os sinais de monitoramento para um ou mais nós em uma única etapa.
- A solução Arcserve Unified Data Protection não liga instantâneos de pontos de recuperação enquanto o sinal de monitoramento estiver no estado pausado.
- Ao atualizar as instalações do agente em nós de origem, o Arcserve Unified Data Protection pausa o sinal de monitoramento dos nós. Para garantir que os servidores de monitoramento monitorem os nós atualizados, retome o sinal de monitoramento dos nós após concluir a atualização nos nós.

Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection.
2. Clique na guia **Recursos**.
3. No painel à esquerda, vá até o **Modo de espera virtual** e clique em **Todos os nós**.

   Se você tiver adicionado alguns nós, os nós serão exibidos no painel central.
4. Selecione o nó que deseja pausar ou retomar.
5. No painel central, clique em **Ações**, **Sinal de monitoramento**, **Pausar** ou **Retomar**.

   O sinal de monitoramento do nó selecionado é pausado ou retomado.

Pausar e retomar a tarefa do modo de espera virtual

A conversão virtual é o processo em que o recurso do modo de espera virtual converte pontos de recuperação do Arcserve Unified Data Protection de nós de origem em formatos da máquina virtual, denominados instantâneos do ponto de recuperação. No caso de um servidor de origem falhar, o recurso de Modo de espera virtual usa os instantâneos de pontos de recuperação para ligar uma máquina virtual no nó de origem.

Como prática recomendada, permita que o processo de conversão virtual opere continuamente. No entanto, se deseja pausar o processo de conversão virtual nos servidores no modo de espera virtual local ou remoto temporariamente, pode fazê-lo no Console. Depois de corrigir os problemas no nó de origem, você pode continuar o processo de conversão virtual.

Quando você faz uma pausa nas tarefas do Modo de espera virtual (tarefas de conversão), a operação de pausa não pausa a tarefa de conversão que está em andamento no momento. A operação de pausa aplica-se somente à tarefa que está aguardando para ser executada no final da próxima tarefa de backup. Como resultado, a próxima tarefa de conversão não é iniciada até que você retome explicitamente a tarefa de conversão (pausada).

Se continuar o modo de espera virtual dos nós e se houver várias sessões de backup sem instantâneo do ponto de recuperação, será exibida uma caixa de diálogo para selecionar a opção de cópia inteligente. Se clicar em Sim, a tarefa em modo de espera virtual poderá converter a sessão combinada em um único instantâneo do ponto de recuperação. Se clicar em Não, a tarefa em modo de espera virtual poderá converter cada sessão individualmente

Observação: como alternativa, é possível pausar e retomar tarefas do Modo de espera virtual diretamente nos nós. Para obter mais informações, consulte o tópico Pausar e retomar tarefas do Virtual Standby nos nós.

Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection.
2. Clique na guia **Recursos**.
3. No painel à esquerda, vá até o **Modo de espera virtual** e clique em **Todos os nós**.

   Se você tiver adicionado alguns nós, os nós serão exibidos no painel central.
4. Selecione o nó que deseja pausar ou retomar.

5. No painel central, clique em **Ações**, **Modo de espera virtual**, **Pausar** ou **Retomar**.

   A função do modo de espera virtual para o nó selecionado é pausada ou retomada.

Verificar o plano

Para verificar seu recurso no modo de espera virtual, verifique se você criou com êxito o plano no modo de espera virtual. Depois de verificar se o plano está criado com êxito, confirme se a tarefa de backup está executando conforme o programado. Depois que a tarefa de backup for concluída com êxito, a tarefa em modo de espera virtual será executada. É possível verificar o status da tarefa de backup e da tarefa no modo de espera virtual na guia **tarefas**.

Siga estas etapas para verificar os planos:

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.

   Uma lista de todos os nós é exibida no painel central.
3. Verifique se os planos são mapeados com nós.

Siga estas etapas para verificar as tarefas no modo de espera virtual:

1. Clique na guia **tarefas**.
2. No painel à esquerda, clique em **Todas as tarefas**.

   O status de cada tarefa é incluído no painel central.
3. Verifique se a tarefa de backup e a tarefa no modo de espera virtual foi bem-sucedida.

   O plano para modo de espera virtual é verificado com êxito.

   O computador no modo de espera virtual é criado.

Como criar um plano no modo de espera virtual

O modo de espera virtual converte os pontos de recuperação em formatos da máquina virtual e prepara um instantâneo para facilitar a recuperação de seus dados quando necessário. Este recurso oferece a capacidade com alta disponibilidade também e garante que a máquina virtual pode assumir o controle imediatamente quando o computador de origem falhar. A máquina virtual em modo de espera é criada pela conversão de pontos de recuperação para formato da máquina virtual VMware ou um Hyper-V.

Observação: a tarefa de modo de espera virtual é executada apenas se a tarefa de backup criar um instantâneo do ponto de recuperação válido. Se a tarefa de backup falhar, a tarefa no modo de espera virtual será ignorada.

O que fazer a seguir?

1. Verificar os pré-requisitos e as considerações
2. Criar um plano com uma tarefa de backup
3. Adicione uma Tarefa no modo de espera virtual ao plano
4. (Opcional) Execute a tarefa no modo de espera virtual manualmente
5. Pause e retome o sinal de monitoramento
6. Pause e retome a tarefa do modo de espera virtual
7. Verificar o plano

Verificar os pré-requisitos e as considerações

Verifique se concluiu os seguintes pré-requisitos:

- Efetue logon no Console.
- Instale o componente do servidor e crie repositórios de dados, caso deseje armazenar os dados de backup no servidor de ponto de recuperação.
- Você tem um ponto de recuperação válido para criar uma máquina no modo de espera virtual. Os pontos de recuperação podem ser provenientes de uma das seguintes tarefas:
  - Backup, Windows com base em agente
  - Backup, sem agente com base em host
  - Replicar
  - Replique de um servidor de ponto de recuperação remoto
- Fazer backup da máquina completa para ativar a tarefa Modo de espera virtual. Não é possível criar uma tarefa Modo de espera virtual se o backup não for um backup completo.
- Verifique se você tem a permissão mínima para executar as tarefas necessárias da VSB. Para obter mais informações, consulte Permissão mínima necessária para tarefas da VSB.
- O modo de espera virtual não tem suporte em origens do Linux. Para ver uma lista de sistemas operacionais, bancos de dados e navegadores com suporte, consulte a Matriz de compatibilidade.

Considerações:

- O modo de espera virtual usa discos com pouco provisionamento para o vSphere.
- O modo de espera virtual usa discos rígidos virtuais de expansão dinâmica para o Hyper-V.
- O VMware usa um computador separado para monitorar o servidor com o agente instalado.
- O próprio Hyper-v atua como o servidor de monitoramento com o agente instalado.

Observação: como prática recomendada, aconselhamos excluir os arquivos da verificação do antivírus para garantir que o modo de espera virtual funcione corretamente. Para obter mais informações, consulte Excluir arquivos da verificação do antivírus.

Permissão mínima necessária para tarefas da VSB

A tabela exibe a lista de permissão mínima necessária para executar todas as tarefas da VSB.

Observação: permissões globais são definidas no nível do vCenter.

Tarefas	Permissão
Repositório de dados	Alocar espaço
	Procurar no repositório de dados
	Operações de arquivo de baixo nível
Global	Desativar métodos
	Ativar métodos
	Licenças
Host > Configuração	Configuração de partição do armazenamento
Rede	Atribuir rede
Resource	Atribuir a máquina virtual ao pool de recursos
Máquina virtual > Configuração	Adicionar disco existente
	Adicionar novo disco
	Adicionar ou remover dispositivo
	Avançado
	Alterar contagem de CPU
	Controle de alterações de disco
	Memória
Máquina virtual > Interação	Desligar
	Ligar
	Interação do console
Máquina virtual > Inventário	Criar a partir de existente
	Criar novo
	Remover
Máquina virtual > Provisionamento	Permitir acesso a disco
	Permitir acesso de somente leitura ao disco
	Permitir download da máquina virtual
Máquina virtual > Gerenciamento de instantâneos	Criar instantâneo
	Remover instantâneo
	Reverter para um instantâneo

Criar um plano com uma tarefa de backup

Um plano inclui tipos diferentes de tarefas que você deseja executar. Para criar a máquina no modo de espera virtual, crie um plano que inclui uma tarefa de backup e uma tarefa no modo de espera virtual. Uma tarefa de backup executa um backup dos nós de origem e armazena os dados para o destino especificado. O recurso de modo de espera virtual usa os dados de backup e se converte em um formato de máquina virtual.

É possível criar uma máquina no modo de espera virtual a partir de um backup do Windows com base em agente, backup com base em host sem agente. Também é possível criar uma máquina no modo de espera virtual a partir de dados que são replicados com a tarefa **Replicar**. O procedimento indicado a seguir é um exemplo para criar backup do Windows com base em agente.

Observações:

- para obter mais informações sobre o backup sem agente e com base em host, consulte Como criar um plano de backup da máquina virtual com base em host.
- Para obter mais informações sobre a replicação de dados de backup, consulte Como replicar dados entre repositórios de dados gerenciados de um console do UDP e gerenciados a partir de diferentes consoles do UDP.

Siga estas etapas:

1. Clique na guia **Recursos** no Console.
2. No painel à esquerda, navegue para **Planos** e clique em **Todos os planos**.

   Se tiver criado os planos anteriores, esses planos serão exibidos no painel central.
3. No painel central, clique em **Adicionar um plano**.

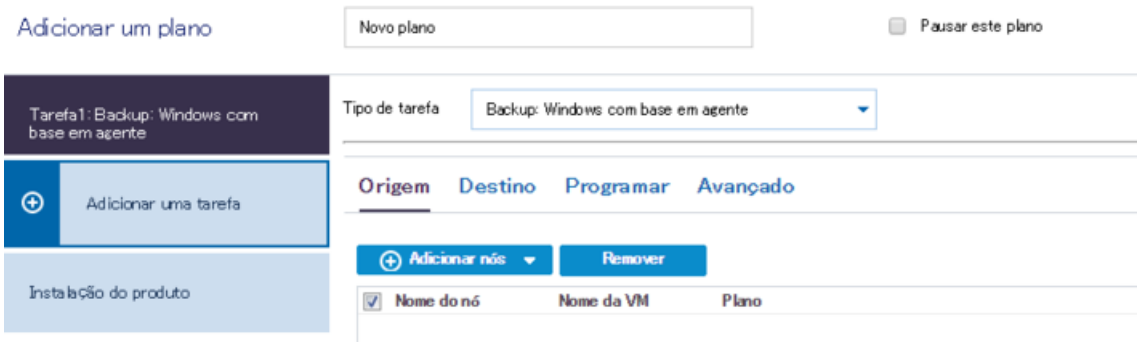
   Adicionar um plano é exibido.
4. Digite o nome do plano.
5. (Opcional) Marque a caixa de seleção **Pausar este plano**.

   O plano não será executado até que você desmarque a caixa de seleção para retomar o plano.

   Observação: se um plano for pausado, nenhuma tarefa em andamento será pausada, mas todas as tarefas programadas correspondentes associadas a esse plano serão pausadas. No entanto, você pode executar uma tarefa manualmente. Por exemplo, você pode executar manualmente a tarefa de backup e a tarefa de replicação para um nó mesmo que o respectivo plano esteja pausado. Nesse caso, a

tarefa seguinte da tarefa sob demanda (manual) não será executada. Por exemplo, há uma tarefa de replicação após uma tarefa de backup sob demanda, a tarefa de replicação não será executada para a tarefa de backup sob demanda. É necessário executar manualmente a tarefa de replicação. Quando você retomar o plano, as tarefas pendentes não são retomadas imediatamente. Depois de retomar o plano, as tarefas pendentes serão executadas no próximo horário programado.

6. Na lista suspensa **Tipo de tarefa**, selecione **Backup, Windows com base em agente**.



Agora, especifique os detalhes de Origem, Destino, Programação e Avançado.

Especificar a origem

A página Origem permite especificar os nós de origem que deseja proteger. É possível selecionar mais de um nó em um plano. Caso não tenha adicionado nós para o console, você pode adicionar nós ao criar ou modificar um plano da página de origem. Também é possível salvar um plano sem adicionar nenhum nó de origem. O plano é implantado somente após você adicionar nós de origem.

Siga estas etapas:

1. Na guia Origem, clique em **Adicionar**.
2. Selecione uma das seguintes opções:

   Selecionar os nós a serem protegidos no Arcserve UDP

   Abre a caixa de diálogo Selecionar nós para proteger no Arcserve UDP. Selecione os nós na lista exibida. Selecione esta opção se você já tiver adicionado os nós para o console.

   Adicionar nó do Windows

   A caixa de diálogo Adicionar nós a um plano é exibida. Selecione esta opção se você não tiver adicionado os nós e desejar adicionar manualmente os nós para proteger.

   Detectar os nós do Active Directory

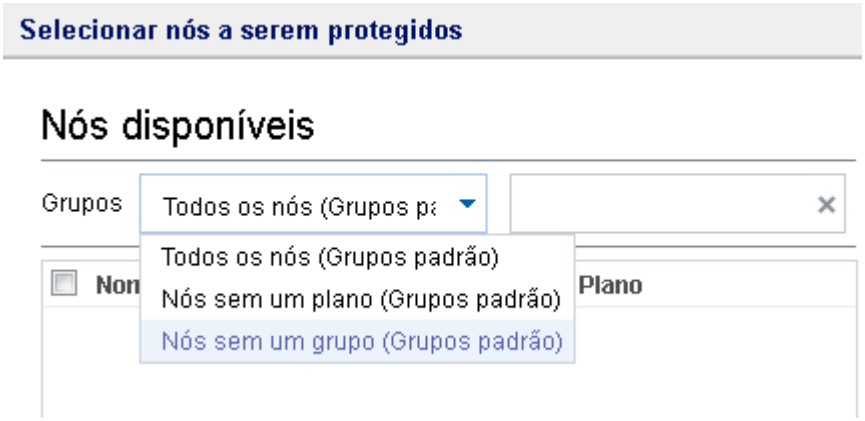
   Abra a caixa de diálogo Adicionar nós ao Console do Arcserve UDP. Selecione essa opção se desejar detectar e adicionar nós do Active Directory.
3. Se você selecionou a opção **Selecionar nós para proteger no Arcserve UDP**, na caixa de diálogo Selecionar nós para proteger, faça o seguinte:
   a. (Opcional) Selecione um filtro na lista suspensa Grupos para filtrar os nós. É possível digitar as palavras-chave para filtrar melhor seus nós.

      Os nós são exibidos na coluna Nós disponíveis.

   b. Selecione os nós na coluna Nós disponíveis e, em seguida, clique na seta simples à direita (>) ou na seta dupla à direita (>>) para mover os nós selecionados ou todos os nós, respectivamente, para a coluna Nós selecionados.

      Os nós são exibidos na coluna Nós selecionados.

   c. Clique em **OK** para fechar a caixa de diálogo.



4. Para escolher Tipo de proteção, selecione uma das seguintes opções:

   Fazer backup de todos os volumes

   Prepara um backup instantâneo de todos os volumes.

   Fazer backup dos volumes selecionados

   Prepara um instantâneo de backup do volume selecionado.

   A origem é especificada.

Especificar o destino

O destino é o local onde você armazena os dados de backup. É necessário, no mínimo, especificar o destino para salvar o plano.

Siga estas etapas:

1. Selecione um dos seguintes **Tipos de destino**:

   Disco local ou uma pasta compartilhada

   Especifica que o destino de backup é um destino local ou uma pasta compartilhada. Se selecionar essa opção, será possível salvar os dados como pontos de recuperação ou conjuntos de recuperação. As opções de pontos de recuperação e de conjuntos de recuperação estão disponíveis na guia **Programar**.

   Servidor de ponto de recuperação do Arcserve UDP

   Especifica que o destino de backup é um servidor do ponto de recuperação. Se selecionar essa opção, os dados serão armazenados como pontos de recuperação. Não é possível armazenar dados como conjuntos de dados de recuperação.

2. Se tiver selecionado **Servidor do ponto de recuperação do Arcserve UDP**, forneça os seguintes detalhes:
   a. Selecione um servidor do ponto de recuperação
   b. Selecione um repositório de dados. A lista exibe todos os repositórios de dados que são criados no servidor do ponto de recuperação especificado.
   c. Forneça uma senha da sessão.
   d. Confirme a senha da sessão.
3. Se tiver selecionado **Disco local ou pasta compartilhada**, forneça os seguintes detalhes:
   a. Forneça o caminho completo do destino local ou de rede. Para o destino de rede, especifique as credenciais com o acesso de gravação.
   b. Selecione o algoritmo de criptografia. Para obter mais informações, consulte Configurações de criptografia.
   c. Como opção, forneça uma senha de criptografia.
   d. Confirme a senha de criptografia.
   e. Selecione um tipo de compactação. para obter mais informações, consulte Tipo de compactação.

Observação: se armazenar os dados em um disco local ou em uma pasta compartilhada, não será possível replicar os dados para outro servidor do ponto de recuperação. A replicação é suportada apenas se armazenar os dados em um servidor do ponto de recuperação.

O destino é especificado.

Especificar a programação

A página Programar permite definir uma programação para o backup e para que as funções Mesclar e Acelerar sejam repetidas em intervalos específicos. Após definir uma programação, as tarefas são executadas automaticamente de acordo com a programação. É possível adicionar várias programações e fornecer configurações de retenção.

Uma Programação de backup se refere a programação regular que é repetida várias vezes ao dia, com base no número de horas ou de minutos selecionado. Além da programação regular, uma programação de backup também fornece opções para adicionar programações diária, semanal e mensal.

Observação: para obter mais informações sobre as configurações de retenção e programação, consulte Entendendo a programação avançada e retenção.

Siga estas etapas:

1. (Opcional) Selecione a opção para gerenciar os pontos de recuperação. Essa opção será visível somente se tiver selecionado o local ou a pasta compartilhada como o destino do backup.

   Reter por pontos de recuperação

   Os dados de backup são armazenadas como pontos de recuperação.

   Reter por conjuntos de recuperação

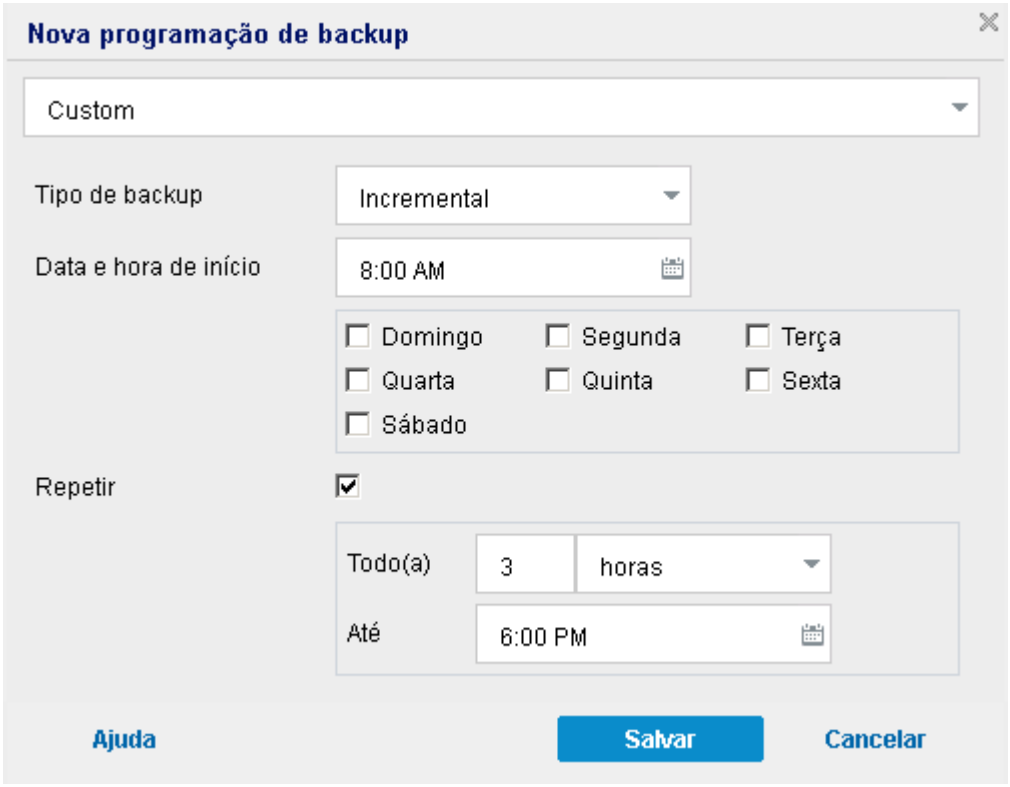
   Os dados de backup são armazenadas como conjuntos de recuperação.

2. Adicionar programações de backup, mesclagem e acelerador.

   Adicionar programação de backup

   a. Clique em **Adicionar** e selecione **Adicionar programação de backups**.

      A caixa de diálogo **Nova programação de backup** é aberta.



b. Selecione uma das seguintes opções:

Personalizado

Especifica a programação de backup que se repete várias vezes por dia.

Diário

Especifica a programação de backup que ocorre uma vez por dia. Por padrão, todos os dias da semana estão selecionados para o backup diário. Se não desejar executar a tarefa de backup em um dia específico, desmarque a caixa de seleção correspondente àquele dia da semana.

Semanal

Especifica a programação de backup que ocorre uma vez por semana.

Mensal

Especifica a programação de backup que ocorre uma vez por mês.

c. Selecione o tipo de backup.

Completo

Especifica a programação de backups para backups completos. Conforme programado, o Arcserve UDP executa um backup completo de todos os blocos usados do computador de origem. Um backup completo em geral, consome tempo, dependendo do tamanho do backup.

Verificar

Especifica a programação de backups para backups de verificação.

A Arcserve UDP verifica se os dados protegidos são válidos e concluídos, executando uma verificação de confiabilidade da imagem de backup armazenada na origem do backup. Se necessário, a imagem será sincronizada novamente. Um backup de verificação examinará o backup mais recente de cada bloco e irá comparar o conteúdo e as informações com a origem. Esta comparação verifica se o backup mais recente dos blocos representa as informações correspondentes na origem. Se a imagem de backup de qualquer bloco não corresponder à origem (possivelmente devido a alterações no sistema desde o último backup), o Arcserve UDP atualizará (fará nova sincronização) o backup do bloco que não corresponder. Também é possível usar um backup de verificação (muito raramente) para obter a garantia de backup completo sem usar o espaço necessário para um backup completo.

Vantagens: produz uma pequena imagem de backup quando comparado ao backup completo, pois somente os blocos alterados (blocos que não coincidem com o último backup) são armazenados em backup.

Desvantagens: o tempo de backup é longo, pois todos os blocos de origem são comparados aos blocos do último backup.

Incremental

Especifica a programação de backups para backups incrementais.

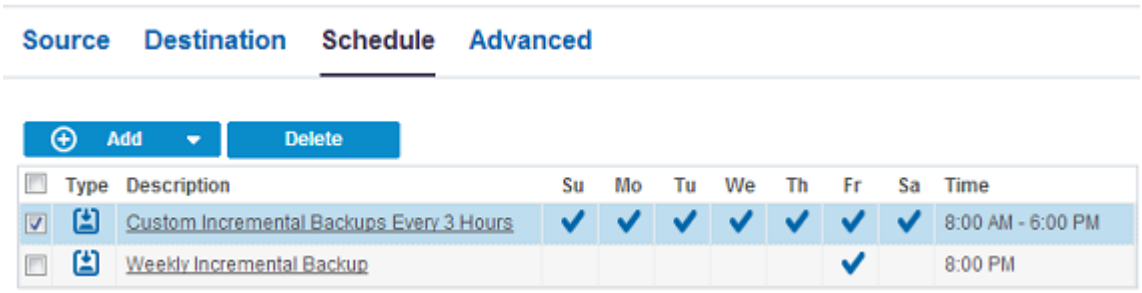
Conforme programado, o Arcserve UDP faz backup incremental apenas dos blocos que foram alterados desde o último backup realizado com êxito. As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a executar um backup.

d. Especifique a hora de início do backup.

e. (Opcional) Marque a caixa de seleção de **Repetição** e especifique a programação a ser repetida.

f. Clique em **Salvar**.

A programação de backup é especificada e exibida na página de **Programação**.



Adicionar Programação de mesclagem

a. Clique em Adicionar e selecione Adicionar programação de mesclagem.

   A caixa de diálogo **Adicionar nova programação de mesclagem** é aberta.

b. Especifique a hora de início para iniciar a tarefa de mesclagem.

c. Especificar **Até** para especificar uma hora de término para a tarefa de mesclagem.

d. Clique em **Salvar**.

   A programação de mesclagem é especificada e exibida na página **Programar**.

Adicionar programação de acelerador

a. Clique em **Adicionar** e selecione **Adicionar programação de acelerador.**

   A caixa de diálogo Adicionar nova programação do acelerador é aberta.

b. Especifique o limite de taxa de transferência em MB por minuto.

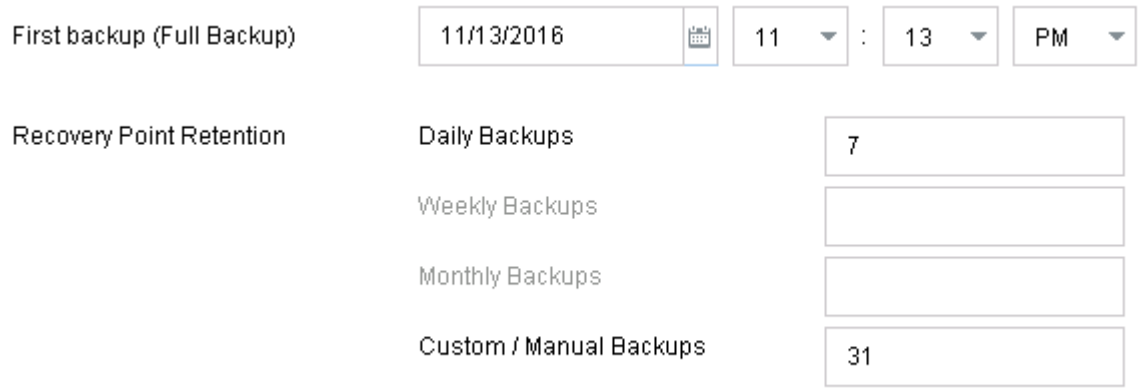
c. Especifique a hora de início para iniciar a tarefa de taxa de transferência de backup.

d. Especifique **Até** para especificar um horário de término para a tarefa de taxa de transferência.

e. Clique em **Salvar**.

   A Programação de acelerador é especificada e exibida na página **Programar**.

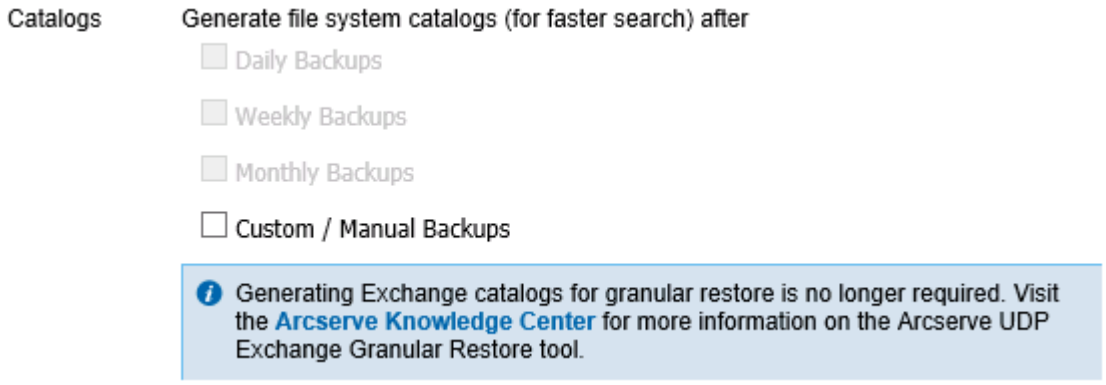
3. Especifique a hora de início do backup programado.



4. Especifique as configurações de retenção de pontos de recuperação para programação diária, semanal e mensal.

   Essas opções serão ativadas se tiver adicionado a programação de backup correspondente. Se você modificar as configurações de retenção desta página, as alterações serão refletidas na caixa de diálogo Programação de backup.

5. Especifique os detalhes de catálogo.



   Os catálogos permitem gerar o catálogo do sistema de arquivos. O catálogo do sistema de arquivos é necessário para agilizar e melhorar a pesquisa. Se marcar as caixas de seleção do catálogo, os catálogos serão ativados de acordo com o tipo de backup que você especificou. Desmarque a caixa de seleção para desativar a geração do catálogo.

   A programação é especificada.

Noções básicas sobre a programação avançada e retenção

A opção de programação permite especificar uma programação personalizada, uma programação diária/semanal/mensal ou ambas. Na programação personalizada, é possível configurar a programação de backups para cada dia da semana ou adicionar até quatro programações de backup em cada dia. É possível escolher um dia específico da semana e criar uma janela para definir quando executar o backup e em que frequência.

Programação	Tarefa com suporte	Comentários
Backup	Tarefa de backup	Definir janelas de tempo para a execução de tarefas de backup.
Limitação de backup	Tarefa de backup	Definir janelas de tempo para controlar a velocidade de backup.
Mesclar	Tarefa de mesclagem	Definir quando executar tarefas de mesclagem.
Programação diária	Tarefa de backup	Definir quando executar tarefas do backup diário.
Programação semanal	Tarefa de backup	Definir quando executar tarefas do backup semanal.
Programação mensal	Tarefa de backup	Definir quando executar tarefas do backup mensal.

Também é possível especificar as configurações de retenção para os pontos de recuperação.

Observação: as configurações de retenção devem ser definidas em cada plano para controlar como os dados dos nós atribuídos a esse plano são retidos no repositório de dados de destino.

As programações para backups diários/semanais/mensais são independentes para a programação personalizada e umas das outras. É possível configurar para executar somente o backup diário, semanal ou mensal, sem configurar a Programação personalizada.

Programação de tarefas de backup

É possível adicionar quatro janelas de tempo por dia na programação do backup. Uma janela de tempo é válida das 00:00 às 23:59. Não é possível especificar uma janela de tempo das 18:00 às 6:00. Nesses casos, você deve especificar manualmente duas janelas de tempo diferentes.

Para cada janela de tempo, a hora de início é inclusiva e a hora de término é exclusiva. Por exemplo, você configurou para executar o backup incremental em intervalos de uma hora entre as 6:00 e as 9:00. O backup será iniciado às 6:00. Isso significa que o backup será executado às 6h00, 7h00 e 8h00, mas NÃO às 9h00.

Observação: se você deseja executar a tarefa de backup várias vezes até o fim do dia, defina a programação para até 0h00. Por exemplo, para executar a tarefa de backup a cada 15 minutos o dia inteiro, defina a programação como das 0h00 às 00h00, a cada 15 minutos.

Programação do acelerador de backup

A programação de aceleração do backup permite controlar a velocidade da taxa de transferência de backup o que, por sua vez, controla o uso de recursos (E/S de disco, CPU, largura de banda de rede) do servidor cujo backup está sendo feito. Isso é útil quando se não quiser afetar o desempenho do servidor durante o horário comercial. É possível adicionar quatro janelas de tempo por dia na sua programação de aceleração do backup. Para cada janela de tempo, é possível especificar um valor, em MB por minuto. Esse valor será usado para controlar a taxa de transferência do backup. Os valores válidos variam entre 1 MB/minutos a 99999 MB/minutos.

Se uma tarefa de backup estende seu tempo especificado, o limite de aceleração será ajustado de acordo com o tempo especificado. Por exemplo, você definiu o limite de aceleração de backup como 500 MB/minuto das 8:00 às 20:00 e 2500 MB/minuto das 20:00 às 22:00. Se uma tarefa de backup iniciar às 19h00 e for executada durante três horas, das 19h00 às 20h00 o limite de aceleração será de 500 MB/minuto e das 20h00 às 22h00, o limite de aceleração será 2500 MB/minuto.

Se não definir nenhuma programação do backup e programação da taxa de transferência do backup, o backup será executado o mais rápido possível.

Mesclar a programação

Permite mesclar pontos de recuperação com base na programação fornecida.

Considere os seguintes pontos para a tarefa de mesclagem:

- A qualquer momento apenas uma tarefa de mesclagem pode ser executada para um nó.
- Se uma tarefa de mesclagem iniciar, ela precisará ser concluída antes que a próxima tarefa de mesclagem seja iniciada. Isso significa que, se um ou mais conjuntos de pontos de recuperação forem mesclados, não será possível adicionar o

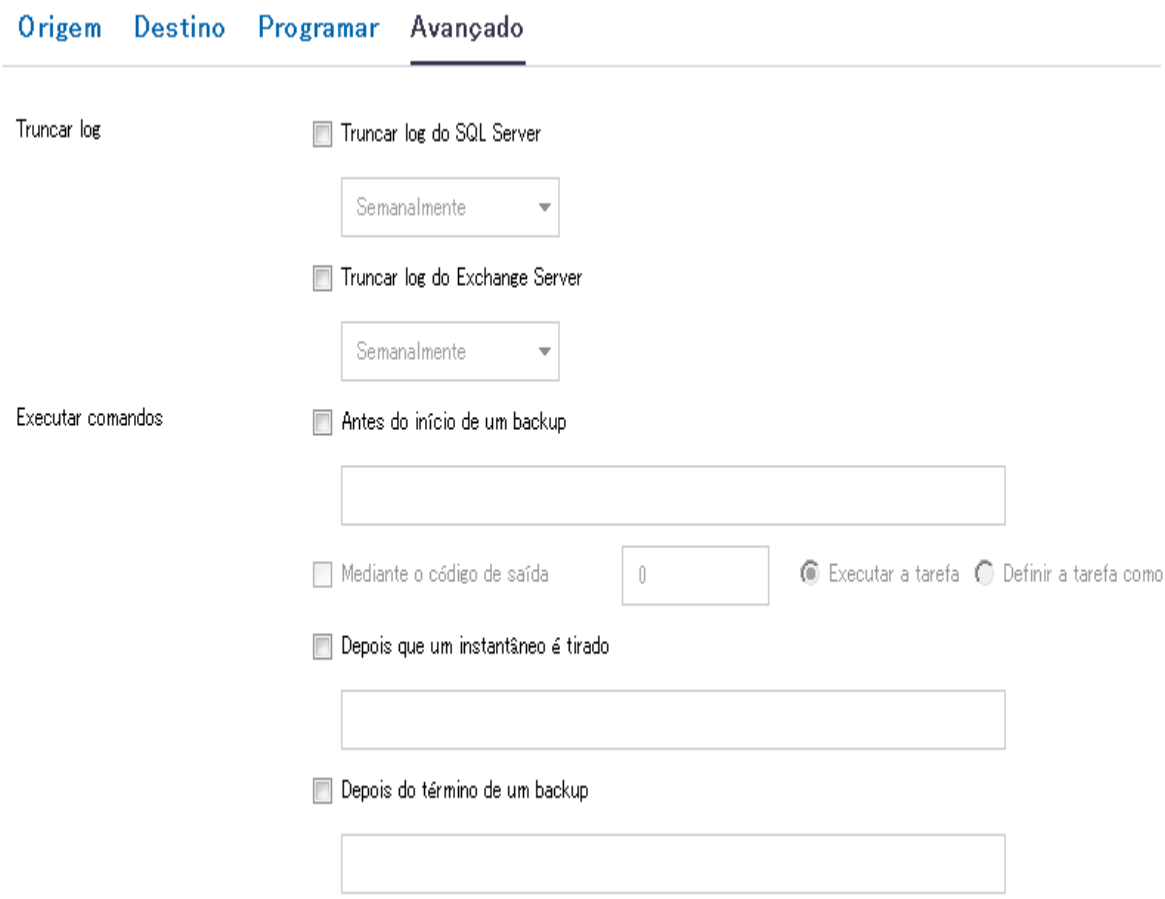
novo ponto de recuperação a este processo de mesclagem, até que o processo de mesclagem do conjunto atual de ponto de recuperação seja concluído.

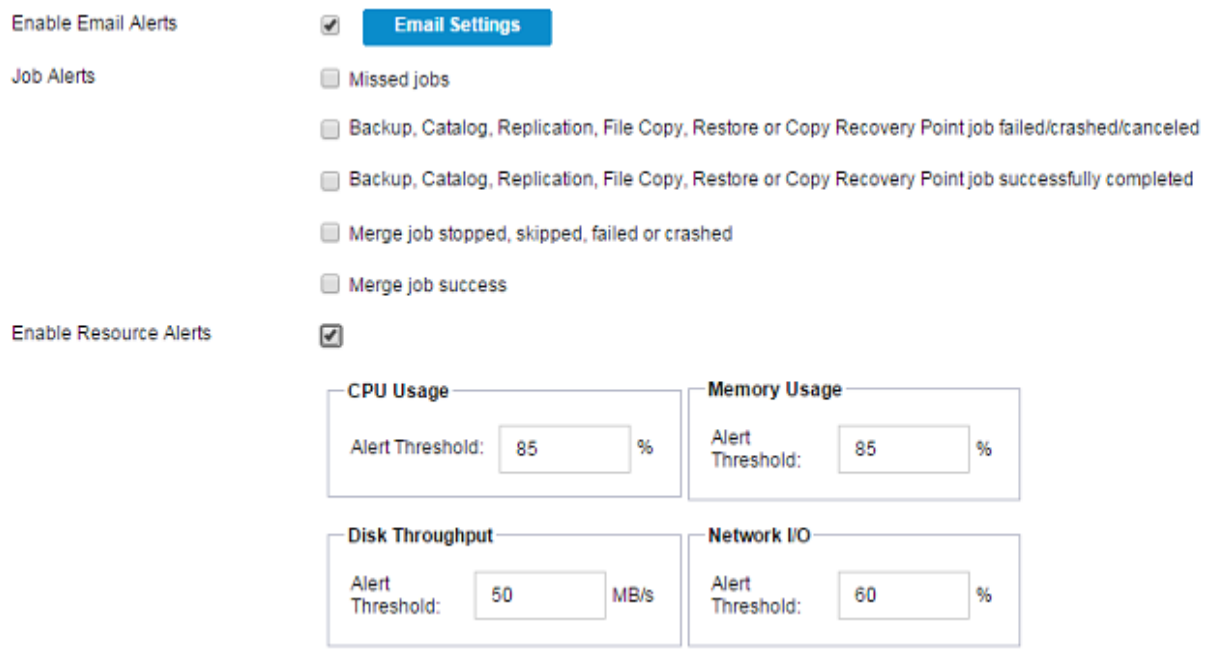
- Se uma tarefa de mesclagem estiver processando mais de um conjunto de pontos de recuperação (por exemplo, conjunto [1~4], conjunto [5~11] e conjunto [12~14]; são três conjuntos) o servidor de ponto de recuperação processará esses conjuntos, um por um.
- Se uma tarefa de mesclagem é retomada após um intervalo, a tarefa detectará em que ponto ela foi pausada e continuará a mesclagem a partir do ponto de pausa.

Especificar as configurações avançadas

A guia **Avançado** permite especificar algumas configurações avançadas para a tarefa de backup. As configurações avançadas incluem fornecer configurações de log de truncamento, a localização de quaisquer scripts e as configurações de email.

A imagem a seguir mostra a guia Avançado:





Siga estas etapas:

1. Especifique os seguintes detalhes.

Truncar log

Permite especificar a programação para truncar logs para o SQL Server e o Exchange Server. É possível especificar a programação como **Diária**, **Semanal** ou **Mensal**.

Nome de usuário

Permite especificar o usuário que possui autorização para executar um script.

Senha

Permite especificar a senha do usuário que está autorizado a executar o script.

Executar um comando antes do início do backup

Permite a execução de um script antes de iniciar a tarefa de backup. Especifique o caminho onde o script está armazenado. Clique em **No código de saída** e especifique o código de saída para **Executar tarefa** ou **Tarefa com falha**. **Executar a tarefa** indica que a tarefa de backup continuará quando o script retornar o código de saída. **Tarefa com falha** indica que a tarefa de backup será interrompida quando o script retornar o código de saída.

Executar um comando após a criação de um instantâneo

Permite executar um script depois que o backup do instantâneo for gerado. Especifique o caminho onde o script está armazenado.

Executar um comando após a conclusão do backup

Permite executar um script depois que a tarefa de backup foi concluída. Especifique o caminho onde o script está armazenado.

Ativar alertas por email

Permite ativar alertas por email. É possível especificar configurações de email e os tipos de alertas que você deseja receber por email. Ao selecionar esta opção, as seguintes opções serão ativadas para a seleção.

Configurações de email

Permite configurar as definições de email. Clique em **Configurações de email** e configure o servidor de email e os detalhes do servidor proxy.

Alertas de tarefa

Permite que você selecione os tipos de emails da tarefa que deseja receber.

Ativar os alertas de recurso

Permite que você especifique um limite de uso da CPU, o uso da memória, a taxa de transferência de disco, E/S de rede. Você pode fornecer o valor em porcentagem. Você receberá um email quando o valor exceder o Limite de alerta.

2. Clique em **Salvar**.

Observação: quando você seleciona um nó como origem de backup ou proxy de backup, o Arcserve UDP verifica se o agente está instalado no nó e se é a versão mais recente. Em seguida, o Arcserve UDP exibe uma caixa de diálogo de verificação que lista todos os nós que possuem uma versão antiga do agente ou que não tem o agente instalado. Para instalar/atualizar o agente nesses nós, selecione o método de instalação e clique em Salvar.

As alterações são salvas e uma marca de seleção verde é exibida ao lado do nome da tarefa. A página do plano é fechada.

Observação: se precisar adicionar outra tarefa, deverá selecionar o plano na guia **Recursos** e modificar o plano. Para modificar o plano, clique no plano do painel central. O plano é exibido e será possível modificá-lo.

O plano de backup é criado e implantado automaticamente para o nó de origem. O backup é executado de acordo com a programação que você configurou na guia **Programar.** Também é possível fazer backup manual quando desejado.

Adicionar uma tarefa no modo de espera virtual ao plano

Criar uma tarefa no modo de espera virtual para que os dados de backup sejam convertidos em formato da máquina virtual e a máquina virtual seja criada. O recurso modo de espera virtual também monitora o sinal de monitoramento do nó de origem de modo que, quando o nó de origem estiver desativado, a máquina virtual imediatamente assume o controle como nó de origem.

Observações:

- O modo de espera virtual não pode ligar automaticamente os instantâneos de ponto de recuperação criados a partir nós de máquina virtual com base em host, nós replicados a partir de um servidor de ponto de recuperação remoto e a origem da tarefa do modo de espera virtual é aquela replicada em um site diferente. É preciso ativar instantâneos do ponto de recuperação manualmente para esses nós.
- se você pausar o plano, a tarefa Modo de espera virtual não será iniciada. Ao retomar o plano novamente, a tarefa do modo de espera virtual não é retomada automaticamente. É necessário executar manualmente outra tarefa de backup para iniciar a tarefa do modo de espera virtual. Além disso, se o plano for pausado, a opção Pausar/Retomar o modo de espera virtual não estará disponível. Se não desejar que a máquina virtual inicie automaticamente após o plano ser pausado, é necessário pausar manualmente o sinal de monitoramento dos nós.

Siga estas etapas:

1. Clique em **Adicionar uma tarefa** no painel esquerdo.

   Uma nova tarefa será adicionada ao painel esquerdo.

2. No menu suspenso, selecione **Tipo de tarefa** do **Modo de espera virtual.**

   A tarefa em Modo de espera virtual é adicionada.

3. Na guia **Origem**, selecione uma origem para a tarefa do modo de espera virtual.

4. Clique na guia **Servidor de virtualização** e digite os detalhes e o servidor de monitoramento e do servidor de virtualização.

   Tipo de virtualização – VMware

   ESX Host/vCenter

   Especifique o nome de host do sistema do servidor ESX ou vCenter.

   Nome de usuário

Especifique o nome de usuário necessário para efetuar logon no sistema VMware.

Observação: a conta especificada deve ser uma conta administrativa ou uma conta com privilégios administrativos no sistema do servidor ESX ou vCenter.

Senha

Especifique a senha para o nome do usuário necessária para efetuar logon no sistema VMware.

Protocolo

Especifique HTTP ou HTTPS como o protocolo que você deseja usar para comunicação entre o Agente do Arcserve Unified Data Protection de origem e o servidor de monitoramento.

Porta

Especifique a porta que deseja usar para a transferência de dados entre o servidor de origem e o servidor de monitoramento.

Nó ESX

Os valores nesse campo variam de acordo com o valor especificado no campo Host do ESX/vCenter:

Sistemas do servidor ESX

Ao especificar um sistema do servidor ESX no campo Host do ESX/vCenter, esse campo exibe o nome do host do sistema do servidor ESX.

Sistemas do servidor vCenter

Ao especificar um sistema do vCenter Server no campo Host do ESX/vCenter, esse campo permite especificar (na lista suspensa) o sistema do servidor ESX que deseja associar a este plano.

Monitor

Especifique o nome do host do servidor que monitora o status do servidor de origem.

Observações:

- Você pode usar qualquer computador físico ou máquina virtual como servidor do monitor.
- Não é possível usar o servidor de origem de backup como servidor do monitor.
- A configuração do servidor do monitor não será necessária se os nós forem replicados a partir de um servidor de ponto de recuperação remoto ou se a

origem da tarefa no modo de espera virtual for replicada para um site diferente.

- A configuração do servidor do monitor não será necessária se a fonte do modo de espera virtual for a tarefa replicada e o servidor RPS de destino de replicação estiver no Azure.

Nome de usuário

Especifique o nome de usuário para efetuar logon no sistema de monitoramento.

Senha

Especifique uma senha para o nome de usuário para efetuar logon no sistema de monitoramento.

Protocolo

Especifique HTTP ou HTTPS como o protocolo que você deseja usar para comunicação entre o Arcserve Unified Data Protection e o sistema do servidor ESX (servidor de monitoramento).

Porta

Especifique a porta que você deseja usar para a transferência de dados entre o Arcserve Unified Data Protection e o sistema do servidor ESX (servidor de monitoramento).

Use o servidor de monitoramento como proxy para transferência de dados

Especifique essa opção para permitir que o servidor de monitoramento copie os dados de conversão do nó do Agente do Arcserve Unified Data Protection para o repositório de dados do servidor ESX. Com essa opção ativada, o recurso modo de espera virtual transfere os dados de conversão do nó do agente para o repositório de dados do ESX Server usando a comunicação de Fibre Channel, que é mais rápida do que usar a comunicação de LAN para transferir dados. Apenas a operação de gravação na conversão acontece no canal de fibra. A operação de leitura acontece através da LAN.

Observação: a opção Usar o servidor de monitoramento como proxy para a transferência de dados fica ativada por padrão. É possível desativar essa opção para permitir que o nó do Agente do Arcserve Unified Data Protection copie os dados de conversão diretamente para o repositório de dados no sistema do servidor ESX.

Tipo de virtualização – Hyper-V

Nome do host HyperV

Especifique o nome de host do sistema Hyper-V.

Nome de usuário

Especifique o nome de usuário necessário para efetuar logon no sistema Hyper-V.

Observação: a conta especificada deve ser uma conta administrativa ou uma conta com privilégios administrativos no sistema Hyper-V.

Senha

Especifique a senha para o Nome do usuário necessária para efetuar logon no sistema Hyper-V.

Protocolo

Especifique HTTP ou HTTPS como o protocolo que você deseja usar para comunicação entre o servidor do Arcserve Unified Data Protection e o sistema do servidor Hyper-V (servidor de monitoramento).

Porta

Especifique a porta que você deseja usar para a transferência de dados entre o servidor do Arcserve Unified Data Protection e o sistema do servidor Hyper-V (servidor de monitoramento).

Observação: para validar o sistema Hyper-V, clique em **Conectar**.

5. Clique na guia **Máquina virtual** e insira os detalhes para as Configurações básicas da VM, Repositório de dados da VM para VMware, Caminho da VM para Hyper-V e Rede da VM.

   Sistemas VMware:

   Aplique as opções a seguir da máquina virtual para sistemas VMware:

   Prefixo do nome da VM

   Especifique o prefixo que deseja adicionar ao nome de exibição da máquina virtual no sistema do servidor ESX.

   Valor padrão: UDPVM_

   Pool de recursos

   Especifique o nome do pool de recursos no qual a máquina virtual em modo de espera será agrupada.

   Contagem da CPU

   Especifique a contagem de CPU mínima e máxima suportada pela máquina virtual em modo de espera.

   Memória

Especifique a quantidade total de RAM em MB a ser alocada para a máquina virtual em modo de espera.

Observação: a quantidade de RAM especificada deve ser um múltiplo de dois.

Instantâneos do ponto de recuperação

Especifique o número de instantâneos dos pontos de recuperação (pontos de recuperação) para a máquina virtual no modo de espera. O número máximo de instantâneos dos pontos de recuperação é 29 para servidores de virtualização do VMware.

Todos os discos virtuais compartilham o mesmo repositório de dados

Selecione esta opção para copiar todos os discos relacionados à máquina virtual para um repositório de dados.

Desmarque a caixa de seleção para copiar as informações relacionadas ao disco da máquina virtual para o repositório de dados correspondente. Especifique o local onde deseja armazenar os dados de conversão.

Rede

Permite definir as NICs, redes virtuais e os caminhos que o sistema do servidor ESX usa para se comunicar com as máquinas virtuais.

Observação: o adaptador de rede flexível e a passagem do VMware SR-IOV não são suportados.

O mesmo número de adaptadores de rede como origem no último backup

Selecione essa opção para definir como mapear NIC virtual para a rede virtual. Especifique essa opção quando a máquina virtual contiver NICs virtuais e uma rede virtual.

Desmarque a caixa de seleção para definir o nome da rede virtual que deseja que a NIC use para se comunicar.

Sistemas Hyper-V:

Aplique as opções a seguir da máquina virtual para sistemas Hyper-V:

Configurações básicas

Preencha as seguintes configurações básicas:

Prefixo do nome da VM

Especifique o prefixo que deseja adicionar ao nome de exibição da máquina virtual no sistema Hyper-V.

Valor padrão: UDPVM_

Contagem da CPU

Especifique a contagem de CPU mínima e máxima suportada pelo sistema virtual em modo de espera.

Memória

Especifique a quantidade total de RAM em MB a ser alocada para a máquina virtual em modo de espera.

Observação: a quantidade de RAM especificada deve ser um múltiplo de quatro.

Instantâneos do ponto de recuperação

Especifique o número de instantâneos dos pontos de recuperação para a máquina virtual no modo de espera. O número máximo de instantâneos dos pontos de recuperação é 24 para servidores de virtualização do Hyper-V.

Todos os discos virtuais compartilham o mesmo caminho

Selecione essa opção para especificar o local no servidor do Hyper-V no qual deseja armazenar os dados de conversão.

Desmarque a caixa de seleção para especificar o local no servidor do Hyper-V no qual deseja armazenar os dados de conversão de cada disco virtual.

Observação: a solução do Arcserve UDP não oferece suporte à criação de imagens de disco virtual (arquivos VHD/VHDX) em volumes compactados e em volumes que foram criptografados pelo sistema de arquivos. Se o caminho especificado residir em volumes compactados ou criptografados do Hyper-V, o Arcserve UDP impede a criação da tarefa do modo de espera virtual.

Rede da VM

Permite definir as NICs, redes virtuais e os caminhos que o servidor Hyper-V usa para se comunicar com as máquinas virtuais. Especifique uma das seguintes opções e preencha os campos solicitados.

O mesmo número de adaptadores de rede como origem no último backup

Selecione essa opção para definir como mapear NIC virtual para a rede virtual. Especifique essa opção quando a máquina virtual contiver NICs virtuais e uma rede virtual.

Desmarque a caixa de seleção para definir o nome da rede virtual que deseja que a NIC use para se comunicar.

6. Clique na guia **Avançado** e forneça os seguintes detalhes:

Iniciar a máquina virtual automaticamente

Especifique se deseja iniciar a máquina virtual automaticamente.

Observação: essa opção não está disponível para os nós de máquina virtual com base em host e nós replicados a partir de um servidor de ponto de recuperação remota e a origem da tarefa no modo de espera virtual é aquela replicada para um local diferente.

Timeout

Especifique o tempo que o servidor de monitoramento deve aguardar por um sinal de monitoramento antes de ligar o instantâneo do ponto de recuperação.

Frequência

Especifique a frequência com que o servidor de origem fará a comunicação dos sinais de monitoramento para o servidor de monitoramento.

Exemplo: o valor de tempo limite especificado é 60. O valor de frequência especificado é 10. O servidor de origem comunicará sinais de monitoramento em intervalos de 10 segundos. Se o servidor de monitoramento não detectar um sinal de monitoramento em 60 segundos do último sinal detectado, ele ligará a máquina virtual usando o instantâneo do ponto de recuperação mais recente.

Ativar alertas por email

Permite receber alertas por email de acordo com as configurações que você fornecer. Quando essa opção for selecionada, outras categorias de alertas por email são ativadas para a seleção.

- **Sinal de monitoramento faltando para a máquina de origem** – o modo de espera virtual envia notificações de alerta quando o servidor de monitoramento não detecta um sinal de monitoramento no servidor de origem.

  Observação: para nós de Replicar a partir de um servidor de ponto de recuperação remoto ou se a origem da tarefa do modo de espera virtual for aquela que é replicada para um site diferente, essa opção não estará disponível.

- **VM ligada para a máquina de origem configurada para ser ligada automaticamente** – o modo de espera virtual envia notificações de alerta quando ele liga uma máquina virtual que foi configurada para ligar automaticamente quando um sinal de monitoramento não é detectado.

  Observação: para nós de Replicar a partir de um servidor de ponto de recuperação remoto ou se a origem da tarefa do modo de espera virtual for aquela que é replicada para um site diferente, essa opção não estará disponível. Essa opção também não está disponível para os nós da máquina virtual com base em host.

- **VM ativada para máquina de origem configurada para ligar manualmente** – o modo de espera virtual envia notificações de alerta quando ativa uma máquina virtual manualmente.
- **Erros/falhas/paralisação no modo de espera virtual** – o modo de espera virtual envia notificações de alerta quando detecta um erro que ocorreu durante o processo de conversão.
- **Operação do modo de espera virtual realizada com êxito** – o modo de espera virtual envia notificações de alerta quando detecta que uma máquina virtual foi ligada com êxito.
- **O modo de espera virtual não foi iniciado com êxito a partir do instantâneo do ponto de recuperação** – o modo de espera virtual envia notificações de alerta quando detecta que uma máquina virtual não foi ligada automaticamente e a opção de início automático da recuperação de substituição da máquina virtual é especificada.
- **O hipervisor não está acessível** – o modo de espera virtual envia notificações de alerta quando detecta que ele não pode se comunicar com o sistema do Servidor ESX ou com o sistema Hyper-V.
- **Espaço livre de armazenamento da VM abaixo de** – o modo de espera virtual envia notificações de alerta quando detecta espaço livre em disco insuficiente no caminho definido pelo hipervisor. A detecção ocorre quando a quantidade de espaço livre em disco é menor do que o limite definido pelo usuário. O limite máximo pode ser representado como um valor absoluto (em MB) ou uma porcentagem da capacidade do volume.

7. Clique em **Salvar**.

   As alterações são salvas e a tarefa no modo de espera virtual é automaticamente implantada no servidor do modo de espera virtual.

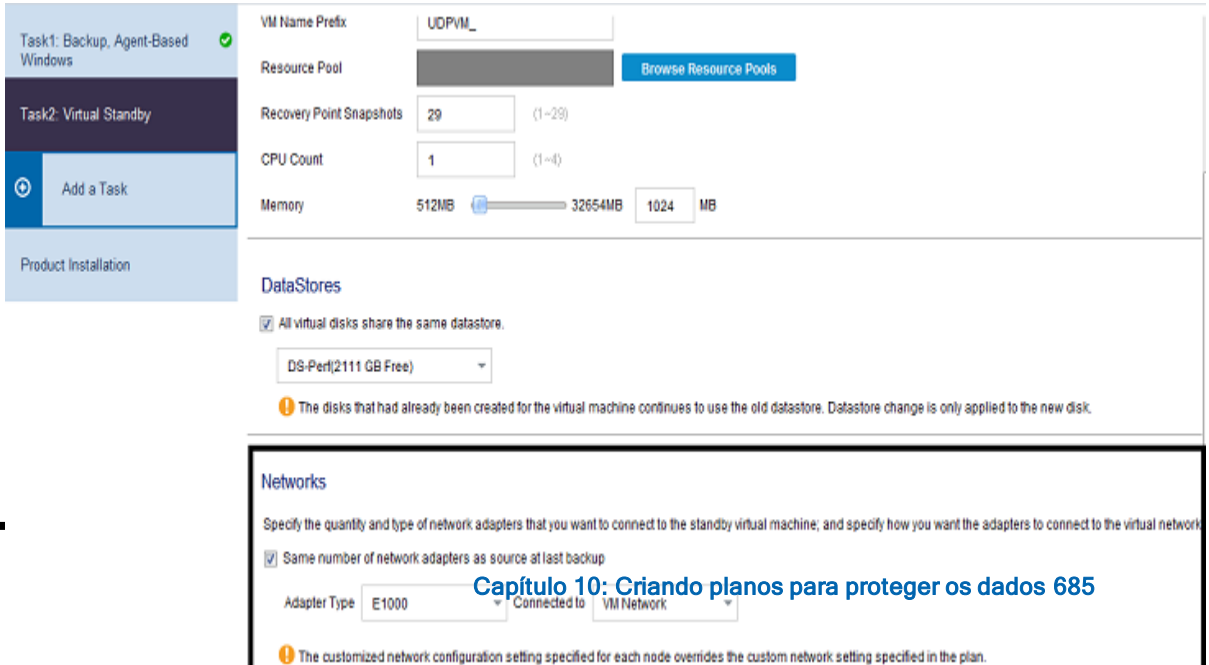
   Você criou com êxito e implantou o plano no modo de espera virtual.

Como o aplicativo determina a quantidade de NICs a ligar

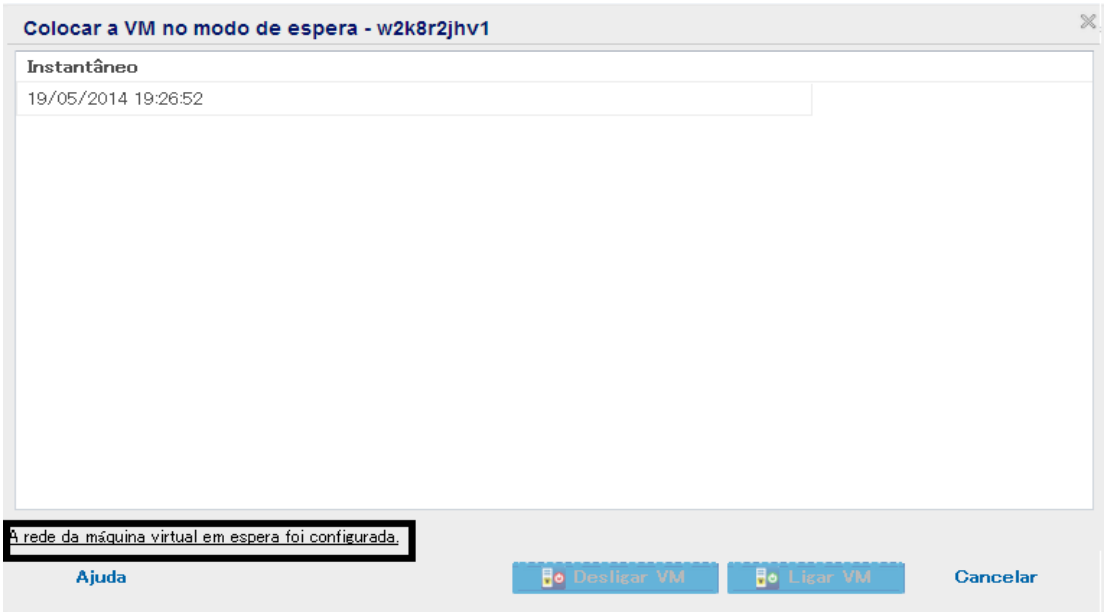
Ao ligar máquinas virtuais, o Modo de espera virtual determina a quantidade de NICs (Network Interface Cards – Placas de Interface de Rede) a serem ligadas se a rede de máquina virtual em modo de espera estiver configurada. A tabela a seguir ilustra como o Modo de espera virtual determina a quantidade de NICs necessária para ligar as máquinas virtuais:

Valores definidos no plano da rede da VM	A opção Ligar máquina virtual em modo de espera com configurações de rede personalizadas não está especificada	A opção Ligar máquina virtual em modo de espera com configurações de rede personalizadas está especificada
Os valores definidos são os mesmos do computador de origem.	O Modo de espera virtual liga a quantidade de NICs definida para a máquina de origem a partir da última tarefa de backup.	O Modo de espera virtual liga a quantidade de NICs com base no maior destes valores: ■ A quantidade definida na configuração de rede personalizada. ■ A quantidade de NICs definida para a máquina de origem desde a última tarefa de backup.
Os valores definidos são valores personalizados.	O Modo de espera virtual liga a quantidade de redes personalizadas definida no plano.	O Modo de espera virtual liga a quantidade de NICs com base no maior destes valores: ■ A quantidade definida na configuração de rede personalizada. ■ A quantidade de NICs definida para a diretiva personalizada.

A caixa de diálogo a seguir (Tarefa Editar no modo de espera virtual de Modificar um plano), na tarefa no modo de espera virtual, consiste em configurações personalizadas de NICs a serem ativadas:



A caixa de diálogo a seguir (Colocar a VM no modo de espera - <nome do host>) ilustra o local onde você deve especificar a opção Ligar máquina virtual em modo de espera com configurações de rede personalizadas:

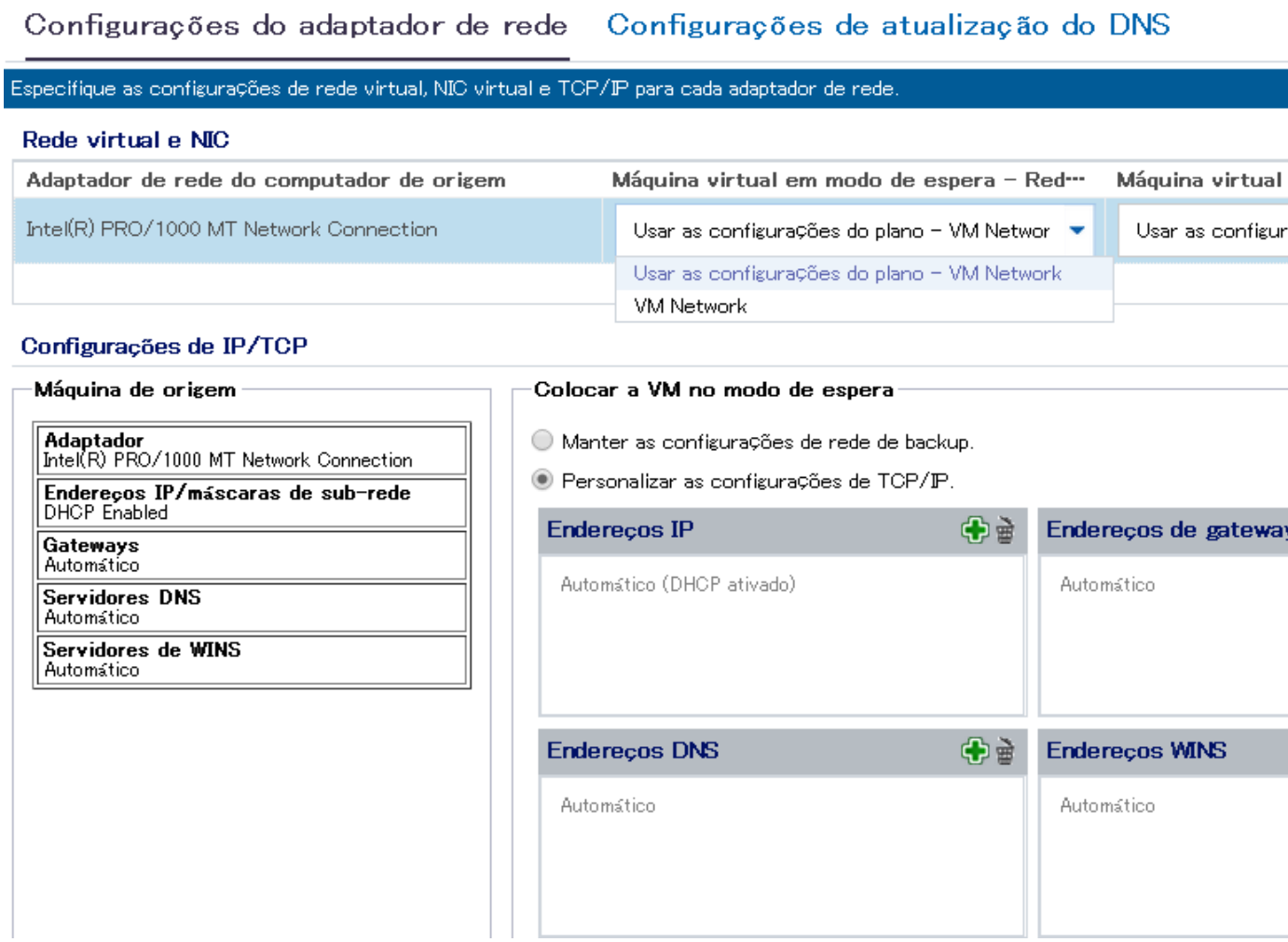


Configurar a rede da VM no modo de espera

É possível acionar a VM no modo de espera com configurações de rede personalizadas. É possível definir as seguintes configurações de rede na VM no modo de espera:

- Especifique a rede virtual e a NIC (Network Interface Card – Placa de Interface de Rede), e as configurações TCP/IP de cada adaptador de rede na guia **Configurações do adaptador de rede**.
- Atualize os servidores DNS para redirecionar clientes do computador de origem para as máquinas virtuais no modo de espera virtual com base nas configurações TCP/IP na guia **Configurações de atualização de DNS**.

O diagrama a seguir mostra a guia **Configurações do adaptador de rede** da **Configuração de rede da máquina virtual no modo de espera**:



Siga estas etapas:

1. Na guia **Recursos**, navegue até o grupo de nós do **Modo de espera virtual**.

   Os nós no Modo de espera virtual são exibidos no painel central.

2. No painel central, selecione o nó e clique em **Configuração de rede da máquina virtual no modo de espera**.

   A página Configuração de rede da máquina virtual no modo de espera – <nome do nó> é exibida.

3. Na guia **Configurações do adaptador de rede**, selecione a rede virtual na lista **Máquina virtual em modo de espera – Rede virtual**.

4. Selecione o tipo de NIC na **Máquina virtual em modo de espera – Tipo de NIC**.

5. Selecione **Personalizar as configurações de TCP/IP**.

6. Clique no botão **Adicionar endereço** e adicione **endereços IP**, **Endereços de gateway**, **Endereços DNS** e **endereços WINS**.

   Observação: se você adicionar **endereços DNS**, deverá configurar os servidores DNS na guia **Configurações de atualização do DNS**.

7. Clique em **Salvar**.

   A página Configuração de rede da máquina virtual no modo de espera – <nome do nó> é fechada.

   É configurada a rede da máquina virtual no modo de espera.

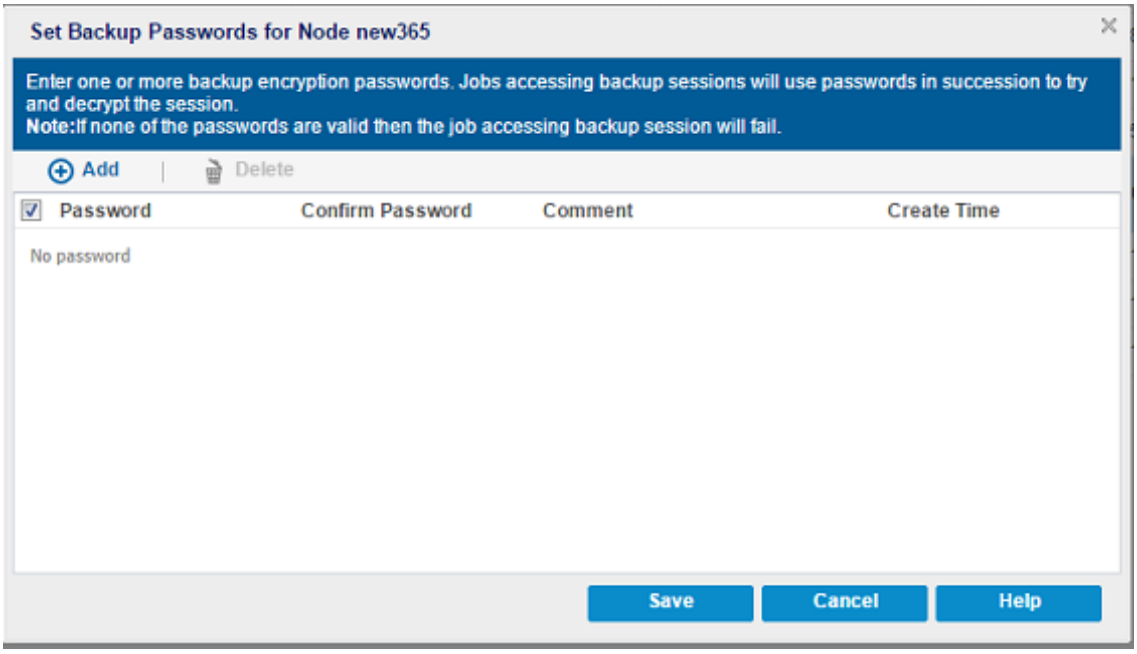
Definir senhas de backup para um ou mais nós

Para garantir que o conversor possa converter os pontos de recuperação replicados, o modo de espera virtual permite especificar senhas de backup para os dados que o conversor pode usar para converter os dados.

Siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.
3. No painel central, clique com o botão direito do mouse no nó e clique em **Definir senhas de backup**.

   A caixa de diálogo **Definir senhas de backup para o nó** será exibida.

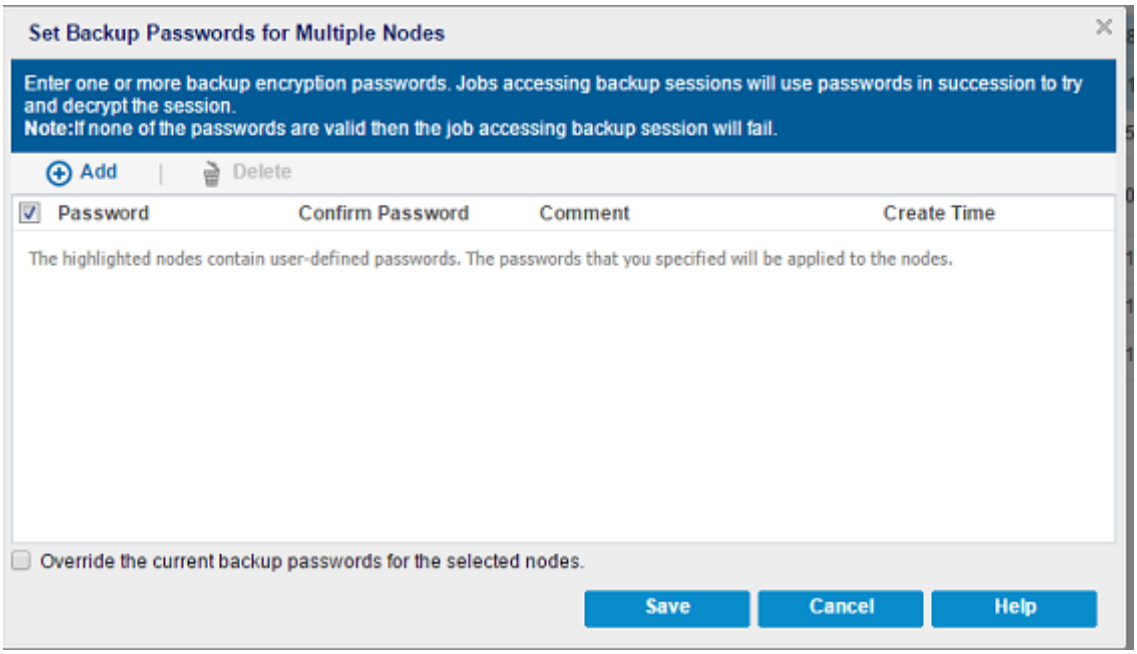


4. Execute as seguintes tarefas para um ou mais nós, na caixa de diálogo **Definir senhas de backup**:

   Adicionar – clique em **Adicionar** para adicionar uma ou mais senhas de backup aos nós selecionados.

   Excluir – clique em **Excluir** para excluir uma ou mais senhas de backup dos nós selecionados.

   Observação: é possível substituir as senhas de backup atuais de vários nós marcando a caixa de seleção **Substituir as senhas de backup atuais** dos nós selecionados.



5. Clique em **Salvar**.

   A caixa de diálogo é fechada, e as senhas de backup são definidas para os nós remotos selecionados.

(Opcional) Execute a tarefa no modo de espera virtual manualmente

Para executar manualmente uma tarefa no modo de espera virtual, você deverá primeiro executar um backup manual. A tarefa no modo de espera virtual está associada a uma tarefa de backup. Se um plano incluir uma tarefa de backup e uma tarefa no modo de espera virtual e você executar a tarefa de backup manualmente, a tarefa do modo de espera virtual será executada automaticamente após a conclusão da tarefa de backup.

Siga estas etapas:

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.

   Exibe os planos que você adicionou.
3. Selecione os nós dos quais deseja fazer backup. O nó selecionado deve ter atribuído um plano.
4. No painel central, clique em **Ações**, **Fazer backup agora**.

   A caixa de diálogo **Fazer backup agora** é exibida.
5. Selecione o tipo de backup e forneça um nome para a tarefa de backup.
6. Clique em **OK**.

   A tarefa de backup é executada.

   A tarefa no modo de espera virtual é executada imediatamente após a tarefa de backup ser concluída.

   A tarefa no modo de espera virtual é executada manualmente.

Pausar e retomar sinal de monitoramento

A solução Arcserve Unified Data Protection permite pausar e retomar os sinais de monitoramento detectados pelo servidor de monitoramento. O sinal de monitoramento é o processo em que o servidor de origem e o servidor de monitoramento se comunicam sobre a integridade do servidor de origem. Se o servidor de monitoramento não detectar um sinal de monitoramento após um determinado período de espera, o recurso do Modo de espera virtual configura a máquina virtual para funcionar como o nó de origem.

Exemplos: quando pausar ou retomar sinais de monitoramento

Os exemplos a seguir descrevem quando pausar e retomar sinais de monitoramento:

- Pause o sinal de monitoramento quando quiser colocar offline um nó (servidor de origem) para manutenção.
- Retome o sinal de monitoramento após as tarefas de manutenção serem concluídas e o nó (servidor de origem) estar online.

Esteja ciente do seguinte:

- É possível pausar e retomar os sinais de monitoramento no nível de grupo ou no nível de nó individual.
- Você pode pausar e retomar os sinais de monitoramento para um ou mais nós em uma única etapa.
- A solução Arcserve Unified Data Protection não liga instantâneos de pontos de recuperação enquanto o sinal de monitoramento estiver no estado pausado.
- Ao atualizar as instalações do agente em nós de origem, o Arcserve Unified Data Protection pausa o sinal de monitoramento dos nós. Para garantir que os servidores de monitoramento monitorem os nós atualizados, retome o sinal de monitoramento dos nós após concluir a atualização nos nós.

Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection.
2. Clique na guia **Recursos**.
3. No painel à esquerda, vá até o **Modo de espera virtual** e clique em **Todos os nós**.

   Se você tiver adicionado alguns nós, os nós serão exibidos no painel central.
4. Selecione o nó que deseja pausar ou retomar.
5. No painel central, clique em **Ações**, **Sinal de monitoramento**, **Pausar** ou **Retomar**.

   O sinal de monitoramento do nó selecionado é pausado ou retomado.

Pausar e retomar a tarefa do modo de espera virtual

A conversão virtual é o processo em que o recurso do modo de espera virtual converte pontos de recuperação do Arcserve Unified Data Protection de nós de origem em formatos da máquina virtual, denominados instantâneos do ponto de recuperação. No caso de um servidor de origem falhar, o recurso de Modo de espera virtual usa os instantâneos de pontos de recuperação para ligar uma máquina virtual no nó de origem.

Como prática recomendada, permita que o processo de conversão virtual opere continuamente. No entanto, se deseja pausar o processo de conversão virtual nos servidores no modo de espera virtual local ou remoto temporariamente, pode fazê-lo no Console. Depois de corrigir os problemas no nó de origem, você pode continuar o processo de conversão virtual.

Quando você faz uma pausa nas tarefas do Modo de espera virtual (tarefas de conversão), a operação de pausa não pausa a tarefa de conversão que está em andamento no momento. A operação de pausa aplica-se somente à tarefa que está aguardando para ser executada no final da próxima tarefa de backup. Como resultado, a próxima tarefa de conversão não é iniciada até que você retome explicitamente a tarefa de conversão (pausada).

Se continuar o modo de espera virtual dos nós e se houver várias sessões de backup sem instantâneo do ponto de recuperação, será exibida uma caixa de diálogo para selecionar a opção de cópia inteligente. Se clicar em Sim, a tarefa em modo de espera virtual poderá converter a sessão combinada em um único instantâneo do ponto de recuperação. Se clicar em Não, a tarefa em modo de espera virtual poderá converter cada sessão individualmente

Observação: como alternativa, é possível pausar e retomar tarefas do Modo de espera virtual diretamente nos nós. Para obter mais informações, consulte o tópico Pausar e retomar tarefas do Virtual Standby nos nós.

Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection.
2. Clique na guia **Recursos**.
3. No painel à esquerda, vá até o **Modo de espera virtual** e clique em **Todos os nós**.

   Se você tiver adicionado alguns nós, os nós serão exibidos no painel central.
4. Selecione o nó que deseja pausar ou retomar.

5. No painel central, clique em **Ações**, **Modo de espera virtual**, **Pausar** ou **Retomar**.

   A função do modo de espera virtual para o nó selecionado é pausada ou retomada.

Verificar o plano

Para verificar seu recurso no modo de espera virtual, verifique se você criou com êxito o plano no modo de espera virtual. Depois de verificar se o plano está criado com êxito, confirme se a tarefa de backup está executando conforme o programado. Depois que a tarefa de backup for concluída com êxito, a tarefa em modo de espera virtual será executada. É possível verificar o status da tarefa de backup e da tarefa no modo de espera virtual na guia **tarefas**.

Siga estas etapas para verificar os planos:

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.

   Uma lista de todos os nós é exibida no painel central.
3. Verifique se os planos são mapeados com nós.

Siga estas etapas para verificar as tarefas no modo de espera virtual:

1. Clique na guia **tarefas**.
2. No painel à esquerda, clique em **Todas as tarefas**.

   O status de cada tarefa é incluído no painel central.
3. Verifique se a tarefa de backup e a tarefa no modo de espera virtual foi bem-sucedida.

   O plano para modo de espera virtual é verificado com êxito.

   O computador no modo de espera virtual é criado.

Como criar um plano de recuperação garantida

Para verificar a acessibilidade e garantir a recuperação dos dados, é necessário criar um plano de recuperação garantida. O plano de recuperação garantida baseia-se em um plano de backup/replicação. Essa tarefa de recuperação permite adicionar uma tarefa de recuperação garantida a um plano de replicação ou de backup existente. A tarefa de recuperação garantida inclui uma origem, configurações de teste, programação e configurações avançadas. Você também pode executar uma tarefa de recuperação garantida manualmente.

O que fazer a seguir?

1. Verificar os pré-requisitos e as considerações
2. Adicionar uma tarefa de recuperação garantida a um plano
3. (Opcional) Executar a tarefa do teste de recuperação garantida manualmente

Verificar os pré-requisitos e as considerações

Estas tarefas de pré-requisito devem ser concluídas:

- Efetue logon no Console.
- Instalar o componente do servidor e criar repositórios de dados caso deseje armazenar os dados de backup em servidores de ponto de recuperação.
- Você tem um ponto de recuperação válido para criar uma máquina virtual instantânea ou um disco virtual instantâneo. Você pode selecionar os pontos de recuperação por uma das seguintes tarefas:
  - Backup, Windows com base em agente
  - Backup, sem agente com base em host
  - Replicar
  - Backup, Office 365 Exchange Online
  - Backup, Office 365 OneDrive
  - Backup, Office 365 SharePoint Online
  - Backup, arquivos no caminho UNC ou NFS
  - Backup, Linux com base em agente
- Verifique se os agentes do Arcserve UDP já estão instalados no servidor proxy.
- Verifique se o sistema operacional do servidor proxy é o Windows Server 2008 R2 de 64 bits ou posterior.

  Observação: para o plano de backup de caminho UNC e o plano de backup do Office 365 (Exchange Online, OneDrive, SharePoint Online), o servidor proxy de recuperação garantida deve ser do Windows 2012 ou posterior.
- Verifique se o servidor proxy tem espaço suficiente para a máquina Virtual instantânea ou o disco virtual instantâneo.

  Observação: o espaço necessário depende altamente do tamanho da memória RAM que você configurou na tarefa de AR para o tipo de teste de AR IVM. Para cada IVM, o hipervisor precisa ter, no máximo, o mesmo tamanho da memória RAM para armazenar dados temporários em arquivos de troca de memória. Por exemplo, se você tiver 5 nós no mesmo plano com a tarefa AR IVM e o tamanho da memória da VM for definido como 4 GB, então você precisará de pelo menos 5 * 4 = 20 GB de memória livre para armazenar os arquivos de troca de memória. Além disso, talvez você precise de um espaço livre de 10 MB para armazenar os arquivos de configuração da VM.

- Verifique se a versão do sistema operacional Windows no servidor proxy de recuperação garantida é igual ou superior à versão do sistema operacional Windows na VM de origem.

Adicionar ao plano uma tarefa de recuperação garantida

Uma tarefa de recuperação garantida inclui uma tarefa de recuperação garantida para um existente plano de backup/replicação. Cada tarefa consiste em parâmetros que definem a origem, as configurações de tarefa, a programação e as configurações avançadas. Crie uma tarefa de recuperação garantida com base na tarefa de backup/replicação para verificar a acessibilidade e a recuperação garantida dados e fornecer a verificação de integridade de dados.

Siga estas etapas:

1. Clique na guia de **recursos** no Console.
2. No painel à esquerda, navegue para **Planos** e clique em **Todos os planos**.

   Se tiver criado os planos anteriores, esses planos serão exibidos no painel central.
3. No painel central, abra um plano de replicação ou de backup existente.
4. No painel selecionado, clique em **Adicionar uma tarefa** no painel esquerdo.
5. (Opcional) Selecione a caixa de seleção **Pausar este plano**.

   O plano não será executado até que você desmarque a caixa de seleção para retomar o plano.

   Observação: se você pausar o plano, a tarefa Recuperação garantida não iniciará. Ao retomar o plano novamente, a tarefa Recuperação garantida não é retomada automaticamente. É necessário executar manualmente outra tarefa de backup para iniciar a tarefa Recuperação garantida.
6. Na lista suspensa **Tipo de tarefa**, selecione **Teste de recuperação garantida**.
7. Agora, especifique a Origem, as configurações da tarefa (IVM ou IVD), a Programação e os detalhes Avançados.
8. Clique em **Salvar.**

   As alterações são salvas e a tarefa de recuperação garantida é automaticamente implantada.

Especificar a origem

A guia Origem permite especificar o ponto de recuperação de origem que você deseja proteger.

Siga estas etapas:

1. Clique na guia **Origem**.
2. Clique na lista suspensa da Origem do ponto de recuperação para o Teste de recuperação garantida e selecione a opção desejada.
3. Selecione os tipos de pontos de recuperação para o teste de recuperação garantida. É possível selecionar qualquer uma das duas opções a seguir:
   - Teste de recuperação garantida a partir dos tipos de backup selecionados

     Você pode selecionar Backups diários, Backups semanais ou Backups mensais. As opções de backup diário, semanal ou mensal são ativadas de acordo com a programação do backup de origem. Por exemplo, se o backup de origem tiver somente o backup mensal programado, o teste de recuperação garantida da opção de tipos de backup selecionados terá somente backups mensais ativados.
   - Teste de recuperação garantida a partir dos pontos de recuperação mais recentes

A origem é especificada

Especificar a configuração de tarefa do Tipo de teste – Máquina virtual instantânea

A seleção da IVM (Instant Virtual Machine - Máquina Virtual Instantânea) como o Tipo de Teste permite iniciar a máquina virtual a partir do ponto de recuperação e, opcionalmente, executa o script personalizado. Considera-se que o ponto de recuperação está em bom estado se a VM for inicializada com êxito, e o script de verificação retorna resultado com êxito no intervalo de tempo especificado pelo usuário.

Observação: essa etapa não é necessária se você estiver selecionando **Disco virtual instantâneo** como Tipo de teste.

Você pode selecionar um tipo de hipervisor no VMware vSphere e no Microsoft Hyper-V e digitar os detalhes das configurações de proxy e as configurações da VM para especificar a configuração de tarefa para a IVM.

Siga estas etapas:

1. selecione **Máquina virtual instantânea** como tipo de teste.

   Observação: quando a tarefa de origem for backup/replicação do Linux com base em agente, a opção de máquina virtual instantânea será o único tipo de teste suportado.

2. selecione uma das opções do hipervisor e insira os detalhes relacionados:

   VMware vSphere

   Observação: se a configuração da tarefa de AR for IVM para vSphere, a licença do VMware necessária será semelhante ao recurso necessário da VM instantânea.

   a. Execute uma das opções a seguir para fornecer um servidor vCenter/ESX(i):

      - Se você já tiver adicionado um nó da VMware ao site selecionado no console, selecione o nó a partir da lista suspensa Servidor do vCenter/ESX(i).
      - Se você não tiver adicionado nós VMware, clique em **Adicionar**.

        A caixa de diálogo **Especificar destino da VM** é aberta.
      - Especifique os detalhes da máquina virtual e clique em OK.

        Todos os pools de recursos ou ESX(i) são exibidos no painel central da página Local da VM.

   b. Selecione uma das opções a partir do ESX(i), agrupamento, pool de recursos ou aplicativo virtual como o local.

A máquina VMware vSphere é especificada.

Observação: se a tarefa de origem for backup/replicação do Linux com base em agente ou com base em host sem agente, especifique o repositório de dados do servidor ESX(i).

Selecionar o Microsoft Hyper-V

Execute uma das opções a seguir para fornecer o Microsoft Hyper-V:

- Se você já tiver adicionado um nó do Hyper-V para o local selecionado no Console, selecione na lista suspensa Servidor/Agrupamento do Hyper-V.
- Se você não tiver adicionado nós do Hyper-V, clique em **Adicionar**.

  A caixa de diálogo Especificar destino da VM é aberta.

  Observação: ao se conectar à VM instantânea do Hyper-V usando uma conta de administrador não integrado local, o UAC remoto precisa ser desativado. Para obter mais informações sobre como desativar o UAC remoto para administrador não integrado, consulte Como desativar o UAC remoto para um administrador não integrado.
- Especifique os detalhes do servidor Hyper-V e clique em **OK**

A máquina virtual do Hyper-V é especificada.

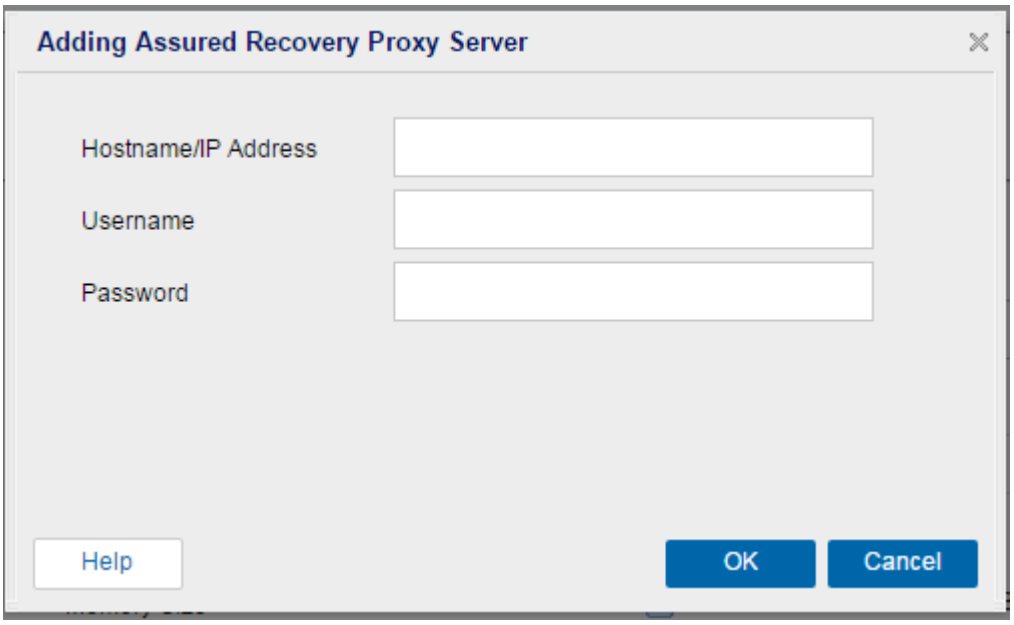
Especificar Nutanix AHV

Esse recurso destina-se apenas ao suporte à VM do Linux. Para obter mais informações, consulte Protegendo uma máquina virtual instantânea no Nutanix AHV para o nó do Linux.

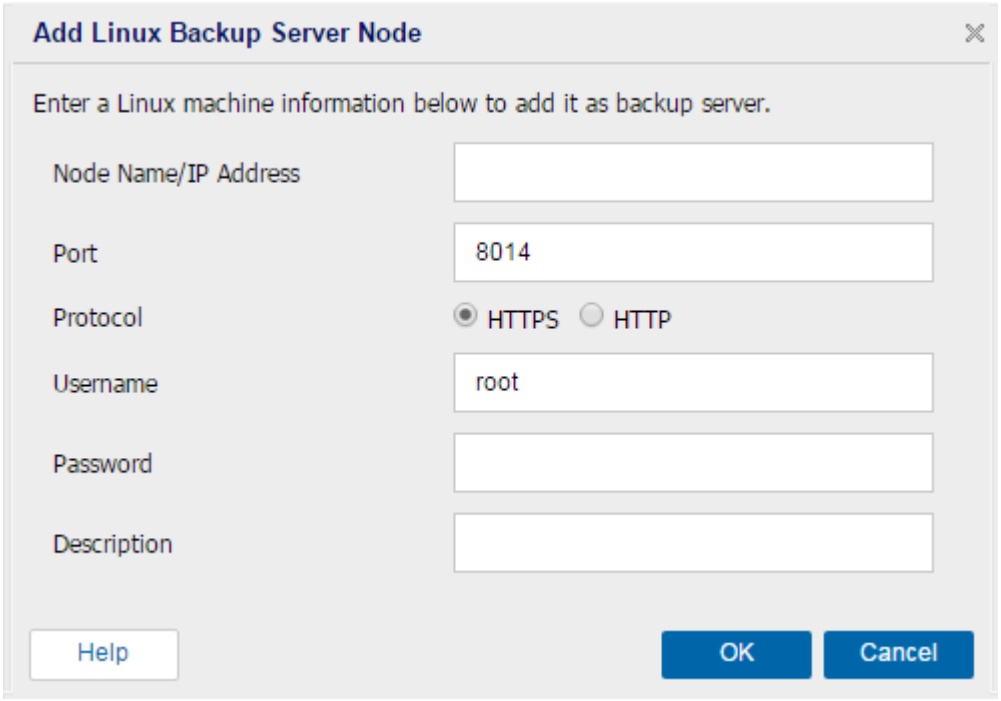
3. Execute uma das opções a seguir para fornecer o **Servidor proxy**:
   - Se você já tiver adicionado um nó de proxy ao site selecionado no console, selecione o nó na lista suspensa do servidor proxy.
   - Se você não tiver adicionado nós de proxy, clique em **Adicionar**.

     A caixa de diálogo **Adicionar servidor proxy de recuperação garantida** é exibida.

     Para o servidor proxy do Windows



Para o servidor proxy do Linux



- Especifique os detalhes do servidor proxy
- Clique em **OK**.

Os nós são exibidos na lista **Nós disponíveis**.

Observações:

- você só precisa selecionar um servidor proxy quando o hipervisor é o VMware vSphere.

- Quando o hipervisor é o VMware vSphere, a função NFS (Network File System - Sistema de arquivos de rede) do Windows deve ser instalada no servidor de ponto de recuperação. O processo da VM instantânea instalará automaticamente o NFS. Para instalar o sistema de arquivos de rede manualmente, consulte o tópico Como instalar manualmente o sistema de arquivos de rede em um servidor Windows.
- Selecione servidores proxy com base nos tipos de nód selecionados incluídos no plano. Por exemplo, servidor proxy do Windows para o nó do Windows e servidor proxy Linux para o nó Linux.

4. (Opcional) Execute as seguintes etapas para especificar as configurações de gateway para a recuperação garantida.

   Observação: aplica-se apenas ao Linux.

   a. Usando as configurações de DHCP ou especifique o endereço IP, a máscara e o gateway padrão manualmente.

   b. Selecione uma rede virtual na lista suspensa.

   Observação: as configurações do gateway serão necessárias somente quando a origem do teste de recuperação garantida for backup/replicação do Linux com base em agente ou com base em host sem agente.

5. Especifique os detalhes das **Configurações da VM** da recuperação garantida.

   Prefixo do nome da VM

   Especifica o prefixo do nome da VM. O nome do nó de origem com um prefixo é o nome padrão da VM instantânea. Alguns caracteres especiais não são permitidos no nome, como '@', ' \' e assim por diante.

   Valor padrão: UDPARVM_

   Pasta dos arquivos da VM

   Especifique o local da pasta da VM da recuperação garantida no servidor proxy. Você pode procurar as informações de volume do servidor proxy.

   Contagem da CPU

   Especifica a quantidade de CPUs que pode ser necessária para a VM da recuperação garantida.

   Tamanho da memória

   Especifica o tamanho da memória que pode ser necessária para a VM da recuperação garantida.

   Configurações de rede

Especifica as configurações de rede na VM da recuperação garantida. É possível selecionar "Conectar a VM da recuperação garantida à rede" ou não. Também é possível usar as configurações de DHCP para a VM de recuperação garantida ou usar as configurações de TCP/IP da sessão de backup.

Tipo de adaptador

Especifica o tipo de adaptador na VM da recuperação garantida. O tipo de adaptador disponível pode variar de acordo com o hipervisor.

Especificar as configurações de tarefa para o tipo de teste – Disco virtual instantâneo

Selecionar o disco virtual instantâneo como o tipo de teste para as configurações de teste permite montar o ponto de recuperação como disco local, verifica a integridade do sistema de arquivos/volume e, opcionalmente, executa o script personalizado. O ponto de recuperação será considerado em bom estado se você montar o ponto de recuperação com êxito e todos os testes retornarem um resultado bem-sucedido.

Observação:

- esta etapa não é necessária se você estiver selecionando **Máquina virtual instantânea** como Tipo de teste.
- A opção **Disco virtual instantâneo** não oferece suporte a nós que não sejam do Windows.

Siga estas etapas:

1. Execute uma das etapas a seguir para fornecer um servidor para o **servidor proxy do Windows:**
   a. Selecione um dos nós disponíveis na lista suspensa.

      Observação: se já tiver adicionado um nó de proxy ao site selecionado no console, você poderá visualizar a lista de nós na lista suspensa **Servidor Proxy do Windows**.

   b. Se não tiver adicionado nenhum nó de proxy, execute as seguintes etapas:
      i. Clique em **Adicionar**.
      ii. A caixa de diálogo **Adicionar servidor proxy de recuperação garantida** é exibida.
      iii. Especifique os detalhes do servidor proxy e clique em **OK**.
2. **Procure** o local da pasta do disco rígido virtual no servidor proxy.

Especificar a programação de tarefas do teste de recuperação garantida

A guia de programação permite especificar a programação de tarefas do teste de recuperação garantida. Se não especificar uma programação, a tarefa será iniciada imediatamente quando você executar a tarefa principal.

Siga estas etapas:

1. Clique na guia **Programar**.
2. Clique em **Adicionar** e, em seguida, **Adicionar programação de tarefas do teste de recuperação garantida**.

   A caixa de diálogo Adicionar programação de tarefas do teste de recuperação garantida é exibida.
3. Especifique a programação e clique em **Salvar**.

   A caixa de diálogo é fechada e o guia de programação exibe o especificado.

   Observações:

   - Se a origem de recuperação garantida for Pontos de recuperação mais recentes + Ativar programação de recuperação garantida, o valor padrão é 1. Como resultado, por padrão, a mais recente é verificada.

     Para o valor <=0, todos os pontos de recuperação não verificados são testados.
   - Se a origem de recuperação garantida for Diário/semanal/mensal + Ativar programação de recuperação garantida, o valor padrão é 9 (7 diárias + 1 semanal + 1 mensal).

     Para o valor <=0, todos os pontos de recuperação não verificados são testados.
   - Se não desejar usar o valor padrão, é possível adicionar uma chave de Registro DWORD de 32 bits no seguinte local:

     HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AssuredRecovery\MaxNumberOfRecoveryPoint

Especificar as configurações avançadas

A guia Avançado ajuda aplicar outras configurações necessárias para a conclusão do plano. Isso é opcional se você não precisar adicionar mais configurações. Algumas das opções que podem ser visualizadas na guia **Avançado** variam de acordo com a seleção na guia anterior. Por exemplo, a opção Propriedades do sinal de monitoramento fica visível somente se você tiver selecionado a máquina virtual instantânea como o Tipo de teste nas **Configurações de teste**.

Propriedades do sinal de monitoramento

Observação: a opção fica visível somente se você tiver selecionado a máquina virtual instantânea como o tipo de teste.

Timeout

Especifica o tempo máximo que o servidor proxy pode aguardar pelo sinal de monitoramento da VM da recuperação garantida. Se a VM da recuperação garantida não estiver disponível por mais tempo que o tempo limite definido, a tarefa de teste da recuperação garantida falhará.

Frequência

Especifica a frequência com a qual o servidor proxy verifica o status de sinal de monitoramento da VM da recuperação garantida.

Observação: Essa opção não será exibida se você selecionou backup/-replicação do Linux com base em agente como origem do ponto de recuperação do teste de recuperação garantida.

Pontos de verificação

Observação: a opção fica visível somente se você tiver selecionado o disco virtual instantâneo como o tipo de teste.

Verificar o sistema de arquivos

Verifica se o sistema de arquivos e o tamanho do volume são semelhantes ao que a máquina de origem tem.

Executar o comando de verificação de disco

Verifica a integridade dos dados executando o comando de verificação de disco nos volumes expostos pelo disco virtual instantâneo.

Local de comando personalizado no proxy

Observação: Essa opção não será exibida se você selecionou backup/replicação do Linux com base em agente como origem do ponto de recuperação do teste de recuperação garantida.

Especifica o script personalizado armazenado no servidor proxy. Você pode procurar as informações de volume do servidor proxy. Se o tipo de recuperação garantida da IVM estiver selecionado, o script é copiado na VM e executado quando a VM for inicializada. Se o tipo de recuperação garantida de IVHD estiver selecionado, o script é executado no servidor proxy.

Observação: a tarefa de recuperação garantida oferece suporte apenas ao script bat executável do Windows ou ao binário executável. Entretanto, essa limitação não restringe o uso da tarefa de recuperação garantida. É possível usar um script em lote do Windows criado para iniciar o script powershell, como o nome test.bat com o seguinte conteúdo:

Powershell.exe -NoProfile -ExecutionPolicy ByPass -Command "& '%ScriptPath%\AR-check.ps1'"

Além disso, os argumentos a seguir são transmitidos para o script de acordo com os requisitos.

- set PlanName=%1%

- set NodeName=%2%

- set ProxyServer=%3%

- set RecoveryPointName=%3%

- set MountPointRootPathName=%5% (aplicável apenas para o tipo de teste de disco virtual instantâneo)

Como resultado, o bat é invocado e executado da seguinte maneira:

Para o tipo de teste de máquina virtual instantânea:

"%ScriptPath%\test.bat PlanName NodeName ProxyServer RecoveryPointName

Para o tipo de teste de disco virtual instantâneo:

%ScriptPath%\test.bat PlanName NodeName ProxyServer RecoveryPointName MountPointRootPathName

Código de saída

Especifica o código de saída para a Tarefa bem-sucedida ou a Tarefa com falha.

Tarefa bem-sucedida

Especifica que a tarefa de recuperação garantida está definida como Bem-sucedida quando o script retorna o código de saída.

Tarefa com falha

Especifica que a tarefa de recuperação garantida está definida como Com falha quando o script retorna o código de saída.

Tarefa com falha se executada por mais tempo

Especifica se o script é executado por mais tempo que as vezes especificadas.

Valor padrão: 15 minutos.

Configuração de scripts anteriores/posteriores Linux no proxy

Observação: essa opção fica visível somente se tiver selecionado backup/-replicação do Linux com base em agente ou com base em host sem agente como a origem do ponto de recuperação do teste de recuperação garantida.

Executar no servidor de backup Linux após a conclusão da tarefa de recuperação garantida

Especifica o script localizado no proxy Linux que é executado após a conclusão da tarefa de recuperação garantida no servidor de backup Linux.

Executar em VM de recuperação garantida após inicialização da VM de recuperação garantida

Especifica o script localizado no proxy Linux que é executado após a VM de recuperação garantida ter sido inicializada na VM de recuperação garantida.

Tarefa com falha se executada por mais tempo

Especifica se o script é executado por mais tempo que as vezes especificadas.

Alertas por email

Permite ativar alertas por email. É possível especificar configurações de email e os tipos de alertas que você deseja receber por email. Ao selecionar esta opção, as seguintes opções serão ativadas para a seleção.

Observações: Não está disponível para tarefas sendo executadas com o servidor de backup Linux.

Configurações de email

Permite configurar as definições de email. Clique em **Configurações de email** e na caixa de diálogo **Configurações de email** configure os detalhes do servidor de email e do servidor proxy.

Definir senhas de backup para um ou mais nós

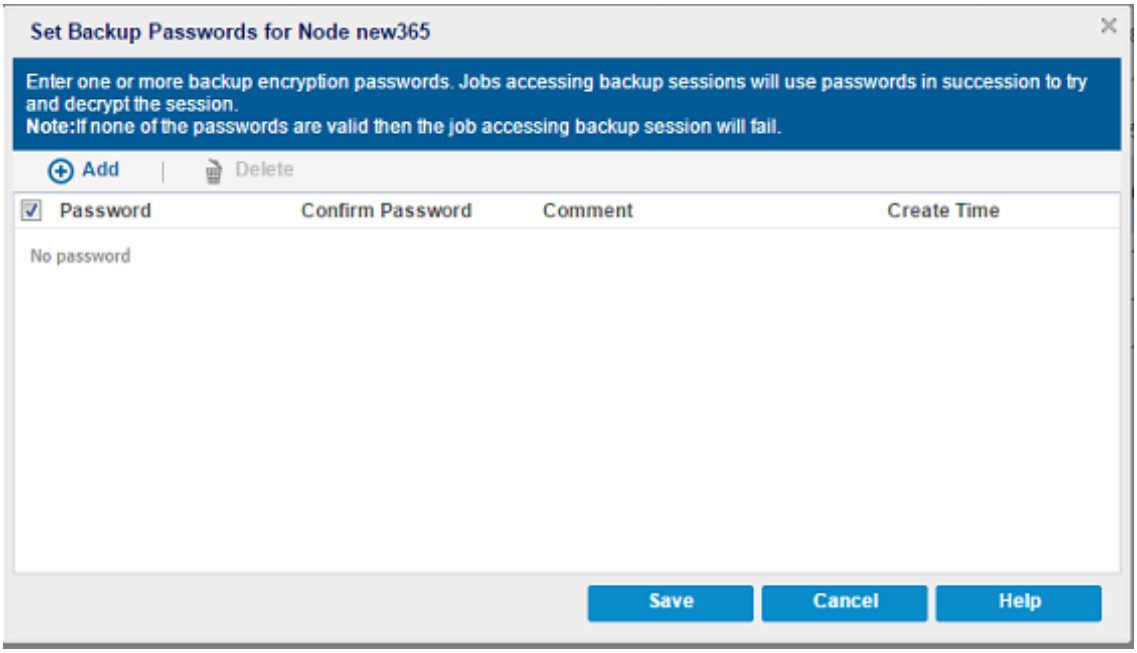
Para garantir que a tarefa de Recuperação garantida possa testar os pontos de recuperação replicados, a recuperação garantida permite que você especifique senhas de backup para os dados. Tarefas que acessam sessões de backup usam senhas continuamente para descriptografar a sessão.

Observação: se nenhuma das senhas for válida, a tarefa que estiver acessando a sessão de backup apresentará falha.

Siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.
3. No painel central, clique com o botão direito do mouse no nó e clique em **Definir senhas de backup**.

   A caixa de diálogo **Definir senhas de backup para o nó** será exibida.

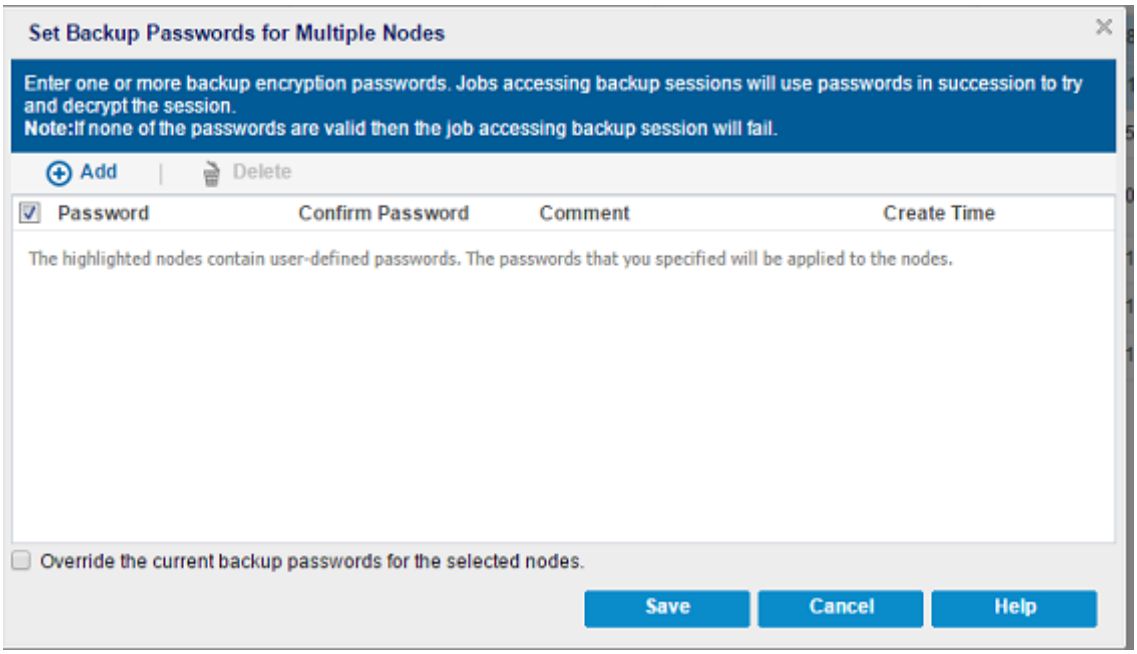


4. Execute as seguintes tarefas para um ou mais nós, na caixa de diálogo **Definir senhas de backup**:

   Adicionar – clique em **Adicionar** para adicionar uma ou mais senhas de backup aos nós selecionados.

   Excluir – clique em **Excluir** para excluir uma ou mais senhas de backup dos nós selecionados.

Observação: é possível substituir as senhas de backup atuais de vários nós marcando a caixa de seleção **Substituir as senhas de backup atuais** dos nós selecionados.



5. Clique em **Salvar**.

   A caixa de diálogo é fechada, e as senhas de backup são definidas para os nós remotos selecionados.

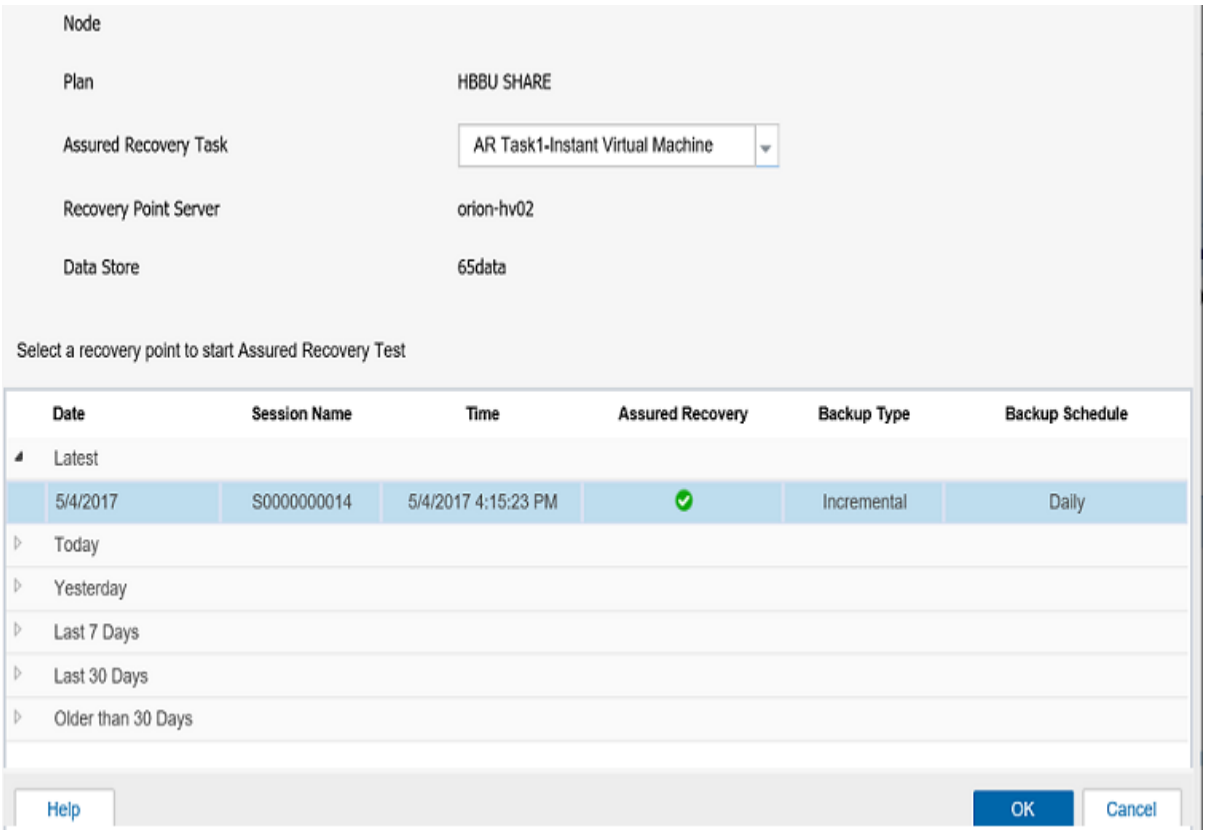
(Opcional) Executar a tarefa do teste de recuperação garantida manualmente

No Arcserve UDP, todos os planos, incluindo tarefas de recuperação garantida, são executados automaticamente e controlados pelas configurações de programação. Para tarefas de recuperação garantida, além da execução programada, o Arcserve UDP permite executar o teste manual de nós e planos para testar a recuperação garantida. Este tópico fornece procedimentos separados para executar um teste de recuperação garantida manual de nós e planos.

Siga estas etapas para executar um teste de recuperação garantida manual do nó:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para Nós e clique em **Todos os nós**.
3. No painel central, selecione os nós que tenham um plano de recuperação garantida atribuído e clique em **Ações**.
4. Entre as opções exibidas para Ações, clique em **Executar o teste de recuperação garantida agora**.

   A caixa de diálogo Recuperação garantida é exibida.



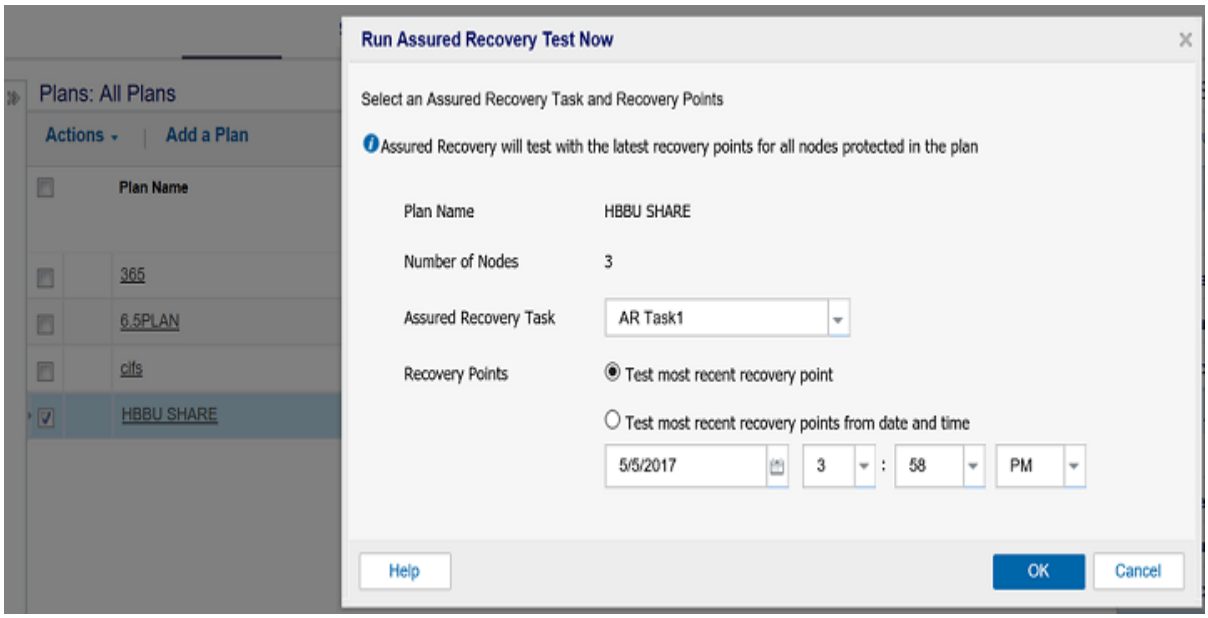
5. Selecione uma tarefa de recuperação garantida e um ponto de recuperação e clique em **OK**.

   O teste de recuperação garantida do nó é executado.

Siga estas etapas para executar um teste de recuperação garantida manual do plano:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para Planos e clique em **Todos os planos**.
3. No painel central, selecione um plano de recuperação garantida e clique em **Ações**.
4. Entre as opções exibidas para Ações, clique em **Executar o teste de recuperação garantida agora**.

   A caixa de diálogo Recuperação garantida é exibida.



5. Selecione uma tarefa de recuperação garantida e uma das opções para o ponto de recuperação e clique em **OK**.

   O teste de recuperação garantida do plano é executado.

Como criar um plano de backup de caminho UNC/NFS

Para proteger seus diretórios e arquivos localizados no caminho UNC/NFS, é necessário criar um plano. O plano do caminho UNC/NFS consiste em uma tarefa de backup. Esta tarefa de backup permite especificar os nós que deseja proteger, o destino do backup e a programação de backup. O destino do backup é um servidor de ponto de recuperação onde você deseja armazenar os dados de backup. O destino é uma pasta compartilhada remota. Para o caminho UNC/NFS, o tamanho máximo do backup é 128 TB.

O que fazer a seguir?

1. Verificar os pré-requisitos e as considerações
2. Criar um compartilhamento de arquivos
3. Criar um plano de backup
4. (Opcional) Executar um backup manual
5. Criar outras tarefas no plano do UNC/NFS
6. Verificar o backup

Verificar os pré-requisitos e as considerações

Estas tarefas de pré-requisito devem ser concluídas:

1. Efetuar logon no console.
2. Prepare um servidor proxy de backup do caminho UNC/NFS no qual o Agente do Arcserve Unified Data Protection para Windows esteja instalado.
3. Tenha credenciais de usuário com pelo menos permissão de leitura para o caminho UNC/NFS que você planeja proteger.

   Observação: para adicionar, atualizar e excluir um nó do caminho UNC/NFS, consulte Como adicionar e gerenciar o caminho UNC/NFS.
4. Tenha um servidor de ponto de recuperação com repositório de dados com redução de redundância ou sem redução de redundância.
5. Crie um repositório de dados para armazenar os dados de backup.
6. Crie um compartilhamento de arquivos no Nutanix Prism Web Portal.

Considerações:

- Consumo de licenças adicionais para os caminhos UNC. Para resolver, consulte a solução de problemas.
- O proxy de backup é sempre um computador Windows.
- Para que o plano NFS do Nutanix funcione, o NfsUtils precisa ser pré-instalado no computador proxy de backup (como é o caso do plano NFS interno).
- Para o Nutanix File Server, se qualquer um dos FSVMs do cluster falhar, o outro FSVM assumirá a propriedade principal do servidor de arquivos e a HA será ativada para o cluster FSVM.

Criar um compartilhamento de arquivos

A página Compartilhar/Exportar permite criar compartilhamentos de arquivos distribuídos ou padrão. Um compartilhamento distribuído ou compartilhamento inicial é um repositório no qual os arquivos pessoais de um usuário residem, enquanto o compartilhamento padrão ou de uso geral é um repositório compartilhado pelo grupo. Um compartilhamento distribuído é distribuído nos diretórios de nível superior, enquanto o compartilhamento padrão está em uma única VM do servidor de arquivos (FSVM). Esta seção fornece informações sobre como criar um compartilhamento de arquivos para executar o backup do UNC/NFS para o Nutanix Files.

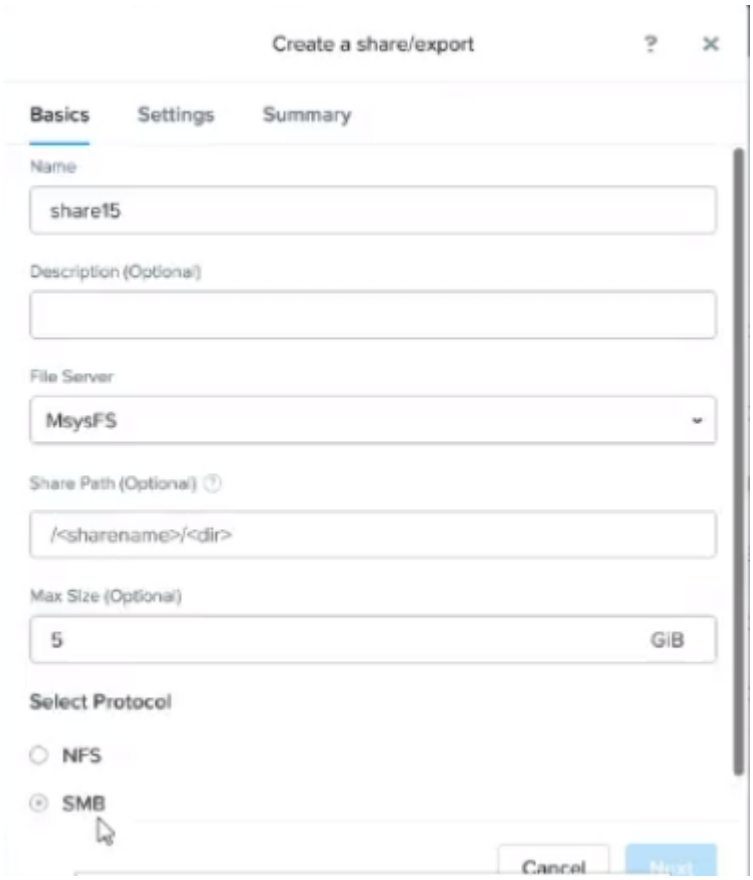
Siga estas etapas:

1. Efetue logon no portal da web do Nutanix Prism.
2. Navegue até **Servidor de arquivos** no menu principal e clique em **Compartilhar/exportar** no painel do servidor de arquivos.

   A janela Criar um compartilhamento/uma exportação é exibida com a guia Básico.
3. Na guia Básico, faça o seguinte e, depois, clique em **Avançar**:
   - Nome: digite um nome para o compartilhamento.

     Observação: as convenções de nomenclatura para o nome do compartilhamento são as seguintes:
     - Cada nome deve ser exclusivo.
     - Os nomes não diferenciam maiúsculas de minúsculas.
     - Os arquivos permitem caracteres Unicode.
     - O comprimento máximo do nome é de 80 caracteres.
     - Um espaço em branco ou caractere de espaço não pode aparecer como o primeiro ou o último caractere no nome.
     - Os nomes que terminam com $ são compartilhamentos ocultos.
   - Descrição (opcional): digite uma descrição para o compartilhamento, se necessário.
   - Servidor de arquivos: na lista suspensa, selecione um servidor de arquivos no qual o compartilhamento reside.
   - Caminho de compartilhamento (opcional): forneça o caminho do arquivo para o compartilhamento.
   - Tamanho máximo (opcional): digite o tamanho máximo do compartilhamento. Por padrão, o tamanho está em GB.
   - Selecionar protocolo: selecione **SMB** como um protocolo.

     Observação: para ativar o recurso de vários protocolos, marque a caixa de seleção **Ativar acesso de vários protocolos para o NFS**.



4. Na guia Configurações, mantenha os padrões ou faça as alterações necessárias e clique em **Avançar**.

   Usar o tipo de compartilhamento "Distribuído" em vez de "Padrão"

   Permite criar um compartilhamento distribuído.

   Observação: como regra, os compartilhamentos em implantações de FSVM único são padrão.

   Ativar a restauração automática

   Permite restaurar arquivos de instantâneos anteriores.

   Ativar a compactação do sistema de arquivos

   Permite economizar espaço e reduzir dados no compartilhamento por meio da compactação em linha dos dados gravados.

   Observação: certifique-se de desativar a compactação no nível do recipiente. Se você ativou a compactação, a opção Ativar compactação do sistema de arquivos será desativada.

   Ativar a enumeração baseada em acesso (ABE)

   Permite ativar a enumeração com base em acesso (ABE).

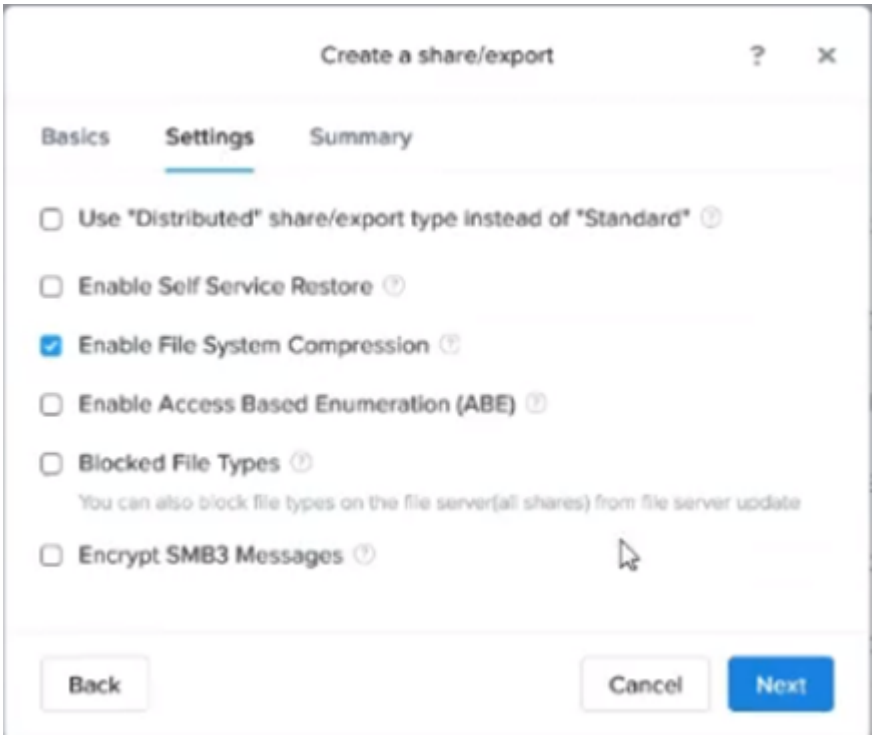
Tipos de arquivos bloqueados

Permite especificar os tipos de arquivos bloqueados.

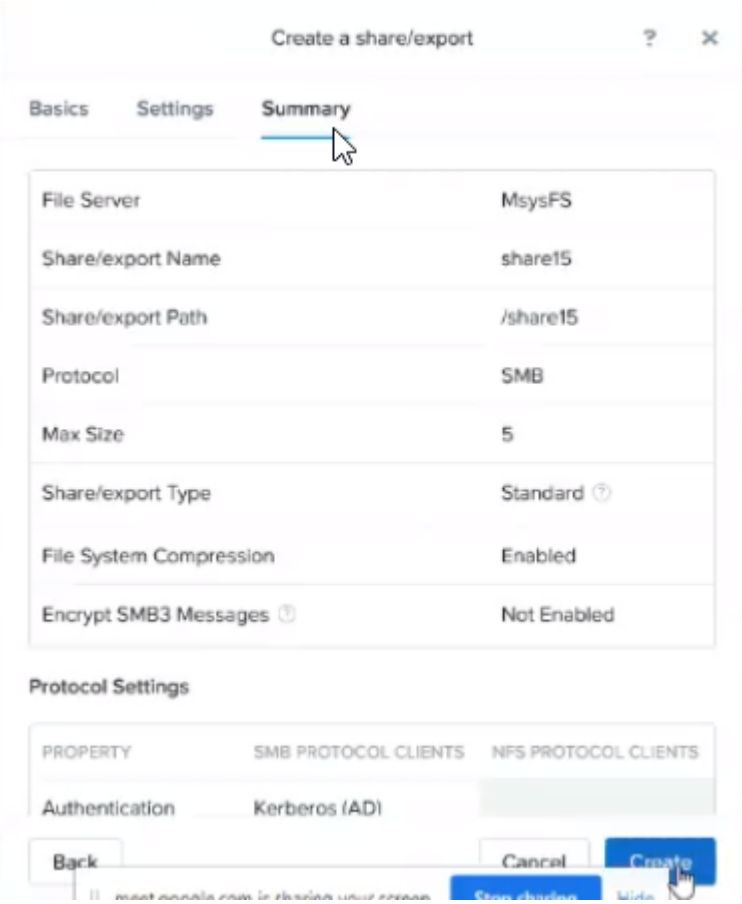
Insira uma lista separada por vírgulas dos tipos de arquivos que deseja bloquear no compartilhamento.

Criptografar as mensagens de SMB3

Permite ativar a criptografia de mensagens entre o servidor de arquivos e o cliente.



5. Na página Resumo, verifique os detalhes e clique em **Criar**.



Observação: para fazer alterações nas configurações das páginas anteriores, clique em **Voltar**.

O compartilhamento de arquivos é criado com êxito.

Observação: em seguida, copie o caminho de montagem e mapeie o compartilhamento recém-criado no UDP local. Para obter mais informações, consulte Etapa 6 (a1) de Especificar a origem.

Criar um plano de backup com uma tarefa de caminho UNC/NFS

Um plano de backup inclui uma tarefa de backup que executa um backup de um nó físico e armazena os dados em um destino especificado. Cada tarefa consiste em parâmetros que definem a origem, o destino, a programação e outros detalhes de backup.

Siga estas etapas:

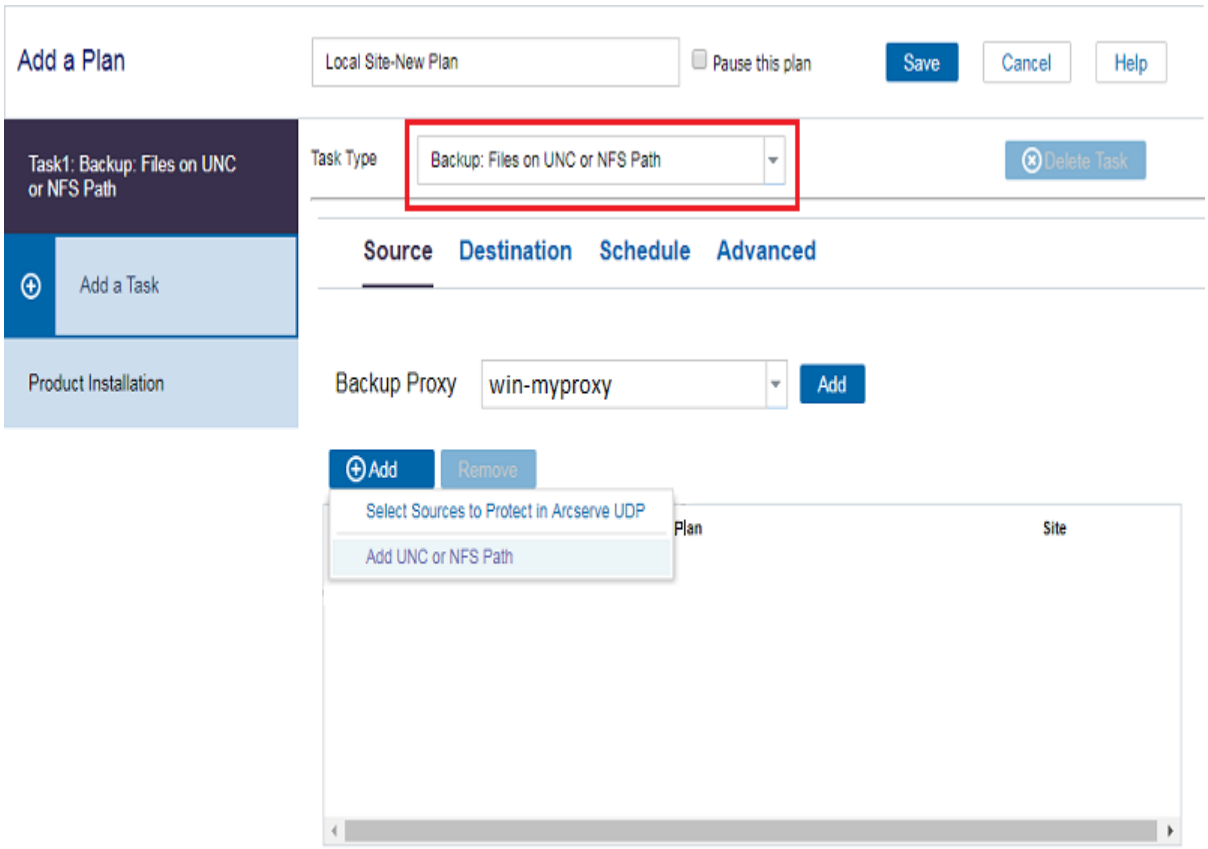
1. Efetue logon no Console do Arcserve UDP.
2. Clique na guia **Recursos**.
3. No painel esquerdo, navegue para **Planos** e clique em **Todos os planos**.

   Se tiver criado os planos anteriores, esses planos serão exibidos no painel central.
4. No painel central, clique em **Adicionar um plano**.

   A opção Adicionar um plano é aberta.
5. Digite o nome do plano.
6. (Opcional) Selecione a caixa de seleção **Pausar este plano**.

   O plano não será executado até que você desmarque a caixa de seleção para retomar o plano.

   Observação: se um plano for pausado, nenhuma tarefa em andamento será pausada, mas todas as tarefas programadas correspondentes associadas a esse plano serão pausadas. No entanto, você pode executar uma tarefa manualmente. Por exemplo, você pode executar manualmente a tarefa de backup e a tarefa de replicação para um nó mesmo que o respectivo plano esteja pausado. Nesse caso, a tarefa seguinte da tarefa sob demanda (manual) não será executada. Por exemplo, há uma tarefa de replicação após uma tarefa de backup sob demanda, a tarefa de replicação não será executada para a tarefa de backup sob demanda. É necessário executar manualmente a tarefa de replicação. Quando você retomar o plano, as tarefas pendentes não são retomadas imediatamente. Depois de retomar o plano, as tarefas pendentes serão executadas no próximo horário programado.
7. Na lista suspensa Tipo de tarefa, selecione **Backup: Arquivos no caminho UNC/NFS**.



Agora especifique os detalhes de Origem, Destino, Programação e Avançado.

Especificar a origem

A página Origem permite especificar os nós de origem que deseja proteger. É possível selecionar mais de um nó em um plano. Caso não tenha adicionado nós para o console, você pode adicionar nós ao criar ou modificar um plano da página de origem. Também é possível salvar um plano sem adicionar nenhum nó de origem. O plano é implantado somente após você adicionar nós de origem.

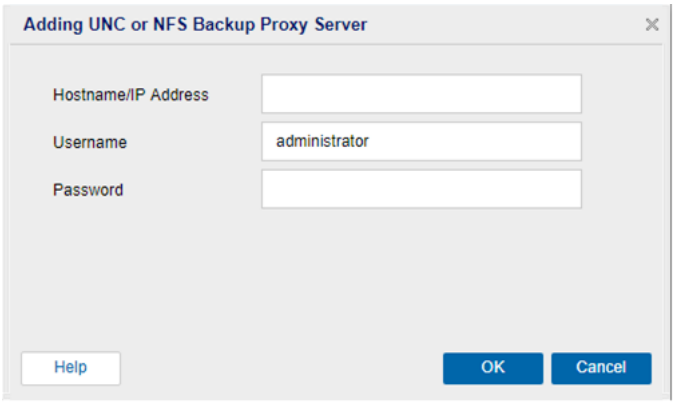
Siga estas etapas:

1. Clique na guia **Origem**.
2. Se o proxy de backup já tiver sido adicionado, selecione o proxy de backup na lista suspensa Proxy de backup.

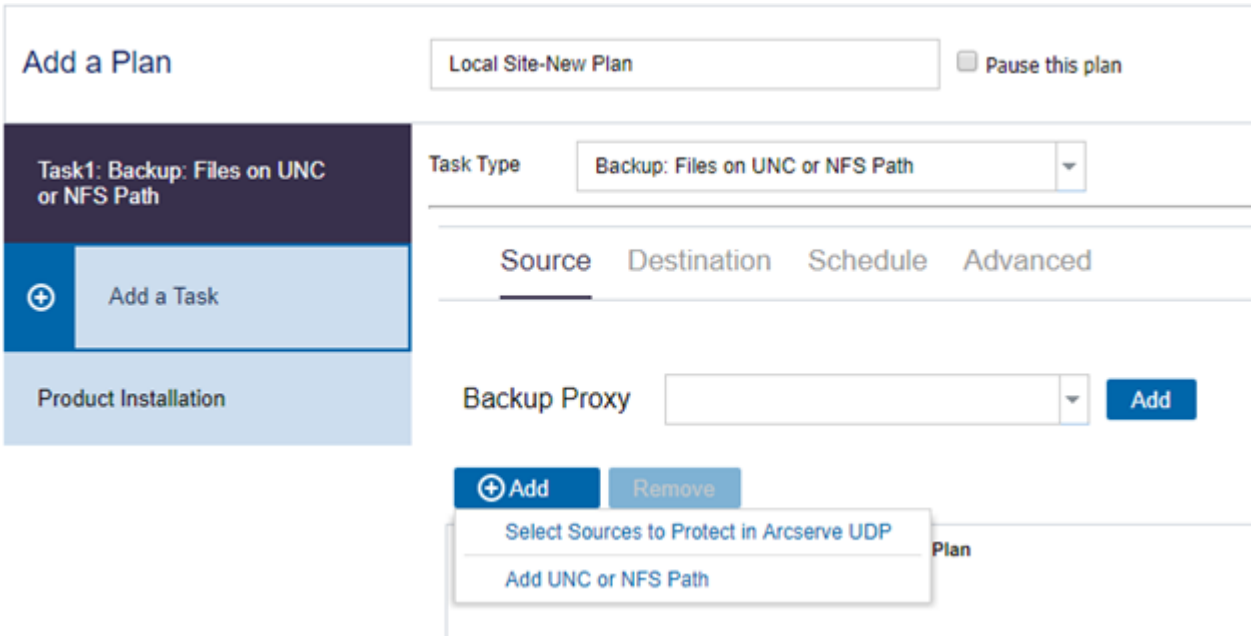
   O servidor proxy é um nó no qual você instala o Agente do Arcserve Unified Data Protection para Windows.

3. Se o proxy de backup não tiver sido adicionado, execute as seguintes etapas:
   a. Clique em **Adicionar**.

      A caixa de diálogo Adicionando o servidor proxy de backup do UNC ou do NFS é aberta.



   b. Especifique os detalhes do servidor proxy e clique em **OK**.
4. Para adicionar o nó do caminho UNC ou NFS, clique em **+ Adicionar** e selecione um dos seguintes:



Selecionar as origens a serem protegidas no Arcserve UDP

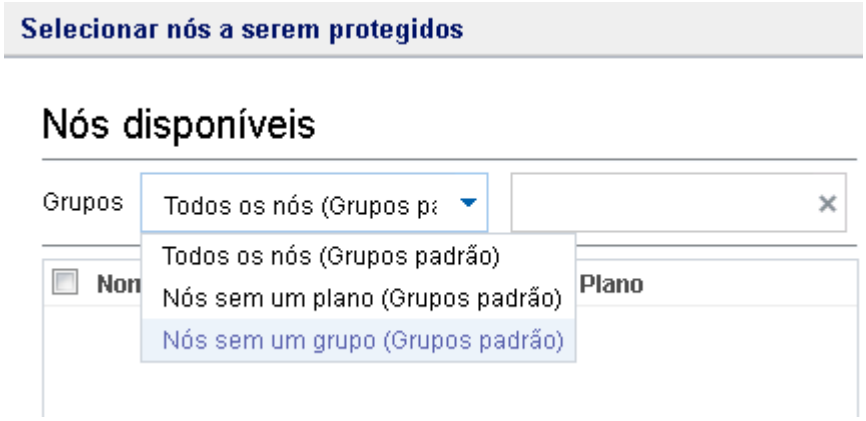
Selecione a caixa de diálogo Selecionar nós a serem protegidos e será possível selecionar os nós na lista exibida. Selecione esta opção se você já tiver adicionado os nós para o console.

Adicionar um caminho UNC/NFS

Abra a caixa de diálogo Adicionar nós ao Console do Arcserve UDP. Selecione esta opção se você não tiver adicionado os nós e desejar adicioná-los manualmente para fins de proteção.

5. Se você selecionar a opção **Selecionar as origens a serem protegidas no Arcserve UDP**, execute as seguintes etapas:

   a. (Opcional) Selecione um filtro na lista suspensa Grupos para filtrar os nós. É possível digitar as palavras-chave para filtrar melhor seus nós.



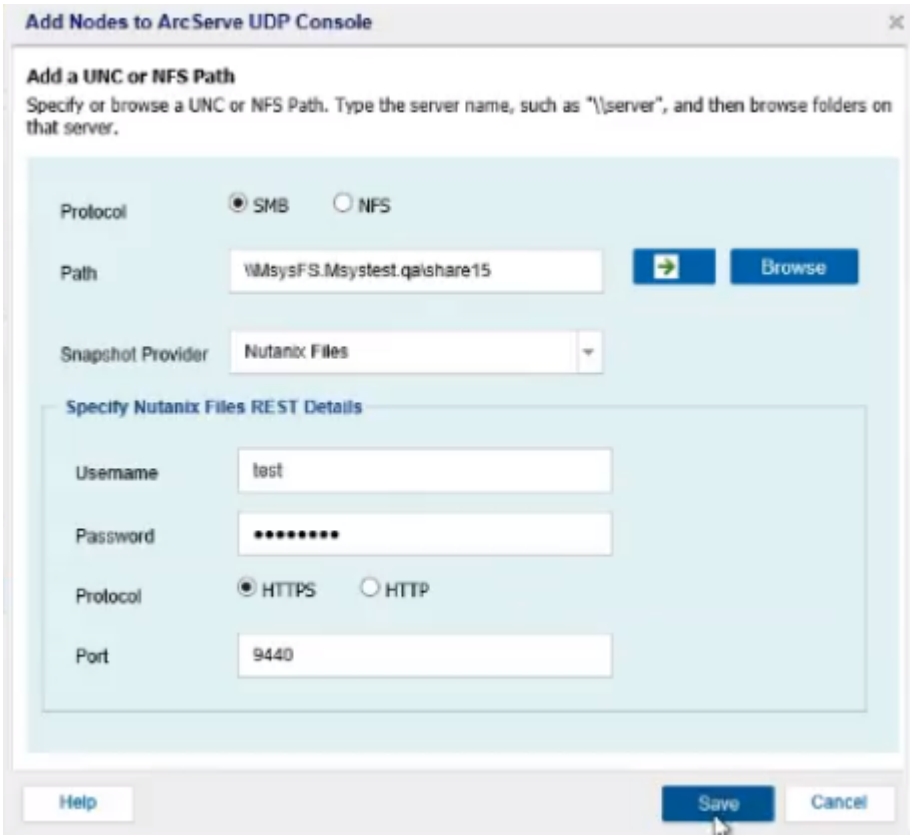
Os nós são exibidos em Nós disponíveis.

b. Selecione os nós em Nós disponíveis e clique no ícone **Adicionar todos os nós** (>>) ou **Adicionar nós selecionados** (>).

   Os nós selecionados são exibidos em Nós selecionados.

c. Clique em **OK** para fechar a caixa de diálogo.

6. Se você selecionar a opção **Adicionar caminho UNC ou NFS**, execute as seguintes etapas na página Adicionar um caminho UNC ou NFS:



a. Selecione **SMB** ou **NFS** como um protocolo.

   - Se você selecionar **SMB**, faça o seguinte:

     1. Digite o caminho UNC no seguinte formato:

        *Hostname**share*

        Observações:

        - Ao fornecer o compartilhamento de arquivos do Nutanix como origem para backup com arquivos do Nutanix como um provedor de instantâneos, os backups podem ser executados apenas no nível de compartilhamento, mas não no nível de subpasta.

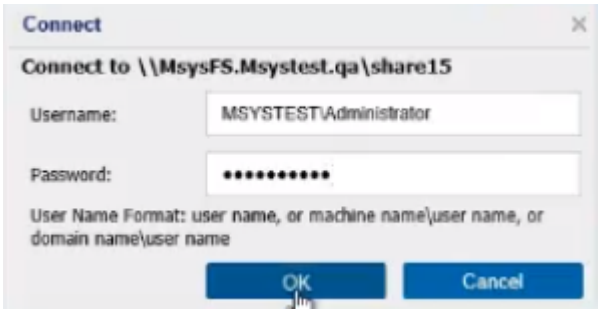
- Para obter o caminho UNC, faça o seguinte:
  a. Selecione o compartilhamento recém-criado no painel central.
  b. Na coluna DETALHES DE COMPARTILHAMENTO/EXPORTAÇÃO, no painel Resumo, navegue até **Caminho de montagem** e copie o caminho de montagem.

     Se o caminho UNC for válido, uma seta para a direita e a opção Procurar serão ativadas.

2. Clique na seta à direita (>) para validar o caminho UNC.

   A caixa de diálogo Conectar é exibida.

3. Digite o nome do usuário e a senha, conforme necessário, e clique em **OK**.



   A caixa de diálogo Adicionar nós ao console do Arcserve UDP exibe o caminho UNC verificado.

- Se você selecionar NFS, faça o seguinte:

  1. Digite o caminho UNC no seguinte formato:

     *Hostname**share*

  2. Selecione a Codificação entre as opções disponíveis - ANSI, GB2312-80, KSC5601, BIG5, SHIFT-JIS, EUC-KR, EUC-TW, EUC-JP.

     O valor padrão é ANSI.

     Observação: durante o backup de uma pasta NFS compartilhada, todos os arquivos e todas as pastas com nomes que tiverem uma codificação de idioma sem suporte serão ignorados ou seus nomes ficarão ilegíveis.

b. Na lista suspensa Provedor de instantâneo, selecione **Nutanix Files**.

c. Para a caixa Especificar detalhes de REST do Nutanix Files, especifique as seguintes credenciais:

Nome de usuário

Refere-se ao nome do usuário criado pelo usuário da API REST usando o Nutanix Prism.

Senha

Refere-se à senha do nome de usuário.

Protocolo

Especifique o protocolo que deseja usar para a comunicação com o servidor de destino. As opções disponíveis são HTTP e HTTPS.

Observação: para uma comunicação mais segura, selecione o protocolo HTTPS.

Porta

Refere-se ao número da porta. O valor da porta padrão é 9440 para acessar as chamadas de API REST e o Prism.

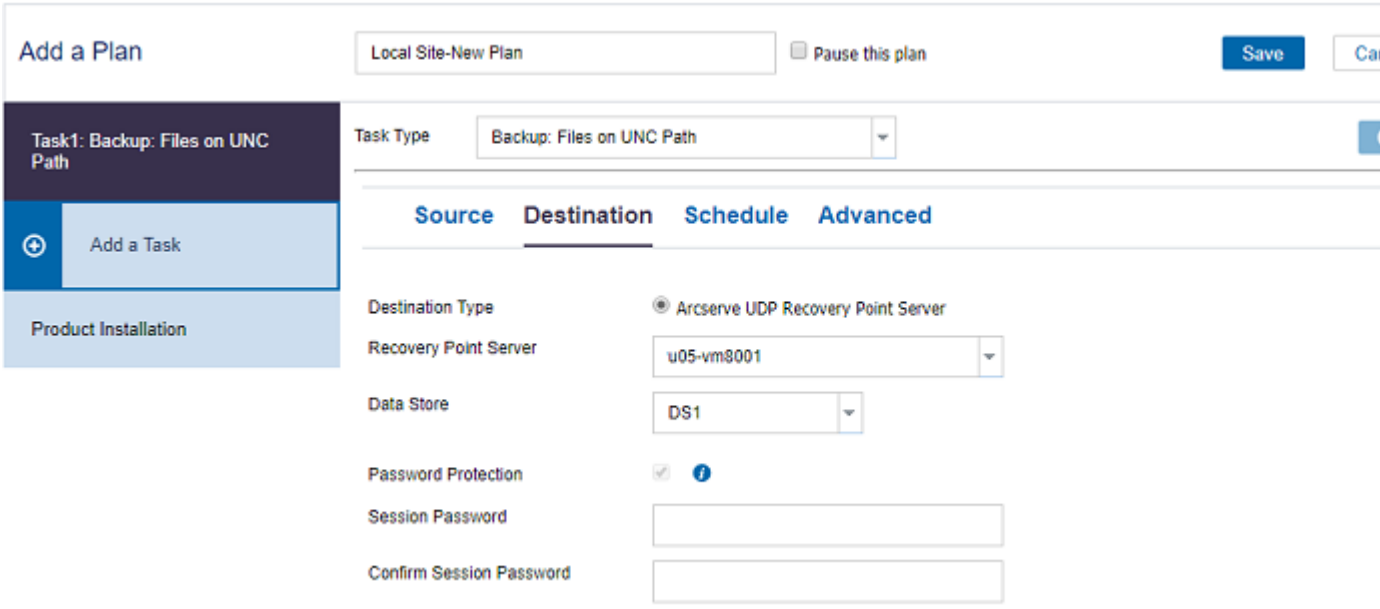
d. Clique em **Salvar**.

Observação: se a conexão com o Nutanix File Server falhar, a caixa de diálogo Erro/uma janela de notificação será exibida. Clique em **OK** para fechar a caixa de diálogo Erro.

A origem é especificada.

Especificar o destino

O destino é o local onde você armazena os dados de backup. É necessário, no mínimo, especificar o destino para salvar o plano.



Especifique os seguintes detalhes:

- Tipo de destino: verifique se a opção **Servidor de ponto de recuperação do Arcserve UDP** está selecionada por padrão.
- Servidor de ponto de recuperação: selecione um servidor de ponto de recuperação na lista suspensa.
- Repositório de dados - selecione um repositório de dados na lista suspensa.

  A lista exibe todos os repositórios de dados que são criados no servidor de ponto de recuperação especificado.
- Proteção por senha: forneça uma senha de sessão e, em seguida, digite-a novamente para confirmar.

  Observação: a senha da sessão é opcional quando o destino de backup é um repositório de dados do RPS não criptografado.

  O destino é especificado.

Especificar a programação

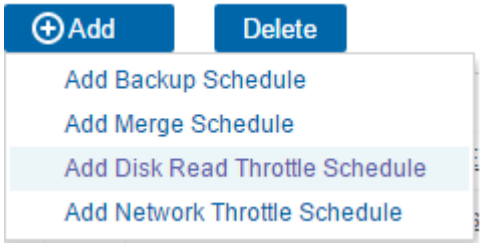
A página Programar permite definir uma programação para o backup e para que as funções Mesclar e Acelerar sejam repetidas em intervalos específicos. Após definir uma programação, as tarefas são executadas automaticamente de acordo com a programação. É possível adicionar várias programações e fornecer configurações de retenção.

Uma Programação de backup se refere a programação regular que é repetida várias vezes ao dia, com base no número de horas ou de minutos selecionado. Além da programação regular, uma programação de backup também fornece opções para adicionar programações diária, semanal e mensal.

Observação: para obter mais informações sobre as configurações de retenção e programação, consulte Entendendo a programação avançada e retenção.

Siga estas etapas:

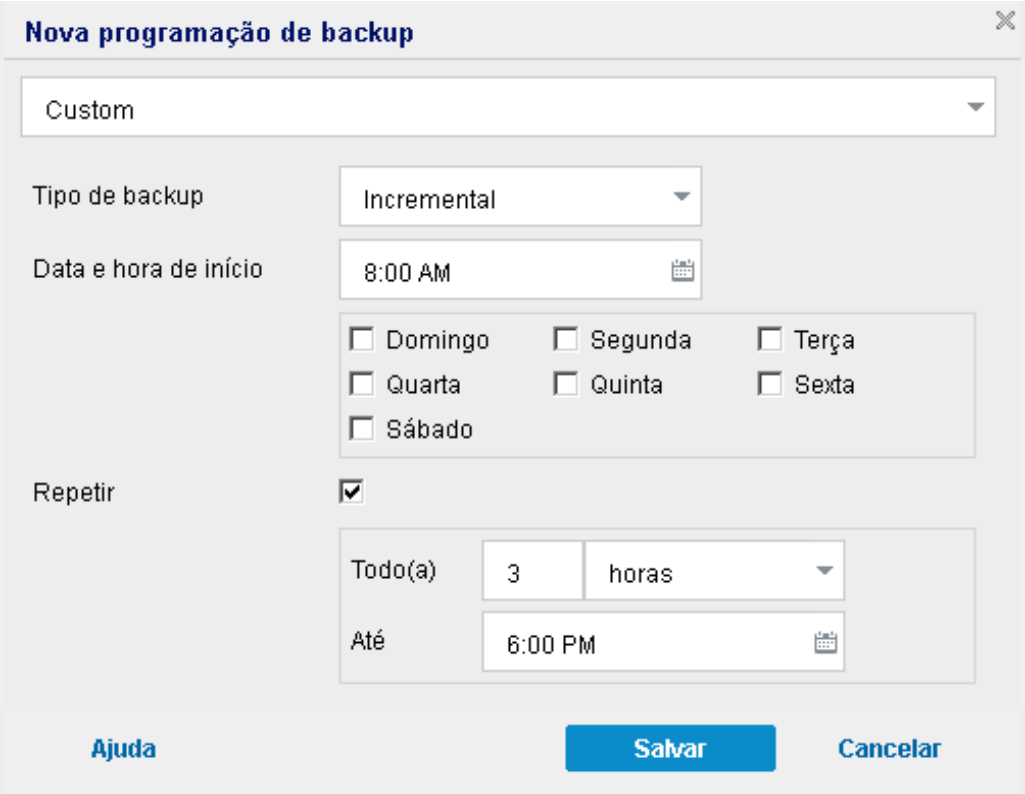
1. Adicione programações de backup, mesclagem, aceleração de leitura de disco e aceleração de rede.



Adicionar programação de backup

a. Clique em **Adicionar** e selecione **Adicionar programação de backups**.

   A caixa de diálogo **Nova programação de backup** é aberta.



b. Selecione uma das seguintes opções:

Personalizado

Especifica a programação de backup que se repete várias vezes por dia.

Diário

Especifica a programação de backup que ocorre uma vez por dia. Por padrão, todos os dias da semana estão selecionados para o backup diário. Se não desejar executar a tarefa de backup em um dia específico, desmarque a caixa de seleção correspondente àquele dia da semana.

Semanal

Especifica a programação de backup que ocorre uma vez por semana.

Mensal

Especifica a programação de backup que ocorre uma vez por mês.

c. Selecione o tipo de backup.

Completo

Especifica a programação de backups para backups completos. Conforme programado, o Arcserve UDP executa um backup completo de todos os blocos usados do computador de origem. Um backup completo em geral, consome tempo, dependendo do tamanho do backup.

Verificar

Especifica a programação de backups para backups de verificação.

A Arcserve UDP verifica se os dados protegidos são válidos e concluídos, executando uma verificação de confiabilidade da imagem de backup armazenada na origem do backup. Se necessário, a imagem será sincronizada novamente. Um backup de verificação examinará o backup mais recente de cada bloco e irá comparar o conteúdo e as informações com a origem. Esta comparação verifica se o backup mais recente dos blocos representa as informações correspondentes na origem. Se a imagem de backup de qualquer bloco não corresponder à origem (possivelmente devido a alterações no sistema desde o último backup), o Arcserve UDP atualizará (fará nova sincronização) o backup do bloco que não corresponder. Também é possível usar um backup de verificação (muito raramente) para obter a garantia de backup completo sem usar o espaço necessário para um backup completo.

Vantagens: produz uma pequena imagem de backup quando comparado ao backup completo, pois somente os blocos alterados (blocos que não coincidem com o último backup) são armazenados em backup.

Desvantagens: o tempo de backup é longo, pois todos os blocos de origem são comparados aos blocos do último backup.

Incremental

Especifica a programação de backups para backups incrementais.

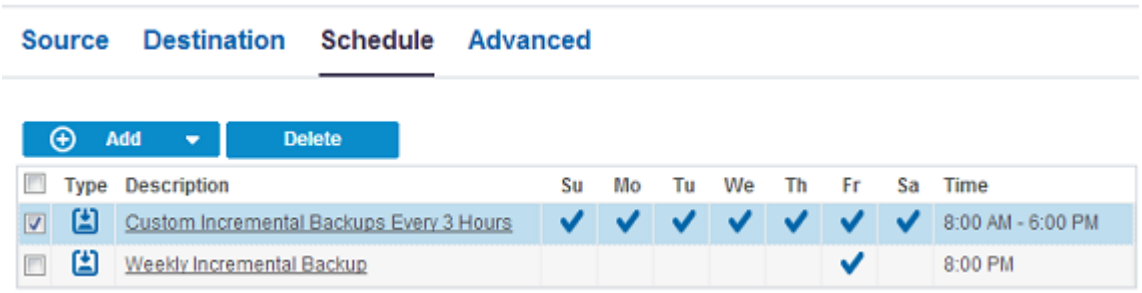
Conforme programado, o Arcserve UDP faz backup incremental apenas dos blocos que foram alterados após o último backup realizado com êxito. As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a executar um backup.

d. Especifique a hora de início do backup.

e. (Opcional) Marque a caixa de seleção de **Repetição** e especifique a programação a ser repetida.

f. Clique em **Salvar**.

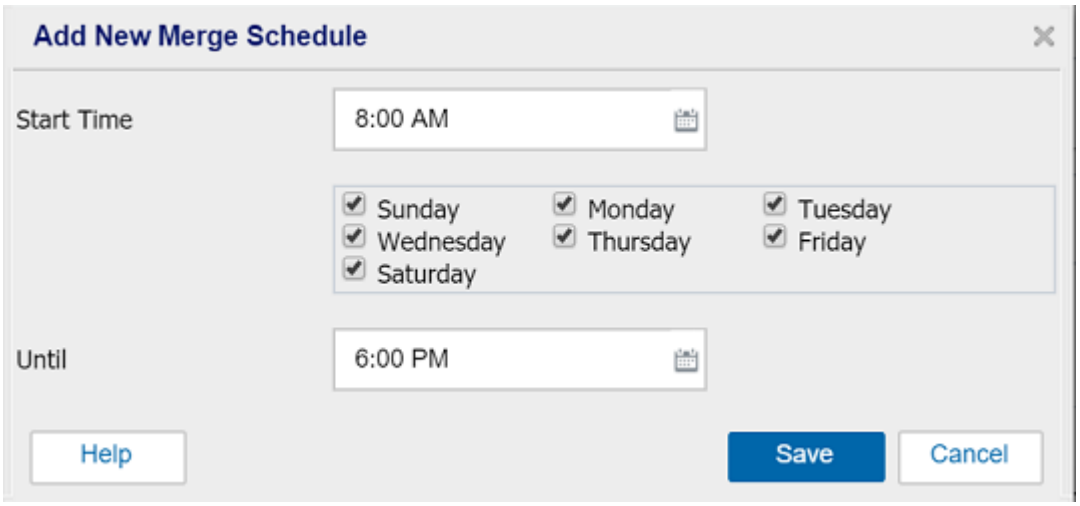
A programação de backup é especificada e aparece na página **Programar**.



Adicionar Programação de mesclagem

a. Clique em **Adicionar** e selecione **Adicionar programação de mesclagem**.

   A caixa de diálogo **Adicionar nova programação de mesclagem** é aberta.



b. Especifique a hora de início para iniciar a tarefa de mesclagem.

c. Especificar **Até** para especificar uma hora de término para a tarefa de mesclagem.

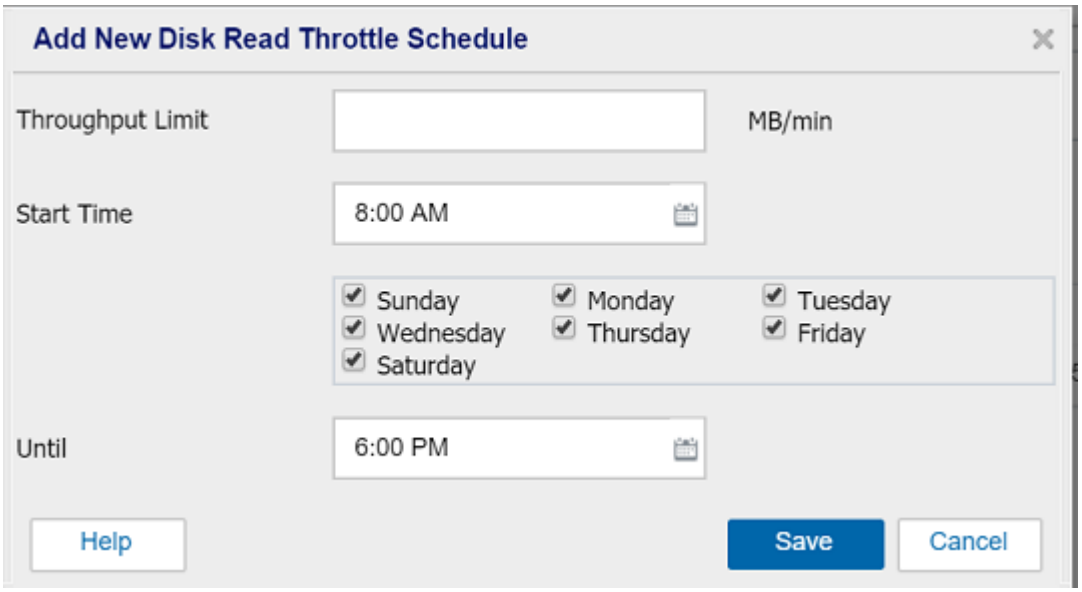
d. Clique em **Salvar**.

A programação de mesclagem é especificada e exibida na página de **Programação**.

Adicionar programação de acelerador de leitura de disco

a. Clique em **Adicionar** e selecione **Adicionar programação de acelerador de leitura de disco**.

   A caixa de diálogo **Adicionar nova programação de acelerador de leitura de disco** é aberta.



b. Especifique o limite de taxa de transferência em MB por minuto.

c. Especifique a hora de início para iniciar a tarefa de taxa de transferência de backup.

d. Especifique **Até** para especificar um horário de término para a tarefa de taxa de transferência.

e. Clique em **Salvar**.

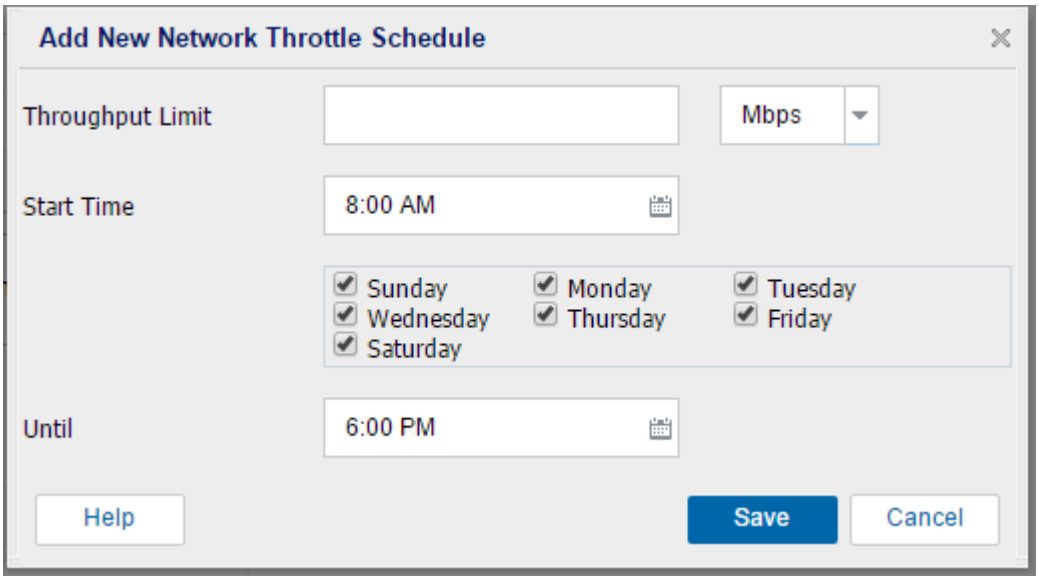
A Programação de acelerador de leitura de disco é especificada e aparece na página **Programação**.

Adicionar programação de acelerador de rede

Observação: a Programação de acelerador de rede é exibida apenas para backup com base em agente do Windows ao definir um repositório de dados com redução de redundância ativada como o destino para o plano.

a. Clique em **Adicionar** e selecione **Adicionar programação de acelerador de rede**.

   A caixa de diálogo **Adicionar nova programação de acelerador de rede** é aberta.



b. Especifique o limite de taxa de transferência em Mbps ou Kbps.

   Observação: o valor mínimo padrão é 500 Kbps. Para alterar o padrão valor, siga estas etapas:

   i. No caminho de registro SOFTWARE\Arcserve\Unified Data Protection\Management\Console, insira uma chave MinNetworkThrottleValueInKpbs, especifique o tipo como REG_SZ e defina um valor para ela.

   ii. Reinicie o serviço de gerenciamento do Arcserve UDP.

   iii. Modifique o plano ou crie outro plano.

   O valor personalizado entra em vigor.

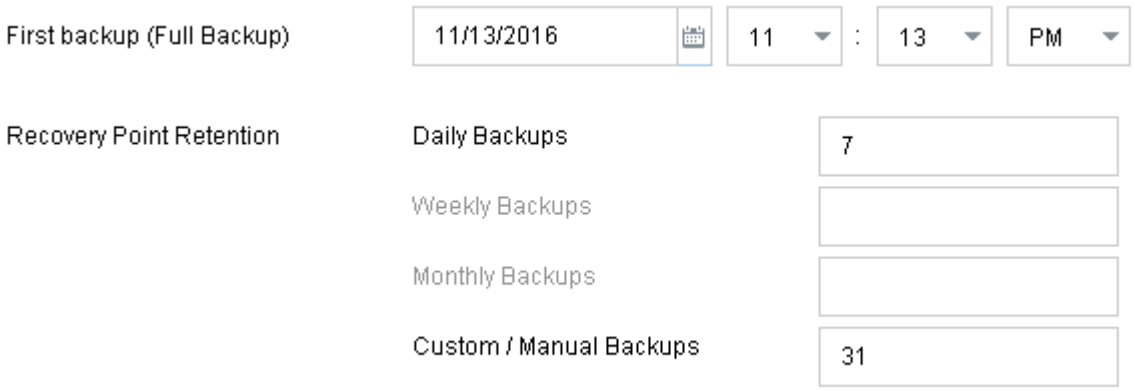
c. Especifique a hora de início para iniciar a tarefa de taxa de transferência de backup.

d. Especifique **Até** para especificar um horário de término para a tarefa de taxa de transferência.

e. Clique em **Salvar**.

A Programação de acelerador de rede é especificada e aparece na página **Programação**.

2. Especifique a hora de início do backup programado.



3. Especifique as configurações de retenção de pontos de recuperação para programação diária, semanal e mensal.

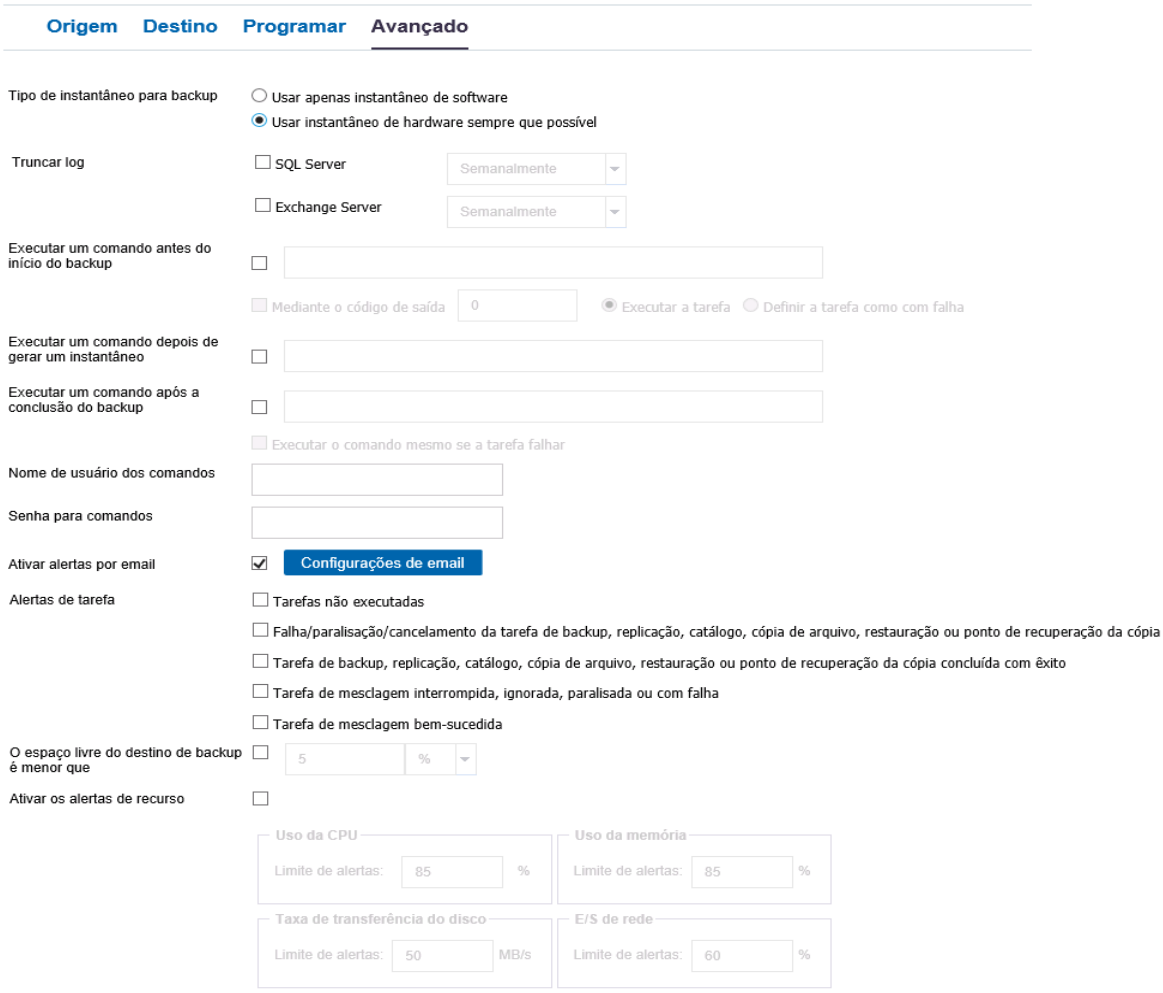
   Essas opções serão ativadas se tiver adicionado a programação de backup correspondente. Se você modificar as configurações de retenção desta página, as alterações serão refletidas na caixa de diálogo Programação de backup.

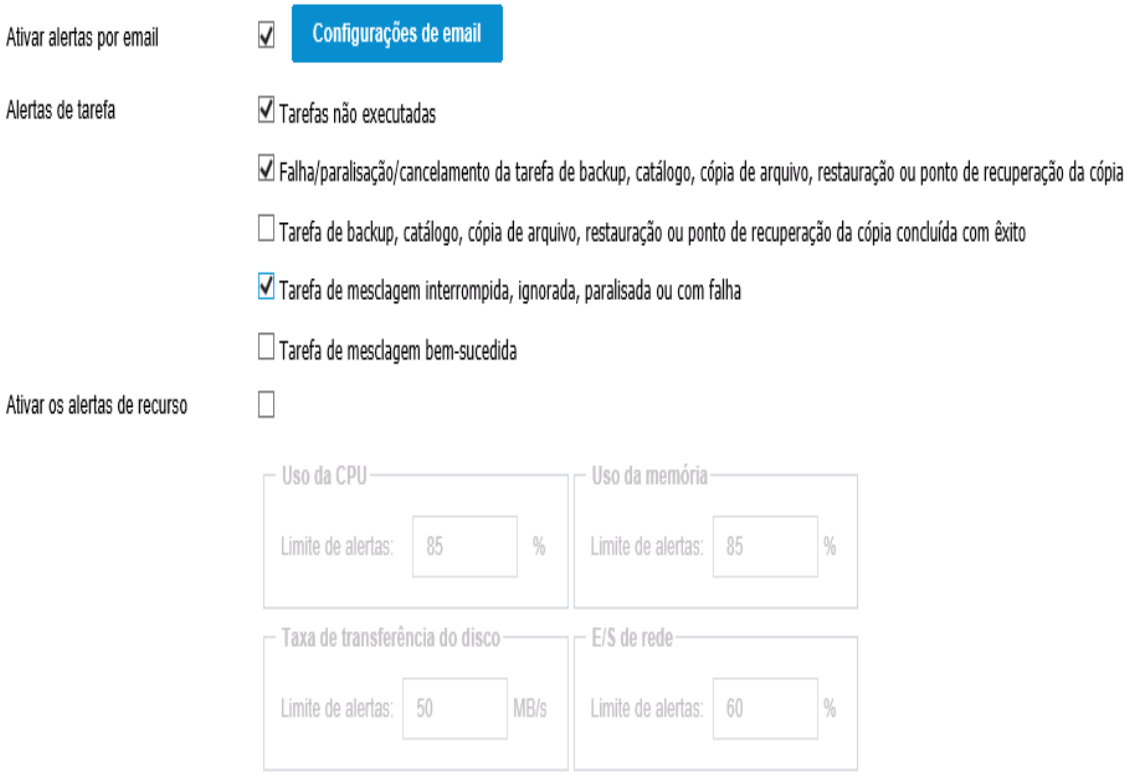
   A programação é especificada.

Especificar as configurações avançadas

A guia **Avançado** permite especificar algumas configurações avançadas para a tarefa de backup. As configurações avançadas incluem fornecer configurações de log de truncamento, a localização de quaisquer scripts e as configurações de email.

A imagem a seguir mostra a guia Avançado:


Origem
Destino
Programar
Avançado
Tipo de instantâneo para backup
Usar apenas instantâneo de software
Usar instantâneo de hardware sempre que possível
Truncar log
SQL Server
Semanalmente
Exchange Server
Semanalmente
Executar um comando antes do início do backup
Mediante o código de saída
0
Executar a tarefa
Definir a tarefa como com falha
Executar um comando depois de gerar um instantâneo
Executar um comando após a conclusão do backup
Executar o comando mesmo se a tarefa falhar
Nome de usuário dos comandos
Senha para comandos
Ativar alertas por email
Configurações de email
Alertas de tarefa
Tarefas não executadas
Falha/paralisação/cancelamento da tarefa de backup, replicação, catálogo, cópia de arquivo, restauração ou ponto de recuperação da cópia
Tarefa de backup, replicação, catálogo, cópia de arquivo, restauração ou ponto de recuperação da cópia concluída com êxito
Tarefa de mesclagem interrompida, ignorada, paralisada ou com falha
Tarefa de mesclagem bem-sucedida
O espaço livre do destino de backup é menor que
5
%
Ativar os alertas de recurso
Uso da CPU
Limite de alertas:
85
%
Uso da memória
Limite de alertas:
85
%
Taxa de transferência do disco
Limite de alertas:
50
MB/s
E/S de rede
Limite de alertas:
60
%



Siga estas etapas:

1. Especifique os seguintes detalhes.

   Tipo de instantâneo para backup

   Selecione uma das opções a seguir para o instantâneo de backup.

   Usar apenas instantâneo de software

   Especifica que o tipo de backup usa apenas o instantâneo do software. O Arcserve UDP não verificará se há instantâneos de hardware. O instantâneo de software utiliza menos recursos nas máquinas virtuais. É possível usar essa opção se o servidor tiver menos configurações e menor velocidade de processamento.

   Usar instantâneo de hardware sempre que possível

   Especifica que o tipo de backup primeiro verifica se há um instantâneo de hardware. Se todos os critérios forem atendidos, o tipo de backup usa o instantâneo de hardware.

   Observação: para obter mais informações sobre os critérios de instantâneo de hardware, consulte o pré-requisito.

   Truncar log

Permite especificar a programação para truncar logs para o SQL Server e o Exchange Server. É possível especificar a programação como **Diária**, **Semanal** ou **Mensal**.

Ativar a limpeza de logs em intervalos por hora para SQL por meio de uma chave de Registro

- Defina as configurações do plano. Marque a opção "SQL Server" na seção "Truncar Log" sob a guia "Avançado" e, em seguida, selecione "Diário".
- Defina a chave de Registro na máquina do SQL Server em que o agente do UDP está hospedado. "PurgeSqlLogPerHour" é o intervalo em horas para a limpeza de logs do SQL.

  Caminho: HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

  Nome do valor: PurgeSqlLogPerHour (indica o intervalo em horas para a limpeza de logs do SQL).

  Tipo de valor: REG_DWORD

Nome de usuário

Permite especificar o usuário que possui autorização para executar um script.

Senha

Permite especificar a senha do usuário que está autorizado a executar o script.

Executar um comando antes do início do backup

Permite a execução de um script antes de iniciar a tarefa de backup. Especifique o caminho completo onde o script está armazenado. Clique em **No código de saída** e especifique o código de saída para **Executar tarefa** ou **Tarefa com falha**. **Executar a tarefa** indica que a tarefa de backup continuará quando o script retornar o código de saída. **Tarefa com falha** indica que a tarefa de backup será interrompida quando o script retornar o código de saída.

Executar um comando após a criação de um instantâneo

Permite executar um script depois que o backup do instantâneo for gerado. Especifique o caminho completo onde o script está armazenado.

Para executar o script pós-instantâneo mesmo durante uma falha do instantâneo, selecione **Executar o comando mesmo quando o instantâneo falha**.

Executar um comando após a conclusão do backup

Permite executar um script depois que a tarefa de backup foi concluída. Especifique o caminho completo onde o script está armazenado.

Ativar alertas por email

Permite ativar alertas por email. É possível especificar configurações de email e os tipos de alertas que você deseja receber por email. Ao selecionar esta opção, as seguintes opções serão ativadas para a seleção.

Configurações de email

Permite configurar as definições de email. Clique em **Configurações de email** e configure o servidor de email e os detalhes do servidor proxy. Para obter mais informações sobre como definir as configurações de email, consulte Configurar email e alerta.

Alertas de tarefa

Permite que você selecione os tipos de emails da tarefa que deseja receber.

Ativar os alertas de recurso

Permite que você especifique um limite de uso da CPU, o uso da memória, a taxa de transferência de disco, E/S de rede. Você pode fornecer o valor em porcentagem. Você receberá um email quando o valor exceder o Limite de alerta.

2. Clique em **Salvar**.

Observação: quando você seleciona um nó como origem de backup ou proxy de backup, o Arcserve UDP verifica se o agente está instalado no nó e se é a versão mais recente. Em seguida, o Arcserve UDP exibe uma caixa de diálogo de verificação que lista todos os nós que possuem uma versão antiga do agente ou que não tem o agente instalado. Para instalar/atualizar o agente nesses nós, selecione o método de instalação e clique em Salvar.

As alterações são salvas e uma marca de seleção verde é exibida ao lado do nome da tarefa. A página do plano é fechada.

Observação: se precisar adicionar outra tarefa, deverá selecionar o plano na guia **Recursos** e modificar o plano. Para modificar o plano, clique no plano do painel central. O plano é exibido e será possível modificá-lo.

O plano de backup é criado e implantado automaticamente para o nó de origem. O backup é executado de acordo com a programação que você configurou na guia **Programar**. Também é possível fazer backup manual quando desejado.

(Opcional) Executar um backup manual

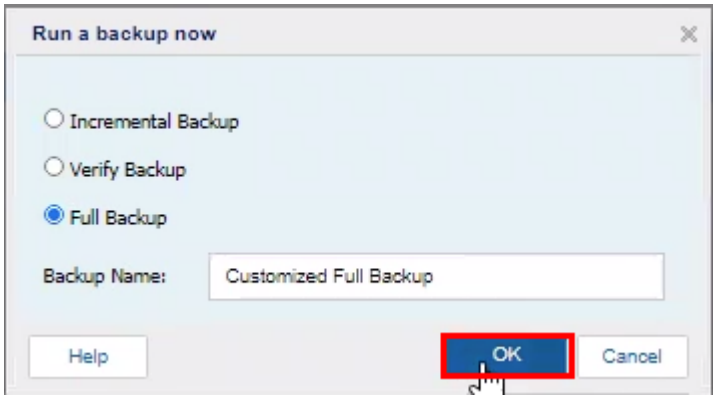
Em geral, os backups são executados automaticamente e controlados pelas configurações da programação. Além do backup programado, um backup manual fornece a opção de fazer backup dos nós de acordo com a necessidade. Por exemplo, se você repetir a programação para backups completos, incrementais e de verificação e desejar fazer grandes alterações em seu computador, deverá executar um backup manual imediato sem esperar até que ocorra o próximo backup programado.

Siga estas etapas:

1. Efetue logon no Console do Arcserve UDP.
2. Navegue até **recursos** > **Plano** > **Todos os planos**.

   A lista de todos os planos é exibida no painel central.
3. Clique com o botão direito do mouse no plano e selecione **Fazer backup agora**.

   A caixa de diálogo Fazer backup agora é exibida.
4. Na caixa de diálogo Executar um backup agora, selecione o tipo de backup que deseja executar e, em seguida, especifique o nome do backup, se necessário.



As opções disponíveis são:

Backup incremental

Inicia um backup incremental do computador inteiro. Um backup incremental realiza backup somente dos blocos que foram alterados desde o backup anterior.

Observação: se estiver executando um backup pela primeira vez, o backup completo será iniciado automaticamente, mesmo que você tenha selecionado a opção Backup incremental.

As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a execução de backups.

Verificar backup

Inicia um backup de verificação do computador, examinando o backup mais recente de cada bloco e comparando o conteúdo e as informações com a origem. Esta comparação verifica se o backup mais recente dos blocos representa as informações correspondentes na origem. Se a imagem de backup de algum bloco não corresponder à origem, o agente do Arcserve UDP (Windows) atualizará (ressincronizará) o backup do bloco divergente.

Vantagem: uma imagem de backup muito pequena é gerada quando comparada ao backup completo porque somente os blocos alterados (blocos que não correspondam ao último backup) são armazenados em backup.

Desvantagem: o tempo do backup fica lento porque todos os blocos do disco de origem são comparados aos blocos do último backup.

Backup completo

Inicia um backup completo do computador inteiro ou dos volumes selecionados.

Observações:

- se você adicionar um novo volume à origem do backup, será feito um backup completo do volume recém-adicionado, independentemente do método de backup geral selecionado.
- Se nenhum nome de backup for especificado, por padrão, ele será automaticamente nomeado como Backup completo/incremental/de verificação personalizado.

5. Clique em **OK**.

   A caixa de diálogo Informações do andamento é exibida.

6. Aguarde até que a tarefa de backup seja concluída e clique em **OK**.

7. Para monitorar as tarefas de backup, navegue até **tarefas** > **Tarefas em andamento**.

   Aguarde até a conclusão da tarefa de backup.

   Observação: apenas uma tarefa pode ser executada em uma hora. Se você tentar iniciar manualmente uma tarefa de backup quando outra tarefa estiver em execução no mesmo momento, uma mensagem de alerta será exibida informando

sobre a existência de outra tarefa em execução e solicitando uma nova tentativa mais tarde.

O backup manual é realizado com êxito.

Outras tarefas no plano do UNC/NFS

Você pode acompanhar a tarefa do plano do caminho UNC/NFS com outras tarefas. Pode criar tarefas de acompanhamento, como cópia de ponto de recuperação, cópia em fita, replicação para a nuvem do Arcserve, replicação e replicação para um RPS gerenciado remotamente.

Tarefa Copiar pontos de recuperação

Permite copiar os pontos de recuperação em uma pasta local, compartilhada ou na nuvem.

Copiar em fita

Permite armazenar o ponto de recuperação em fita por meio da integração com o Arcserve Backup.

Tarefa de replicação

Permite criar uma tarefa para replicar dados de backup de um servidor de ponto de recuperação para outro servidor de ponto de recuperação.

Replicar para um RPS gerenciado remotamente

Permite criar uma tarefa para replicar ou enviar dados para um servidor de ponto de recuperação remoto.

Replicar para a nuvem do Arcserve

Permite criar uma tarefa para replicar ou enviar dados para um servidor de ponto de recuperação de nuvem.

Teste de recuperação garantida

Permite verificar a acessibilidade e garantir a recuperação dos dados.

Verificar o backup

Para verificar a tarefa de backup, confirme se você criou com êxito o plano de backup. Depois de verificar se o plano está criado com êxito, confirme se a tarefa de backup é executada conforme o programado. É possível verificar o status das tarefas de backup na guia **Tarefas**.

Siga estas etapas para verificar os planos:

1. Clique na guia **Recursos**.
2. No painel esquerdo, navegue para **Nós** e clique em **Todos os nós**.

   Uma lista de todos os nós é exibida no painel central.
3. Verifique se os planos são mapeados com nós.

Siga um destes métodos para verificar as tarefas de backup:

Método 1

1. Clique na guia **Tarefas**.
2. No painel à esquerda, clique em **Todas as tarefas concluídas**.

   O status de cada tarefa é incluído no painel central.
3. Verifique se a tarefa de backup é concluída com êxito.

   A tarefa de backup é verificada.

Método 2

1. Clique na guia **Tarefas**.
2. No painel esquerdo, clique em **Tarefas concluídas com êxito**.

   A lista de tarefas de backup concluídas é exibida no painel central.
3. Clique na tarefa que você deseja verificar.

   O painel direito é atualizado.
4. Em Detalhes da tarefa, clique no hiperlink **Exibir logs**.
5. Verifique se a tarefa de backup é concluída com êxito.

   A tarefa de backup é verificada.

Como proteger máquinas em modo de espera virtual

É possível fazer o backup de máquinas no modo de espera virtual e proteger os dados de serem corrompidos. Para proteger o computador, é preciso ligar o computador.

O seguinte diagrama ilustra o processo para proteger uma máquina em modo de espera virtual:

O que fazer a seguir?

- Verificar os pré-requisitos e as considerações
- Ligar máquinas do Virtual Standby
- Proteger máquinas no modo de espera virtual após serem ligadas
- Verifique se a máquina em modo de espera virtual está protegida

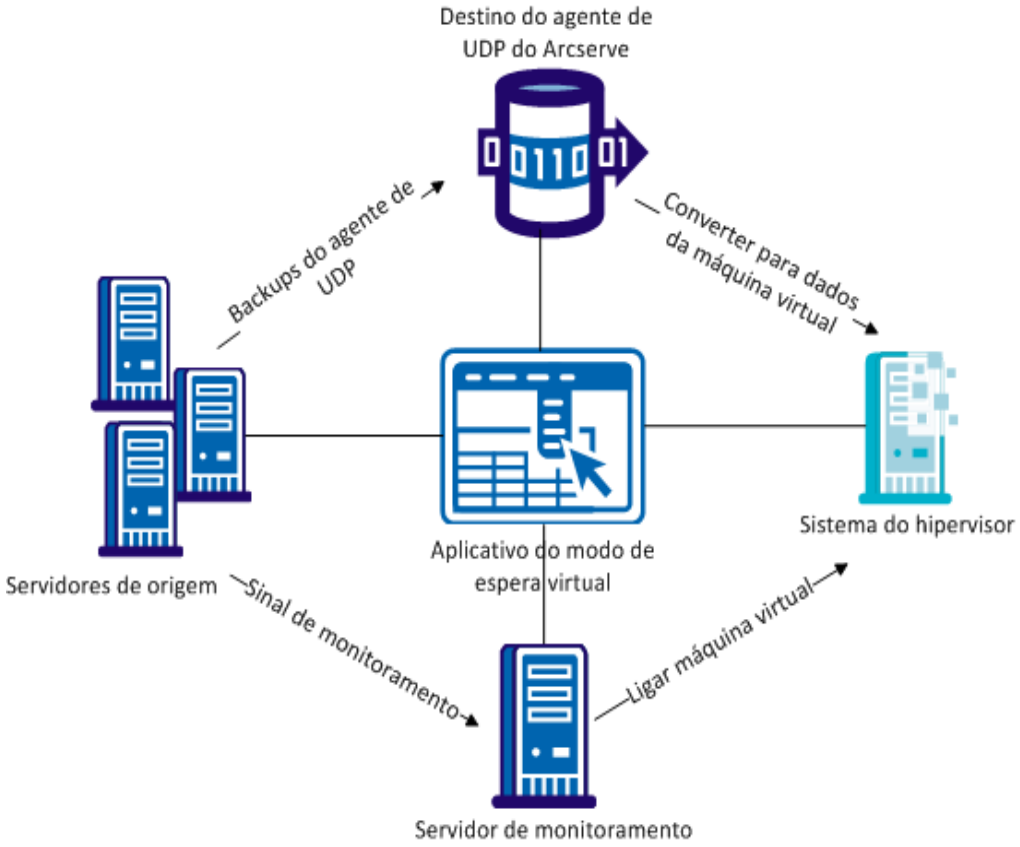
Verificar os pré-requisitos e as considerações

Verifique se concluiu as seguintes tarefas de pré-requisito:

- Efetuou logon no console
- Preparou uma máquina virtual em modo de espera.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Ligar máquinas do Virtual Standby

É possível ligar máquinas no modo de espera virtual e proteger as máquinas virtuais depois de serem ligadas. O diagrama a seguir descreve o fluxo do processo para ligar as máquinas virtuais:



Ligar máquinas virtuais do Virtual Standby a partir de instantâneos do ponto de recuperação

O Virtual Standby pode ser configurado para ligar máquinas no modo de espera virtual automaticamente a partir de instantâneos de ponto de recuperação quando o servidor de monitoramento não detectar nenhum sinal de monitoramento do servidor de origem. Como alternativa, é possível ligar as máquinas no modo de espera virtual manualmente a partir de instantâneos de ponto de recuperação, caso haja uma emergência ou falha em um servidor de origem ou caso deseje colocá-lo offline para manutenção.

Observação: as etapas a seguir descrevem como ligar manualmente máquinas no modo de espera virtual a partir de instantâneos de ponto de recuperação. Para obter informações sobre como permitir que o Virtual Standby ligue Instantâneos do ponto de recuperação automaticamente, consulte Adicionar ao plano uma tarefa de Modo de espera virtual para EC2.

Siga estas etapas:

1. Na guia **Recursos**, navegue até o grupo de nós do **Modo de espera virtual**.

   Os nós no modo de espera virtual são exibidos no painel central.

2. No painel central, selecione o nó e clique em **Colocar a VM no modo de espera**.

   A caixa de diálogo **Colocar a VM no modo de espera** é exibida.

3. Na caixa de diálogo **VM no modo de espera**, execute as seguintes tarefas:

   - Selecione um instantâneo de data e hora do instantâneo do ponto de recuperação para ligar a máquina virtual.

     Observação: se a máquina virtual em modo de espera ainda não tiver sido configurada, o link "A rede da máquina virtual em modo de espera não está configurada" será exibido.

     a. Clique neste link para configurar a rede.

     b. Clique em **Salvar**. As configurações são salvas na máquina virtual do Virtual Standby.

     c. Clique em **Fechar** e a caixa de diálogo **Instantâneo do ponto de recuperação** é exibida.

   - Clique em **Ligar VM**.

     A máquina virtual é ligada usando os dados contidos no instantâneo do ponto de recuperação.

Observação: Observação: após ligar a máquina virtual, poderá ser solicitado que você reinicie o computador uma ou mais vezes. Este comportamento ocorre porque o driver do Amazon PV está instalado na máquina virtual.

Depois de ligar as máquinas no modo de espera virtual a partir dos instantâneos do ponto de recuperação, talvez seja preciso concluir as seguintes tarefas:

- Ativar o sistema operacional do Windows em execução na máquina virtual.
- Iniciar o Agente do Arcserve Unified Data Protection para Windows na máquina virtual.
- Atualize o Arcserve UDP com o nome do host, endereço IP e as credenciais de logon na máquina virtual.
- Atribua o nó ao plano.

Observação: esta tarefa é necessária somente se você deseja criar instantâneos do ponto de recuperação para a máquina virtual que foi ligada.

Ligar máquinas virtuais do Virtual Standby a partir do Hyper-V Manager

Quando você quiser ligar máquinas virtuais no Modo de espera virtual manualmente, a prática recomendada é ligar as VMs pela caixa de diálogo Colocar a VM no modo de espera do servidor do Arcserve Unified Data Protection. Para obter mais informações, consulte Ligar máquinas virtuais no modo de espera virtual em Instantâneos do ponto de recuperação. No entanto, se desejar iniciar máquinas em modo de espera virtual pelo servidor Hyper-V, é possível fazer isso usando o Hyper-V Manager.

Observação: o Hyper-V Manager permite acessar os instantâneos de ponto de recuperação que o modo de espera virtual criou para proteger o nó. Você não deve excluir os instantâneos. Ao excluir os instantâneos, a relação entre os dados contidos nos instantâneos torna-se inconsistente na próxima vez em que uma tarefa do Virtual Standby é executada. Com dados inconsistentes, não é possível ligar as máquinas virtuais do Virtual Standby de forma adequada.

Siga estas etapas:

1. Efetue logon no servidor Hyper-V responsável por monitorar os nós que você está protegendo.
2. Inicie o Gerenciador do Hyper-V seguindo estas etapas:
   a. Clique em Iniciar, Todos os programas, Ferramentas Administrativas e, em seguida, clique em Gerenciador Hyper-V.

      O Hyper-V Manager é aberto.

   b. Na árvore de diretórios, expanda o Gerenciador Hyper-V e clique no servidor Hyper-V contendo a máquina virtual que deseja ligar.

      As máquinas virtuais associadas ao servidor Hyper-V, especificadas na lista de máquinas virtuais, são exibidas no painel central.
3. Execute uma das seguintes tarefas:
   - **Para ligar a máquina virtual usando o instantâneo mais recente**: na lista de máquinas virtuais, clique com o botão direito do mouse na máquina virtual que deseja ligar e clique em Start no menu pop-up.
   - **Para ligar a máquina virtual usando um instantâneo mais antigo:**
     a. Na lista de máquinas virtuais, clique na máquina virtual que deseja ligar.

Os instantâneos associados à máquina virtual são exibidos na lista Instantâneos.

b. Clique com o botão direito do mouse no instantâneo que deseja usar para ligar a máquina virtual e clique em Aplicar no menu pop-up.

   A caixa de diálogo Apply Snapshot é aberta.

c. Clique em Aplicar.

d. Na lista de máquinas virtuais, clique com o botão direito do mouse na máquina virtual que deseja ligar e clique em Start no menu pop-up.

   A máquina no modo de espera virtual é ligada.

Se necessário, é possível fazer backup das máquinas virtuais e criar instantâneos de ponto de recuperação depois de ligar a máquina virtual.

Ligar máquinas no modo de espera virtual a partir do VMware vSphere Client

Para ligar máquinas no modo de espera virtual manualmente, a prática recomendada é ligar as VMs pela caixa de diálogo Colocar a VM no modo de espera do Arcserve UDP. Para obter mais informações, consulte Ligar máquinas virtuais no modo de espera virtual em Instantâneos do ponto de recuperação. No entanto, se desejar iniciar as máquinas no modo de espera virtual pelo sistema do ESX Server ou vCenter Server, é possível fazê-lo usando o VMware vSphere Client.

Observação: o VMware vSphere Client permite acessar os instantâneos de ponto de recuperação que o modo de espera virtual criou para proteger o nó. Você não deve excluir os instantâneos. Ao excluir os instantâneos, a relação entre os dados contidos nos instantâneos torna-se inconsistente na próxima vez em que o modo de espera virtual é executado. Com dados inconsistentes, não é possível ligar as máquinas no modo de espera virtual de forma adequada.

Siga estas etapas:

1. Abra o VMware vSphere Client e efetue logon no sistema do ESX Server ou vCenter Server que estiver monitorando os nós que você está protegendo.
2. Na árvore de diretórios, expanda o sistema do ESX Server ou vCenter Server, localize e clique na máquina virtual que deseja ligar.
3. Execute uma das seguintes tarefas:

   Para ligar a máquina virtual usando um instantâneo mais antigo: Clique na guia Introdução e, em seguida, clique em Ligar na máquina virtual, localizado na parte inferior da tela.

   Para ligar a máquina virtual usando um instantâneo mais antigo:

   a. Clique no botão do gerenciador de instantâneos na barra de ferramentas.

      A caixa de diálogo Snapshots for (nome da máquina virtual) é aberta para exibir uma lista dos instantâneos disponíveis para a máquina virtual.

   b. Na lista de instantâneos, clique no que deseja usar para ligar a máquina virtual e, em seguida, clique em Go to.

      A máquina no modo de espera virtual é ligada.

   Se necessário, é possível fazer backup das máquinas virtuais e criar instantâneos de ponto de recuperação depois de ligar a máquina virtual.

Proteger máquinas no modo de espera virtual depois de serem ligadas

Depois que uma máquina no modo de espera virtual estiver ligada (manual ou automaticamente), a tarefa de backup do Agente do Arcserve Unified Data Protection para Windows e a tarefa no modo de espera virtual não serão executadas como foram programadas. É preciso configurar manualmente a máquina no modo de espera virtual para protegê-la.

Siga estas etapas:

1. Modifique o **Prefixo do nome da VM** na tarefa do Modo de espera virtual.

   Quando ligar as máquinas no modo de espera virtual, o aplicativo define os nomes das máquinas virtuais ligadas nas máquinas virtuais de acordo com a opção de **Prefixo do nome da VM** especificada na tarefa do Modo de espera virtual e o nome do host do nó de origem.

   Exemplo:

   - Prefixo do nome da VM: AA_
   - Nome do host do nó de origem: Server1
   - Nome da máquina virtual no modo de espera virtual: AA_Server1

   Depois de ligar as máquinas no modo de espera virtual, pode haver conflito com o nome da máquina virtual, caso o **Prefixo do nome da VM** não seja modificado na tarefa do Modo de espera virtual. Problemas desse tipo ocorrem quando os nós de origem e as máquinas modo de espera virtual residem no mesmo hypervisor.

   Se necessário, pode-se atualizar outras configurações de tarefas do Virtual Standby. Opcionalmente, você pode criar uma nova tarefa do Virtual Standby para proteger a máquina virtual do Virtual Standby.

2. Depois de implantar a tarefa na máquina no modo de espera virtual, retome a tarefa do Virtual Standby.

   Para obter mais informações, consulte Pausar e retomar tarefas virtuais no modo de espera.

3. Depois de implantar o plano, efetue logon no Agente do Arcserve Unified Data Protection para Windows, na máquina no modo de espera virtual e programe um método de repetição para a tarefa de backup do Agente do Arcserve Unified Data Protection para Windows.

   Para obter mais informações, consulte o *Guia do Usuário do Agente do Arcserve Uni-*

fied Data Protection para Windows.

Observação: pause e continue as tarefas do Virtual Standby.

Verifique se a máquina em modo de espera virtual está protegida

Verifique se as máquinas no modo de espera virtual estão protegidas confirmando que os pontos de recuperação válidos estão disponíveis no destino de backup.

Siga estas etapas:

1. Efetue logon no destino de backup e navegue até a pasta de destino de backup.
2. Verifique se o backup da máquina no modo de espera virtual foi bem-sucedido e se os pontos de recuperação estão disponíveis.

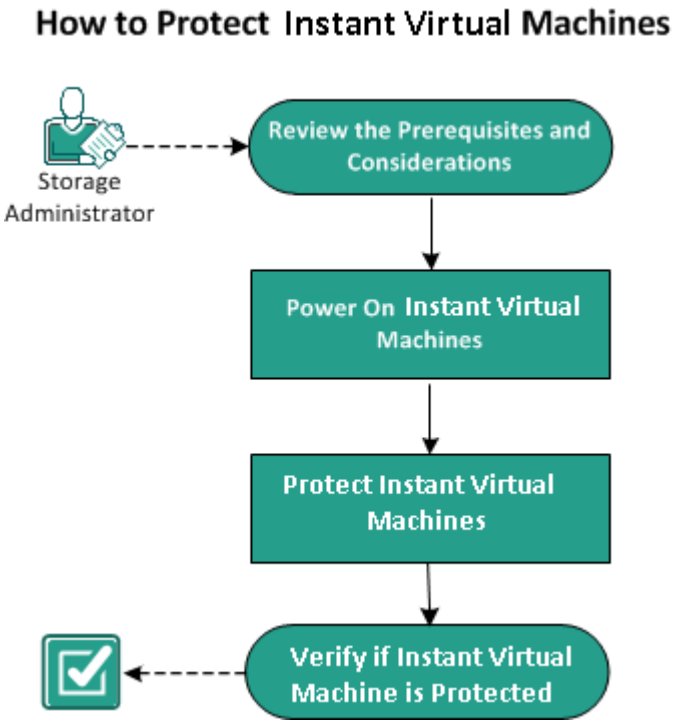
   O computador no modo de espera virtual é verificado.

   As máquinas no modo de espera virtual estão protegidas com êxito.

Como proteger máquinas virtuais instantâneas

É possível fazer backup das máquinas virtuais instantâneas e evitar que os dados sejam corrompidos. Para proteger o computador, talvez você precise ligar o computador.

O seguinte diagrama ilustra o processo para proteger as máquinas virtuais instantâneas:



O que fazer a seguir?

- Verificar os pré-requisitos e as considerações
- Ligar máquinas virtuais instantâneas
- Proteger máquinas virtuais instantâneas
- Verificar se a máquina virtual instantânea está protegida

Verificar os pré-requisitos e as considerações

Verifique se concluiu as seguintes tarefas de pré-requisito:

- Efetuou logon no console.
- Tem uma máquina virtual instantânea pronta.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Ligar máquinas virtuais instantâneas a partir do ponto de recuperação

Você pode criar máquinas virtuais instantâneas e proteger as máquinas virtuais manualmente a partir do ponto de recuperação, depois de se ligarem as máquinas.

Você pode selecionar Inicializar agora ou Inicializar mais tarde ao criar uma máquina virtual instantânea. Selecionar a opção Inicializar agora inicializa a máquina virtual instantânea imediatamente após a sua criação bem-sucedida. Caso contrário, você precisará ligar a VM instantânea manualmente.

É possível ligar as VMs instantâneas a partir do ponto de recuperação somente quando você deseja criar um ponto de recuperação para a máquina virtual que foi ligada.

Siga estas etapas:

1. na guia **recursos**, navegue até **Infraestrutura:** Grupo de nós **Máquinas virtuais instantâneas**.

   Os nós da VM instantânea são exibidos no painel central.

2. No painel central, selecione o nó, clique em **Ações** e, em seguida, clique em **Ligar** na lista suspensa.

   A máquina virtual é ligada usando os dados contidos no instantâneo do ponto de recuperação.

   Observação: após ligar a máquina virtual, poderá ser solicitado que você reinicie o computador uma ou mais vezes. Este comportamento ocorre pois o VMware instala o VMware Tools na máquina virtual e o Windows Hyper-V instala os serviços de integração.

   Depois de ligar as máquinas virtuais instantâneas a partir dos instantâneos do ponto de recuperação, talvez seja preciso concluir as seguintes tarefas:

   - Ativar o sistema operacional do Windows em execução na máquina virtual.
   - Iniciar o Agente do Arcserve Unified Data Protection para Windows na máquina virtual.
   - Atualize o Arcserve UDP com o nome do host, o endereço IP e as credenciais de logon na máquina virtual.

Proteger uma máquina virtual instantânea quando ela está ligada

Depois que uma máquina virtual instantânea estiver ligada (manual ou automaticamente), a tarefa de backup do Agente do Arcserve Unified Data Protection para Windows e a tarefa no modo de espera virtual não serão executadas como foram programadas. É preciso configurar manualmente a máquina virtual instantânea a ser protegida.

Siga estas etapas:

1. adicione uma máquina virtual instantânea ao console.

   Observação: você pode adicionar um nó especificando manualmente os detalhes do nó ou importando máquinas virtuais dos servidores ESX/vCenter e Hyper-V.

   Para obter mais informações, consulte Adicionar nós.

2. Adicionar um destino.

   Um destino pode ser um servidor do ponto de recuperação, uma pasta local ou uma pasta compartilhada remota.

3. Crie um plano para proteger o nó da máquina virtual instantânea.

   Um plano é um grupo de tarefas para gerenciar backup, replicação e criação de computadores no modo de espera virtual.

   Observação: você pode criar um plano com a tarefa de backup do Windows com base em agente ou a tarefa de backup sem agente com base em host.

4. Execute tarefas como backup, criar modo de espera virtual e replicar.

   Para obter mais informações, consulte o *Guia do Usuário do Agente do Arcserve UDP (Windows)*.

Verificar se a máquina virtual instantânea está protegida

Verifique se a máquina virtual instantânea está protegida confirmando que os pontos de recuperação válidos estão disponíveis no destino de backup.

Siga estas etapas:

1. Efetue logon no destino de backup e navegue até a pasta de destino de backup.
2. Verifique se o backup da máquina virtual instantânea foi bem-sucedido e se os pontos de recuperação estão disponíveis.

   A Máquina virtual instantânea é verificada.

   A proteção da máquina virtual foi realizada com êxito.

Como replicar dados entre repositórios de dados gerenciados de um console do UDP

Usando o Arcserve UDP, é possível replicar os dados de backup de um repositório de dados para outro. Esses repositórios de dados são gerenciados do mesmo console do UDP, mas estão em diferentes servidores de ponto de recuperação. É necessário criar um plano com duas tarefas--backup e replicar. A tarefa de backup irá fazer backup de dados com base na programação e a tarefa de replicação replicará os dados submetidos a backup para o servidor de ponto de recuperação especificado. A tarefa de replicação é executada de acordo com a programação especificada por você na tarefa de replicação. É possível criar várias tarefas de replicação em um plano.

Se a tarefa de replicação falhar por algum motivo (por exemplo, problema de rede), a tarefa de replicação com falha é retomada antes de transferir qualquer nova sessão. A tarefa de replicação é retomada do ponto de interrupção da última tarefa de replicação com falha.

O que fazer a seguir?

1. Verificar os pré-requisitos e as considerações
2. Criar um plano com uma tarefa de backup
3. Adicionar uma Tarefa de replicação ao Plano
4. (Opcional) Executar uma replicação manual
5. Verificar o plano

Verificar os pré-requisitos e as considerações

Verifique se concluiu os seguintes pré-requisitos:

- Efetue logon no Console.
- Instale o componente do servidor e crie Repositórios de dados.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Criar uma tarefa de backup

Um plano inclui tipos diferentes de tarefas que você deseja executar. Geralmente um plano inclui uma lista de tarefas principais seguida de uma tarefa secundária. Em geral, uma tarefa principal é uma tarefa de backup ou replicação a partir de uma tarefa remota do Console. A função de uma tarefa de backup é criar um backup de nós de origem que você deseja proteger. É possível fazer backup de dados do Windows, e de máquinas virtuais e físicas Linux. Em seguida, é possível salvar os dados de backup em outro local, como precaução adicional.

Para obter mais informações sobre:

- Como fazer backup de um nó do Windows, consulte Como criar um plano de backup do Windows.
- Como fazer backup de máquinas virtuais, consulte Como criar um plano de backup da máquina virtual com base em host.
- Como fazer backup de nós do Linux, consulte Como criar um plano de backup do Linux.

Adicionar uma Tarefa de replicação ao Plano

Crie uma tarefa de replicação para proteger ainda mais os seus dados, copiando os dados de backup a partir de um servidor de ponto de recuperação para outro servidor de ponto de recuperação. Você também pode copiar os dados de backup de um repositório de dados em outro repositório de dados no mesmo servidor de ponto de recuperação. O destino da replicação deve ser um repositório de dados no servidor de ponto de recuperação. É possível criar várias tarefas de replicação para executar várias replicações.

Observações:

- **Para a tarefa de mesclagem:** quando uma tarefa de replicação estiver configurada e você executar uma tarefa de mesclagem por demanda do repositório de dados de origem, a tarefa não verifica se as sessões estão replicadas ou não. Como resultado, as sessões de mesclagem não podem ser replicadas para o repositório de dados de destino e você acaba replicando mais dados. Por exemplo, considere que há cinco sessões, s1, s2, s3, s4 e s5, respectivamente. s1 e s2 são replicadas. Agora, você executa uma tarefa de mesclagem sob demanda no lado de origem e retém duas sessões. s4 e s5 são retidas. s4 é uma sessão completa. Portanto, quando a próxima tarefa de replicação for iniciada, a tarefa precisa replicar uma sessão completa.
- **Para a tarefa de limpeza:** quando uma tarefa de replicação estiver configurada e se você executar a tarefa de limpeza no repositório de dados de destino, a próxima tarefa de replicação replica todas as sessões para o repositório de dados de destino.
- Não é possível replicar do repositório de dados ativado com redução de redundância para o repositório de dados sem redução de redundância.
- Não é possível replicar do repositório de dados com criptografia ativada para o repositório de dados sem criptografia.

Siga estas etapas:

1. Clique em **Adicionar uma tarefa** no painel esquerdo.

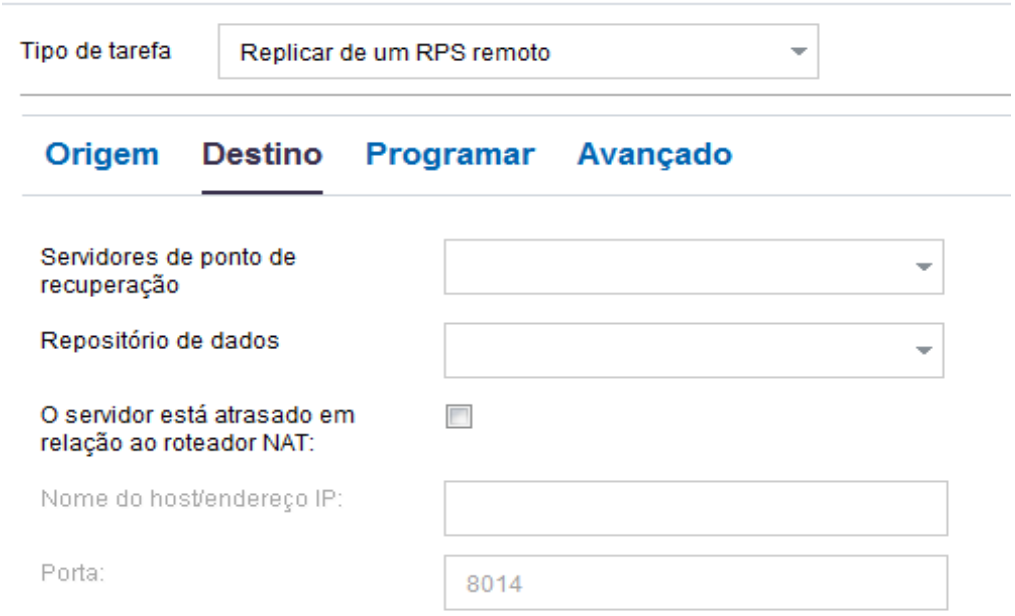
   Uma nova tarefa será adicionada ao painel esquerdo.

2. No menu suspenso, selecione **Tipo de tarefa,** selecione **Replicar**.

   A tarefa de Replicação é adicionada. Você não precisa configurar a guia **Origem** na tarefa de Replicação porque ela reflete o destino de backup da tarefa de backup.

   Observação: não é possível replicar uma tarefa sem a tarefa principal, como o backup do servidor de ponto de recuperação.

3. Clique na guia **Destino** e digite os detalhes do servidor de ponto de recuperação e repita os detalhes da programação.



Servidor de ponto de recuperação

Selecione o servidor de ponto de recuperação na lista.

Repositório de dados

Selecione o armazenamento de dados na lista.

Iniciar a repetição

Especifique o tempo (em minutos) para reiniciar a tarefa de replicação após falha da tarefa. Por exemplo, se especificar 10 minutos, a tarefa de replicação será reiniciada após 10 minutos da falha.

Limite: 1 a 60

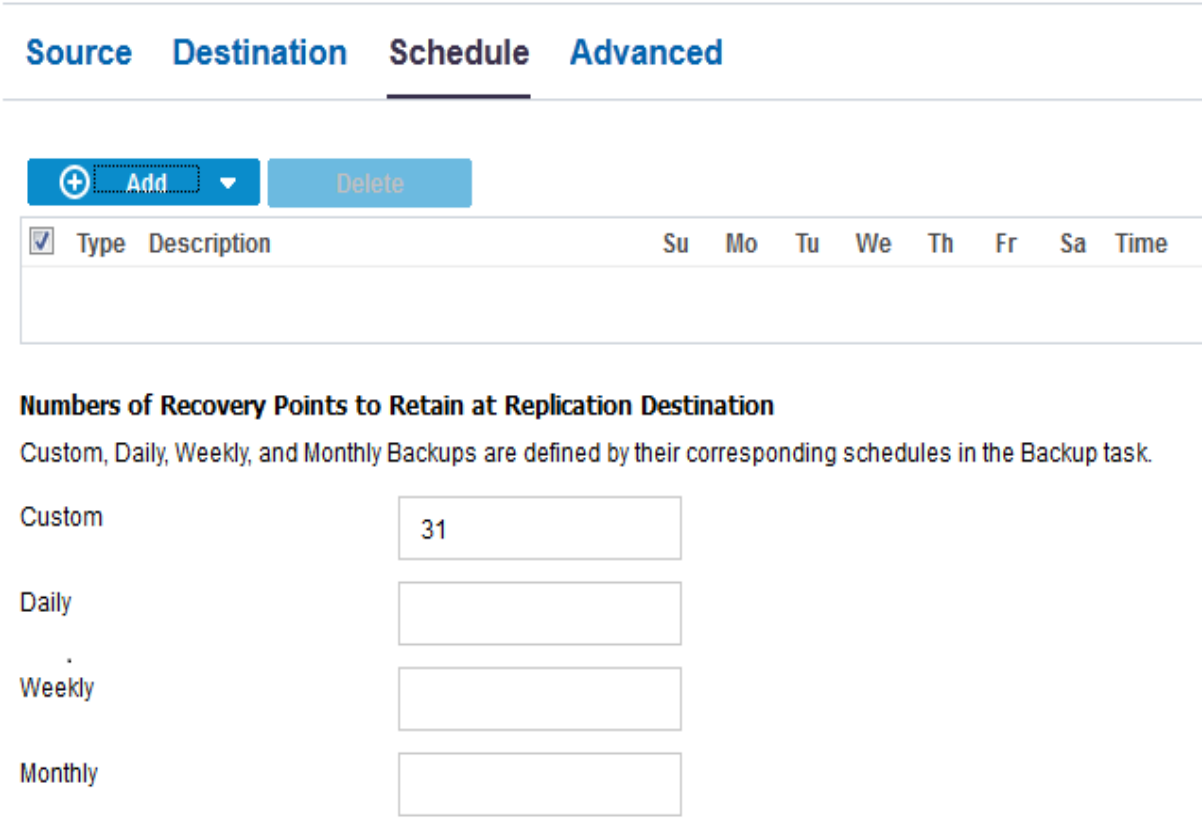
Repetir

Especifique o número de vezes que deseja iniciar a tarefa de replicação quando ocorrer uma falha na tarefa. A tarefa de replicação é executada até que a tarefa seja executada com êxito ou até que o limite seja alcançado.

Limite: 1 a 99

4. Clique na guia **Programar** e adicionar **Programação da tarefa de replicação**, **Programação do acelerador de replicação**, **Programação de mesclagem** e **Configurações de retenção**.

Observação: a cota do acelerador replicação é medianamente compartilhada por todas as tarefas de replicação começou a partir de todos os nós de um plano atual.



5. Clique na guia **Avançada** e digite os detalhes.
6. Clique em **Salvar alterações** ou **Adicionar uma tarefa**.

   Se tiver adicionado uma tarefa, será possível criar outra tarefa de replicação para executar vários níveis de replicação. É possível adicionar várias tarefas de replicação no plano.

   Se você salvar as alterações, o plano será salvo e a tarefa de replicação será implantada no destino de replicação.

   A tarefa de replicação é criada.

   Você criou com êxito e implantou automaticamente um plano de replicação.

(Opcional) Executar uma replicação manual

Para executar manualmente uma tarefa de replicação, é necessário ter pelo menos um backup de dados com êxito. Se não tiver definido a programação de replicação, essa tarefa de replicação será executada imediatamente após a tarefa de backup, caso contrário, ela depende da configuração de programação de replicação.

Siga estas etapas:

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.

   Caso você tenha adicionado algum planos, esse plano será exibido no painel central.
3. Selecione os nós que deseja fazer backup e que tenha um plano atribuído a ele.
4. No painel central, clique em **Ações**, **Replicar agora**.

   A caixa de diálogo **Replicar nó** é exibida.
5. Selecione o RPS de origem e o RPS de destino para a tarefa.
6. Clique em **OK**.

   A tarefa de replicação é executada.

   A replicação manual é realizada com êxito.

Verificar o plano

Para verificar o recurso de replicação, confirme se você criou com êxito o plano de replicação. Depois de verificar se o plano está criado com êxito, confirme se a tarefa de backup está executando conforme o programado. Depois que a tarefa de backup for concluída com êxito, a tarefa de replicação será executada. É possível verificar o status da tarefa de backup e da tarefa de replicação na guia **tarefas**.

Siga estas etapas: para verificar os planos

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.

   Uma lista de todos os nós é exibida no painel central.
3. Verifique se os planos são mapeados com nós.

Siga estas etapas: para verificar tarefas de replicação

1. Clique na guia **tarefas**.
2. No painel à esquerda, clique em **Todas as tarefas**.

   O status de cada tarefa é incluído no painel central.
3. Verifique se a tarefa de backup e a tarefa de replicação foram bem-sucedidas.

Como replicar dados entre repositórios de dados gerenciados a partir de diferentes consoles do UDP

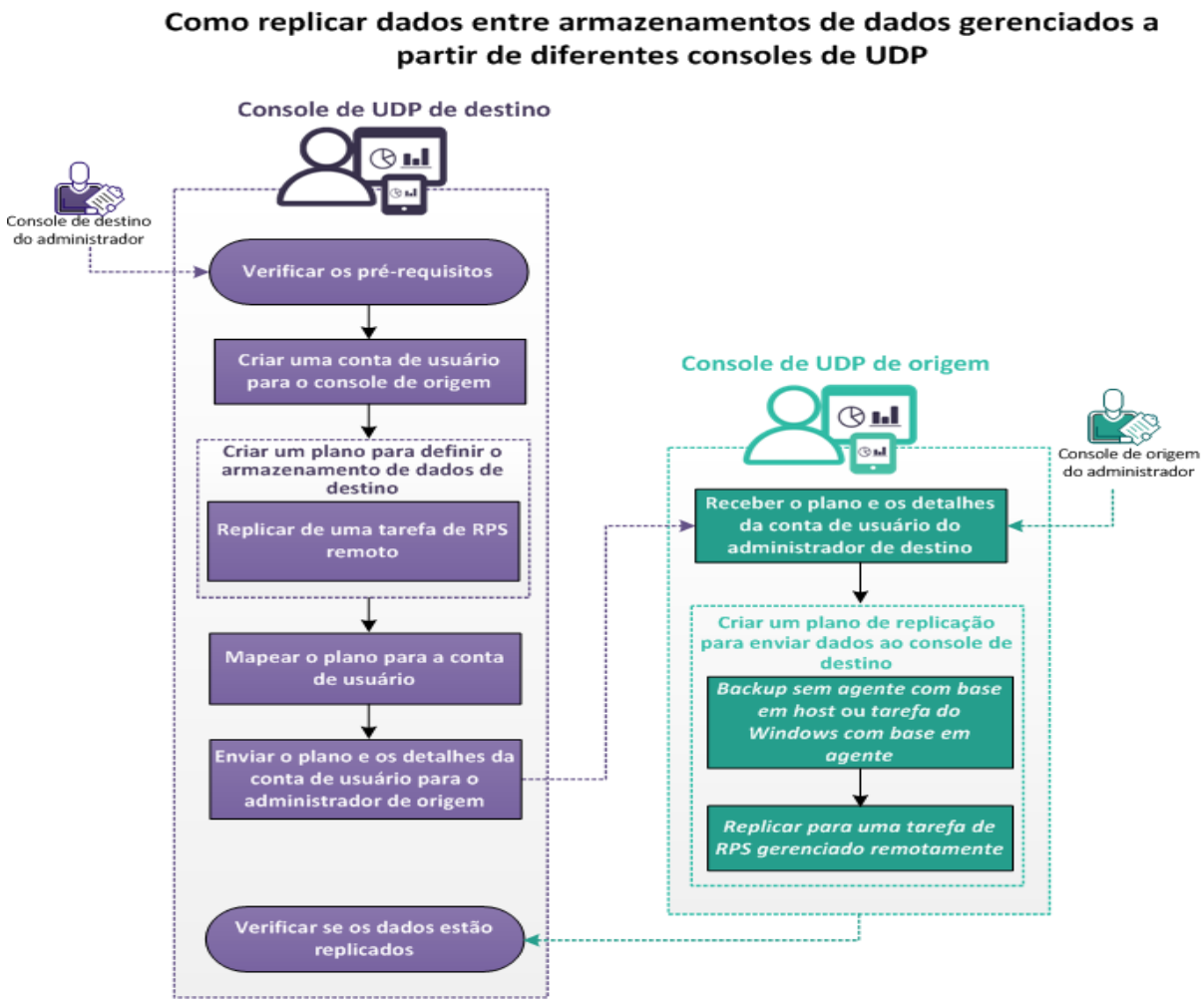
Para proteger os dados, talvez seja preciso replicar os dados de backup para outro servidor de ponto de recuperação que seja gerenciado a partir de um console diferente do Arcserve UDP. Por exemplo, você pode replicar os dados para um provedor de serviços que ofereça seus serviços de replicação a diversos clientes. Neste exemplo, os dados são replicados a partir de um repositório de dados de origem (no console de origem) para um repositório de dados de destino (no console de destino).

Como administrador do console de destino, crie um nome de usuário, uma senha e um plano de origem exclusivos para o console de origem. O plano define o repositório de dados de destino e o nome de usuário e a senha ajudam o administrador de origem a se conectar ao servidor e a replicar os dados.

Como administrador do console de origem, crie um plano para replicar dados para o repositório de dados de destino. Durante a criação do plano, conecte-se ao servidor de destino e selecione o plano que está atribuído a você pelo administrador de destino.

Observação: como prática recomendada, aconselhamos a configuração de parâmetros de multitransmissão. Para obter mais informações, consulte Configurar parâmetros de multitransmissão.

O diagrama a seguir ilustra como replicar dados para outro repositório de dados que é gerenciado a partir de um console diferente:



O que fazer a seguir?

1. Verificar os pré-requisitos
2. Criar uma conta de usuário para o console de origem
3. Criar um plano para definir o repositório de dados de destino
4. Mapear o plano para a conta de usuário
5. Enviar o plano e os detalhes da conta de usuário para o administrador de origem

6. Receber o plano e os detalhes da conta de usuário do administrador de destino
7. Criar um plano de replicação para enviar dados ao console de destino
8. Verificar se os dados estão replicados

Verificar os pré-requisitos

Verifique os pré-requisitos a seguir antes de replicar os dados:

- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Administrador — Console de destino

- Verifique se instalou o Arcserve UDP no servidor de destino.
- Verifique se você tem privilégios totais para criar contas de usuário do Windows no servidor de destino.
- Verifique se você ativou a caixa de seleção **Permitir a recuperação de pontos de recuperação** nas configurações avançadas durante a replicação de uma criação do plano de RPS gerenciado remotamente.

  Observação: se você não ativar a caixa de seleção **Permitir a recuperação de pontos de recuperação** e iniciar a tarefa de replicação inversa para o console remoto, será solicitado que ative o sinalizador Permitir recuperação remota para a replicação inversa.

Administrador — Console do UDP de origem

- Verifique se instalou o Arcserve UDP no servidor de origem.
- Verifique se você concluiu pelo menos um backup completo em um repositório de dados.

Criar uma conta de usuário para o console de origem

Administrador do destino

Para identificar e gerenciar os dados replicados no servidor de destino, crie uma conta de usuário do Windows. Se estiver gerenciando mais de um console de origem, crie uma conta de usuário para cada console de origem.

O administrador do console de origem usa esses detalhes da conta para estabelecer conexão com o servidor de destino.

Para criar uma conta de usuário em um sistema operacional Windows, use a seção Contas de usuário no Painel de Controle do Windows. Para obter mais informações sobre a criação de contas de usuário no Microsoft Windows, consulte a documentação da Microsoft.

Criar um plano para definir o repositório de dados de destino

Administrador do destino

Os dados de origem são replicados para este repositório de dados de destino. Para definir esse repositório de dados de destino, crie um plano. O plano permite definir o repositório de dados de destino e a programação de mesclagem.

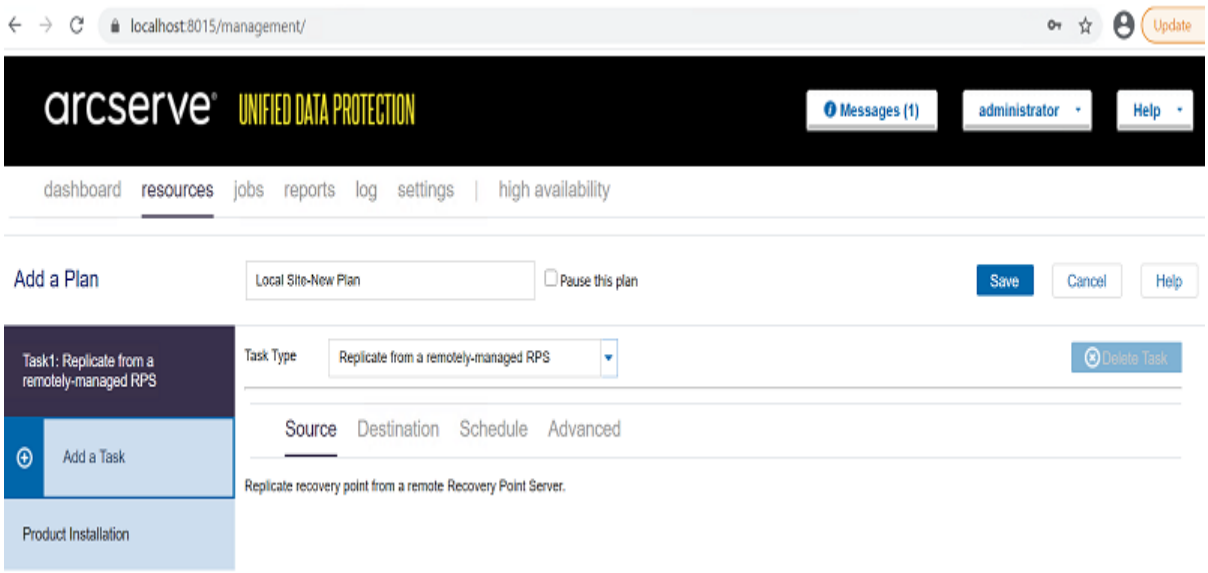
Siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Planos** e clique em **Todos os planos**.

   Caso tenha adicionado algum plano, ele estará no painel central.
3. No painel central, clique em **Adicionar um plano**.

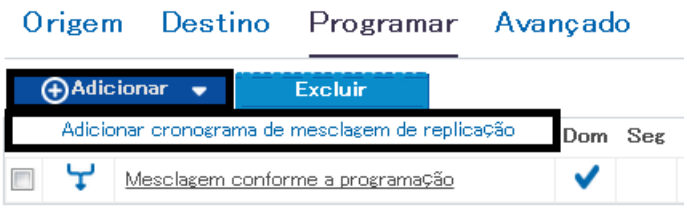
   A opção **Adicionar um plano** é aberta.
4. Digite um nome do plano no campo **Novo plano**.
5. Na lista suspensa **Tipo de tarefa**, selecione **Replicar de um RPS gerenciado remotamente**.

   A guia **Origem** é exibida. Não é possível fornecer nenhum detalhe na guia Origem. O administrador de origem no console de origem fornece os detalhes da origem.



6. Clique na guia **Destino** e especifique o servidor de ponto de recuperação e o repositório de dados.

7. (Opcional) Marque a caixa de seleção **Servidor está atrás do roteador NAT** e forneça o endereço do servidor e o número da porta.
8. Clique na guia **Programar**.

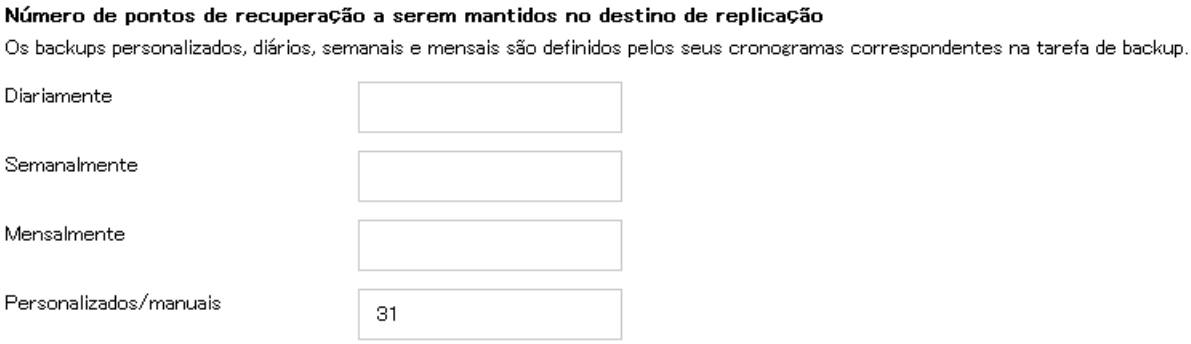


9. Clique em **Adicionar** e selecione **Adicionar programação de mesclagem de replicação**.

   A caixa de diálogo **Adicionar nova programação de mesclagem** é aberta.
10. Insira a programação de mesclagem.

    Observação: para saber mais sobre as programações, consulte Entendendo a programação avançada e a retenção.
11. Clique em **Salvar**.

    A caixa de diálogo **Adicionar nova programação de mesclagem** é fechada.
12. Digite os detalhes de retenção de pontos de recuperação.



13. Clique na guia **Avançado** e forneça os seguintes detalhes.

    Configuração de recuperação

    Permite executar a recuperação dos pontos de recuperação. Para ativar, marque a caixa de seleção **Permitir a recuperação dos pontos de recuperação**.

    Ativar alertas por email

    Permite ativar alertas por email. É possível especificar configurações de email e os tipos de alertas que você deseja receber por email. Ao selecionar esta opção, as seguintes opções serão ativadas para a seleção.

    Configurações de email

Permite configurar as definições de email. Clique em **Configurações de email** e configure o servidor de email e os detalhes do servidor proxy.

Alertas de tarefa

Permite selecionar os tipos de alertas de tarefas que deseja receber.

14. Clique em **Salvar**.

    As alterações são salvas e o plano é criado.

    O plano de replicação foi criado com êxito. Você também pode adicionar tarefas de replicação, tarefas de replicação para um RPS gerenciado remotamente e tarefas no modo de espera virtual ao plano.

Mapear o plano para a conta de usuário

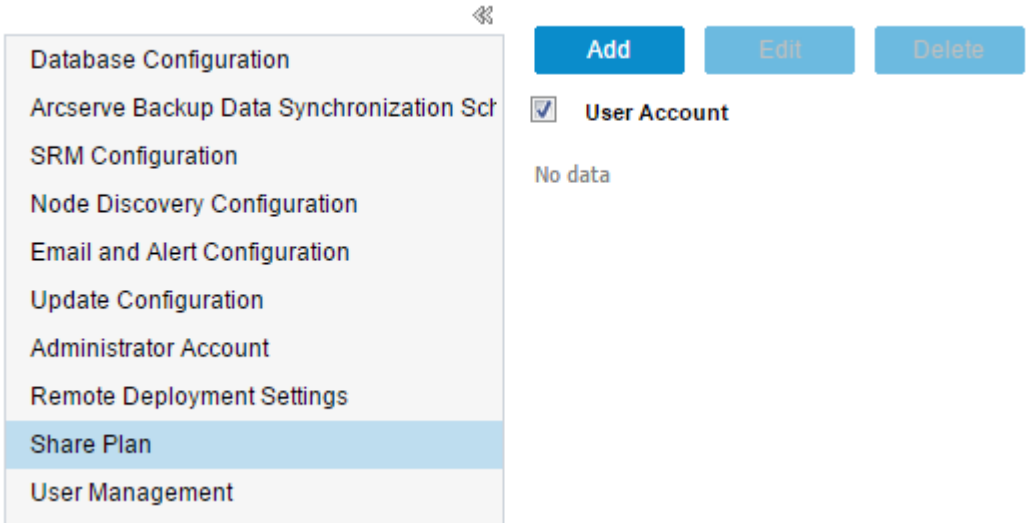
Administrador do destino

Você já criou uma conta de usuário e um plano para um console de origem. Para identificar e gerenciar dados replicados, atribua o plano à conta de usuário.

Observação: é possível atribuir mais de um plano a uma conta de usuário, mas duas contas diferentes não podem compartilhar um plano. No entanto, recomendamos atribuir um único plano a uma conta de usuário, para que você possa identificar e gerenciar facilmente os dados replicados.

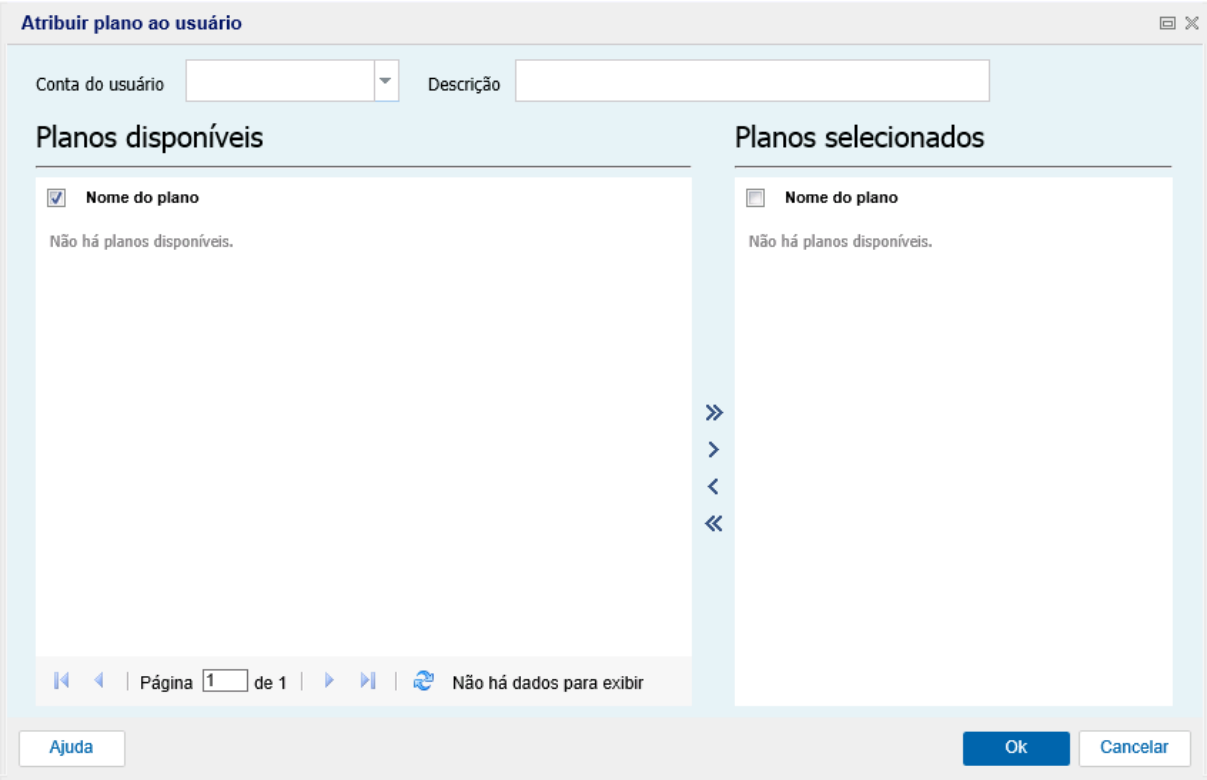
Siga estas etapas:

1. No Console, clique na guia **Configurações**.
2. No painel à esquerda, clique em **Plano de compartilhamento**.



3. No painel central, clique em **Adicionar**.

   A caixa de diálogo **Atribuir plano ao usuário** é exibida.



4. Selecione a **conta de usuário**.
5. Selecione um plano na coluna **Planos disponíveis**.

   Observação: se um plano já foi adicionado a um nome de usuário, ele não será exibido na coluna **Plano disponível**.
6. Clique em **Adicionar todos os planos** ou em **Adicionar planos selecionados** para adicionar os planos na coluna **Planos selecionados**.
7. Clique em **OK**.

   A caixa de diálogo **Atribuir plano ao usuário** é fechada. O nome de usuário e os planos associados são exibidos na página **Plano de compartilhamento**.

   A conta de usuário está mapeada para o plano criado para o console de origem.

   É possível usar a opção **Editar** para modificar a configuração do usuário ou **Excluir** para remover a conta de usuário da lista.

Enviar o plano e os detalhes da conta de usuário para o administrador de origem

Administrador do destino

Após o plano ser associado à conta de usuário, envie o plano e os detalhes da conta de usuário para o administrador de origem. O administrador de origem usa esses detalhes para se conectar ao console de destino.

Como administrador de destino, você concluiu todas as suas tarefas.

Receber o plano e os detalhes da conta de usuário do administrador de destino

Administrador de origem

Para replicar dados para o console de origem, você precisa do servidor de destino, do plano e dos detalhes da conta de usuário do administrador de destino. Você recebe os detalhes do administrador de destino. Compreenda os detalhes e obtenha esclarecimento para suas perguntas do administrador de origem antes de começar a criar os planos de replicação.

Criar um plano de replicação para enviar dados ao console de destino

Administrador de origem

Para replicar os dados de backup para o servidor de ponto de recuperação de destino que é gerenciado a partir de um console diferente, crie um plano de replicação. Esse plano de replicação inclui uma tarefa de backup e uma tarefa de replicação gerenciada remotamente. Na tarefa de replicação, especifique o servidor remoto e os detalhes do plano, e conecte-se ao servidor remoto. Se a conexão for bem-sucedida, selecione o plano que o administrador do destino criou para você.

Siga estas etapas:

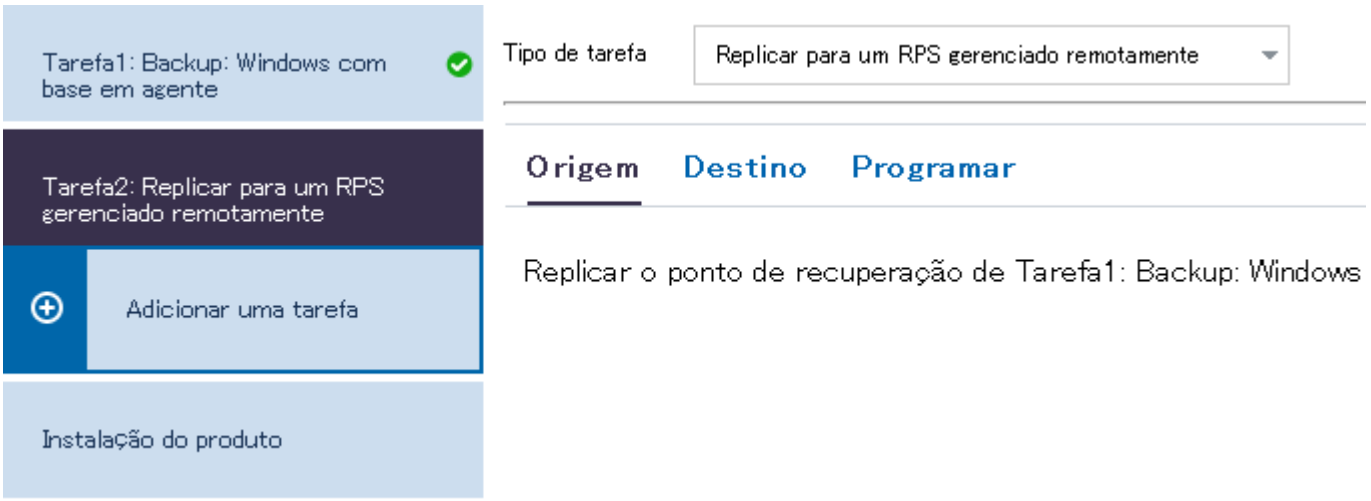
1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Planos** e clique em **Todos os planos**.
3. Clique em **Adicionar um plano**.

   A opção **Adicionar um plano** é aberta.
4. Digite o nome de um plano, selecione uma das seguintes tarefas de backup e crie a tarefa:
   - **Backup: Windows com base em agente**
   - **Backup: sem agente com base em host**
   - **Backup: Linux com base em agente**

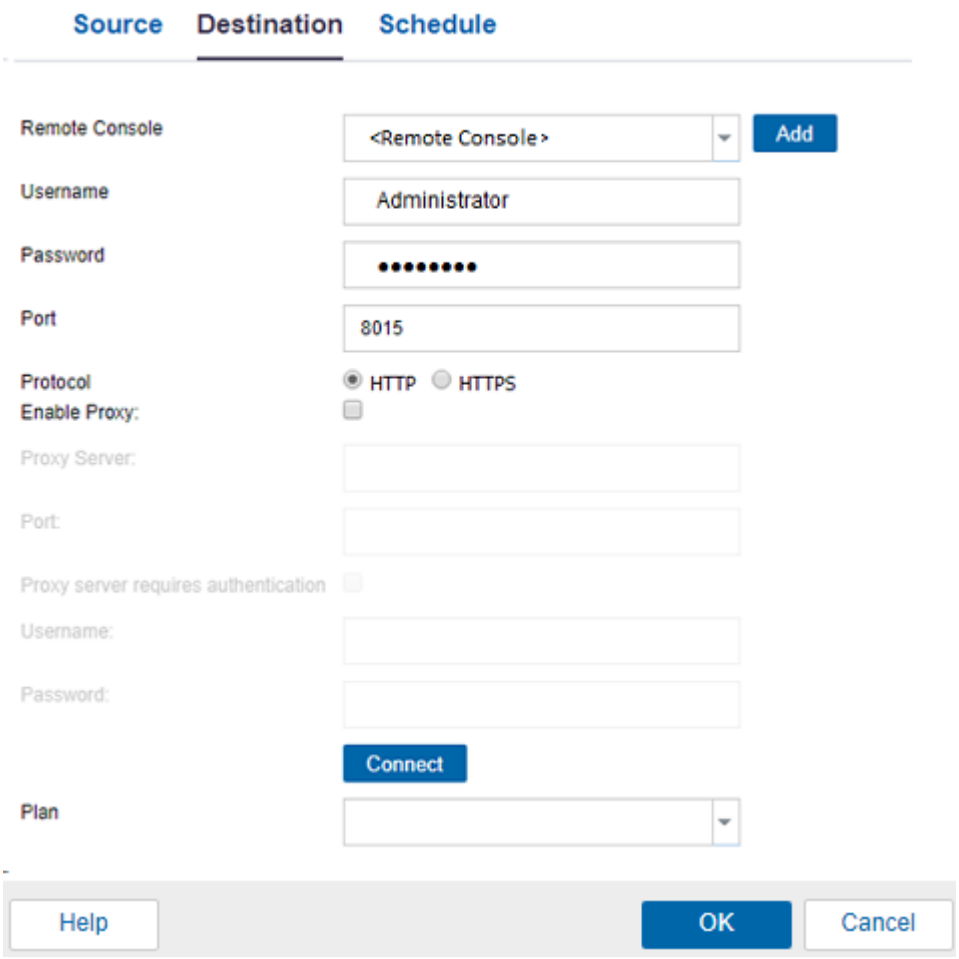
     Observação: para obter mais informações sobre como criar uma tarefa de backup, consulte os tópicos a seguir:
     - Como criar um plano de backup do Windows
     - Como criar um plano do Host-Based VM Backup
     - Como criar um plano de backup Linux
5. No painel à esquerda, clique em **Adicionar uma tarefa**.

   Uma nova tarefa será adicionada ao painel esquerdo.
6. No menu suspenso **Tipo de tarefa**, selecione **Replicar para um RPS gerenciado remotamente**.

   A tarefa Replicar é adicionada e a página **Origem** é aberta. Para a guia **Origem**, o destino da tarefa de backup (por exemplo, Backup: Windows com base em agente) é a origem da tarefa **Replicar para um RPS gerenciado remotamente**.



7. Clique na guia **Destino** e forneça os seguintes detalhes.



Console remoto

Selecione uma conta de console remoto da lista suspensa ou adicione uma nova conta de console remoto clicando no botão **Adicionar**.

Para obter mais informações, clique em Adicionar console remoto.

Nome de usuário

Especifique o nome de usuário criado pelo administrador do destino. O administrador de destino fornece o nome de usuário.

Senha

Especifique a senha criada pelo administrador de destino. O administrador de destino fornece a senha.

Porta

Especifique o número da porta do console de destino. O administrador de destino fornece o número da porta do console de destino.

Protocolo

Especifique o protocolo usado pelo administrador de destino para estabelecer conexão com o console de destino.

Ativar proxy

Marque a caixa de seleção para ativar a seleção do servidor proxy.

Servidor proxy

Especifica o endereço do servidor proxy.

Porta

Especifique o número da porta do servidor proxy.

O servidor proxy exige autenticação

Marque a caixa de seleção para ativar os campos de autenticação para o servidor proxy.

Nome de usuário

Especifique o nome de usuário para se conectar ao servidor proxy.

Senha

Especifique a senha para autenticar a conexão com o servidor proxy.

Conectar

Verifica a conexão entre o console de origem e o console de destino. Se a conexão for bem-sucedida, será possível ver o nome do plano no campo **Plano**. Esse nome do plano é atribuído a este console pelo administrador de destino.

Plano

Especifique o plano que o administrador de destino criou para você. Se houver vários planos na lista, entre em contato com o administrador de destino para saber o plano correto.

Iniciar a repetição

Executa novamente a tarefa de replicação após a hora especificada se houver uma falha. Digite um valor entre 1 e 60 e a hora é definido em minutos.

Repetir

Especifique o número de repetições que deseja executar se houver uma falha na tarefa. Após o número de repetições terminar, a tarefa de replicação será executada somente na próxima hora programada. Digite um valor entre 1 e 99.

8. Clique na guia **Programar** e forneça a cronograma da tarefa de replicação e a cronograma do acelerador de replicação.

   Cronograma da tarefa de replicação

   Especifique a data e a hora para iniciar as tarefas de replicação. É possível editar ou excluir a cronograma da tarefa de replicação.

   Cronograma do acelerador de replicação

   Especifique a velocidade máxima (Mbps) em que a replicação é realizada. É possível acelerar a velocidade da replicação para reduzir a utilização da CPU ou da rede. Para uma tarefa de replicação, a guia **tarefas** exibe a velocidade média de leitura e gravação da tarefa em andamento e o limite de velocidade do acelerador configurado.

   É possível editar ou excluir um cronograma do acelerador de replicação.

9. Clique em **Salvar**.

   O plano é salvo e executado de acordo com a programação.

   Você criou com êxito e implantou automaticamente um plano de replicação. Quando o plano é executado, os dados são replicados a partir do local de origem para o local de destino de dados em uma rede.

   Observação: depois que o processo de replicação estiver concluído, os detalhes do nó de replicação são automaticamente adicionados ao console de destino.

   Você replicou com êxito os dados entre dois repositórios de dados gerenciados por diferentes consoles do UDP.

Verificar se os dados estão replicados

Administrador do destino

Depois que os dados são replicados, é possível verificar se a replicação foi bem-sucedida.

Siga estas etapas:

1. No console de destino, vá até o repositório de dados de destino no servidor de ponto de recuperação.
2. Verifique se o tamanho dos dados replicados corresponde ao dados de origem.

   Você replicou com êxito os dados entre dois repositórios de dados gerenciados por diferentes consoles do UDP.

Como executar uma replicação de dados offline usando o início rápido do RPS

Replicar um grande repositório de dados para outro servidor de ponto de recuperação (gerenciado de um outro console do UDP) é demorado em uma rede (LAN, WAN, internet). Para replicar um grande repositório de dados de forma rápida, o Arcserve UDP fornece um método de replicação de dados offline. Esse método é chamado de Início rápido do RPS.

O início rápido do RPS é um método de replicação offline que usa um dispositivo de armazenamento externo, como uma unidade flash USB, para replicar um repositório de dados. Essa replicação é entre dois repositórios de dados que são gerenciados de diferentes consoles do UDP. Por exemplo, considere um provedor de serviços que oferece seus serviços de replicação para diversos clientes. O cliente replica os dados para um dispositivo de armazenamento e envia o dispositivo de armazenamento para o provedor de serviços. O provedor de serviços replica os dados do dispositivo de armazenamento para o servidor de destino. Tanto o provedor de serviços quanto o cliente devem ter o Arcserve UDP instalado em seus locais.

A replicação offline exige que os dois administradores (o da origem e o de destino) concluam as etapas a seguir em seus respectivos locais.

Importante: se você estiver replicando de uma pasta compartilhada para um repositório de dados selecionado no servidor de ponto de recuperação, consulte Como migrar o ponto de recuperação r16.5 para o Arcserve UDP.

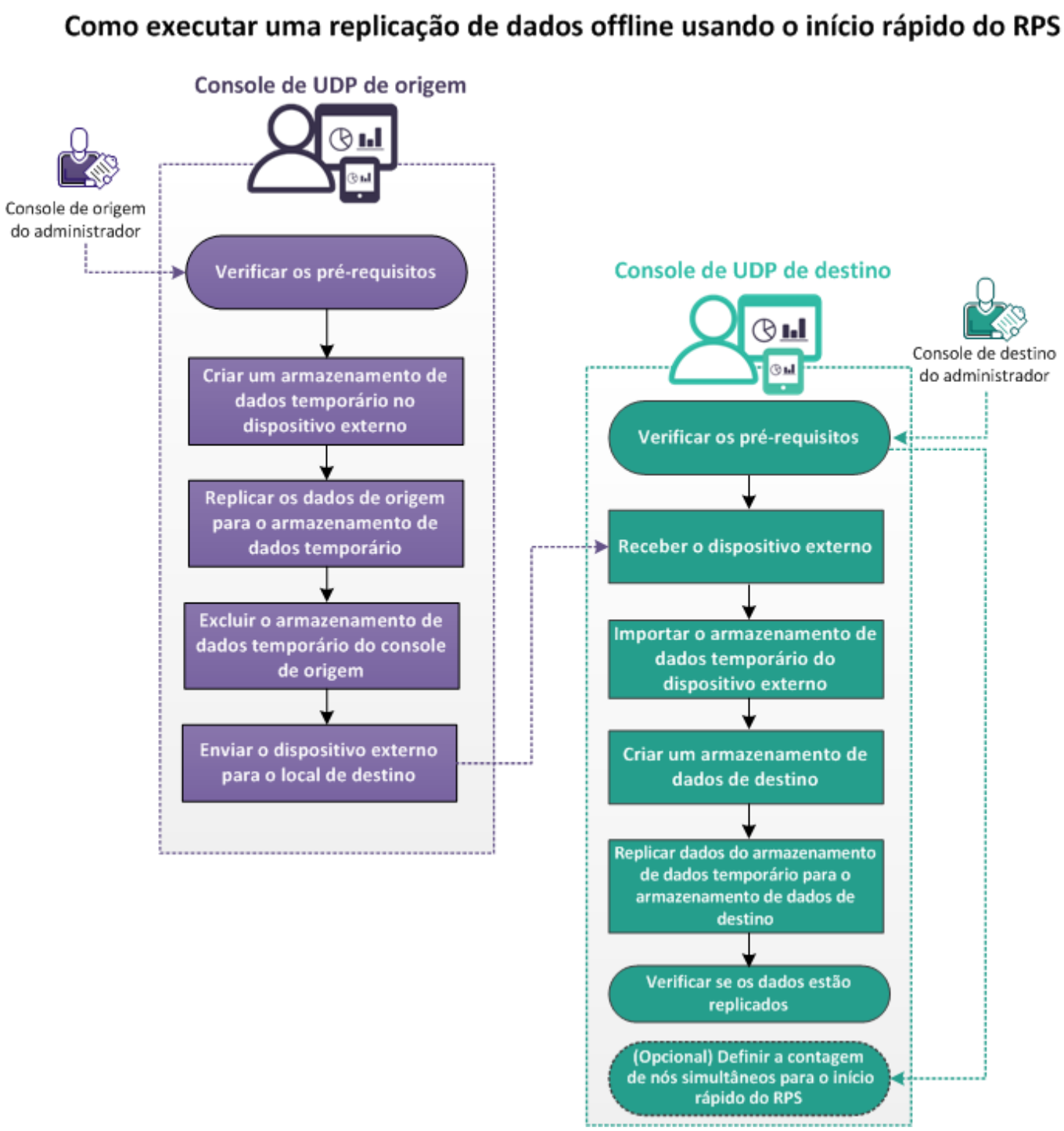
Administrador de origem

1. Replicar o repositório de dados de origem para um dispositivo externo.
2. Enviar o dispositivo externo para o local de destino.

Administrador do destino

1. Receber o dispositivo externo.
2. Replicar o repositório de dados de origem a partir do dispositivo externo para o servidor de ponto de recuperação de destino.

O diagrama a seguir ilustra como executar uma replicação de dados offline usando o início rápido do RPS.



O que fazer a seguir?

- Verificar os pré-requisitos
- Criar um repositório de dados temporário em um dispositivo externo
- Replicar os dados de origem para o repositório de dados temporário
- Excluir o repositório de dados temporário do console de origem

- Enviar o dispositivo externo para o local de destino
- Receber o dispositivo externo
- Importar os dados temporários do dispositivo externo
- Criar um repositório de dados de destino
- Replicar dados do repositório de dados temporário para o repositório de dados de destino
- Verificar se os dados são replicados
- (Opcional) Definir a contagem de nós simultâneos para o início rápido do RPS

Verificar os pré-requisitos

Verifique os pré-requisitos a seguir antes de realizar uma replicação de dados offline:

- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.
- Se a origem for um repositório de dados ativado para a redução de redundância, o destino também deverá ser um repositório de dados ativado para a redução de redundância.
- Se a origem for um repositório de dados ativado para criptografia, o destino também deverá ser um repositório de dados ativado para criptografia.

Administrador — Console de origem

- Verifique se você criou o repositório de dados de origem.
- Verifique se você concluiu pelo menos um backup em um repositório de dados.
- (Opcional) Verifique se você configurou a contagem de nós simultâneos para o início rápido do RPS. Para obter mais informações sobre a configuração da contagem de nós simultâneos, consulte Definir a contagem de nós simultâneos para o início rápido do RPS.

Administrador — Console de destino

- Verifique se você tem espaço disponível suficiente para a replicação.
- Verifique se você tem os privilégios necessários no dispositivo externo.

Criar um repositório de dados temporário em um dispositivo externo

Administrador de origem

Para importar dados de um repositório de dados existente para um dispositivo externo, primeiro crie um repositório de dados temporário no dispositivo externo. Para criar o repositório de dados temporário, conecte o dispositivo externo ao computador.

Siga estas etapas:

1. Efetue logon no console do UDP.
2. Navegue para **Destinos**, **Servidor do ponto de recuperação**.
3. Selecione o servidor do ponto de recuperação.
4. Clique com o botão direito do mouse e selecione **Adicionar um armazenamento de dados**.
5. Digite os detalhes na página **Adicionar um repositório de dados**.

   Observação: certifique-se de que as pastas de destino do backup estejam no dispositivo externo.
6. Salve o repositório de dados.

   O repositório de dados temporário é criado no dispositivo externo.

Replicar os dados de origem para o repositório de dados temporário

Administrador de origem

Depois de criar o repositório de dados temporário no dispositivo externo, é possível replicar os dados de origem para o dispositivo externo usando o início rápido do RPS.

Observação: antes de começar o processo de início rápido do RPS, pause o plano relacionado. Pausar o plano garante que nenhuma tarefa de replicação programada inicie quando o processo de início rápido estiver em andamento.

Siga estas etapas:

1. Clique em **Ações** e, em seguida, clique em **Início rápido do RPS**.

   O **Assistente do RPS Jumpstart** será exibido.

2. Selecione se você deseja migrar do mesmo repositório de dados ou de um local compartilhado.
3. Selecione o servidor do ponto de recuperação de origem, o repositório de dados de origem e o plano.

   Os nós que pertencem ao plano são exibidos.

4. Selecione os nós que você deseja migrar.
5. Clique em **Avançar**.

   A página **Selecionar armazenamento de dados de destino** é aberta. Se o repositório de dados de origem for criptografado, somente os repositórios de dados criptografados serão exibidos na lista suspensa.

6. Selecione o repositório de dados de origem. Selecione o repositório de dados de destino no dispositivo externo.
7. Clique em **Concluir**.

   A seção **Eventos recentes** no painel direito exibe o andamento da replicação.

   Após a conclusão do processo de replicação, os dados são replicados para o repositório de dados temporário. Você pode verificar o tamanho de ambos os repositórios de dados a partir da página **Destinos: Servidores de ponto de recuperação**.

Excluir o repositório de dados temporário do console de origem

Administrador de origem

Para manter a integridade dos dados no dispositivo externo, exclua o repositório de dados temporário do console do UDP antes de remover o dispositivo externo.

Observação: excluir o repositório de dados temporário do console do UDP de origem não exclui os arquivos do repositório de dados do dispositivo externo.

Siga estas etapas:

1. Clique com o botão direito do mouse no repositório de dados temporário e clique em **Interromper**.

   O repositório de dados é interrompido.

2. Clique com o botão direito do mouse no repositório de dados temporário e selecione **Excluir**.

   Uma caixa de diálogo de confirmação é exibida.

3. Clique em **Sim**.

   O repositório de dados é excluído.

   Agora você pode remover o dispositivo externo do computador.

Enviar o dispositivo externo para o local de destino

Administrador de origem

Depois que você remover o dispositivo externo, envie o dispositivo para o local de destino.

Receber o dispositivo externo

Administrador do destino

Receba o dispositivo externo que inclui os dados de origem. Agora, conecte esse dispositivo externo ao servidor de destino.

Importar o repositório de dados temporário do dispositivo externo

Administrador do destino

Antes de poder replicar os dados de origem para o repositório de dados de destino, importe o repositório de dados temporário para o servidor de ponto de recuperação de destino.

Siga estas etapas:

1. Navegue até a guia **Recursos** e selecione o servidor do ponto de recuperação para o qual deseja importar o armazenamento de dados.
2. Clique com o botão direito do mouse no servidor do ponto de recuperação e selecione **Importar armazenamento de dados**.

   A caixa de diálogo **Importar um repositório de dados** é aberta.
3. Selecione a pasta de destino de backup a partir do dispositivo externo.
4. Clique em **Avançar**.

   Os detalhes do repositório de dados temporário são exibidos. Se necessário, altere os dados, o índice e o caminho de hash.
5. Clique em **Salvar**.

   O repositório de dados é importado e você pode vê-lo no console de destino.

Criar um repositório de dados de destino

Administrador do destino

Para replicar dados do repositório de dados temporário, primeiro crie um repositório de dados de destino. Para obter mais informações, consulte Adicionar um repositório de dados.

Observação: também é possível usar um repositório de dados existente como um repositório de dados de destino.

Replicar dados do repositório de dados temporário para o repositório de dados de destino

Depois de criar o repositório de dados de destino, replique os dados do repositório de dados temporário para o repositório de dados de destino. Depois que os dados são replicados para o repositório de dados de destino, você pode excluir o repositório de dados temporário.

Siga estas etapas:

1. Clique em **Ações** e, em seguida, clique em **Início rápido do RPS**.

   O **Assistente do RPS Jumpstart** será exibido.

2. Selecione o servidor do ponto de recuperação de destino e o repositório de dados de origem. Qual plano deve ser selecionado aqui.

   Os nós são exibidos.

3. Selecione os nós que você deseja migrar.

4. Clique em **Avançar**.

   A página **Selecionar armazenamento de dados de destino** é aberta. Se o repositório de dados de origem for criptografado, somente os repositórios de dados criptografados serão exibidos na lista suspensa.

5. Selecione o repositório de dados de origem. Selecione o repositório de dados de destino no dispositivo externo.

6. Clique em **Concluir**.

   A seção **Eventos recentes** no painel direito exibe o andamento da replicação.

   Após a conclusão do processo de replicação, os dados são replicados para o repositório de dados temporário. Você pode verificar o tamanho de ambos os repositórios de dados a partir da página **Destinos: Servidores de ponto de recuperação**.

   Os dados são replicados para o repositório de dados de destino.

Verificar se os dados são replicados

Administrador do destino

Depois que os dados são replicados, é possível verificar se a replicação foi bem-sucedida.

Siga estas etapas:

1. No console de destino, vá até o repositório de dados de destino no servidor de ponto de recuperação.
2. Verifique se o tamanho dos dados replicados corresponde ao dados de origem.

   Você replicou com êxito os dados entre dois repositórios de dados gerenciados por diferentes consoles do UDP.

(Opcional) Definir a contagem de nós simultâneos para o início rápido do RPS

Administrador de origem

Ao iniciar uma tarefa de início rápido do RPS, o valor do nó simultâneo para o repositório de dados é 4, por padrão. Para especificar a contagem de nós simultâneos, crie uma chave e adicione manualmente um DWORD para definir a contagem.

Siga estas etapas:

1. Efetue logon no servidor do ponto de recuperação.
2. Vá até o seguinte local:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine
3. Crie uma chave no diretório de mecanismo e nomeie a chave como *Início rápido do RPS*.
4. Adicione o DWORD a seguir na chave Início rápido do RPS:

   JumpStartConCurrencyCount
5. Forneça um valor de DWORD.

   Exemplo: se desejar limitar a 10 nós por tarefa de início rápido do RPS, adicione o seguinte valor como DWORD:

   JumpStartConCurrencyCount=10

   A contagem de nós simultâneos é definida para o início rápido do RPS.

Como executar a replicação inversa

Usando esse recurso, é possível replicar dados (ponto de recuperação) da nuvem, do MSP ou do RPS gerenciado remotamente para o UDP local ou o servidor RPS no local. Para recuperar os dados replicados de volta para o UDP local ou para o servidor local a partir de um servidor de ponto de recuperação que é gerenciado a partir de um console do Arcserve UDP diferente, como nuvem, MSP ou RPS gerenciado remotamente, é necessário executar a replicação inversa. Na replicação inversa, os dados são replicados de um repositório de dados de destino (no console de destino) para um repositório de dados de origem (no console de origem).

Esta seção contém os seguintes tópicos:

Verificar os pré-requisitos

Verifique os pré-requisitos a seguir antes de replicar os dados:

- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Administrador — Console de destino

- Verifique se instalou o Arcserve UDP no servidor de destino.
- Verifique se você tem privilégios totais para criar contas de usuário do Windows no servidor de destino.
- Verifique se você ativou a caixa de seleção **Permitir a recuperação de pontos de recuperação** nas configurações avançadas durante a replicação de uma criação do plano de RPS gerenciado remotamente.

  Observação: se você não ativar a caixa de seleção **Permitir a recuperação de pontos de recuperação** e iniciar a tarefa de replicação inversa para o console remoto, será solicitado que ative o sinalizador Permitir recuperação remota para a replicação inversa.

Administrador — Console do UDP de origem

- Verifique se instalou o Arcserve UDP no servidor de origem.
- Verifique se você concluiu pelo menos um backup completo em um repositório de dados.

Executar replicação ad hoc

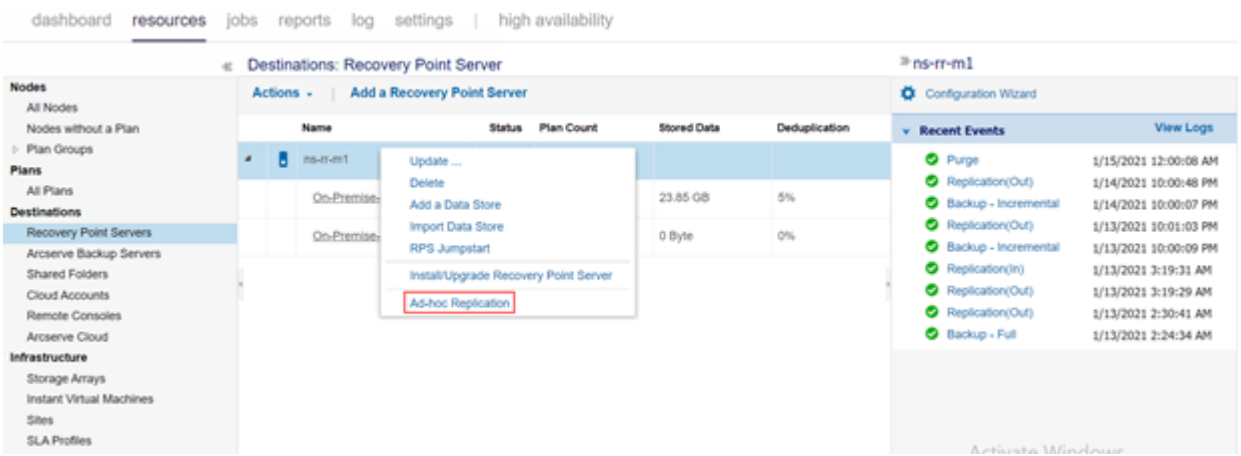
Esta seção explica como iniciar a replicação ad hoc.

Observação: antes de executar a replicação ad hoc, certifique-se de que a replicação de encaminhamento seja executada com êxito. Para verificar se a replicação de encaminhamento foi bem-sucedida, consulte Verificar se os dados estão replicados.

Siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel esquerdo, navegue para **Destinos** > **Servidores de ponto de recuperação**.

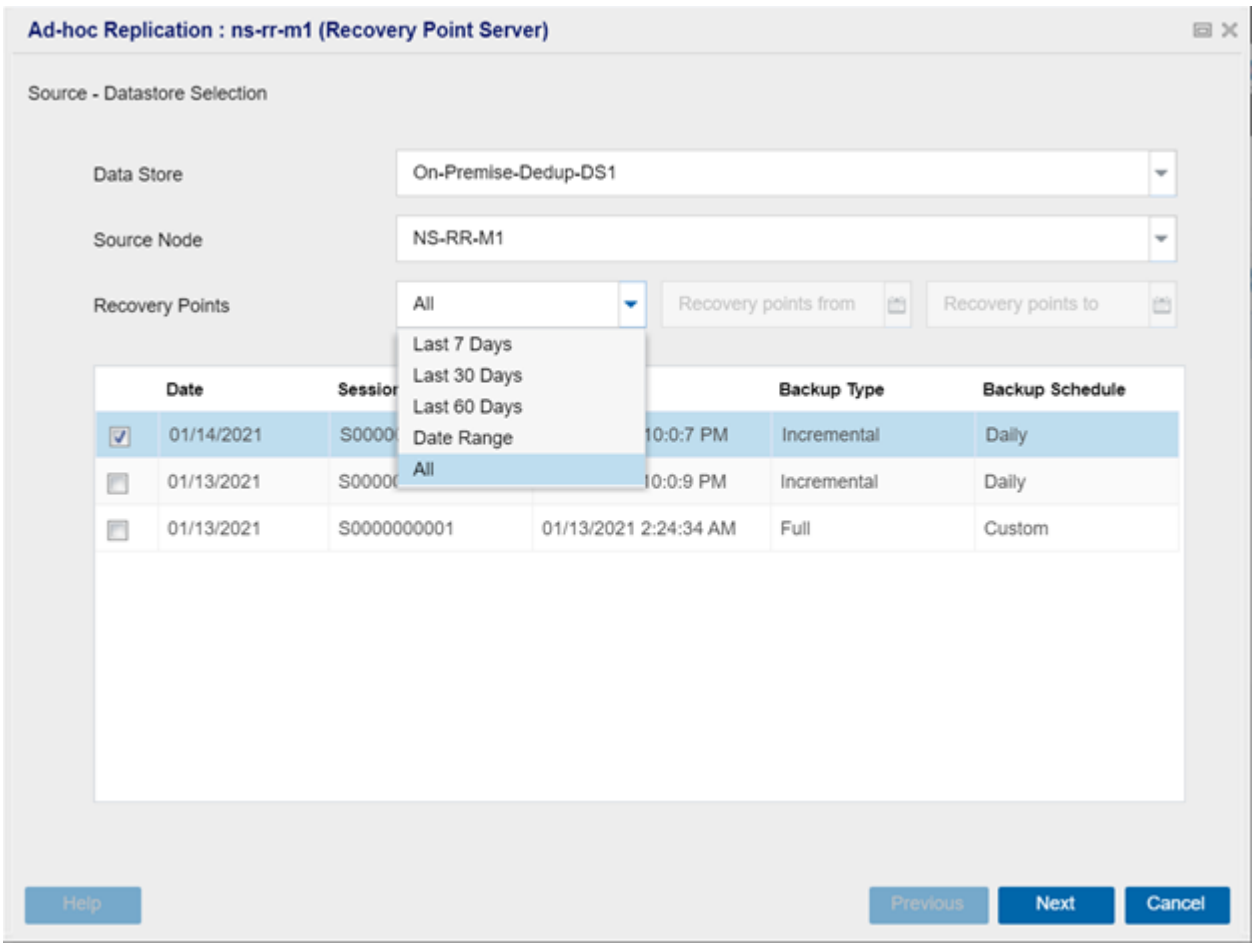
   A lista de servidores de ponto de recuperação é exibida no painel central.
3. Clique com o botão direito do mouse no servidor de ponto de recuperação e selecione **Replicação ad hoc**.



Aguarde até que você se conecte ao servidor de ponto de recuperação.

A caixa de diálogo Replicação ad hoc: xx-xx-xx (Servidor de ponto de recuperação) é aberta.

4. Na página Origem - seleção do repositório de dados, faça o seguinte:



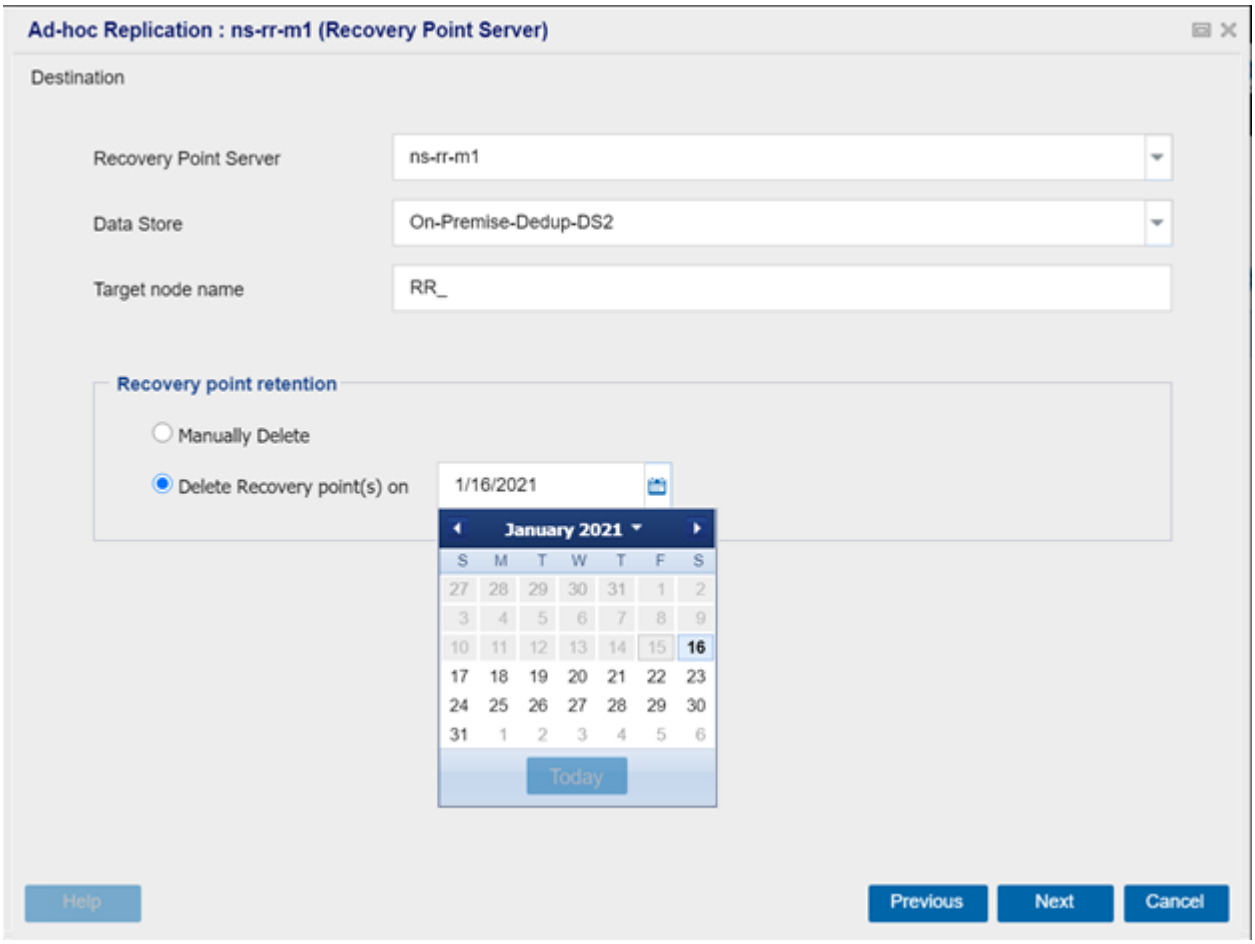
- Repositório de dados - selecione o repositório de dados de origem na lista suspensa.

- Nó de origem - selecione o nó de origem na lista suspensa.
- Pontos de recuperação - execute um dos seguintes procedimentos:
  - Se desejar que todos os pontos de recuperação armazenados em backup sejam exibidos, selecione **Todos** na lista suspensa.
  - Se desejar que os pontos de recuperação sejam exibidos por uma duração específica, selecione um dos seguintes itens na lista suspensa:
    - Últimos 7 dias
    - Últimos 30 dias
    - Últimos 60 dias
    - Intervalo de datas

    Observação: se você selecionou **Intervalo de datas**, defina a data nos campos **Pontos de recuperação de** e **Ponto de recuperação até**.

  Todos os pontos de recuperação associados entre a duração especificada serão exibidos.
- Na tabela, clique nas caixas de seleção para selecionar um ou mais pontos de recuperação.

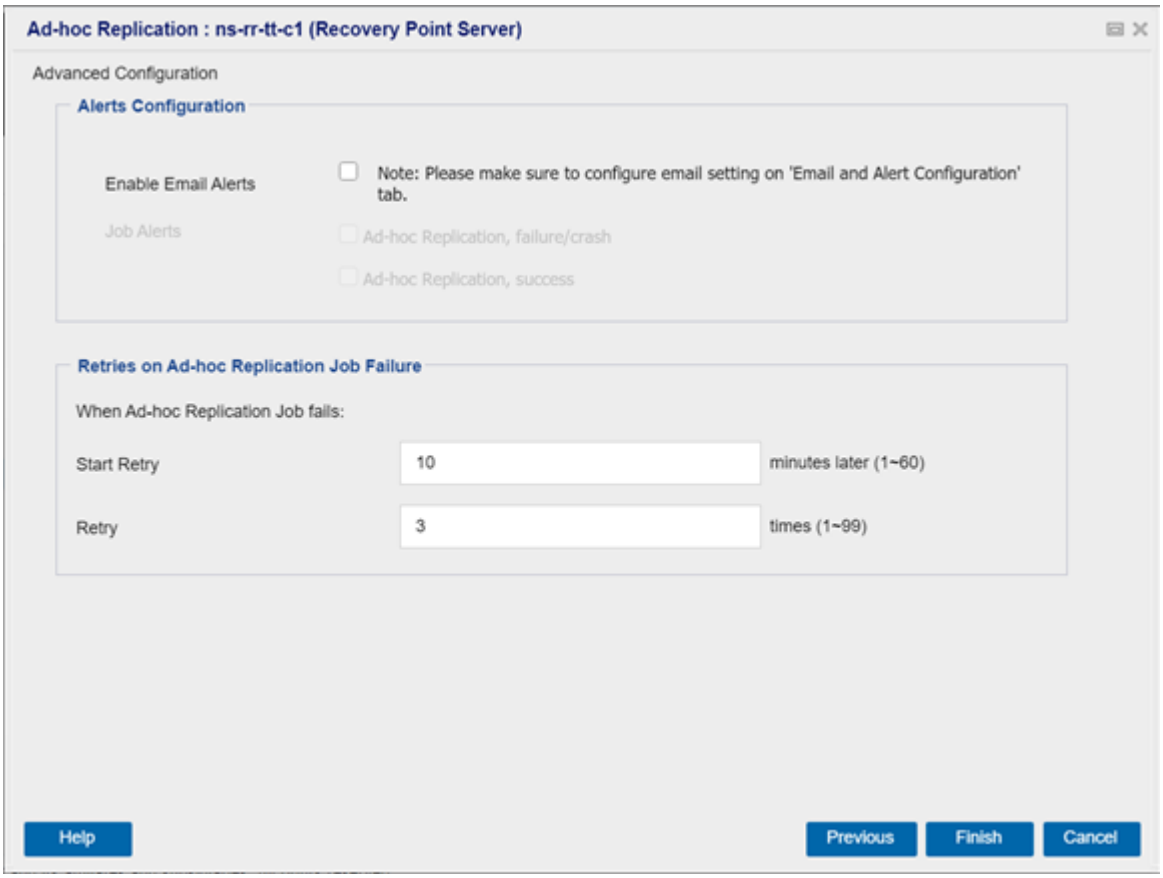
5. Clique em **Avançar**.
6. Na página Destino, faça o seguinte:



- Servidor de ponto de recuperação - selecione o servidor de ponto de recuperação de destino na lista suspensa.
- Repositório de dados - selecione o repositório de dados de destino na lista suspensa.
- Nome do nó de destino - digite um nome de nó de destino de sua escolha.
- Retenção do ponto de recuperação - exclua os pontos de recuperação de uma das seguintes maneiras:
  - Para excluir pontos de recuperação manualmente, selecione a opção **Excluir manualmente**.
  - Se desejar que os pontos de recuperação sejam excluídos automaticamente, selecione a opção **Excluir pontos de recuperação em** e, em seguida, especifique a data. Todos os pontos de recuperação correspondentes a essa data serão excluídos automaticamente.

7. Clique em **Avançar**.

8. Na página Configuração avançada, faça o seguinte:



- Para a configuração de alertas

  Ativar alertas por email

  Permite ativar alertas por email. É possível especificar configurações de email e os tipos de alertas que você deseja receber por email. Ao marcar a caixa de seleção **Observação: certifique-se de definir a configuração de email na guia "Configuração de email e alerta".**, a seguinte opção é ativada para sua seleção:

  Alertas de tarefa

  Permite selecionar os tipos de emails de alerta de tarefas que você deseja receber.

- Se desejar receber alertas por email sobre falhas ou travamentos na replicação ad hoc, marque a caixa de seleção **Replicação ad hoc, Falha ou travamento**.

  Observação: este alerta por email é enviado com uma importância alta. Os alertas por email que apresentam uma con-

figuração com nível de prioridade alta, exibem um indicador visual de um ponto de exclamação em sua caixa de entrada.

- Se desejar receber alertas por email sobre o êxito da replicação ad hoc, marque a caixa de seleção **Replicação ad hoc, Êxito**.

- Para novas tentativas em relação à falha na tarefa de replicação ad hoc

  Quando a tarefa de replicação ad hoc falhar, faça o seguinte:

  Iniciar nova tentativa

  Permite especificar o tempo (em minutos) para reiniciar a tarefa de replicação após a falha na tarefa. Por exemplo, se você especificar 10 minutos, a tarefa de replicação será reiniciada após 10 minutos da falha.

  Limite: 1 a 60

  Repetir

  Permite especificar o número de novas tentativas que você deseja executar se houver falha na tarefa de replicação. A tarefa de replicação é executada até que a tarefa seja executada com êxito ou até que o limite seja alcançado. Após o término do número de novas tentativas, a tarefa de replicação é executada somente na próxima hora programada.

  Limite: 1 a 99

9. Clique em **Concluir**.

   Observação: se desejar alterar as configurações das telas anteriores, clique em **Voltar** e altere a configuração conforme necessário.

   A caixa de diálogo Informações é exibida e mostra a mensagem *Tarefa de replicação ad hoc enviada com êxito!*.

10. Clique em **OK** para fechar a caixa de diálogo Informação.

    A replicação ad hoc é executada com êxito.

Monitorar o status da replicação ad hoc

Administrador de origem

Depois que a replicação ad hoc é bem-sucedida, é possível monitorar o status da tarefa de replicação ad hoc.

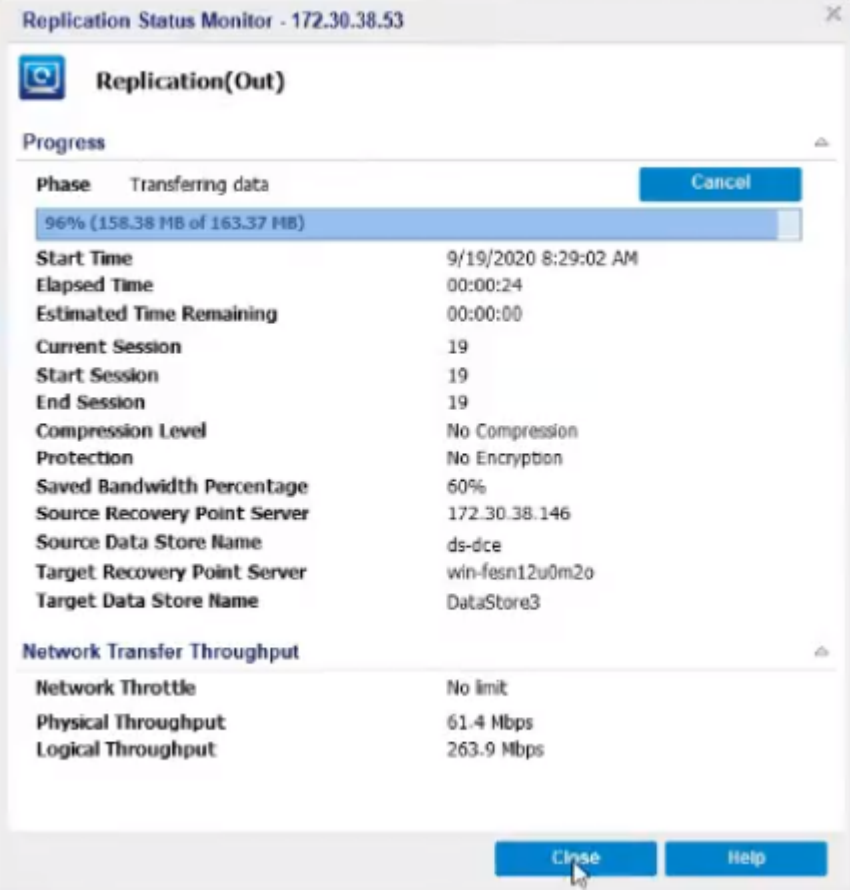
Siga estas etapas:

1. Navegue até **tarefas** > **Tarefas em andamento**.

   As tarefas de Replicação (Saída) e Replicação (Entrada) em andamento são exibidas no painel central.

2. Para monitorar o status de uma tarefa específica, clique em **Detalhes**, ao lado da barra de andamento correspondente a essa tarefa.

   A caixa de diálogo Monitor de status de replicação - xx.xx.xx.xx é exibida.



3. Aguarde até que a transferência de dados esteja 100% e, em seguida, clique em **Fechar**.

Você monitorou com êxito o status da replicação ad hoc.

Verificar se a replicação ad hoc foi bem-sucedida

Administrador de origem

Depois que os dados são replicados, é possível verificar se a replicação ad hoc foi bem-sucedida.

Siga estas etapas:

1. No console de origem, navegue até **tarefas** > **Tarefas concluídos com êxito**.

   Uma lista de tarefas concluídas é exibida no painel central.

2. Clique na tarefa de replicação inversa concluída. O painel direito é atualizado.
3. Em Detalhes da tarefa, clique no hiperlink **Exibir logs**.
4. Verifique se a replicação dos dados foi bem-sucedida.

Você verificou com êxito a replicação ad hoc.

Executar a replicação inversa do console remoto para o servidor RPS local

Esta seção explica como executar a replicação inversa do console remoto para o servidor de RPS local ou UDP local.

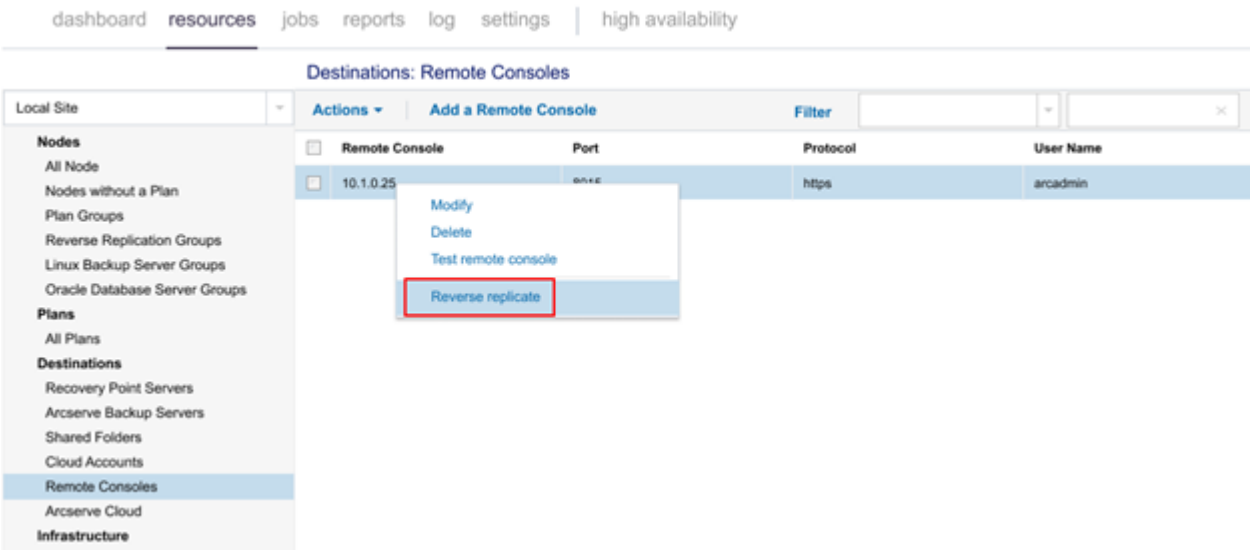
Observação: antes de executar a replicação inversa, certifique-se de que a replicação de encaminhamento seja executada com êxito. Para verificar se a replicação de encaminhamento foi bem-sucedida, consulte Verificar se os dados estão replicados.

Siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel esquerdo, navegue até **Destinos** > **Consoles remotos**.

   A lista de consoles remotos é exibida no painel central.

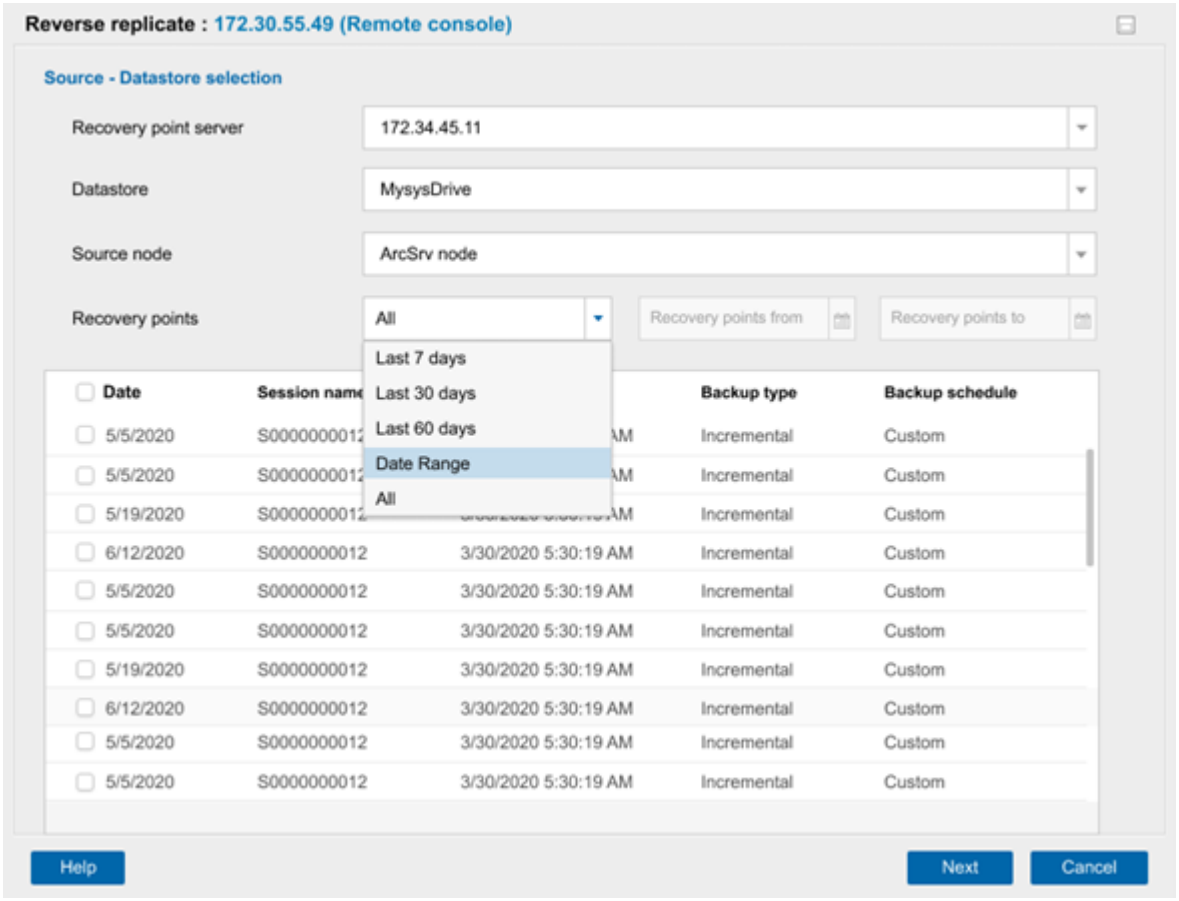
3. Clique com o botão direito do mouse no console remoto e selecione **Replicação inversa**.



Aguarde até se conectar ao console remoto.

A caixa de diálogo Replicação inversa: xxx.xx.xx.xxx (console remoto) é aberta.

4. Na página Origem - seleção do repositório de dados, faça o seguinte:



- Servidor de ponto de recuperação - selecione o servidor de ponto de recuperação de origem na lista suspensa.
- Repositório de dados - selecione o repositório de dados de origem na lista suspensa.
- Nó de origem - selecione o nó de origem na lista suspensa.
- Pontos de recuperação - execute um dos seguintes procedimentos:
  - Se desejar que todos os pontos de recuperação armazenados em backup sejam exibidos, selecione **Todos** na lista suspensa.
  - Se desejar que os pontos de recuperação sejam exibidos por uma duração específica, selecione um dos seguintes itens na lista suspensa:

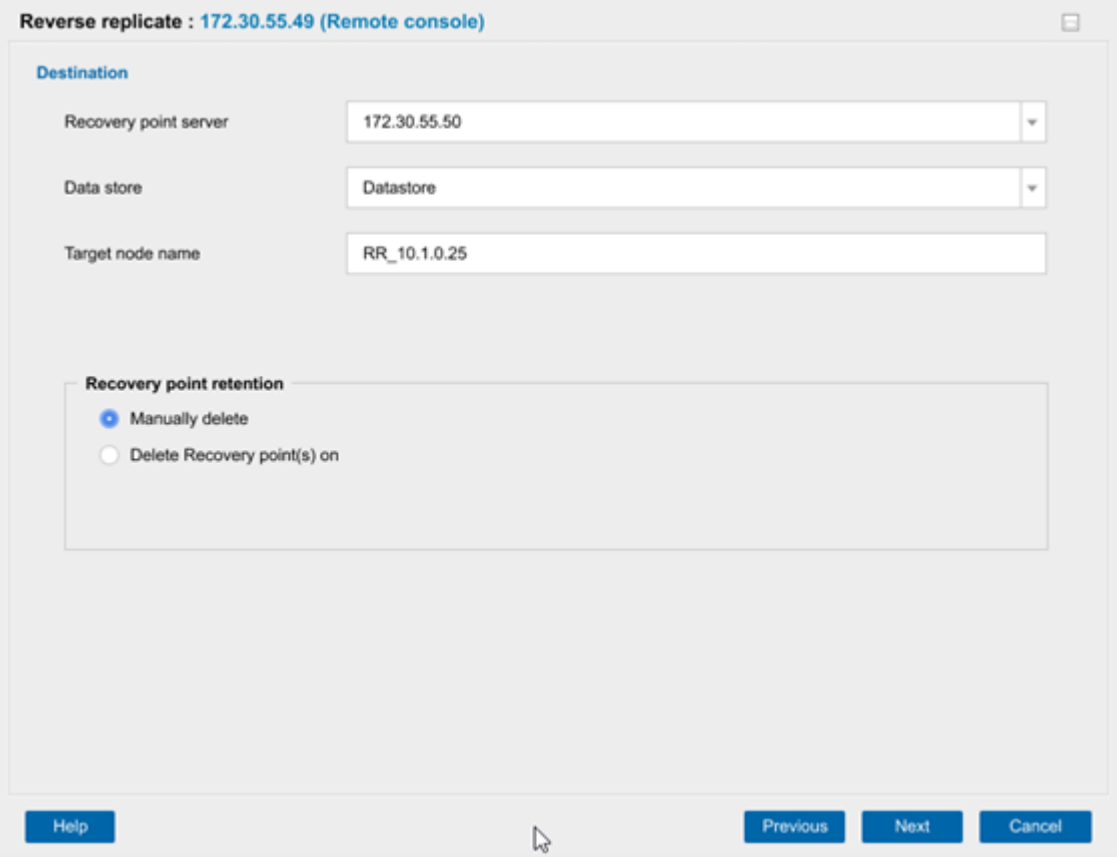
- Últimos 7 dias
- Últimos 30 dias
- Últimos 60 dias
- Intervalo de datas

Observação: se você selecionou **Intervalo de datas**, defina a data nos campos **Pontos de recuperação de** e **Ponto de recuperação até**.

Todos os pontos de recuperação associados entre a duração especificada serão exibidos.

- Na tabela, clique nas caixas de seleção para selecionar um ou mais pontos de recuperação.

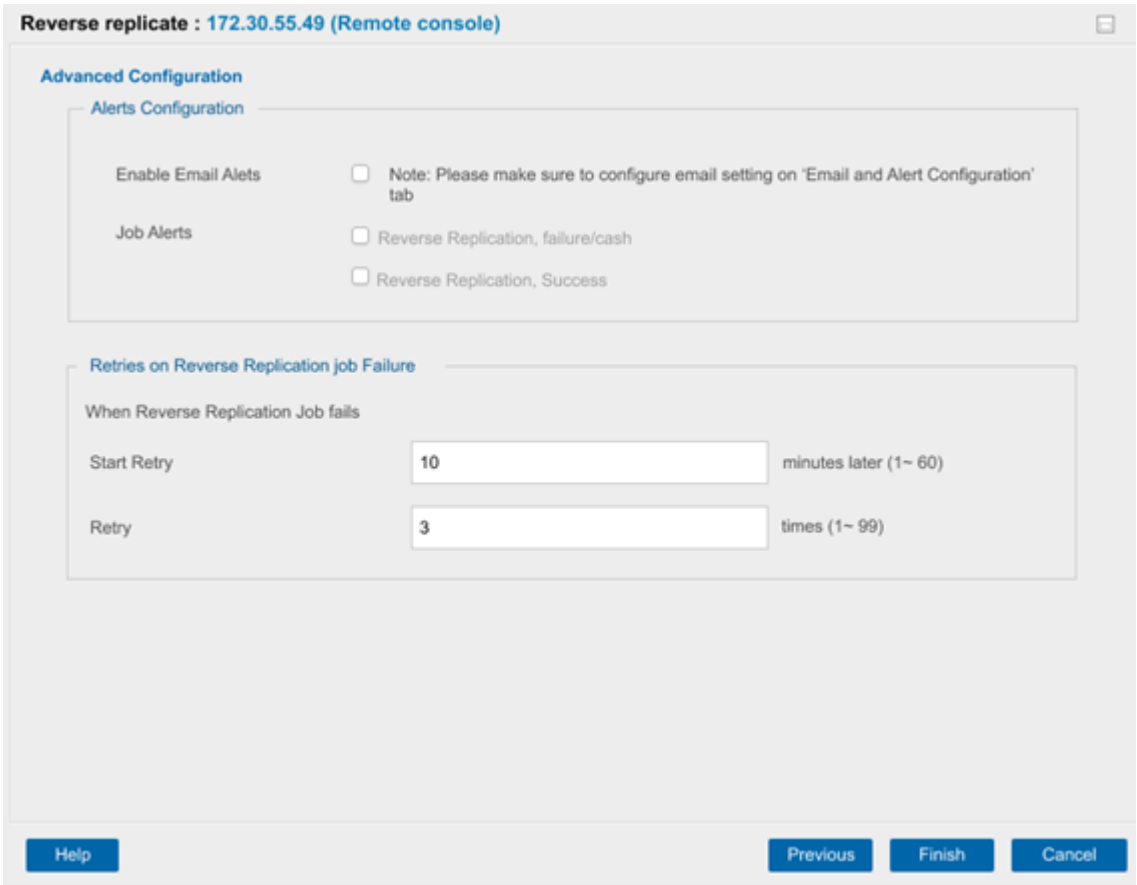
5. Clique em **Avançar**.
6. Na página Destino, faça o seguinte:



- Servidor de ponto de recuperação - selecione o servidor de ponto de recuperação de destino na lista suspensa.

- Repositório de dados - selecione o repositório de dados de destino na lista suspensa.
- Nome do nó de destino - digite um nome de nó de destino de sua escolha.
- Retenção do ponto de recuperação - exclua os pontos de recuperação de uma das seguintes maneiras:
  - Para excluir pontos de recuperação manualmente, selecione a opção **Excluir manualmente**.
  - Se desejar que os pontos de recuperação sejam excluídos automaticamente, selecione a opção **Excluir pontos de recuperação em** e, em seguida, especifique a data. Todos os pontos de recuperação correspondentes a essa data serão excluídos automaticamente.

7. Clique em **Avançar**.
8. Na página Configuração avançada, faça o seguinte:



- Para a configuração de alertas

  Ativar alertas por email

Permite ativar alertas por email. É possível especificar configurações de email e os tipos de alertas que você deseja receber por email. Ao marcar a caixa de seleção **Observação: certifique-se de definir a configuração de email na guia "Configuração de email e alerta".**, a seguinte opção é ativada para sua seleção:

Alertas de tarefa

Permite selecionar os tipos de emails de alerta de tarefas que você deseja receber.

- Se desejar receber alertas por email sobre falhas ou travamentos na replicação inversa, marque a caixa de seleção **Replicação inversa, falha ou travamento**.

  Observação: este alerta por email é enviado com uma importância alta. Os alertas pro email que apresentam uma configuração com nível de prioridade alta, exibem um indicador visual de um ponto de exclamação em sua caixa de entrada.

- Se desejar receber alertas por email sobre o êxito da replicação inversa, marque a caixa de seleção **Replicação inversa, êxito**.

- Para novas tentativas em relação à falha na tarefa de replicação inversa

  Quando a tarefa de replicação inversa falhar, faça o seguinte:

  Iniciar nova tentativa

  Permite especificar o tempo (em minutos) para reiniciar a tarefa de replicação após a falha na tarefa. Por exemplo, se você especificar 10 minutos, a tarefa de replicação será reiniciada após 10 minutos da falha.

  Limite: 1 a 60

  Repetir

  Permite especificar o número de novas tentativas que você deseja executar se houver falha na tarefa de replicação. A tarefa de replicação é executada até que a tarefa seja executada com êxito ou até que o limite seja alcançado. Após o término do número de novas tentativas, a tarefa de replicação é executada somente na próxima hora programada.

  Limite: 1 a 99

9. Clique em **Concluir**.

Observação: se desejar alterar as configurações das telas anteriores, clique em **Voltar** e altere a configuração conforme necessário.

A caixa de diálogo Informações é exibida, exibindo a mensagem *Tarefa de replicação inversa enviada com êxito!*.

10. Clique em **OK** para fechar a caixa de diálogo Informação.

    A replicação inversa foi concluída com êxito no console remoto para o servidor local ou UDP local.

Monitorar o status da replicação inversa

Administrador de origem

Após o êxito da replicação inversa, é possível monitorar o status da tarefa de replicação inversa.

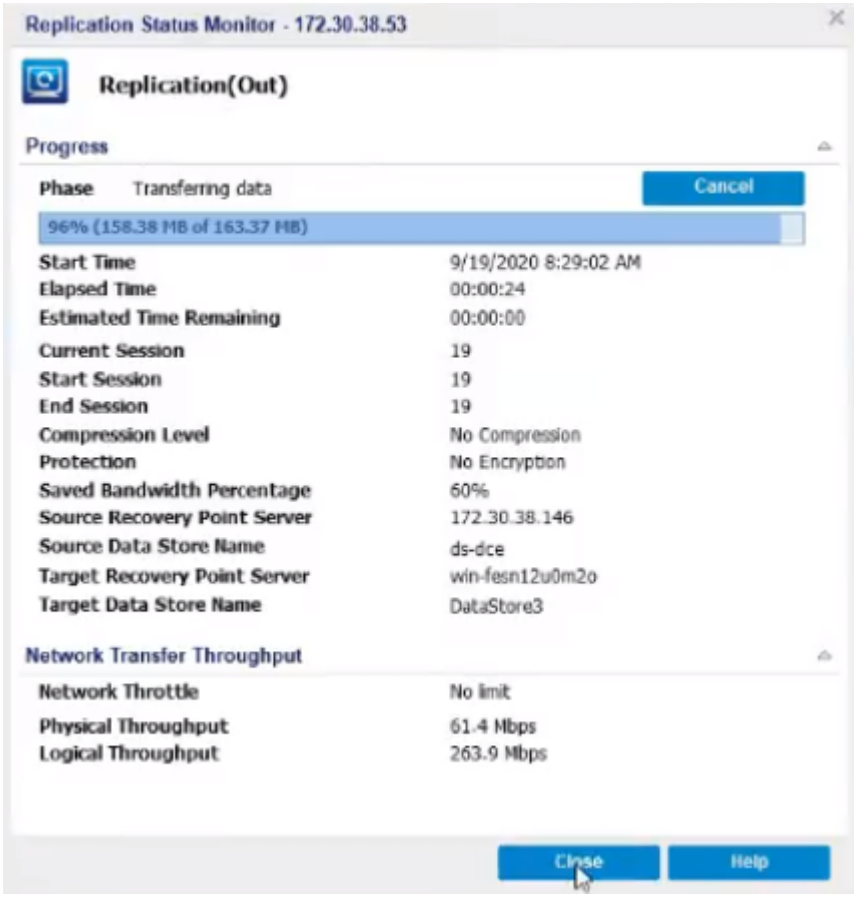
Siga estas etapas:

1. Navegue até **tarefas** > **Tarefas em andamento**.

   As tarefas de Replicação (Saída) e Replicação (Entrada) em andamento são exibidas no painel central.

2. Para monitorar o status de uma tarefa específica, clique em **Detalhes**, ao lado da barra de andamento correspondente a essa tarefa.

   A caixa de diálogo Monitor de status de replicação - xx.xx.xx.xx é exibida.



3. Aguarde até que a transferência de dados esteja 100% e, em seguida, clique em **Fechar**.

Você monitorou o status da replicação inversa com êxito.

Verificar se a replicação inversa foi bem-sucedida

Administrador de origem

Depois que os dados são replicados, é possível verificar se a replicação inversa foi bem-sucedida.

Siga estas etapas:

1. No console de origem, navegue até **tarefas** > **Tarefas concluídos com êxito**.

   Uma lista de tarefas concluídas é exibida no painel central.

2. Clique na tarefa de replicação inversa concluída. O painel direito é atualizado.
3. Em Detalhes da tarefa, clique no hiperlink **Exibir logs**.
4. Verifique se a replicação dos dados foi bem-sucedida.

Você verificou com êxito a replicação inversa de dados do console remoto para o servidor de RPS local ou UDP local.

Como criar um plano de pontos de recuperação de cópia

Com o uso do Arcserve Unified Data Protection, é possível copiar os pontos de recuperação na nuvem ou em uma pasta compartilhada ou um volume local para proteger os pontos de recuperação. Esse processo ajuda a garantir que você tenha uma cópia adicional dos pontos de recuperação, caso seus pontos de recuperação originais sejam excluídos acidentalmente. A tarefa de cópia dos pontos de recuperação copia os pontos de recuperação do destino de backup na nuvem ou em uma pasta compartilhada ou apenas em um volume local. Não é possível copiar o ponto de recuperação para um servidor de ponto de recuperação.

Você pode adicionar somente uma tarefa de cópia de pontos de recuperação a um plano.

Observações:

- Na versão atual, as tarefas de Copiar ponto de recuperação não serão suportadas se o **Backup: Linux com base em agente** for criado como Task1.
- As tarefas de Copiar ponto de recuperação são sempre executadas no agente, mesmo se o backup estiver configurado no RPS.

  Para backup de VM sem agente, o proxy do agente UDP usado na Task1 processará a tarefa de Copiar para o ponto de recuperação.

Solução de problemas: congestionamento de largura de banda com tarefas de cópia do ponto de recuperação para a nuvem

O que fazer a seguir?

- Verificar os pré-requisitos e as considerações
- Criar um plano com uma tarefa de backup
- Adicionar uma tarefa de Copiar pontos de recuperação ao plano
- Verificar o plano

Verificar os pré-requisitos e as considerações

Verifique se concluiu os seguintes pré-requisitos:

- Efetue logon no Console.
- Instale o componente do servidor e crie repositórios de dados, caso deseje armazenar os dados de backup no servidor do ponto de recuperação.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Criar um plano com uma tarefa de backup

Um plano inclui tipos diferentes de tarefas que você deseja executar. Para criar uma tarefa de cópia de pontos de recuperação, é necessário, primeiramente, ter um ponto de recuperação válido. Para obter um ponto de recuperação válido, crie uma tarefa de backup.

Uma tarefa de backup executa um backup dos nós de origem e armazena os dados para o destino especificado. A cópia dos pontos de recuperação é suportada para Windows com base em agente e no backup sem agente com base em host. O procedimento a seguir explica as etapas para criar a tarefa de backup do Windows com base em agente. Não é possível copiar o ponto de recuperação para planos de backup com base no agente do Linux.

Observação: para obter mais informações sobre o backup sem agente com base em host, consulte Como criar um plano de backup da máquina virtual com base em host.

Para obter mais informações sobre o backup do caminho UNC, consulte Como criar um plano de backup de caminho UNC.

Para obter mais informações sobre o backup do Exchange Online, consulte Como criar um plano de backup do Exchange Online.

Siga estas etapas:

1. Clique na guia **Recursos** no Console.
2. No painel à esquerda, navegue para **Planos** e clique em **Todos os planos**.

   Se tiver criado os planos anteriores, esses planos serão exibidos no painel central
3. No painel central, clique em **Adicionar um plano**.

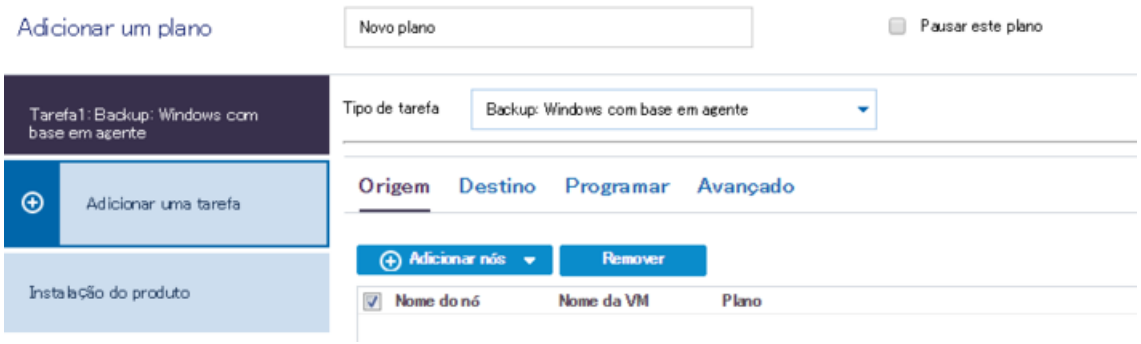
   Adicionar um plano é exibido.
4. Digite o nome do plano.
5. (Opcional) Selecione a caixa de seleção **Pausar este plano** para fazer uma pausa no plano.

   O plano não será executado até que você desmarque a caixa de seleção para retomar o plano.

   Observação: se um plano for pausado, nenhuma tarefa em andamento será pausada, mas todas as tarefas programadas correspondentes associadas a esse plano serão pausadas. No entanto, você pode executar uma tarefa manualmente. Por exemplo, você pode executar manualmente a tarefa de backup e a tarefa de replicação para um nó mesmo que o respectivo plano esteja pausado. Nesse caso, a

tarefa seguinte da tarefa sob demanda (manual) não será executada. Por exemplo, há uma tarefa de replicação após uma tarefa de backup sob demanda, a tarefa de replicação não será executada para a tarefa de backup sob demanda. É necessário executar manualmente a tarefa de replicação. Quando você retomar o plano, as tarefas pendentes não são retomadas imediatamente. Depois de retomar o plano, as tarefas pendentes serão executadas no próximo horário programado.

6. Na lista suspensa **Tipo de tarefa**, selecione **Backup, Windows com base em agente**.



Agora, especifique os detalhes de Origem, Destino, Programação e Avançado.

Especificar a origem

A página Origem permite especificar os nós de origem que deseja proteger. É possível selecionar mais de um nó em um plano. Caso não tenha adicionado nós para o console, você pode adicionar nós ao criar ou modificar um plano da página de origem. Também é possível salvar um plano sem adicionar nenhum nó de origem. O plano é implantado somente após você adicionar nós de origem.

Siga estas etapas:

1. Na guia Origem, clique em **Adicionar**.
2. Selecione uma das seguintes opções:

   Selecionar os nós a serem protegidos no Arcserve UDP

   Abre a caixa de diálogo Selecionar nós para proteger no Arcserve UDP. Selecione os nós na lista exibida. Selecione esta opção se você já tiver adicionado os nós para o console.

   Adicionar nó do Windows

   A caixa de diálogo Adicionar nós a um plano é exibida. Selecione esta opção se você não tiver adicionado os nós e desejar adicionar manualmente os nós para proteger.

   Detectar os nós do Active Directory

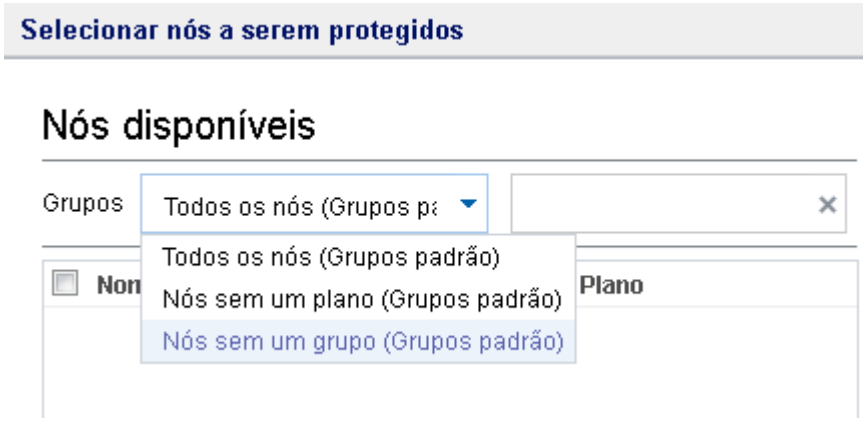
   Abra a caixa de diálogo Adicionar nós ao Console do Arcserve UDP. Selecione essa opção se desejar detectar e adicionar nós do Active Directory.
3. Se você selecionou a opção **Selecionar nós para proteger no Arcserve UDP**, na caixa de diálogo Selecionar nós para proteger, faça o seguinte:
   a. (Opcional) Selecione um filtro na lista suspensa Grupos para filtrar os nós. É possível digitar as palavras-chave para filtrar melhor seus nós.

      Os nós são exibidos na coluna Nós disponíveis.

   b. Selecione os nós na coluna Nós disponíveis e, em seguida, clique na seta simples à direita (>) ou na seta dupla à direita (>>) para mover os nós selecionados ou todos os nós, respectivamente, para a coluna Nós selecionados.

      Os nós são exibidos na coluna Nós selecionados.

   c. Clique em **OK** para fechar a caixa de diálogo.



4. Para escolher Tipo de proteção, selecione uma das seguintes opções:

   Fazer backup de todos os volumes

   Prepara um backup instantâneo de todos os volumes.

   Fazer backup dos volumes selecionados

   Prepara um instantâneo de backup do volume selecionado.

   A origem é especificada.

Especificar o destino

O destino é o local onde você armazena os dados de backup. É necessário, no mínimo, especificar o destino para salvar o plano.

Siga estas etapas:

1. Selecione um dos seguintes **Tipos de destino**:

   Disco local ou uma pasta compartilhada

   Especifica que o destino de backup é um destino local ou uma pasta compartilhada. Se selecionar essa opção, será possível salvar os dados como pontos de recuperação ou conjuntos de recuperação. As opções de pontos de recuperação e de conjuntos de recuperação estão disponíveis na guia **Programar**.

   Servidor de ponto de recuperação do Arcserve UDP

   Especifica que o destino de backup é um servidor de ponto de recuperação. Se selecionar essa opção, os dados serão armazenados como pontos de recuperação. Não é possível armazenar dados como conjuntos de dados de recuperação.

2. Se tiver selecionado **Servidor de ponto de recuperação do Arcserve UDP**, forneça os seguintes detalhes:
   a. Selecione um servidor de ponto de recuperação
   b. Selecione um repositório de dados. A lista exibe todos os repositórios de dados que são criados no servidor de ponto de recuperação especificado.
   c. Forneça uma senha da sessão.
   d. Confirme a senha da sessão.
3. Se tiver selecionado **Disco local ou pasta compartilhada**, forneça os seguintes detalhes:
   a. Forneça o caminho completo do destino local ou de rede. Para o destino de rede, especifique as credenciais com o acesso de gravação.
   b. Selecione o algoritmo de criptografia. Para obter mais informações, consulte Configurações de criptografia.
   c. Como opção, forneça uma senha de criptografia.
   d. Confirme a senha de criptografia.
   e. Selecione um tipo de compactação. para obter mais informações, consulte Tipo de compactação.

Observações:

- CRP (Copy Recovery Point - Copiar ponto de recuperação) não oferece suporte a backups personalizados, mesmo quando a programação de CRP é adicionada. Além disso, a tarefa CRP não oferece suporte à programação de backup personalizada.
- A tarefa CRP para a nuvem oferece suporte somente a partir de um console. Ela não oferece suporte a um agente autônomo.
- *Pastas de compartilhamento/disco local* e *backups armazenados no RPS* oferecem suporte às tarefas CRP.

O destino é especificado.

Especificar a programação

A página Programar permite definir uma programação de backup. A opção Copiar pontos de recuperação oferece suporte a backups diários, semanais e mensais do console. Após definir uma programação, as tarefas são executadas automaticamente de acordo com a programação. É possível adicionar programações diárias, semanais e mensais, bem como fornecer configurações de retenção.

Observação: para obter mais informações sobre as configurações de retenção e programação, consulte Entendendo a programação avançada e retenção.

Siga estas etapas:

1. (Opcional) Selecione a opção para gerenciar os pontos de recuperação. Essa opção será visível somente se tiver selecionado o local ou a pasta compartilhada como o destino do backup.

   Reter por pontos de recuperação

   Os dados de backup são armazenadas como pontos de recuperação.

   Reter por conjuntos de recuperação

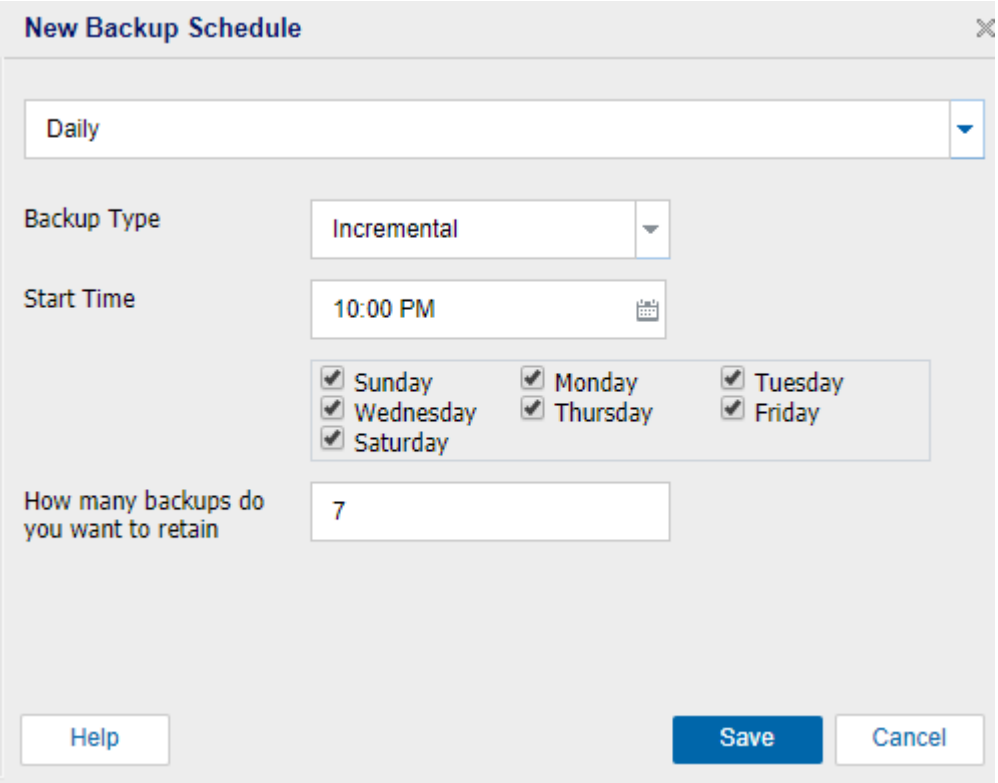
   Os dados de backup são armazenadas como conjuntos de recuperação.

   Observação: a opção Reter por conjuntos de recuperação não tem suporte para Copiar pontos de recuperação.

2. Adicionar uma programação de backup.

   a. Clique em **Adicionar** e selecione **Adicionar programação de backups**.

      A caixa de diálogo **Nova programação de backup** é aberta.



b. Selecione uma das seguintes opções:

Diário

Especifica a programação de backup que ocorre uma vez por dia. Por padrão, todos os dias da semana estão selecionados para o backup diário. Se não desejar executar a tarefa de backup em um dia específico, desmarque a caixa de seleção correspondente àquele dia da semana.

Semanal

Especifica a programação de backup que ocorre uma vez por semana.

Mensal

Especifica a programação de backup que ocorre uma vez por mês.

c. Selecione o tipo de backup.

Completo

Especifica a programação de backups para backups completos. Conforme programado, o Arcserve UDP executa um backup completo de todos os blocos usados do computador de origem. Um backup completo em geral, consome tempo, dependendo do tamanho do backup.

Incremental

Especifica a programação de backups para backups incrementais.

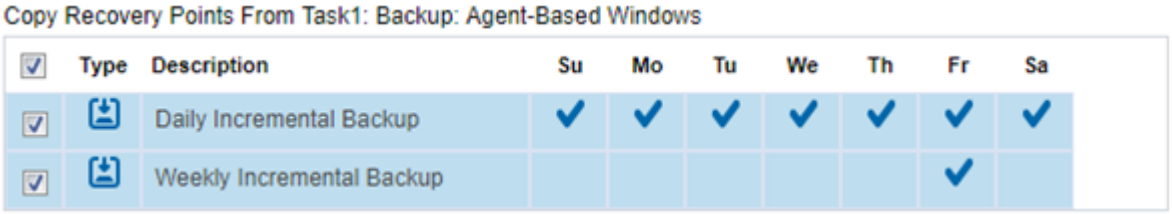
Conforme programado, o Arcserve UDP faz backup incremental apenas dos blocos que foram alterados desde o último backup realizado com êxito. As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a executar um backup.

d. Especifique a hora de início do backup.

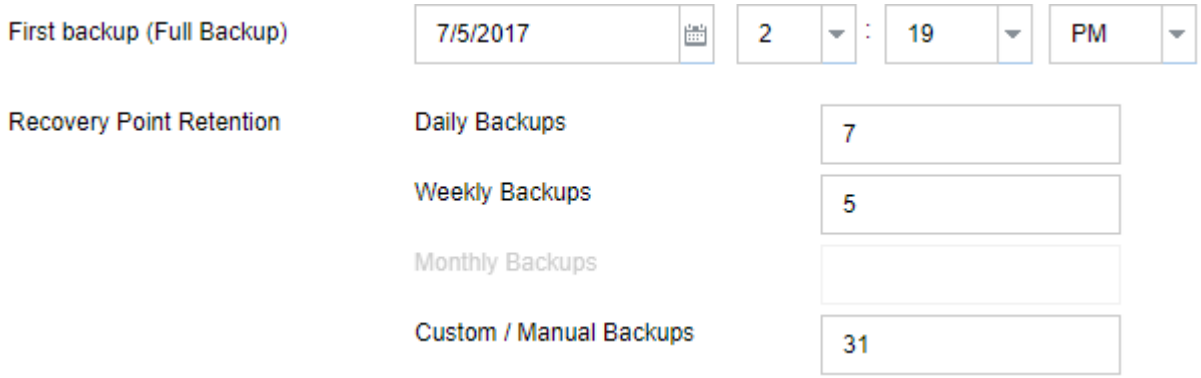
e. (Opcional) Marque a caixa de seleção de **Repetição** e especifique a programação a ser repetida.

f. Clique em **Salvar**.

A programação de backup é especificada e exibida na página de **Programação**.



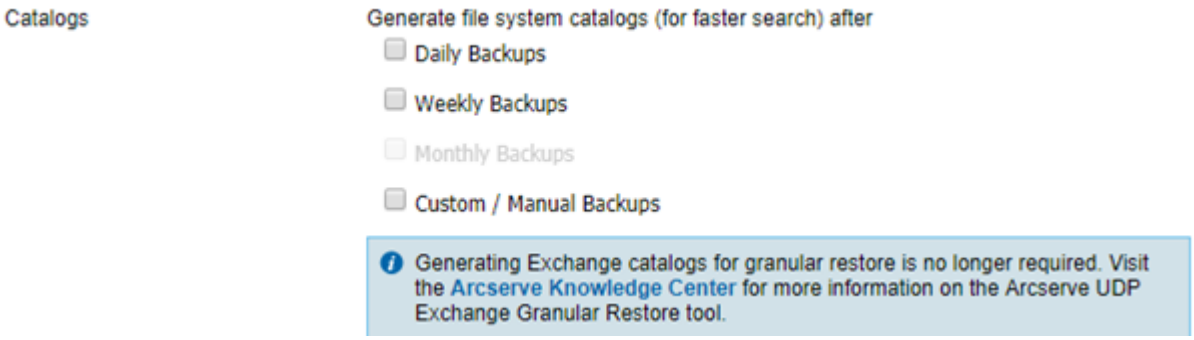
3. Especifique a hora de início do backup programado.



4. Especifique as configurações de retenção de pontos de recuperação para programação diária, semanal e mensal.

Essas opções serão ativadas se tiver adicionado a programação de backup correspondente. Se você modificar as configurações de retenção desta página, as alterações serão refletidas na caixa de diálogo Programação de backup.

5. Especifique os detalhes de catálogo.



Os catálogos permitem gerar o catálogo do sistema de arquivos. O catálogo do sistema de arquivos é necessário para agilizar e melhorar a pesquisa. Se marcar as caixas de seleção do catálogo, os catálogos serão ativados de acordo com o tipo de backup que você especificou. Desmarque a caixa de seleção para desativar a geração do catálogo.

A programação é especificada.

Noções básicas sobre a programação avançada e retenção

A opção de programação permite especificar uma programação personalizada, uma programação diária/semanal/mensal ou ambas. Na programação personalizada, é possível configurar a programação de backups para cada dia da semana ou adicionar até quatro programações de backup em cada dia. É possível escolher um dia específico da semana e criar uma janela para definir quando executar o backup e em que frequência.

Programação	Tarefa com suporte	Comentários
Backup	Tarefa de backup	Definir janelas de tempo para a execução de tarefas de backup.
Limitação de backup	Tarefa de backup	Definir janelas de tempo para controlar a velocidade de backup.
Mesclar	Tarefa de mesclagem	Definir quando executar tarefas de mesclagem.
Programação diária	Tarefa de backup	Definir quando executar tarefas do backup diário.
Programação semanal	Tarefa de backup	Definir quando executar tarefas do backup semanal.
Programação mensal	Tarefa de backup	Definir quando executar tarefas do backup mensal.

Também é possível especificar as configurações de retenção para os pontos de recuperação.

Observação: as configurações de retenção devem ser definidas em cada plano para controlar como os dados dos nós atribuídos a esse plano são retidos no repositório de dados de destino.

As programações para backups diários/semanais/mensais são independentes para a programação personalizada e umas das outras. É possível configurar para executar somente o backup diário, semanal ou mensal, sem configurar a Programação personalizada.

Programação de tarefas de backup

É possível adicionar quatro janelas de tempo por dia na programação do backup. Uma janela de tempo é válida das 00:00 às 23:59. Não é possível especificar uma janela de tempo das 18:00 às 6:00. Nesses casos, você deve especificar manualmente duas janelas de tempo diferentes.

Para cada janela de tempo, a hora de início é inclusiva e a hora de término é exclusiva. Por exemplo, você configurou para executar o backup incremental em intervalos de uma hora entre as 6:00 e as 9:00. O backup será iniciado às 6:00. Isso significa que o backup será executado às 6h00, 7h00 e 8h00, mas NÃO às 9h00.

Observação: se você deseja executar a tarefa de backup várias vezes até o fim do dia, defina a programação para até 0h00. Por exemplo, para executar a tarefa de backup a cada 15 minutos o dia inteiro, defina a programação como das 0h00 às 00h00, a cada 15 minutos.

Programação do acelerador de backup

A programação de aceleração do backup permite controlar a velocidade da taxa de transferência de backup o que, por sua vez, controla o uso de recursos (E/S de disco, CPU, largura de banda de rede) do servidor cujo backup está sendo feito. Isso é útil quando se não quiser afetar o desempenho do servidor durante o horário comercial. É possível adicionar quatro janelas de tempo por dia na sua programação de aceleração do backup. Para cada janela de tempo, é possível especificar um valor, em MB por minuto. Esse valor será usado para controlar a taxa de transferência do backup. Os valores válidos variam entre 1 MB/minutos a 99999 MB/minutos.

Se uma tarefa de backup estende seu tempo especificado, o limite de aceleração será ajustado de acordo com o tempo especificado. Por exemplo, você definiu o limite de aceleração de backup como 500 MB/minuto das 8:00 às 20:00 e 2500 MB/minuto das 20:00 às 22:00. Se uma tarefa de backup iniciar às 19h00 e for executada durante três horas, das 19h00 às 20h00 o limite de aceleração será de 500 MB/minuto e das 20h00 às 22h00, o limite de aceleração será 2500 MB/minuto.

Se não definir nenhuma programação do backup e programação da taxa de transferência do backup, o backup será executado o mais rápido possível.

Mesclar a programação

Permite mesclar pontos de recuperação com base na programação fornecida.

Considere os seguintes pontos para a tarefa de mesclagem:

- A qualquer momento apenas uma tarefa de mesclagem pode ser executada para um nó.
- Se uma tarefa de mesclagem iniciar, ela precisará ser concluída antes que a próxima tarefa de mesclagem seja iniciada. Isso significa que, se um ou mais conjuntos de pontos de recuperação forem mesclados, não será possível adicionar o

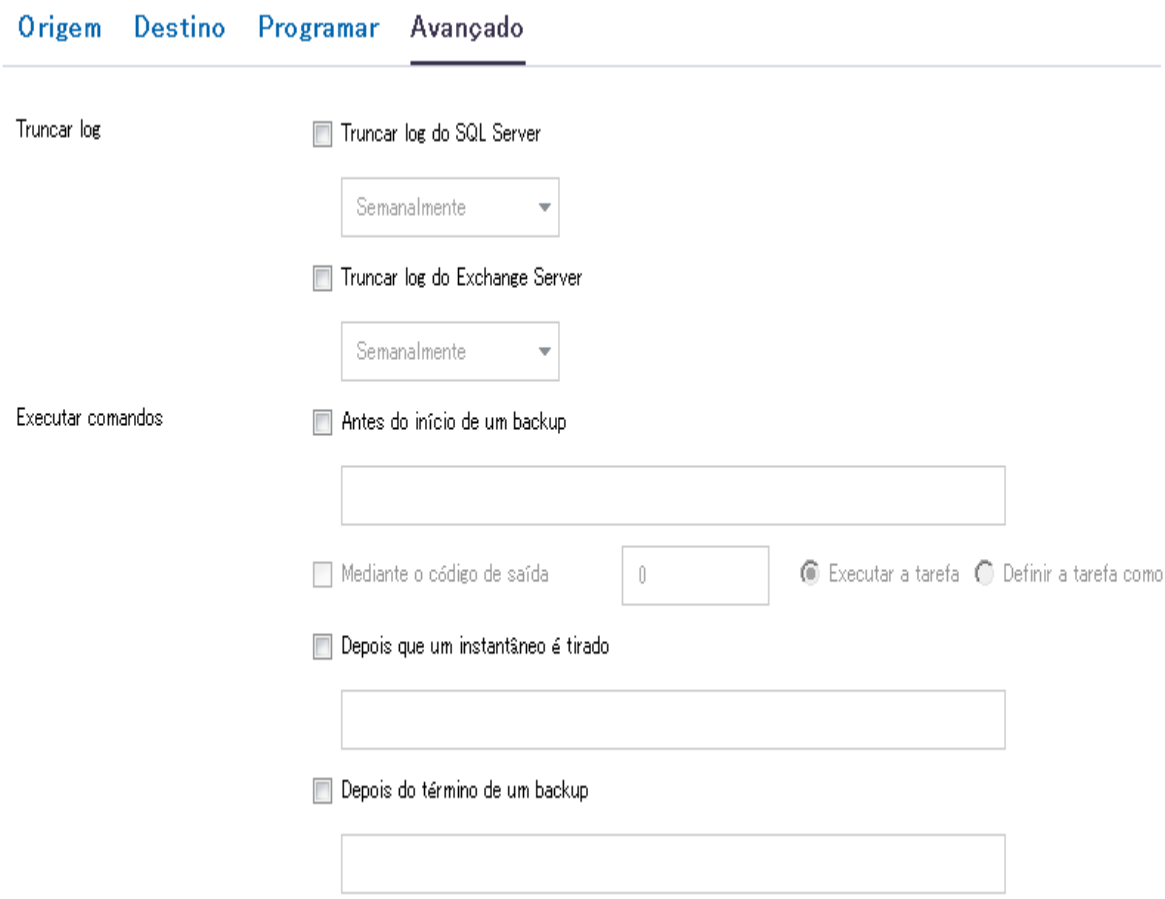
novo ponto de recuperação a este processo de mesclagem, até que o processo de mesclagem do conjunto atual de ponto de recuperação seja concluído.

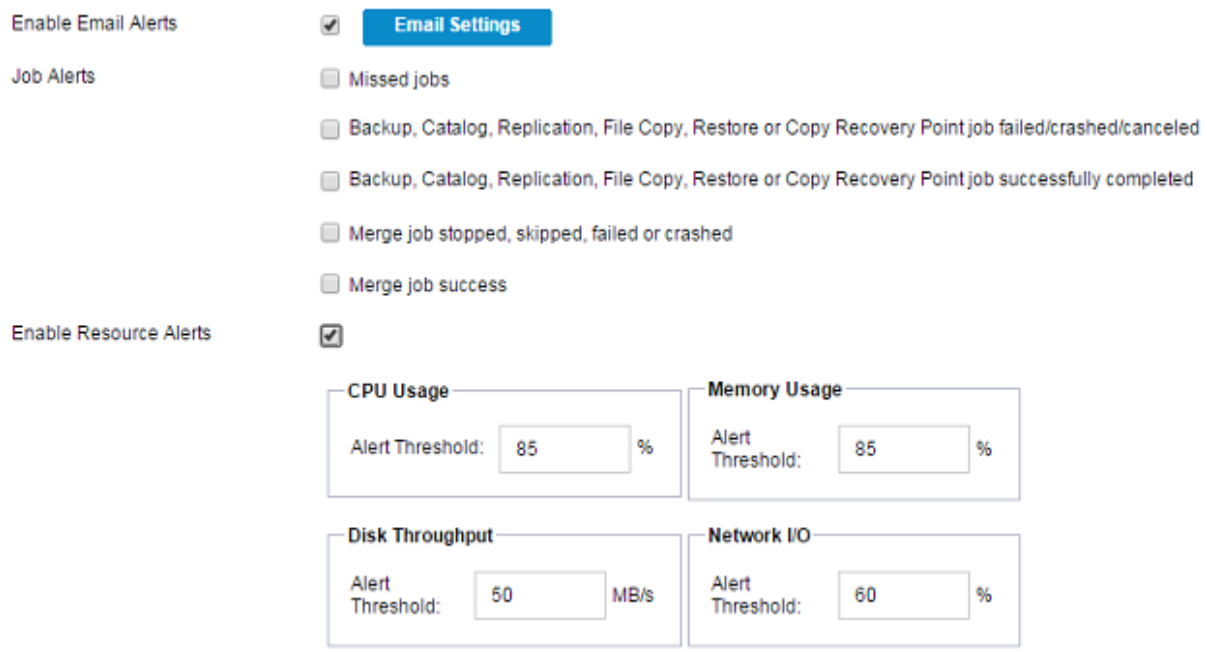
- Se uma tarefa de mesclagem estiver processando mais de um conjunto de pontos de recuperação (por exemplo, conjunto [1~4], conjunto [5~11] e conjunto [12~14]; são três conjuntos) o servidor de ponto de recuperação processará esses conjuntos, um por um.
- Se uma tarefa de mesclagem é retomada após um intervalo, a tarefa detectará em que ponto ela foi pausada e continuará a mesclagem a partir do ponto de pausa.

Especificar as configurações avançadas

A guia **Avançado** permite especificar algumas configurações avançadas para a tarefa de backup. As configurações avançadas incluem fornecer configurações de log de truncamento, a localização de quaisquer scripts e as configurações de email.

A imagem a seguir mostra a guia Avançado:





Siga estas etapas:

1. Especifique os seguintes detalhes.

Truncar log

Permite especificar a programação para truncar logs para o SQL Server e o Exchange Server. É possível especificar a programação como **Diária**, **Semanal** ou **Mensal**.

Nome de usuário

Permite especificar o usuário que possui autorização para executar um script.

Senha

Permite especificar a senha do usuário que está autorizado a executar o script.

Executar um comando antes do início do backup

Permite a execução de um script antes de iniciar a tarefa de backup. Especifique o caminho onde o script está armazenado. Clique em **No código de saída** e especifique o código de saída para **Executar tarefa** ou **Tarefa com falha**. **Executar a tarefa** indica que a tarefa de backup continuará quando o script retornar o código de saída. **Tarefa com falha** indica que a tarefa de backup será interrompida quando o script retornar o código de saída.

Executar um comando após a criação de um instantâneo

Permite executar um script depois que o backup do instantâneo for gerado. Especifique o caminho onde o script está armazenado.

Executar um comando após a conclusão do backup

Permite executar um script depois que a tarefa de backup foi concluída. Especifique o caminho onde o script está armazenado.

Ativar alertas por email

Permite ativar alertas por email. É possível especificar configurações de email e os tipos de alertas que você deseja receber por email. Ao selecionar esta opção, as seguintes opções serão ativadas para a seleção.

Configurações de email

Permite configurar as definições de email. Clique em **Configurações de email** e configure o servidor de email e os detalhes do servidor proxy.

Alertas de tarefa

Permite que você selecione os tipos de emails da tarefa que deseja receber.

Ativar os alertas de recurso

Permite que você especifique um limite de uso da CPU, o uso da memória, a taxa de transferência de disco, E/S de rede. Você pode fornecer o valor em porcentagem. Você receberá um email quando o valor exceder o Limite de alerta.

2. Clique em **Salvar**.

Observação: quando você seleciona um nó como origem de backup ou proxy de backup, o Arcserve UDP verifica se o agente está instalado no nó e se é a versão mais recente. Em seguida, o Arcserve UDP exibe uma caixa de diálogo de verificação que lista todos os nós que possuem uma versão antiga do agente ou que não tem o agente instalado. Para instalar/atualizar o agente nesses nós, selecione o método de instalação e clique em Salvar.

As alterações são salvas e uma marca de seleção verde é exibida ao lado do nome da tarefa. A página do plano é fechada.

Observação: se precisar adicionar outra tarefa, deverá selecionar o plano na guia **Recursos** e modificar o plano. Para modificar o plano, clique no plano do painel central. O plano é exibido e será possível modificá-lo.

O plano de backup é criado e implantado automaticamente para o nó de origem. O backup é executado de acordo com a programação que você configurou na guia **Programar.** Também é possível fazer backup manual quando desejado.

Adicionar uma tarefa de Copiar pontos de recuperação ao plano

A tarefa de cópia de recuperação copia os pontos de recuperação do destino de backup na nuvem ou em uma pasta compartilhada ou um volume local.

Observação: se uma tarefa de backup estiver em andamento e você fizer uma pausa no plano, a tarefa de backup irá obter o controle e a tarefa de cópia de pontos de recuperação não será iniciada. Ao retomar o plano novamente, a tarefa de cópia de pontos de recuperação não é retomada automaticamente. É necessário executar manualmente outra tarefa de backup para iniciar a tarefa de cópia de pontos de recuperação.

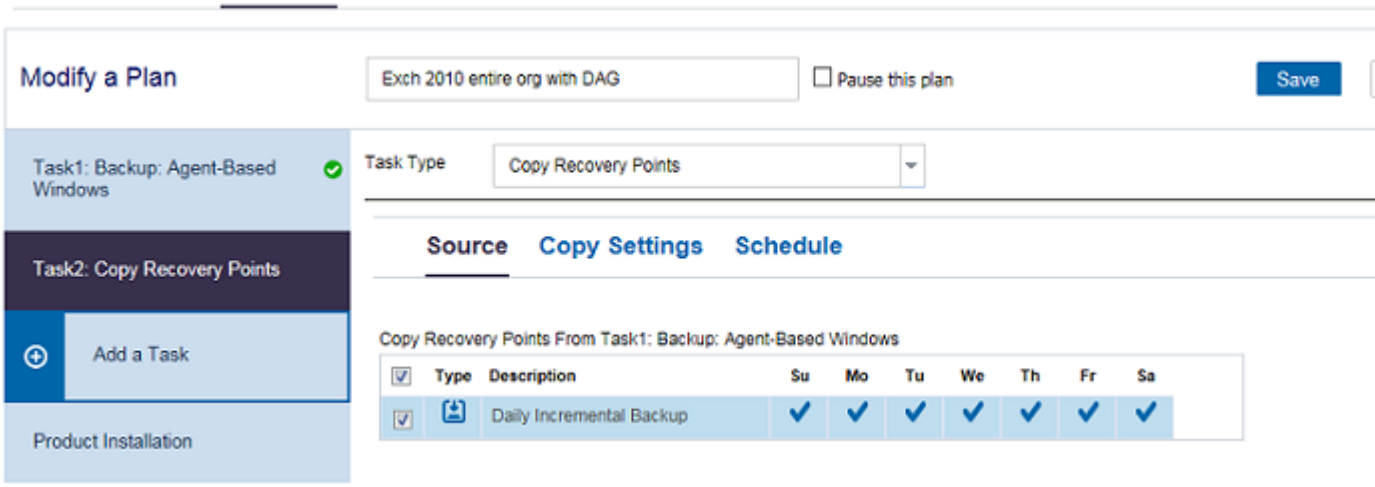
Siga estas etapas:

1. No painel esquerdo, clique em **Adicionar uma tarefa**.

   Uma nova tarefa será adicionada ao painel esquerdo.

2. Na lista suspensa **Tipo de tarefa**, selecione **Copiar pontos de recuperação**.

   A tarefa Copiar pontos de recuperação é adicionada. Não é necessário configurar a guia **Origem** na tarefa CRP (Copy Recovery Points - Copiar pontos de recuperação). Além disso, você pode exibir o destino do backup na tarefa de backup.



Observação: você pode configurar o caminho de Copiar ponto de recuperação para um local personalizado usando a chave de registro abaixo.

Caminho: *HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFCopySession*

Nome da chave: *LocalTempPath*

Tipo de chave: *REG_SZ (cadeia de caracteres)*

Valor da chave: *"Local_disk_path"*

3. Na guia Origem, selecione uma programação.
4. Na guia Configurações de cópia, forneça os seguintes detalhes:

Tipo de destino

Especifica o tipo de destino. É possível selecionar uma das opções de armazenamento na nuvem ou um disco local ou uma pasta compartilhada. Não é possível optar por Servidor de ponto de recuperação como o tipo de destino.

Disco local ou uma pasta compartilhada

É necessário inserir os detalhes de destino.

Destino

Especifica o destino no qual deseja manter a cópia de pontos de recuperação.

Observação: clique na seta para validar o destino especificado. Seta fica visível ao fornecer o destino.

Armazenamento na nuvem

É preciso selecionar o serviço de nuvem e adicionar um armazenamento na nuvem.

Para obter informações detalhadas sobre a estrutura de diretórios, consulte o tópico Estrutura de diretórios de pontos de recuperação no compartimento de memória na nuvem S3.

Serviço de nuvem

Permite selecionar uma das opções dentre os vários serviços de armazenamento disponíveis.

Armazenamento na nuvem

Permite selecionar a conta de nuvem do serviço de armazenamento selecionado. Se a lista suspensa não exibir nenhuma conta, clique em **Adicionar** para adicionar uma conta.

Ativar bloqueio de objeto

Permite proteger o armazenamento na nuvem usando o recurso de bloqueio de objeto. Quando você seleciona o seguinte como serviço de nuvem, a caixa de seleção Ativar bloqueio de objeto é exibida.

- Amazon S3
- Wasabi Hot Cloud Storage
- Nutanix Objects

  Quando você marca a caixa de seleção **Ativar bloqueio de objeto**, o botão Configurações de bloqueio de objeto é ativado. Você deve definir as configurações de bloqueio de objeto após ativar a caixa de seleção Bloqueio de objeto. Para obter mais informações sobre como definir as configurações de bloqueio de objeto, consulte Definir configurações de bloqueio de objeto para um serviço de nuvem.

Observações:

- Para Amazon S3 e Wasabi Hot Cloud Storage:
  - Você pode ativar a opção de bloqueio de objeto somente para novos compartimentos de memória.
  - Ao modificar um plano, considere o seguinte:
    - Se um plano for criado com o bloqueio de objeto ativado, a caixa de seleção *Ativar bloqueio de objeto* será desativada e o botão *Configurações de bloqueio de objeto* será ativado. Você pode modificar o modo de retenção e o período de retenção usando o botão *Configurações de bloqueio de objeto*.
    - Se um plano for criado com o bloqueio de objeto desativado, a caixa de seleção *Ativar bloqueio de objeto* e o botão *Configurações de bloqueio de objeto* serão desativados.
- Para objetos do Nutanix:
  - É possível ativar a opção de bloqueio de objeto para compartimentos de memória antigos e novos.
  - Ao modificar um plano, considere o seguinte:
    - Se um plano for criado com o bloqueio de objeto ativado, não será possível desativar a caixa de seleção *Ativar bloqueio de objeto*. Você só pode aumentar o período de retenção usando o botão *Configurações de bloqueio de objeto*.

- Se um plano for criado com o bloqueio de objeto desativado, será possível ativar a caixa de seleção *Ativar bloqueio de objeto* e definir as configurações de bloqueio de objeto.

- Quando a opção de bloqueio de objeto é ativada, as configurações de retenção na guia Programar não são aplicáveis.

Compactação

Especifica para selecionar um nível de compactação para cópias de ponto de recuperação. A compactação geralmente é executada para reduzir o uso de espaço em disco, mas também tem um impacto adverso sobre a velocidade do backup devido ao aumento no uso da CPU. As opções disponíveis são:

Sem compactação - a compactação não será executada. Os arquivos estão no formato VHD puro. Essa opção exige menos uso da CPU (mais velocidade), mas também mais uso de espaço em disco para a imagem de backup.

Sem compactação - VHD - a compactação não será executada. Os arquivos são convertidos para o formato .vhd diretamente, sem a necessidade de operações manuais. Essa opção exige menos uso da CPU (mais velocidade), mas também mais uso de espaço em disco para a imagem de backup.

Compactação padrão - alguma compactação será executada. Essa opção proporciona um bom equilíbrio entre o uso da CPU e o uso do espaço em disco. Essa é a configuração padrão.

Compactação máxima - a compactação máxima será executada. Essa opção proporciona maior uso da CPU (menos velocidade), mas também menos uso de espaço em disco para a imagem de backup.

Observação: se a imagem de backup contiver dados não compactáveis (como imagens JPG ou arquivos ZIP), espaço adicional de armazenamento poderá ser alocado para lidar com esses dados. Como resultado, se você selecionar qualquer opção de compactação e possuir dados não compactáveis no backup, poderá na verdade resultar em um aumento do uso de espaço em disco.

Algoritmo de criptografia

Especifica o tipo de algoritmo de criptografia usado para cópias de ponto de recuperação. As opções de formatação são Sem criptografia, AES-128, AES-192 e AES-256.

Senha de criptografia

Especifica o fornecimento de uma senha de criptografia, que será usada para criptografar a sessão de destino. Ao restaurar a partir da cópia de pontos de recuperação, você deve fornecer essa senha para confirmar sua autenticação.

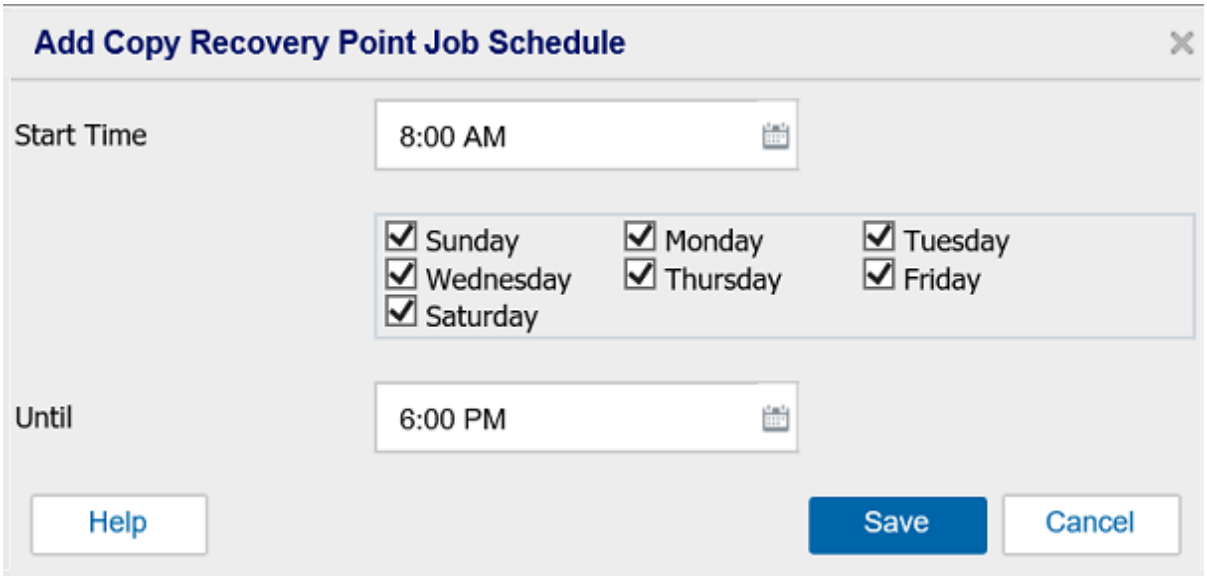
Confirmar senha de criptografia

Especifica para digitar a senha novamente.

5. Clique na guia **Programar** e especifique uma programação para a tarefa.

   Usando a opção de programação, é possível adicionar várias programações para um ponto de recuperação. Além disso, considere os seguintes detalhes:

   - Se nenhuma programação estiver configurada, a tarefa Copiar pontos de recuperação é executada imediatamente após a conclusão da tarefa de backup.
   - Agora, é possível configurar os pontos de recuperação de cópia para a hora de início e hora de término.



   - A CRP sempre tenta verificar a sessão disponível no momento.
   - Durante o período especificado, se qualquer sessão de backup configurada na guia Origem estiver disponível, a CRP copiará a sessão para o respectivo destino.
   - Também é possível configurar pontos de retenção para diário, semanal e mensal.

   Observação: o número de backups com êxito é contado para quaisquer backups diários, semanais ou mensais configurados.

6. Clique em **Salvar alterações**.

   As alterações são salvas e a tarefa de cópia de pontos de recuperação é automaticamente implantada no nó.

   Você criou com êxito e implantou o plano de cópia de pontos de recuperação.

Definir configurações de bloqueio de objeto para um serviço de nuvem

Esta seção fornece informações sobre como definir as configurações de bloqueio de objeto para um serviço de nuvem:

Siga estas etapas:

1. Marque a caixa de seleção Ativar bloqueio de objeto.

   O botão Configurações de bloqueio de objeto é ativado.

2. Clique no botão Configurações de bloqueio de objeto.

   A caixa de diálogo Configurações de bloqueio de objeto é exibida.

3. Na caixa de diálogo Configurações de bloqueio de objeto, faça o seguinte:

   Observação: na caixa de diálogo Configurações de bloqueio de objeto, as opções podem variar de acordo com o serviço de nuvem selecionado durante a criação de um plano.

   Amazon S3

   Modo de retenção padrão

   Permite ativar diferentes níveis de proteção em versões de objetos. Para ativar, selecione uma das seguintes opções:

   - **Controle:** se você tiver permissões especiais do IAM durante o período de retenção, será possível substituir ou excluir as versões do objeto protegido ou alterar as configurações de bloqueio.
   - **Conformidade:** não é possível substituir ou excluir versões de objetos protegidos, mesmo se você for um usuário raiz na conta do AWS.

   Período de retenção padrão

   Permite especificar uma quantidade fixa de tempo para proteger as versões do objeto. Você pode fornecer o período de retenção em dias ou anos.

   Wasabi Hot Cloud Storage

   Modo de retenção padrão

   Permite ativar diferentes níveis de proteção em versões de objetos. Para ativar, selecione uma das seguintes opções:

- **Controle:** se você tiver permissões especiais do IAM durante o período de retenção, será possível substituir ou excluir as versões do objeto protegido ou alterar as configurações de bloqueio.
- **Conformidade:** não é possível substituir ou excluir versões de objetos protegidos, mesmo se você for um usuário raiz na conta do AWS.

Período de retenção padrão

Permite especificar uma quantidade fixa de tempo para proteger as versões do objeto. Você pode fornecer o período de retenção em dias ou anos.

Nutanix Objects

Período de retenção padrão

Permite especificar uma quantidade fixa de tempo para proteger as versões do objeto. Você pode fornecer o período de retenção em dias ou anos.

Observação: quando o bloqueio de objeto é ativado durante a criação de um plano para objetos do Nutanix, o seguinte também é ativado:

- **WORM (Write-Once-Read-Many):** não é possível substituir ou excluir os objetos existentes durante um período de retenção especificado.
- **Controle de versão:** é possível manter várias versões de objetos do Nutanix em um compartimento de memória.

4. Clique em **OK**.

Estrutura de diretórios de pontos de recuperação no recipiente/compartimento de memória na nuvem

Todos os pontos de recuperação de nós com um único plano de CRP e uma conta de nuvem (criada no console de gerenciamento do Arcserve) como um destino são armazenados dentro de um compartimento de memória na nuvem.

Segue abaixo a estrutura de diretórios de pontos de recuperação no recipiente/compartimento de memória na nuvem:

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>

Observações:

- As novas alterações do prefixo arcserve-{random-generated-id}- não têm efeito nos planos existentes.
- O prefixo arcserve-{random-generated-id}- é adicionado ao nome do compartimento de memória configurado na conta da nuvem.
- O nome do nó é semelhante ao que aparece no destino de backup.
- AAA-MM-DD: formato de data (A – ano, M – mês, D – dia)
- HH-MM-SS: formato de hora (H – hora, M – minuto, S – segundo)
- <ScheduleType> é o tipo de programação de backup e refere-se a uma das seguintes opções:

  - Diariamente: ponto de recuperação de backup diário
  - Semanalmente: ponto de recuperação de backup semanal
  - Mensalmente: ponto de recuperação de backup mensal
  - Personalizado: ponto de recuperação carregado usando a opção de carregamento de ponto de recuperação na nuvem (cópia de ponto de recuperação ad hoc)

- Os pontos de recuperação de nós que compartilham o mesmo nome são armazenados em um único diretório se eles forem destinados à mesma conta da nuvem. Como resultado, é recomendável usar uma conta da nuvem diferente para nós que compartilham o mesmo nome para que eles sejam armazenados em compartimentos de memória diferentes.

Verificar o plano

Para verificar o recurso de cópia de pontos de recuperação, confirme se o plano foi criado com êxito. Depois de verificar se o plano está criado com êxito, confirme se a tarefa de backup está executando conforme o programado. Depois que a tarefa de backup for concluída com êxito, a tarefa de cópia de pontos de recuperação será executada. É possível verificar o status da tarefa de backup e da tarefa de cópia dos pontos de recuperação na guia **tarefas**.

Siga estas etapas para verificar os planos:

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.

   Uma lista de todos os nós é exibida no painel central.
3. Verifique se os planos são mapeados com nós.

Siga estas etapas para verificar as tarefas de cópia de pontos de recuperação:

1. Clique na guia **tarefas**.
2. No painel à esquerda, clique em **Todas as tarefas**.

   O status de cada tarefa é incluído no painel central.
3. Verifique se a tarefa de backup e a tarefa de cópia dos pontos de recuperação foram bem-sucedidas.

Como criar um plano de cópia de arquivo

Com o Arcserve Unified Data Protection, você pode copiar ou mover arquivos de origem selecionados para um destino. O destino pode ser uma conta em nuvem ou uma rede compartilhada. O arquivo de origem deve ser do mesmo volume que já foi copiado para backup. Por exemplo, se tiver feito o backup de todo o volume D:\ do nó de origem. Agora você deseja copiar um arquivo específico do volume D:\ do nó de origem. É possível criar uma tarefa de cópia de arquivo para executar essa operação.

A cópia de arquivo pode ser usada para copiar dados críticos em locais secundários e também como solução de arquivamento.

As vantagens de copiar arquivos são:

- Melhorar a eficiência - ajuda-o a acelerar os processos de recuperação e de backup ao copiar e mover dados inalterados e, dessa forma, reduzir a quantidade de dados reais armazenados em fita ou disco e cujo backup está sendo feito.
- Atender à conformidade normativa - ajuda-o a preservar importantes documentos, emails e outros dados essenciais, conforme necessário, para cumprir as normas e regulamentações internas e externas.
- Reduzir o custo de armazenamento - ajuda-o a recuperar a capacidade de armazenamento ao migrar dados mais antigos ou pouco acessados dos sistemas principais para locais de armazenamento de arquivos econômicos.
- Manter várias versões de arquivo - ajuda-o a reverter versões anteriores de arquivos de backup (se necessário) ou manter várias versões dos mesmos arquivos em outros destinos.

O que fazer a seguir?

- Verificar os pré-requisitos
- Criar um plano com uma tarefa de backup
- Adicionar uma Tarefa de cópia de arquivo ao plano
- (Opcional) Executar uma cópia de arquivo manual
- Verificar o plano

Verificar os pré-requisitos e as considerações

Verifique se concluiu os seguintes pré-requisitos:

- Efetue logon no Console.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Considerações:

- a tabela a seguir fornece o limite do comprimento do nome de arquivo de uma tarefa de cópia de arquivo. Os arquivos que excederem os limites serão ignorados.

Destino	Limite
Compartilhamento de rede	240
Nuvem	245

- Se a cópia de arquivo estiver em execução na sessão replicada e Replicar *origem* tiver várias sessões de backup, a tarefa de cópia de arquivo será executada separadamente para cada sessão. Por exemplo, se houver **cinco** *sessões de backup* no destino de backup e você adicionar uma tarefa de replicação, a tarefa de replicação replicará todas as sessões em *uma única tarefa*. Agora, se você adicionar uma tarefa de cópia de arquivo, e a origem da cópia de arquivo for o destino de replicação, então **cinco** *tarefas de cópia de arquivo* serão executadas para replicar cada sessão.

Criar um plano com uma tarefa de backup

Um plano inclui tipos diferentes de tarefas que você deseja executar. Para criar uma tarefa de cópia de arquivo, é necessário, primeiramente, ter um ponto de recuperação válido. Para obter um ponto de recuperação válido, crie uma tarefa de backup.

Uma tarefa de backup executa um backup dos nós de origem e armazena os dados para o destino especificado. A cópia de arquivo é suportada apenas para backup no Windows com base no agente. O procedimento a seguir explica as etapas para criar a tarefa de backup do Windows com base em agente.

Siga estas etapas:

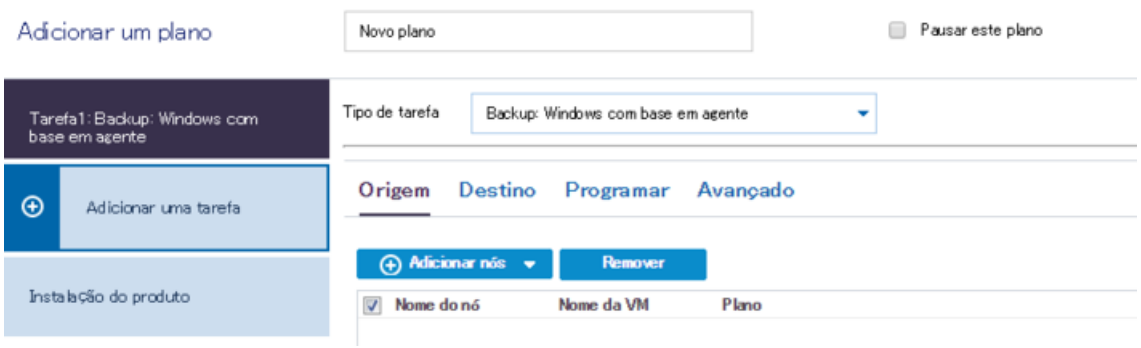
1. Clique na guia de **recursos** no Console.
2. No painel à esquerda, navegue para **Planos** e clique em **Todos os planos**.

   Se tiver criado os planos anteriores, esses planos serão exibidos no painel central.
3. No painel central, clique em **Adicionar um plano**.

   Adicionar um plano é exibido.
4. Digite o nome do plano.
5. (Opcional) Selecione a caixa de seleção **Pausar este plano**.

   O plano não será executado até que você desmarque a caixa de seleção para retomar o plano.

   Observação: se um plano for pausado, nenhuma tarefa em andamento será pausada, mas todas as tarefas programadas correspondentes associadas a esse plano serão pausadas. No entanto, você pode executar uma tarefa manualmente. Por exemplo, você pode executar manualmente a tarefa de backup e a tarefa de replicação para um nó mesmo que o respectivo plano esteja pausado. Nesse caso, a tarefa seguinte da tarefa sob demanda (manual) não será executada. Por exemplo, há uma tarefa de replicação após uma tarefa de backup sob demanda, a tarefa de replicação não será executada para a tarefa de backup sob demanda. É necessário executar manualmente a tarefa de replicação. Quando você retomar o plano, as tarefas pendentes não são retomadas imediatamente. Depois de retomar o plano, as tarefas pendentes serão executadas no próximo horário programado.
6. Na lista suspensa **Tipo de tarefa**, selecione **Backup, Windows com base em agente.**



Agora especifique a origem, o destino, a programação e as configurações avançadas.

Especificar a origem

A página Origem permite especificar os nós de origem que deseja proteger. É possível selecionar mais de um nó em um plano. Caso não tenha adicionado nós para o console, você pode adicionar nós ao criar ou modificar um plano da página de origem. Também é possível salvar um plano sem adicionar nenhum nó de origem. O plano é implantado somente após você adicionar nós de origem.

Siga estas etapas:

1. Na guia Origem, clique em **Adicionar**.
2. Selecione uma das seguintes opções:

   Selecionar os nós a serem protegidos no Arcserve UDP

   Abre a caixa de diálogo Selecionar nós para proteger no Arcserve UDP. Selecione os nós na lista exibida. Selecione esta opção se você já tiver adicionado os nós para o console.

   Adicionar nó do Windows

   A caixa de diálogo Adicionar nós a um plano é exibida. Selecione esta opção se você não tiver adicionado os nós e desejar adicionar manualmente os nós para proteger.

   Detectar os nós do Active Directory

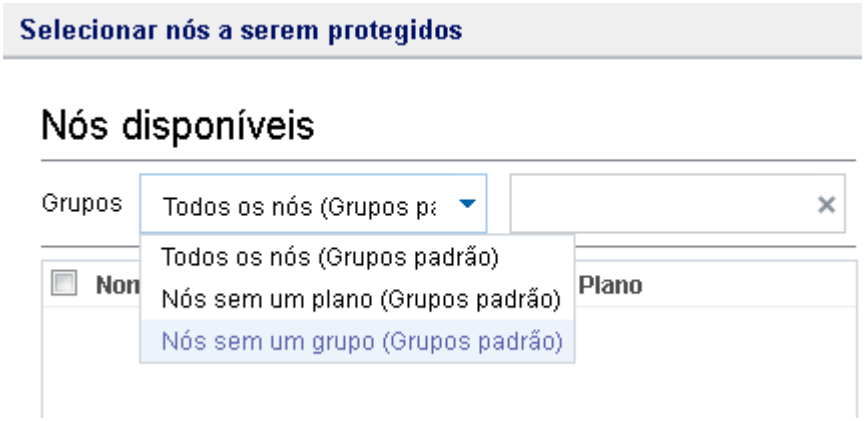
   Abra a caixa de diálogo Adicionar nós ao Console do Arcserve UDP. Selecione essa opção se desejar detectar e adicionar nós do Active Directory.
3. Se você selecionou a opção **Selecionar nós para proteger no Arcserve UDP**, na caixa de diálogo Selecionar nós para proteger, faça o seguinte:
   a. (Opcional) Selecione um filtro na lista suspensa Grupos para filtrar os nós. É possível digitar as palavras-chave para filtrar melhor seus nós.

      Os nós são exibidos na coluna Nós disponíveis.

   b. Selecione os nós na coluna Nós disponíveis e, em seguida, clique na seta simples à direita (>) ou na seta dupla à direita (>>) para mover os nós selecionados ou todos os nós, respectivamente, para a coluna Nós selecionados.

      Os nós são exibidos na coluna Nós selecionados.

   c. Clique em **OK** para fechar a caixa de diálogo.



4. Para escolher Tipo de proteção, selecione uma das seguintes opções:

   Fazer backup de todos os volumes

   Prepara um backup instantâneo de todos os volumes.

   Fazer backup dos volumes selecionados

   Prepara um instantâneo de backup do volume selecionado.

   A origem é especificada.

Especificar o destino

O destino é o local onde você armazena os dados de backup. É necessário, no mínimo, especificar o destino para salvar o plano.

Siga estas etapas:

1. Selecione um dos seguintes **Tipos de destino**:

   Disco local ou uma pasta compartilhada

   Especifica que o destino de backup é um destino local ou uma pasta compartilhada. Se selecionar essa opção, será possível salvar os dados como pontos de recuperação ou conjuntos de recuperação. As opções de pontos de recuperação e de conjuntos de recuperação estão disponíveis na guia **Programar**.

   Servidor de ponto de recuperação do Arcserve UDP

   Especifica que o destino de backup é um servidor do ponto de recuperação. Se selecionar essa opção, os dados serão armazenados como pontos de recuperação. Não é possível armazenar dados como conjuntos de dados de recuperação.

2. Se tiver selecionado **Servidor do ponto de recuperação do Arcserve UDP**, forneça os seguintes detalhes:
   a. Selecione um servidor do ponto de recuperação
   b. Selecione um repositório de dados. A lista exibe todos os repositórios de dados que são criados no servidor do ponto de recuperação especificado.
   c. Forneça uma senha da sessão.
   d. Confirme a senha da sessão.
3. Se tiver selecionado **Disco local ou pasta compartilhada**, forneça os seguintes detalhes:
   a. Forneça o caminho completo do destino local ou de rede. Para o destino de rede, especifique as credenciais com o acesso de gravação.
   b. Selecione o algoritmo de criptografia. Para obter mais informações, consulte Configurações de criptografia.
   c. Como opção, forneça uma senha de criptografia.
   d. Confirme a senha de criptografia.
   e. Selecione um tipo de compactação. para obter mais informações, consulte Tipo de compactação.

Observação: se armazenar os dados em um disco local ou em uma pasta compartilhada, não será possível replicar os dados para outro servidor do ponto de recuperação. A replicação é suportada apenas se armazenar os dados em um servidor do ponto de recuperação.

O destino é especificado.

Especificar a programação

A página Programar permite definir uma programação para o backup e para que as funções Mesclar e Acelerar sejam repetidas em intervalos específicos. Após definir uma programação, as tarefas são executadas automaticamente de acordo com a programação. É possível adicionar várias programações e fornecer configurações de retenção.

Uma Programação de backup se refere a programação regular que é repetida várias vezes ao dia, com base no número de horas ou de minutos selecionado. Além da programação regular, uma programação de backup também fornece opções para adicionar programações diária, semanal e mensal.

Observação: para obter mais informações sobre as configurações de retenção e programação, consulte Entendendo a programação avançada e retenção.

Siga estas etapas:

1. (Opcional) Selecione a opção para gerenciar os pontos de recuperação. Essa opção será visível somente se tiver selecionado o local ou a pasta compartilhada como o destino do backup.

   Reter por pontos de recuperação

   Os dados de backup são armazenadas como pontos de recuperação.

   Reter por conjuntos de recuperação

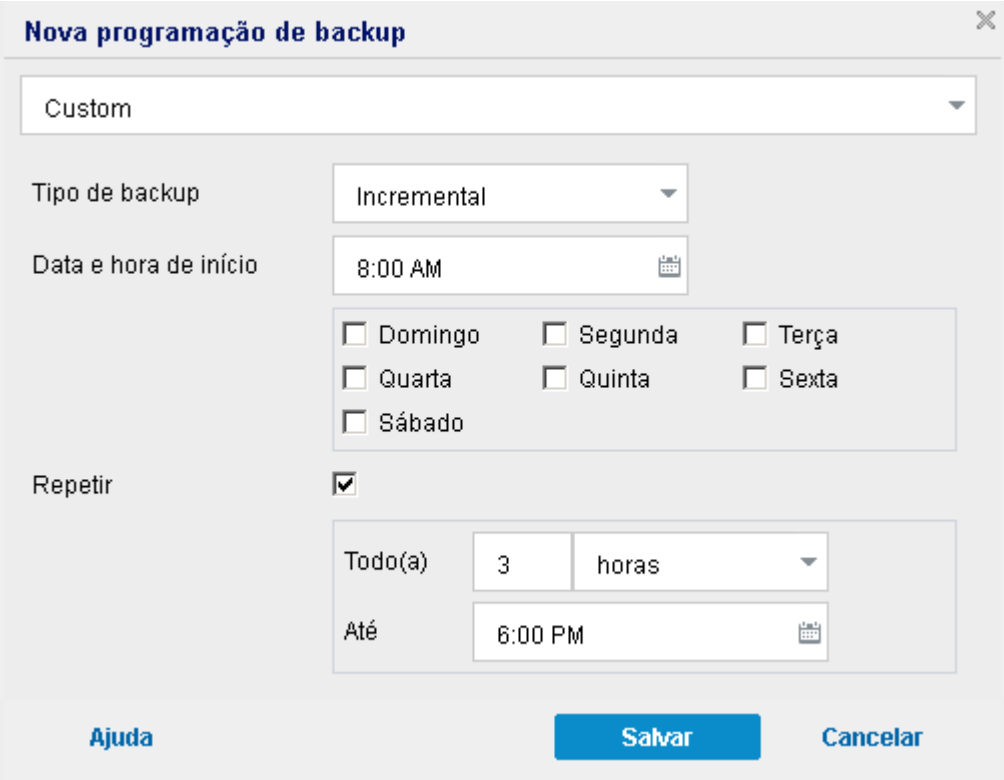
   Os dados de backup são armazenadas como conjuntos de recuperação.

2. Adicionar programações de backup, mesclagem e acelerador.

   Adicionar programação de backup

   a. Clique em **Adicionar** e selecione **Adicionar programação de backups**.

      A caixa de diálogo **Nova programação de backup** é aberta.



b. Selecione uma das seguintes opções:

Personalizado

Especifica a programação de backup que se repete várias vezes por dia.

Diário

Especifica a programação de backup que ocorre uma vez por dia. Por padrão, todos os dias da semana estão selecionados para o backup diário. Se não desejar executar a tarefa de backup em um dia específico, desmarque a caixa de seleção correspondente àquele dia da semana.

Semanal

Especifica a programação de backup que ocorre uma vez por semana.

Mensal

Especifica a programação de backup que ocorre uma vez por mês.

c. Selecione o tipo de backup.

Completo

Especifica a programação de backups para backups completos. Conforme programado, o Arcserve UDP executa um backup completo de todos os blocos usados do computador de origem. Um backup completo em geral, consome tempo, dependendo do tamanho do backup.

Verificar

Especifica a programação de backups para backups de verificação.

A Arcserve UDP verifica se os dados protegidos são válidos e concluídos, executando uma verificação de confiabilidade da imagem de backup armazenada na origem do backup. Se necessário, a imagem será sincronizada novamente. Um backup de verificação examinará o backup mais recente de cada bloco e irá comparar o conteúdo e as informações com a origem. Esta comparação verifica se o backup mais recente dos blocos representa as informações correspondentes na origem. Se a imagem de backup de qualquer bloco não corresponder à origem (possivelmente devido a alterações no sistema desde o último backup), o Arcserve UDP atualizará (fará nova sincronização) o backup do bloco que não corresponder. Também é possível usar um backup de verificação (muito raramente) para obter a garantia de backup completo sem usar o espaço necessário para um backup completo.

Vantagens: produz uma pequena imagem de backup quando comparado ao backup completo, pois somente os blocos alterados (blocos que não coincidem com o último backup) são armazenados em backup.

Desvantagens: o tempo de backup é longo, pois todos os blocos de origem são comparados aos blocos do último backup.

Incremental

Especifica a programação de backups para backups incrementais.

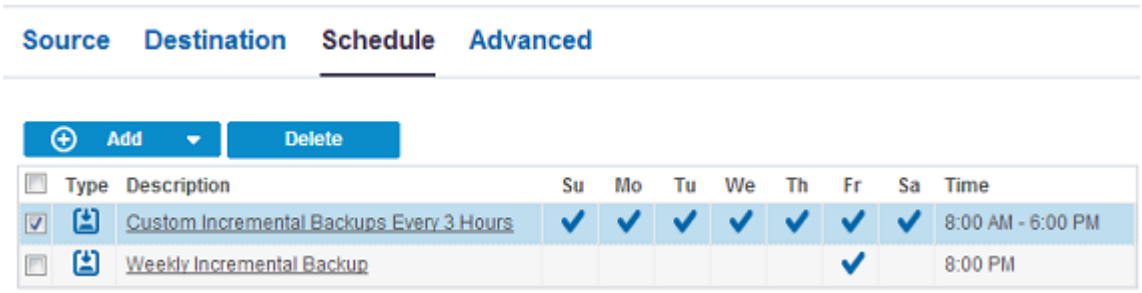
Conforme programado, o Arcserve UDP faz backup incremental apenas dos blocos que foram alterados desde o último backup realizado com êxito. As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a executar um backup.

d. Especifique a hora de início do backup.

e. (Opcional) Marque a caixa de seleção de **Repetição** e especifique a programação a ser repetida.

f. Clique em **Salvar**.

A programação de backup é especificada e exibida na página de **Programação**.



Adicionar Programação de mesclagem

a. Clique em Adicionar e selecione Adicionar programação de mesclagem.

   A caixa de diálogo **Adicionar nova programação de mesclagem** é aberta.

b. Especifique a hora de início para iniciar a tarefa de mesclagem.

c. Especificar **Até** para especificar uma hora de término para a tarefa de mesclagem.

d. Clique em **Salvar**.

   A programação de mesclagem é especificada e exibida na página **Programar**.

Adicionar programação de acelerador

a. Clique em **Adicionar** e selecione **Adicionar programação de acelerador.**

   A caixa de diálogo Adicionar nova programação do acelerador é aberta.

b. Especifique o limite de taxa de transferência em MB por minuto.

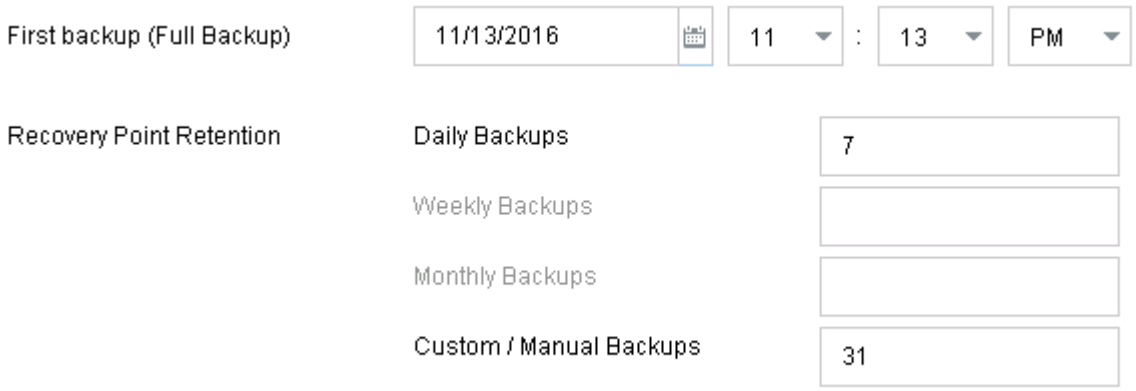
c. Especifique a hora de início para iniciar a tarefa de taxa de transferência de backup.

d. Especifique **Até** para especificar um horário de término para a tarefa de taxa de transferência.

e. Clique em **Salvar**.

   A Programação de acelerador é especificada e exibida na página **Programar**.

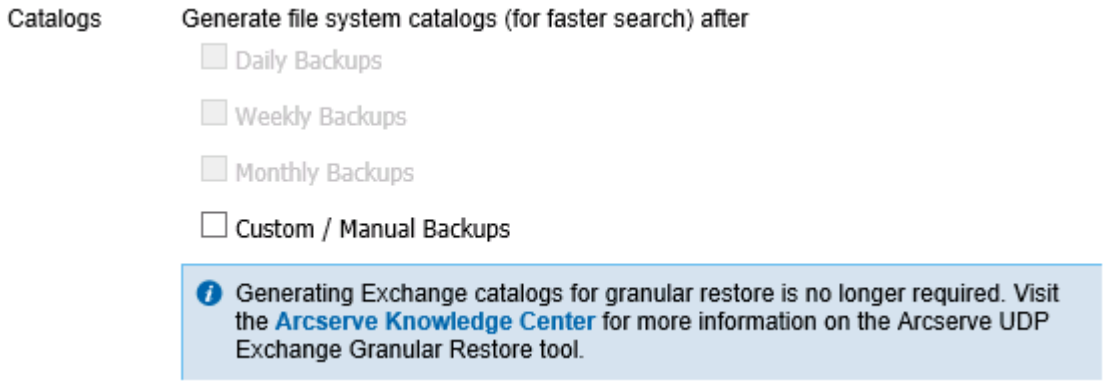
3. Especifique a hora de início do backup programado.



4. Especifique as configurações de retenção de pontos de recuperação para programação diária, semanal e mensal.

   Essas opções serão ativadas se tiver adicionado a programação de backup correspondente. Se você modificar as configurações de retenção desta página, as alterações serão refletidas na caixa de diálogo Programação de backup.

5. Especifique os detalhes de catálogo.



   Os catálogos permitem gerar o catálogo do sistema de arquivos. O catálogo do sistema de arquivos é necessário para agilizar e melhorar a pesquisa. Se marcar as caixas de seleção do catálogo, os catálogos serão ativados de acordo com o tipo de backup que você especificou. Desmarque a caixa de seleção para desativar a geração do catálogo.

   A programação é especificada.

Noções básicas sobre a programação avançada e retenção

A opção de programação permite especificar uma programação personalizada, uma programação diária/semanal/mensal ou ambas. Na programação personalizada, é possível configurar a programação de backups para cada dia da semana ou adicionar até quatro programações de backup em cada dia. É possível escolher um dia específico da semana e criar uma janela para definir quando executar o backup e em que frequência.

Programação	Tarefa com suporte	Comentários
Backup	Tarefa de backup	Definir janelas de tempo para a execução de tarefas de backup.
Limitação de backup	Tarefa de backup	Definir janelas de tempo para controlar a velocidade de backup.
Mesclar	Tarefa de mesclagem	Definir quando executar tarefas de mesclagem.
Programação diária	Tarefa de backup	Definir quando executar tarefas do backup diário.
Programação semanal	Tarefa de backup	Definir quando executar tarefas do backup semanal.
Programação mensal	Tarefa de backup	Definir quando executar tarefas do backup mensal.

Também é possível especificar as configurações de retenção para os pontos de recuperação.

Observação: as configurações de retenção devem ser definidas em cada plano para controlar como os dados dos nós atribuídos a esse plano são retidos no repositório de dados de destino.

As programações para backups diários/semanais/mensais são independentes para a programação personalizada e umas das outras. É possível configurar para executar somente o backup diário, semanal ou mensal, sem configurar a Programação personalizada.

Programação de tarefas de backup

É possível adicionar quatro janelas de tempo por dia na programação do backup. Uma janela de tempo é válida das 00:00 às 23:59. Não é possível especificar uma janela de tempo das 18:00 às 6:00. Nesses casos, você deve especificar manualmente duas janelas de tempo diferentes.

Para cada janela de tempo, a hora de início é inclusiva e a hora de término é exclusiva. Por exemplo, você configurou para executar o backup incremental em intervalos de uma hora entre as 6:00 e as 9:00. O backup será iniciado às 6:00. Isso significa que o backup será executado às 6h00, 7h00 e 8h00, mas NÃO às 9h00.

Observação: se você deseja executar a tarefa de backup várias vezes até o fim do dia, defina a programação para até 0h00. Por exemplo, para executar a tarefa de backup a cada 15 minutos o dia inteiro, defina a programação como das 0h00 às 00h00, a cada 15 minutos.

Programação do acelerador de backup

A programação de aceleração do backup permite controlar a velocidade da taxa de transferência de backup o que, por sua vez, controla o uso de recursos (E/S de disco, CPU, largura de banda de rede) do servidor cujo backup está sendo feito. Isso é útil quando se não quiser afetar o desempenho do servidor durante o horário comercial. É possível adicionar quatro janelas de tempo por dia na sua programação de aceleração do backup. Para cada janela de tempo, é possível especificar um valor, em MB por minuto. Esse valor será usado para controlar a taxa de transferência do backup. Os valores válidos variam entre 1 MB/minutos a 99999 MB/minutos.

Se uma tarefa de backup estende seu tempo especificado, o limite de aceleração será ajustado de acordo com o tempo especificado. Por exemplo, você definiu o limite de aceleração de backup como 500 MB/minuto das 8:00 às 20:00 e 2500 MB/minuto das 20:00 às 22:00. Se uma tarefa de backup iniciar às 19h00 e for executada durante três horas, das 19h00 às 20h00 o limite de aceleração será de 500 MB/minuto e das 20h00 às 22h00, o limite de aceleração será 2500 MB/minuto.

Se não definir nenhuma programação do backup e programação da taxa de transferência do backup, o backup será executado o mais rápido possível.

Mesclar a programação

Permite mesclar pontos de recuperação com base na programação fornecida.

Considere os seguintes pontos para a tarefa de mesclagem:

- A qualquer momento apenas uma tarefa de mesclagem pode ser executada para um nó.
- Se uma tarefa de mesclagem iniciar, ela precisará ser concluída antes que a próxima tarefa de mesclagem seja iniciada. Isso significa que, se um ou mais conjuntos de pontos de recuperação forem mesclados, não será possível adicionar o

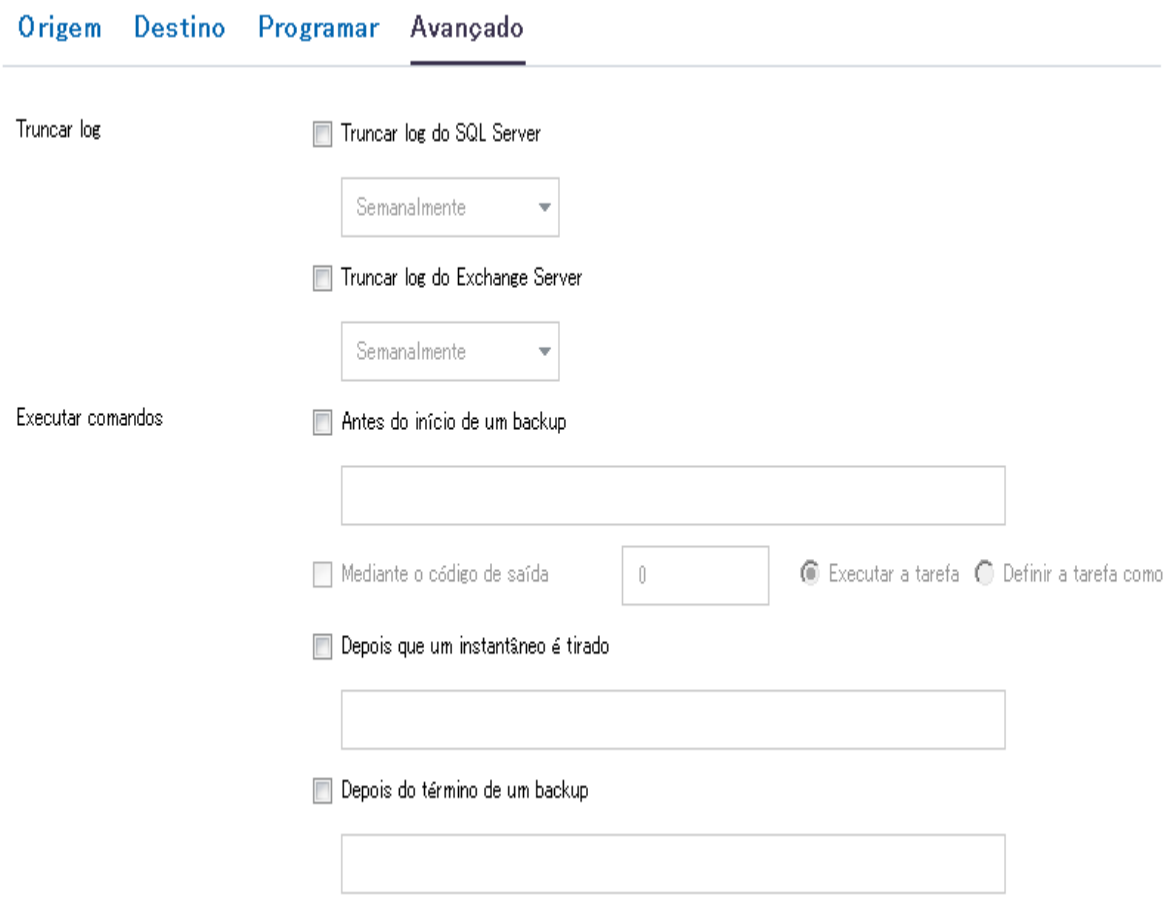
novo ponto de recuperação a este processo de mesclagem, até que o processo de mesclagem do conjunto atual de ponto de recuperação seja concluído.

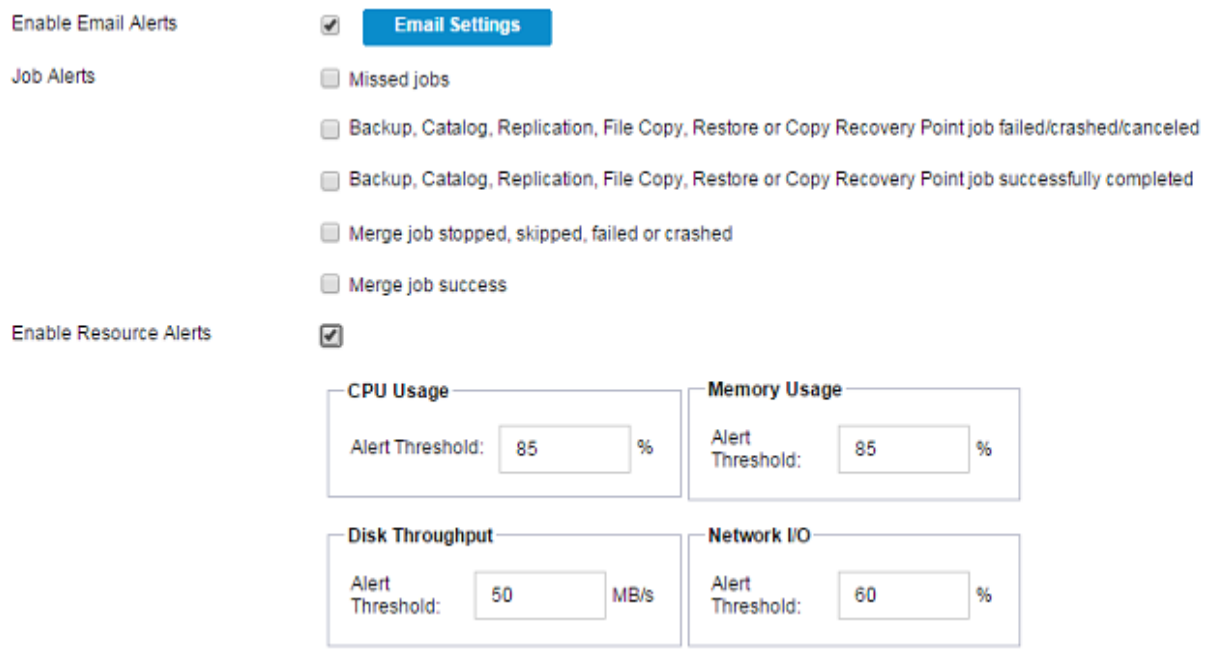
- Se uma tarefa de mesclagem estiver processando mais de um conjunto de pontos de recuperação (por exemplo, conjunto [1~4], conjunto [5~11] e conjunto [12~14]; são três conjuntos) o servidor de ponto de recuperação processará esses conjuntos, um por um.
- Se uma tarefa de mesclagem é retomada após um intervalo, a tarefa detectará em que ponto ela foi pausada e continuará a mesclagem a partir do ponto de pausa.

Especificar as configurações avançadas

A guia **Avançado** permite especificar algumas configurações avançadas para a tarefa de backup. As configurações avançadas incluem fornecer configurações de log de truncamento, a localização de quaisquer scripts e as configurações de email.

A imagem a seguir mostra a guia Avançado:





Siga estas etapas:

1. Especifique os seguintes detalhes.

Truncar log

Permite especificar a programação para truncar logs para o SQL Server e o Exchange Server. É possível especificar a programação como **Diária**, **Semanal** ou **Mensal**.

Nome de usuário

Permite especificar o usuário que possui autorização para executar um script.

Senha

Permite especificar a senha do usuário que está autorizado a executar o script.

Executar um comando antes do início do backup

Permite a execução de um script antes de iniciar a tarefa de backup. Especifique o caminho onde o script está armazenado. Clique em **No código de saída** e especifique o código de saída para **Executar tarefa** ou **Tarefa com falha**. **Executar a tarefa** indica que a tarefa de backup continuará quando o script retornar o código de saída. **Tarefa com falha** indica que a tarefa de backup será interrompida quando o script retornar o código de saída.

Executar um comando após a criação de um instantâneo

Permite executar um script depois que o backup do instantâneo for gerado. Especifique o caminho onde o script está armazenado.

Executar um comando após a conclusão do backup

Permite executar um script depois que a tarefa de backup foi concluída. Especifique o caminho onde o script está armazenado.

Ativar alertas por email

Permite ativar alertas por email. É possível especificar configurações de email e os tipos de alertas que você deseja receber por email. Ao selecionar esta opção, as seguintes opções serão ativadas para a seleção.

Configurações de email

Permite configurar as definições de email. Clique em **Configurações de email** e configure o servidor de email e os detalhes do servidor proxy.

Alertas de tarefa

Permite que você selecione os tipos de emails da tarefa que deseja receber.

Ativar os alertas de recurso

Permite que você especifique um limite de uso da CPU, o uso da memória, a taxa de transferência de disco, E/S de rede. Você pode fornecer o valor em porcentagem. Você receberá um email quando o valor exceder o Limite de alerta.

2. Clique em **Salvar**.

Observação: quando você seleciona um nó como origem de backup ou proxy de backup, o Arcserve UDP verifica se o agente está instalado no nó e se é a versão mais recente. Em seguida, o Arcserve UDP exibe uma caixa de diálogo de verificação que lista todos os nós que possuem uma versão antiga do agente ou que não tem o agente instalado. Para instalar/atualizar o agente nesses nós, selecione o método de instalação e clique em Salvar.

As alterações são salvas e uma marca de seleção verde é exibida ao lado do nome da tarefa. A página do plano é fechada.

Observação: se precisar adicionar outra tarefa, deverá selecionar o plano na guia **Recursos** e modificar o plano. Para modificar o plano, clique no plano do painel central. O plano é exibido e será possível modificá-lo.

O plano de backup é criado e implantado automaticamente para o nó de origem. O backup é executado de acordo com a programação que você configurou na guia **Programar.** Também é possível fazer backup manual quando desejado.

Adicionar uma Tarefa de cópia de arquivo ao plano

A tarefa de cópia de arquivo permite copiar arquivos individuais para o destino especificado. A cópia original é mantida após você copiar os arquivos no destino especificado. A cópia de arquivo não depende de tarefas de geração de catálogo. Se o destino do backup for um repositório de dados de redução de redundância ou de não redução de redundância, a pasta Catálogo é movida para o destino de backup. A tarefa de catálogo faz parte da tarefa de cópia de arquivo. A tarefa de cópia de arquivo é executada no servidor de ponto de recuperação e, assim, o Arcserve UDP descarrega a tarefa dos agentes.

O Arcserve UDP oferece suporte à cópia de arquivo a partir de um repositório de replicação.

Verificação prévia para nós de cópia de arquivo: você também pode realizar uma PFC para cópia de arquivo. Apenas os nós adicionados para a cópia de arquivo qualificam-se para a PFC. Para executar a PFC para a cópia de arquivo, clique com o botão direito do mouse no nó Todos os nós e selecione Verificação prévia de cópia de arquivo.

Observação: se uma tarefa de backup estiver em andamento e fizer uma pausa no plano, a tarefa de backup irá obter o controle e a tarefa de cópia de arquivo não será iniciada. Ao retomar o plano novamente, a tarefa de cópia de arquivo não é retomada automaticamente. É necessário executar manualmente outra tarefa de backup para acionar a tarefa de cópia de arquivo.

Siga estas etapas:

1. Clique em **Adicionar uma tarefa** no painel esquerdo.

   Uma nova tarefa será adicionada ao painel esquerdo.

2. No menu suspenso, selecione **Tipo de tarefa,** selecione **Cópia de arquivo**.

   A tarefa de cópia de arquivo é adicionada.

3. Clique na guia **Origem** e especifique os detalhes.

   Origem de pontos de recuperação para a cópia de arquivo

   Permite selecionar a origem dos pontos de recuperação. Se houver apenas uma origem, ela é exibida automaticamente. Se houver mais de uma origem, você precisa selecionar a origem correta na lista suspensa.

   Tipos de pontos de recuperação

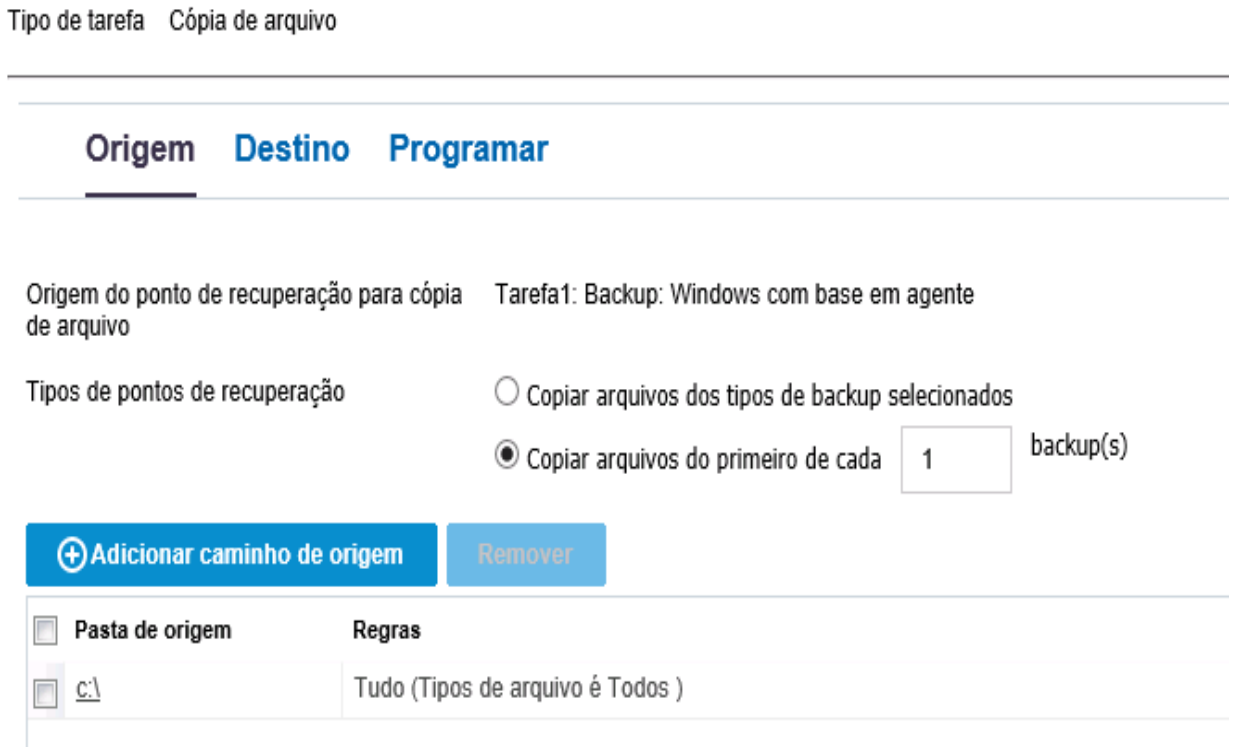
   Permite selecionar os pontos de recuperação para a cópia de arquivo. É possível selecionar qualquer uma das duas opções a seguir:

   Copiar arquivos de tipos de backup selecionados

Você pode selecionar **Backups diários**, **Backups semanais** ou **Backups mensais**. As opções de backup diário, semanal ou mensal são ativadas de acordo com a programação do backup de origem. Por exemplo, se o backup de origem tiver somente o backup mensal programado, a opção **Copiar arquivos de tipos de backup selecionados** tem somente **Backups mensais** ativado.

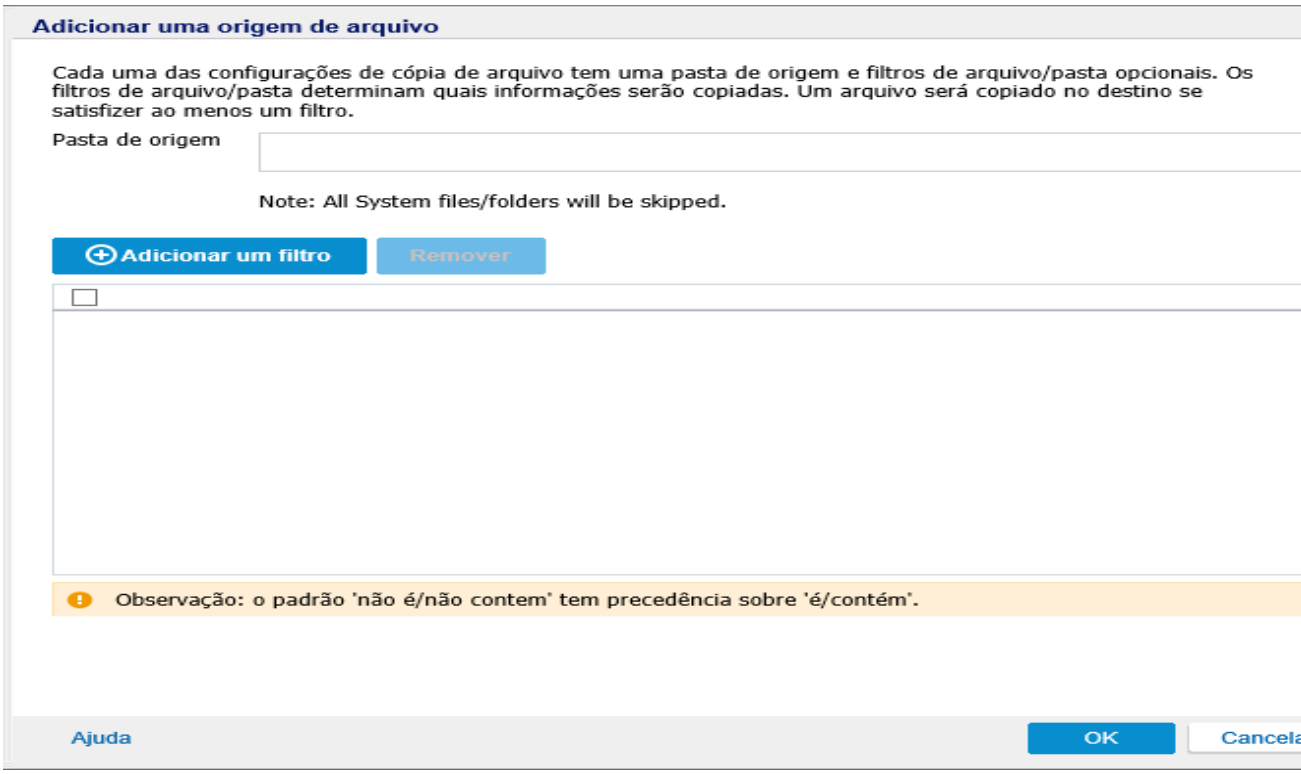
Copiar arquivo do primeiro de cada backup ou mais

É possível especificar o número do backup que você deseja copiar. Por exemplo, se você especificar 3, o terceiro backup será copiado. A cópia de arquivo oferece suporte a até 700 pontos de recuperação dos quais copiar.



4. Clique em **Adicionar caminho de origem**.

   A caixa de diálogo **Adicionar uma origem de arquivo** é aberta.



Você pode evitar ignorar o sistema do Windows (C:\Windows), arquivos de programas (C:\Program Files e diretórios C:\Program Files (x86)) usando a seguinte configuração:

Adicione a seguinte marca XML, se ela não estiver presente, ou atualize no arquivo FileCopyDebugSetting.xml presente na pasta $UDPHome\Engine\Configuration:

<SkipWindowsFolders>0</SkipWindowsFolders>

O arquivo XML aparece da seguinte maneira:

<?xml version="1.0" encoding="UTF-8"?>

<HKLM>

<AFArchiveDLL>

.....

<SkipWindowsFolders>0</SkipWindowsFolders>

</AFArchiveDLL>

</HKLM>

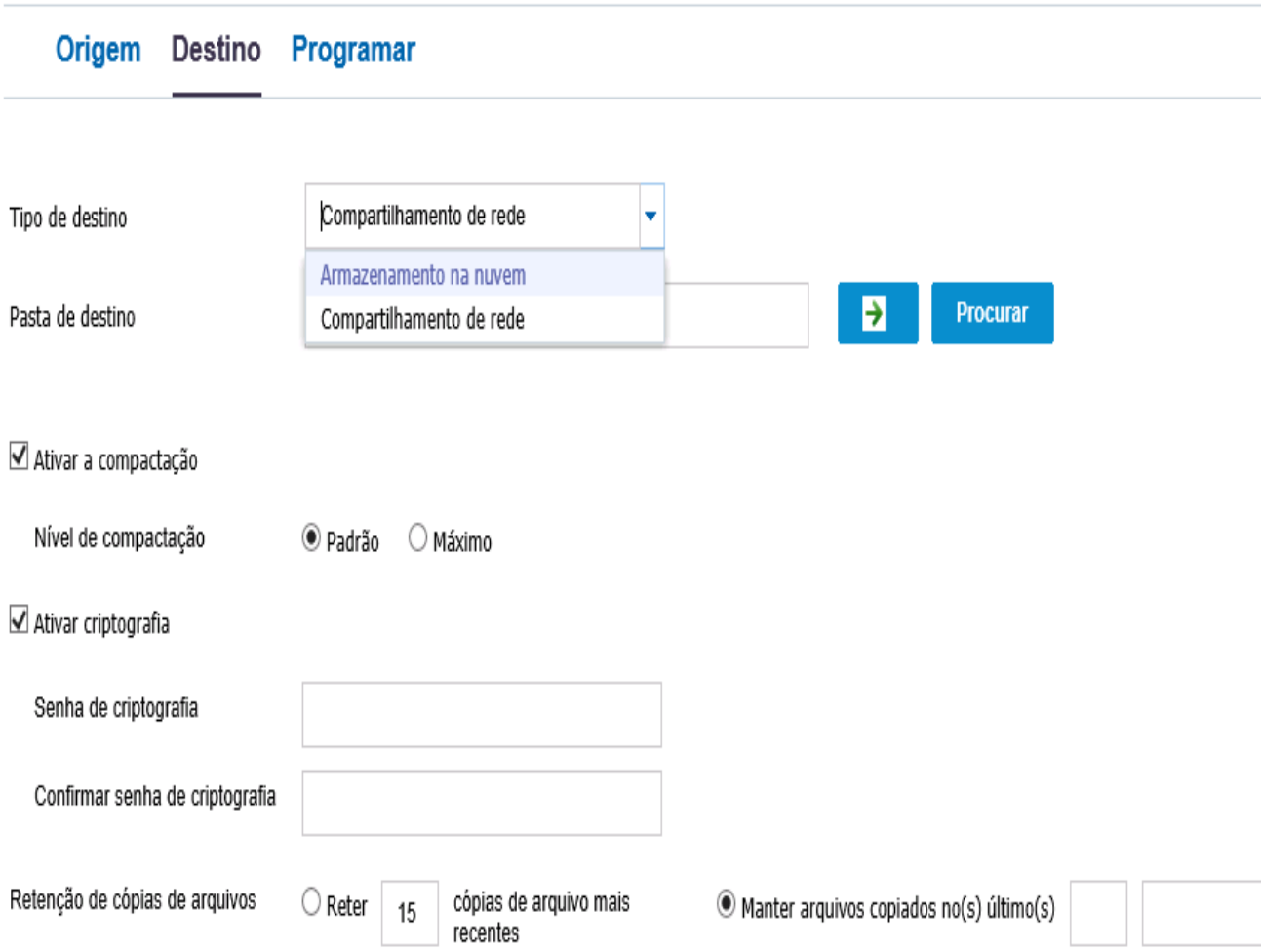
5. Especifique o caminho da pasta de origem que você deseja copiar.
6. Clique em **Adicionar um filtro**.

O filtro é adicionado abaixo do botão **Adicionar um filtro.** É possível adicionar vários filtros e remover os filtros. Para obter mais informações, consulte Adicionar filtros de cópia de arquivo.

7. Selecione o filtro na lista e clique em **OK**.

   A caixa de diálogo **Adicionar uma origem de arquivo** fecha.

8. Clique na guia **Destino** e especifique os detalhes do destino.



Tipo de destino

Especifica que o tipo de destino é um compartilhamento de rede ou um armazenamento na nuvem. Para a opção de destino, se a conexão com o destino especificado for perdida ou interrompida, o Arcserve UDP fará várias tentativas para continuar a tarefa de cópia de arquivo. Se essas novas tentativas não forem bem-sucedidas, uma tarefa de constituição será executada a partir do ponto em que a falha ocorreu. Além disso, o log de atividades será atualizado com uma mensagem de erro correspondente e uma notificação por email será enviada (se configurada).

Compartilhamento de rede

Especifica que o destino é uma pasta compartilhada. Quando selecionado, permite especificar o caminho completo do local onde deseja mover ou copiar os arquivos/pastas de origem.

Pasta de destino

Especifica o destino onde os arquivos copiados serão armazenados. O destino pode ser um volume ou uma pasta local ou um compartilhamento de arquivo acessível por qualquer UNC (Uniform naming convention - Convenção de nomenclatura uniforme). Esse campo é disponibilizado quando você seleciona Compartilhamento de rede como o tipo de destino. Também é possível procurar a pasta de destino.

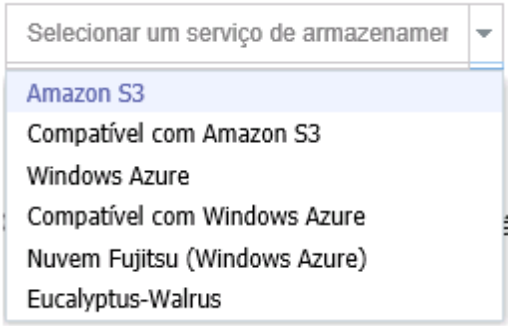
Armazenamento na nuvem

Especifica que os arquivos copiados serão armazenados em um ambiente na nuvem. O Arcserve UDP atualmente oferece suporte à cópia de arquivos para vários fornecedores de nuvem, como Amazon S3 (Simple Storage Service), compatível com Amazon S3, Windows Azure, compatível com Windows Azure, Eucalyptus-Walrus e FUJITSU Hybrid IT Service FJcloud-O. Esses fornecedores de nuvem são serviços da web disponíveis publicamente que permitem armazenar e recuperar qualquer quantidade de dados, a qualquer momento, de qualquer lugar na web, em um ambiente seguro e protegido.

Observação: para eliminar um possível erro de precisão do relógio ao tentar se conectar à nuvem, verifique se o computador tem o fuso horário adequado definido, e se o relógio está em sincronia com o horário mundial. É necessário sempre verificar o horário do computador referente ao horário GMT. Se a hora do computador não estiver sincronizada com o tempo global adequado (de 5 a 10 minutos), o a conexão com a nuvem pode não funcionar. Se necessário, redefina a hora correta do computador e execute novamente a tarefa cópia de arquivo.

Dispositivo de armazenamento

Selecione o tipo de dispositivo na lista suspensa.



Armazenamento na nuvem

Selecione o caminho do armazenamento na nuvem na lista suspensa. A lista suspensa será disponibilizada se você especificar os detalhes do armazenamento na nuvem. Se estiver especificando a conta de armazenamento na nuvem pela primeira vez, clique em Adicionar para adicionar a conta de nuvem. Quando você seleciona Armazenamento na nuvem, na próxima vez, a conta será exibida na lista suspensa Armazenamento na nuvem.

Observação: para obter mais informações sobre a adição de uma conta de nuvem, consulte Adicionar uma conta de nuvem.

Compactação

Especifica o tipo de compactação usada para tarefas de cópia de arquivo.

A compactação é executada para reduzir o espaço de armazenamento no destino da cópia do arquivo, mas também tem um impacto inverso na velocidade da cópia de arquivo devido ao aumento no uso da CPU.

Observação: para obter uma cópia do arquivo compactado, o log de atividades exibe apenas o tamanho descompactado.

As opções disponíveis são:

Compactação padrão

Alguma compactação será realizada. Esta opção proporciona um bom equilíbrio entre o uso da CPU e o requisito do espaço de armazenamento. Essa é a configuração padrão.

Compactação máxima

A compactação máxima será realizada. Essa opção exige mais uso da CPU (menos velocidade), mas também requer menos espaço de armazenamento para a cópia de arquivo.

Ativar criptografia

Especifica o uso de criptografia para cópia de arquivo.

A criptografia de dados é a conversão de dados em uma forma ininteligível sem um mecanismo decodificador. A proteção de dados do Arcserve UDP usa algoritmos de criptografia seguros AES-256 (padrão de criptografia avançada) para atingir o máximo de segurança e privacidade dos dados especificados. É necessário fornecer (e confirmar) uma senha criptografada quando uma criptografia for selecionada.

Observação: quando você modifica uma tarefa de cópia de arquivo, não é possível modificar a criptografia nem a compactação.

Retenção de arquivo

Mantém os arquivos no destino de cópia de arquivo se os critérios especificados forem atendidos.

Arquivo criado no último

Especifica o tempo (anos, meses, semanas) que os dados armazenados devem ser mantidos no local de destino. No final do período de retenção especificado, os dados armazenados serão removidos do destino.

Importante: no final do tempo de retenção especificado, quando os dados forem removidos do destino, todos esses dados movidos não serão mais armazenados ou salvos.

Observação: o processo de limpeza do período de retenção só é acionado quando a opção Programação da cópia de arquivo estiver ativada.

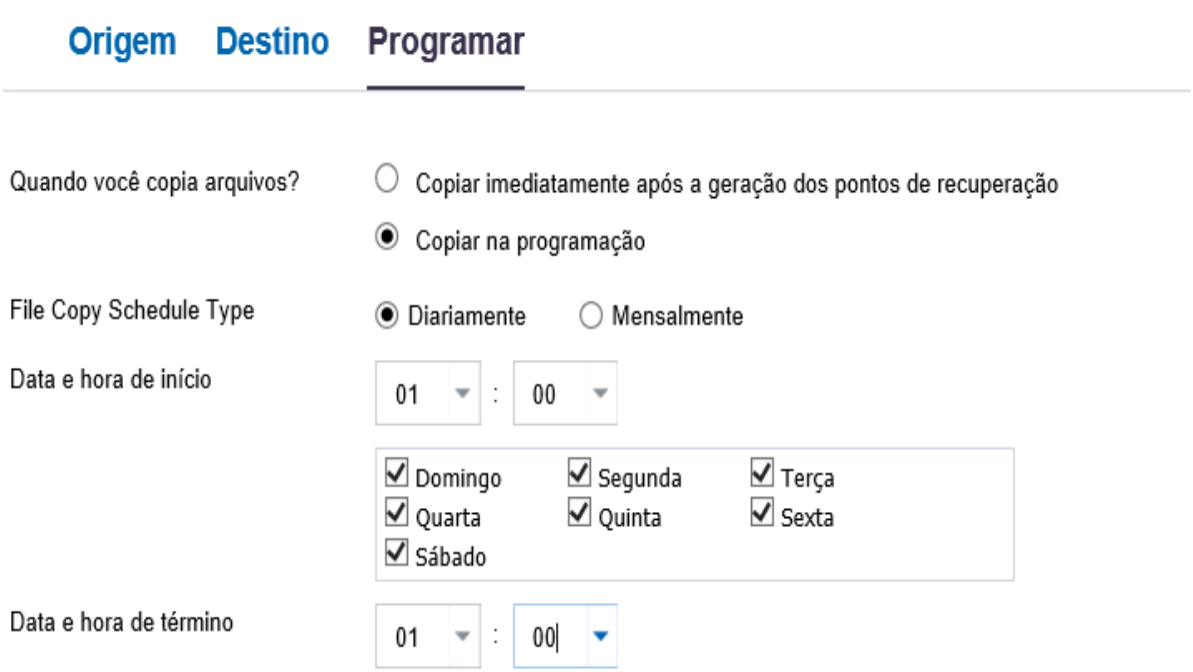
Versão de arquivo anterior a

Especifica o número de cópias mantidas e armazenadas no local de destino. Quando este número for excedido, a primeira versão (mais antiga) será descartada. O ciclo de descartar a versão armazenada mais antiga será repetido à medida que versões mais novas forem adicionadas ao destino, permitindo que você sempre mantenha a quantidade especificada de versões armazenadas.

Por exemplo, se a contagem de retenção de versões de arquivo especificada for definida como 5 e se você fizer cinco cópias de arquivo nas horas t1, t2, t3, t4 e t5, estas se tornarão as cinco versões de cópia de arquivo retidas e disponíveis para recuperação. Depois que a sexta cópia de arquivo foi executada (a versão nova foi salva), o Arcserve UDP removerá a cópia t1 e as cinco versões disponíveis para recuperação agora são t2, t3, t4, t5 e t6.

Por padrão, a quantidade de cópias mantida no local de destino antes de descartar é 15.

9. Clique na guia **Programar** e especifique a programação da cópia de arquivo.



Se a execução de uma tarefa de cópia de arquivo exceder a hora de término, ela continuará até que ela seja concluída. A próxima tarefa de cópia de arquivo não será executada até que a tarefa de cópia de arquivo anterior seja concluída, mesmo que uma tarefa programada se sobreponha à tarefa em execução.

A tarefa de cópia de arquivo é executada conforme especificado na programação.

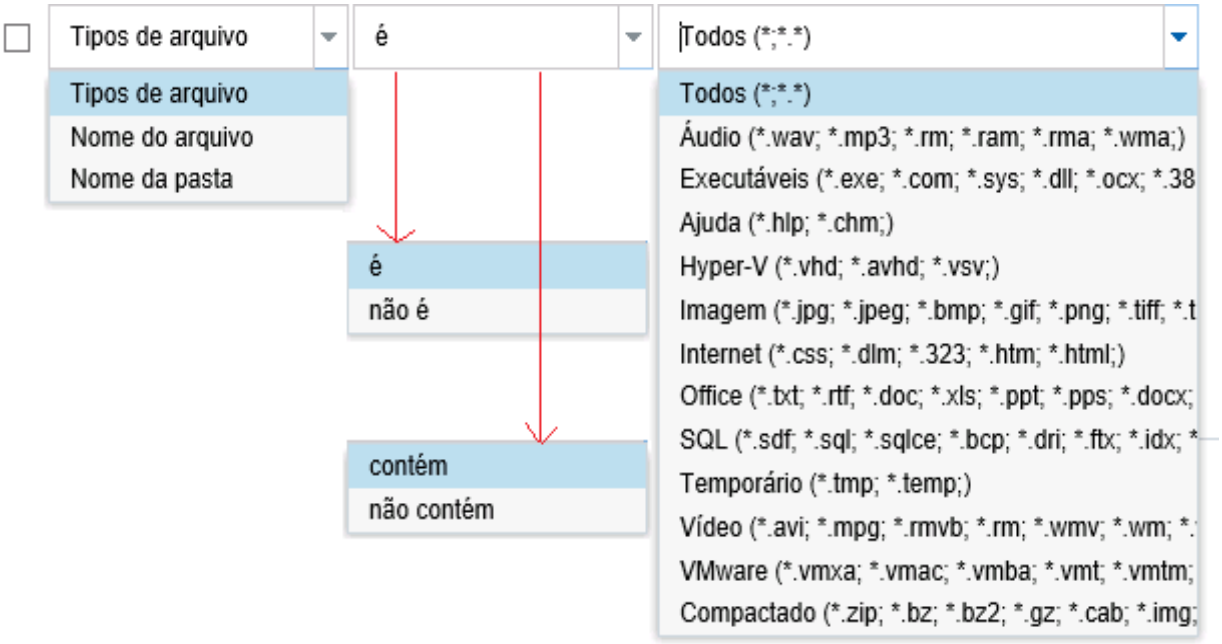
10. Clique em **Salvar**.

    As alterações são salvas e a tarefa de cópia de arquivo é automaticamente implantada no nó.

Adicionar filtros de cópia de arquivo

Adicionar um filtro

Permite adicionar um filtro. Os filtros permitem limitar os objetos a ser copiados em arquivo por determinados tipos e valores especificados.



Categoria de filtro

Há três categorias de filtro disponíveis: **Tipo de arquivo**, **Nome do arquivo** e **Nome da pasta**. O campo Variável do filtro e Valor do filtro é alterado dependendo da categoria de filtro.

Variável do filtro

Se a categoria do filtro for **Tipo de arquivo**, as opções da Variável do filtro são **é** e **não é**. Se a Categoria do filtro for **Nome do arquivo ou Nome da pasta**, as opções da Variável do filtro são **contém** ou **não contém**.

Você pode especificar vários filtros na mesma solicitação de cópia de arquivo. É possível especificar a mesma categoria de filtro mas uma diferente variável de filtro.

Observação: quando a variável do filtro entra em conflito com a mesma categoria de filtro, a variável **não é** ou **não contém** é sempre uma prioridade mais alta e será aplicada.

Valor do filtro

O valor do filtro permite limitar as informações que são copiadas em arquivo selecionando apenas as informações sobre o parâmetro especificado como arquivos .txt.

O Arcserve UDP oferece suporte ao uso de caracteres curinga para ajudar a selecionar vários objetos à cópia de arquivo com uma única solicitação. Um caractere curinga é um caractere especial que pode ser usado como um substituto para representar um único caractere ou uma sequência de caracteres de texto.

Há suporte para o asterisco dos caracteres curinga e para o ponto de interrogação no campo Valor. Se não souber preencher o valor padrão do arquivo/pasta, basta simplificar os resultados do filtro especificando um caractere curinga.

"*" -- Use o asterisco para substituir zero ou mais caracteres no valor.

"?" - Use o ponto de interrogação para substituir um único caractere no valor.

É possível, por exemplo, digitar *.txt para excluir todos os arquivos com uma extensão .txt se não souber o nome do arquivo específico. Pode-se fornecer o máximo de nome de arquivo que souber, use curingas para preencher os espaços em branco.

Observação: quando você selecionar **Tipo de arquivo** como o tipo de filtro, uma lista suspensa de filtros predefinidos para muitos arquivos usados com frequência é disponibilizada (arquivos do Microsoft Office, arquivos de imagem, arquivos executáveis, arquivos temporários etc.). Após selecionar qualquer um dos filtros pré-definidos, ainda é possível anexar ou modificar os valores correspondentes.

Proteger as pastas do sistema de serem ignoradas

A tarefa de cópia de arquivos ignora as pastas do sistema por padrão quando a tarefa é executada em volumes que contêm pastas do sistema. Para proteger essas pastas e copiá-las no destino, você pode alterar o texto padrão adicionando uma entrada de configuração.

Adicione a seguinte entrada de marca XML no arquivo FileCopyDebugSetting.xml no diretório $UDPHome\Engine\Configuration:

FileName : FileCopyDebugSetting.xml

TagName: SkipWindowsFolders

DefaultValue: 1

Para proteger, altere o valor para: 0

Observação: essa opção está limitada apenas à tarefa de cópia de arquivo. O arquivamento ignora todas as pastas do sistema independentemente do valor de TagValue configurado.

(Opcional) Executar uma cópia de arquivo manual

Em geral, uma cópia de arquivo é executada automaticamente e é controlada pelas configurações da programação de cópia de arquivo. Além da cópia de arquivo programada, uma cópia de arquivo manual fornece a opção de fazer cópia de seus arquivos importantes de acordo com a necessidade.

Ao executar uma cópia de arquivo manual, a tarefa Cópia de arquivo é executada apenas para a primeira sessão de backup, que está qualificada para uma cópia de arquivo. (Sessões de backup qualificam para cópia de arquivo de acordo com a programação de backup e se as sessões estiverem em uma fila. Por exemplo, se especificar a execução de cópia de arquivo para backup a para cada segundo, depois apenas o backup a cada segundo é qualificado para a cópia de arquivo, não todos os backups são qualificados para cópia de arquivo.) Após a conclusão da cópia de arquivo, a primeira sessão é removida, e a segunda sessão na linha torna-se a primeira sessão. Por exemplo, se houver sessões de backup de três (S1, S2, S3 respectivamente) e você executar uma cópia de arquivo manual, a tarefa de cópia de arquivo será executada apenas para S1. A tarefa Cópia de arquivo não será executada para S2 e S3. Quando você executar novamente a tarefa de cópia de arquivo manual, S2 será copiado.

A cópia de arquivo pode ser executada manualmente na exibição de nós e exibição de planos clicando no menu **Ações** ou no menu de contexto.

Siga estas etapas para executar a cópia de arquivo manualmente no modo de exibição de nós:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.

   Os nós são exibidos no painel central.
3. Selecione os nós para uma tarefa de cópia de arquivo. Os nós devem ter um plano de cópia de arquivo atribuído a eles.
4. No painel central, clique em **Ações**, **Copiar arquivo agora**.

   A caixa de diálogo **Executar cópia de arquivo agora** é aberta.
5. Clique em **OK**.

   A tarefa de cópia de arquivo é executada.

   A cópia de arquivo manual é realizada com êxito.

Verificar o plano

Para verificar o plano de cópia de arquivo, confirme se o plano foi criado com êxito. Depois de verificar se o plano está criado com êxito, confirme se a tarefa de backup está executando conforme o programado. Depois que a tarefa de backup for concluída com êxito, a tarefa de cópia de arquivo será executada conforme o programado. É possível verificar o status da tarefa de backup e da tarefa de cópia de arquivo na guia **tarefas**.

Siga estas etapas para verificar os planos:

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.

   Uma lista de todos os nós é exibida no painel central.
3. Verifique se os planos são mapeados com nós.

Siga estas etapas para verificar tarefas de cópia de arquivo:

1. Clique na guia **tarefas**.
2. No painel à esquerda, clique em **Todas as tarefas concluídas**.

   O status de cada tarefa é incluído no painel central.
3. Verifique se a tarefa de backup e a tarefa de cópia de arquivo foi bem-sucedida.

Como criar um plano de arquivo morto

Com o Arcserve Unified Data Protection, você pode arquivar arquivos de origem selecionados em um destino. O destino pode ser uma conta em nuvem ou uma rede compartilhada. O arquivo de origem deve ser do mesmo volume que já foi copiado para backup. Por exemplo, se tiver feito o backup de todo o volume D:\ do nó de origem. Agora você deseja copiar um tipo de arquivo específico (por exemplo, .htm) do volume D:\ do nó de origem. Depois de copiar o arquivo, você deseja excluir esse arquivo do nó de origem. É possível criar um plano de arquivo morto para executar essa operação.

O arquivo morto permite excluir os dados de origem com segurança após eles serem copiados em um local externo ou em um repositório de armazenamento secundário.

As vantagens do arquivo morto são:

- Melhorar a eficiência - ajuda você a acelerar os processos de backup e recuperação ao arquivar dados inalterados e a reduzir a quantidade de dados reais armazenados em backup ou em fita ou disco.
- Atender à conformidade normativa - ajuda-o a preservar importantes documentos, emails e outros dados essenciais, conforme necessário, para cumprir as normas e regulamentações internas e externas.
- Reduzir o custo de armazenamento - ajuda-o a recuperar a capacidade de armazenamento ao migrar dados mais antigos ou pouco acessados dos sistemas principais para locais de armazenamento de arquivos econômicos.
- Manter várias versões de arquivo - ajuda-o a reverter versões anteriores de arquivos de backup (se necessário) ou manter várias versões dos mesmos arquivos em outros destinos.

O que fazer a seguir?

Verificar os pré-requisitos e as considerações

Verifique se concluiu os seguintes pré-requisitos:

- Efetue logon no Console.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Observe as seguintes considerações:

- Execução de tarefa de arquivo morto da sessão de backup mais recente disponível.
- A tarefa de arquivo morto é executada somente uma vez por dia conforme a programação.
- Arquivo morto exclui a tarefa executada como uma nova tarefa para excluir os arquivos de origem.
- A tabela a seguir fornece o limite sobre o comprimento do nome de arquivo para uma tarefa de arquivo morto. Os arquivos que excederem os limites serão ignorados.

Destino	Limite
Compartilhamento de rede	240
Nuvem	245

Criar um plano com uma tarefa de backup

Um plano inclui tipos diferentes de tarefas que você deseja executar. Para criar uma tarefa de arquivamento, é necessário, primeiramente, ter um ponto de recuperação válido. Para obter um ponto de recuperação válido, crie uma tarefa de backup.

Uma tarefa de backup executa um backup dos nós de origem e armazena os dados para o destino especificado. O arquivamento é suportado apenas para backup no Windows com base no agente. O procedimento a seguir explica as etapas para criar a tarefa de backup do Windows com base em agente.

Siga estas etapas:

1. Clique na guia de **recursos** no Console.
2. No painel à esquerda, navegue para **Planos** e clique em **Todos os planos**.

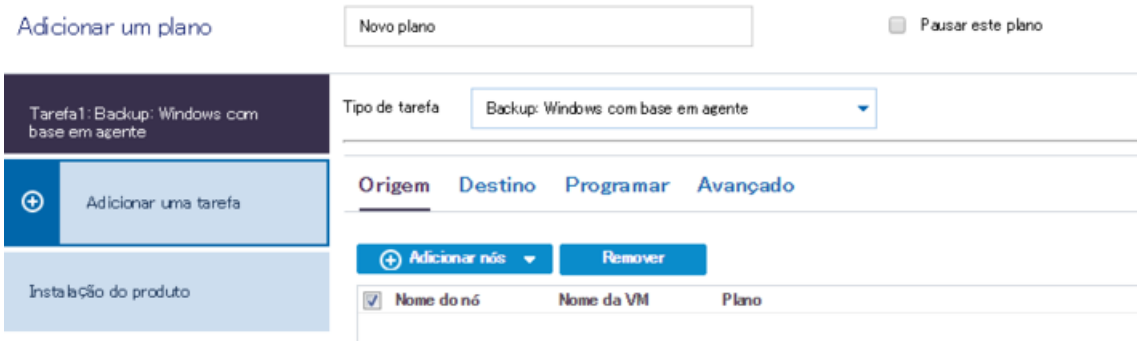
   Se tiver criado os planos anteriores, esses planos serão exibidos no painel central.
3. No painel central, clique em **Adicionar um plano**.

   Adicionar um plano é exibido.
4. Digite o nome do plano.
5. (Opcional) Selecione a caixa de seleção **Pausar este plano**.

   O plano não será executado até que você desmarque a caixa de seleção para retomar o plano.

   Observação: se um plano for pausado, nenhuma tarefa em andamento será pausada, mas todas as tarefas programadas correspondentes associadas a esse plano serão pausadas. No entanto, você pode executar uma tarefa manualmente. Por exemplo, você pode executar manualmente a tarefa de backup e a tarefa de replicação para um nó mesmo que o respectivo plano esteja pausado. Nesse caso, a tarefa seguinte da tarefa sob demanda (manual) não será executada. Por exemplo, há uma tarefa de replicação após uma tarefa de backup sob demanda, a tarefa de replicação não será executada para a tarefa de backup sob demanda. É necessário executar manualmente a tarefa de replicação. Quando você retomar o plano, as tarefas pendentes não são retomadas imediatamente. Depois de retomar o plano, as tarefas pendentes serão executadas no próximo horário programado.
6. Na lista suspensa **Tipo de tarefa**, selecione **Backup, Windows com base em**

agente.



Agora especifique a origem, o destino, a programação e as configurações avançadas.

Especificar a origem

A página Origem permite especificar os nós de origem que deseja proteger. É possível selecionar mais de um nó em um plano. Caso não tenha adicionado nós para o console, você pode adicionar nós ao criar ou modificar um plano da página de origem. Também é possível salvar um plano sem adicionar nenhum nó de origem. O plano é implantado somente após você adicionar nós de origem.

Siga estas etapas:

1. Na guia Origem, clique em **Adicionar**.
2. Selecione uma das seguintes opções:

   Selecionar os nós a serem protegidos no Arcserve UDP

   Abre a caixa de diálogo Selecionar nós para proteger no Arcserve UDP. Selecione os nós na lista exibida. Selecione esta opção se você já tiver adicionado os nós para o console.

   Adicionar nó do Windows

   A caixa de diálogo Adicionar nós a um plano é exibida. Selecione esta opção se você não tiver adicionado os nós e desejar adicionar manualmente os nós para proteger.

   Detectar os nós do Active Directory

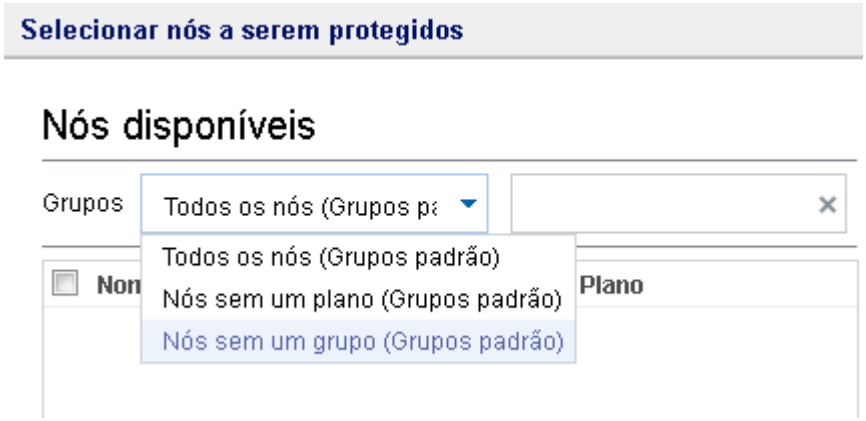
   Abra a caixa de diálogo Adicionar nós ao Console do Arcserve UDP. Selecione essa opção se desejar detectar e adicionar nós do Active Directory.
3. Se você selecionou a opção **Selecionar nós para proteger no Arcserve UDP**, na caixa de diálogo Selecionar nós para proteger, faça o seguinte:
   a. (Opcional) Selecione um filtro na lista suspensa Grupos para filtrar os nós. É possível digitar as palavras-chave para filtrar melhor seus nós.

      Os nós são exibidos na coluna Nós disponíveis.

   b. Selecione os nós na coluna Nós disponíveis e, em seguida, clique na seta simples à direita (>) ou na seta dupla à direita (>>) para mover os nós selecionados ou todos os nós, respectivamente, para a coluna Nós selecionados.

      Os nós são exibidos na coluna Nós selecionados.

   c. Clique em **OK** para fechar a caixa de diálogo.



4. Para escolher Tipo de proteção, selecione uma das seguintes opções:

   Fazer backup de todos os volumes

   Prepara um backup instantâneo de todos os volumes.

   Fazer backup dos volumes selecionados

   Prepara um instantâneo de backup do volume selecionado.

   A origem é especificada.

Especificar o destino

O destino é o local onde você armazena os dados de backup. É necessário, no mínimo, especificar o destino para salvar o plano.

Siga estas etapas:

1. Selecione um dos seguintes **Tipos de destino**:

   Disco local ou uma pasta compartilhada

   Especifica que o destino de backup é um destino local ou uma pasta compartilhada. Se selecionar essa opção, será possível salvar os dados como pontos de recuperação ou conjuntos de recuperação. As opções de pontos de recuperação e de conjuntos de recuperação estão disponíveis na guia **Programar**.

   Servidor de ponto de recuperação do Arcserve UDP

   Especifica que o destino de backup é um servidor do ponto de recuperação. Se selecionar essa opção, os dados serão armazenados como pontos de recuperação. Não é possível armazenar dados como conjuntos de dados de recuperação.

2. Se tiver selecionado **Servidor do ponto de recuperação do Arcserve UDP**, forneça os seguintes detalhes:
   a. Selecione um servidor do ponto de recuperação
   b. Selecione um repositório de dados. A lista exibe todos os repositórios de dados que são criados no servidor do ponto de recuperação especificado.
   c. Forneça uma senha da sessão.
   d. Confirme a senha da sessão.
3. Se tiver selecionado **Disco local ou pasta compartilhada**, forneça os seguintes detalhes:
   a. Forneça o caminho completo do destino local ou de rede. Para o destino de rede, especifique as credenciais com o acesso de gravação.
   b. Selecione o algoritmo de criptografia. Para obter mais informações, consulte Configurações de criptografia.
   c. Como opção, forneça uma senha de criptografia.
   d. Confirme a senha de criptografia.
   e. Selecione um tipo de compactação. para obter mais informações, consulte Tipo de compactação.

Observação: se armazenar os dados em um disco local ou em uma pasta compartilhada, não será possível replicar os dados para outro servidor do ponto de recuperação. A replicação é suportada apenas se armazenar os dados em um servidor do ponto de recuperação.

O destino é especificado.

Especificar a programação

A página Programar permite definir uma programação para o backup e para que as funções Mesclar e Acelerar sejam repetidas em intervalos específicos. Após definir uma programação, as tarefas são executadas automaticamente de acordo com a programação. É possível adicionar várias programações e fornecer configurações de retenção.

Uma Programação de backup se refere a programação regular que é repetida várias vezes ao dia, com base no número de horas ou de minutos selecionado. Além da programação regular, uma programação de backup também fornece opções para adicionar programações diária, semanal e mensal.

Observação: para obter mais informações sobre as configurações de retenção e programação, consulte Entendendo a programação avançada e retenção.

Siga estas etapas:

1. (Opcional) Selecione a opção para gerenciar os pontos de recuperação. Essa opção será visível somente se tiver selecionado o local ou a pasta compartilhada como o destino do backup.

   Reter por pontos de recuperação

   Os dados de backup são armazenadas como pontos de recuperação.

   Reter por conjuntos de recuperação

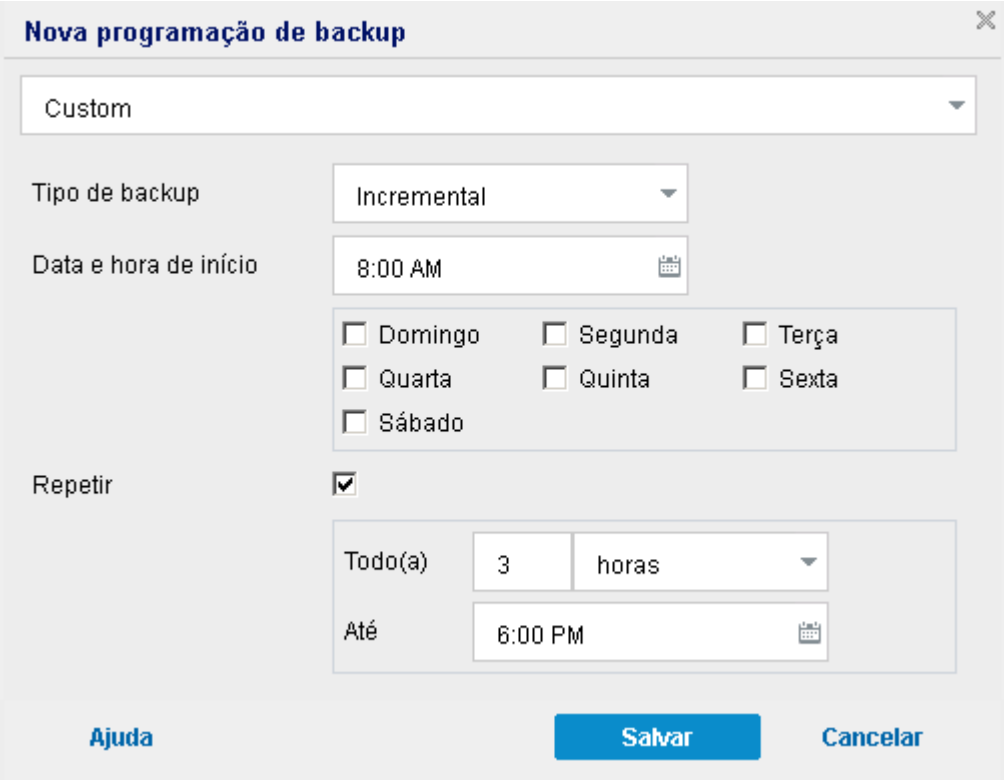
   Os dados de backup são armazenadas como conjuntos de recuperação.

2. Adicionar programações de backup, mesclagem e acelerador.

   Adicionar programação de backup

   a. Clique em **Adicionar** e selecione **Adicionar programação de backups**.

      A caixa de diálogo **Nova programação de backup** é aberta.



b. Selecione uma das seguintes opções:

Personalizado

Especifica a programação de backup que se repete várias vezes por dia.

Diário

Especifica a programação de backup que ocorre uma vez por dia. Por padrão, todos os dias da semana estão selecionados para o backup diário. Se não desejar executar a tarefa de backup em um dia específico, desmarque a caixa de seleção correspondente àquele dia da semana.

Semanal

Especifica a programação de backup que ocorre uma vez por semana.

Mensal

Especifica a programação de backup que ocorre uma vez por mês.

c. Selecione o tipo de backup.

Completo

Especifica a programação de backups para backups completos. Conforme programado, o Arcserve UDP executa um backup completo de todos os blocos usados do computador de origem. Um backup completo em geral, consome tempo, dependendo do tamanho do backup.

Verificar

Especifica a programação de backups para backups de verificação.

A Arcserve UDP verifica se os dados protegidos são válidos e concluídos, executando uma verificação de confiabilidade da imagem de backup armazenada na origem do backup. Se necessário, a imagem será sincronizada novamente. Um backup de verificação examinará o backup mais recente de cada bloco e irá comparar o conteúdo e as informações com a origem. Esta comparação verifica se o backup mais recente dos blocos representa as informações correspondentes na origem. Se a imagem de backup de qualquer bloco não corresponder à origem (possivelmente devido a alterações no sistema desde o último backup), o Arcserve UDP atualizará (fará nova sincronização) o backup do bloco que não corresponder. Também é possível usar um backup de verificação (muito raramente) para obter a garantia de backup completo sem usar o espaço necessário para um backup completo.

Vantagens: produz uma pequena imagem de backup quando comparado ao backup completo, pois somente os blocos alterados (blocos que não coincidem com o último backup) são armazenados em backup.

Desvantagens: o tempo de backup é longo, pois todos os blocos de origem são comparados aos blocos do último backup.

Incremental

Especifica a programação de backups para backups incrementais.

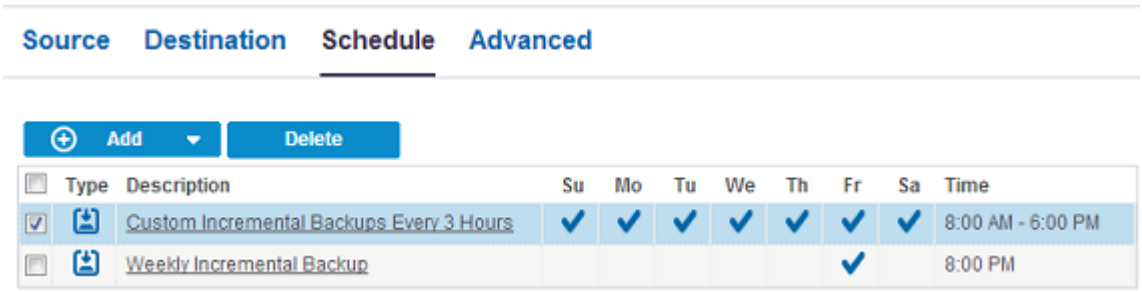
Conforme programado, o Arcserve UDP faz backup incremental apenas dos blocos que foram alterados desde o último backup realizado com êxito. As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a executar um backup.

d. Especifique a hora de início do backup.

e. (Opcional) Marque a caixa de seleção de **Repetição** e especifique a programação a ser repetida.

f. Clique em **Salvar**.

A programação de backup é especificada e exibida na página de **Programação**.



Adicionar Programação de mesclagem

a. Clique em Adicionar e selecione Adicionar programação de mesclagem.

   A caixa de diálogo **Adicionar nova programação de mesclagem** é aberta.

b. Especifique a hora de início para iniciar a tarefa de mesclagem.

c. Especificar **Até** para especificar uma hora de término para a tarefa de mesclagem.

d. Clique em **Salvar**.

   A programação de mesclagem é especificada e exibida na página **Programar**.

Adicionar programação de acelerador

a. Clique em **Adicionar** e selecione **Adicionar programação de acelerador.**

   A caixa de diálogo Adicionar nova programação do acelerador é aberta.

b. Especifique o limite de taxa de transferência em MB por minuto.

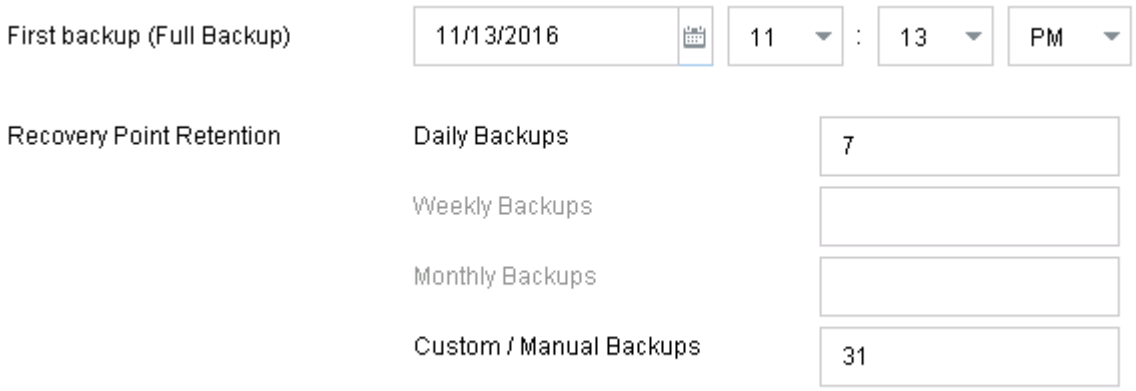
c. Especifique a hora de início para iniciar a tarefa de taxa de transferência de backup.

d. Especifique **Até** para especificar um horário de término para a tarefa de taxa de transferência.

e. Clique em **Salvar**.

   A Programação de acelerador é especificada e exibida na página **Programar**.

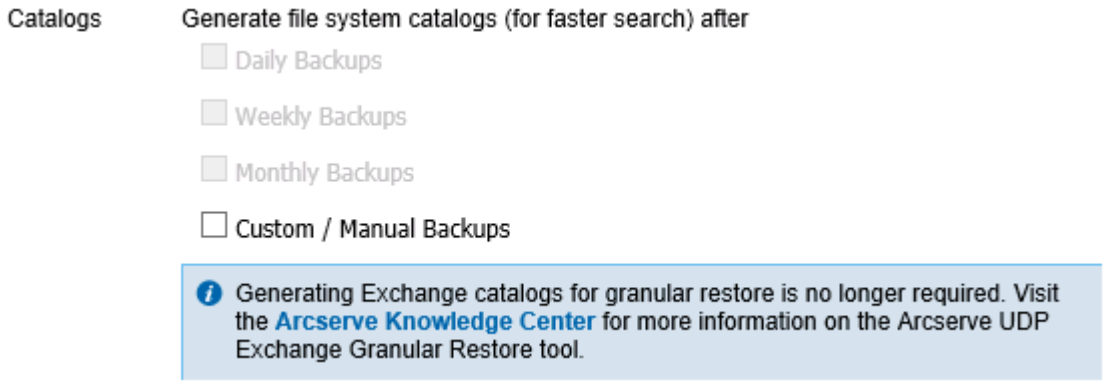
3. Especifique a hora de início do backup programado.



4. Especifique as configurações de retenção de pontos de recuperação para programação diária, semanal e mensal.

   Essas opções serão ativadas se tiver adicionado a programação de backup correspondente. Se você modificar as configurações de retenção desta página, as alterações serão refletidas na caixa de diálogo Programação de backup.

5. Especifique os detalhes de catálogo.



   Os catálogos permitem gerar o catálogo do sistema de arquivos. O catálogo do sistema de arquivos é necessário para agilizar e melhorar a pesquisa. Se marcar as caixas de seleção do catálogo, os catálogos serão ativados de acordo com o tipo de backup que você especificou. Desmarque a caixa de seleção para desativar a geração do catálogo.

   A programação é especificada.

Noções básicas sobre a programação avançada e retenção

A opção de programação permite especificar uma programação personalizada, uma programação diária/semanal/mensal ou ambas. Na programação personalizada, é possível configurar a programação de backups para cada dia da semana ou adicionar até quatro programações de backup em cada dia. É possível escolher um dia específico da semana e criar uma janela para definir quando executar o backup e em que frequência.

Programação	Tarefa com suporte	Comentários
Backup	Tarefa de backup	Definir janelas de tempo para a execução de tarefas de backup.
Limitação de backup	Tarefa de backup	Definir janelas de tempo para controlar a velocidade de backup.
Mesclar	Tarefa de mesclagem	Definir quando executar tarefas de mesclagem.
Programação diária	Tarefa de backup	Definir quando executar tarefas do backup diário.
Programação semanal	Tarefa de backup	Definir quando executar tarefas do backup semanal.
Programação mensal	Tarefa de backup	Definir quando executar tarefas do backup mensal.

Também é possível especificar as configurações de retenção para os pontos de recuperação.

Observação: as configurações de retenção devem ser definidas em cada plano para controlar como os dados dos nós atribuídos a esse plano são retidos no repositório de dados de destino.

As programações para backups diários/semanais/mensais são independentes para a programação personalizada e umas das outras. É possível configurar para executar somente o backup diário, semanal ou mensal, sem configurar a Programação personalizada.

Programação de tarefas de backup

É possível adicionar quatro janelas de tempo por dia na programação do backup. Uma janela de tempo é válida das 00:00 às 23:59. Não é possível especificar uma janela de tempo das 18:00 às 6:00. Nesses casos, você deve especificar manualmente duas janelas de tempo diferentes.

Para cada janela de tempo, a hora de início é inclusiva e a hora de término é exclusiva. Por exemplo, você configurou para executar o backup incremental em intervalos de uma hora entre as 6:00 e as 9:00. O backup será iniciado às 6:00. Isso significa que o backup será executado às 6h00, 7h00 e 8h00, mas NÃO às 9h00.

Observação: se você deseja executar a tarefa de backup várias vezes até o fim do dia, defina a programação para até 0h00. Por exemplo, para executar a tarefa de backup a cada 15 minutos o dia inteiro, defina a programação como das 0h00 às 00h00, a cada 15 minutos.

Programação do acelerador de backup

A programação de aceleração do backup permite controlar a velocidade da taxa de transferência de backup o que, por sua vez, controla o uso de recursos (E/S de disco, CPU, largura de banda de rede) do servidor cujo backup está sendo feito. Isso é útil quando se não quiser afetar o desempenho do servidor durante o horário comercial. É possível adicionar quatro janelas de tempo por dia na sua programação de aceleração do backup. Para cada janela de tempo, é possível especificar um valor, em MB por minuto. Esse valor será usado para controlar a taxa de transferência do backup. Os valores válidos variam entre 1 MB/minutos a 99999 MB/minutos.

Se uma tarefa de backup estende seu tempo especificado, o limite de aceleração será ajustado de acordo com o tempo especificado. Por exemplo, você definiu o limite de aceleração de backup como 500 MB/minuto das 8:00 às 20:00 e 2500 MB/minuto das 20:00 às 22:00. Se uma tarefa de backup iniciar às 19h00 e for executada durante três horas, das 19h00 às 20h00 o limite de aceleração será de 500 MB/minuto e das 20h00 às 22h00, o limite de aceleração será 2500 MB/minuto.

Se não definir nenhuma programação do backup e programação da taxa de transferência do backup, o backup será executado o mais rápido possível.

Mesclar a programação

Permite mesclar pontos de recuperação com base na programação fornecida.

Considere os seguintes pontos para a tarefa de mesclagem:

- A qualquer momento apenas uma tarefa de mesclagem pode ser executada para um nó.
- Se uma tarefa de mesclagem iniciar, ela precisará ser concluída antes que a próxima tarefa de mesclagem seja iniciada. Isso significa que, se um ou mais conjuntos de pontos de recuperação forem mesclados, não será possível adicionar o

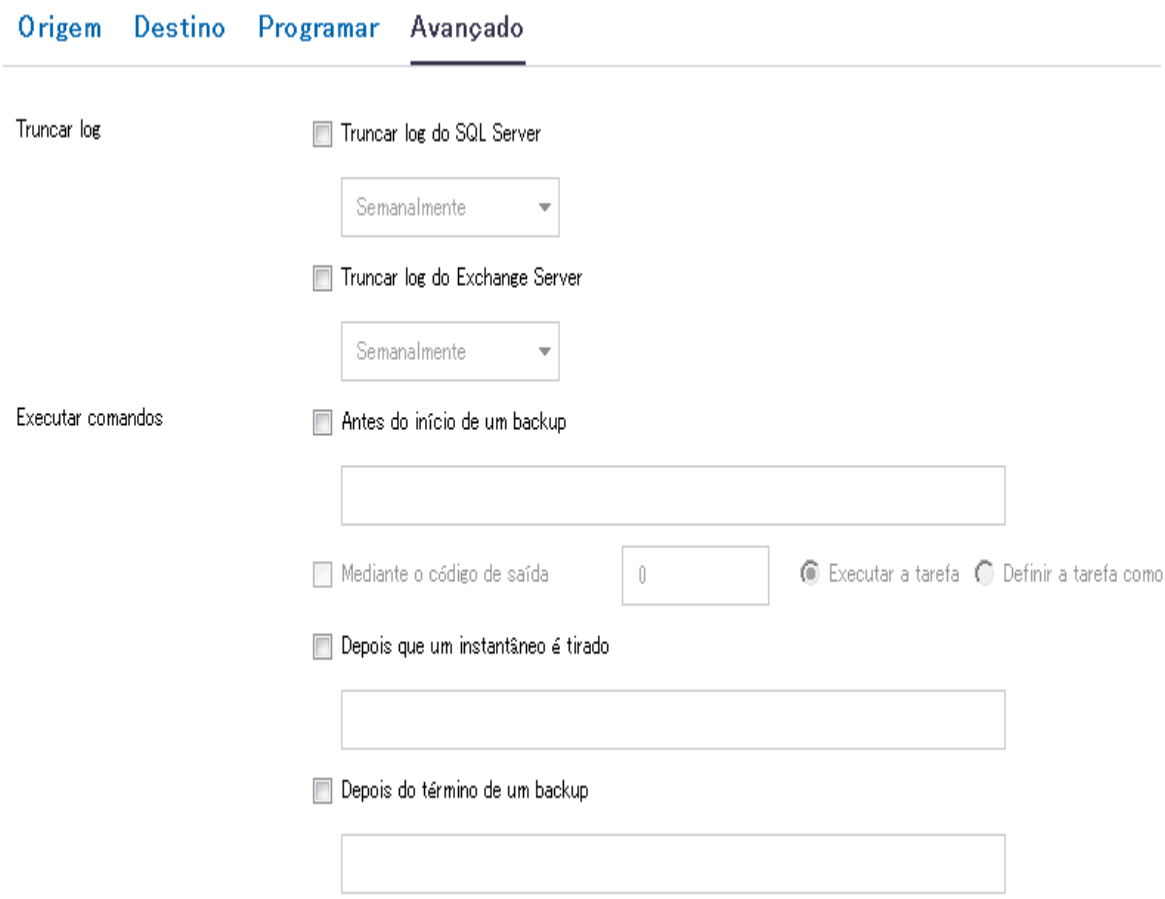
novo ponto de recuperação a este processo de mesclagem, até que o processo de mesclagem do conjunto atual de ponto de recuperação seja concluído.

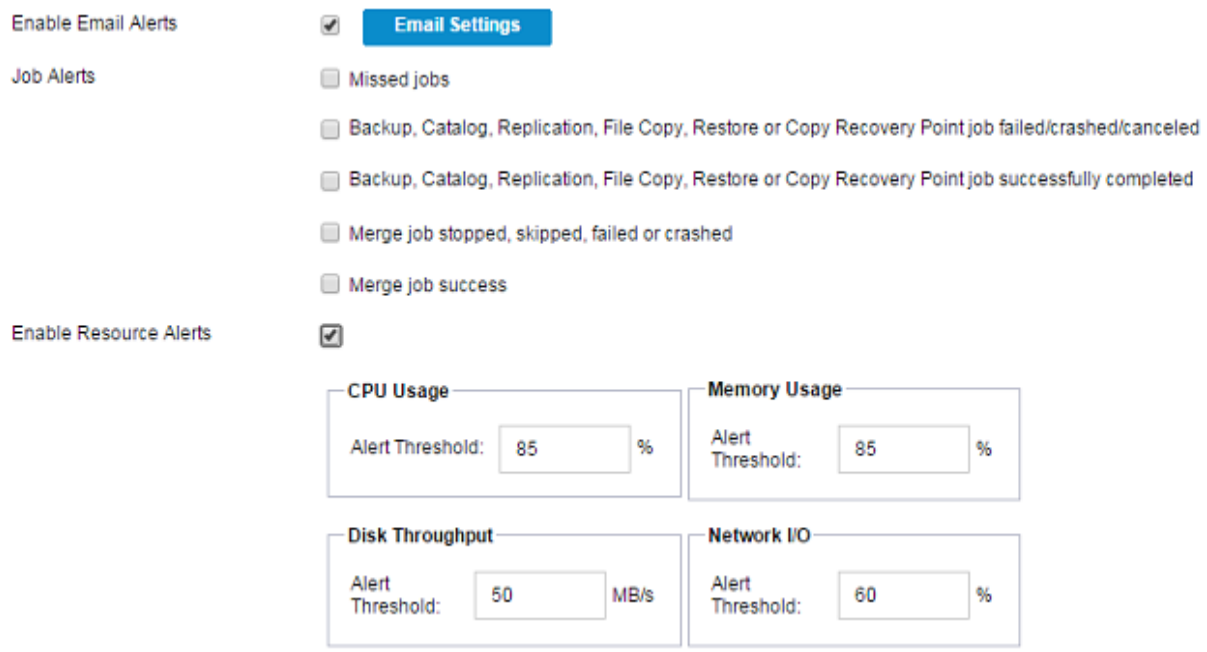
- Se uma tarefa de mesclagem estiver processando mais de um conjunto de pontos de recuperação (por exemplo, conjunto [1~4], conjunto [5~11] e conjunto [12~14]; são três conjuntos) o servidor de ponto de recuperação processará esses conjuntos, um por um.
- Se uma tarefa de mesclagem é retomada após um intervalo, a tarefa detectará em que ponto ela foi pausada e continuará a mesclagem a partir do ponto de pausa.

Especificar as configurações avançadas

A guia **Avançado** permite especificar algumas configurações avançadas para a tarefa de backup. As configurações avançadas incluem fornecer configurações de log de truncamento, a localização de quaisquer scripts e as configurações de email.

A imagem a seguir mostra a guia Avançado:





Siga estas etapas:

1. Especifique os seguintes detalhes.

Truncar log

Permite especificar a programação para truncar logs para o SQL Server e o Exchange Server. É possível especificar a programação como **Diária**, **Semanal** ou **Mensal**.

Nome de usuário

Permite especificar o usuário que possui autorização para executar um script.

Senha

Permite especificar a senha do usuário que está autorizado a executar o script.

Executar um comando antes do início do backup

Permite a execução de um script antes de iniciar a tarefa de backup. Especifique o caminho onde o script está armazenado. Clique em **No código de saída** e especifique o código de saída para **Executar tarefa** ou **Tarefa com falha**. **Executar a tarefa** indica que a tarefa de backup continuará quando o script retornar o código de saída. **Tarefa com falha** indica que a tarefa de backup será interrompida quando o script retornar o código de saída.

Executar um comando após a criação de um instantâneo

Permite executar um script depois que o backup do instantâneo for gerado. Especifique o caminho onde o script está armazenado.

Executar um comando após a conclusão do backup

Permite executar um script depois que a tarefa de backup foi concluída. Especifique o caminho onde o script está armazenado.

Ativar alertas por email

Permite ativar alertas por email. É possível especificar configurações de email e os tipos de alertas que você deseja receber por email. Ao selecionar esta opção, as seguintes opções serão ativadas para a seleção.

Configurações de email

Permite configurar as definições de email. Clique em **Configurações de email** e configure o servidor de email e os detalhes do servidor proxy.

Alertas de tarefa

Permite que você selecione os tipos de emails da tarefa que deseja receber.

Ativar os alertas de recurso

Permite que você especifique um limite de uso da CPU, o uso da memória, a taxa de transferência de disco, E/S de rede. Você pode fornecer o valor em porcentagem. Você receberá um email quando o valor exceder o Limite de alerta.

2. Clique em **Salvar**.

Observação: quando você seleciona um nó como origem de backup ou proxy de backup, o Arcserve UDP verifica se o agente está instalado no nó e se é a versão mais recente. Em seguida, o Arcserve UDP exibe uma caixa de diálogo de verificação que lista todos os nós que possuem uma versão antiga do agente ou que não tem o agente instalado. Para instalar/atualizar o agente nesses nós, selecione o método de instalação e clique em Salvar.

As alterações são salvas e uma marca de seleção verde é exibida ao lado do nome da tarefa. A página do plano é fechada.

Observação: se precisar adicionar outra tarefa, deverá selecionar o plano na guia **Recursos** e modificar o plano. Para modificar o plano, clique no plano do painel central. O plano é exibido e será possível modificá-lo.

O plano de backup é criado e implantado automaticamente para o nó de origem. O backup é executado de acordo com a programação que você configurou na guia **Programar.** Também é possível fazer backup manual quando desejado.

Adicionar uma tarefa de arquivo morto ao plano

A tarefa de arquivo morto permite arquivar arquivos individuais no destino especificado. Os arquivos originais são excluídos da origem, depois que você copiar os arquivos no destino especificado e disponibiliza-se mais espaço livre em sua origem. A tarefa de arquivamento de arquivo não depende de uma tarefa de geração de catálogo.

Observação: se uma tarefa de backup estiver em andamento e você pausar o plano, a tarefa de backup será encerrada e a tarefa de arquivo morto não será iniciada. Ao retomar o plano novamente, a tarefa de arquivamento de arquivo não é retomada automaticamente. É necessário executar manualmente outra tarefa de backup para acionar a tarefa de arquivamento de arquivo.

Para arquivos copiados usando-se o arquivamento de arquivo, o Arcserve UDP deixa um arquivo stub com a extensão "UDP.txt". Para obter mais informações sobre como atualizar o arquivo stub, consulte Atualizar arquivos stub.

Siga estas etapas:

1. Clique em **Adicionar uma tarefa** no painel esquerdo.

   Uma nova tarefa será adicionada ao painel esquerdo.

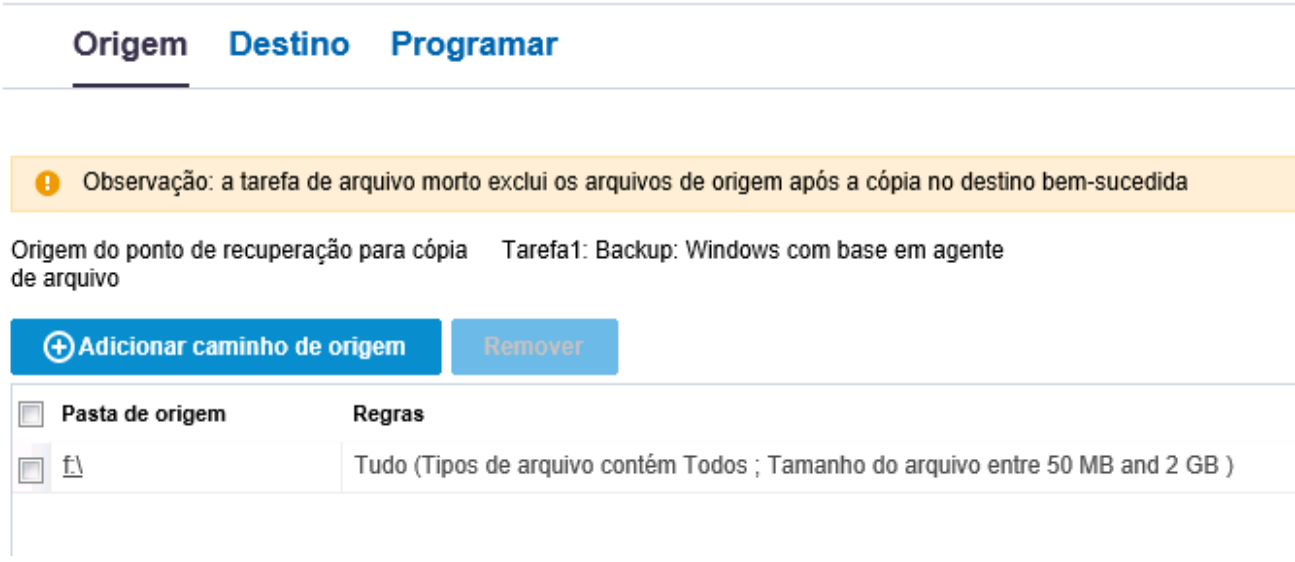
2. No menu suspenso **Tipo de tarefa**, selecione **Arquivo morto**.

   A tarefa Arquivo morto é adicionada.

3. Clique na guia **Origem** e especifique os detalhes.

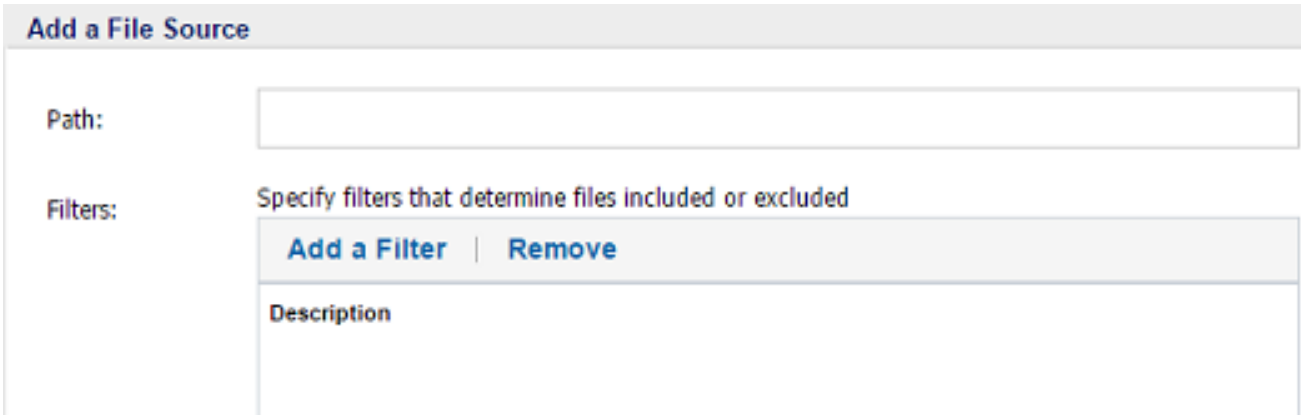
   Local do ponto de recuperação

   Especifica o local dos pontos de recuperação que serão arquivados. Este campo é pré-selecionado.

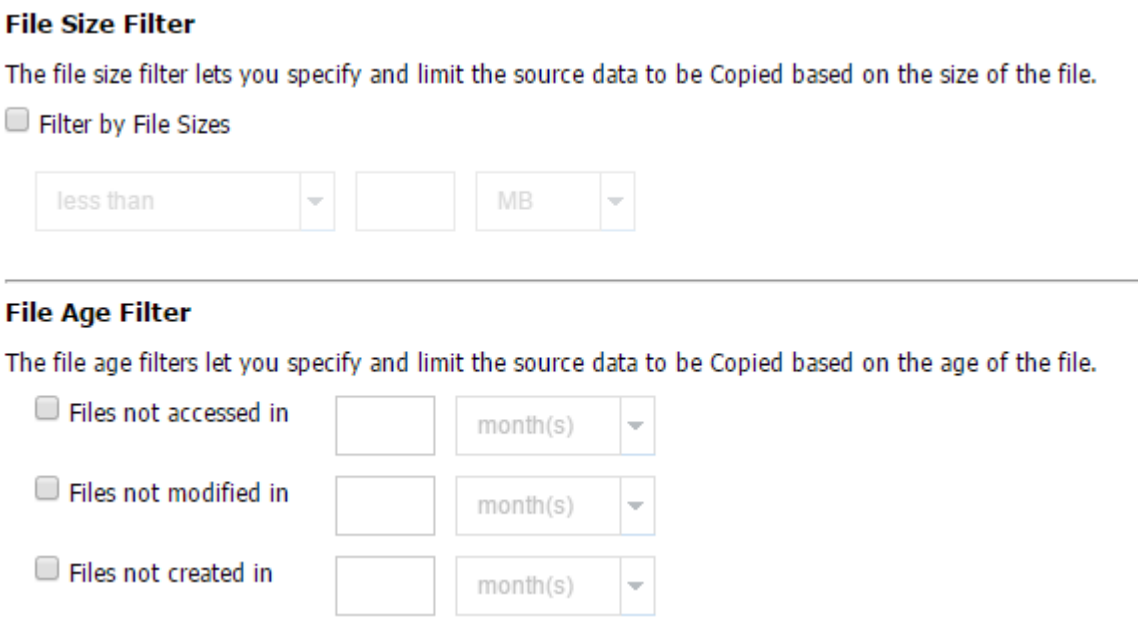


4. Clique em **Adicionar uma origem**.

   A caixa de diálogo **Adicionar uma origem de arquivo** é aberta.

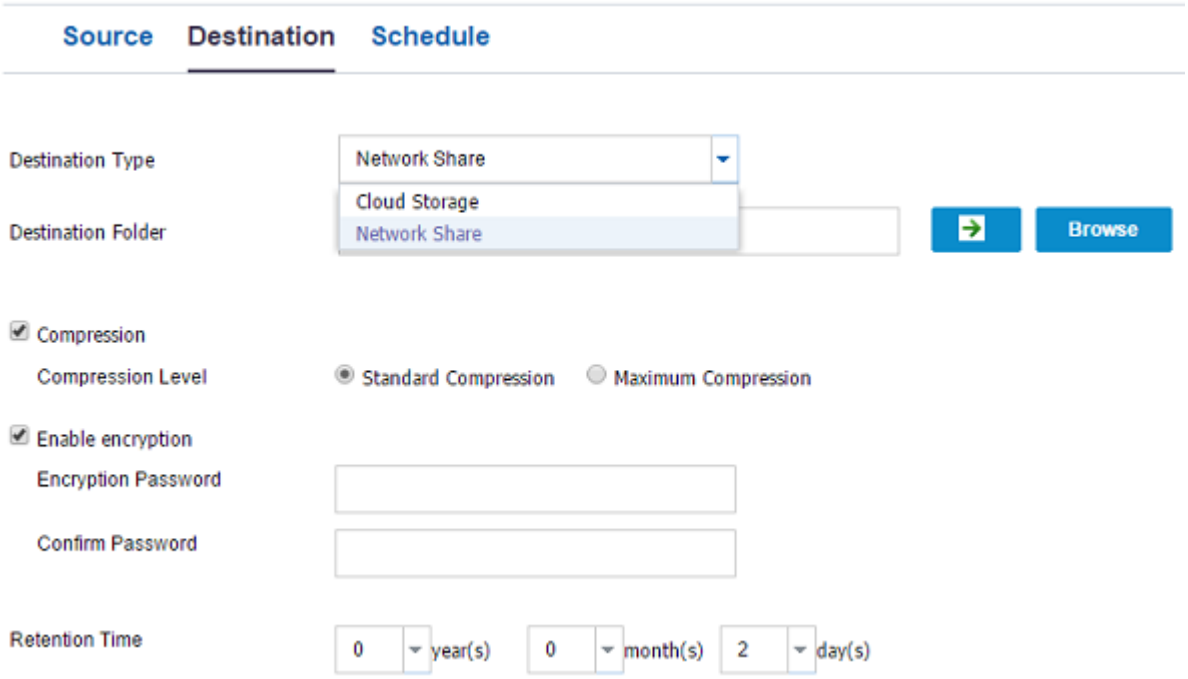


5. Especifique o caminho de arquivo do caminho de origem que você deseja copiar.
6. Especifique o **Filtro de tamanho de arquivo** e o **Filtro de tempo de vida de arquivo**.



7. Clique em **Adicionar um filtro**.
8. Selecione o filtro na lista e clique em **Aplicar**.
9. Clique em **OK**.

   A caixa de diálogo **Adicionar uma origem de arquivo** fecha.
10. Clique na guia **Destinos** e especifique os detalhes do destino.



Tipo de destino

Especifica que o tipo de destino é um compartilhamento de rede ou um armazenamento na nuvem. Para a opção de destino, se a conexão com o destino especificado for perdida ou interrompida, o Arcserve UDP fará várias tentativas para continuar a tarefa de arquivamento de arquivo. Se essas novas tentativas não forem bem-sucedidas, uma tarefa de constituição será executada a partir do ponto em que a falha ocorreu. Além disso, o log de atividades será atualizado com uma mensagem de erro correspondente e uma notificação por email será enviada (se configurada).

Compartilhamento de rede

Especifica que o destino é uma pasta compartilhada. Quando selecionada, essa opção permite especificar o caminho completo do local para o qual deseja mover os arquivos/as pastas de origem.

Pasta de destino

Especifica o destino onde os itens arquivados serão armazenados. O destino pode ser um volume ou uma pasta local ou um compartilhamento de arquivo acessível por qualquer UNC (Uniform naming convention - Convenção de nomenclatura uniforme). Esse campo é disponibilizado quando você seleciona Compartilhamento de rede ou Volume no nó protegido como o tipo de destino. Também é possível procurar a pasta de destino.

Armazenamento na nuvem

Especifica que os arquivos copiados serão armazenados em um ambiente na nuvem. O Arcserve UDP atualmente oferece suporte à cópia de arquivos para vários fornecedores de nuvem, como Amazon S3 (Simple Storage Service), compatível com Amazon S3, Windows Azure, compatível com Windows Azure, Eucalyptus-Walrus e FUJITSU Hybrid IT Service FJcloud-O. Esses fornecedores de nuvem são serviços da web disponíveis publicamente que permitem armazenar e recuperar qualquer quantidade de dados a qualquer momento de qualquer lugar na web em um ambiente seguro e protegido.

Observação: para eliminar um possível erro de precisão do relógio ao tentar se conectar à nuvem, verifique se o computador tem o fuso horário adequado definido, e se o relógio está em sincronia com o horário mundial. É necessário sempre verificar o horário do computador referente ao horário GMT. Se a hora do computador não estiver sincronizada com o tempo global adequado (de 5 a 10 minutos), o a conexão com a nuvem pode não funcionar. Se necessário, redefina a hora correta do computador e execute novamente a tarefa cópia de arquivo.

Dispositivo de armazenamento

Selecione o tipo de dispositivo na lista suspensa.

Armazenamento na nuvem

Selecione o caminho do armazenamento na nuvem na lista suspensa. A lista suspensa será disponibilizada se você especificar os detalhes do armazenamento na nuvem. Se estiver especificando a conta de armazenamento na nuvem pela primeira vez, clique em Adicionar para adicionar a conta de nuvem. Quando você seleciona Armazenamento na nuvem, na próxima vez, a conta será exibida na lista suspensa Armazenamento na nuvem.

Observação: para obter mais informações sobre a adição de uma conta de nuvem, consulte Adicionar uma conta de nuvem.

Compactação

Especifica o tipo de compactação usada para tarefas de arquivo morto.

A compactação é executada para reduzir o espaço de armazenamento no destino do Arquivo morto, mas também tem um impacto inverso na velocidade de seu arquivo morto devido ao aumento no uso da CPU.

Observação: para tarefas de arquivo morto compactado, o log de atividades exibe apenas o tamanho descompacto.

As opções disponíveis são:

Compactação padrão

Alguma compactação será realizada. Esta opção proporciona um bom equilíbrio entre o uso da CPU e o requisito do espaço de armazenamento. Essa é a configuração padrão.

Compactação máxima

A compactação máxima será realizada. Essa opção exige mais uso da CPU (menos velocidade), mas também requer menos espaço de armazenamento para a cópia de arquivo.

Ativar criptografia

Especifica o uso de criptografia no arquivo morto.

A criptografia de dados é a conversão de dados em uma forma ininteligível sem um mecanismo decodificador. A proteção de dados do Arcserve UDP usa algoritmos de criptografia seguros AES-256 (padrão de criptografia avançada) para atingir o máximo de segurança e privacidade dos dados especificados. É necessário fornecer (e confirmar) uma senha criptografada quando uma criptografia for selecionada.

Tempo de retenção

Especifica o tempo (anos, meses, semanas) que os dados armazenados devem ser mantidos no local de destino. No final do período de retenção especificado, os dados armazenados serão removidos do destino.

Os cálculos do tempo de retenção tem como base um mês de 30 dias e um ano de 365 dias. Por exemplo: se especificar um período de retenção de 2 anos, 2 meses e 5 dias, o total de tempo de retenção dos dados copiados em arquivo é de 795 dias (365 + 365 + 30 + 30 + 5).

Importante: No final do tempo de retenção especificado quando os dados forem removidos do destino, todos esses dados movidos não serão mais armazenados ou salvos.

Observação: o processo de limpeza do período de retenção só é acionado quando a opção Programação da cópia de arquivo estiver ativada.

Versão de arquivo anterior a

Esta configuração se aplica apenas a dados copiados que foram retidos (não os que foram movidos).

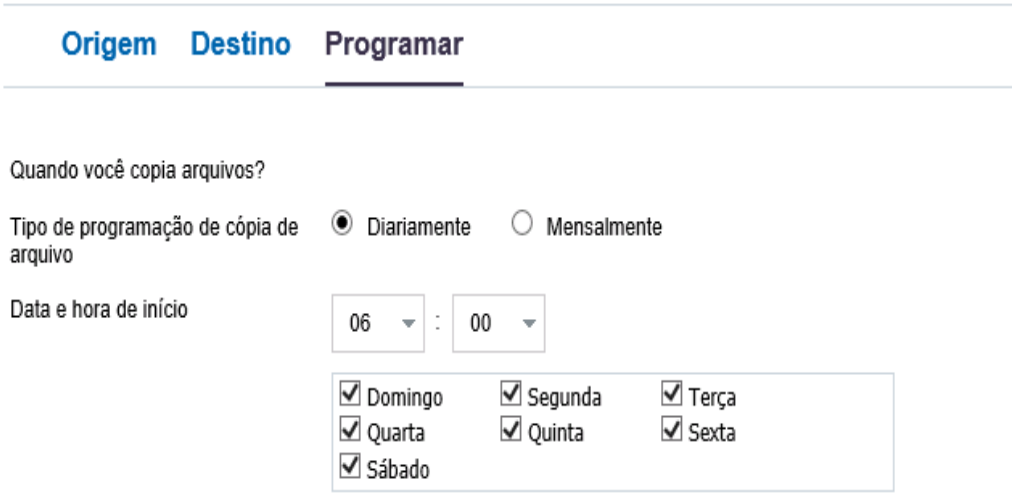
Especifica o número de cópias mantidas e armazenadas no local de destino (nuvem ou disco). Quando este número for excedido, a primeira versão (mais antiga) será descartada. O ciclo de descartar a versão armazenada mais antiga será repetido à medida que versões mais novas forem adi-

cionadas ao destino, permitindo que você sempre mantenha a quantidade especificada de versões armazenadas.

Por exemplo, se a contagem de retenção de versões de arquivo especificada for definida como 5 e se você fizer cinco cópias de arquivo nas horas t1, t2, t3, t4 e t5, estas se tornarão as cinco versões de cópia de arquivo retidas e disponíveis para recuperação. Depois que a sexta cópia de arquivo foi executada (a versão nova foi salva), o Arcserve UDP remove a cópia t1 e as cinco versões disponíveis para recuperação agora são t2, t3, t4, t5 e t6.

Por padrão, a quantidade de cópias mantida no local de destino antes de descartar é 15.

11. Clique na guia **Programar** e especifique a hora da execução da tarefa de arquivo morto.



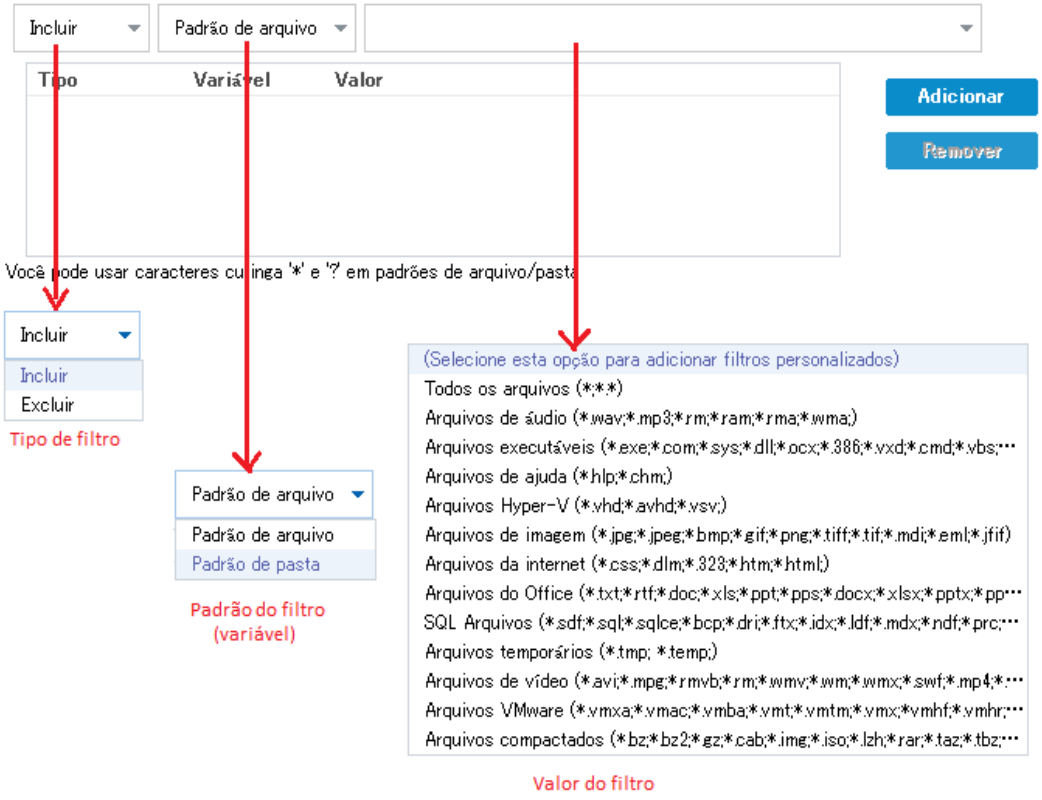
12. Clique em **Salvar**.

As alterações são salvas e a tarefa de arquivo morto é automaticamente implantada no nó.

Adicionar filtros do arquivo morto

Adicionar um filtro

Permite adicionar um filtro. Os filtros permitem limitar os objetos a ser copiados em arquivo por determinados tipos e valores especificados.



Tipo de filtro

Há dois tipos de filtros: Incluir e Excluir.

Um filtro Incluir copia somente os objetos da origem da cópia de arquivo que correspondem ao valor especificado.

Um filtro Excluir copia todos os objetos da origem da cópia de arquivo, exceto os que corresponderem ao valor especificado.

É possível especificar vários filtros na mesma solicitação de cópia de arquivo separando cada valor de filtro com uma vírgula.

- Se especificar vários filtros Incluir, os dados serão incluídos na cópia de arquivo se qualquer um desses filtros for correspondente.
- Se especificar vários filtros Excluir, os dados serão excluídos da cópia de arquivo se qualquer um desses filtros for correspondente.

- É possível misturar os filtros Incluir e Excluir na mesma solicitação de cópia de arquivo.

  Observação: quando os parâmetros especificados dos filtros Incluir e Excluir estiverem em conflito, o filtro Excluir terá sempre uma prioridade mais alta e será aplicado. Um filtro Incluir nunca pode arquivar um objeto que também foi excluído.

Variável de filtro (padrão)

Há dois tipos de filtros de padrão variável: Padrão de arquivo e Padrão de pasta.

É possível usar um filtro Padrão de arquivo ou Padrão de pasta para incluir ou excluir alguns objetos da cópia de arquivo.

Valor do filtro

O valor do filtro permite limitar as informações que são copiadas em arquivo selecionando apenas as informações sobre o parâmetro especificado como arquivos .txt.

O Arcserve UDP oferece suporte ao uso de caracteres curinga para ajudar a selecionar vários objetos à cópia de arquivo com uma única solicitação. Um caractere curinga é um caractere especial que pode ser usado como um substituto para representar um único caractere ou uma sequência de caracteres de texto.

Há suporte para o asterisco dos caracteres curinga e para o ponto de interrogação no campo Valor. Se não souber preencher o valor padrão do arquivo/pasta, basta simplificar os resultados do filtro especificando um caractere curinga.

"*" -- Use o asterisco para substituir zero ou mais caracteres no valor.

"?" - Use o ponto de interrogação para substituir um único caractere no valor.

É possível, por exemplo, digitar *.txt para excluir todos os arquivos com uma extensão .txt se não souber o nome do arquivo específico. Pode-se fornecer o máximo de nome de arquivo que souber, use curingas para preencher os espaços em branco.

Observação: quando você seleciona Padrão de arquivo como o tipo de filtro, uma lista suspensa de filtros predefinidos para muitos arquivos usados com frequência é disponibilizada (arquivos do Microsoft Office, arquivos de imagem, arquivos executáveis, arquivos temporários etc.). Após selecionar qual-

quer um dos filtros pré-definidos, ainda é possível anexar ou modificar os valores correspondentes.

Filtro de tamanhos de arquivos

Os filtros Tamanho do arquivo permitem limitar que os objetos de origem sejam copiados em arquivo com base no tamanho do arquivo. Ao ativar este filtro, os parâmetros especificados se tornarão o filtro para os objetos que serão ou não incluídos na cópia de arquivo. É possível selecionar o intervalo (igual ou maior que, igual ou menor que, ou entre) e digitar um valor para o tamanho.

Por exemplo, caso especifique um valor igual ou maior do que 10 MB, o Arcserve UDP copia em arquivo apenas objetos que atendem a este critério. Todos os outros objetos que não atenderem ao critério de tamanho de arquivo não serão copiados em arquivo.

Filtro de tempo de vida do arquivo

Os filtros Tempo de vida do arquivo permitem incluir automaticamente objetos de origem a serem copiados em arquivo com base em determinadas datas do arquivo. É possível selecionar um parâmetro (arquivos não acessados em, não modificados em e/ou não criados em) e digitar um valor para o número de dias, meses ou anos do filtro de tempo de vida de arquivo. É possível selecionar vários filtros de tempo de vida do arquivo para serem copiados em arquivo automaticamente.

Por exemplo, se você especificar Arquivos não modificados em 180 dias, o Arcserve UDP copiará automaticamente todos os arquivos que atenderem a esse critério (não foram modificados durante os últimos 180 dias).

Importante: Se especificar os filtros Tamanho do arquivo e Tempo de vida do arquivo (ou vários filtros Tempo de vida do arquivo), somente os arquivos que atenderem a todos os parâmetros de filtro especificado serão copiados em arquivo. Os arquivos que não atenderem a nenhum destes parâmetros especificados não serão copiados.

Atualizar arquivos stub

Para arquivos copiados usando a opção Arquivamento de arquivo, o Arcserve UDP deixa um arquivo stub com a extensão "UDP.txt". O arquivo stub contém informações sobre o destino onde os arquivos foram movidos e algumas informações adicionais. Se um arquivo for restaurado para o local original e for movido novamente para o destino especificado, o arquivo stub será atualizado com as informações sobre a movimentação. Se necessário, esses arquivos stub de cópia de arquivo podem ser desativados ou excluídos com segurança sem nenhum impacto negativo. (Os arquivos stub existentes não serão excluídos quando a chave de registro for alterada para não criar mais arquivos stub).

As informações a seguir estão presentes no arquivo stub por padrão:

Entre em contato com o departamento de TI para restaurar esse arquivo.

É possível alterar o texto padrão adicionando uma entrada de configuração. Adicione a seguinte entrada de marca XML no arquivo FileCopyDebugSetting.xml no diretório $UDPHome\Engine\Configuration:

<ArchiveStubFileText> O novo texto pode ser adicionado aqui para ser exibido no arquivo stub

</ArchiveStubFileText>

Exemplo: o arquivo FileCopyDebugSetting.xml deve parecer com o seguinte

```
<?xml version="1.0" encoding="UTF-8"?>
<HKLM>
<AFArchiveDLL>
<ArchiveStubFileText> O novo texto pode ser adicionado aqui para ser exibido no arquivo stub </ArchiveStubFileText>.
</AFArchiveDLL>
</HKLM>
```

Se o arquivo FileCopyDebugSetting.xml não estiver presente no diretório $UDPHome\Engine\Configuration, crie o arquivo XML.

Se você quiser desativar a criação do arquivo stub, adicione a seguinte entrada de marca XML no arquivo FileCopyDebugSetting.xml no diretório $UDPHome\Engine\Configuration:

<CreateStubFile>0</CreateStubFile>

Exemplo: o arquivo FileCopyDebugSetting.xml deve parecer com o seguinte

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<HKLM>

<AFArchiveDLL>
<CreateStubFile>0</CreateStubFile>
</AFArchiveDLL>
</HKLM>
```

Observação: se desativar ou excluir os arquivos stub de cópia de arquivo, não será mais possível rastrear o status e o local dos arquivos movidos.

(Opcional) Executar uma cópia de arquivo manual

Em geral, um arquivo morto é executado automaticamente e é controlado pelas configurações da programação de arquivo morto. Além do arquivamento programado, um arquivamento manual fornece a opção de copiar seus arquivos importantes de acordo com a necessidade. Quando você executa um arquivo morto manual, a tarefa arquiva todas as sessões na origem do arquivo morto.

Arquivo morto pode ser executado manualmente da exibição de nós e exibição de planos clicando no menu **Ações** ou no menu de contexto.

Siga estas etapas para executar manualmente o Arquivo morto no modo de exibição de nós:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.

   Os nós são exibidos no painel central.
3. Selecione os nós de uma tarefa de arquivo morto. Os nós devem ter um plano de arquivo morto atribuído a eles.
4. No painel central, clique em **Ações**, **Arquivamento de arquivo agora** .

   A caixa de diálogo **Executar arquivamento de arquivo agora** é aberta.
5. Clique em **OK**.

   A tarefa de arquivo morto é executada.

   O arquivamento manual é realizado com êxito.

Verificar o plano

Para verificar o plano de cópia de arquivo, confirme se o plano foi criado com êxito. Depois de verificar se o plano está criado com êxito, confirme se a tarefa de backup está executando conforme o programado. Depois que a tarefa de backup for concluída com êxito, a tarefa de cópia de arquivo será executada conforme o programado. É possível verificar o status da tarefa de backup e da tarefa de cópia de arquivo na guia **tarefas**.

Siga estas etapas para verificar os planos:

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.

   Uma lista de todos os nós é exibida no painel central.
3. Verifique se os planos são mapeados com nós.

Siga estas etapas para verificar tarefas de cópia de arquivo:

1. Clique na guia **tarefas**.
2. No painel à esquerda, clique em **Todas as tarefas concluídas**.

   O status de cada tarefa é incluído no painel central.
3. Verifique se a tarefa de backup e a tarefa de cópia de arquivo foi bem-sucedida.

Como criar um plano de cópia em fita

O Arcserve UDP integra-se ao Backup do Arcserve para copiar dados de backup em um destino de mídia de fita. É possível criar um plano para fazer backup de dados de origem e copiar os dados de backup na fita. Você pode criar e gerenciar o plano a partir do Console.

As vantagens dos pontos de recuperação de arquivamento em uma mídia de fita são:

- Atender à conformidade normativa - ajuda a preservar documentos e emails importantes e outros dados essenciais, conforme necessário, para cumprir com regras internas e regulamentos externos.
- Reduzir o custo de armazenamento - ajuda-o a recuperar a capacidade de armazenamento ao migrar dados mais antigos ou pouco acessados dos sistemas principais para locais de armazenamento de arquivos econômicos.
- Manter várias versões de arquivo - ajuda-o a reverter versões anteriores de arquivos de backup (se necessário) ou manter várias versões dos mesmos arquivos em outros destinos.

Cenários com suporte

- Se o destino da tarefa 1 for o **Servidor do Ponto de Recuperação do Arcserve UDP**, instale o agente cliente no nó RPS.
- Para o plano com base em agente com o destino como **Compartilhamento local/remoto**, instale o agente cliente em todos os nós do agente do Arcserve UDP.
- Para o plano sem agente com base em host, instale o agente cliente no nó do proxy do Arcserve UDP.

O que fazer a seguir?

- Verificar os pré-requisitos
- Crie um plano com uma tarefa de backup
- Adicionar um plano de copia em fita
- Verificar o plano

Verificar os pré-requisitos e as considerações

Os seguintes pré-requisitos devem ser concluídos:

- Efetue logon no Console.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.
- Adicionado o servidor de backup do Arcserve ao Console. Para obter mais informações sobre como adicionar o servidor de backup do Arcserve no console, consulte o tópico Adicionar servidores de backup do Arcserve.
- O servidor de ponto de recuperação especificado na tarefa principal de um plano deve ter o agente do servidor de backup do Arcserve instalado.

Crie um plano com uma tarefa de backup

Um plano inclui tipos diferentes de tarefas que você deseja executar. Geralmente um plano inclui uma lista de tarefas principais seguida de uma tarefa secundária. Em geral, uma tarefa principal é uma tarefa de backup ou replicação a partir de uma tarefa remota do Console. A função de uma tarefa de backup é criar um backup de nós de origem que você deseja proteger. É possível fazer backup de dados do Windows, e de máquinas virtuais e físicas Linux. Em seguida, é possível salvar os dados de backup em outro local, como precaução adicional.

Para obter mais informações sobre:

- Como fazer backup de um nó do Windows, consulte Como criar um plano de backup do Windows.
- Como fazer backup de máquinas virtuais, consulte Como criar um plano de backup da máquina virtual com base em host.
- Como fazer backup de nós do Linux, consulte Como criar um plano de backup do Linux.
- Replicação de dados de backup para um destino remoto, consulte Como replicar dados entre os dados armazenamentos gerenciados por diferentes Consoles do UDP.

Adicionar uma tarefa de Cópia em fita ao plano

A tarefa de cópia em fita permite copiar os dados em uma fita. A mídia de fita é identificada no servidor de backup do Arcserve que você adicionou.

Siga estas etapas:

1. Clique em **Adicionar uma tarefa** no painel esquerdo.

   Uma nova tarefa será adicionada ao painel esquerdo.

2. No menu suspenso, selecione **Tipo de tarefa,** selecione **Copiar em fita**.

   A tarefa Copiar em fita é adicionada.

   Observação: os backups personalizados não acionam as tarefas de cópia em fita.

   Agora especifique os detalhes de Origem, Destino, Programação e Avançado.

Especificar a origem

Normalmente, o arquivo de origem é um destino de backup ou um destino de replicação.

Siga estas etapas:

1. Especifique os seguintes detalhes na página **Origem**.

   Origem da cópia em fita

   Especifica o local dos pontos de recuperação que serão arquivados. Se houver apenas uma origem, esse campo será pré-selecionado. Por exemplo, se o plano tiver apenas uma tarefa de backup e, em seguida, você adicionar a tarefa de Cópia em fita, o destino da tarefa de backup torna-se a origem da cópia em fita. Se você tiver várias origens para cópia em fita, é possível adicionar uma cópia em fita para cada uma dessas origens. Por exemplo, se a primeira tarefa for uma tarefa de backup, a segunda e a terceira tarefas são tarefas de replicação, assim é possível adicionar três tarefas de cópia em fita para o plano.

   Tipos de pontos de recuperação

   Especifique os tipos de pontos de recuperação. As opções disponíveis são backups diários, backups semanais e backups mensais.

2. Clique na guia **Destino**.

   A página **Destino** é exibida.

   Você forneceu com êxito os detalhes de origem.

Especificar o destino

O destino é um grupo de mídias de fita em seu Servidor do Arcserve Backup. É necessário adicionar o Servidor do Arcserve Backup ao console antes de criar essa tarefa.

Siga estas etapas:

1. Especifique os detalhes a seguir para o destino do backup.

   Servidor do Arcserve Backup

   Selecione o servidor do Arcserve Backup na lista suspensa.

   Grupo de mídias

   Selecione o grupo de mídias na lista suspensa. O grupo de mídias depende do Servidor do Arcserve Backup. Por padrão, o dispositivo com base em disco do <ASBU> não é listado no grupo de mídias. Além disso, o grupo RAID de fita não é listado no grupo de mídias.

   Para migrar pontos de recuperação do Arcserve UDP para um dispositivo com base em disco do Arcserve Backup, os pontos de recuperação incrementais devem ser convertidos em pontos de recuperação completos. É a maneira recomendada para migrar o ponto de recuperação do Arcserve UDP para um dispositivo com base em disco executar uma replicação de repositório de dados do Arcserve UDP para outro repositório de dados.

   Somente os grupos de fitas podem ser configurados como o destino para uma tarefa Copiar em fita. É possível modificar uma chave de configuração no arquivo ConsoleConfiguration.xml, disponível no caminho da Configuração de gerenciamento do UDP para exibir o grupo de FSD de ASBU como o destino de Copiar em fita:

   C:\Arquivos de programas\Arcserve\Unified Data Protection\Management\Configuration\ConsoleConfiguration.xml

   <displayASBUFSDGroup>0</displayASBUFSDGroup>

   Quando o valor é 0, o grupo de FSD de ASBU não é exibido.

   <displayASBUFSDGroup>1</displayASBUFSDGroup>

   Quando o valor é 1, o grupo de FSD de ASBU é exibido.

   Depois de alterar as configurações, reinicie o serviço de gerenciamento do Arcserve UDP para efetivar.

A lista do grupo de mídias é consultada no Servidor do Arcserve Backup. Ela é correspondente à lista de grupos de dispositivos no Servidor do Arcserve Backup.

Multiplexação

Marque a caixa de seleção para ativar a multiplexação. Defina o número máximo de transmissões que podem ser gravadas em uma fita simultaneamente. O número padrão de fluxos é 4 e o intervalo para o qual há suporte está em 2 e 32.

Criptografia

Especifica o uso de criptografia ao se copiar em fita.

Ativar a criptografia garante que os dados sejam criptografados na fita. É necessário fornecer (e confirmar) uma senha criptografada quando uma criptografia for selecionada.

Compactação

Ativar a compactação garante que os dados sejam compactados na fita.

2. Verifique os detalhes do grupo de mídias para o servidor do Arcserve Backup e o grupo de mídias selecionados.
3. Clique na guia **Programar**.

   A página Programar abre.

   Você especificou o destino.

Especificar a programação

É possível especificar a programação para iniciar a tarefa de cópia em fita. Você também pode decidir o modo de uso da fita e a diretiva de retenção de mídia.

Siga estas etapas:

1. Clique em **Adicionar**, **Adicionar programação de cópia em fita**.

   A caixa de diálogo **Adicionar nova programação de cópia em fita** abre.

2. Especifique uma programação de cópia em fita.

   Uma programação define o intervalo de tempo para iniciar uma tarefa de cópia em fita. Se você adicionar uma programação, a tarefa de cópia em fita é executada apenas durante a programação de tempo definida. Se você não especificar uma programação, a tarefa de cópia em fita é executada dentro de 30 minutos depois que um ponto de recuperação qualificado estiver pronto em um repositório de dados.

3. Clique em **Salvar**.

   A caixa de diálogo **Adicionar nova programação de cópia em fita** fecha.

4. Selecione **Nome do pool de mídias** na lista suspensa.

   Um nome de pool de mídias padrão é selecionado com base no nome do plano.

   Também é possível selecionar um nome de pool de mídia existente na lista suspensa. Nesse caso, a diretiva de retenção de mídia e o modo de uso da fita associado a esse pool de mídia podem ser copiados nessa tarefa. Você pode compartilhar as fitas entre vários planos do Arcserve UDP especificando o mesmo pool de mídias em todos os planos do Arcserve UDP.

   Também é possível especificar o nome de outro pool. Um nome de pool de mídias pode ter no máximo 13 caracteres.

5. Especifique um diretiva de **Retenção de ponto de recuperação**.

   Uma diretiva de retenção de ponto de recuperação permite a retenção dos pontos de recuperação em uma base diária, semanal ou mensal. É possível especificar um período de retenção diferente para diferentes tipos de pontos de recuperação. Por exemplo, se você selecionar **Backups diários** e **Backups semanais** na guia **Origem**, poderá especificar o período de retenção de ponto de recuperação diferente para esses tipos de backup.

6. Selecione uma das opções **Uso da fita**.

   Acrescentar a fitas existentes

Indica que todos os pontos de recuperação gerados dentro do período de retenção especificado são copiados na mesma fita. Por exemplo, se você tiver especificado o período de retenção para o backup diário como 7, todos os pontos de recuperação do Dia 1 ao Dia 7 são copiados na mesma fita. Em seguida, todos os pontos de recuperação dos próximos 7 dias (Dia 8 ao Dia 14) serão copiados em uma fita diferente e assim por diante.

Os pontos de recuperação da primeira semana (Dia 1 ao Dia 7)) são retidos pelos próximos 7 dias (Dia 8 ao Dia 14). A partir do dia 15, os pontos de recuperação serão copiados novamente na Fita 1 porque a diretiva de retenção para os pontos de recuperação da primeira semana terá expirado.

A lista a seguir mostra o tempo de retenção padrão para Acrescentar às fitas existentes:

- Diariamente - 7 dias
- Semanalmente - 5 semanas
- Mensalmente - 12 meses

Sete pontos de recuperação diários são copiados na mesma fita, cinco pontos de recuperação semanais são copiados na mesma fita e 12 pontos de recuperação mensais são copiados na mesma fita.

Copiar em fitas separadas

Indica que os pontos de recuperação de cada dia são copiados em uma fita separada. Por exemplo, se você tiver especificado o período de retenção para o backup diário como 7, os pontos de recuperação do dia 1 são copiados na Fita 1, os pontos de recuperação do dia 2 são copiados na Fita 2, os pontos de recuperação do dia 3 são copiados na Fita 3 e assim por diante.

Os pontos de recuperação do dia 1 são retidos durante 7 dias. No dia 8, os pontos de recuperação são copiados na fita 1 porque a diretiva de retenção terá expirado para os pontos de recuperação do dia 1.

A lista a seguir mostra o tempo de retenção padrão da Cópia em fitas separadas:

- Diariamente - 7 dias
- Semanalmente - 5 semanas
- Mensalmente - 12 meses

Cada um dos sete pontos de recuperação diários são copiados em fitas separadas, cada um dos cinco pontos de recuperação semanais são copiados em fitas separadas, e cada um dos doze pontos de recuperação mensais são copiados em fitas separadas.

7. Clique na guia **Avançado**.

   A página **Avançado** é exibida.

   Você especificou a programação.

Especificar as configurações avançadas

As configurações avançadas permitem configurar algumas configurações adicionais para a tarefa de cópia em fita.

1. Especifique os seguintes detalhes.

Ejeção de mídia

Especifica que a mídia deve ser ejetada da unidade após a conclusão da tarefa. Isso ajuda a evitar que qualquer outra tarefa sobrescreva as informações dessa mídia.

Verificação de backup

Especifica que o Arcserve Backup verifica a confiabilidade do backup analisando a legibilidade do cabeçalho de cada arquivo. Essa opção não se aplica aos backups multiplexados.

Executar um comando antes do início da tarefa de cópia em fita

Permite a execução de um script antes de iniciar a tarefa de backup. Especifique o caminho onde o script está armazenado. Clique em No código de saída e especifique o código de saída para Executar tarefa ou Tarefa com falha. Executar a tarefa indica que a tarefa de backup continuará quando o script retornar o código de saída. Tarefa com falha indica que a tarefa de backup será interrompida quando o script retornar o código de saída.

Executar um comando após a conclusão da tarefa de cópia em fita

Permite executar um script depois que a tarefa de backup foi concluída. Especifique o caminho onde o script está armazenado.

Nome de usuário para comandos

Permite especificar o nome de usuário para executar o script.

Senha para comandos

Permite especificar a senha para executar o script.

Ativar alertas por email

Permite ativar alertas por email. É possível especificar configurações de email e os tipos de alertas que você deseja receber por email. Ao selecionar esta opção, as seguintes opções serão ativadas para a seleção.

Configurações de email

Permite configurar as definições de email. Clique em **Configurações de email** e configure o servidor de email e os detalhes do servidor proxy.

Alertas de tarefa

Permite que você selecione os tipos de emails da tarefa que deseja receber.

2. Clique em **Salvar**.

   As alterações são salvas e uma marca de seleção verde é exibida ao lado do nome da tarefa. A página do plano é fechada.

   A tarefa de cópia em fita é criada e executada de acordo com a programação.

   Observação: quando você executa a tarefa **Cópia em fita**, os valores do monitor de tarefas no console do Arcserve UDP são diferentes daqueles do Arcserve Backup.

   Importante: depois de copiar os pontos de recuperação em uma fita, não será possível restaurar os dados em fita no Console do Arcserve UDP. Você precisa restaurar os dados do Gerenciador do Arcserve Backup. Para obter mais informações sobre como restaurar os dados em fita, consulte Backup e restauração de dados do D2D/UDP no Guia do Administrador do Arcserve Backup.

Como criar e gerenciar uma máquina virtual instantânea no Microsoft Azure

A máquina virtual instantânea (VM instantânea) oferece suporte à criação de uma máquina virtual no Microsoft Azure instantaneamente A IVM no Microsoft Azure tem as seguintes vantagens:

- Oferece acesso imediato aos dados e aos aplicativos presentes nas sessões de backup do Arcserve UDP.
- Elimina o tempo de inatividade associado a uma restauração ou conversão tradicional da sessão de backup em uma máquina virtual.
- Fornece uma alternativa para a criação da máquina virtual na nuvem, em vez de no local.

É possível criar uma VM instantânea a partir das seguintes sessões de backup:

- Backup do Linux com base em agente
- Backup sem agente com base em host para VM do Linux

Observação: para seguir as práticas recomendadas para um computador instantâneo no Microsoft Azure, consulte Práticas recomendadas.

O que fazer a seguir?

- Verificar os pré-requisitos
- Criar um plano de máquina virtual instantânea no Microsoft Azure
- Gerenciar um plano de máquina virtual instantânea no Microsoft Azure

Rever os pré-requisitos de uma máquina virtual instantânea no Microsoft Azure

Conclua os pré-requisitos a seguir antes de criar uma VM instantânea:

- Na Matriz de compatibilidade, verifique se a VM é suportada pelo Microsoft Azure e pelo UDP.
- Adicionar uma conta de nuvem do Microsoft Azure
- Verifique se você tem pelo menos um servidor de ponto de recuperação no computador local, como o destino de backup.
- Verifique se você tem pelo menos um servidor de ponto de recuperação no Microsoft Azure, como o destino de replicação.
- Verifique se você tem pelo menos um servidor de backup Linux localmente, para a tarefa de backup.
- Verifique se você tem pelo menos um servidor de backup Linux no Microsoft Azure, para a tarefa da VM instantânea.
- Verifique se uma conta do Microsoft Azure foi adicionada.

Limitação

- Não há suporte para computadores Linux inicializados com UEFI.
- Computadores Linux com o sistema de arquivos Btrfs em vários discos NÃO têm suporte.

Criar uma máquina virtual instantânea no Microsoft Azure

Para criar um IVM no plano do Microsoft Azure, é recomendável executar uma das seguintes opções:

- Faça backup do nó protegido local no repositório de dados local do servidor de ponto de recuperação e, em seguida, replique o servidor de ponto de recuperação no Microsoft Azure. Para obter informações sobre a adição de nós, consulte Como adicionar nós ao console.
- Faça backup do nó protegido local no lugar de compartilhamento CIFS (NFS) local e, em seguida, copie no local de compartilhamento CIFS (NFS) no Microsoft Azure. Para obter mais informações sobre como fazer backup de nós protegidos, consulte Como criar um plano de backup do Linux.

A criação de uma VM instantânea envolve estas cinco etapas abrangentes:

1. Abrir o Assistente de VM instantânea
2. Selecionar o ponto de recuperação
3. Selecionar o local da VM
4. Selecionar o servidor de recuperação
5. Especificar os detalhes da VM instantânea.
6. Enviar a tarefa da VM instantânea

Abrir o assistente de máquina virtual instantânea

É possível configurar e criar uma VM instantânea a partir do assistente de VM instantânea. Há três maneiras de abrir o assistente de VM instantânea:

- No gerenciamento do nó
- No Gerenciamento de destino: servidor de ponto de recuperação
- No Gerenciamento de destino: pasta compartilhada

Abrir o assistente no modo de exibição de gerenciamento de nós

1. Clique na guia **Recursos**.
2. No painel esquerdo, navegue para **Nós** e clique em **Todos os nós**.
3. Todos os nós são exibidos no painel central.
4. Clique com o botão direito em um nó e selecione **Criar uma VM instantânea**.

   A página de Assistente da VM instantânea é exibida.

   Observação: se um nó não estiver associado a um plano, esse nó não terá a opção **Criar uma VM instantânea**.

Abrir o assistente no modo de exibição de gerenciamento de destino

Em Destinos: servidor de ponto de recuperação

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Destinos** e clique em **Servidores de ponto de recuperação**.

   Caso você tenha adicionado repositórios de dados, eles serão exibidos no painel central.
3. Clique no repositório de dados.

   Se você já tiver feito backup dos dados para o servidor RPS, todos os nós de origem serão listados no painel.
4. Clique com o botão direito em um nó e selecione **Criar uma VM instantânea**.

   A página de Assistente da VM instantânea é exibida.

Em Destinos: pasta compartilhada

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Pastas compartilhadas**.

3. Caso você tenha adicionado pastas compartilhadas, essas pastas são exibidas no painel central.
4. Clique em uma pasta compartilhada e selecione **Navegador do ponto de recuperação**.

   Se você já tiver feito backup dos dados para a pasta compartilhada, todos os nós de origem serão listados no painel.
5. Clique com o botão direito em um nó e selecione **Criar uma VM instantânea**.

   A página de Assistente da VM instantânea é exibida.

Selecionar um ponto de recuperação

A página Selecionar ponto de recuperação exibe o local do ponto de recuperação e permite selecionar um ponto de recuperação. O ponto de recuperação pode estar em um local compartilhado ou em um repositório de dados no RPS.

O console reconhece automaticamente o local do ponto de recuperação e pré-seleciona os campos **Tipo de local**, **Servidor do ponto de recuperação** e **Repositório de dados** ou **Pasta de compartilhamento de rede**.

Observação: selecione a sessão Servidor de ponto de recuperação (pasta compartilhada) como destino de replicação para poupar tempo e largura de banda da rede.

Expanda a lista Data, selecione o ponto de recuperação necessário na lista e clique em **Avançar**.

A página **Local da VM** abre.

Observação: se você criar uma máquina virtual instantânea na exibição Gerenciamento de nós, serão listados apenas os servidores de ponto de recuperação que estiverem no mesmo site que o nó de origem. Se você deseja criar uma máquina virtual instantânea do servidor de ponto de recuperação gerenciado a partir de um site diferente, vá para o Site e abra o Assistente na exibição de gerenciamento de destino.

Selecionar um local da VM

Especifique o local da máquina virtual no qual você deseja criar a VM instantânea.

Siga estas etapas:

1. Selecione Microsoft Azure.
2. Selecione um nome de conta.

   Observação: selecione a conta correspondente. Se ela não estiver adicionada, consulte Adicionar uma conta de nuvem do Microsoft Azure.
3. Clique em **Avançar**.

   A página do **Servidor de recuperação** é aberta.

Selecionar um servidor de recuperação

O servidor de recuperação hospeda o módulo principal da VM instantânea. O servidor de recuperação padrão é o RPS. Também é possível atribuir um nó como um servidor de recuperação.

Em sessões de backup do Linux, o servidor de recuperação é um servidor de backup Linux.

Siga estas etapas:

1. selecione um servidor de backup Linux a partir da lista de nós.

   Observações: selecione a sessão Servidor de ponto de recuperação (pasta compartilhada) como destino de replicação para poupar tempo e largura de banda da rede.

2. Clique em **Avançar**.

   A página de Detalhes da VM instantânea será exibida.

   Observação: certifique-se de selecionar Servidor de ponto de recuperação, localizado em Microsoft Azure.

Especificar os detalhes da máquina virtual instantânea

Especifique os detalhes da VM instantânea.

Siga estas etapas:

1. Especifique o nome e a descrição da VM instantânea.

Nome da VM

Especifica o nome da VM instantânea. O nome do prefixo de nó de origem com “UDPIVM_” torna-se o nome padrão da VM instantânea. É possível modificar o nome. Alguns caracteres especiais, como '@', \ e assim por diante, não são permitidos no nome.

Descrição

(Opcional) Especifica a descrição da VM instantânea.

Local

Especifica o local de sua conta do Microsoft Azure.

Tipo de disco

Especifica o tipo de disco.

Tamanho da VM do Azure

Especifica o tamanho da VM com suporte.

Rede

Especifica a rede existente na conta do Microsoft Azure.

Sub-rede

Especifica a sub-rede existente na conta do Microsoft Azure.

IP público de atribuição automática

Especifica o IP público atribuído à VM.

IP principal

Especifica o IP principal da VM. Especifica automaticamente se você não especificar.

Selecionar um grupo de segurança

Especifica o grupo de segurança. É possível selecionar vários grupos. Se você não selecionar algum, cria-se automaticamente um novo grupo de segurança.

Avançar: alterar o nome do host

Especifica o nome do host da nova VM.

Avançar: recuperar dados automaticamente após a inicialização da VM instantânea

Especifica se a recuperação de dados ocorre automaticamente, após a criação da VM instantânea.

2. Clique em **Concluir**.

Agora, você pode enviar a tarefa.

Enviar a tarefa de máquina virtual instantânea

Para criar a VM instantânea, envie a tarefa de VM instantânea. Depois que a tarefa é concluída, é possível ver a VM instantânea em **Recursos**, **Infraestrutura**, **Máquina virtual instantânea**.

Siga estas etapas:

1. Clique em **Criar VM**.

   A caixa de diálogo **Criar VM** é exibida.

2. Selecione uma das seguintes opções:

   Inicializar agora

   Envia uma tarefa para criar a VM instantânea. Após a criação da VM, ela é iniciada automaticamente.

   Inicializar depois

   Cria uma VM instantânea. É necessário iniciar a VM manualmente. É possível iniciar a VM após a conclusão da tarefa de VM instantânea.

   Cancelar

   Fecha a caixa de diálogo Criar VM sem criar nenhuma VM. Você volta à página Criar VM.

   A tarefa de VM instantânea é criada com êxito.

Gerenciar uma máquina virtual instantânea

É possível gerenciar a VM instantânea a partir do console. Você pode ligar ou desligar uma VM instantânea a partir do console. Além disso, é possível excluir qualquer VM instantânea.

Observação: o console exibe somente as VMs instantâneas criadas a partir de pontos de recuperação gerenciados no site selecionado.

- Iniciar ou interromper uma máquina virtual instantânea
- Excluir uma máquina virtual instantânea

Iniciar ou interromper uma máquina virtual instantânea

É possível iniciar ou interromper uma VM instantânea após sua criação. O botão Iniciar ou Parar é exibido dependendo do status da VM.

Siga estas etapas:

1. No console, clique em **Recursos**.
2. Navegue até **Infraestruturas** e clique em **Máquinas virtuais instantâneas**.
3. Selecione a máquina virtual no painel central e clique em **Ações**.
4. Selecione **Ligar** ou **Desligar**, de acordo com o status da máquina virtual.

   A máquina virtual é iniciada ou interrompida com êxito.

Excluir uma máquina virtual instantânea

Você pode excluir qualquer VM instantânea que não for mais necessária.

Siga estas etapas:

1. No console, clique em **Recursos**.
2. Navegue até **Infraestruturas** e clique em **Máquinas virtuais instantâneas**.
3. Selecione a máquina virtual no painel central e clique em **Ações**.
4. Clique em **Excluir**.

   Uma caixa de diálogo de confirmação será aberta.
5. Clique em **OK**.

   A máquina virtual é excluída com êxito.

Como criar e gerenciar uma máquina virtual instantânea em servidores Hyper-V e VMware ESX

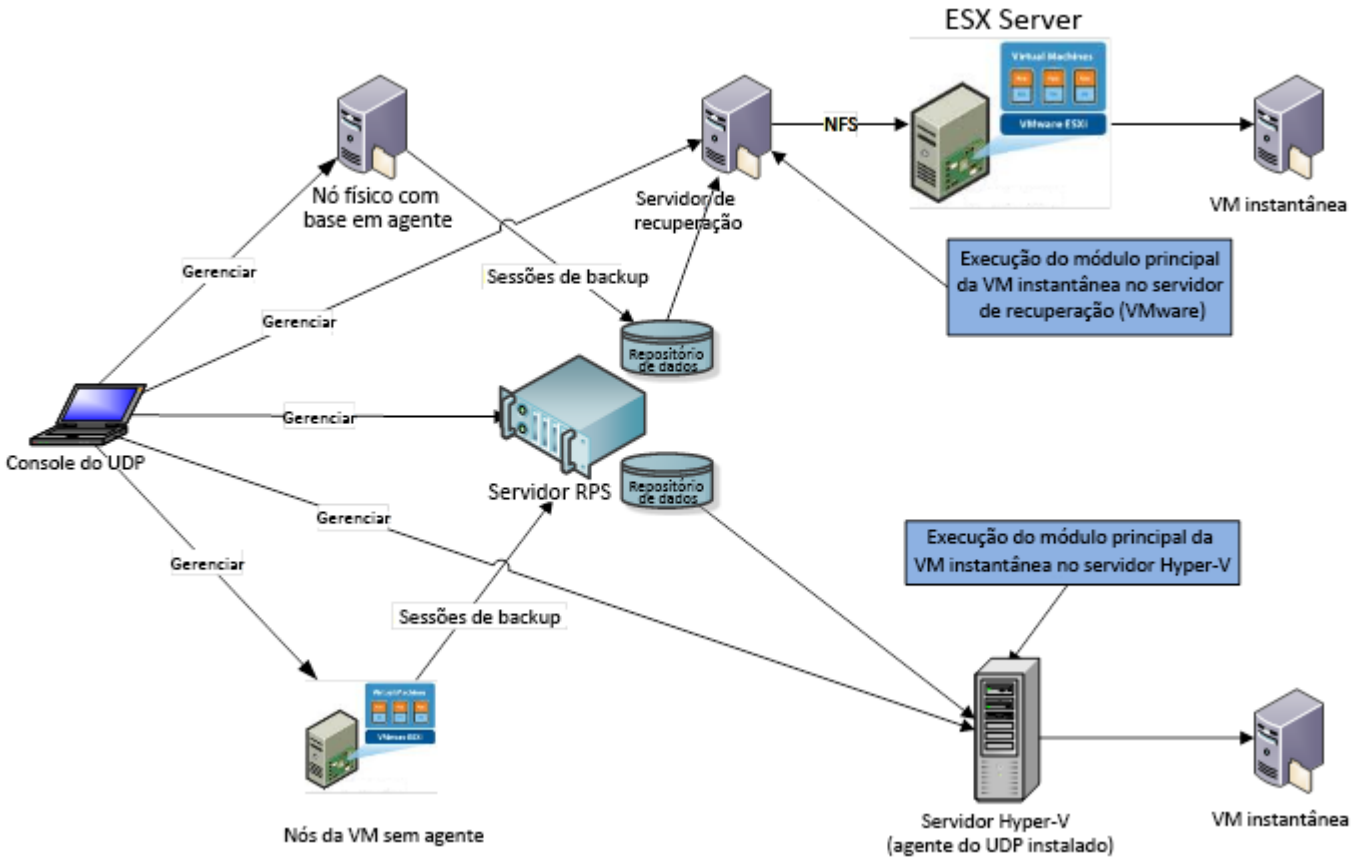
A máquina virtual instantânea (VM instantânea) cria uma máquina virtual no hipervisor e executa a sessão de backup na máquina virtual sem qualquer conversão anterior. A vantagem de uma máquina virtual instantânea é que ela oferece acesso imediato aos dados e aos aplicativos presentes nas sessões de backup do Arcserve UDP. A VM instantânea elimina o downtime associado a uma conversão ou restauração tradicional da sessão de backup para uma máquina física ou virtual.

É possível criar uma VM instantânea a partir das seguintes sessões de backup:

- Backup do Windows com base em agente
- Backup do Linux com base em agente
- Backup sem agente com base em host

Você pode escolher o servidor VMware vCenter/ESX(i) ou o servidor Windows Hyper-V como hypervisor.

O diagrama a seguir explica a arquitetura de uma VM instantânea:



O que fazer a seguir?

- Revisar os pré-requisitos de uma máquina virtual instantânea
- Criar uma máquina virtual instantânea
- Gerenciar uma máquina virtual instantânea

Revisar os pré-requisitos de uma máquina virtual instantânea

Conclua os pré-requisitos a seguir antes de criar uma VM instantânea:

- Verifique se há, pelo menos, um backup do Arcserve UDP.
- Verifique se os agentes do Arcserve UDP já estão instalados no servidor de recuperação.
- Verifique se o recurso NFS está instalado no servidor de recuperação, caso o hypervisor de destino seja um servidor de VMware vCenter/ESX(i).
- Verifique se o sistema operacional do servidor de recuperação é o Windows Server 2008 R2 de 64 bits ou posterior.
- Verifique se o servidor de recuperação tem espaço suficiente para a VM instantânea.
- Verifique se você tem a permissão mínima para executar as tarefas necessárias da VM instantânea. Para obter mais informações, consulte Permissão mínima do VMware necessária para tarefas da IVM.

Observação: a máquina pode ser inicializada. Os NIC(s) são configurados de acordo com a entrada do usuário na interface do usuário.

Considerações

- O recurso de migração de VM instantânea entre nós não é suportado quando uma VM instantânea é iniciada em um agrupamento do Hyper-V.
- Quando você cria uma VM instantânea a partir de um backup de agente Linux, as configurações de uma máquina virtual criada pela VM instantânea não podem ser modificadas usando um cliente do vSphere. É necessário usar o cliente web do vSphere para modificar as configurações da máquina virtual.
- Se a quantidade de repositórios de dados NFS alcançar o número máximo de montagens do NFS em um host do ESX/ESXi e você criar uma VM instantânea, o Arcserve UDP falhará ao criar o repositório de dados NFS. Para aumentar o número máximo de montagens do NFS no host do ESX/ESXi, consulte o artigo da base de conhecimento da VMware.
- Se o ponto de recuperação vier do backup sem agente e o hypervisor de destino for o vsphere ESX/VC, o servidor do NFS é necessário no computador do servidor de backup Linux.

- Se o hipervisor de destino for o MS Hyper-V, o comando net deve estar disponível no servidor de backup Linux. Esse comando pode ser instalado por pacotes de cliente do Samba.
- A máquina virtual não funciona nas seguintes situações:
  - Reinicializações do servidor de recuperação.
  - Falha no servidor de recuperação.
  - A conexão de rede entre o servidor de recuperação e o destino de backup (armazenamento de dados ou pasta de compartilhamento) desconecta.

Permissão mínima do VMware necessária para tarefas da IVM

A tabela exibe a lista de permissão mínima da VMware necessária para executar as tarefas da VM instantânea.

Observação: permissões globais são definidas no nível do vCenter.

Tarefas	Permissão
Repositório de dados	Alocar espaço
Global	Desativar métodos
	Ativar métodos
	Licenças
Host > Configuração	Configuração de partição do armazenamento
Rede	Atribuir rede
Resource	Atribuir a máquina virtual ao pool de recursos
Máquina virtual > Configuração	Adicionar disco existente
	Avançado
Máquina virtual > Interação	Desligar
	Ligar
	Redefinir
	Interação do console
Máquina virtual > Inventário	Criar novo
	Remover
Máquina virtual > Provisionamento	Permitir acesso a disco
	Permitir acesso de somente leitura ao disco
	Permitir download da máquina virtual
Máquina virtual > Gerenciamento de instantâneos	Criar instantâneo
	Remover instantâneo
	Reverter para um instantâneo
Máquina virtual > Operações de convidado	Consultas de operações de convidado

Criar uma máquina virtual instantânea

A criação de uma VM instantânea envolve estas cinco etapas abrangentes:

1. Abrir o Assistente de VM instantânea
2. Selecionar um ponto de recuperação
3. Especificar o local da VM
4. Especificar o servidor de recuperação
5. Especificar os detalhes da VM instantânea
6. Enviar a tarefa da VM instantânea

Após a conclusão bem-sucedida da tarefa, uma VM instantânea será criada.

Abrir o assistente de máquina virtual instantânea

É possível configurar e criar uma VM instantânea a partir do assistente de VM instantânea. Há três maneiras de abrir o assistente de VM instantânea:

- No gerenciamento do nó
- No gerenciamento do destino: Servidor do ponto de recuperação
- No gerenciamento do destino: Pasta compartilhada

Abrir o assistente no modo de exibição de gerenciamento de nós

1. Clique na guia **Recursos**.
2. No painel esquerdo, navegue para **Nós** e clique em **Todos os nós**.
3. Todos os nós são exibidos no painel central.
4. Clique com o botão direito em um nó e selecione **Criar uma VM instantânea**.

   A página de Assistente da VM instantânea é exibida.

   Observação: Se um nó não estiver associado com algum plano, esse nó não terá a opção **Criar uma VM instantânea**.

Abrir o assistente no modo de exibição de gerenciamento de destino

Nos destinos: Servidor do ponto de recuperação

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Destinos** e clique em **Servidores de ponto de recuperação**.

   Caso você tenha adicionado repositórios de dados, eles serão exibidos no painel central.
3. Clique no repositório de dados.

   Se você já tiver feito backup dos dados para o servidor RPS, todos os nós de origem serão listados no painel.
4. Clique com o botão direito em um nó e selecione **Criar uma VM instantânea**.

   A página de Assistente da VM instantânea é exibida.

Nos destinos: Pasta compartilhada

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Pastas compartilhadas**.

3. Caso você tenha adicionado pastas compartilhadas, essas pastas são exibidas no painel central.
4. Clique em uma pasta compartilhada e selecione **Navegador do ponto de recuperação**.

   Se você já tiver feito backup dos dados para a pasta compartilhada, todos os nós de origem serão listados no painel.
5. Clique com o botão direito em um nó e selecione **Criar uma VM instantânea**.

   A página de Assistente da VM instantânea é exibida.

Selecionar um ponto de recuperação

A página Selecionar ponto de recuperação exibe o local do ponto de recuperação e permite selecionar um ponto de recuperação. O ponto de recuperação pode estar em um local compartilhado ou em um repositório de dados no RPS.

O console reconhece automaticamente o local do ponto de recuperação e pré-seleciona os campos **Tipo de local**, **Servidor do ponto de recuperação** e **Repositório de dados** ou **Pasta de compartilhamento de rede**.

Expanda a lista Data, selecione o ponto de recuperação necessário na lista e clique em **Avançar**.

A página **Local da VM** abre.

Observação: se você criar uma Máquina virtual instantânea na exibição Gerenciamento de nós, são listados apenas os servidores de ponto de recuperação que estão no mesmo Site que o nó de origem. Se você deseja criar uma máquina virtual instantânea do servidor de ponto de recuperação gerenciado a partir de um site diferente, vá para o Site e abra o Assistente na exibição de gerenciamento de destino.

Selecionar um local da VM

Especifique o local da máquina virtual no qual você deseja criar a VM instantânea. É possível especificar uma máquina virtual da VMware ou do Microsoft Hyper-V.

Siga estas etapas:

1. selecione um tipo de hipervisor;

VMware vSphere

a. Selecione **VMware vSphere**.

b. Se você já tiver adicionado um nó do VMware ao site selecionado no console, selecione o nó na lista suspensa **Host**.

c. Se você não tiver adicionado nenhum nó do VMware, na lista suspensa Host, clique em **+Adicionar novo hipervisor**.

A caixa de diálogo Adicionar hipervisor é exibida.

d. Especifique os detalhes do servidor VMware vCenter ou ESX(i) e clique em **OK**.

A caixa de diálogo Adicionar hipervisor é fechada e a página **Local da VM** é exibida novamente. Todos os pools de recursos ou ESX(i) são exibidos no painel central.

e. Selecione ESX(i), agrupamento, pool de recursos, aplicativo virtual como o local.

A máquina VMware vSphere é especificada.

Microsoft Hyper-V

a. Selecione **Microsoft Hyper-V**.

b. Se você já tiver adicionado um nó do Hyper-V para o local selecionado no Console, selecione na lista suspensa **Servidor/Agrupamento do Hyper-V**.

c. Se você não tiver adicionado nós do Hyper-V, clique em **Adicionar**.

A caixa de diálogo **Especificar destino da VM** é aberta.

Observação: ao se conectar à VM instantânea do Hyper-V usando uma conta de administrador não integrado local, o UAC remoto precisa ser desativado. Para obter mais informações sobre como desativar o UAC remoto para administrador não integrado, consulte Como desativar o UAC remoto para um administrador não integrado.

d. Especifique os detalhes do servidor Hyper-V e clique em **OK**.

A máquina virtual do Hyper-V é especificada.

Observação: o auxiliar da VM instantânea não pode instalar o serviço de integração em máquinas virtuais instantâneas com o Microsoft Hyper-V 2016 se o nó de origem for do Windows 2008 ou versões anteriores.

2. Clique em **Avançar**.

   A página do **Servidor de recuperação** é aberta.

Como desativar o UAC remoto para um administrador não integrado

A conta de administrador adicional faz referência a essas contas que não são os administradores padrão. Essas contas também são conhecidas como contas administrativas não integradas. Para importar a máquina virtual de um host do Hyper-V, é possível usar a conta de administrador interno do host do Hyper-V ou uma conta de domínio que esteja no grupo de administradores locais do host do Hyper-V, ou um usuário administrativo que não seja interno.

O usuário com a conta administrativa adicional pode usar os procedimentos para desativar o acesso remoto do UAC.

Observações:

- Esse procedimento não é semelhante à desativação do UAC. Com esse procedimento, você pode desativar algumas das funcionalidades do UAC.
- Considerando que a tecnologia WMI (Windows Management Instrumentation - Instrumentação de Gerenciamento do Windows) é usada para importação, verifique se a WMI não está bloqueada pelo firewall.

Siga estas etapas:

1. Clique em Iniciar, digite *regedit* no campo Pesquisar programas e arquivos e pressione Enter.

   O Editor do registro do Windows é exibido.

   Observação: talvez você precise fornecer credenciais administrativas para abrir o Editor do registro do Windows.

2. Localize e clique na chave de registro a seguir:

   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

3. No menu Editar, clique em Novo e, em seguida, clique em Valor DWORD (32 bits).
4. Especifique *LocalAccountTokenFilterPolicy* como o nome da nova entrada e pressione Enter.
5. Clique com o botão direito do mouse em *LocalAccountTokenFilterPolicy* e, em seguida, clique em Modificar.
6. Especifique 1 no campo Dados do valor e clique em OK.
7. Feche o Editor do Registro.

   Para obter mais informações sobre o comportamento do Windows, consulte a documentação da Microsoft.

Selecionar um servidor de recuperação

O servidor de recuperação hospeda o módulo principal da VM instantânea. O servidor de recuperação padrão é o RPS. Também é possível atribuir um nó como um servidor de recuperação.

Em sessões de backup do Linux, o servidor de recuperação é um servidor de backup Linux.

Siga estas etapas:

1. Selecione um dos seguintes como servidor de recuperação:

   Usar servidor do ponto de recuperação

   Especifica que o RPS é usado como um servidor de recuperação.

   Selecionar um nó do Windows da lista de nós

   Especifica que o servidor de recuperação é um nó do Windows. É possível selecionar o nó na lista. São exibidos somente os nós gerenciados pelo Site selecionado.

   Observações:

   - É necessário selecionar um servidor de recuperação somente quando o hipervisor é o VMware vSphere.
   - Quando o hipervisor é o VMware vSphere, a função NFC (Network File System) do Windows deve ser instalada no servidor de ponto de recuperação. Ele poderia ser instalado automaticamente pelo processo de VM instantânea. Para instalar o sistema de arquivos de rede manualmente, consulte o tópico Como instalar manualmente o sistema de arquivos de rede em um servidor Windows.
   - Se Arcserve Backup estiver instalado no servidor de recuperação, o serviço NFS (Network File System) do Windows pode falhar ao iniciar. Isso acontece porque o número da porta padrão do serviço NFS do Windows é 111 e ele é usado pelo serviço **Servidor de chamada de procedimento remoto** do Arcserve Backup. Para alterar o número da porta padrão do serviço **Servidor de chamadas de procedimento remoto** do Arcserve Backup consulte Modificar o arquivo de configuração de portas e Portas de comunicação do servidor principal e servidor integrante na documentação do Arcserve Backup

2. Clique em **Avançar**.

   A página de Detalhes da VM instantânea será exibida.

Como instalar manualmente o Sistema de arquivo de rede em um servidor Windows

Você pode instalar manualmente o NFS (Network File System – Sistema de Arquivos da Rede) em um servidor do Windows usando o Gerenciador de servidores.

Siga estas etapas:

1. Abra o Gerenciador de servidores e clique em Gerenciar, e no assistente Adicionar funções e recursos.

   O assistente Adicionar funções e recursos é aberto.
2. Clique em funções do servidor e selecione *Arquivos e serviços de armazenamento*.
3. Expanda *Arquivo e serviços iSCSI*.
4. Selecione o *Servidor de arquivos* e o *Servidor para NFS*.
5. Clique em Adicionar recursos para incluir os recursos NFS selecionados.
6. Clique em Instalar para instalar os Componentes NFS no servidor.

   Você instalou manualmente o sistema de arquivos de rede no servidor Windows.

Especificar os detalhes da máquina virtual instantânea

Especifique os detalhes da VM instantânea. As opções podem variar de acordo com o hipervisor.

Siga estas etapas:

1. Especifique o nome e a descrição da VM instantânea.

   Nome da VM

   Especifica o nome da VM instantânea. O nome do nó de origem com um prefixo é o nome padrão da VM instantânea. Alguns caracteres especiais não são permitidos no nome, como '@', ' \' e assim por diante.

   Descrição

   (Opcional) Especifica a descrição da VM instantânea.

2. Especifique o local da pasta da VM instantânea no servidor de recuperação.

   É possível procurar as informações do volume do servidor de recuperação.

   Observação: se você selecionar **VMware vSphere** como o local da VM, a pasta selecionada monta-se como Repositório de dados do NFS para a VMware. Um ícone compartilhado aparece nessa pasta no computador local. Por padrão, o repositório de dados NFS é montado no mesmo local de pasta, e você só pode desmontá-lo manualmente a partir do servidor VMware ESX(i).

3. Especifique as configurações da VM instantânea.

   Contagem da CPU

   Especifica a quantidade de CPUs que pode ser necessária para a VM instantânea.

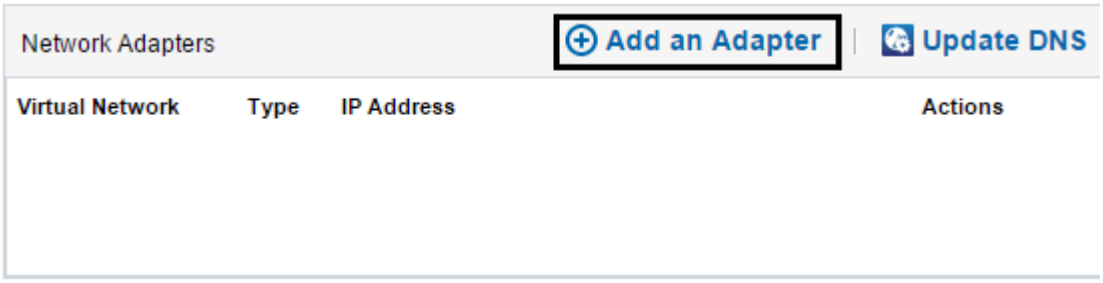
   Tamanho da memória

   Especifica o tamanho da memória que pode ser necessária na VM instantânea.

4. Adicione adaptadores de rede.

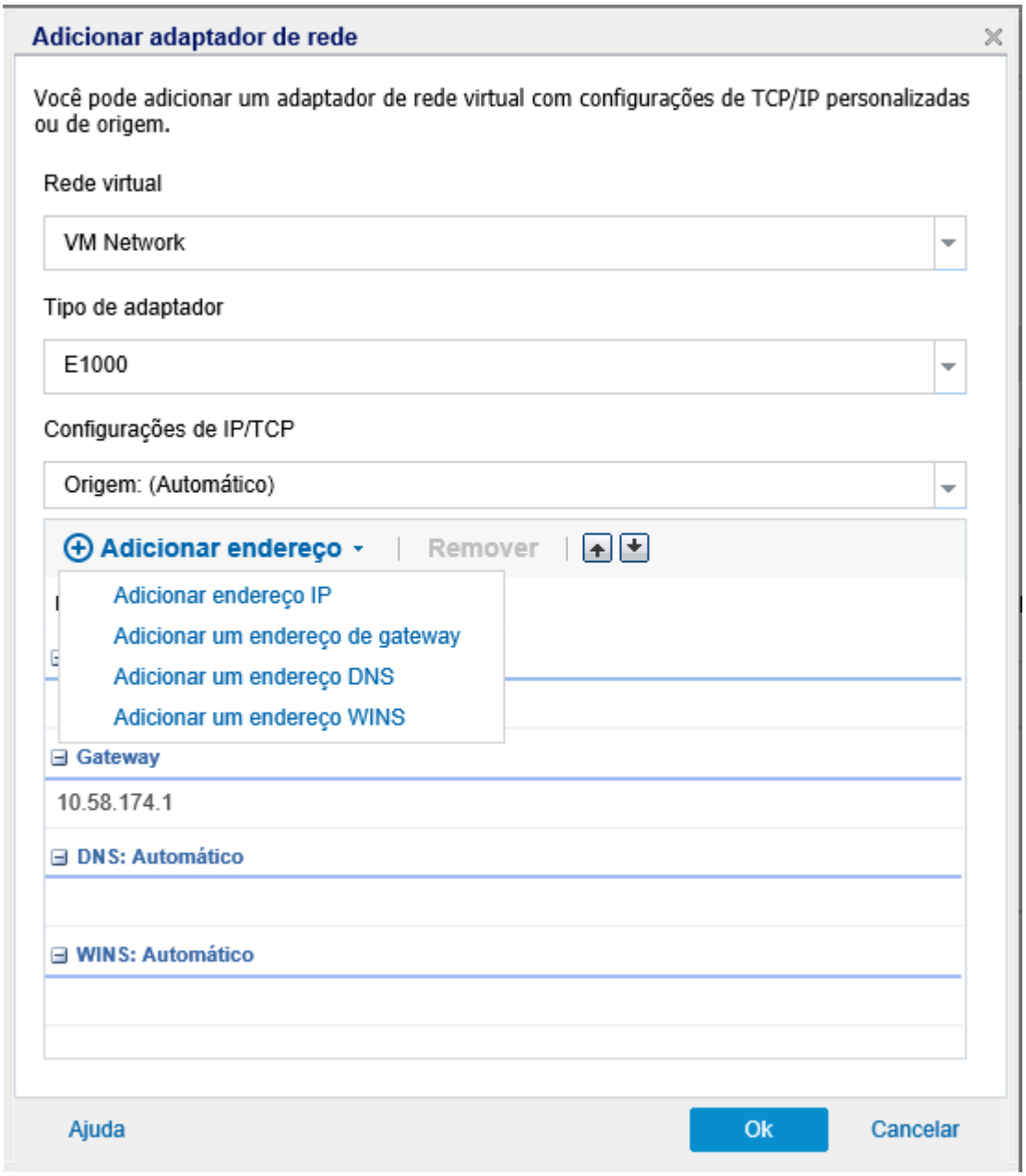
   Observação: para uma VM instantânea do Linux, pelo menos uma NIC virtual pode ser usada para se conectar ao servidor de backup Linux.

   a. Clique no botão **Adicionar um adaptador** para adicionar um adaptador e especificar os detalhes da rede.



É possível adicionar vários adaptadores de rede. Depois de adicionar um adaptador de rede, é possível editar e excluir o adaptador de rede da coluna **Ações**.

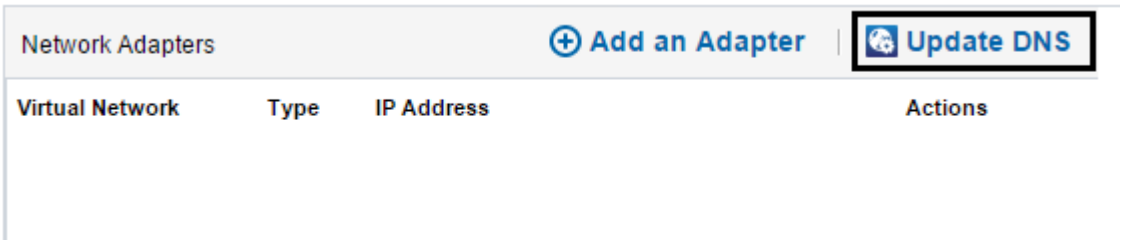
b. Especifique a **Rede Virtual**, o **Tipo de Adaptador** e as **Configurações de TCP/IP**. Se deseja especificar o endereço IP da VM instantânea, clique em **Adicionar um endereço** e selecione o endereço que você deseja configurar.



5. Atualize o DNS.

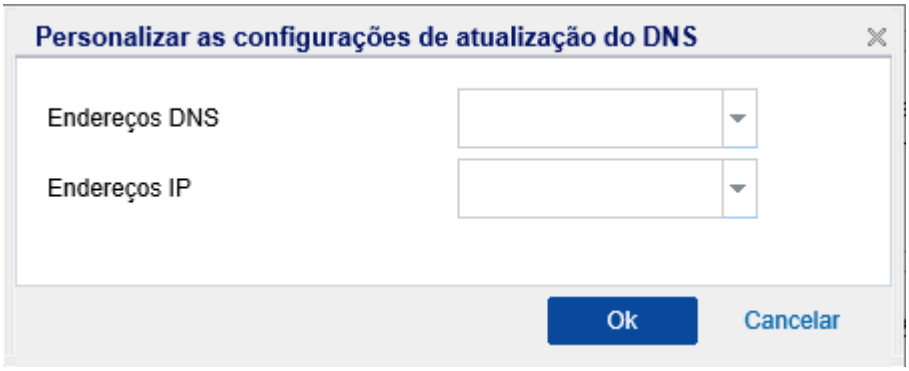
   Observação: esse recurso só está disponível para a VM instantânea do Windows.

   a. Clique no botão **Atualização de DNS** para especificar os detalhes do DNS.



Observação: você pode especificar os detalhes da Atualização de DNS se você tiver especificado um endereço IP e o endereço DNS no adaptador de rede e o computador de origem estiver em um domínio.

b. Clique em **Adicionar um endereço DNS** para adicionar um registro de atualização de DNS. Clique em **Remover** para remover o registro de atualização de DNS. Clique nos botões Para cima e Para baixo para ajustar a sequência dos registros.



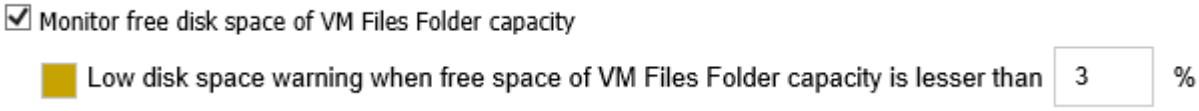
c. Selecione um endereço DNS e um endereço IP na lista suspensa e, em seguida, clique em **OK**.

d. Especifique o **TTL** (Time to Live - Tempo de Vida).

e. Especifique a autenticação de DNS.

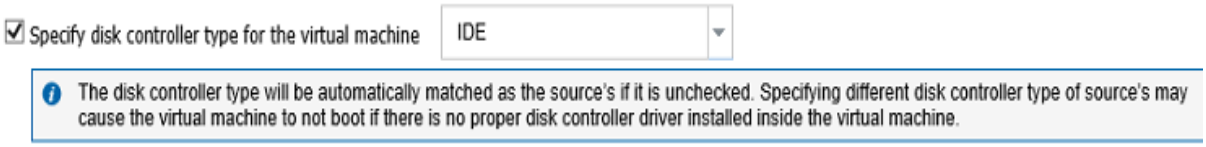
Para o servidor DNS da Microsoft, digite o nome de usuário e a senha. Para o Servidor Bind, é necessário especificar o caminho completo, incluindo o nome de arquivo do arquivo de chave no servidor de recuperação.

6. Verifique o espaço livre em disco da capacidade da pasta de arquivos da VM.



Observação: a caixa de seleção **Monitore o espaço livre em disco da capacidade da pasta de arquivos da VM** vem marcada por padrão. A barra de capacidade será exibida em amarelo na página Máquinas virtuais instantâneas se o espaço livre da capacidade da pasta de arquivos da VM for menor do que o valor-limite. O valor-limite padrão é 3%. É possível alterar o valor, se necessário.

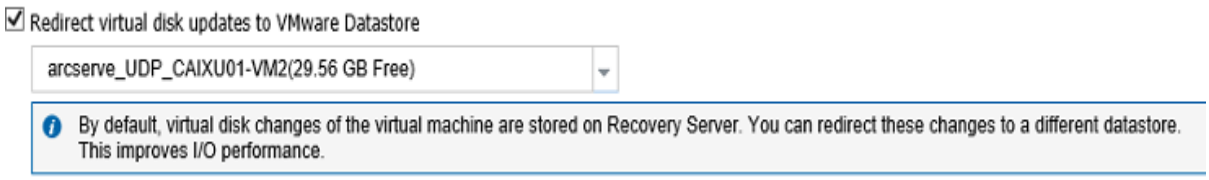
7. Marque a caixa de seleção **Especificar o tipo de controlador de disco para a máquina virtual** e selecione o tipo do controlador de disco para a máquina virtual no menu suspenso.



Observação: a caixa de seleção **Especificar o tipo de controlador de disco para a máquina virtual** estará disponível se você tiver selecionado **VMware vSphere** como o local da VM.

A máquina virtual instantânea é criada aplicando-se o controlador do disco especificado na VMware.

8. Para redirecionar as atualizações de disco virtual para o VMware Datastore, siga estas etapas:
   a. Marque a caixa de seleção **Redirecionar as atualizações de disco virtual para o Repositório de Dados VMware**.

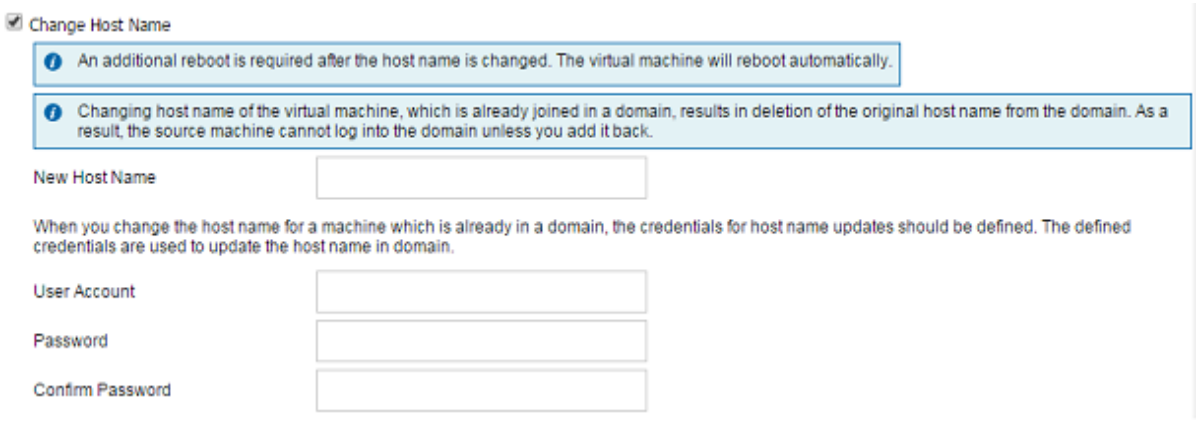


   Observação: a caixa de seleção **Redirecionar as atualizações de disco virtual para o Repositório de Dados VMware** estará disponível se você tiver selecionado **VMware vSphere** como o local da VM.

   b. Selecione o Repositório de Dados VMware necessário no menu suspenso.

   As atualizações do disco virtual são redirecionadas para o repositório de dados VMware selecionado.

9. Para alterar o nome de host da máquina virtual instantânea, siga estas etapas:
   a. Clique na caixa de seleção **Alterar o nome de host** para atualizar o nome do host da VM instantânea.



b. Especifique um novo nome de host para a máquina virtual instantânea. Se o computador de origem estiver em um domínio, forneça a conta de usuário e a senha.

Observação: se o computador de origem estiver em um domínio, a conta deve ter permissão para alterar o nome do host no domínio.

10. (Opcional) Para a **VM instantânea do Linux**, selecione a opção **Recuperar dados automaticamente depois de iniciar a VM instantânea** para ativar a recuperação automática dos dados quando o destino da VM instantânea for iniciado.

    O comportamento padrão da **VM instantânea do Linux** é primeiro recuperar os dados necessários e, depois, iniciar a VM. Se a opção não for selecionada, quando a VM iniciar, os dados restantes não serão recuperados, mesmo se ela for usada como uma VM normal. Se a opção for selecionada, os dados restantes serão recuperados no back-end ao usar a VM. Também é possível preservar o destino da VM instantânea permanentemente ao concluir a recuperação de dados.

    Observação: quando o status do destino da VM instantânea do Linux estiver desligado, a tarefa de VM instantânea falhará. Se esse ponto de recuperação for mesclado, a VM instantânea do Linux falhará ao ligar.

    Agora, você pode enviar a tarefa.

Enviar a tarefa de máquina virtual instantânea

Para criar a VM instantânea, envie a tarefa de VM instantânea. Depois que a tarefa é concluída, é possível ver a VM instantânea em **Recursos**, **Infraestrutura**, **Máquina virtual instantânea**.

Siga estas etapas:

1. Clique em **Concluir**.

   A caixa de diálogo **Inicializar VM** é exibida.

2. Selecione uma das seguintes opções:

   Inicializar agora

   Envia uma tarefa para criar a VM instantânea. Após a criação da VM, ela é iniciada automaticamente.

   Inicializar depois

   Cria uma VM instantânea. É necessário iniciar a VM manualmente. É possível iniciar a VM após a conclusão da tarefa de VM instantânea.

   Cancelar

   Fecha a caixa de diálogo Criar VM sem criar nenhuma VM. Você volta à página Criar VM.

   A tarefa de VM instantânea é criada com êxito.

Gerenciar uma máquina virtual instantânea

É possível gerenciar a VM instantânea a partir do console. Você pode ligar ou desligar uma VM instantânea a partir do console. Além disso, é possível excluir qualquer VM instantânea.

Observação: o console exibe apenas as VMs instantâneas criadas nos pontos de recuperação gerenciados no site selecionado.

- Iniciar ou interromper uma máquina virtual instantânea
- Reiniciar uma máquina virtual instantânea
- Excluir uma máquina virtual instantânea
- Converter a máquina virtual instantânea do Linux em uma máquina virtual independente
- Migrar a máquina virtual instantânea do Linux para uma máquina física

Iniciar ou interromper uma máquina virtual instantânea

É possível iniciar ou interromper uma VM instantânea após sua criação. O botão Iniciar ou Parar é exibido dependendo do status da VM.

Siga estas etapas:

1. No console, clique em **Recursos**.
2. Navegue até **Infraestruturas** e clique em **Máquinas virtuais instantâneas**.
3. Selecione a máquina virtual no painel central e clique em **Ações**.
4. Selecione **Ligar** ou **Desligar**, de acordo com o status da máquina virtual.

   A máquina virtual é iniciada ou interrompida com êxito.

Reiniciar uma máquina virtual instantânea

Você pode reiniciar uma VM instantânea após sua criação.

Observação: é possível reiniciar uma VM instantânea apenas se ela estiver no status de **Falha/Travada**.

Siga estas etapas:

1. No console, clique em **Recursos**.
2. Navegue até **Infraestrutura** e clique em **Máquinas virtuais instantâneas**.
3. Selecione a máquina virtual no status **Falha/Travada** no painel central e clique em **Ações**.
4. Clique em **Reiniciar**.

   A máquina virtual reinicia.

Excluir uma máquina virtual instantânea

Você pode excluir qualquer VM instantânea que não for mais necessária.

Siga estas etapas:

1. No console, clique em **Recursos**.
2. Navegue até **Infraestruturas** e clique em **Máquinas virtuais instantâneas**.
3. Selecione a máquina virtual no painel central e clique em **Ações**.
4. Clique em **Excluir**.

   Uma caixa de diálogo de confirmação é exibida.
5. Clique em **OK**.

   A máquina virtual é excluída com êxito.

Converter a máquina virtual instantânea do Linux em uma máquina virtual independente

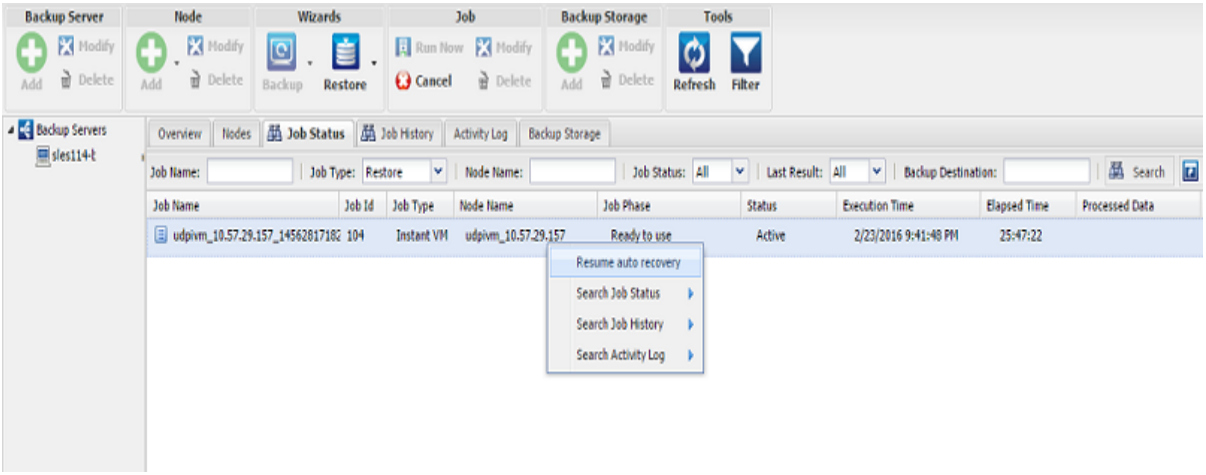
É possível alterar uma IVM (Instant Virtual Machine – Máquina Virtual Instantânea) do Linux para uma VM (Virtual Machine – Máquina Virtual) independente.

Observações:

- Para continuar, é necessário ter um item de menu disponível somente após a IVM ter executado na fase da tarefa “Pronto para uso”.
- O item de menu não está disponível, se o ponto de recuperação for backup sem agente, e o hipervisor de destino for o vSphere ESX/VC. É necessário usar o VMware Storage vMotion para converter a IVM em uma VM independente.

Siga estas etapas:

1. Abra a interface do usuário do servidor de backup Linux.



2. Na guia Status da tarefa, selecione a tarefa IVM, clique com o botão direito no menu de contexto.
3. Selecione Retomar recuperação automática.

   A tarefa IVM é movida para o histórico de tarefas depois que o processo é concluído com êxito.

Migrar a máquina virtual instantânea do Linux para uma máquina física

Para migrar a máquina Virtual instantânea do Linux em um computador físico, consulte **Como executar uma BMR de migração para máquinas Linux** na seção no *Guia do usuário de Agente para Linux*.

Como criar e gerenciar uma máquina virtual instantânea no Amazon EC2

A máquina virtual instantânea (VM instantânea) oferece suporte à criação de uma máquina virtual no Amazon EC2 instantaneamente A IVM no Amazon EC2 tem as seguintes vantagens:

- Oferece acesso imediato aos dados e aos aplicativos presentes nas sessões de backup do Arcserve UDP.
- Elimina o tempo de inatividade associado a uma restauração ou conversão tradicional da sessão de backup em uma máquina virtual.
- Fornece uma alternativa para a criação da máquina virtual na nuvem, em vez de no local.

É possível criar uma VM instantânea a partir das seguintes sessões de backup:

- Backup do Linux com base em agente
- Backup sem agente com base em host

O que fazer a seguir?

- Verificar os pré-requisitos
- Criar um plano de máquina virtual instantânea no Amazon EC2
- Gerenciar um plano de máquina virtual instantânea no Amazon EC2

É possível criar uma VM instantânea das seguintes sessões de backup: na conclusão com êxito da tarefa, uma VM instantânea é criada no Amazon EC2.

Rever os pré-requisitos de uma máquina virtual instantânea no Amazon EC2

Conclua os pré-requisitos a seguir antes de criar uma VM instantânea:

- Na Matriz de compatibilidade, verifique se a VM é suportada pelo Amazon EC2 e pelo UDP.
- Verifique se você tem pelo menos um servidor de ponto de recuperação no computador local, como o destino de backup.
- Verifique se você tem pelo menos um servidor de ponto de recuperação no Amazon EC2 como destino de replicação.
- Verifique se você tem pelo menos um servidor de backup Linux localmente, para a tarefa de backup.
- Verifique se você tem pelo menos um servidor de backup Linux no Amazon EC2, para a tarefa da VM instantânea.
- Verifique se a conta do Amazon EC2 tem cota de instância em execução suficiente para a VM instantânea.

Limitação

NÃO há suporte para o backup de Máquina virtual do Windows sem agente com base em host e do Windows com base em agente.

Criar uma máquina virtual instantânea no Amazon EC2

A criação de uma VM instantânea envolve estas cinco etapas abrangentes:

1. Abrir o Assistente de VM instantânea
2. Selecionar o ponto de recuperação
3. Selecionar o local da VM
4. Selecionar o servidor de recuperação
5. Especificar os detalhes da VM instantânea
6. Enviar a tarefa da VM instantânea

Abrir o assistente de máquina virtual instantânea

É possível configurar e criar uma VM instantânea a partir do assistente de VM instantânea. Há três maneiras de abrir o assistente de VM instantânea:

- No gerenciamento do nó
- No gerenciamento do destino: Servidor do ponto de recuperação
- No gerenciamento do destino: Pasta compartilhada

Abrir o assistente no modo de exibição de gerenciamento de nós

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.
3. Todos os nós são exibidos no painel central.
4. Clique com o botão direito em um nó e selecione **Criar uma VM instantânea**.

   A página de Assistente da VM instantânea é exibida.

   Observação: Se um nó não estiver associado com algum plano, esse nó não terá a opção **Criar uma VM instantânea**.

Abrir o assistente no modo de exibição de gerenciamento de destino

Nos destinos: Servidor do ponto de recuperação

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Destinos** e clique em **Servidores de ponto de recuperação**.

   Caso você tenha adicionado repositórios de dados, eles serão exibidos no painel central.
3. Clique no repositório de dados.

   Se você já tiver feito backup dos dados para o servidor RPS, todos os nós de origem serão listados no painel.
4. Clique com o botão direito em um nó e selecione **Criar uma VM instantânea**.

   A página de Assistente da VM instantânea é exibida.

Nos destinos: Pasta compartilhada

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Pastas compartilhadas**.

3. Caso você tenha adicionado pastas compartilhadas, essas pastas são exibidas no painel central.
4. Clique em uma pasta compartilhada e selecione **Navegador do ponto de recuperação**.

   Se você já tiver feito backup dos dados para a pasta compartilhada, todos os nós de origem serão listados no painel.
5. Clique com o botão direito em um nó e selecione **Criar uma VM instantânea**.

   A página de Assistente da VM instantânea é exibida.

Selecionar um ponto de recuperação

A página Selecionar ponto de recuperação exibe o local do ponto de recuperação e permite selecionar um ponto de recuperação. O ponto de recuperação pode estar em um local compartilhado ou em um repositório de dados no RPS.

O console reconhece automaticamente o local do ponto de recuperação e pré-seleciona os campos **Tipo de local**, **Servidor do ponto de recuperação** e **Repositório de dados** ou **Pasta de compartilhamento de rede**.

Observação: selecione a sessão Servidor de ponto de recuperação (pasta compartilhada) como destino de replicação para poupar tempo e largura de banda da rede.

Expanda a lista Data, selecione o ponto de recuperação necessário na lista e clique em **Avançar**.

A página **Local da VM** abre.

Observação: se você criar uma Máquina virtual instantânea na exibição Gerenciamento de nós, são listados apenas os servidores de ponto de recuperação que estão no mesmo Site que o nó de origem. Se você deseja criar uma máquina virtual instantânea do servidor de ponto de recuperação gerenciado a partir de um site diferente, vá para o Site e abra o Assistente na exibição de gerenciamento de destino.

Selecionar um local da VM

Especifique o local da máquina virtual no qual você deseja criar a VM instantânea. É possível especificar o Amazon EC2 ou o Amazon EC2 (China) de acordo com o tipo de conta.

Siga estas etapas:

1. Selecione Amazon EC2 ou Amazon EC2 (China).
2. Selecione um nome de conta.

   Observação: selecione a conta correspondente. Se ela não estiver adicionada, consulte Adicionar uma conta da nuvem.
3. Clique em **Avançar**.

   A página do **Servidor de recuperação** é aberta.

Selecionar um servidor de recuperação

O servidor de recuperação hospeda o módulo principal da VM instantânea. O servidor de recuperação padrão é o RPS. Também é possível atribuir um nó como um servidor de recuperação.

Em sessões de backup do Linux, o servidor de recuperação é um servidor de backup Linux.

Siga estas etapas:

1. selecione um servidor de backup Linux a partir da lista de nós.

   Observações: selecione a sessão Servidor de ponto de recuperação (pasta compartilhada) como destino de replicação para poupar tempo e largura de banda da rede.

2. Clique em **Avançar**.

   A página de Detalhes da VM instantânea será exibida.

Especificar os detalhes da máquina virtual instantânea

Especifique os detalhes da VM instantânea.

Siga estas etapas:

1. Especifique o nome e a descrição da VM instantânea.

Nome da VM

Especifica o nome da VM instantânea. O nome do prefixo de nó de origem com “UDPIVM_” torna-se o nome padrão da VM instantânea. É possível modificar o nome. Alguns caracteres especiais, como '@', \ e assim por diante, não são permitidos no nome.

Descrição

(Opcional) Especifica a descrição da VM instantânea.

Região

Especifica a região da sua conta do Amazon EC2.

Tipo de instância

Especifica o tipo de instância com suporte.

Tipo de volume

Especifica o tipo de volume.

Rede

Especifica a rede existente na conta do Amazon EC2.

Sub-rede

Especifica a sub-rede existente na conta do Amazon EC2.

IP público de atribuição automática

Especifica o IP público atribuído à VM. .

IP principal

Especifica o IP principal da VM. Especifica automaticamente se você não especificar.

Selecionar um grupo de segurança

Especifica o grupo de segurança. É possível selecionar vários grupos. Se você não selecionar algum, cria-se automaticamente um novo grupo de segurança.

Avançado: Alterar o nome do host

Especifica o nome do host da nova VM.

Avançado: Recuperar dados automaticamente após a inicialização da VM instantânea

Especifica se a recuperação de dados ocorre automaticamente, após a criação da VM instantânea.

2. Clique em **Concluir**.

Agora, você pode enviar a tarefa.

Enviar a tarefa de máquina virtual instantânea

Para criar a VM instantânea, envie a tarefa de VM instantânea. Depois que a tarefa é concluída, é possível ver a VM instantânea em **Recursos**, **Infraestrutura**, **Máquina virtual instantânea**.

Siga estas etapas:

1. Clique em **Criar VM**.

   A caixa de diálogo **Criar VM** é exibida.

2. Selecione uma das seguintes opções:

   Inicializar agora

   Envia uma tarefa para criar a VM instantânea. Após a criação da VM, ela é iniciada automaticamente.

   Inicializar depois

   Cria uma VM instantânea. É necessário iniciar a VM manualmente. É possível iniciar a VM após a conclusão da tarefa de VM instantânea.

   Cancelar

   Fecha a caixa de diálogo Criar VM sem criar nenhuma VM. Você volta à página Criar VM.

   A tarefa de VM instantânea é criada com êxito.

Gerenciar uma máquina virtual instantânea

É possível gerenciar a VM instantânea a partir do console. Você pode ligar ou desligar uma VM instantânea a partir do console. Além disso, é possível excluir qualquer VM instantânea.

Observação: o console exibe somente as VMs instantâneas criadas a partir de pontos de recuperação gerenciados no site selecionado.

- Iniciar ou interromper uma máquina virtual instantânea
- Reiniciar uma máquina virtual instantânea
- Excluir uma máquina virtual instantânea
- Converter a máquina virtual instantânea do Linux em uma máquina virtual independente
- Migrar a máquina virtual instantânea do Linux para uma máquina física

Iniciar ou interromper uma máquina virtual instantânea

É possível iniciar ou interromper uma VM instantânea após sua criação. O botão Iniciar ou Parar é exibido dependendo do status da VM.

Siga estas etapas:

1. No console, clique em **Recursos**.
2. Navegue até **Infraestruturas** e clique em **Máquinas virtuais instantâneas**.
3. Selecione a máquina virtual no painel central e clique em **Ações**.
4. Selecione **Ligar** ou **Desligar**, de acordo com o status da máquina virtual.

   A máquina virtual é iniciada ou interrompida com êxito.

Reiniciar uma máquina virtual instantânea

Você pode reiniciar uma VM instantânea após sua criação.

Observação: é possível reiniciar uma VM instantânea apenas se ela estiver no status de **Falha/Travada**.

Siga estas etapas:

1. No console, clique em **Recursos**.
2. Navegue até **Infraestrutura** e clique em **Máquinas virtuais instantâneas**.
3. Selecione a máquina virtual no status **Falha/Travada** no painel central e clique em **Ações**.
4. Clique em **Reiniciar**.

   A máquina virtual reinicia.

Excluir uma máquina virtual instantânea

Você pode excluir qualquer VM instantânea que não for mais necessária.

Siga estas etapas:

1. No console, clique em **Recursos**.
2. Navegue até **Infraestruturas** e clique em **Máquinas virtuais instantâneas**.
3. Selecione a máquina virtual no painel central e clique em **Ações**.
4. Clique em **Excluir**.

   Uma caixa de diálogo de confirmação é exibida.
5. Clique em **OK**.

   A máquina virtual é excluída com êxito.

Converter a máquina virtual instantânea do Linux em uma máquina virtual independente

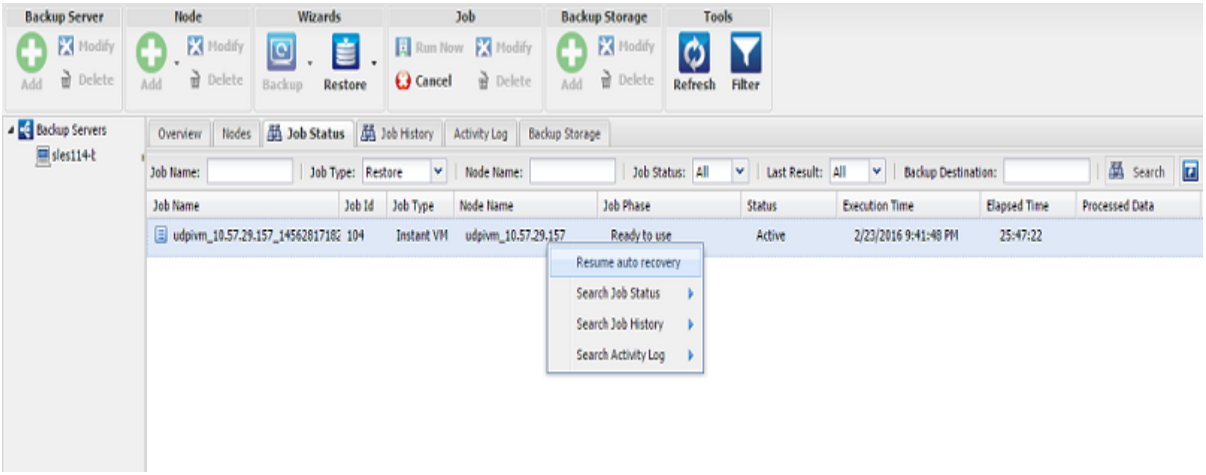
É possível alterar uma IVM (Instant Virtual Machine – Máquina Virtual Instantânea) do Linux para uma VM (Virtual Machine – Máquina Virtual) independente.

Observações:

- Para continuar, é necessário ter um item de menu disponível somente após a IVM ter executado na fase da tarefa “Pronto para uso”.
- O item de menu não está disponível, se o ponto de recuperação for backup sem agente, e o hipervisor de destino for o vSphere ESX/VC. É necessário usar o VMware Storage vMotion para converter a IVM em uma VM independente.

Siga estas etapas:

1. Abra a interface do usuário do servidor de backup Linux.



2. Na guia Status da tarefa, selecione a tarefa IVM, clique com o botão direito no menu de contexto.
3. Selecione Retomar recuperação automática.

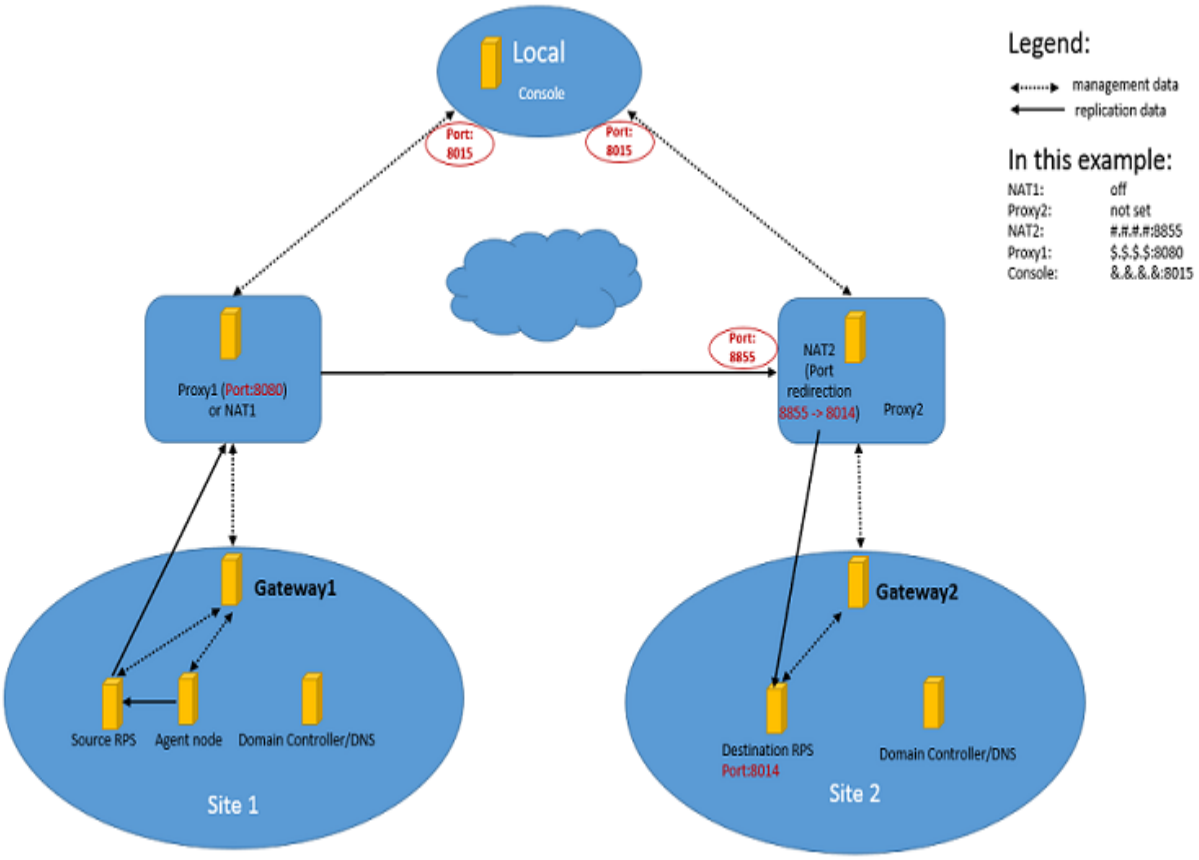
   A tarefa IVM é movida para o histórico de tarefas depois que o processo é concluído com êxito.

Migrar a máquina virtual instantânea do Linux do Amazon EC2 para uma máquina física

Para migrar a máquina virtual instantânea do Linux para uma máquina física, consulte a seção **Como executar uma BMR de migração para máquinas Linux do Amazon EC2 para local** no *Guia do Usuário do Agente para Linux*.

Como criar um plano para replicação entre sites

O recurso de replicação entre sites permite usar o mesmo Console para replicar dados entre sites diferentes. O diagrama a seguir ilustra a conexão entre o Console, Site 1 e Site 2:



O Console (por exemplo, na rede pública), o Site 1 (por exemplo, em uma rede privada) e o Site 2 (por exemplo, em outra rede privada) podem estar em diferentes segmentos da rede. O Site 1 e o Site 2 são gerenciados pelo console por meio do gateway.

O diagrama dá um exemplo para ilustrar esse recurso do UDP, que é apenas uma referência porque o ambiente real que você está usando talvez não seja semelhante ao descrito aqui. O exemplo tem o objetivo de replicar dados do RPS de origem do Site 1 para o RPS de destino do Site 2. O gateway no site 1 e no site 2 pode se conectar ao console usando o proxy ou o NAT. O proxy e o NAT devem estar configurados corretamente.

Descrição do diagrama:

- O Proxy1 ou o NAT1 têm a interface pública e a interface privada. Por exemplo: IP-1 como o IP público está no mesmo segmento com o console e IP-2 como IP particular está no mesmo segmento com o Site 1. Na configuração de rede da máquina do Gateway 1, o gateway padrão está definido como IP privado do Proxy 1 ou NAT 1.
- O Proxy 2 e o NAT 2 também têm a mesma configuração com o Proxy 1/NAT 1, além disso o NAT 2 precisa de configuração extra de uma regra de redirecionamento de porta para que a partir da rede pública se possa acessar o serviço privado por este mapeamento. Nesse exemplo, vemos o RPS de origem por meio do qual o redirecionamento da porta NAT 2 pode se conectar ao RPS de destino.
- Com o sistema operacional do Windows Server 2012 R2, a GUI e o comando do Windows podem definir a direção da porta para o NAT. Aqui está um exemplo de comando, que significa: insira esse endereço a partir do https ou http://<NAT2 IP-1>:<número da porta=8855> do explorador da web do RPS de destino, e ele será redirecionado para o https ou http://<RPS de destino IP=192.168.30.102>:8014 de RPS de destino, em seguida, você pode executar a replicação entre sites.

netsh interface portproxy add v4tov4 listenport=8855 connectaddress="192.168.30.102" connectport=8014 protocol=tcp

Criar um plano para a replicação entre sites

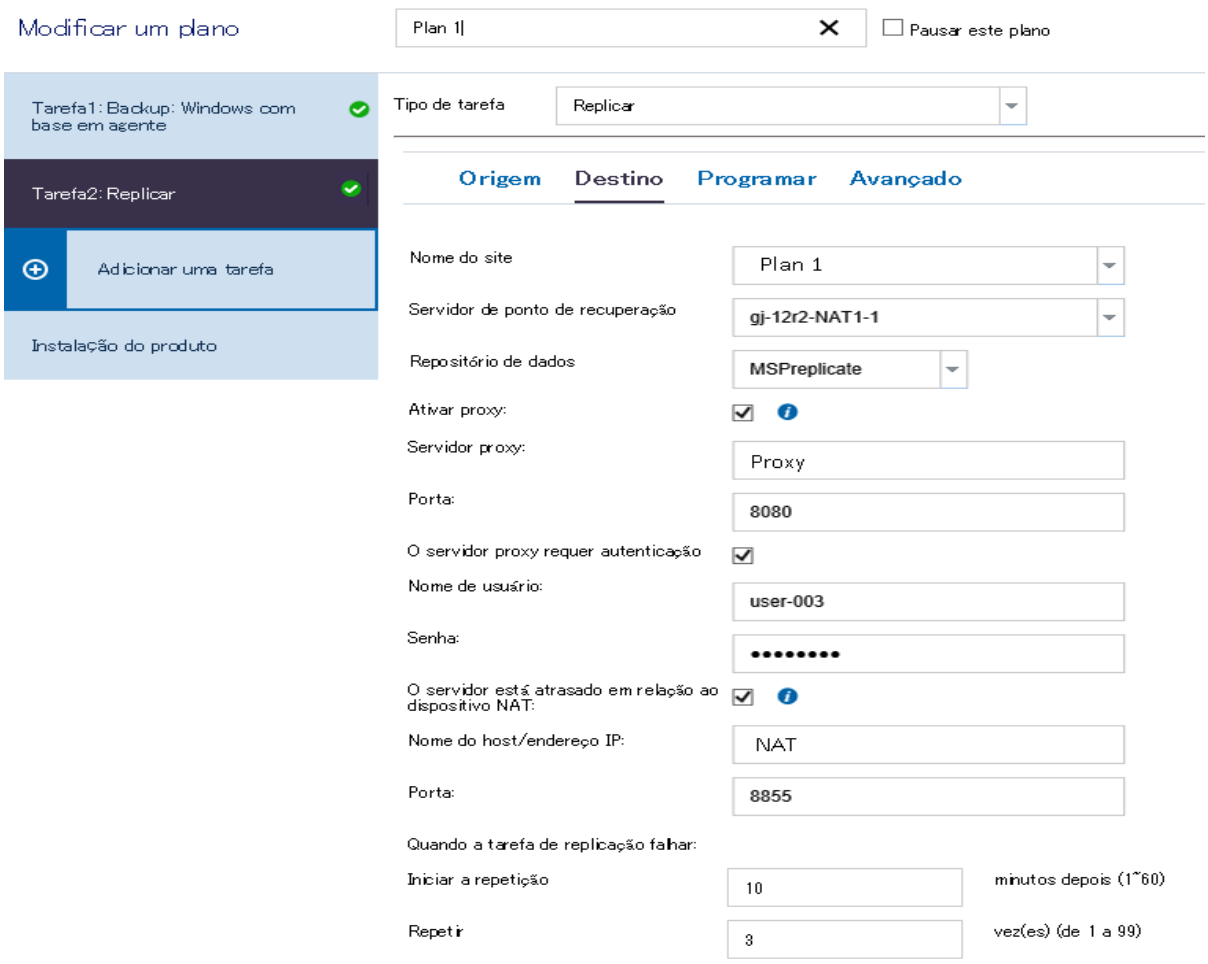
É possível criar um plano para a replicação entre sites.

Siga estas etapas:

1. No Site 1, que é o RPS de origem, crie uma tarefa de backup como Task1.
2. Adicionar uma tarefa de **Replicação** no mesmo plano.
3. Na guia **Destino**, selecione o outro site (site 2 no exemplo) em que o repositório de dados ou o RPS de destino está localizado.
4. (Opcional) Ative os detalhes do proxy (servidor, porta e autenticação).

   Observação: antes de ativar os detalhes do proxy, é preciso configurar o servidor proxy entre o site 1 e o console.
5. (Opcional) Ative os detalhes do NAT.

   Observação: antes de ativar os detalhes do NAT, é necessário configurar o servidor NAT e o redirecionamento de porta entre o Console e o site 2.



6. Configure as outras guias como **Programar** e **Avançado** e salve o plano.
7. Quando a tarefa for executada, verifique o status do monitor e do log de backup, replicação (saída) e replicação (entrada).

Como proteger os dados do Microsoft Office 365

Esta seção contém os seguintes tópicos:

Autenticação moderna

Esta seção fornece informações sobre como configurar os pré-requisitos para os backups do Office 365 usando a autenticação moderna. Para configurar, siga estas etapas:

1. Preparando a máquina proxy
2. Configurando um aplicativo no portal do Azure
3. Atribuindo as permissões de administrador globais ao aplicativo do Azure
4. Fazendo download do certificado do UDP e carregando-o no Azure
5. Atribuindo a função de representação do aplicativo à conta de usuário especificada para o backup

Preparando a máquina proxy

Esta seção fornece informações sobre como preparar a máquina proxy.

Siga estas etapas:

1. Instale o PowerShell versão 5.1 ou posterior (parte da WMF, Windows Management Framework - Estrutura de Gerenciamento do Windows).

   Observação: para verificar a versão do PowerShell, execute o seguinte comando:

   Get-Host | Select-Object Version

2. Para instalar os componentes necessários do sistema, faça o seguinte:
   - Para instalar os componentes necessários do sistema automaticamente, faça o seguinte:
     a. Faça download do script do PowerShell. Para fazer download, clique em *Script2InstallPrerequisites.ps1_*.
     b. Renomeie *Script2InstallPrerequisites.ps1_* para *Script2InstallPrerequisites.ps1*.
     c. Abra a janela do PowerShell usando a opção *Executar como administrador* e execute *Script2InstallPrerequisites.ps1*.

- Para instalar os componentes necessários do sistema manualmente, execute os seguintes comandos do PowerShell:
  - *Install-Module -Name AzureAD -Force*
  - *Install-Module -Name ExchangeOnlineManagement -Force*
  - *Install-Module -Name PackageManagement -Force*
  - *Install-Module -Name PowerShellGet -Force*

  Observação: ao instalar módulos do PowerShell usando os comandos acima, uma versão mais recente dos módulos poderá ser instalada dependendo da versão do GA do componente disponível no repositório da Microsoft.

Configurando um aplicativo no portal do Azure

Esta seção fornece informações sobre como configurar um aplicativo no portal do Azure.

Siga estas etapas:

1. Efetue logon no portal do Azure.
2. Para navegar até a página de registros do aplicativo, execute um dos seguintes procedimentos:
   - No painel à esquerda, selecione **Azure Active Directory** e clique em **Registros do aplicativo**.
   - Procure registros de aplicativos na barra de pesquisa e, em seguida, selecione **Registros do aplicativo**.
3. Na página de registros do aplicativo, clique em **Novo registro**.
4. Na página Registrar um aplicativo, siga as etapas abaixo e clique em **Registrar**:
   - Nome - Digite um nome para o aplicativo. Por exemplo, *UDP365*.
   - Tipos de contas com suporte - selecione a opção **Contas apenas neste diretório organizacional (somente "your-domain" - locatário único)**.
5. Copie e salve a **ID do aplicativo (cliente)** para uso futuro.

Atribuindo as permissões de administrador globais ao aplicativo do Azure

Esta seção fornece informações sobre como atribuir as permissões de administrador global ao aplicativo do Azure.

Para atribuir a função de administrador global ao aplicativo AzureAD, execute um dos seguintes procedimentos:

- Para atribuir a função automaticamente, siga estas etapas:
  1. Faça download do script do PowerShell. Para fazer download, clique em *AssignGlobalAdminRoleToADApplication.ps1*.
  2. Abra a janela do PowerShell usando a opção *Executar como administrador*, navegue até o caminho do script baixado e execute o seguinte:

     .\AssignGlobalAdminRoleToADApplication.ps1 <Application(client) id generated from the Azure portal>

     Por exemplo:

     .\AssignGlobalAdminRoleToADApplication.ps1 60f92079-d1bf-40f7-9ab5-59caab8e7534
- Para atribuir a função manualmente usando os cmdlets do PowerShell, siga estas etapas:
  1. Para instalar o módulo MSOnline, execute o seguinte comando na janela do PowerShell usando a opção Executar como administrador:

     Install-Module MSOnline
  2. Para iniciar uma conexão com o Azure Active Directory (AzureAD), execute o seguinte comando:

     Connect-MSolService
  3. Obtenha a ID do aplicativo usando o seguinte comando:

     $sp = Get-MsolServicePrincipal -AppPrincipalID <APP ID GUID>

     Observação: APP ID GUID é a ID do aplicativo UDP.
  4. Obtenha a função de administrador global/da empresa usando o seguinte comando:

     $role = Get-MsolRole -RoleName "Company Administrator"
  5. Para adicionar a função de administrador global/da empresa ao aplicativo AzureAD, use o seguinte comando:

     Add-MsolRoleMember -RoleObjectId $role.ObjectId -RoleMemberType ServicePrincipal -RoleMemberObjectId $Sp.ObjectId

Fazendo download do certificado do UDP e carregando-o no Azure

Esta seção fornece informações sobre como fazer download do certificado a partir do UDP e carregá-lo no portal do Azure.

No console do UDP, ao criar um plano do Office 365 novo ou existente para o Exchange Online, SharePoint ou OneDrive, após selecionar a opção Autenticação moderna, execute uma das seguintes ações:

Método 1: para gerar e fazer download de um novo certificado autoassinado para autenticação, siga estas etapas:

1. Para gerar um novo certificado autoassinado, selecione **Gerar e fazer download do novo certificado autoassinado**.
2. Digite e redigite a senha do certificado, conforme necessário.
3. Para fazer download do certificado, clique em uma das seguintes opções:
   - **Certificado público** - faça download do certificado para carregá-lo no portal do Azure.
   - **Certificado privado** - faça download do certificado para salvá-lo no computador para uso futuro.

     Observação: depois de fazer download do certificado público, a opção de download do certificado privado é ativada.
4. Efetue logon no portal do Azure.
5. Procure registros de aplicativos na barra de pesquisa e, em seguida, selecione **Registros do aplicativo**.
6. Na lista de aplicativos registrados, clique no aplicativo criado anteriormente na seção *Configurando um aplicativo no portal do Azure*.
7. Navegue até Certificados e segredos, clique em **Carregar certificado**, procure o certificado existente [arquivo .cer] e, em seguida, clique em **Adicionar**.
8. No painel esquerdo, selecione as permissões de API e clique em **Oferecer consentimento de administrador para <nome do locatário>**.

   Uma mensagem de confirmação é exibida.
9. Clique em **Sim**.
10. No console do UDP, clique em **Avançar** para prosseguir para o registro do nó.

Método 2 : para autenticar usando um certificado existente, siga estas etapas:

Observações:

- Quando a opção *Usar certificado existente* é selecionada, espera-se que o usuário tenha seus arquivos de certificado (arquivo .cer) e certificado de chave privada (arquivo .PFX com senha), e que esses certificados possam ser autoassinados ou assinados por uma CA (Certifying Authority - Autoridade de Certificação).
- Se o mesmo certificado for usado para várias criações de planos, será suficiente carregar o certificado apenas uma vez no portal do Azure.
- Se estiver usando o Internet Explorer (IE 11), ele será bloqueado quando você selecionar a opção *Usar certificado existente*. Para resolver isso, consulte Definir as configurações de segurança do Internet Explorer (IE 11).

1. Efetue logon no portal do Azure.
2. Procure registros de aplicativos na barra de pesquisa e, em seguida, selecione **Registros do aplicativo**.
3. Na lista de aplicativos registrados, clique no aplicativo criado anteriormente na seção *Configurando um aplicativo no portal do Azure*.
4. Navegue até Certificados e segredos, clique em **Carregar certificado**, procure o certificado existente [arquivo .cer] e, em seguida, clique em **Adicionar**.
5. No painel esquerdo, selecione as permissões de API e clique em **Oferecer consentimento de administrador para <nome do locatário>**.

   Uma mensagem de confirmação é exibida.
6. Clique em **Sim**.
7. Siga estas etapas no console do UDP:
   a. Procure o certificado de chave privada [arquivo .PFX] e digite a senha.
   b. Clique em **Avançar** para prosseguir para Registro de nó.

Atribuindo a função de representação do aplicativo à conta de usuário especificada para o backup

Esta seção fornece informações sobre como adicionar a conta de backup ao grupo de funções Gerenciamento de detecção e sobre como atribuir a permissão de representação do aplicativo.

Para adicionar a função e o grupo necessários, execute uma das seguintes ações:

Método 1: usando o portal do Office 365

Siga estas etapas:

1. Efetue logon no portal do Office 365 como administrador ou com uma conta que possua as permissões de administrador global.

   A página central do administrador do Exchange é exibida.

2. Vá para **permissões** e, na lista suspensa **Adicionar**, clique duas vezes em **Gerenciamento de detecção**.

   A caixa de diálogo Gerenciamento de detecção é exibida.

   Observação: o membro do grupo de funções de gerenciamento de detecção poderá pesquisar nas caixas de correio da organização do Exchange quanto aos dados que atendem a critérios específicos.

3. Em **Funções**, clique no **+** para adicionar a função *ApplicationImpersonation*.

   A caixa de diálogo Selecionar uma função é exibida.

4. Na lista suspensa **Nome de exibição**, selecione **ApplicationImpersonation**.

   Observação: a função *ApplicationImpersonation* permite que os aplicativos representem usuários em uma organização para executar tarefas em nome do usuário.

5. Clique em **Adicionar** para adicionar a função ApplicationImpersonation e clique em **OK**.

6. Na caixa de diálogo Gerenciamento de detecção, em **Membros**, clique em **+** para adicionar a conta de backup como um membro.

   A caixa de diálogo Selecionar membros é exibida.

7. Na lista suspensa Nome, selecione a conta de backup, clique em **Adicionar** para adicionar o membro e, em seguida, clique em **OK**.

   A conta de backup selecionada é exibida em **Membros** na caixa de diálogo **Gerenciamento de detecção**.

8. Clique em **Salvar**.

Método 2: usando o PowerShell remoto

Siga estas etapas:

1. Conecte-se ao locatário do Exchange Online usando o PowerShell remoto. Para obter mais informações, consulte Conectar-se ao Exchange Online PowerShell.

2. Depois de conectado, para adicionar a conta de backup como membro do grupo de funções Gerenciamento de detecção, use o seguinte:

   ```
   "Add-RoleGroupMember"
   ```

Por exemplo: *Add-RoleGroupMember "discovery management" -member userName@domain.onmicrosoft.com.*

3. Para atribuir a função de representação de aplicativo à conta de backup, use o seguinte:

   `"New-ManagementRoleAssignment"`

   Por exemplo: *New-ManagementRoleAssignment -Nome: impersonationAssignmentName -Função:ApplicationImpersonation - Usuário: "username@domain.onmicrosoft.com"*

A função *ApplicationImpersonation* e o grupo de membros são adicionados à conta de backup do Exchange Online.

Como criar um plano de backup do Exchange Online

O Exchange Online é um aplicativo de email hospedado na nuvem da Microsoft. Para proteger seus itens de email do Exchange Online (emails, itens de calendário, contatos e assim por diante) a partir da nuvem da Microsoft, você precisa criar um plano. Um plano do Exchange Online consiste em uma tarefa de backup. Esta tarefa de backup permite especificar os nós do Exchange Online que você deseja proteger, o destino do backup e a programação de backup.

O que fazer a seguir?

1. Verificar os pré-requisitos e as considerações
2. Criar um plano de backup do Exchange Online
3. (Opcional) Executar um backup manual
4. Fazer a configuração da autenticação multifator

Verificar os pré-requisitos e as considerações

Revise os seguintes pré-requisitos e considerações antes de criar um plano de backup do Exchange Online.

Criando um plano de backup do Exchange Online:

Pré-requisitos:

Para a conta de backup:

- Use uma conta de serviço de backup com permissões de administrador global.
- Adicionar permissões de representação para o usuário do backup para a conta de backup do Exchange Online para conectar-se à organização do Exchange Online, executar backups e restaurar.

  Observação: se você não adicionar a conta de backup ao grupo de funções de Gerenciamento de detecção e não atribuir a permissão Reprodução de aplicativo, o backup apresentará falha.

- Associe a conta de usuário de backup a uma caixa de correio do Exchange Online.

Para o proxy de backup:

- Efetue logon no console.
- Instale o agente do Arcserve UDP no computador proxy em que você deseja executar o backup/a restauração.

Considerações:

- Ao fazer backup de um grande número de usuários, é possível usar grupos do Exchange para melhorar o backup e a otimização.
- A configuração padrão do backup do Exchange Online usa 4 segmentos de backup (um por usuário) de cada vez. Você também pode modificar os segmentos no arquivo de configuração de *Engine\BIN\Office365\Arcserve.Office365.Exchange.config*da seguinte forma:

```
<!--#region for multi thread--> <!--MultiThreadEnable default value:0. if enable, set 1.--> <add key="MultiThreadEnable" value ="1"/> <!--set how many thread will be used to backup mailbox. O valor padrão é 4--> <add key-y="MaxDegreeOfParallelismForMailbox" value="4"/> <!--#en-dregion-->
```

É recomendável definir um valor de 1 a 5. O valor máximo possível é 10. No entanto, não aconselhamos que você defina nenhum valor de 6 a 10.

Observação: o UDP 8.0 oferece suporte ao seguinte:

- Caixa de correio do usuário
- Caixa de correio compartilhada
- Pastas públicas ativadas para email
- Caixas de correio de sala
- Caixas de correio de equipamentos
- Caixas de correio de grupo

Observação: para obter mais informações sobre as práticas recomendadas para o Exchange Online, consulte Assuntos relacionados ao Exchange Online.

Criando um plano de backup do Exchange Online usando BA (Basic Authentication - Autenticação básica):

Revise os seguintes pré-requisitos:

- Instale o PowerShell versão 5.1 ou superior (parte da WMF, Windows Management Framework - Estrutura de Gerenciamento do Windows) no servidor proxy (computador de 64 bits).
- Instale os seguintes módulos do PowerShell no servidor proxy usando a janela do PowerShell:
  - Para instalar o módulo do Azure, execute o seguinte comando:

    Install-Module -Name AzureAD -Force
  - Para instalar o módulo ExchangeOnlineManagement, execute o seguinte comando:

    Install-Module -Name ExchangeOnlineManagement -Force

Observação: ao instalar módulos do PowerShell usando os comandos acima, uma versão mais recente dos módulos poderá ser instalada dependendo da versão do GA do componente disponível no repositório da Microsoft.

Criando um plano de backup do Exchange Online usando MA (Modern Authentication - Autenticação moderna):

Revise os Pré-requisitos antes de criar um plano usando a autenticação moderna.

Atribuindo a função de representação do aplicativo à conta de usuário especificada para o backup

Esta seção fornece informações sobre como adicionar a conta de backup ao grupo de funções Gerenciamento de detecção e sobre como atribuir a permissão de representação do aplicativo.

Para adicionar a função e o grupo necessários, execute uma das seguintes ações:

Método 1: usando o portal do Office 365

Siga estas etapas:

1. Efetue logon no portal do Office 365 como administrador ou com uma conta que possua as permissões de administrador global.

   A página central do administrador do Exchange é exibida.

2. Vá para **permissões** e, na lista suspensa **Adicionar**, clique duas vezes em **Gerenciamento de detecção**.

   A caixa de diálogo Gerenciamento de detecção é exibida.

   Observação: o membro do grupo de funções de gerenciamento de detecção poderá pesquisar nas caixas de correio da organização do Exchange quanto aos dados que atendem a critérios específicos.

3. Em **Funções**, clique no **+** para adicionar a função *ApplicationImpersonation*.

   A caixa de diálogo Selecionar uma função é exibida.

4. Na lista suspensa **Nome de exibição**, selecione **ApplicationImpersonation**.

   Observação: a função *ApplicationImpersonation* permite que os aplicativos representem usuários em uma organização para executar tarefas em nome do usuário.

5. Clique em **Adicionar** para adicionar a função ApplicationImpersonation e clique em **OK**.

6. Na caixa de diálogo Gerenciamento de detecção, em **Membros**, clique em **+** para adicionar a conta de backup como um membro.

   A caixa de diálogo Selecionar membros é exibida.

7. Na lista suspensa Nome, selecione a conta de backup, clique em **Adicionar** para adicionar o membro e, em seguida, clique em **OK**.

   A conta de backup selecionada é exibida em **Membros** na caixa de diálogo **Gerenciamento de detecção**.

8. Clique em **Salvar**.

Método 2: usando o PowerShell remoto

Siga estas etapas:

1. Conecte-se ao locatário do Exchange Online usando o PowerShell remoto. Para obter mais informações, consulte Conectar-se ao Exchange Online PowerShell.
2. Depois de conectado, para adicionar a conta de backup como membro do grupo de funções Gerenciamento de detecção, use o seguinte:

   `"Add-RoleGroupMember"`

   Por exemplo: *Add-RoleGroupMember "discovery management" -member userName@domain.onmicrosoft.com.*
3. Para atribuir a função de representação de aplicativo à conta de backup, use o seguinte:

   `"New-ManagementRoleAssignment"`

   Por exemplo: *New-ManagementRoleAssignment -Nome: impersonationAssignmentName -Função:ApplicationImpersonation - Usuário: "username@domain.onmicrosoft.com"*

A função *ApplicationImpersonation* e o grupo de membros são adicionados à conta de backup do Exchange Online.

Criar um plano de backup do Exchange Online

Um plano de backup inclui uma tarefa de backup que executa um backup dos itens de dados de email do Exchange Online (emails, itens de calendário, contatos etc.) e armazena os dados em um repositório de dados sem redução de redundância ou um repositório de dados de redução de redundância. Além disso, esse plano de backup permite que o UDP detecte e especifique os grupos do Exchange Online para os quais uma tarefa de backup é executada. Cada tarefa consiste em parâmetros que definem a origem, o destino, a programação e outros detalhes de backup.

Siga estas etapas:

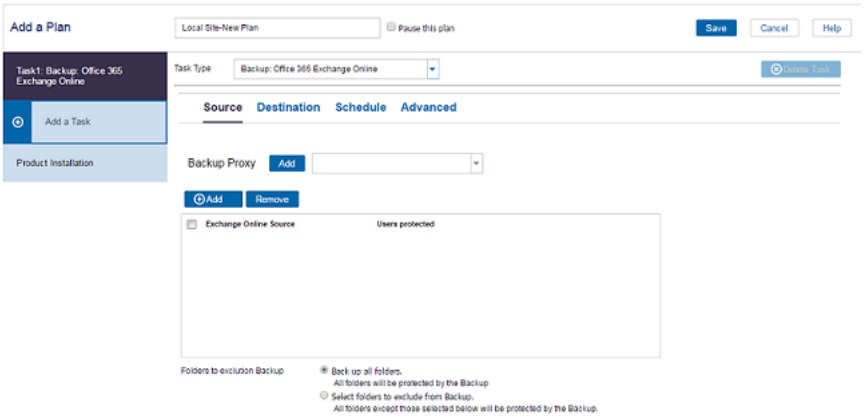
1. Clique na guia **Recursos** no Console.
2. No painel à esquerda, navegue para **Planos** e clique em **Todos os planos**.

   Se tiver criado os planos anteriores, esses planos serão exibidos no painel central.
3. No painel central, clique em **Adicionar um plano**.

   A caixa de diálogo **Adicionar um plano** abre.
4. Digite o nome do plano.
5. (Opcional) Selecione a caixa de seleção **Pausar este plano**.

   O plano não será executado até que você desmarque a caixa de seleção para retomar o plano.

   Observação: se um plano for pausado, nenhuma tarefa em andamento será pausada, mas todas as tarefas programadas correspondentes associadas a esse plano serão pausadas. No entanto, você pode executar uma tarefa manualmente. Por exemplo, você pode executar manualmente a tarefa de backup e a tarefa de replicação para um nó mesmo que o respectivo plano esteja pausado. Nesse caso, a tarefa seguinte da tarefa sob demanda (manual) não será executada. Por exemplo, há uma tarefa de replicação após uma tarefa de backup sob demanda, a tarefa de replicação não será executada para a tarefa de backup sob demanda. É necessário executar manualmente a tarefa de replicação. Quando você retomar o plano, as tarefas pendentes não são retomadas imediatamente. Depois de retomar o plano, as tarefas pendentes serão executadas no próximo horário programado.
6. Na lista suspensa Tipo de tarefa, selecione **Backup: Office 365 Exchange Online**.



Agora especifique os detalhes de Origem, Destino, Programação e Avançado.

Especificar a origem

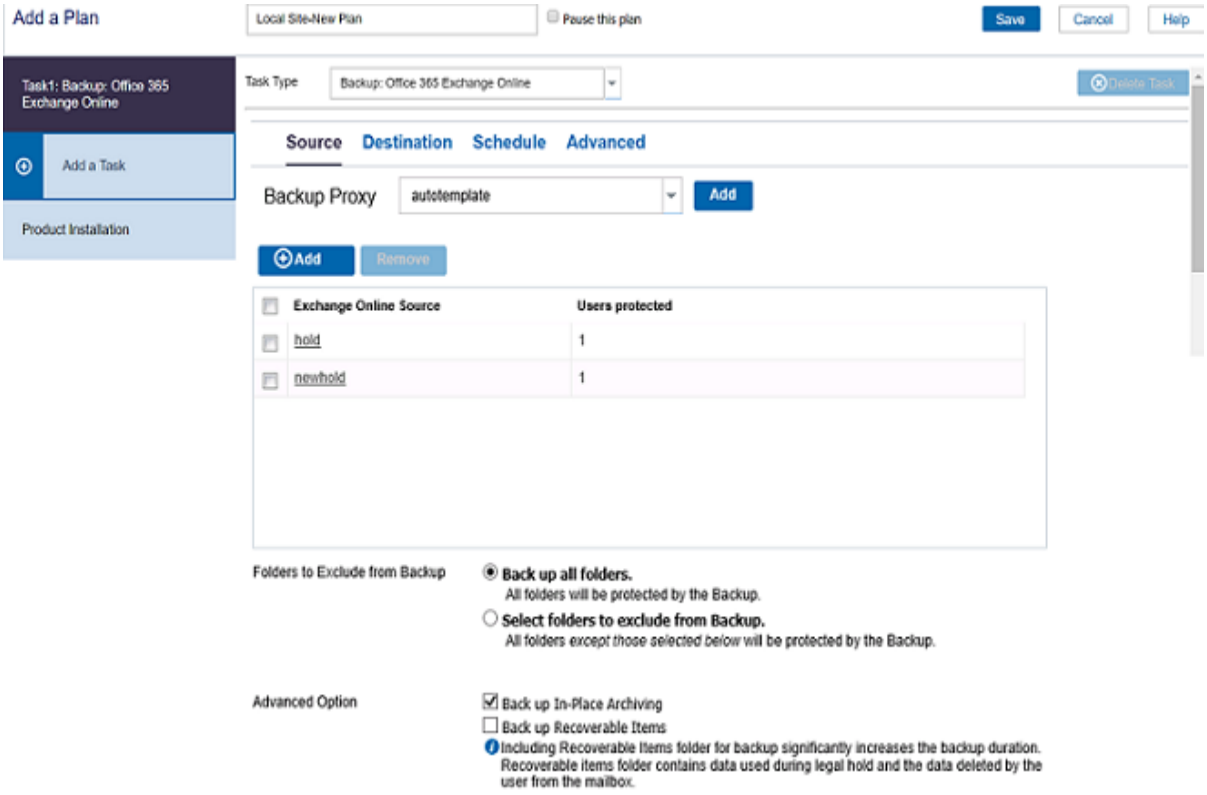
A página Origem permite especificar os nós de origem do Exchange Online que você deseja proteger. É possível selecionar mais de um nó de origem do Exchange Online em um plano. Caso não tenha adicionado nós no console, você pode adicionar nós de origem do Exchange Online a partir da página Origem.

Observação: é possível salvar um plano sem adicionar nós de origem, mas o plano só será implantado se você adicionar os nós.

Você também pode gerenciar os nós do Exchange Online usando o suporte a caixa de correio de pasta pública para a proteção do Exchange Online.

Siga estas etapas:

1. Clique na guia **Origem**.



2. Para o proxy de backup, execute um dos seguintes procedimentos:
   - Na lista suspensa, selecione um proxy de backup existente.
   - Para adicionar um novo proxy de backup, ao lado da lista suspensa, clique em **Adicionar**.
3. Adicione o nó do Exchange Online usando uma das seguintes opções:

   Método 1

a. Clique em **Adicionar** e em **Selecionar as origens a serem protegidas no Arcserve UDP**.

   A caixa de diálogo Adicionar nós ao plano é exibida.

b. Selecione um nó e clique em **Conectar**.

   Observação: também é possível procurar os nós do Exchange Online que você deseja proteger na **Pesquisa**.

c. Marque a caixa de seleção **Proteger todas as origens do Office 365 Exchange** para proteger todas as contas do Exchange Online em todas as páginas.

   Observação: para adicionar à lista protegida todas as contas do Exchange Online, clique na seta para a direita (>).

   As contas do Microsoft Exchange Online que você selecionar são adicionadas.

Método 2

- Clique em **Adicionar** e, em seguida, clique em **Adicionar origem do Exchange Online**.

  O diálogo Adicionar nós a um plano é exibido.

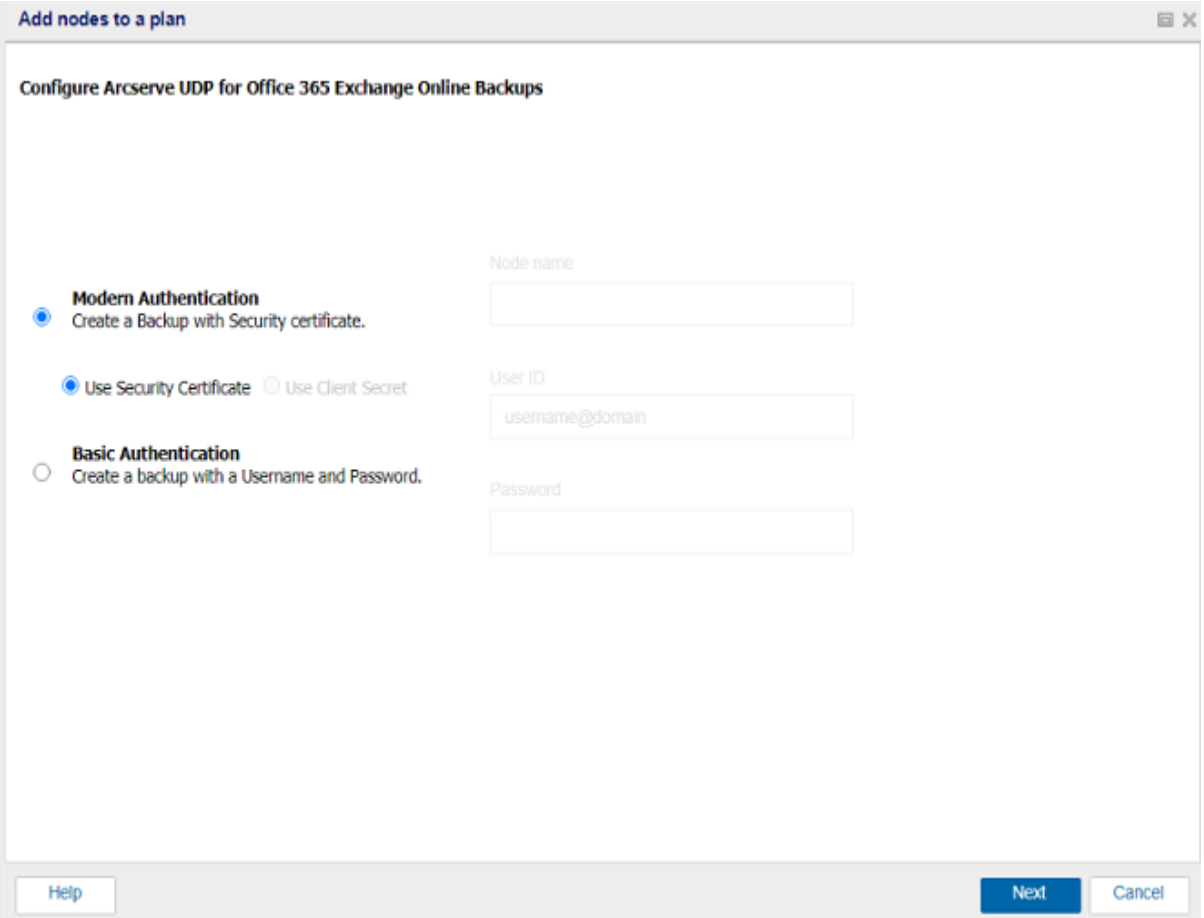
  Observação: diferentemente de outros nós, não é possível adicionar o nó do Exchange Online na página **Todos os nós**. Só é possível adicionar um nó do Exchange Online em um plano ou quando você modificar um plano.

  Vários nós do Exchange Online podem usar a mesma conta de usuário (conta de serviço) do Exchange Online.

4. Para aplicar a autenticação, siga um destes procedimentos:

Autenticação moderna

Para a autenticação moderna, você pode executar um backup usando o certificado de segurança.



Usar certificado de segurança

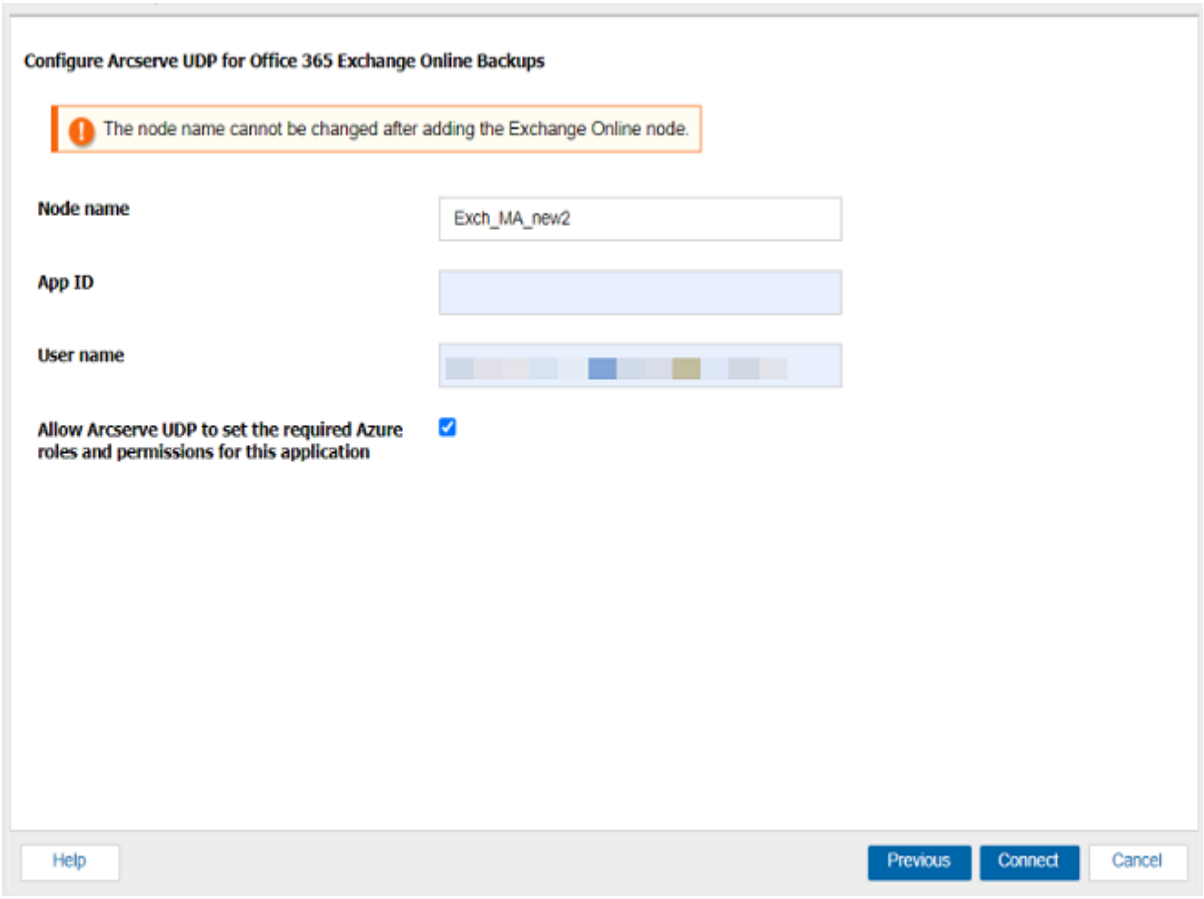
Observação: por padrão, o plano de backup seleciona **Usar certificado de segurança** para a autenticação moderna.

Siga estas etapas:

a. Para autenticar o aplicativo UDP com certificados de segurança, consulte Fazendo download do certificado do UDP e carregando-o no Azure.

b. Digite os seguintes detalhes:

- Nome do nó
- ID do aplicativo
- Nome de usuário



c. Para aplicar as permissões de API automaticamente, marque a caixa de seleção **Permitir que o Arcserve UDP defina as permissões de API necessárias para este aplicativo**.

   Observação: para aplicar as permissões manualmente sem usar a função de administrador global/de empresa, consulte Configurando as permissões da API manualmente sem usar a função de administrador global/de empresa.

d. Clique em **Conectar**.

Observações:

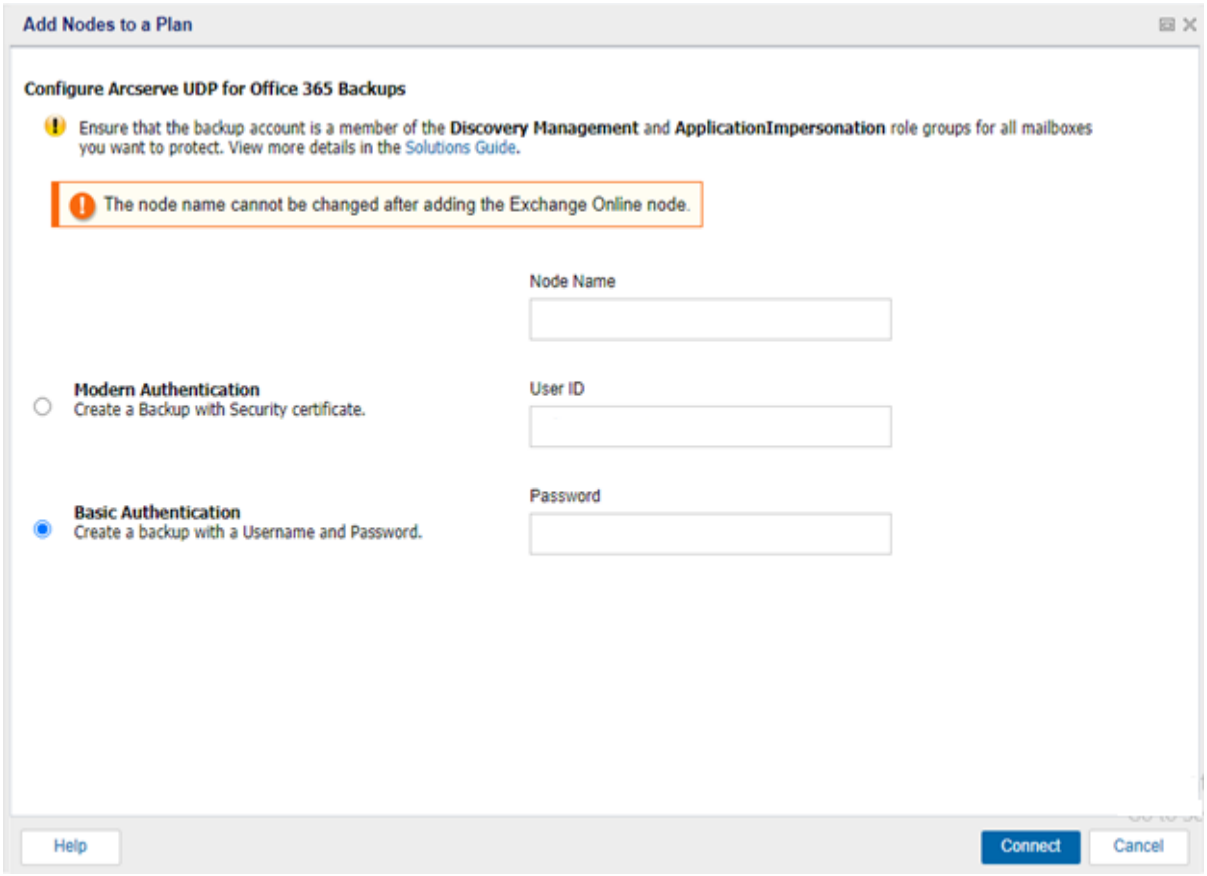
- O nome do nó do Exchange Online não pode ser alterado após a adição do nó.
- Digite o nome de usuário da conta de backup do Exchange Online que atender aos pré-requisitos em **Nome de usuário do administrador**.
- A Autenticação moderna não se aplica ao seguinte:

- Os clientes que usam o Microsoft 365 (Office 365) para suas instâncias do Arcserve Cloud Hybrid ou o Arcserve Cloud Backup para Office 365, que foi criado antes de 18 de outubro de 2020, não poderão usar a Autenticação moderna.
- Os clientes que continuam a usar a autenticação básica.

Autenticação básica

Para a autenticação básica, para continuar com o backup, forneça as seguintes informações e clique em **Conectar**:

- Nome do nó
- ID do usuário
- Senha



Observação: a atualização ou alteração da conta de usuário pode mudar o número de caixas de correio protegidas. Você precisa verificar se as contas de serviço novas ou atualizadas têm direitos de representação para as caixas de correio serem protegidas.

5. Para proteger as caixas de correio do Exchange Online, siga um destes procedimentos:

   - Para proteger todas as caixas de correio e grupos do Exchange Online, marque a caixa de seleção **Proteger todas as origens do Office 365 Exchange**.

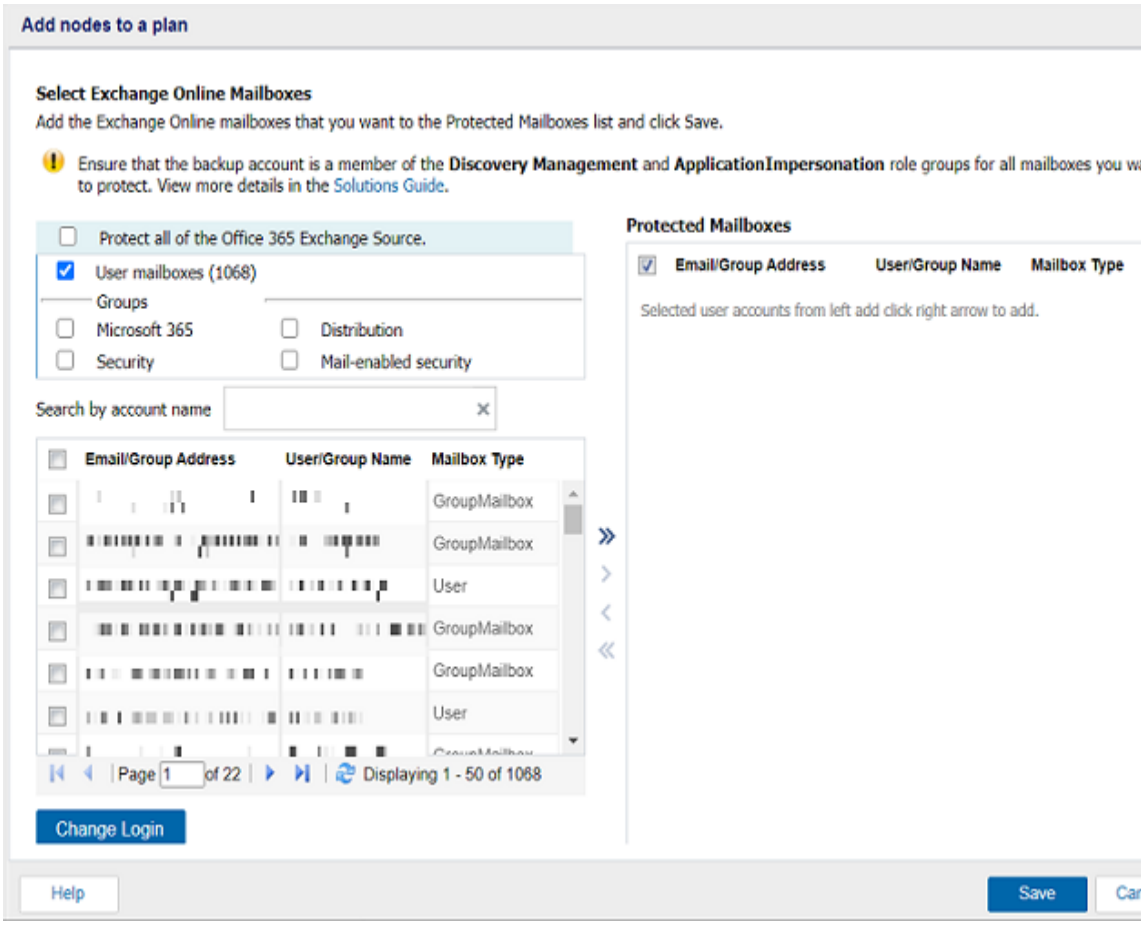
     Observação: essa opção é selecionada automaticamente por padrão quando a tela Selecionar caixas de correio do Exchange Online é exibida.

   - Para Caixas de correio do usuário, siga estas etapas:

     a. Marque a caixa de seleção **Caixas de correio do usuário**.

        Uma lista de caixas de correio do usuário é exibida.

     b. (Opcional) Para pesquisar uma conta na lista, no campo Pesquisar por nome de conta, digite o nome da conta.



     c. Na lista de caixas de correio do usuário, selecione as caixas de correio que deseja proteger.

d. Clique na seta para a direita (>) para mover as caixas de correio selecionadas para a lista Caixas de correio protegidas.

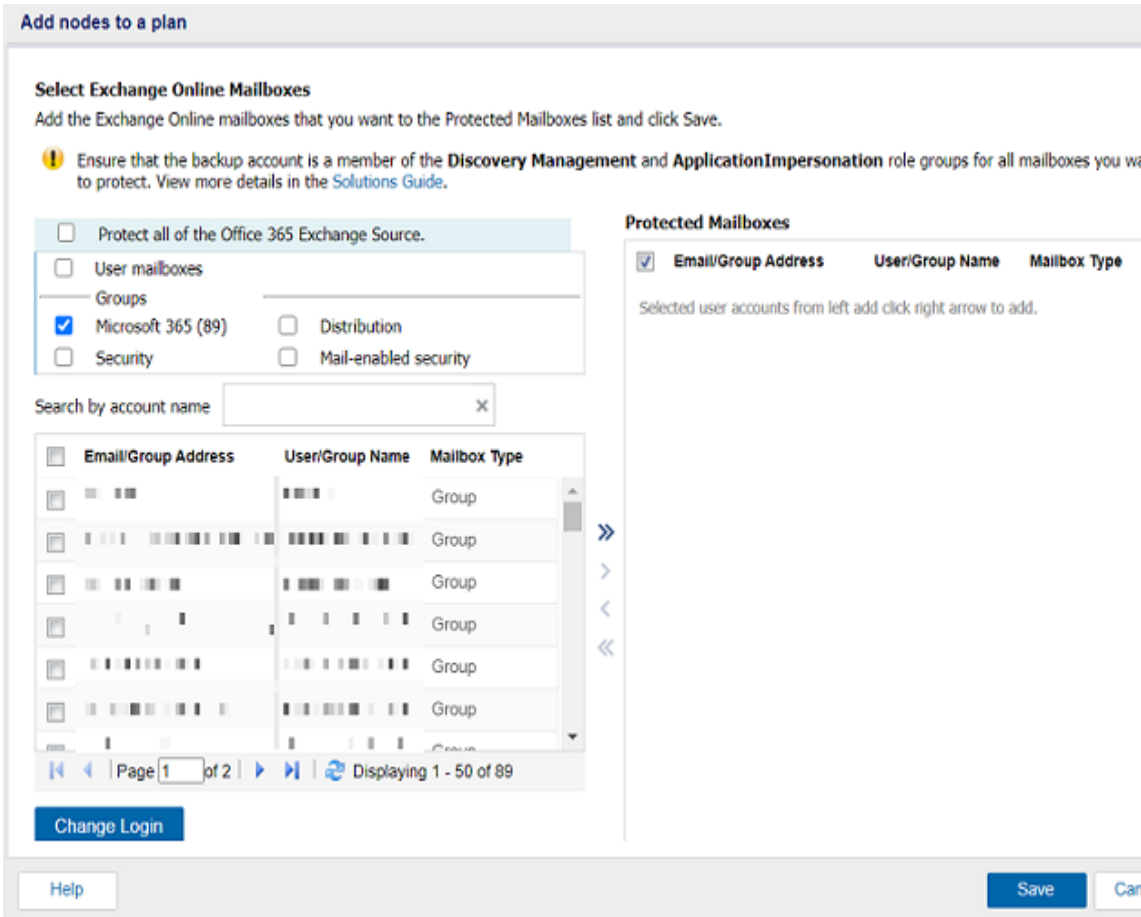
- Para Grupos, siga estas etapas:

a. Marque a caixa de seleção **Microsoft 365**.

Uma lista de grupos é exibida.

Observação: se desejar selecionar grupos juntamente com subgrupos, como **Distribuição**, **Segurança** ou **Segurança ativada por email**, marque a caixa de seleção **Microsoft 365** e, em seguida, marque a caixa de seleção de um subgrupo, conforme necessário.

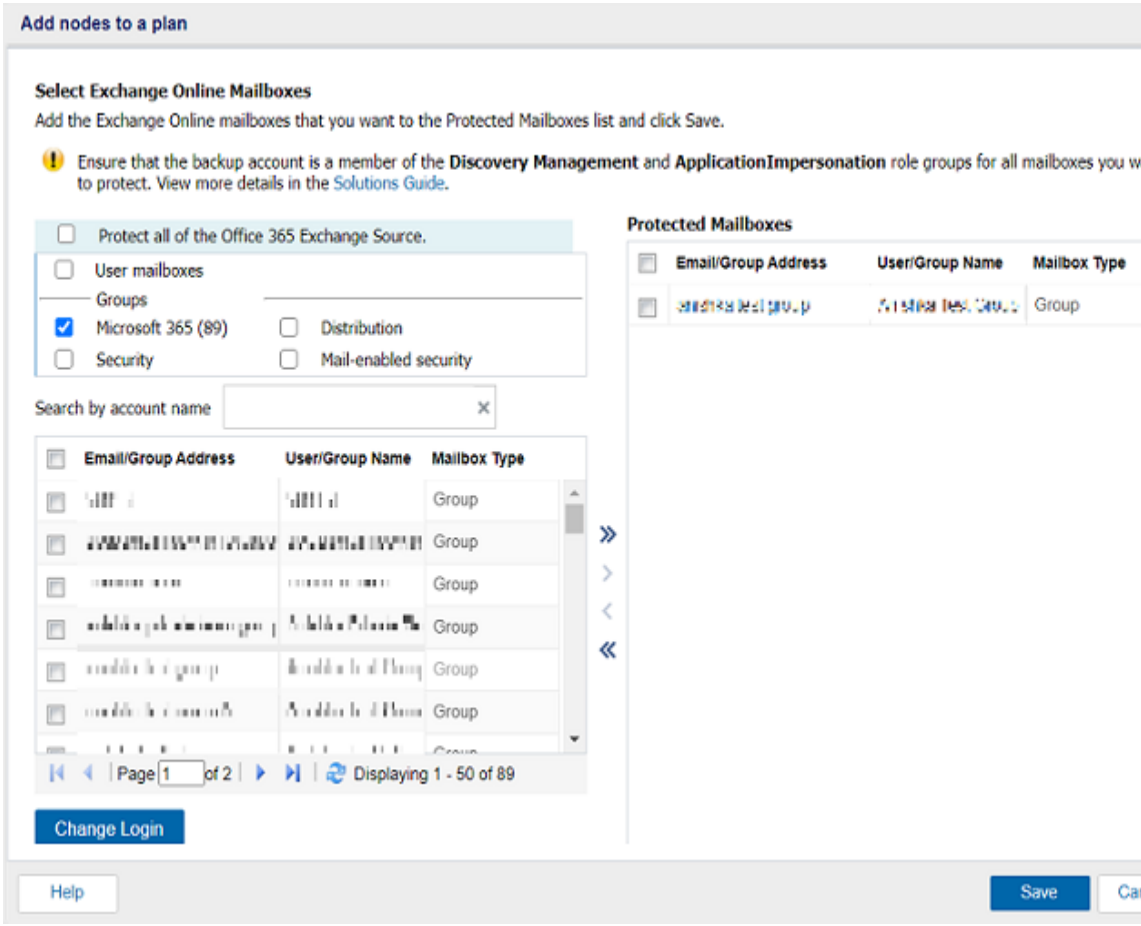
b. (Opcional) Para pesquisar uma conta na lista, no campo Pesquisar por nome de conta, digite o nome da conta.



c. Na lista de grupos, selecione os grupos que deseja proteger.

d. Clique na seta para a direita (>) para mover os grupos sele-

cionados para a lista Caixas de correio protegidas.



6. Clique em **Salvar**.
7. Na guia Origens, vá para **Pastas a serem excluídas do backup** e marque a caixa de seleção desejada.
8. Em Opção avançada, marque a caixa de seleção desejada.
   - Para permitir que a proteção do Exchange Online ofereça suporte a uma caixa de correio de arquivo morto, marque a caixa de seleção **Fazer backup do arquivo morto local**.

     Observação: para obter mais informações sobre caixa de correio de arquivo morto, clique neste link.
   - Marque a caixa de seleção **Fazer backup dos itens recuperáveis** para permitir a proteção da caixa de correio que ativa o recurso Retenção local ou Retenção de litígio.

     Observação: para Retenção local e Retenção de litígio do arquivo morto do Exchange Online, clique neste link.

Observação: para ativar ambos os recursos na caixa de correio ao mesmo tempo, de modo a fazer backup dos itens recuperáveis presentes na caixa de correio de arquivo morto, selecione as opções **Fazer backup do arquivo morto local** e **Fazer backup dos itens recuperáveis**.

Especificar o destino

O destino é o local onde você armazena os dados de backup. É necessário, no mínimo, especificar o destino para salvar o plano.

Siga estas etapas:

1. Clique na guia **Destino**.
2. Selecione a opção **Servidor de ponto de recuperação do Arcserve UDP. O servidor de ponto de recuperação do Arcserve UDP** especifica que o destino de backup é um servidor de ponto de recuperação. Se você selecionar essa opção, os dados serão armazenados como pontos de recuperação. Não é possível armazenar dados como conjuntos de dados de recuperação.
3. Forneça os detalhes a seguir:
   a. Selecione um servidor do ponto de recuperação.
   b. Selecione um repositório de dados de redução de redundância ou de não redução de redundância. A lista exibe todos os repositórios de dados criados no servidor do ponto de recuperação especificado.
   c. Forneça uma senha da sessão. a senha da sessão é opcional quando o destino de backup é um repositório de dados do RPS não criptografado.
   d. Confirme a senha da sessão.

O destino é especificado.

Especificar a programação

A página Programar permite definir uma programação para o backup e para que as funções Mesclar e Acelerar sejam repetidas em intervalos específicos. Após definir uma programação, as tarefas são executadas automaticamente de acordo com a programação. É possível adicionar várias programações e fornecer configurações de retenção.

Uma Programação de backup se refere a programação regular que é repetida várias vezes ao dia, com base no número de horas ou de minutos selecionado. Além da programação regular, uma programação de backup também fornece opções para adicionar programações diária, semanal e mensal.

Observação: para obter mais informações sobre as configurações de retenção e programação, consulte Entendendo a programação avançada e retenção.

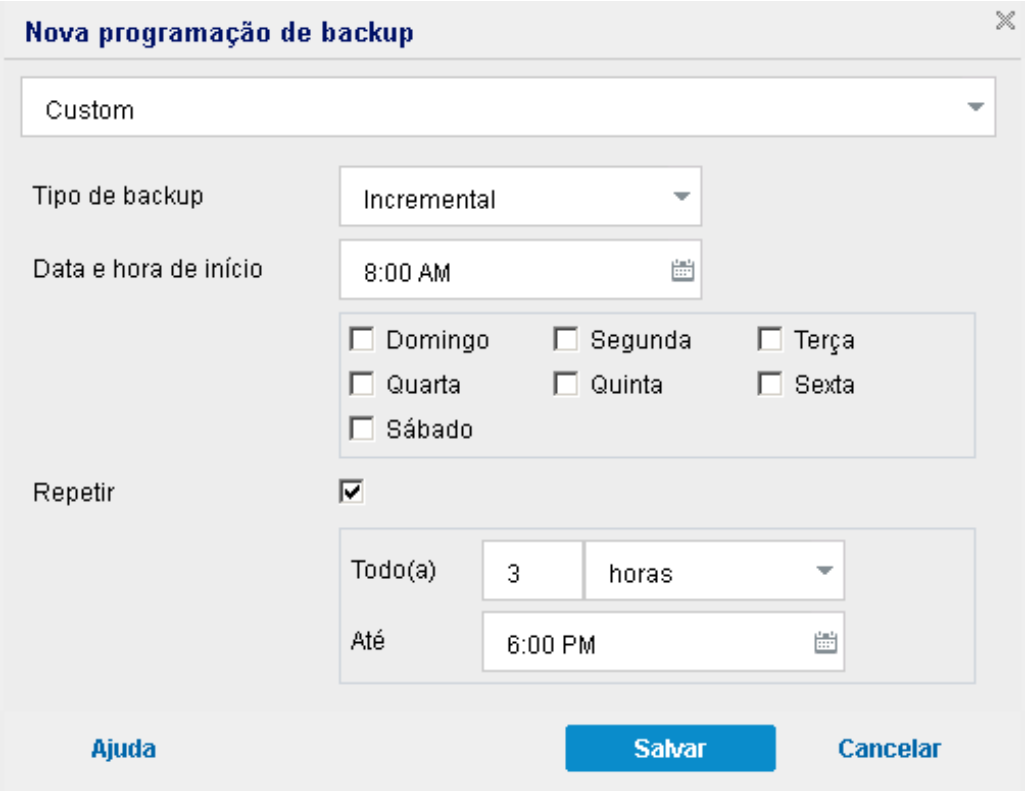
Siga estas etapas:

1. Adicionar programações de backup, mesclagem e acelerador.

   Adicionar programação de backup

   a. Clique em **Adicionar** e selecione **Adicionar programação de backups.**

      A caixa de diálogo **Nova programação de backup** é aberta.



   b. Selecione uma das seguintes opções:

Personalizado

Especifica a programação de backup que se repete várias vezes por dia.

Diário

Especifica a programação de backup que ocorre uma vez por dia. Por padrão, todos os dias da semana estão selecionados para o backup diário. Se não desejar executar a tarefa de backup em um dia específico, desmarque a caixa de seleção correspondente àquele dia da semana.

Semanal

Especifica a programação de backup que ocorre uma vez por semana.

Mensal

Especifica a programação de backup que ocorre uma vez por mês.

c. Selecione o tipo de backup.

Completo

Especifica a programação de backups para backups completos. Conforme programado, o Arcserve UDP executa um backup completo de todos os blocos usados do computador de origem. Um backup completo em geral, consome tempo, dependendo do tamanho do backup.

Incremental

Especifica a programação de backups para backups incrementais.

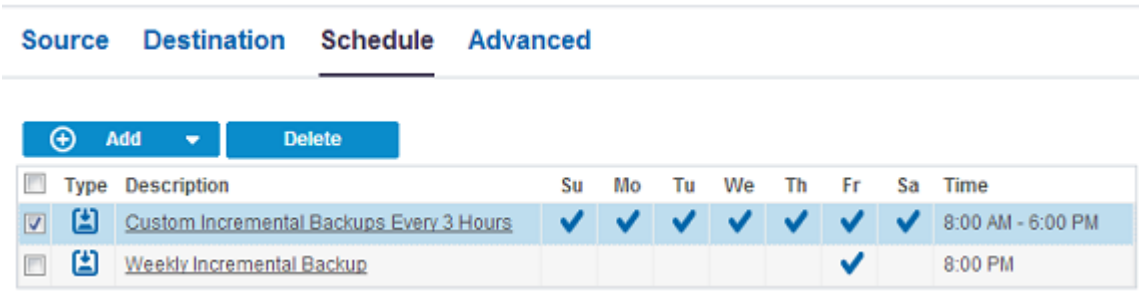
Conforme programado, o Arcserve UDP faz backup incremental apenas dos blocos que foram alterados após o último backup realizado com êxito. As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a executar um backup.

d. Especifique a hora de início do backup.

e. (Opcional) Marque a caixa de seleção de **Repetição** e especifique a programação a ser repetida.

f. Clique em **Salvar**.

A programação de backup é especificada e aparece na página de **Programação**.



Adicionar Programação de mesclagem

a. Clique em **Adicionar** e selecione **Adicionar programação de mesclagem.**

   A caixa de diálogo **Adicionar nova programação de mesclagem** é aberta.

b. Especifique a hora de início para iniciar a tarefa de mesclagem.

c. Especificar **Até** para especificar uma hora de término para a tarefa de mesclagem.

d. Clique em **Salvar**.

A programação de mesclagem é especificada e aparece na página de **Programação**.

Adicionar programação de acelerador

a. Clique em **Adicionar** e selecione **Adicionar programação de acelerador.**

   A caixa de diálogo **Adicionar nova programação do acelerador** é aberta.

b. Especifique o limite de taxa de transferência em unidades de MB por minuto.

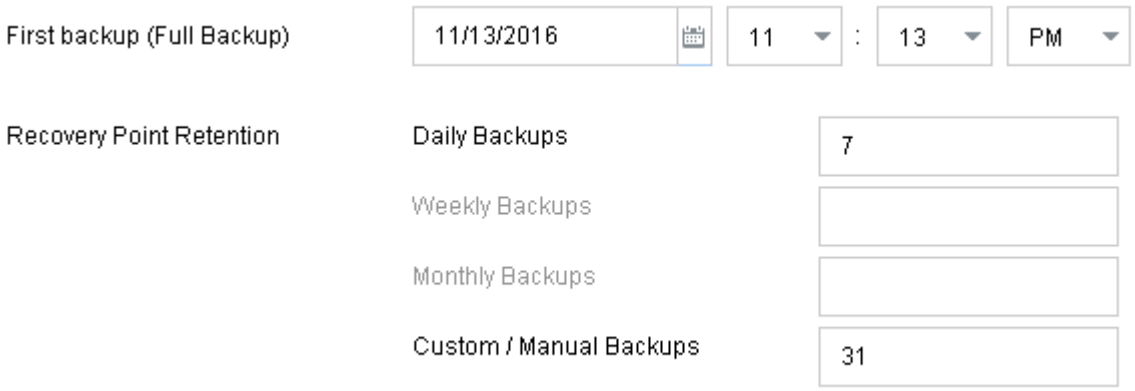
c. Especifique a hora de início para iniciar a tarefa de taxa de transferência de backup.

d. Especifique **Até** para especificar um horário de término para a tarefa de taxa de transferência.

e. Clique em **Salvar**.

A Programação de acelerador é especificada e exibida na página **Programar**.

2. Especifique a hora de início do backup programado.



3. Especifique as configurações de retenção de pontos de recuperação para programação diária, semanal e mensal.

   Essas opções serão ativadas se tiver adicionado a programação de backup correspondente. Se você modificar as configurações de retenção desta página, as alterações serão refletidas na caixa de diálogo **Programação de backup**.

   A programação é especificada.

Noções básicas sobre a programação avançada e retenção

A opção de programação permite especificar uma programação personalizada, uma programação diária/semanal/mensal ou ambas. Na programação personalizada, é possível configurar a programação de backups para cada dia da semana ou adicionar até quatro programações de backup em cada dia. É possível escolher um dia específico da semana e criar uma janela para definir quando executar o backup e em que frequência.

Programação	Tarefa com suporte	Comentários
Backup	Tarefa de backup	Definir janelas de tempo para a execução de tarefas de backup.
Limitação de backup	Tarefa de backup	Definir janelas de tempo para controlar a velocidade de backup.
Mesclar	Tarefa de mesclagem	Definir quando executar tarefas de mesclagem.
Programação diária	Tarefa de backup	Definir quando executar tarefas do backup diário.
Programação semanal	Tarefa de backup	Definir quando executar tarefas do backup semanal.
Programação mensal	Tarefa de backup	Definir quando executar tarefas do backup mensal.

Também é possível especificar as configurações de retenção para os pontos de recuperação.

Observação: as configurações de retenção devem ser definidas em cada plano para controlar como os dados dos nós atribuídos a esse plano são retidos no repositório de dados de destino.

As programações para backups diários/semanais/mensais são independentes para a programação personalizada e umas das outras. É possível configurar para executar somente o backup diário, semanal ou mensal, sem configurar a Programação personalizada.

Programação de tarefas de backup

É possível adicionar quatro janelas de tempo por dia na programação do backup. Uma janela de tempo é válida das 00:00 às 23:59. Não é possível especificar uma janela de tempo das 18:00 às 6:00. Nesses casos, você deve especificar manualmente duas janelas de tempo diferentes.

Para cada janela de tempo, a hora de início é inclusiva e a hora de término é exclusiva. Por exemplo, você configurou para executar o backup incremental em intervalos de uma hora entre as 6:00 e as 9:00. O backup será iniciado às 6:00. Isso significa que o backup será executado às 6h00, 7h00 e 8h00, mas NÃO às 9h00.

Observação: se você deseja executar a tarefa de backup várias vezes até o fim do dia, defina a programação para até 0h00. Por exemplo, para executar a tarefa de backup a cada 15 minutos o dia inteiro, defina a programação como das 0h00 às 00h00, a cada 15 minutos.

Programação do acelerador de backup

A programação de aceleração do backup permite controlar a velocidade da taxa de transferência de backup o que, por sua vez, controla o uso de recursos (E/S de disco, CPU, largura de banda de rede) do servidor cujo backup está sendo feito. Isso é útil quando se não quiser afetar o desempenho do servidor durante o horário comercial. É possível adicionar quatro janelas de tempo por dia na sua programação de aceleração do backup. Para cada janela de tempo, é possível especificar um valor, em MB por minuto. Esse valor será usado para controlar a taxa de transferência do backup. Os valores válidos variam entre 1 MB/minutos a 99999 MB/minutos.

Se uma tarefa de backup estende seu tempo especificado, o limite de aceleração será ajustado de acordo com o tempo especificado. Por exemplo, você definiu o limite de aceleração de backup como 500 MB/minuto das 8:00 às 20:00 e 2500 MB/minuto das 20:00 às 22:00. Se uma tarefa de backup iniciar às 19h00 e for executada durante três horas, das 19h00 às 20h00 o limite de aceleração será de 500 MB/minuto e das 20h00 às 22h00, o limite de aceleração será 2500 MB/minuto.

Se não definir nenhuma programação do backup e programação da taxa de transferência do backup, o backup será executado o mais rápido possível.

Mesclar a programação

Permite mesclar pontos de recuperação com base na programação fornecida.

Considere os seguintes pontos para a tarefa de mesclagem:

- A qualquer momento apenas uma tarefa de mesclagem pode ser executada para um nó.
- Se uma tarefa de mesclagem iniciar, ela precisará ser concluída antes que a próxima tarefa de mesclagem seja iniciada. Isso significa que, se um ou mais conjuntos de pontos de recuperação forem mesclados, não será possível adicionar o

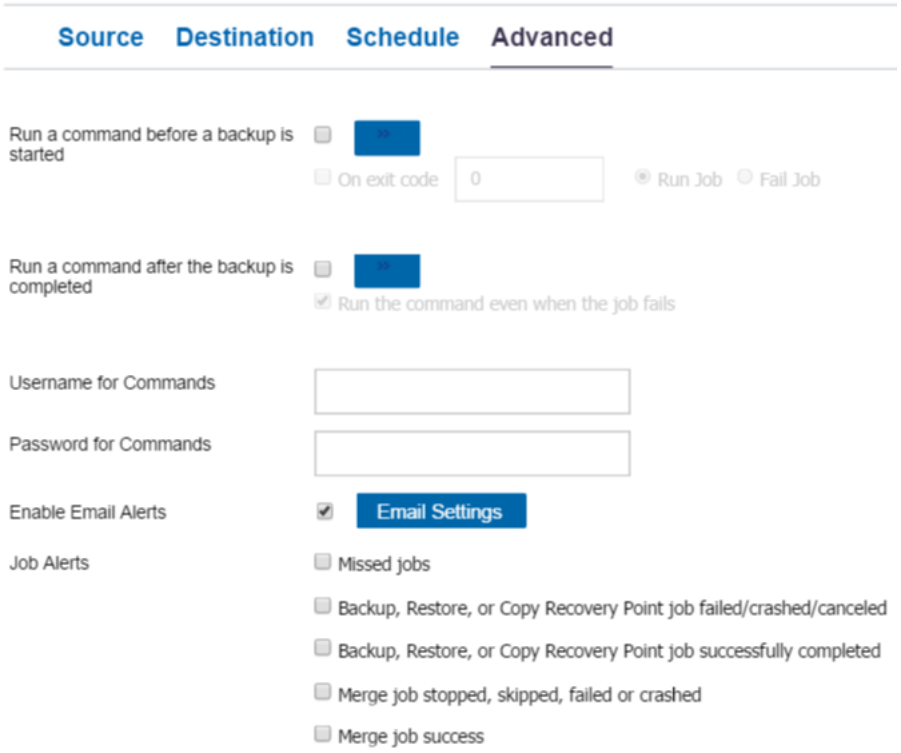
novo ponto de recuperação a este processo de mesclagem, até que o processo de mesclagem do conjunto atual de ponto de recuperação seja concluído.

- Se uma tarefa de mesclagem estiver processando mais de um conjunto de pontos de recuperação (por exemplo, conjunto [1~4], conjunto [5~11] e conjunto [12~14]; são três conjuntos) o servidor de ponto de recuperação processará esses conjuntos, um por um.
- Se uma tarefa de mesclagem é retomada após um intervalo, a tarefa detectará em que ponto ela foi pausada e continuará a mesclagem a partir do ponto de pausa.

Especificar as configurações avançadas

A guia **Avançado** permite especificar algumas configurações avançadas para a tarefa de backup. As configurações avançadas incluem o fornecimento da localização dos scripts e as configurações de email.

A imagem a seguir mostra a guia **Avançado**:



Siga estas etapas:

1. Especifique os seguintes detalhes.

   Executar um comando antes do início do backup

   Permite a execução de um script antes de iniciar a tarefa de backup. Especifique o caminho em que o script está armazenado dentro do nó do proxy. Clique em **No código de saída** e especifique o código de saída para **Executar tarefa** ou **Tarefa com falha**. **Executar a tarefa** indica que a tarefa de backup continuará quando o script retornar o código de saída. **Tarefa com falha** indica que a tarefa de backup será interrompida quando o script retornar o código de saída.

   Executar um comando após a conclusão do backup

   Permite executar um script depois que a tarefa de backup foi concluída. Especifique o caminho completo onde o script está armazenado.

   Executar um comando, mesmo quando a tarefa falhar

Se essa caixa de seleção for selecionada, o script especificado em **Executar um comando após a conclusão do backup** é executado mesmo quando a tarefa de backup falha. Caso contrário, o script é executado somente quando a tarefa de backup é concluída com êxito.

Nome de usuário para comandos

Permite especificar o nome de usuário para executar os comandos.

Senha para comandos

Permite especificar a senha para executar os comandos.

Ativar alertas por email

Permite ativar alertas por email. É possível especificar configurações de email e os tipos de alertas que você deseja receber por email. Ao selecionar esta opção, as seguintes opções serão ativadas para a seleção.

Configurações de email

Permite configurar as definições de email. Clique em **Configurações de email** e configure o servidor de email e os detalhes do servidor proxy. Para obter mais informações sobre como configurar Configurações de email, consulte o tópico Configuração de email e alerta.

Alertas de tarefa

Permite selecionar os tipos de emails de alerta de tarefas que deseja receber.

2. Clique em **Salvar**.

Observação: quando você seleciona um nó como origem de backup ou proxy de backup, o Arcserve UDP verifica se o agente está instalado no nó do proxy e se é a versão mais recente. Em seguida, o Arcserve UDP exibe uma caixa de diálogo de verificação que lista todos os nós que possuem uma versão antiga do agente ou que não tem o agente instalado. Para instalar/atualizar o agente nesses nós, selecione o método de instalação e clique em **Salvar**.

As alterações são salvas e uma marca de seleção verde aparece ao lado do nome da tarefa. A página do plano é fechada.

Observação: se precisar adicionar outra tarefa, você deverá selecionar o plano na guia **Recursos** e modificá-lo. Para modificar o plano, clique no plano do painel central. O plano é exibido e será possível modificá-lo. É possível adicionar as tarefas **Copiar ponto de recuperação**, **Cópia em fita**, **Replicar** e **Replicar de um RPS remoto**como tarefas de acompanhamento.

O plano é automaticamente implantado ao nó do servidor proxy.

O plano de backup do exchange online para o servidor proxy é criado. O backup é executado de acordo com a programação que você configurou na guia **Programar**. Também é possível fazer backup manual quando desejado.

(Opcional) Executar um backup manual

Normalmente, com base nas configurações de programação aplicadas, os backups são executados automaticamente. Além do backup programado, um backup manual fornece a opção de fazer backup dos nós de acordo com a necessidade. Por exemplo, se repetir a programação para backups completos e incrementais e desejar fazer grandes alterações em seu computador, você deverá executar um backup manual imediato sem esperar até que ocorra o próximo backup programado.

Para executar um backup manual dos nós do Exchange Online, siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel esquerdo, navegue para **Nós** e clique em **Todos os nós**.

   Os nós Exchange Online são exibidos no painel central.
3. Selecione os nós do Exchange Online (por exemplo, Caixa de correio@<nomedaorganização.com>) dos quais você deseja fazer backup e certifique-se de ter um plano atribuído a ele. O nome do nó é a conta usada durante a adição do nó do Exchange Online e de sua conexão.
4. Clique com o botão direito do mouse no nó e selecione **Fazer backup agora**.

   A caixa de diálogo Fazer backup agora é exibida.
5. Selecione o tipo de backup que deseja executar e clique em **OK**.

   A caixa de diálogo Informações do andamento é exibida.
6. Aguarde até que a tarefa de backup seja concluída e clique em **OK**.
7. Para monitorar as tarefas de backup, navegue até **tarefas** > **Tarefas em andamento**.

   Aguarde até a conclusão da tarefa de backup.

   O backup manual é realizado com êxito.

Para executar um backup manual do plano do Exchange Online, siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel esquerdo, navegue para **Planos** e clique em **Todos os planos**.

   Os planos de backup do Exchange Online são exibidos no painel central.
3. Selecione o plano do qual você deseja fazer backup e certifique-se de que tenha um plano atribuído a ele.
4. Clique com o botão direito do mouse no plano e selecione **Fazer backup agora**.

A caixa de diálogo Fazer backup agora é exibida.

5. Selecione o tipo de backup que deseja executar e clique em **OK**.

   A caixa de diálogo Informações do andamento é exibida.

6. Aguarde até que a tarefa de backup seja concluída e clique em **OK**.
7. Para monitorar as tarefas de backup, navegue até **tarefas** > **Tarefas em andamento**.

   Aguarde até a conclusão da tarefa de backup.

   O backup manual é realizado com êxito.

Verificar o backup

Para verificar a tarefa de backup, confirme se você criou com êxito o plano de backup. Depois de verificar se o plano está criado com êxito, confirme se a tarefa de backup é executada conforme o programado. É possível verificar o status das tarefas de backup na guia **Tarefas**.

Siga estas etapas para verificar os planos:

1. Clique na guia **Recursos**.
2. No painel esquerdo, navegue para **Nós** e clique em **Todos os nós**.

   Uma lista de todos os nós é exibida no painel central.
3. Verifique se os planos são mapeados com nós.

Siga um destes métodos para verificar as tarefas de backup:

Método 1

1. Clique na guia **Tarefas**.
2. No painel à esquerda, clique em **Todas as tarefas concluídas**.

   O status de cada tarefa é incluído no painel central.
3. Verifique se a tarefa de backup é concluída com êxito.

   A tarefa de backup é verificada.

Método 2

1. Clique na guia **Tarefas**.
2. No painel esquerdo, clique em **Tarefas concluídas com êxito**.

   A lista de tarefas de backup concluídas é exibida no painel central.
3. Clique na tarefa que você deseja verificar.

   O painel direito é atualizado.
4. Em Detalhes da tarefa, clique no hiperlink **Exibir logs**.
5. Verifique se a tarefa de backup é concluída com êxito.

   A tarefa de backup é verificada.

Fazer a configuração da autenticação multifator

Quando uma organização tiver a autenticação multifatorial (MFA) ativada para os usuários, use a Autenticação moderna para adicionar nós.

Observação: embora a autenticação básica esteja ativada no locatário, você pode usar a Autenticação moderna para adicionar nós. Para obter mais informações sobre como adicionar nós a um plano usando a Autenticação moderna, consulte Autenticação moderna.

Como criar um plano de backup do SharePoint Online

A proteção do SharePoint é usada para fazer backup e restaurar sites e itens de lista do Microsoft SharePoint Online. O SharePoint Online é um dos produtos principais do Microsoft Office 365. Para proteger seu conteúdo do SharePoint, é necessário criar um plano.

O que fazer a seguir?

1. Verificar os pré-requisitos e as considerações
2. Criar um plano de backup do SharePoint Online
3. Verificar o plano de backup
4. Fazer a configuração da autenticação multifator

Verificar os pré-requisitos

Revise os seguintes pré-requisitos antes de criar um plano de backup do SharePoint Online.

Criando um plano de backup do SharePoint Online:

Pré-requisitos:

A conta de backup é integrante dos grupos de administradores da coleção do site ou é atribuída à função de *Administrador do SharePoint*.

Para adicionar uma conta ao grupo Administradores da coleção de sites, consulte o link.

Criando um plano de backup do SharePoint Online usando BA (Basic Authentication - Autenticação básica):

Revise os seguintes pré-requisitos:

- Instale o PowerShell versão 5.1 ou superior (parte da WMF, Windows Management Framework - Estrutura de Gerenciamento do Windows) no servidor proxy (computador de 64 bits).
- Instale os seguintes módulos do PowerShell no servidor proxy usando a janela do PowerShell:
  - Para instalar o módulo do Azure, execute o seguinte comando:

    Install-Module -Name AzureAD -Force
  - Para instalar o módulo ExchangeOnlineManagement, execute o seguinte comando:

    Install-Module -Name ExchangeOnlineManagement -Force

  Observação: ao instalar módulos do PowerShell usando os comandos acima, uma versão mais recente dos módulos poderá ser instalada dependendo da versão do GA do componente disponível no repositório da Microsoft.

Criando um plano de backup do SharePoint Online usando MA (Modern Authentication - Autenticação moderna):

Revise os Pré-requisitos antes de criar um plano usando a autenticação moderna.

Criar um site pessoal no SharePoint

Esta seção fornece informações sobre como criar um site pessoal no SharePoint.

Siga estas etapas:

1. Vá para a página de logon da Microsoft e faça logon na conta de administrador do Microsoft Office 365.
2. Navegue até a página **Central de administração do SharePoint** e, em seguida, no painel esquerdo, clique em **Mais recursos**.
3. Na página de coleções de sites clássicos, clique em **Abrir**.

   A página Coleção de sites é exibida.
4. Na página Coleção de sites, clique em **Novo** > **Coleção de sites privados**.

   A caixa de diálogo da nova coleção de sites é exibida.
5. Na caixa de diálogo da nova coleção de sites, forneça os seguintes detalhes e clique em **OK**.
   - **Título** - digite um nome para o site.
   - **Endereço do site** - nas listas suspensas, selecione um nome de domínio e um caminho de URL, conforme necessário, e, em seguida, digite um nome do URL do site.
   - **Seleção de modelo** - na seção Seleção de modelo, faça o seguinte:
     - Na lista suspensa **Selecionar um idioma**, selecione um idioma para o site.
     - Em **Selecionar um modelo**, selecione o modelo para o site.
   - **Fuso horário** - selecione o fuso horário com base no local do site.
   - **Administrador** - digite o nome da pessoa que você deseja que seja o administrador do site. Você também pode usar o botão Verificar nomes ou Procurar para procurar usuários e torná-los administradores do site.
   - **Cota de armazenamento** - digite o tamanho (MBs) do site que você deseja alocar.
   - **Cota de recursos do servidor** - aceite a cota de recursos padrão.

   O site pessoal é criado no SharePoint.

Criar um plano de backup do SharePoint Online

Um plano de backup inclui uma tarefa **Backup: Office 365 SharePoint Online** que executa um backup de itens do SharePoint Online (listas, bibliotecas, documentos e assim por diante) e armazena dados em um repositório de dados com redução de redundância ou sem redução de redundância. Além disso, esse plano de backup permite que o UDP detecte e especifique itens do SharePoint Online para os quais uma tarefa de backup é executada. Cada tarefa consiste em parâmetros que definem a origem, o destino, a programação e outros detalhes de backup.

Siga estas etapas:

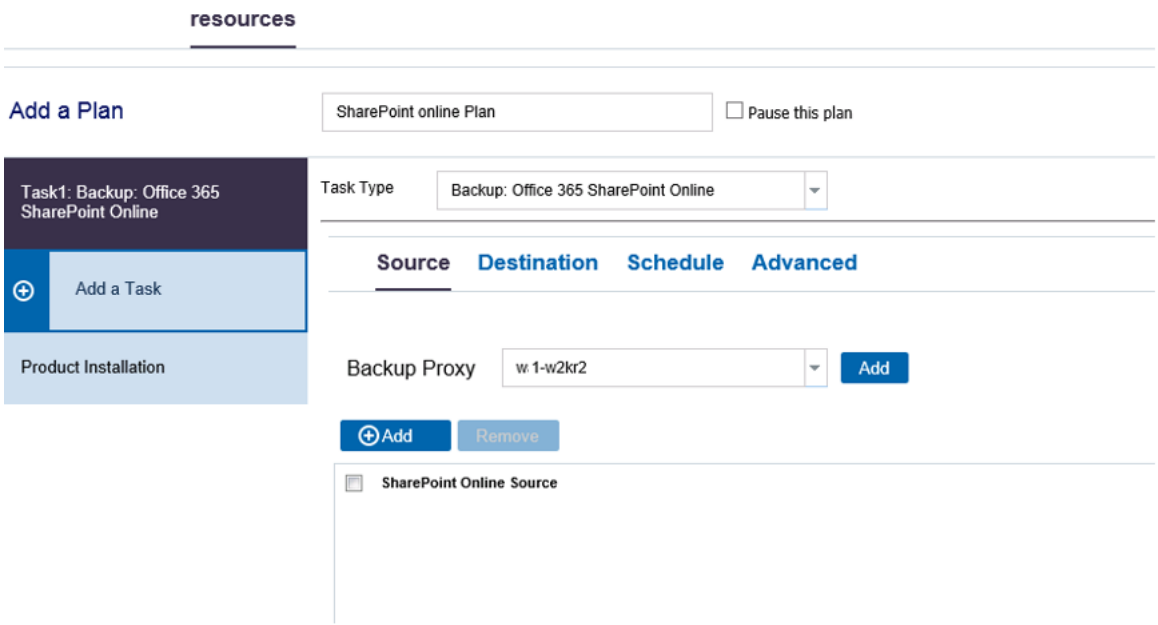
1. Clique na guia **Recursos** no Console.
2. No painel à esquerda, navegue para **Planos** e clique em **Todos os planos**.

   Se tiver criado os planos anteriores, esses planos serão exibidos no painel central.
3. No painel central, clique em **Adicionar um plano**.

   A caixa de diálogo **Adicionar um plano** abre.
4. Digite o nome do plano.
5. (Opcional) Selecione a caixa de seleção **Pausar este plano**.

   O plano não será executado até que você desmarque a caixa de seleção para retomar o plano.

   Observação: se um plano for pausado, nenhuma tarefa em andamento será pausada, mas todas as tarefas programadas correspondentes associadas a esse plano serão pausadas. No entanto, você pode executar uma tarefa manualmente. Por exemplo, você pode executar manualmente a tarefa de backup e a tarefa de replicação para um nó mesmo que o respectivo plano esteja pausado. Nesse caso, a tarefa seguinte da tarefa sob demanda (manual) não será executada. Por exemplo, há uma tarefa de replicação após uma tarefa de backup sob demanda, a tarefa de replicação não será executada para a tarefa de backup sob demanda. É necessário executar manualmente a tarefa de replicação. Quando você retomar o plano, as tarefas pendentes não são retomadas imediatamente. Depois de retomar o plano, as tarefas pendentes serão executadas no próximo horário programado.
6. Na lista suspensa Tipo de tarefa, selecione **Backup: Office 365 SharePoint Online**.



Agora especifique os detalhes de Origem, Destino, Programação e Avançado.

Especificar a origem

A página Origem permite especificar os nós de origem do SharePoint Online que você deseja proteger. É possível selecionar mais de um nó de origem do SharePoint Online em um plano.

Observação: é possível salvar um plano sem adicionar nós de origem, mas o plano só será implantado se você adicionar um nó.

Siga estas etapas:

1. Clique na guia **Origem**.
2. Selecione o **Proxy de Backup** na lista suspensa.
3. Adicione o nó do SharePoint Online usando um dos seguintes métodos:

   Método 1:

   a. Clique em **Adicionar** e em **Selecionar as origens a serem protegidas no Arcserve UDP**.

      A caixa de diálogo Adicionar nós ao plano é exibida.

      Observação: use essa opção somente se você já tiver adicionado o nó do SharePoint.

   b. Selecione um nó e clique em **Conectar**.

      Observação: para localizar os nós do SharePoint Online que você deseja proteger, use **Pesquisar**.

   Método 2:

   - Clique em **Adicionar** e, em seguida, clique em **Adicionar origem do SharePoint Online**.

     O diálogo Adicionar nós a um plano é exibido.

     Observação:

     - Use essa opção para detectar e especificar itens online para a origem do SharePoint Online.
     - Diferentemente de outros nós, não é possível adicionar o nó do SharePoint Online a partir da página Todos os nós. É possível adicionar um nó do SharePoint Online apenas durante a criação ou modificação de um plano.
4. Para aplicar a autenticação, siga um destes procedimentos:

Autenticação moderna

Para a autenticação moderna, você pode executar um backup usando o certificado de segurança.

Usar certificado de segurança

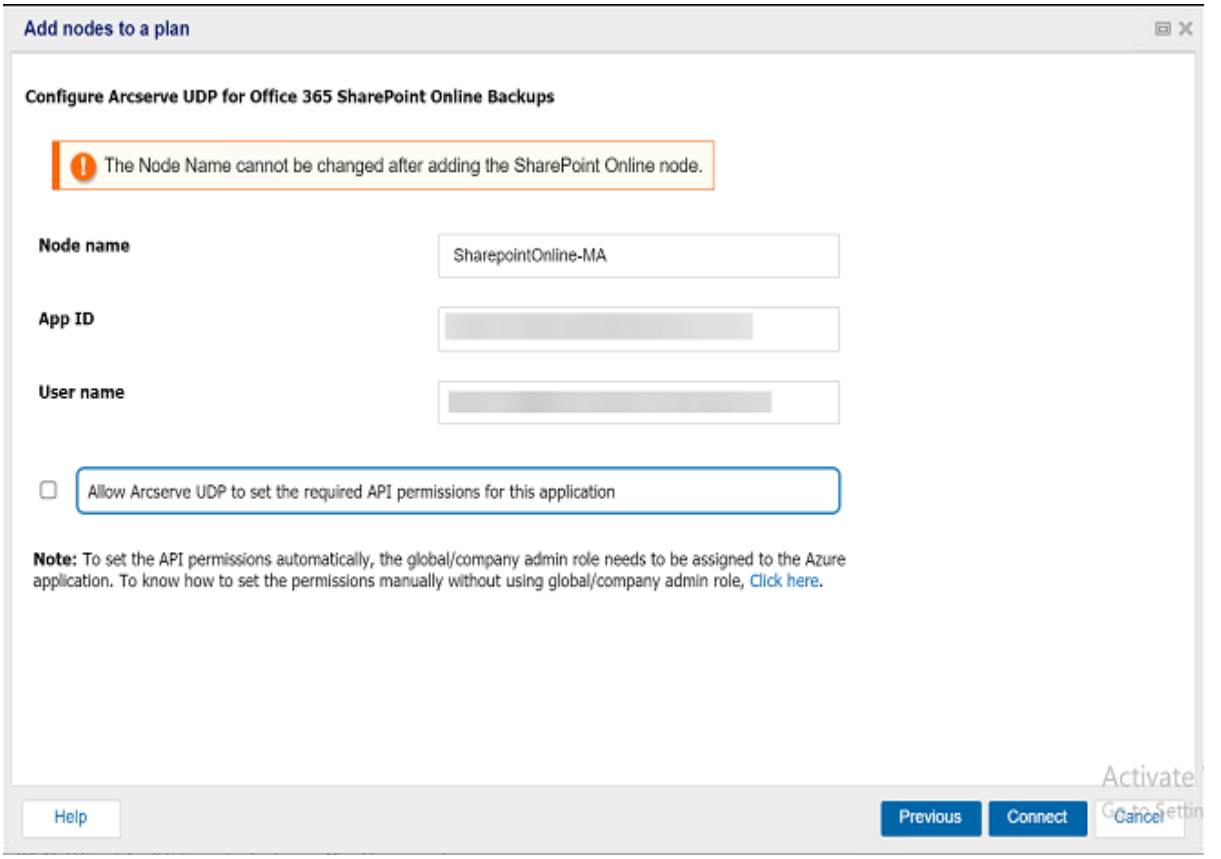
Observação: por padrão, o plano de backup seleciona **Usar certificado de segurança** para a autenticação moderna.

Siga estas etapas:

a. Para autenticar o aplicativo UDP com certificados de segurança, consulte Fazendo download do certificado do UDP e carregando-o no Azure.

b. Digite os seguintes detalhes:

- Nome do nó
- ID do aplicativo
- Nome de usuário



c. Para aplicar as permissões de API automaticamente, marque a caixa de seleção **Permitir que o Arcserve UDP defina as permissões de API necessárias para este aplicativo**.

Observação: para aplicar as permissões manualmente sem usar a função de administrador global/de empresa, consulte Configurando as permissões da API manualmente sem usar a função de administrador global/de empresa.

d. Clique em **Conectar**.

Observações:

- Os nomes dos nós de origem do SharePoint Online não podem ser alterados após a criação do nó.
- Você pode usar uma única conta para proteger vários nós do SharePoint Online.

Autenticação básica

Para a autenticação básica, para continuar com o backup, forneça as seguintes informações e clique em **Conectar**:

- Nome do nó
- ID do usuário
- Senha

5. Para proteger os itens do SharePoint Online, faça o seguinte e clique em **Salvar**.
   - Na lista suspensa Tipo de site, selecione o tipo de site que deseja proteger, como sites do SharePoint ou sites pessoais.
   - Para Proteger todos os sites/subsites, faça o seguinte:

     Observações:

     - Esta opção é selecionada automaticamente por padrão quando a tela Selecionar conteúdo do SharePoint Online é exibida.
       - Para proteger todos os itens no tipo de site selecionado, marque a caixa de seleção **Proteger todos os sites/-subsites**.
       - Para proteger itens específicos no tipo de site selecionado, desmarque a caixa de seleção **Proteger todos os sites/-subsites** e, em seguida, selecione os itens específicos que deseja proteger.

- Ao configurar o plano do SharePoint Online existente, se você selecionou sites manualmente para proteção e agora deseja marcar a caixa de seleção **Proteger todos os sites/subsites**, siga estas etapas:
  a. Modifique o plano do SharePoint Online existente.
  b. Limpe os sites do SharePoint selecionados manualmente para proteção.
  c. Marque a caixa de seleção **Proteger todos os sites/-subsites** e salve o plano.

- Para excluir itens específicos da proteção, marque a caixa de seleção **Excluir sites selecionados** e, em seguida, selecione itens específicos no tipo de site selecionado.

As origens do SharePoint Online que você deseja proteger são adicionadas ao plano.

Especificar o destino

O destino é o local onde você armazena os dados de backup. É necessário, no mínimo, especificar o destino para salvar o plano.

Siga estas etapas:

1. Clique na guia **Destino**.

   A opção **Servidor de ponto de recuperação do Arcserve UDP**. **O servidor de ponto de recuperação do Arcserve UDP** especifica que o destino de backup é um servidor de ponto de recuperação.

   Não é possível armazenar dados como conjuntos de dados de recuperação.

2. Siga as seguintes etapas:

   a. Selecione um servidor do ponto de recuperação.

   b. Selecione um repositório de dados de redução de redundância ou de não redução de redundância.

      A lista exibe todos os repositórios de dados criados no servidor do ponto de recuperação especificado.

   c. Forneça uma senha da sessão.

      A senha da sessão é opcional quando o destino de backup é um repositório de dados do RPS não criptografado.

   d. Confirme a senha da sessão.

   O destino é especificado.

Especificar a programação

A página Programar permite definir uma programação para o backup e para que as funções Mesclar e Acelerar sejam repetidas em intervalos específicos. Após definir uma programação, as tarefas são executadas automaticamente de acordo com a programação. É possível adicionar várias programações e fornecer configurações de retenção.

Uma Programação de backup se refere a programação regular que é repetida várias vezes ao dia, com base no número de horas ou de minutos selecionado. Além da programação regular, uma programação de backup também fornece opções para adicionar programações diária, semanal e mensal.

Observação: para obter mais informações sobre as configurações de retenção e programação, consulte Entendendo a programação avançada e retenção.

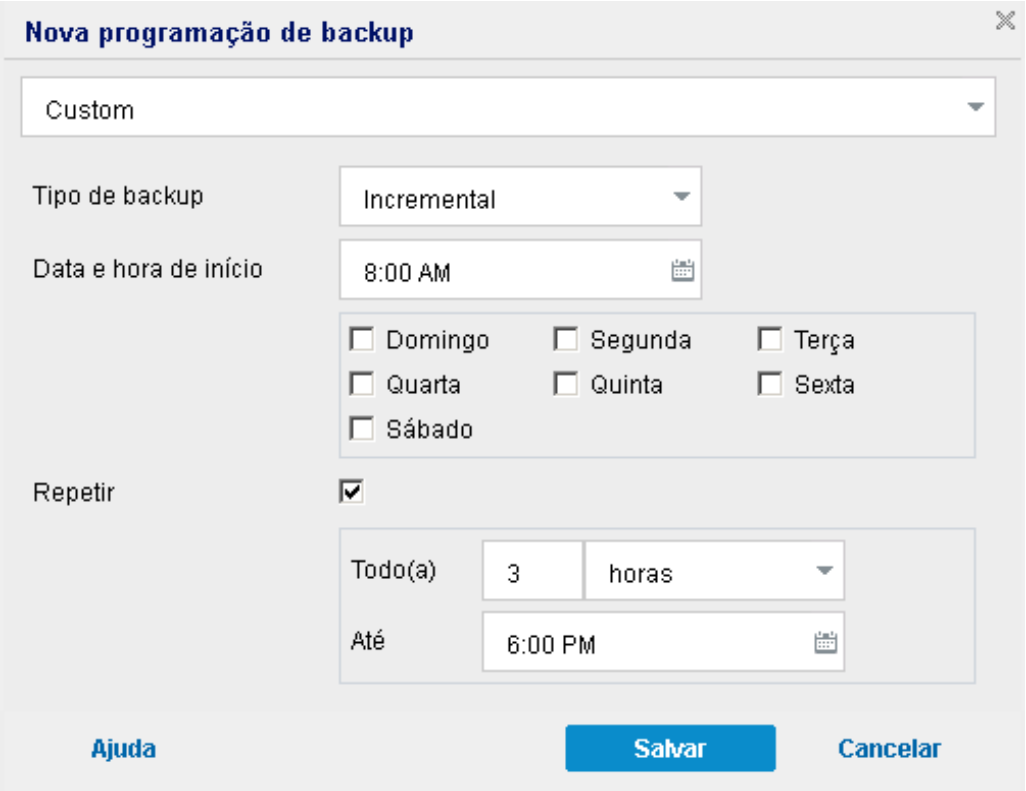
Siga estas etapas:

1. Adicionar programações de backup, mesclagem e acelerador.

   Adicionar programação de backup

   a. Clique em **Adicionar** e selecione **Adicionar programação de backups**.

      A caixa de diálogo **Nova programação de backup** é aberta.



   b. Selecione uma das seguintes opções:

Personalizado

Especifica a programação de backup que se repete várias vezes por dia.

Diário

Especifica a programação de backup que ocorre uma vez por dia. Por padrão, todos os dias da semana estão selecionados para o backup diário. Se não desejar executar a tarefa de backup em um dia específico, desmarque a caixa de seleção correspondente àquele dia da semana.

Semanal

Especifica a programação de backup que ocorre uma vez por semana.

Mensal

Especifica a programação de backup que ocorre uma vez por mês.

c. Selecione o tipo de backup.

Completo

Especifica a programação de backups para backups completos. Conforme programado, o Arcserve UDP executa um backup completo de todos os blocos usados do computador de origem. Um backup completo em geral, consome tempo, dependendo do tamanho do backup.

Incremental

Especifica a programação de backups para backups incrementais.

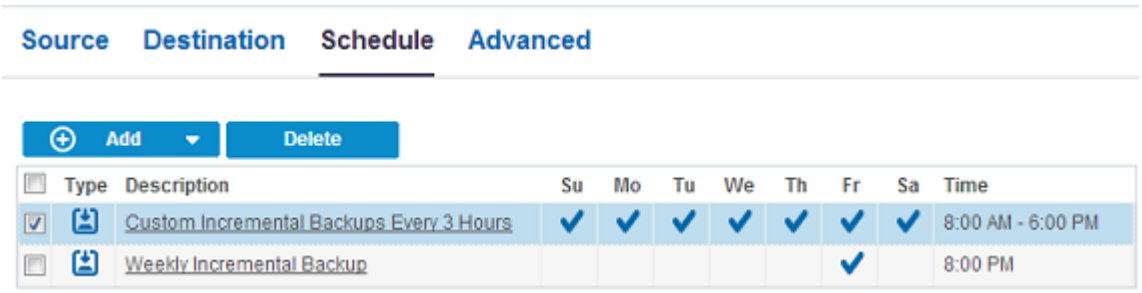
Conforme programado, o Arcserve UDP faz backup incremental apenas dos blocos que foram alterados após o último backup realizado com êxito. As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a executar um backup.

d. Especifique a hora de início do backup.

e. (Opcional) Marque a caixa de seleção de **Repetição** e especifique a programação a ser repetida.

f. Clique em **Salvar**.

A programação de backup é especificada e aparece na página **Programar**.



Adicionar Programação de mesclagem

a. Clique em **Adicionar** e selecione **Adicionar programação de mesclagem**.

   A caixa de diálogo **Adicionar nova programação de mesclagem** é aberta.

b. Especifique a hora de início da tarefa de mesclagem.

c. Especifique **Até** para fornecer uma hora de término para a tarefa de mesclagem.

d. Clique em **Salvar**.

A programação de mesclagem é especificada e aparece na página **Programar**.

Adicionar programação de acelerador

a. Clique em **Adicionar** e selecione **Adicionar programação de acelerador.**

   A caixa de diálogo **Adicionar nova programação do acelerador** é aberta.

b. Especifique o limite de taxa de transferência em unidades de MB por minuto.

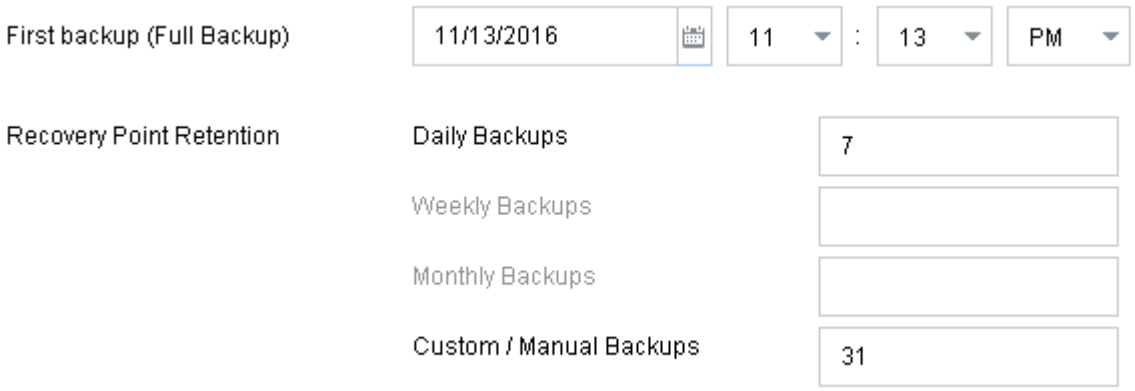
c. Especifique a hora de início da tarefa de taxa de transferência de backup.

d. Especifique **Até** para fornecer um horário de término para a tarefa de taxa de transferência.

e. Clique em **Salvar**.

A Programação de acelerador é especificada e exibida na página **Programar**.

2. Especifique a hora de início do backup programado.



3. Especifique as configurações de retenção de pontos de recuperação para programação diária, semanal e mensal.

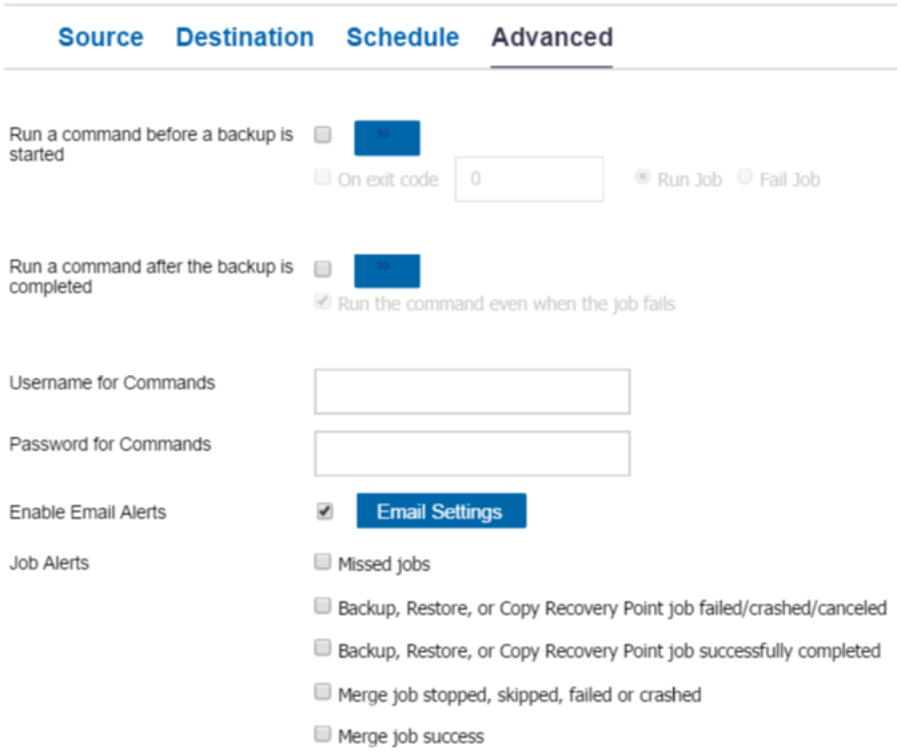
   As opções serão ativadas se tiver adicionado a programação de backup correspondente. Se você modificar as configurações de retenção desta página, as alterações serão refletidas na caixa de diálogo **Programação de backup**.

   A programação é especificada.

Especificar as configurações avançadas

A guia **Avançado** permite especificar algumas configurações avançadas para a tarefa de backup. As configurações avançadas incluem o fornecimento da localização dos scripts e as configurações de email.

A imagem a seguir mostra a guia **Avançado**:



Siga estas etapas:

1. Especifique os seguintes detalhes.

   Executar um comando antes do início do backup

   Permite a execução de um script antes de iniciar a tarefa de backup. Especifique o caminho em que o script está armazenado dentro do nó do proxy. Clique em **No código de saída** e especifique o código de saída para **Executar tarefa** ou **Tarefa com falha**. **Executar a tarefa** indica que a tarefa de backup continuará quando o script retornar o código de saída. **Tarefa com falha** indica que a tarefa de backup será interrompida quando o script retornar o código de saída.

   Executar um comando após a conclusão do backup

   Permite executar um script depois que a tarefa de backup foi concluída. Especifique o caminho completo onde o script está armazenado.

   Executar um comando, mesmo quando a tarefa falhar

Se essa caixa de seleção for selecionada, o script especificado em **Executar um comando após a conclusão do backup** é executado mesmo quando a tarefa de backup falha. Caso contrário, aquele script é executado somente quando a tarefa de backup é concluída com êxito.

Nome de usuário para comandos

Permite especificar o nome de usuário para executar os comandos.

Senha para comandos

Permite especificar a senha para executar os comandos.

Ativar alertas por email

Permite ativar alertas por email. É possível especificar configurações de email e os tipos de alertas que você deseja receber por email. Ao selecionar esta opção, as seguintes opções serão ativadas para a seleção.

Configurações de email

Permite configurar as definições de email. Clique em **Configurações de email** e configure o servidor de email e os detalhes do servidor proxy. Para obter mais informações sobre como configurar Configurações de email, consulte o tópico Configuração de email e alerta.

Alertas de tarefa

Permite selecionar os tipos de emails de alerta de tarefas que deseja receber.

2. Clique em **Salvar**.

Observação: quando você seleciona um nó como origem de backup ou proxy de backup, o Arcserve UDP verifica se o agente está instalado no nó do proxy e se é a versão mais recente. Em seguida, o Arcserve UDP exibe uma caixa de diálogo de verificação que lista todos os nós que possuem uma versão antiga do agente ou que não tem o agente instalado. Para instalar/atualizar o agente nesses nós, selecione o método de instalação e clique em **Salvar**.

As alterações são salvas e uma marca de seleção verde aparece ao lado do nome da tarefa. A página do plano é fechada.

Observação: se precisar adicionar outra tarefa, deverá selecionar o plano na guia **Recursos** e modificar o plano. Para modificar o plano, clique no plano do painel central. O plano é exibido e será possível modificá-lo. É possível adicionar as tarefas **Copiar ponto de recuperação**, **Cópia em fita**, **Replicar** e **Replicar de um RPS remoto** como tarefas de acompanhamento.

O plano é automaticamente implantado ao nó do servidor proxy.

O plano de backup do SharePoint Online para o servidor proxy é criado. O backup é executado de acordo com a programação que você configurou na guia **Programar**. Também é possível fazer backup manual quando desejado.

(Opcional) Executar um backup manual

Normalmente, com base nas configurações de programação aplicadas, os backups são executados automaticamente. Além do backup programado, um backup manual fornece a opção de fazer backup dos nós de acordo com a necessidade. Por exemplo, se repetir a programação para backups completos e incrementais e desejar fazer grandes alterações em seu computador, você deverá executar um backup manual imediato sem esperar até que ocorra o próximo backup programado.

Para executar um backup manual dos nós do SharePoint Online, siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel esquerdo, navegue para **Nós** e clique em **Todos os nós**.

   Os nós do SharePoint Online são exibidos no painel central.
3. Selecione os nós do SharePoint Online (por exemplo, Caixa de correio@<nomedaorganização.com>) dos quais você deseja fazer backup e certifique-se de ter um plano atribuído a ele. O nome do nó é a conta usada durante a adição do nó do SharePoint Online e de sua conexão.
4. Clique com o botão direito do mouse no nó e selecione **Fazer backup agora**.

   A caixa de diálogo Fazer backup agora é exibida.
5. Selecione o tipo de backup que deseja executar e clique em **OK**.

   A caixa de diálogo Informações do andamento é exibida.
6. Aguarde até que a tarefa de backup seja concluída e clique em **OK**.
7. Para monitorar as tarefas de backup, navegue até **tarefas** > **Tarefas em andamento**.

   Aguarde até a conclusão da tarefa de backup.

   O backup manual é realizado com êxito.

Para executar um backup manual do plano do SharePoint Online, siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel esquerdo, navegue para **Planos** e clique em **Todos os planos**.

   Os planos de backup do SharePoint Online são exibidos no painel central.

3. Selecione o plano do qual você deseja fazer backup e certifique-se de que tenha um plano atribuído a ele.
4. Clique com o botão direito do mouse no plano e selecione **Fazer backup agora**.

   A caixa de diálogo Fazer backup agora é exibida.
5. Selecione o tipo de backup que deseja executar e clique em **OK**.

   A caixa de diálogo Informações do andamento é exibida.
6. Aguarde até que a tarefa de backup seja concluída e clique em **OK**.
7. Para monitorar as tarefas de backup, navegue até **tarefas** > **Tarefas em andamento**.

   Aguarde até a conclusão da tarefa de backup.

   O backup manual é realizado com êxito.

Verificar o backup

Para verificar a tarefa de backup, confirme se você criou com êxito o plano de backup. Depois de verificar se o plano está criado com êxito, confirme se a tarefa de backup é executada conforme o programado. É possível verificar o status das tarefas de backup na guia **Tarefas**.

Siga estas etapas para verificar os planos:

1. Clique na guia **Recursos**.
2. No painel esquerdo, navegue para **Nós** e clique em **Todos os nós**.

   Uma lista de todos os nós é exibida no painel central.
3. Verifique se os planos são mapeados com nós.

Siga um destes métodos para verificar as tarefas de backup:

Método 1

1. Clique na guia **Tarefas**.
2. No painel à esquerda, clique em **Todas as tarefas concluídas**.

   O status de cada tarefa é incluído no painel central.
3. Verifique se a tarefa de backup é concluída com êxito.

   A tarefa de backup é verificada.

Método 2

1. Clique na guia **Tarefas**.
2. No painel esquerdo, clique em **Tarefas concluídas com êxito**.

   A lista de tarefas de backup concluídas é exibida no painel central.
3. Clique na tarefa que você deseja verificar.

   O painel direito é atualizado.
4. Em Detalhes da tarefa, clique no hiperlink **Exibir logs**.
5. Verifique se a tarefa de backup é concluída com êxito.

   A tarefa de backup é verificada.

Fazer a configuração da autenticação multifator

Quando uma organização tiver a autenticação multifatorial (MFA) ativada para os usuários, use a Autenticação moderna para adicionar nós.

Observação: embora a autenticação básica esteja ativada no locatário, você pode usar a Autenticação moderna para adicionar nós. Para obter mais informações sobre como adicionar nós a um plano usando a Autenticação moderna, consulte Autenticação moderna.

Como criar um plano de backup do Microsoft Office 365 OneDrive

O OneDrive, parte do serviço de nuvem do Microsoft Office 365, facilita o compartilhamento de arquivos e o armazenamento na nuvem. Para proteger seus itens do OneDrive (arquivos, pastas e outros) na nuvem da Microsoft, é necessário criar um plano. O plano para o OneDrive consiste em uma tarefa de backup. Essa tarefa de backup permite especificar os nós do OneDrive que você deseja proteger, o destino do backup e a programação do backup.

O que fazer a seguir?

1. Verificar os pré-requisitos e as considerações
2. Criar um plano de backup do OneDrive
3. (Opcional) Executar um backup manual
4. Fazer a configuração da autenticação multifator

Revisar os pré-requisitos e as considerações

Revise os seguintes pré-requisitos e considerações antes de criar um plano de backup do OneDrive.

Criando um plano de backup do OneDrive:

Pré-requisito:

- A execução do script do PowerShell está ativada no servidor proxy. Se não estiver ativada, execute o comando: *Set-ExecutionPolicy RemoteSigned*
- O servidor proxy deve se conectar ao Microsoft Azure.

Considerações:

Os serviços do Microsoft Cloud são diferentes para nuvens nacionais da Alemanha, da China e do governo dos EUA. Para obter mais detalhes, consulte o link. É necessário modificar a configuração durante a implantação do produto nessas regiões.

Siga estas etapas:

1. Abra o arquivo de configuração cujo caminho é o de instalação do $UDP.

   $/Engine/Bin/Office365/Arcserve.Office365.Onedrive.json

2. Localize a configuração **Região** e defina o valor como Alemanha, China ou governo dos EUA.

   Valor padrão: Normal

Criando um plano de backup do OneDrive usando BA (Basic Authentication - Autenticação básica):

Revise o seguinte:

- Instale o PowerShell versão 5.1 ou superior (parte da WMF, Windows Management Framework - Estrutura de Gerenciamento do Windows) no servidor proxy (computador de 64 bits).
- Instale os seguintes módulos do PowerShell no servidor proxy usando a janela do PowerShell:
  - Para instalar o módulo do Azure, execute o seguinte comando:

    Install-Module -Name AzureAD -Force
  - Para instalar o módulo ExchangeOnlineManagement, execute o seguinte comando:

    Install-Module -Name ExchangeOnlineManagement -Force

  Observação: ao instalar módulos do PowerShell usando os comandos acima, uma versão mais recente dos módulos poderá ser instalada dependendo da versão do GA do componente disponível no repositório da Microsoft.

Criando um plano de backup do OneDrive usando MA (Modern Authentication - Autenticação moderna):

Revise os Pré-requisitos antes de criar um plano usando a autenticação moderna.

Criar um plano de backup do OneDrive

Um plano de backup inclui uma tarefa de backup que executa um backup dos itens de dados do OneDrive (arquivos, pastas e outros) e armazena os dados em um repositório de dados sem redução de redundância ou em um repositório de dados de redução de redundância. Além disso, esse plano de backup permite que o UDP detecte e especifique grupos do OneDrive para os quais uma tarefa de backup é executada. Cada tarefa consiste em parâmetros que definem a origem, o destino, a programação e outros detalhes de backup.

Siga estas etapas:

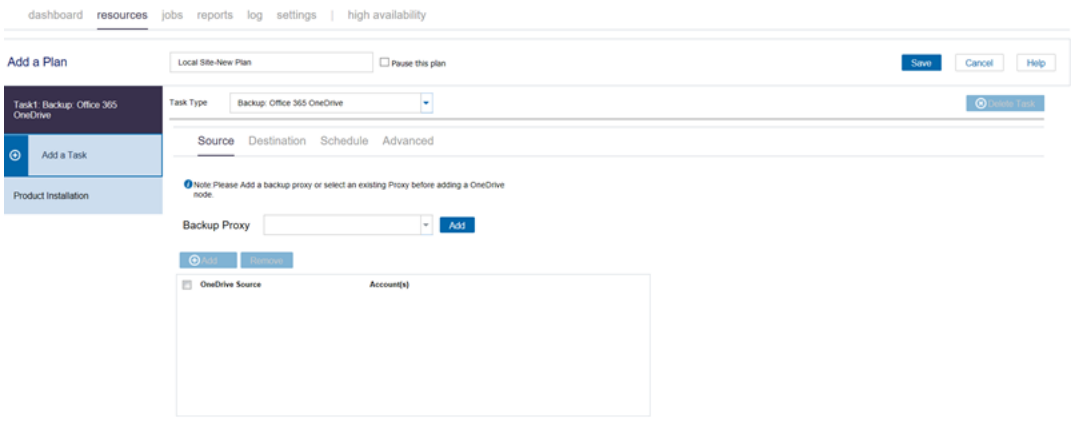
1. Clique na guia **Recursos** no Console.
2. No painel à esquerda, navegue para **Planos** e clique em **Todos os planos**.

   Se tiver criado os planos anteriores, esses planos serão exibidos no painel central.
3. No painel central, clique em **Adicionar um plano**.

   A caixa de diálogo **Adicionar um plano** abre.
4. Digite o nome do plano.
5. (Opcional) Selecione a caixa de seleção **Pausar este plano**.

   O plano não será executado até que você desmarque a caixa de seleção para retomar o plano.

   Observação: se um plano for pausado, nenhuma tarefa em andamento será pausada, mas todas as tarefas programadas correspondentes associadas a esse plano serão pausadas. No entanto, você pode executar uma tarefa manualmente. Por exemplo, você pode executar manualmente a tarefa de backup e a tarefa de replicação para um nó mesmo que o respectivo plano esteja pausado. Nesse caso, a tarefa seguinte da tarefa sob demanda (manual) não será executada. Por exemplo, há uma tarefa de replicação após uma tarefa de backup sob demanda, a tarefa de replicação não será executada para a tarefa de backup sob demanda. É necessário executar manualmente a tarefa de replicação. Quando você retomar o plano, as tarefas pendentes não são retomadas imediatamente. Depois de retomar o plano, as tarefas pendentes serão executadas no próximo horário programado.
6. Na lista suspensa Tipo de tarefa, selecione **Backup: Office 365 OneDrive**.



Agora especifique os detalhes de Origem, Destino, Programação e Avançado.

Especificar a origem

A página Origem permite especificar os nós de origem do OneDrive que você deseja proteger. É possível selecionar mais de um nó de origem do OneDrive em um plano. Caso não tenha adicionado nenhum nó ao console, você pode adicionar nós de origem do OneDrive a partir da página Origem.

Observação: é possível salvar um plano sem adicionar nós de origem, mas o plano só será implantado se você adicionar os nós.

Siga estas etapas:

1. Clique na guia **Origem**.
2. Selecione o **Proxy de Backup** na lista suspensa.
3. Adicione o nó do OneDrive usando um dos seguintes métodos:

   Método 1

   a. Clique em **Adicionar** e em **Selecionar as origens a serem protegidas no Arcserve UDP**.

      A caixa de diálogo Adicionar nós ao plano é exibida.

   b. Selecione um nó e clique em **Conectar**.

      Observação: também é possível procurar os nós do OneDrive que você deseja proteger em Pesquisar.

   c. Marque a caixa de seleção **Proteger todas as contas do OneDrive** para proteger todas as contas do OneDrive em todas as páginas. Para selecionar algumas contas, clique na seta no lado direito da caixa de seleção e especifique as contas.

      As contas do OneDrive que você selecionar serão adicionadas.

Método 2

a. Clique em **Adicionar** e, em seguida, clique em **Adicionar a origem do OneDrive**.

   Observações:

   - Use essa opção para detectar e especificar grupos de distribuição para o OneDrive.
   - Diferentemente de outros nós, não é possível adicionar o nó do OneDrive a partir da página Todos os nós. Você só pode adicionar um nó do OneDrive em um plano ou ao modificar um plano.

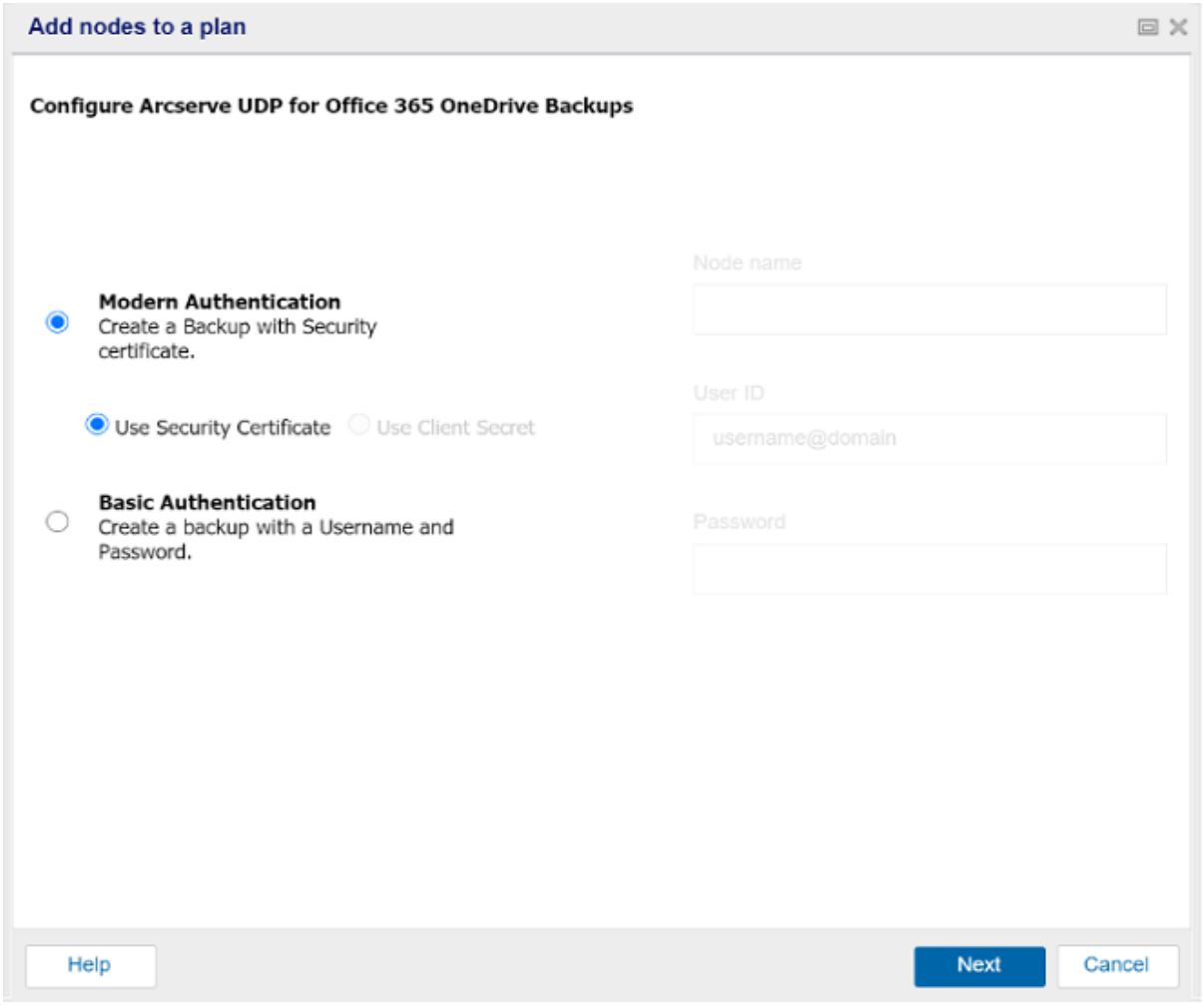
b. Para adicionar um nó do OneDrive por plano, especifique o nome do nó, a ID do usuário e a senha. Não é possível alterar o nome do nó após criar o nó do OneDrive. Vários nós do OneDrive podem usar a mesma conta de usuário (conta de serviço) do OneDrive.

   Observação: é recomendável selecionar contas de usuário de administradores do Azure Active Directory.

4. Para aplicar a autenticação, siga um destes procedimentos:

   Autenticação moderna

   Para a autenticação moderna, você pode executar um backup usando o certificado de segurança.



Usar certificado de segurança

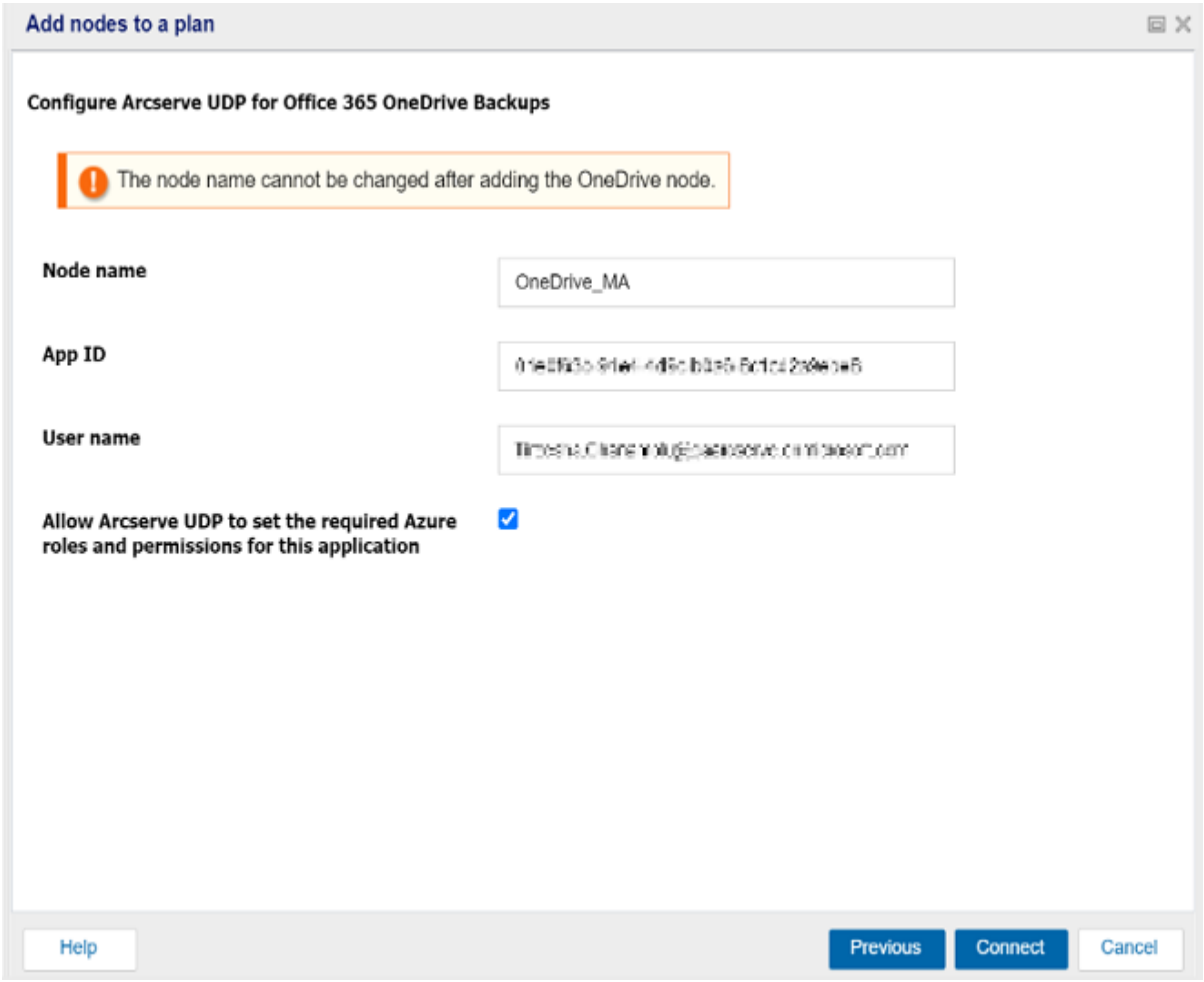
Observação: por padrão, o plano de backup seleciona **Usar certificado de segurança** para a autenticação moderna.

Siga estas etapas:

a. Para autenticar o aplicativo UDP com certificados de segurança, consulte Fazendo download do certificado do UDP e carregando-o no Azure.

b. Digite os seguintes detalhes:

- Nome do nó
- ID do aplicativo
- Nome de usuário



Observação: os nomes dos nós do OneDrive não podem ser alterados após a criação de um nó.

c. Para aplicar as permissões de API automaticamente, marque a caixa de seleção **Permitir que o Arcserve UDP defina as permissões de API necessárias para este aplicativo**.

Observação: para aplicar as permissões manualmente sem usar a função de administrador global/de empresa, consulte Configurando as permissões da API manualmente sem usar a função de administrador global/de empresa.

d. Clique em **Conectar**.

Autenticação básica

Para a autenticação básica, para continuar com o backup, siga estas etapas:

a. Selecione Autenticação básica, digite o nome do nó, o nome do usuário e a senha e, em seguida, clique em **Conectar**.

O URL do Arcserve UDP é aberto em um navegador e solicita permissão para todos os dados de leitura e gravação do Arcserve UDP do portal do OneDrive.

b. No navegador, use as credenciais de administrador do Microsoft Azure para entrar.

   O portal do Azure é aberto.

c. No portal do Microsoft Azure, execute as seguintes etapas para configurar o aplicativo UDP:

   Clique em **Permissões da API**.

   ii. No painel direito, clique no botão **Conceder permissões para**.

   iii. Clique em **Sim** para concordar em conceder permissões.

   iv. Após conceder a permissão, no Arcserve UDP, vá até **Adicionar um plano > Adicionar nós a um plano** e clique no botão **Avançar**.

Observação: se você tiver fechado o URL de concessão de permissão e quiser abri-lo novamente, clique no botão **Aqui** na tela Adicionar nó ao plano do UDP.

O Arcserve UDP lista todas as contas no locatário atual.

5. Para proteger as contas do OneDrive, siga um destes procedimentos:

   - Para proteger todas as contas e grupos do OneDrive, marque a caixa de seleção **Proteger todas as contas do OneDrive**.

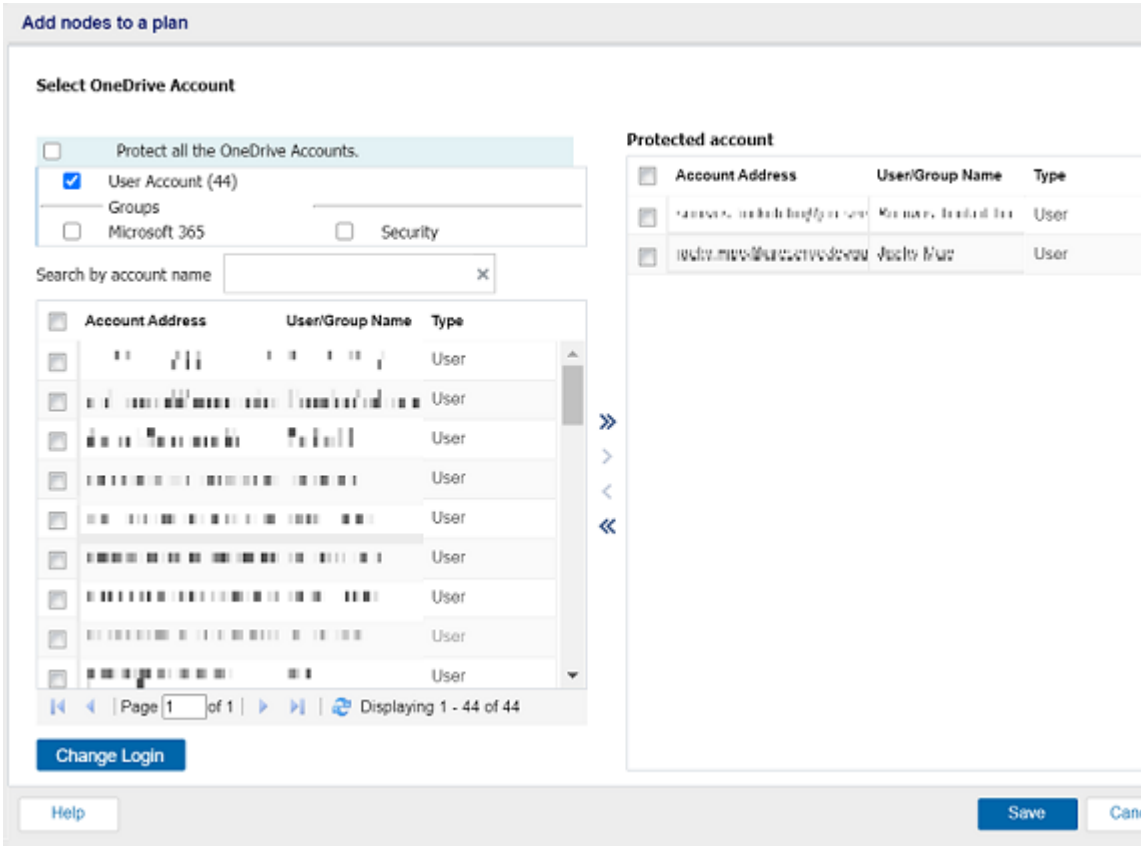
     Observação: esta opção é selecionada automaticamente por padrão quando a tela Selecionar conta do OneDrive é exibida.

   - Para Conta do usuário, siga estas etapas:

     a. Marque a caixa de seleção **Conta do usuário**.

        Uma lista de contas de usuários é exibida.

     b. (Opcional) Para pesquisar uma conta na lista, no campo Pesquisar por nome de conta, digite o nome da conta.



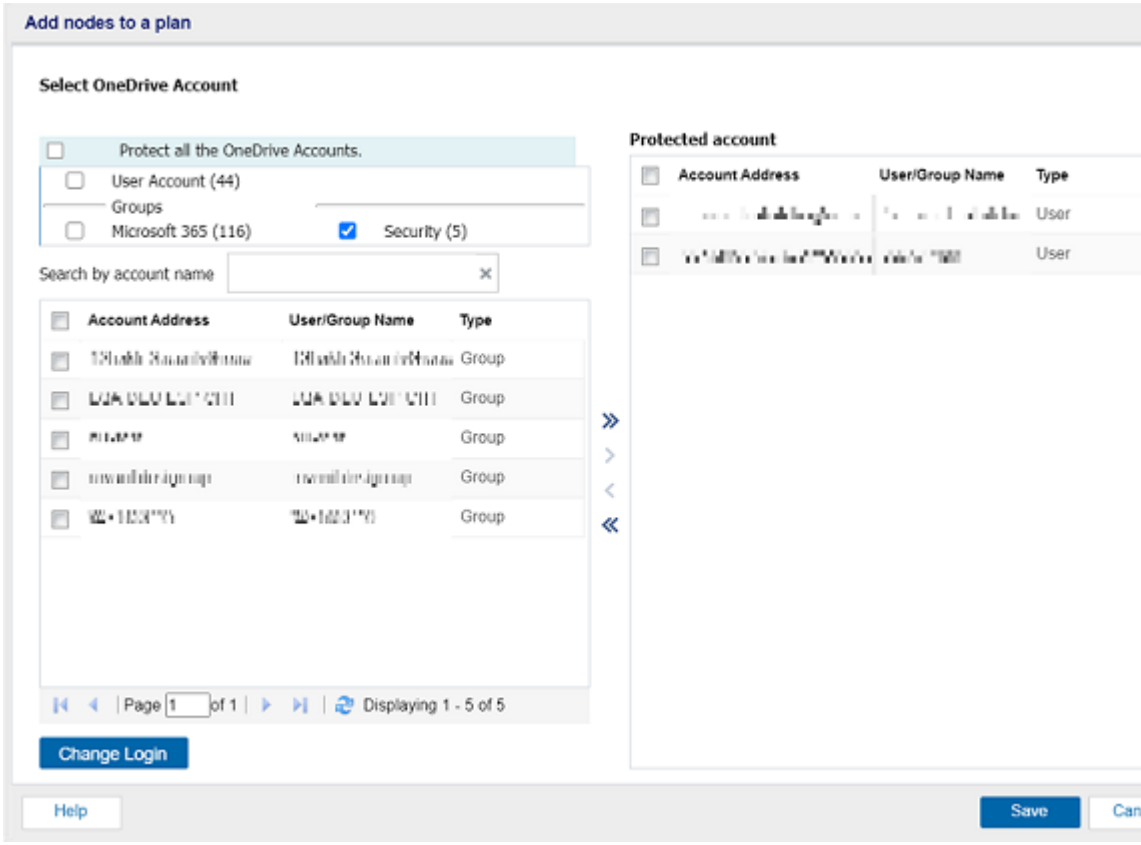
c. Na lista de contas de usuários, selecione as contas que deseja proteger.

d. Clique na seta para a direita (>) para mover as contas selecionadas para a lista de contas protegidas.

- Para Grupos, siga estas etapas:

a. Marque a caixa de seleção **Microsoft 365** ou **Segurança**.

Com base na seleção, uma lista de grupos é exibida.



b. (Opcional) Para pesquisar uma conta na lista, no campo Pesquisar por nome de conta, digite o nome da conta.

c. Na lista de grupos, selecione os grupos que deseja proteger.

d. Clique na seta para a direita (>) para mover os grupos selecionados para a lista de contas protegidas.

6. Clique em **Salvar**.

   As contas do OneDrive selecionadas são adicionadas.

Especificar o destino

O destino é o local onde você armazena os dados de backup. É necessário, no mínimo, especificar o destino para salvar o plano.

Siga estas etapas:

1. Clique na guia **Destino**.

   A opção **Servidor de ponto de recuperação do Arcserve UDP** é selecionada automaticamente. **O servidor de ponto de recuperação do Arcserve UDP** especifica que o destino de backup é um servidor de ponto de recuperação. Se você sele-

cionar essa opção, os dados serão armazenados como pontos de recuperação. Não é possível armazenar dados como conjuntos de dados de recuperação.

2. Forneça os detalhes a seguir:
   a. Selecione um servidor de ponto de recuperação.
   b. Selecione um repositório de dados de redução de redundância ou de não redução de redundância. A lista exibe todos os repositórios de dados criados no servidor de ponto de recuperação especificado.
   c. Forneça uma senha da sessão. A senha da sessão é opcional quando o destino de backup é um repositório de dados do RPS não criptografado.
   d. Confirme a senha da sessão.

   O destino é especificado. Agora, especifique os detalhes de Programar e Avançado.

Especificar a programação

A página Programar permite definir uma programação para o backup e para que as funções Mesclar e Acelerar sejam repetidas em intervalos específicos. Após definir uma programação, as tarefas são executadas automaticamente de acordo com a programação. É possível adicionar várias programações e fornecer configurações de retenção.

Uma Programação de backup se refere a programação regular que é repetida várias vezes ao dia, com base no número de horas ou de minutos selecionado. Além da programação regular, uma programação de backup também fornece opções para adicionar programações diária, semanal e mensal.

Observação: para obter mais informações sobre as configurações de retenção e programação, consulte Entendendo a programação avançada e retenção.

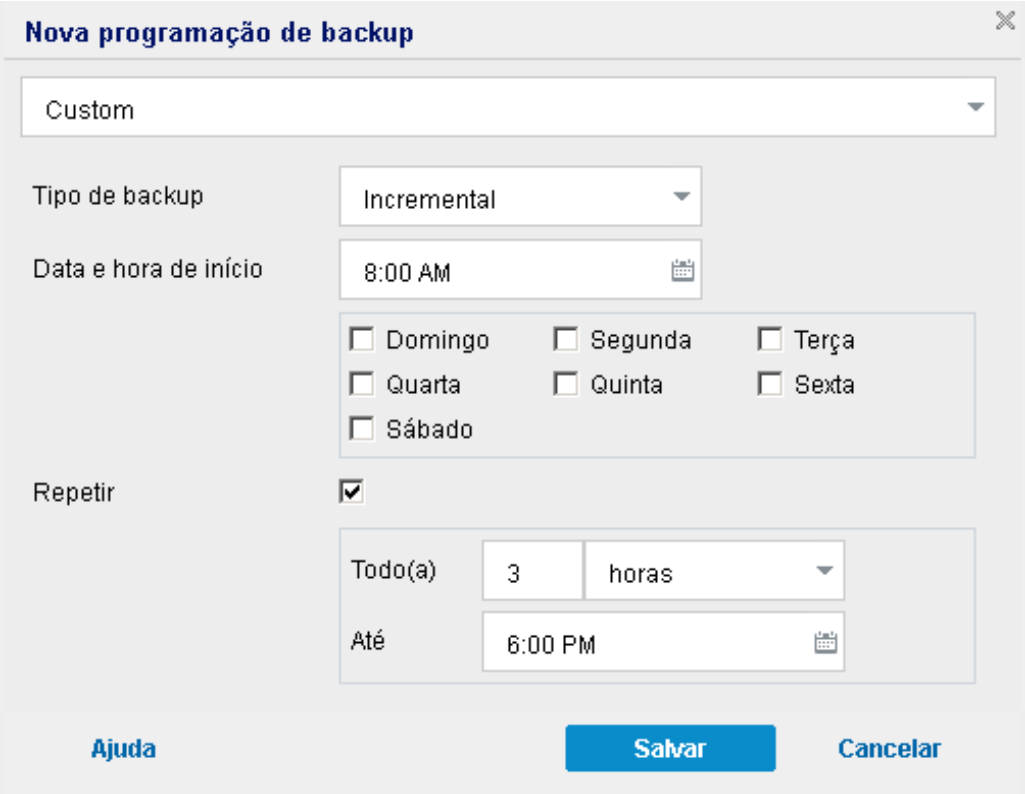
Siga estas etapas:

1. Adicionar programações de backup, mesclagem e acelerador.

   Adicionar programação de backup

   a. Clique em **Adicionar** e selecione **Adicionar programação de backups**.

      A caixa de diálogo **Nova programação de backup** é aberta.



b. Selecione uma das seguintes opções:

Personalizado

Especifica a programação de backup que se repete várias vezes por dia.

Diário

Especifica a programação de backup que ocorre uma vez por dia. Por padrão, todos os dias da semana estão selecionados para o backup diário. Se não desejar executar a tarefa de backup em um dia específico, desmarque a caixa de seleção correspondente àquele dia da semana.

Semanal

Especifica a programação de backup que ocorre uma vez por semana.

Mensal

Especifica a programação de backup que ocorre uma vez por mês.

c. Selecione o tipo de backup.

Completo

Especifica a programação de backups para backups completos. Conforme programado, o Arcserve UDP executa um backup completo de todos os blocos usados do computador de origem. Um backup completo em geral, consome tempo, dependendo do tamanho do backup.

Incremental

Especifica a programação de backups para backups incrementais.

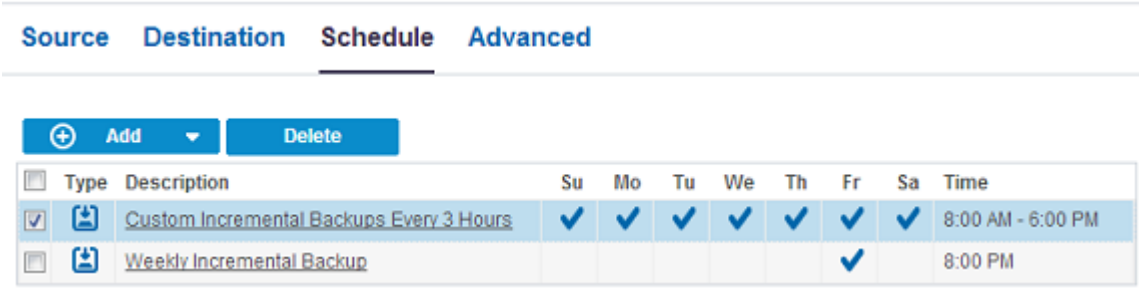
Conforme programado, o Arcserve UDP faz backup incremental apenas dos blocos que foram alterados após o último backup realizado com êxito. As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta opção é a maneira mais ideal de executar um backup.

d. Especifique a hora de início do backup.

e. (Opcional) Marque a caixa de seleção de **Repetição** e especifique a programação a ser repetida.

f. Clique em **Salvar**.

A programação de backup é especificada e aparece na página **Programar**.



Adicionar Programação de mesclagem

a. Clique em **Adicionar** e selecione **Adicionar programação de mesclagem**.

A caixa de diálogo **Adicionar nova programação de mesclagem** é aberta.

b. Especifique a hora de início para iniciar a tarefa de mesclagem.

c. Especificar **Até** para especificar uma hora de término para a tarefa de mesclagem.

d. Clique em **Salvar**.

A programação de mesclagem é especificada e aparece na página **Programar**.

Adicionar programação de acelerador

a. Clique em **Adicionar** e selecione **Adicionar programação de acelerador.**

A caixa de diálogo **Adicionar nova programação do acelerador** é aberta.

b. Especifique o limite de taxa de transferência em unidades de MB por minuto.

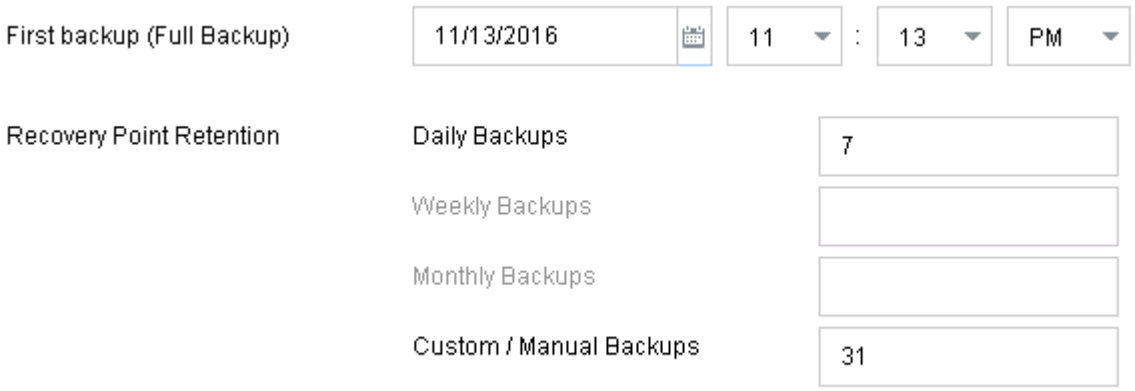
c. Especifique a hora de início para iniciar a tarefa de taxa de transferência de backup.

d. Especifique **Até** para especificar um horário de término para a tarefa de taxa de transferência.

e. Clique em **Salvar**.

A Programação de acelerador é especificada e exibida na página **Programar**.

2. Especifique a hora de início do backup programado.



3. Especifique as configurações de retenção de pontos de recuperação para programação diária, semanal e mensal.

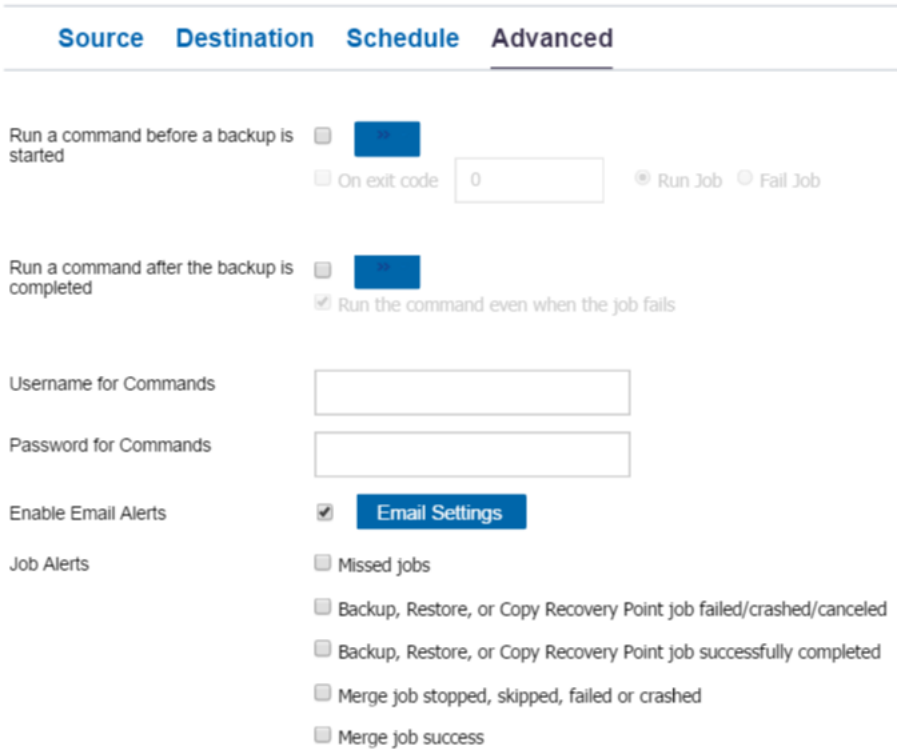
   Essas opções serão ativadas se tiver adicionado a programação de backup correspondente. Se você modificar as configurações de retenção desta página, as alterações serão refletidas na caixa de diálogo **Programação de backup**.

   A programação é especificada. Agora, especifique os detalhes de Avançado.

Especificar as configurações avançadas

A guia **Avançado** permite especificar algumas configurações avançadas para a tarefa de backup. As configurações avançadas incluem o fornecimento da localização dos scripts e as configurações de email.

A imagem a seguir mostra a guia **Avançado**:



Siga estas etapas:

1. Especifique os seguintes detalhes.

Executar um comando antes do início do backup

Permite a execução de um script antes de iniciar a tarefa de backup. Especifique o caminho em que o script está armazenado dentro do nó do proxy. Clique em **No código de saída** e especifique o código de saída para **Executar tarefa** ou **Tarefa com falha**. **Executar a tarefa** indica que a tarefa de backup continuará quando o script retornar o código de saída. **Tarefa com falha** indica que a tarefa de backup será interrompida quando o script retornar o código de saída.

Executar um comando após a conclusão do backup

Permite executar um script depois que a tarefa de backup foi concluída. Especifique o caminho completo onde o script está armazenado.

Executar um comando, mesmo quando a tarefa falhar

Se essa caixa de seleção for selecionada, o script especificado em **Executar um comando após a conclusão do backup** é executado mesmo quando a tarefa de backup falha. Caso contrário, aquele script é executado somente quando a tarefa de backup é concluída com êxito.

Nome de usuário para comandos

Permite especificar o nome de usuário para executar os comandos.

Senha para comandos

Permite especificar a senha para executar os comandos.

Ativar alertas por email

Permite ativar alertas por email. É possível especificar configurações de email e os tipos de alertas que você deseja receber por email. Ao selecionar esta opção, as seguintes opções serão ativadas para a seleção.

Configurações de email

Permite configurar as definições de email. Clique em **Configurações de email** e configure o servidor de email e os detalhes do servidor proxy. Para obter mais informações sobre como configurar Configurações de email, consulte o tópico Configuração de email e alerta.

Alertas de tarefa

Permite selecionar os tipos de emails de alerta de tarefas que deseja receber.

2. Clique em **Salvar**.

Observação: quando você seleciona um nó como origem de backup ou proxy de backup, o Arcserve UDP verifica se o agente está instalado no nó do proxy e se é a versão mais recente. Em seguida, o Arcserve UDP exibe uma caixa de diálogo de verificação que lista todos os nós que possuem uma versão antiga do agente ou que não tem o agente instalado. Para instalar/atualizar o agente nesses nós, selecione o método de instalação e clique em **Salvar**.

As alterações são salvas e uma marca de seleção verde aparece ao lado do nome da tarefa. A página do plano é fechada.

Observação: se precisar adicionar outra tarefa, deverá selecionar o plano na guia **Recursos** e modificar o plano. Para modificar o plano, clique no plano do painel central. O plano é exibido e será possível modificá-lo. É possível adicionar as tarefas **Copiar ponto de recuperação**, **Cópia em fita**, **Replicar** e **Replicar de um RPS remoto** como tarefas de acompanhamento.

O plano é automaticamente implantado ao nó do servidor proxy.

O plano de backup do exchange online para o servidor proxy é criado. O backup é executado de acordo com a programação que você configurou na guia **Programar**. Também é possível fazer backup manual quando desejado.

(Opcional) Executar um backup manual

Normalmente, com base nas configurações de programação aplicadas, os backups são executados automaticamente. Além do backup programado, um backup

manual fornece a opção de fazer backup dos nós de acordo com a necessidade. Por exemplo, se repetir a programação para backups completos e incrementais e desejar fazer grandes alterações em seu computador, você deverá executar um backup manual imediato sem esperar até que ocorra o próximo backup programado. É possível enviar a tarefa de backup a partir de ambos: console e interface de usuário proxy. Usando o Monitor de tarefas, é possível exibir o status da tarefa e cancelar a tarefa em andamento.

Para executar um backup manual dos nós do OneDrive, Siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.

   Os nós do OneDrive são exibidos no painel central.
3. Selecione os nós do OneDrive dos quais deseja fazer backup e que possuem um plano atribuído a eles.
4. No painel central, clique em **Ações**, **Fazer backup agora**.

   A caixa de diálogo **Fazer backup agora** é exibida.
5. Selecione um tipo de backup e forneça um nome para a tarefa de backup.
6. Clique em **OK**.

   A tarefa de backup é executada.

Siga estas etapas: para executar um backup manual de um plano do OneDrive

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Planos** e clique em **Todos os planos**.

   Os planos de backup do OneDrive são exibidos no painel central.
3. Selecione o plano do qual você deseja fazer backup e certifique-se de que tenha um plano atribuído a ele.
4. No painel central, clique em **Ações**, **Fazer backup agora**.

   A caixa de diálogo **Fazer backup agora** é exibida.
5. Selecione um tipo de backup e forneça um nome para a tarefa de backup.
6. Clique em **OK**.

   A tarefa de backup é executada.

   O backup manual é realizado com êxito. Agora, você pode verificar o backup.

Verificar o backup

Para verificar a tarefa de backup, confirme se você criou com êxito o plano de backup. Depois de verificar se o plano está criado com êxito, confirme se a tarefa

de backup é executada conforme o programado. É possível verificar o status das tarefas de backup na guia **Tarefas**.

Siga estas etapas para verificar os planos:

1. Clique na guia **Recursos**.
2. No painel esquerdo, navegue para **Nós** e clique em **Todos os nós**.

   Uma lista de todos os nós é exibida no painel central.
3. Verifique se os planos são mapeados com nós.

Siga um destes métodos para verificar as tarefas de backup:

Método 1

1. Clique na guia **Tarefas**.
2. No painel à esquerda, clique em **Todas as tarefas concluídas**.

   O status de cada tarefa é incluído no painel central.
3. Verifique se a tarefa de backup é concluída com êxito.

   A tarefa de backup é verificada.

Método 2

1. Clique na guia **Tarefas**.
2. No painel esquerdo, clique em **Tarefas concluídas com êxito**.

   A lista de tarefas de backup concluídas é exibida no painel central.
3. Clique na tarefa que você deseja verificar.

   O painel direito é atualizado.
4. Em Detalhes da tarefa, clique no hiperlink **Exibir logs**.
5. Verifique se a tarefa de backup é concluída com êxito.

   A tarefa de backup é verificada.

Fazer a configuração da autenticação multifator

Quando uma organização tiver a autenticação multifatorial (MFA) ativada para os usuários, use a Autenticação moderna para adicionar nós.

Observação: embora a autenticação básica esteja ativada no locatário, você pode usar a Autenticação moderna para adicionar nós. Para obter mais informações sobre como adicionar nós a um plano usando a Autenticação moderna, consulte Autenticação moderna.

Gerenciando o backup e a restauração do Microsoft Teams

Esta seção fornece informações sobre como fazer backup e restaurar os dados do Microsoft Teams usando o Exchange Online e o SharePoint Online. O Arcserve UDP fornece o backup de mensagens (bate-papo) e arquivos compartilhados entre os canais privados, públicos e de grupo.

Sempre que você cria um canal privado, público e de grupo no Microsoft Teams, um site do SharePoint Online é criado automaticamente para ele. Este site do SharePoint Online tem uma pasta de biblioteca de documentos padrão, na qual todos os arquivos compartilhados em todas as conversas são salvos automaticamente. Você também pode personalizar as permissões e as opções de segurança para informações confidenciais.

Esta seção contém os seguintes tópicos:

Como fazer backup e restaurar as mensagens do Microsoft Teams (bate-papo) usando o Exchange Online

É possível fazer backup de bate-papos individuais usando a caixa de correio do usuário no backup do nó do Exchange Online do UDP. Todas as mensagens são armazenadas no servidor do Exchange Online, na pasta TeamsMessagesData, que está em uma pasta raiz. Esta seção fornece informações sobre como fazer backup e restaurar as mensagens do Microsoft Teams (bate-papo) usando o Exchange Online.

Esta seção contém os seguintes tópicos:

Fazer backup de mensagens do Microsoft Teams (bate-papo) usando o Exchange Online

Esta seção fornece informações sobre como fazer backup de mensagens do Microsoft Teams (bate-papo) usando o Exchange Online.

Esta seção contém os seguintes tópicos:

Como criar um plano de backup do Exchange Online

O Exchange Online é um aplicativo de email hospedado na nuvem da Microsoft. Para proteger seus itens de email do Exchange Online (emails, itens de calendário, contatos e assim por diante) a partir da nuvem da Microsoft, você precisa criar um plano. Um plano do Exchange Online consiste em uma tarefa de backup. Esta tarefa de backup permite especificar os nós do Exchange Online que você deseja proteger, o destino do backup e a programação de backup.

Esta seção contém os seguintes tópicos:

Verificar os pré-requisitos e as considerações

Revise os seguintes pré-requisitos e considerações antes de criar um plano de backup do Exchange Online.

Criando um plano de backup do Exchange Online:

Pré-requisitos:

Para a conta de backup:

- Use uma conta de serviço de backup com permissões de administrador global.
- Adicionar permissões de representação para o usuário do backup para a conta de backup do Exchange Online para conectar-se à organização do Exchange Online, executar backups e restaurar.

  Observação: se você não adicionar a conta de backup ao grupo de funções de Gerenciamento de detecção e não atribuir a permissão Reprodução de aplicativo, o backup apresentará falha.

- Associe a conta de usuário de backup a uma caixa de correio do Exchange Online.

Para o proxy de backup:

- Efetue logon no console.
- Instale o agente do Arcserve UDP no computador proxy em que você deseja executar o backup/a restauração.

Considerações:

- Ao fazer backup de um grande número de usuários, é possível usar grupos do Exchange para melhorar o backup e a otimização.
- A configuração padrão do backup do Exchange Online usa 4 segmentos de backup (um por usuário) de cada vez. Você também pode modificar os segmentos no arquivo de configuração de *Engine\BIN\Office365\Arcserve.Office365.Exchange.config*da seguinte forma:

```
<!--#region for multi thread--> <!--MultiThreadEnable default value:0. if enable, set 1.--> <add key="MultiThreadEnable" value ="1"/> <!--set how many thread will be used to backup mailbox. O valor padrão é 4--> <add key-y="MaxDegreeOfParallelismForMailbox" value="4"/> <!--#en-dregion-->
```

É recomendável definir um valor de 1 a 5. O valor máximo possível é 10. No entanto, não aconselhamos que você defina nenhum valor de 6 a 10.

Observação: o UDP 8.0 oferece suporte ao seguinte:

- Caixa de correio do usuário
- Caixa de correio compartilhada
- Pastas públicas ativadas para email
- Caixas de correio de sala
- Caixas de correio de equipamentos
- Caixas de correio de grupo

Observação: para obter mais informações sobre as práticas recomendadas para o Exchange Online, consulte Assuntos relacionados ao Exchange Online.

Criando um plano de backup do Exchange Online usando BA (Basic Authentication - Autenticação básica):

Revise os seguintes pré-requisitos:

- Instale o PowerShell versão 5.1 ou superior (parte da WMF, Windows Management Framework - Estrutura de Gerenciamento do Windows) no servidor proxy (computador de 64 bits).
- Instale os seguintes módulos do PowerShell no servidor proxy usando a janela do PowerShell:
  - Para instalar o módulo do Azure, execute o seguinte comando:

    Install-Module -Name AzureAD -Force
  - Para instalar o módulo ExchangeOnlineManagement, execute o seguinte comando:

    Install-Module -Name ExchangeOnlineManagement -Force

Observação: ao instalar módulos do PowerShell usando os comandos acima, uma versão mais recente dos módulos poderá ser instalada dependendo da versão do GA do componente disponível no repositório da Microsoft.

Criando um plano de backup do Exchange Online usando MA (Modern Authentication - Autenticação moderna):

Revise os Pré-requisitos antes de criar um plano usando a autenticação moderna.

Adicionar o grupo e a função necessários à conta de backup do Exchange Online para executar backup e restauração

Adicione a conta de backup ao grupo de funções de Gerenciamento de detecção e atribuir a permissão de representação de aplicativo a ela.

Siga estas etapas:

1. Adicione o grupo e a função necessários por meio de uma das seguintes maneiras:

   Usando o portal do Office 365

a. Efetue logon no portal do Office 365 como administrador ou com uma conta que possua as permissões de administrador global.

   A página central do administrador do Exchange é exibida.

b. Vá para **permissões** e, na lista suspensa Adicionar, clique duas vezes em **Gerenciamento de detecção**.

   A caixa de diálogo Gerenciamento de detecção é exibida.

   Observação: o membro do grupo de funções de gerenciamento de detecção poderá pesquisar nas caixas de correio da organização do Exchange quanto aos dados que atendem a critérios específicos.

c. Em **Funções**, clique no **+** para adicionar a função ApplicationImpersonation.

   A caixa de diálogo Selecionar uma função é exibida.

d. Na lista suspensa **Nome de exibição**, selecione **ApplicationImpersonation**.

   Observação: a função ApplicationImpersonation permite que os aplicativos representem usuários em uma organização para executar tarefas em nome do usuário.

e. Clique em **Adicionar** para adicionar a função ApplicationImpersonation e clique em **OK**.

f. Na caixa de diálogo Gerenciamento de detecção, em **Membros**, clique em **+** para adicionar a conta de backup como um membro.

   A caixa de diálogo Selecionar membros é exibida.

g. Na lista suspensa Nome, selecione a conta de backup, clique em **Adicionar** para adicionar o membro e, em seguida, clique em **OK**.

   A conta de backup selecionada é exibida em **Membros** na caixa de diálogo **Gerenciamento de detecção**.

h. Clique em **Salvar**.

   Usando o PowerShell remoto

a. Para se conectar ao inquilino do Exchange Online usando o PowerShell remoto, consulte o link.

b. Depois de conectado, para adicionar a conta de backup como membro do grupo de funções de Gerenciamento de detecção, use o cmdlet:

   `"Add-RoleGroupMember"`

   Por exemplo: Add-RoleGroupMember "discovery management" -member userName@domain.onmicrosoft.com.

c. Para atribuir a função de representação de aplicativo à conta de backup, use o cmdlet:

   `"New-ManagementRoleAssignment"`

   Por exemplo:

   New-ManagementRoleAssignment -Nome: impersonationAssignmentName -Função:ApplicationImpersonation - Usuário: "user-name@domain.onmicrosoft.com"

A função ApplicationImpersonation e o grupo de membros são adicionados à conta de backup do Exchange Online.

Criar um plano de backup do Exchange Online

Um plano de backup inclui uma tarefa de backup que executa um backup dos itens de dados de email do Exchange Online (emails, itens de calendário, contatos etc.) e armazena os dados em um repositório de dados sem redução de redundância ou um repositório de dados de redução de redundância. Além disso, esse plano de backup permite que o UDP detecte e especifique os grupos do Exchange Online para os quais uma tarefa de backup é executada. Cada tarefa consiste em parâmetros que definem a origem, o destino, a programação e outros detalhes de backup.

Siga estas etapas:

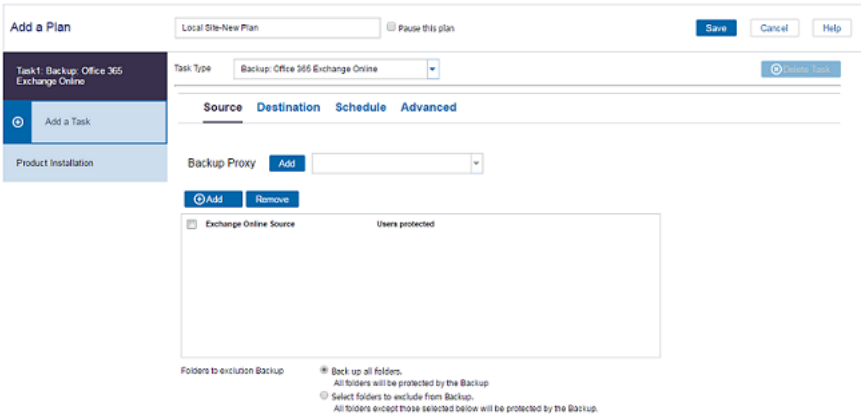
1. Clique na guia **Recursos** no Console.
2. No painel à esquerda, navegue para **Planos** e clique em **Todos os planos**.

   Se tiver criado os planos anteriores, esses planos serão exibidos no painel central.
3. No painel central, clique em **Adicionar um plano**.

   A caixa de diálogo **Adicionar um plano** abre.
4. Digite o nome do plano.
5. (Opcional) Selecione a caixa de seleção **Pausar este plano**.

   O plano não será executado até que você desmarque a caixa de seleção para retomar o plano.

   Observação: se um plano for pausado, nenhuma tarefa em andamento será pausada, mas todas as tarefas programadas correspondentes associadas a esse plano serão pausadas. No entanto, você pode executar uma tarefa manualmente. Por exemplo, você pode executar manualmente a tarefa de backup e a tarefa de replicação para um nó mesmo que o respectivo plano esteja pausado. Nesse caso, a tarefa seguinte da tarefa sob demanda (manual) não será executada. Por exemplo, há uma tarefa de replicação após uma tarefa de backup sob demanda, a tarefa de replicação não será executada para a tarefa de backup sob demanda. É necessário executar manualmente a tarefa de replicação. Quando você retomar o plano, as tarefas pendentes não são retomadas imediatamente. Depois de retomar o plano, as tarefas pendentes serão executadas no próximo horário programado.
6. Na lista suspensa Tipo de tarefa, selecione **Backup: Office 365 Exchange Online**.



Agora especifique os detalhes de Origem, Destino, Programação e Avançado.

Especificar a origem

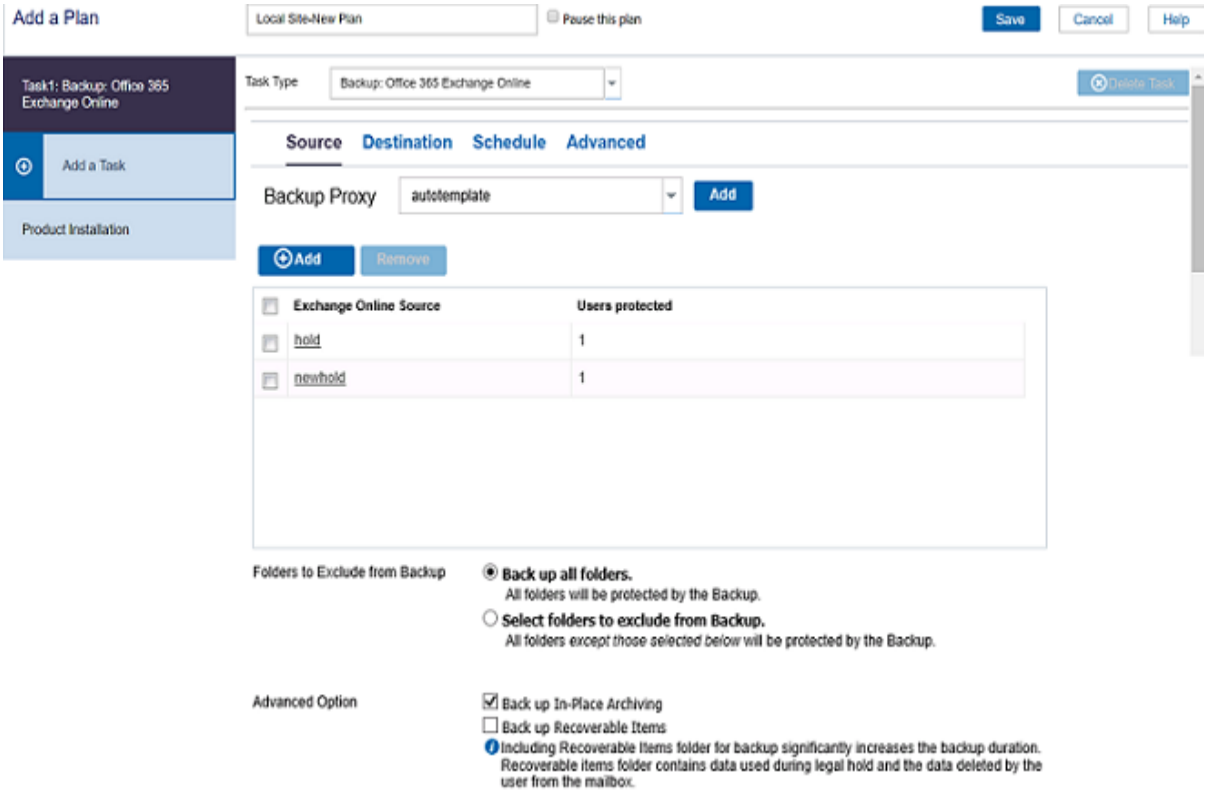
A página Origem permite especificar os nós de origem do Exchange Online que você deseja proteger. É possível selecionar mais de um nó de origem do Exchange Online em um plano. Caso não tenha adicionado nós no console, você pode adicionar nós de origem do Exchange Online a partir da página Origem.

Observação: é possível salvar um plano sem adicionar nós de origem, mas o plano só será implantado se você adicionar os nós.

Você também pode gerenciar os nós do Exchange Online usando o suporte a caixa de correio de pasta pública para a proteção do Exchange Online.

Siga estas etapas:

1. Clique na guia **Origem**.



2. Para o proxy de backup, execute um dos seguintes procedimentos:
   - Na lista suspensa, selecione um proxy de backup existente.
   - Para adicionar um novo proxy de backup, ao lado da lista suspensa, clique em **Adicionar**.
3. Adicione o nó do Exchange Online usando uma das seguintes opções:

   Método 1

a. Clique em **Adicionar** e em **Selecionar as origens a serem protegidas no Arcserve UDP**.

   A caixa de diálogo Adicionar nós ao plano é exibida.

b. Selecione um nó e clique em **Conectar**.

   Observação: também é possível procurar os nós do Exchange Online que você deseja proteger na **Pesquisa**.

c. Marque a caixa de seleção **Proteger todas as origens do Office 365 Exchange** para proteger todas as contas do Exchange Online em todas as páginas.

   Observação: para adicionar à lista protegida todas as contas do Exchange Online, clique na seta para a direita (>).

   As contas do Microsoft Exchange Online que você selecionar são adicionadas.

Método 2

- Clique em **Adicionar** e, em seguida, clique em **Adicionar origem do Exchange Online**.

  O diálogo Adicionar nós a um plano é exibido.

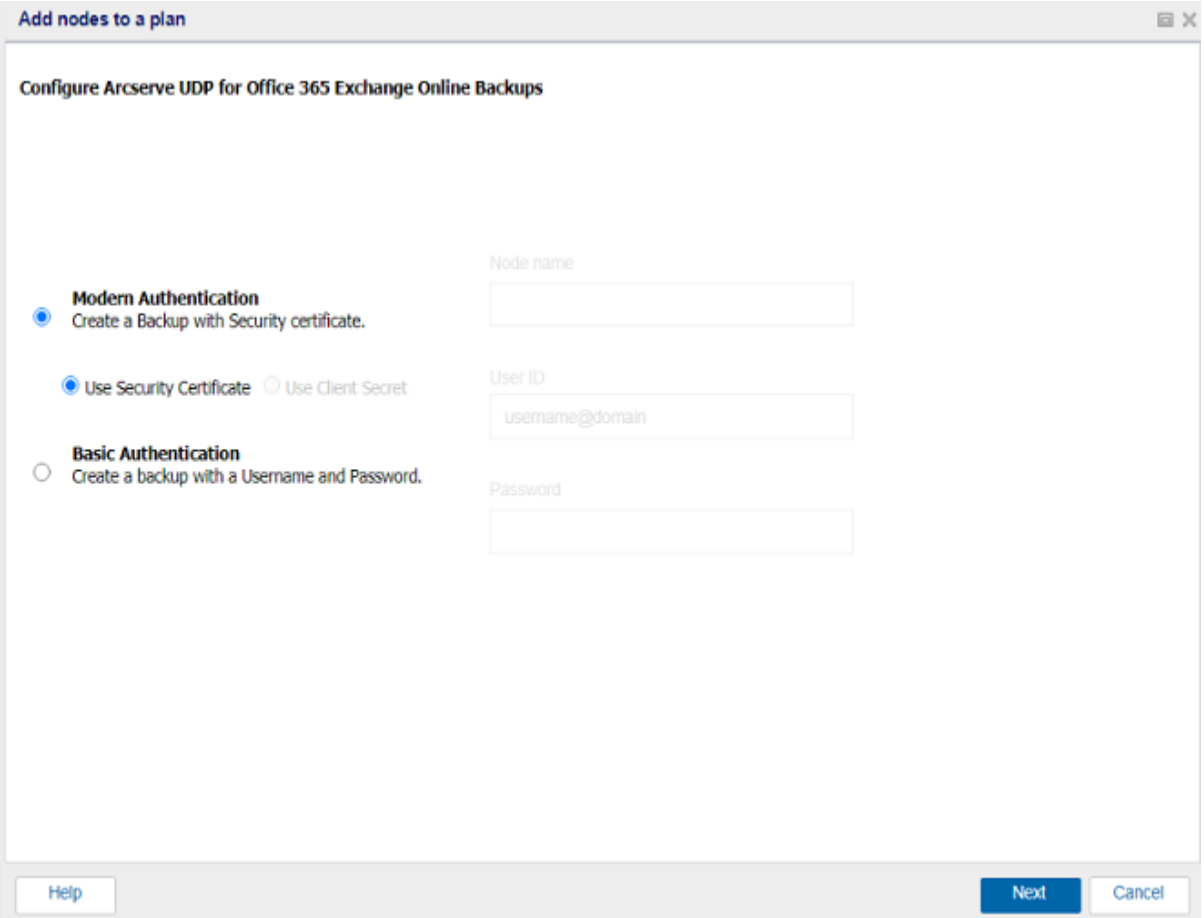
  Observação: diferentemente de outros nós, não é possível adicionar o nó do Exchange Online na página **Todos os nós**. Só é possível adicionar um nó do Exchange Online em um plano ou quando você modificar um plano.

  Vários nós do Exchange Online podem usar a mesma conta de usuário (conta de serviço) do Exchange Online.

4. Para aplicar a autenticação, siga um destes procedimentos:

Autenticação moderna

Para a autenticação moderna, você pode executar um backup usando o certificado de segurança.



Usar certificado de segurança

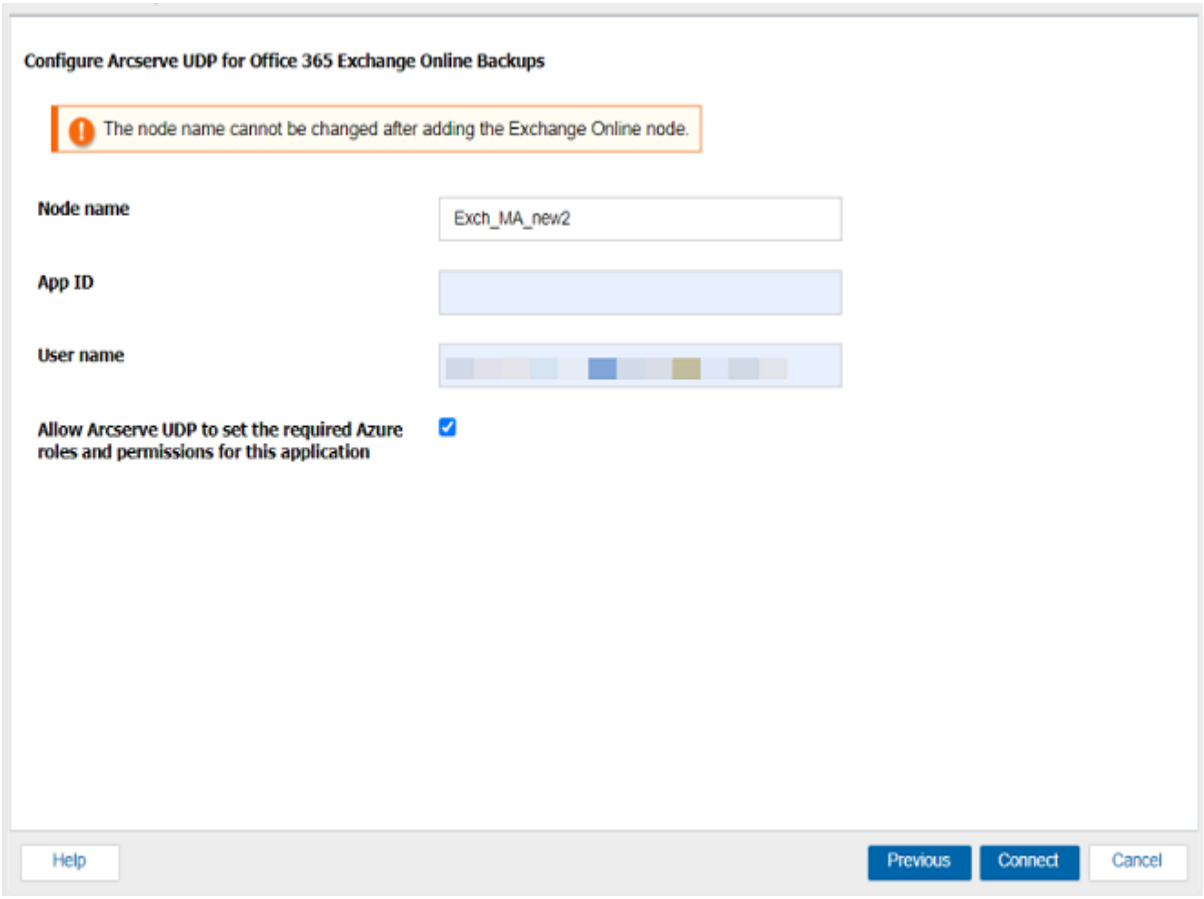
Observação: por padrão, o plano de backup seleciona **Usar certificado de segurança** para a autenticação moderna.

Siga estas etapas:

a. Para autenticar o aplicativo UDP com certificados de segurança, consulte Fazendo download do certificado do UDP e carregando-o no Azure.

b. Digite os seguintes detalhes:

- Nome do nó
- ID do aplicativo
- Nome de usuário



c. Para aplicar as permissões de API automaticamente, marque a caixa de seleção **Permitir que o Arcserve UDP defina as permissões de API necessárias para este aplicativo**.

   Observação: para aplicar as permissões manualmente sem usar a função de administrador global/de empresa, consulte Configurando as permissões da API manualmente sem usar a função de administrador global/de empresa.

d. Clique em **Conectar**.

Observações:

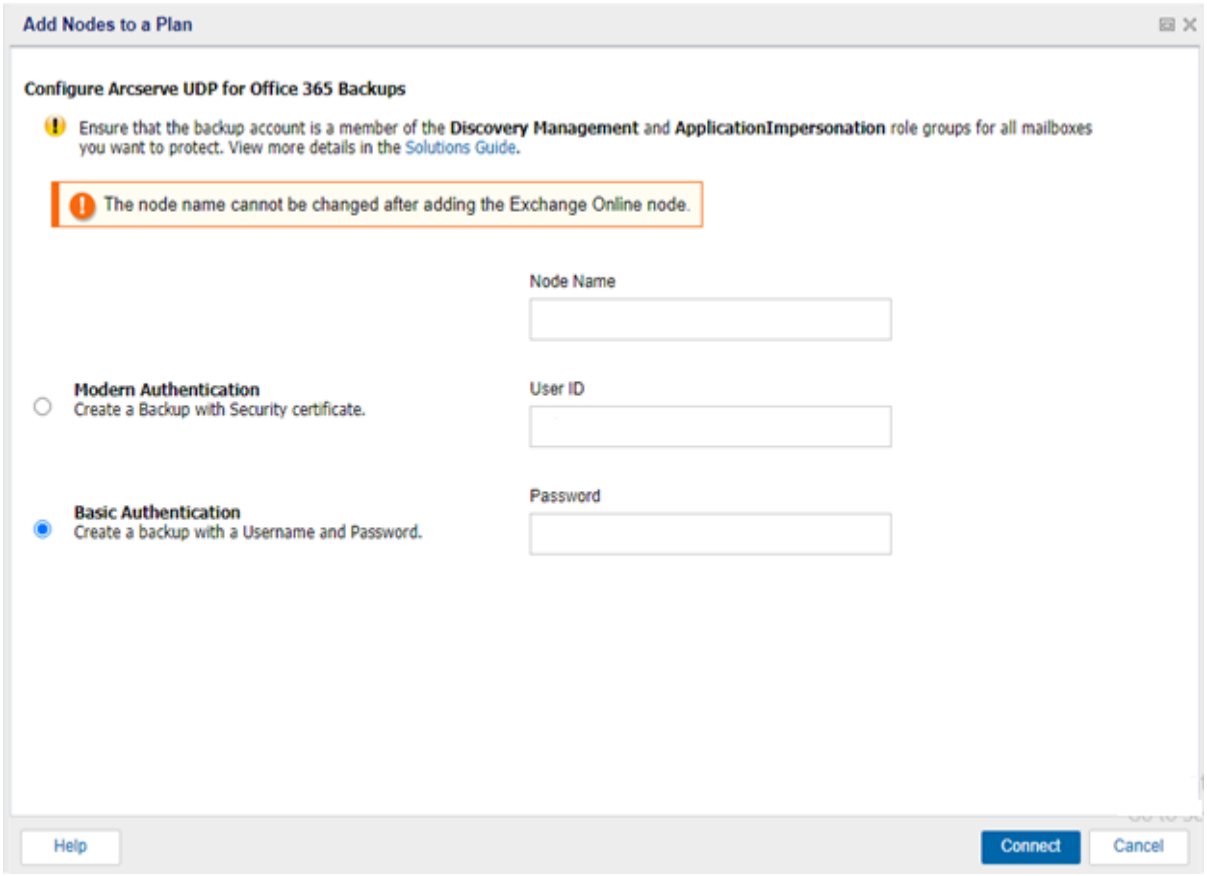
- O nome do nó do Exchange Online não pode ser alterado após a adição do nó.
- Digite o nome de usuário da conta de backup do Exchange Online que atender aos pré-requisitos em **Nome de usuário do administrador**.
- A Autenticação moderna não se aplica ao seguinte:

- Os clientes que usam o Microsoft 365 (Office 365) para suas instâncias do Arcserve Cloud Hybrid ou o Arcserve Cloud Backup para Office 365, que foi criado antes de 18 de outubro de 2020, não poderão usar a autenticação moderna.
- Os clientes que continuam usando a autenticação básica.

Autenticação básica

Para a autenticação básica, para continuar com o backup, forneça as seguintes informações e clique em **Conectar**:

- Nome do nó
- ID do usuário
- Senha



Observação: a atualização ou alteração da conta de usuário pode mudar o número de caixas de correio protegidas. Você precisa verificar se as contas de serviço novas ou atualizadas têm direitos de representação para as caixas de correio serem protegidas.

5. Para proteger as caixas de correio do Exchange Online, siga um destes procedimentos:

   - Para proteger todas as caixas de correio e grupos do Exchange Online, marque a caixa de seleção **Proteger todas as origens do Office 365 Exchange**.

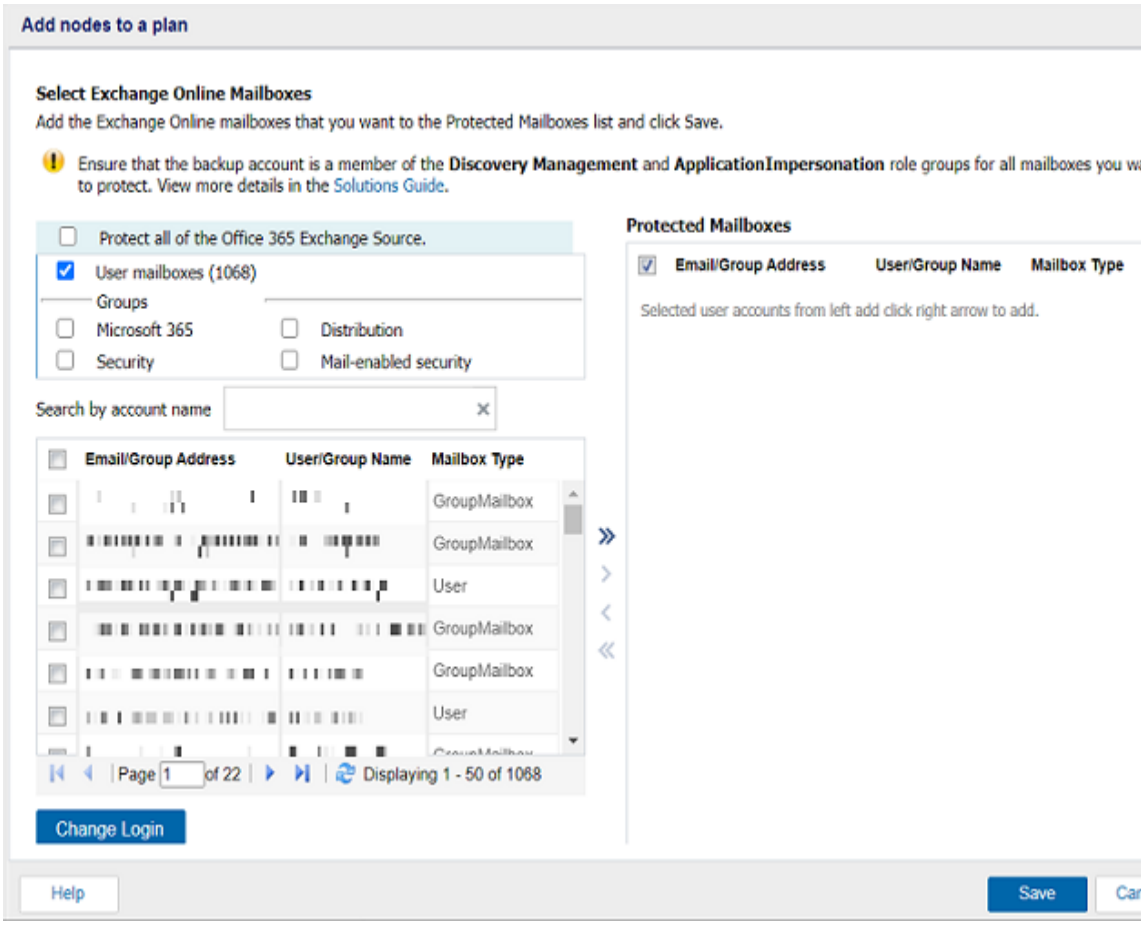
     Observação: essa opção é selecionada automaticamente por padrão quando a tela Selecionar caixas de correio do Exchange Online é exibida.

   - Para Caixas de correio do usuário, siga estas etapas:

     a. Marque a caixa de seleção **Caixas de correio do usuário**.

        Uma lista de caixas de correio do usuário é exibida.

     b. (Opcional) Para pesquisar uma conta na lista, no campo Pesquisar por nome de conta, digite o nome da conta.



     c. Na lista de caixas de correio do usuário, selecione as caixas de correio que deseja proteger.

d. Clique na seta para a direita (>) para mover as caixas de correio selecionadas para a lista Caixas de correio protegidas.

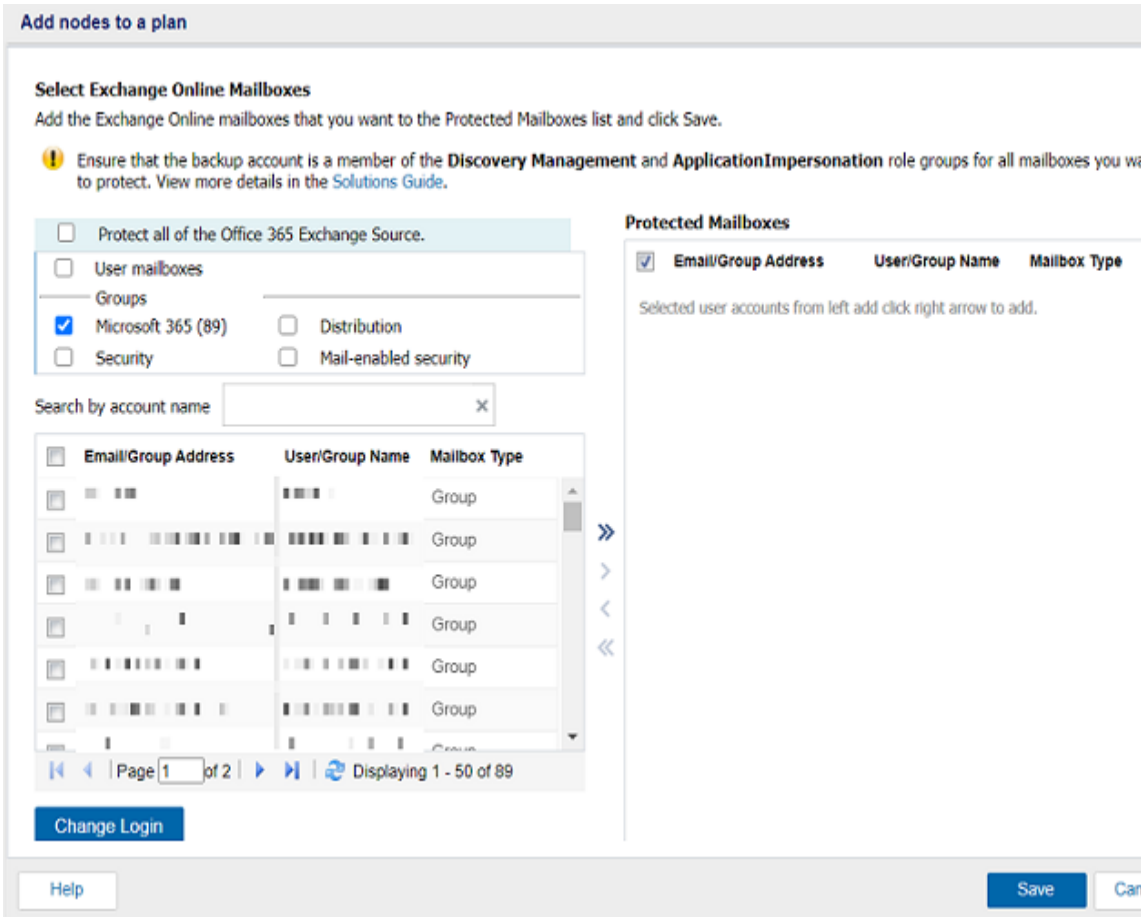
- Para Grupos, siga estas etapas:

a. Marque a caixa de seleção **Microsoft 365**.

Uma lista de grupos é exibida.

Observação: se desejar selecionar grupos juntamente com subgrupos, como **Distribuição**, **Segurança** ou **Segurança ativada por email**, marque a caixa de seleção **Microsoft 365** e, em seguida, marque a caixa de seleção de um subgrupo, conforme necessário.

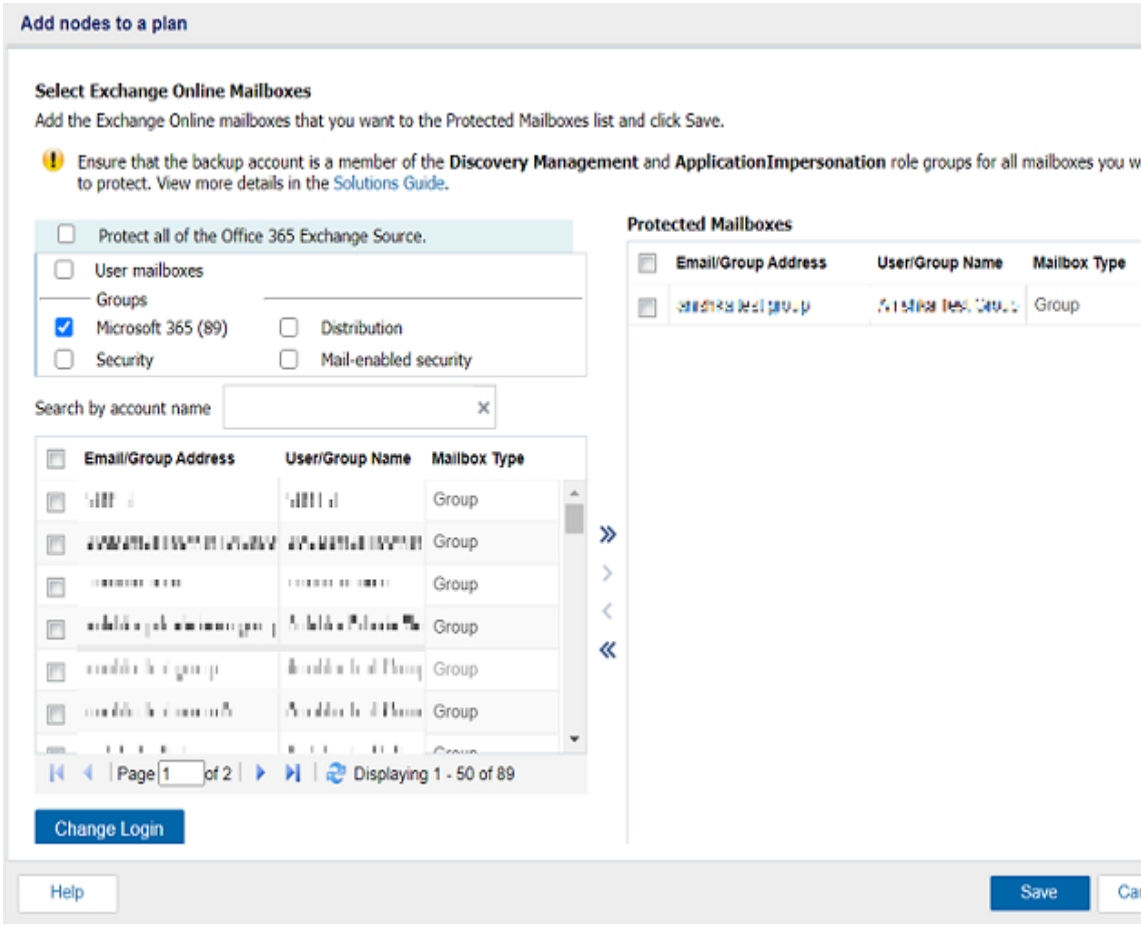
b. (Opcional) Para pesquisar uma conta na lista, no campo Pesquisar por nome de conta, digite o nome da conta.



c. Na lista de grupos, selecione os grupos que deseja proteger.

d. Clique na seta para a direita (>) para mover os grupos sele-

cionados para a lista Caixas de correio protegidas.



6. Clique em **Salvar**.
7. Na guia Origens, vá para **Pastas a serem excluídas do backup** e marque a caixa de seleção desejada.
8. Em Opção avançada, marque a caixa de seleção desejada.
    - Para permitir que a proteção do Exchange Online ofereça suporte a uma caixa de correio de arquivo morto, marque a caixa de seleção **Fazer backup do arquivo morto local**.

      Observação: para obter mais informações sobre caixa de correio de arquivo morto, clique neste link.
    - Marque a caixa de seleção **Fazer backup dos itens recuperáveis** para permitir a proteção da caixa de correio que ativa o recurso Retenção local ou Retenção de litígio.

      Observação: para Retenção local e Retenção de litígio do arquivo morto do Exchange Online, clique neste link.

Observação: para ativar ambos os recursos na caixa de correio ao mesmo tempo, de modo a fazer backup dos itens recuperáveis presentes na caixa de correio de arquivo morto, selecione as opções **Fazer backup do arquivo morto local** e **Fazer backup dos itens recuperáveis**.

Especificar o destino

O destino é o local onde você armazena os dados de backup. É necessário, no mínimo, especificar o destino para salvar o plano.

Siga estas etapas:

1. Clique na guia **Destino**.
2. Selecione a opção **Servidor de ponto de recuperação do Arcserve UDP. O servidor de ponto de recuperação do Arcserve UDP** especifica que o destino de backup é um servidor de ponto de recuperação. Se você selecionar essa opção, os dados serão armazenados como pontos de recuperação. Não é possível armazenar dados como conjuntos de dados de recuperação.
3. Forneça os detalhes a seguir:
   a. Selecione um servidor de ponto de recuperação.
   b. Selecione um repositório de dados de redução de redundância ou de não redução de redundância. A lista exibe todos os repositórios de dados criados no servidor de ponto de recuperação especificado.
   c. Forneça uma senha da sessão. A senha da sessão é opcional quando o destino de backup é um repositório de dados do RPS não criptografado.
   d. Confirme a senha da sessão.

O destino é especificado.

Especificar a programação

A página Programar permite definir uma programação para o backup e para que as funções Mesclar e Acelerar sejam repetidas em intervalos específicos. Após definir uma programação, as tarefas são executadas automaticamente de acordo com a programação. É possível adicionar várias programações e fornecer configurações de retenção.

Uma Programação de backup se refere a programação regular que é repetida várias vezes ao dia, com base no número de horas ou de minutos selecionado. Além da programação regular, uma programação de backup também fornece opções para adicionar programações diária, semanal e mensal.

Observação: para obter mais informações sobre as configurações de retenção e programação, consulte Entendendo a programação avançada e retenção.

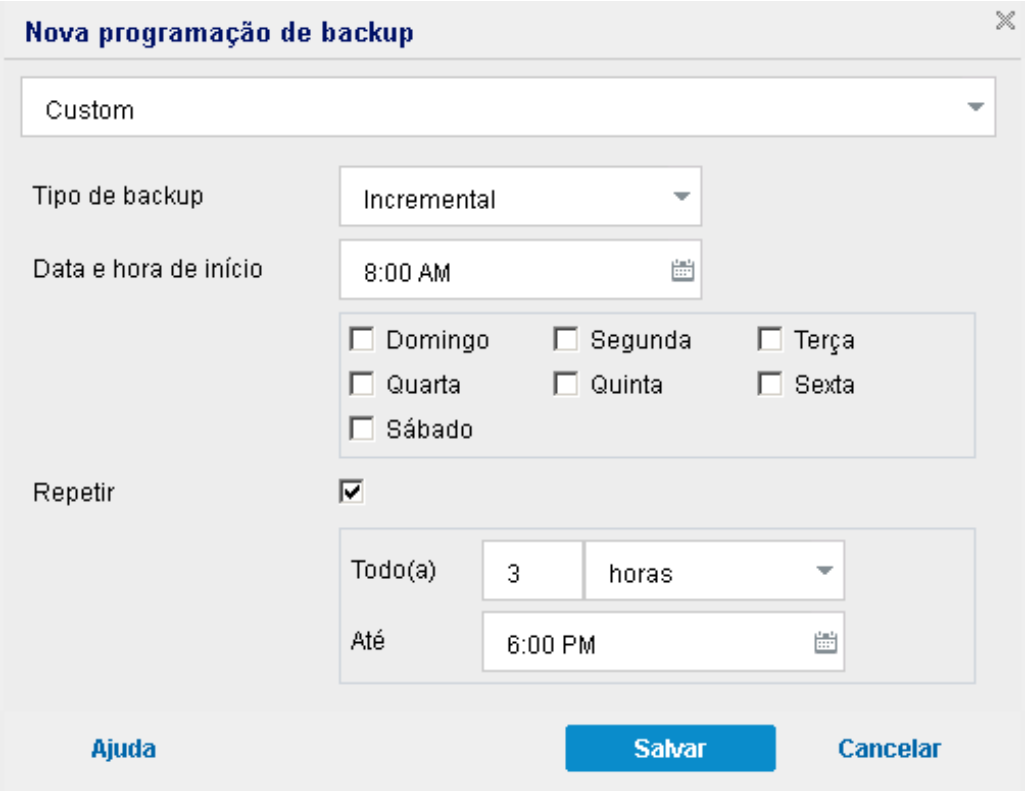
Siga estas etapas:

1. Adicionar programações de backup, mesclagem e acelerador.

   Adicionar programação de backup

   a. Clique em **Adicionar** e selecione **Adicionar programação de backups**.

      A caixa de diálogo **Nova programação de backup** é aberta.



   b. Selecione uma das seguintes opções:

Personalizado

Especifica a programação de backup que se repete várias vezes por dia.

Diário

Especifica a programação de backup que ocorre uma vez por dia. Por padrão, todos os dias da semana estão selecionados para o backup diário. Se não desejar executar a tarefa de backup em um dia específico, desmarque a caixa de seleção correspondente àquele dia da semana.

Semanal

Especifica a programação de backup que ocorre uma vez por semana.

Mensal

Especifica a programação de backup que ocorre uma vez por mês.

c. Selecione o tipo de backup.

Completo

Especifica a programação de backups para backups completos. Conforme programado, o Arcserve UDP executa um backup completo de todos os blocos usados do computador de origem. Um backup completo em geral, consome tempo, dependendo do tamanho do backup.

Incremental

Especifica a programação de backups para backups incrementais.

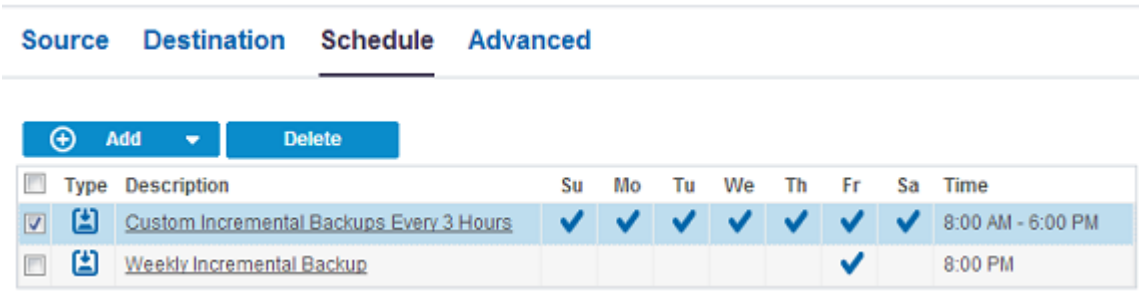
Conforme programado, o Arcserve UDP faz backup incremental apenas dos blocos que foram alterados após o último backup realizado com êxito. As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a executar um backup.

d. Especifique a hora de início do backup.

e. (Opcional) Marque a caixa de seleção de **Repetição** e especifique a programação a ser repetida.

f. Clique em **Salvar**.

A programação de backup é especificada e aparece na página **Programar**.



Adicionar Programação de mesclagem

a. Clique em **Adicionar** e selecione **Adicionar programação de mesclagem**.

   A caixa de diálogo **Adicionar nova programação de mesclagem** é aberta.

b. Especifique a hora de início para iniciar a tarefa de mesclagem.

c. Especificar **Até** para especificar uma hora de término para a tarefa de mesclagem.

d. Clique em **Salvar**.

A programação de mesclagem é especificada e aparece na página **Programar**.

Adicionar programação de acelerador

a. Clique em **Adicionar** e selecione **Adicionar programação de acelerador.**

   A caixa de diálogo **Adicionar nova programação do acelerador** é aberta.

b. Especifique o limite de taxa de transferência em unidades de MB por minuto.

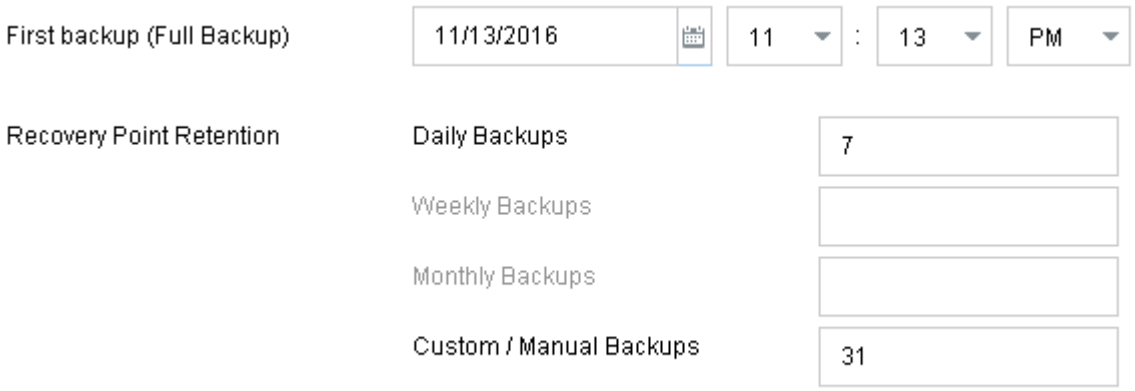
c. Especifique a hora de início para iniciar a tarefa de taxa de transferência de backup.

d. Especifique **Até** para especificar um horário de término para a tarefa de taxa de transferência.

e. Clique em **Salvar**.

A Programação de acelerador é especificada e exibida na página **Programar**.

2. Especifique a hora de início do backup programado.



3. Especifique as configurações de retenção de pontos de recuperação para programação diária, semanal e mensal.

   Essas opções serão ativadas se tiver adicionado a programação de backup correspondente. Se você modificar as configurações de retenção desta página, as alterações serão refletidas na caixa de diálogo **Programação de backup**.

   A programação é especificada.

Noções básicas sobre a programação avançada e retenção

A opção de programação permite especificar uma programação personalizada, uma programação diária/semanal/mensal ou ambas. Na programação personalizada, é possível configurar a programação de backups para cada dia da semana ou adicionar até quatro programações de backup em cada dia. É possível escolher um dia específico da semana e criar uma janela para definir quando executar o backup e em que frequência.

Programação	Tarefa com suporte	Comentários
Backup	Tarefa de backup	Definir janelas de tempo para a execução de tarefas de backup.
Limitação de backup	Tarefa de backup	Definir janelas de tempo para controlar a velocidade de backup.
Mesclar	Tarefa de mesclagem	Definir quando executar tarefas de mesclagem.
Programação diária	Tarefa de backup	Definir quando executar tarefas do backup diário.
Programação semanal	Tarefa de backup	Definir quando executar tarefas do backup semanal.
Programação mensal	Tarefa de backup	Definir quando executar tarefas do backup mensal.

Também é possível especificar as configurações de retenção para os pontos de recuperação.

Observação: as configurações de retenção devem ser definidas em cada plano para controlar como os dados dos nós atribuídos a esse plano são retidos no repositório de dados de destino.

As programações para backups diários/semanais/mensais são independentes para a programação personalizada e umas das outras. É possível configurar para executar somente o backup diário, semanal ou mensal, sem configurar a Programação personalizada.

Programação de tarefas de backup

É possível adicionar quatro janelas de tempo por dia na programação do backup. Uma janela de tempo é válida das 00:00 às 23:59. Não é possível especificar uma janela de tempo das 18:00 às 6:00. Nesses casos, você deve especificar manualmente duas janelas de tempo diferentes.

Para cada janela de tempo, a hora de início é inclusiva e a hora de término é exclusiva. Por exemplo, você configurou para executar o backup incremental em intervalos de uma hora entre as 6:00 e as 9:00. O backup será iniciado às 6:00. Isso significa que o backup será executado às 6h00, 7h00 e 8h00, mas NÃO às 9h00.

Observação: se você deseja executar a tarefa de backup várias vezes até o fim do dia, defina a programação para até 0h00. Por exemplo, para executar a tarefa de backup a cada 15 minutos o dia inteiro, defina a programação como das 0h00 às 00h00, a cada 15 minutos.

Programação do acelerador de backup

A programação de aceleração do backup permite controlar a velocidade da taxa de transferência de backup o que, por sua vez, controla o uso de recursos (E/S de disco, CPU, largura de banda de rede) do servidor cujo backup está sendo feito. Isso é útil quando se não quiser afetar o desempenho do servidor durante o horário comercial. É possível adicionar quatro janelas de tempo por dia na sua programação de aceleração do backup. Para cada janela de tempo, é possível especificar um valor, em MB por minuto. Esse valor será usado para controlar a taxa de transferência do backup. Os valores válidos variam entre 1 MB/minutos a 99999 MB/minutos.

Se uma tarefa de backup estende seu tempo especificado, o limite de aceleração será ajustado de acordo com o tempo especificado. Por exemplo, você definiu o limite de aceleração de backup como 500 MB/minuto das 8:00 às 20:00 e 2500 MB/minuto das 20:00 às 22:00. Se uma tarefa de backup iniciar às 19h00 e for executada durante três horas, das 19h00 às 20h00 o limite de aceleração será de 500 MB/minuto e das 20h00 às 22h00, o limite de aceleração será 2500 MB/minuto.

Se não definir nenhuma programação do backup e programação da taxa de transferência do backup, o backup será executado o mais rápido possível.

Mesclar a programação

Permite mesclar pontos de recuperação com base na programação fornecida.

Considere os seguintes pontos para a tarefa de mesclagem:

- A qualquer momento apenas uma tarefa de mesclagem pode ser executada para um nó.
- Se uma tarefa de mesclagem iniciar, ela precisará ser concluída antes que a próxima tarefa de mesclagem seja iniciada. Isso significa que, se um ou mais conjuntos de pontos de recuperação forem mesclados, não será possível adicionar o

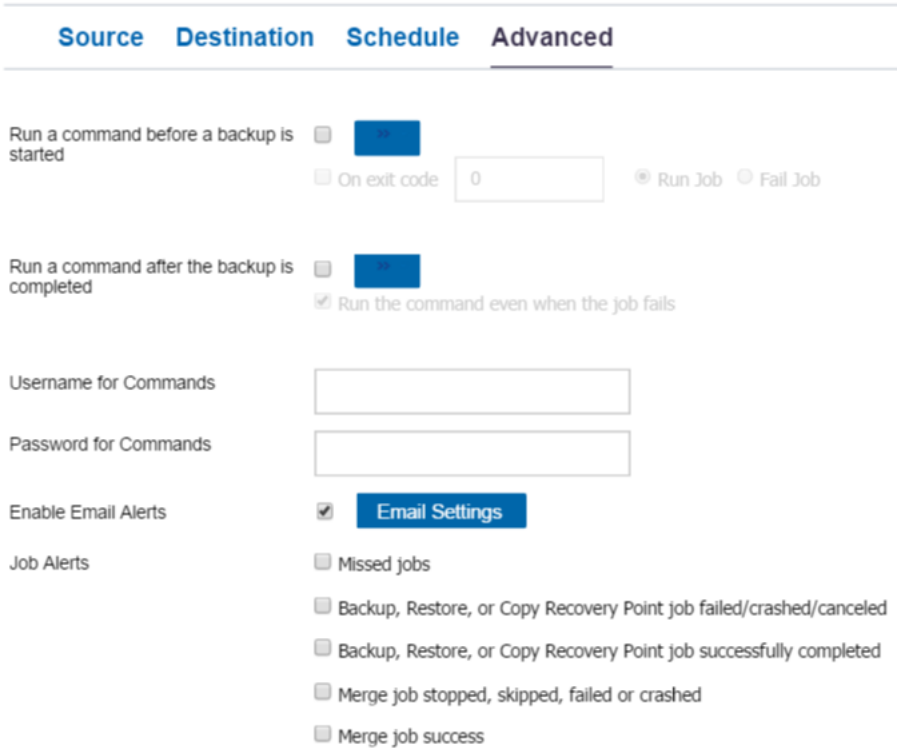
novo ponto de recuperação a este processo de mesclagem, até que o processo de mesclagem do conjunto atual de ponto de recuperação seja concluído.

- Se uma tarefa de mesclagem estiver processando mais de um conjunto de pontos de recuperação (por exemplo, conjunto [1~4], conjunto [5~11] e conjunto [12~14]; são três conjuntos) o servidor de ponto de recuperação processará esses conjuntos, um por um.
- Se uma tarefa de mesclagem é retomada após um intervalo, a tarefa detectará em que ponto ela foi pausada e continuará a mesclagem a partir do ponto de pausa.

Especificar as configurações avançadas

A guia **Avançado** permite especificar algumas configurações avançadas para a tarefa de backup. As configurações avançadas incluem o fornecimento da localização dos scripts e as configurações de email.

A imagem a seguir mostra a guia **Avançado**:



Siga estas etapas:

1. Especifique os seguintes detalhes.

   Executar um comando antes do início do backup

   Permite a execução de um script antes de iniciar a tarefa de backup. Especifique o caminho em que o script está armazenado dentro do nó do proxy. Clique em **No código de saída** e especifique o código de saída para **Executar tarefa** ou **Tarefa com falha**. **Executar a tarefa** indica que a tarefa de backup continuará quando o script retornar o código de saída. **Tarefa com falha** indica que a tarefa de backup será interrompida quando o script retornar o código de saída.

   Executar um comando após a conclusão do backup

   Permite executar um script depois que a tarefa de backup foi concluída. Especifique o caminho completo onde o script está armazenado.

   Executar um comando, mesmo quando a tarefa falhar

Se essa caixa de seleção for selecionada, o script especificado em **Executar um comando após a conclusão do backup** é executado mesmo quando a tarefa de backup falha. Caso contrário, aquele script é executado somente quando a tarefa de backup é concluída com êxito.

Nome de usuário para comandos

Permite especificar o nome de usuário para executar os comandos.

Senha para comandos

Permite especificar a senha para executar os comandos.

Ativar alertas por email

Permite ativar alertas por email. É possível especificar configurações de email e os tipos de alertas que você deseja receber por email. Ao selecionar esta opção, as seguintes opções serão ativadas para a seleção.

Configurações de email

Permite configurar as definições de email. Clique em **Configurações de email** e configure o servidor de email e os detalhes do servidor proxy. Para obter mais informações sobre como definir as configurações de email, consulte Configuração de email e alerta.

Alertas de tarefa

Permite selecionar os tipos de emails de alerta de tarefas que deseja receber.

2. Clique em **Salvar**.

Observação: quando você seleciona um nó como origem de backup ou proxy de backup, o Arcserve UDP verifica se o agente está instalado no nó do proxy e se é a versão mais recente. Em seguida, o Arcserve UDP exibe uma caixa de diálogo de verificação que lista todos os nós que possuem uma versão antiga do agente ou que não tem o agente instalado. Para instalar/atualizar o agente nesses nós, selecione o método de instalação e clique em **Salvar**.

As alterações são salvas e uma marca de seleção verde aparece ao lado do nome da tarefa. A página do plano é fechada.

Observação: se precisar adicionar outra tarefa, deverá selecionar o plano na guia **Recursos** e modificar o plano. Para modificar o plano, clique no plano do painel central. O plano é exibido e será possível modificá-lo. É possível adicionar as tarefas **Copiar ponto de recuperação**, **Cópia em fita**, **Replicar** e **Replicar de um RPS remoto** como tarefas de acompanhamento.

O plano é automaticamente implantado ao nó do servidor proxy.

O plano de backup do exchange online para o servidor proxy é criado. O backup é executado de acordo com a programação que você configurou na guia **Programar**. Também é possível fazer backup manual quando desejado.

(Opcional) Executar um backup manual

Em geral, os backups são executados automaticamente e controlados pelas configurações da programação. Além do backup programado, um backup manual fornece a opção de fazer backup dos nós de acordo com a necessidade. Por exemplo, se repetir a programação para backups completos e incrementais e desejar fazer grandes alterações em seu computador, você deverá executar um backup manual imediato sem esperar até que ocorra o próximo backup programado.

Para executar um backup manual dos nós do Exchange Online, siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.

   Os nós Exchange Online são exibidos no painel central.
3. Selecione os nós do Exchange Online (por exemplo, Caixa de correio@<nomedaorganização.com>) dos quais você deseja fazer backup e que tenha um plano atribuído a ele. O nome do nó é a conta usada durante a adição do nó do Exchange Online e de sua conexão.
4. Clique com o botão direito do mouse no nó e selecione **Fazer backup agora**.

   A caixa de diálogo Fazer backup agora é exibida.
5. Selecione o tipo de backup que deseja executar e clique em **OK**.

   A caixa de diálogo Informações do andamento é exibida.
6. Aguarde até que a tarefa de backup seja concluída e clique em **OK**.
7. Para monitorar as tarefas de backup, navegue até **tarefas** > **Tarefas em andamento**.

   Aguarde até a conclusão da tarefa de backup.

   O backup manual é realizado com êxito.

Para executar um backup manual do plano do Exchange Online, siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Planos** e clique em **Todos os planos**.

   Os planos de backup do Exchange Online são exibidos no painel central.
3. Selecione o plano do qual você deseja fazer backup e que tenha um plano atribuído a ele.
4. Clique com o botão direito do mouse no plano e selecione **Fazer backup agora**.

A caixa de diálogo Fazer backup agora é exibida.

5. Selecione o tipo de backup que deseja executar e clique em **OK**.

   A caixa de diálogo Informações do andamento é exibida.

6. Aguarde até que a tarefa de backup seja concluída e clique em **OK**.

7. Para monitorar as tarefas de backup, navegue até **tarefas** > **Tarefas em andamento**.

   Aguarde até a conclusão da tarefa de backup.

   O backup manual é realizado com êxito.

Verificar o backup

Para verificar o backup, confirme se você criou com êxito o plano de backup. Depois de verificar se o plano está criado com êxito, confirme se a tarefa de backup é executada conforme o programado. É possível verificar o status das tarefas de backup na guia **Tarefas**.

Siga estas etapas para verificar os planos:

1. Clique na guia **Recursos**.
2. No painel esquerdo, navegue para **Nós** e clique em **Todos os nós**.

   Uma lista de todos os nós é exibida no painel central.
3. Verifique se os planos são mapeados com nós.

Siga um destes métodos para verificar as tarefas de backup:

Método 1

1. Clique na guia **Tarefas**.
2. No painel à esquerda, clique em **Todas as tarefas**.

   O status de cada tarefa é incluído no painel central.
3. Verifique se a tarefa de backup é concluída com êxito.

   A tarefa de backup é verificada.

Método 2

1. Clique na guia **Tarefas**.
2. No painel esquerdo, clique em **Tarefas concluídas com êxito**.

   A lista de tarefas de backup concluídas é exibida no painel central.
3. Clique na tarefa que você deseja verificar.

   O painel direito é atualizado.
4. Em Detalhes da tarefa, clique no hiperlink **Exibir logs**.
5. Verifique se a tarefa de backup é concluída com êxito.

   A tarefa de backup é verificada.

Restaurar as mensagens do Microsoft Teams (bate-papo) usando o Exchange Online

É possível restaurar as mensagens do Microsoft Teams (bate-papo) usando o Exchange Online a partir da nuvem da Microsoft usando qualquer computador. Você pode restaurar dados do ponto de recuperação para o local original ou um local alternativo.

Execute as tarefas a seguir para restaurar os dados do Exchange Online:

1. Selecionar os itens de caixa de correio do Exchange Online a serem restaurados
2. Definir as opções de restauração
3. Restaurar os itens recuperáveis
4. Restaure o conteúdo do ponto de recuperação
5. Verificar se o conteúdo foi restaurado

Selecione os itens de email do Exchange Online a serem restaurados

É possível restaurar dados de email do Exchange Online a partir de um ponto de recuperação. Ao selecionar uma data de recuperação e, em seguida, especificar a hora, todos os pontos de recuperação associados a esse período são exibidos. Você pode procurar e selecionar o conteúdo do backup (incluindo aplicativos) a ser restaurado.

Siga estas etapas:

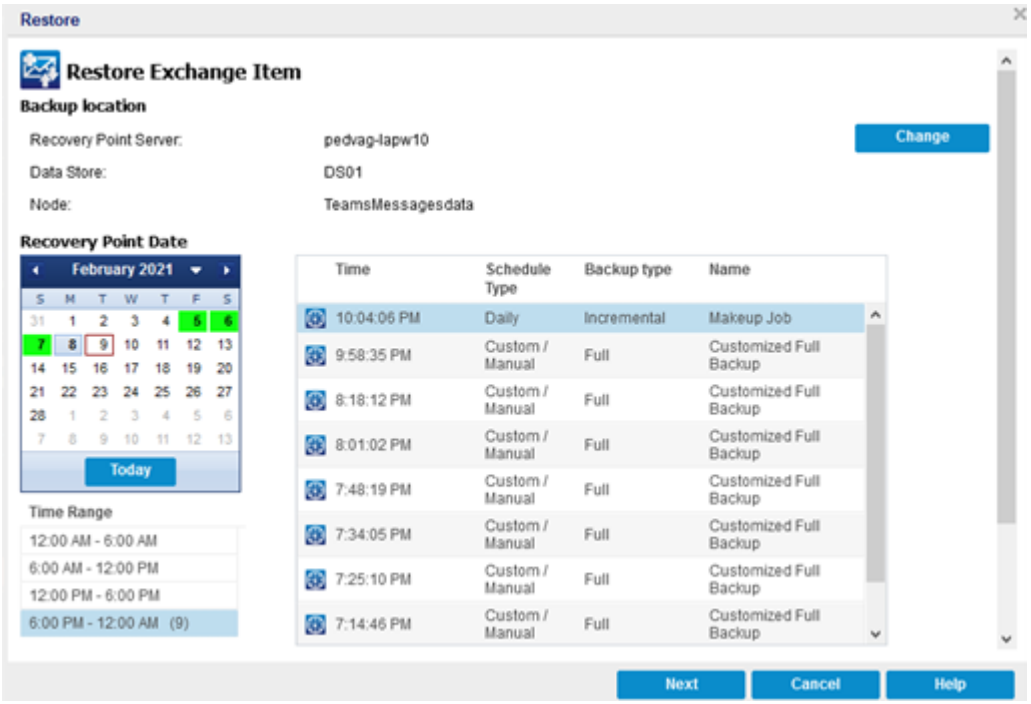
1. Efetue logon no Arcserve UDP.
2. Clique na guia **Recursos**.
3. Selecione **Todos os nós** no painel esquerdo.

   Todos os nós do adicionados são exibidos no painel central.
4. No painel central, selecione o nó do Exchange Online e clique em **Ações**.
5. Clique em **Restaurar** na lista suspensa Ações.

   A caixa de diálogo Restaurar item do Exchange é exibida.

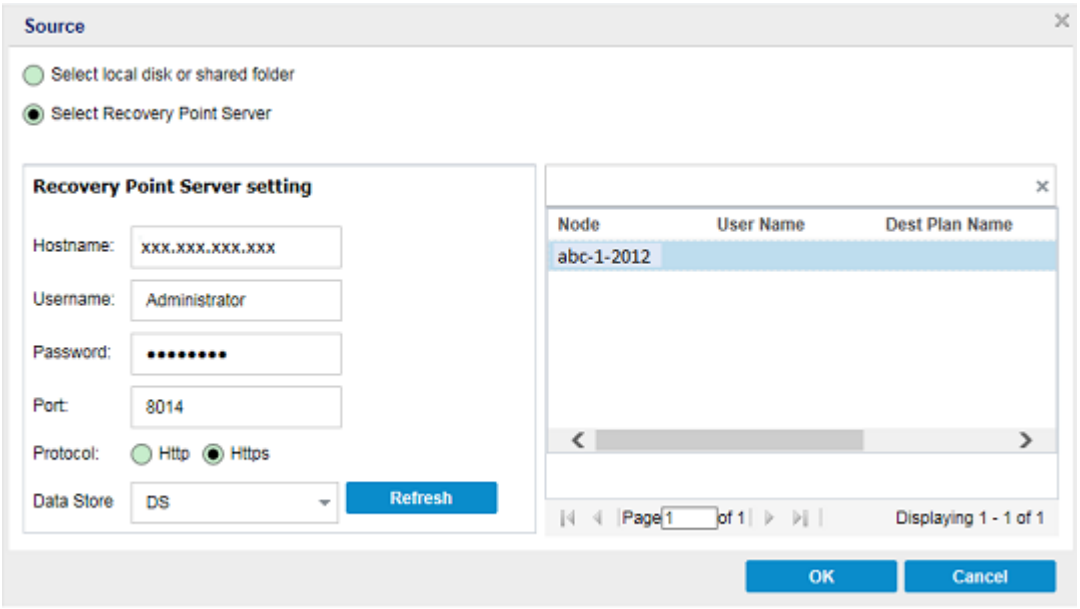
   Observação: você é automaticamente conectado ao nó do agente, e a caixa de diálogo **Restaurar item do Exchange** é aberta.

   É possível ver os detalhes do Servidor de ponto de recuperação no Local do backup.



6. (Opcional) Para modificar o local do backup, clique em **Alterar**.

   A caixa de diálogo Origem é exibida. É possível selecionar o local do backup na caixa de diálogo.



   Observação: quando você adiciona uma tarefa de cópia em fita ao plano e deseja restaurar o ponto de recuperação de backup da cópia em fita, selecione o ponto de recuperação no backup da cópia em fita. Para obter mais informações, consulte Procurar ponto de recuperação de cópia em fita para restauração.

7. Para especificar a origem, selecione uma das opções a seguir e clique em **OK**:

   Selecionar o disco local ou uma pasta compartilhada

   Observação: no Arcserve UDP, não recomendamos que você marque a opção **Selecionar o disco local ou a pasta compartilhada**.

   Selecionar servidor de ponto de recuperação

   a. Especifique os detalhes da configuração do servidor de ponto de recuperação e clique em **Atualizar**.

      Todos os agentes estão listados na coluna Agente de proteção de dados na caixa de diálogo Origem.

   b. Selecione o agente na lista exibida e clique em **OK**.

      Os pontos de recuperação são listados na caixa de diálogo Restaurar item do Exchange.

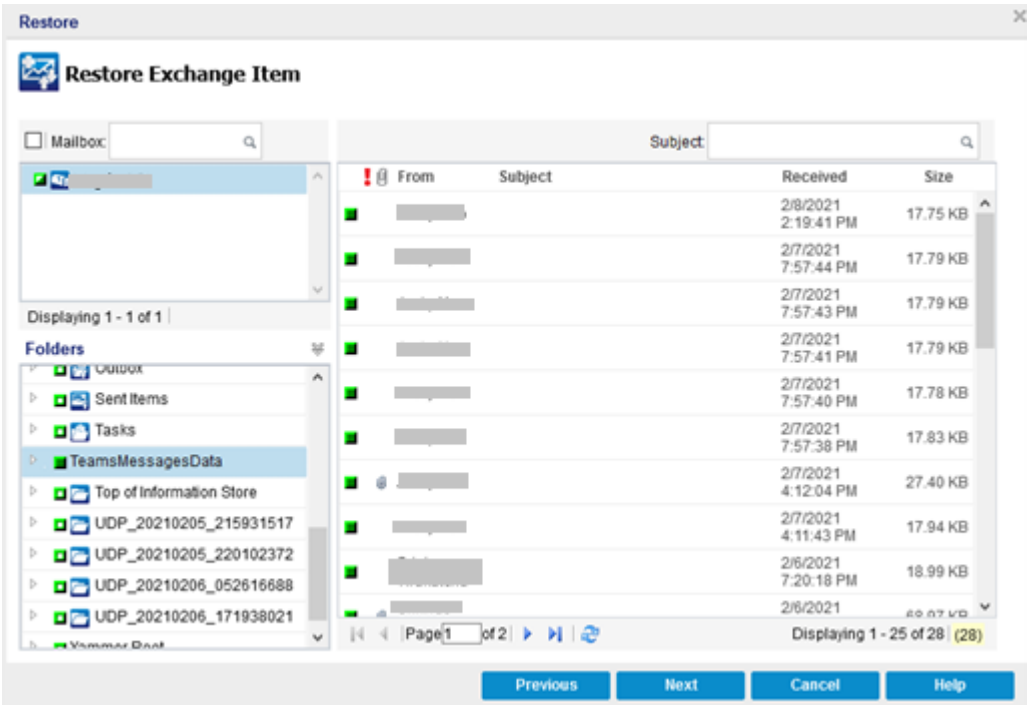
Observação: na **Pasta** do ponto de recuperação, você pode ver várias subpastas de mesmo nome junto com os nós do Exchange Online. Isso acontece porque a GUID do nó muda e uma nova pasta de ponto de recuperação é criada quando você exclui um nó e o adiciona novamente no plano de teste.

8. Selecione a data do calendário para a imagem de backup a ser restaurada e clique em **Avançar**.

   Todas as datas que contém pontos de recuperação para a origem do backup especificado são realçadas em verde.

   Os pontos de recuperação correspondentes a essa data são exibidos, juntamente com a hora do backup, o tipo de backup que foi executado (completo, incremental ou de verificação) e o nome do backup.

9. No painel **Caixa de correio**, clique na caixa de correio que deseja restaurar.



   Todos os itens de email relacionados à caixa de correio são exibidos no painel Pastas.

10. Selecione a pasta **TeamsMessagesData** e clique em **Avançar**.

    Observações:

    - É possível selecionar parte ou todo o conteúdo do objeto do Exchange a ser restaurado. Para selecionar o conteúdo parcial, expanda o objeto e clique na caixa de seleção do conteúdo.
    - Você pode selecionar vários objetos do Exchange a serem restaurados.

    A caixa de diálogo Opções de restauração é exibida.

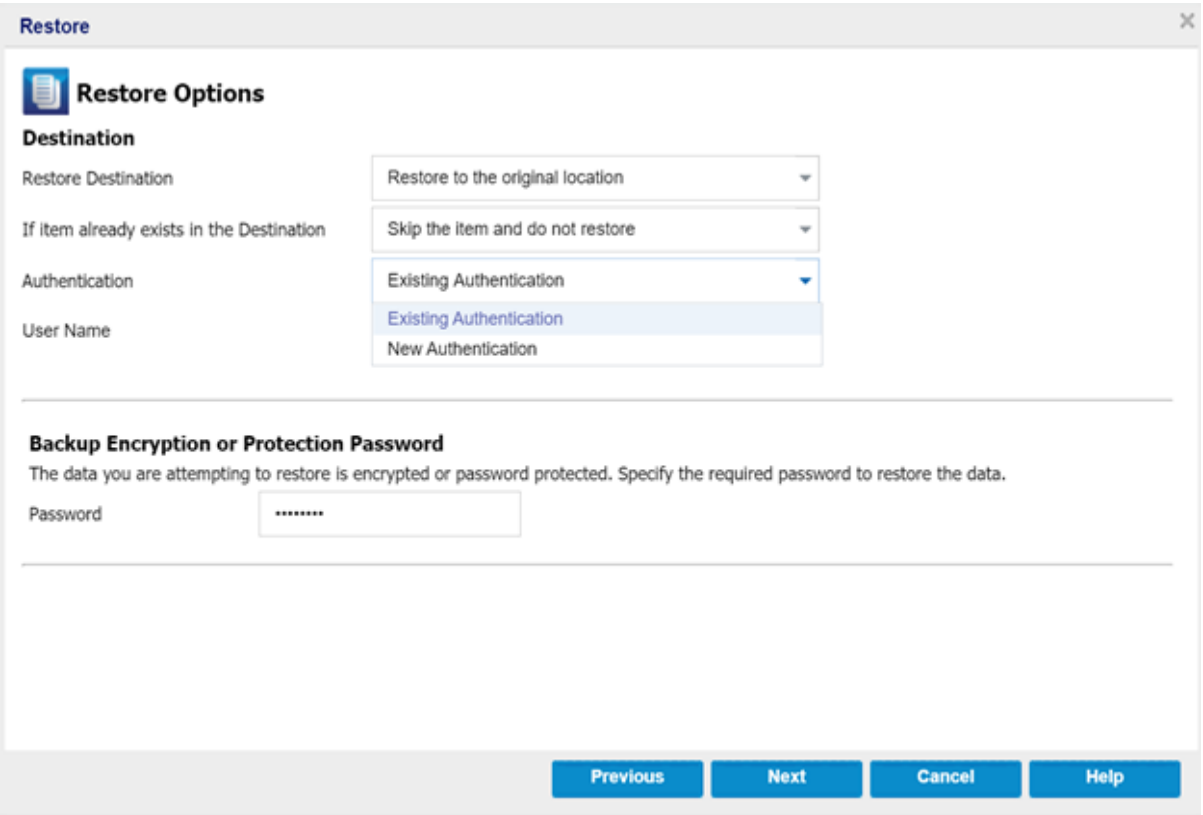
Os itens de email do Exchange Online a serem restaurados são selecionados. Agora, você pode definir as opções de restauração.

Definir as opções de restauração

Depois de especificar as informações do Exchange Online a serem restauradas, defina as opções de restauração do conteúdo selecionado.

Siga estas etapas:

1. Na caixa de diálogo Opções de restauração, selecione o destino da restauração.



As opções de destino disponíveis são:

Restaurar no local original

Restaura os dados de email para o mesmo local do qual você fez um backup.

Observações:

- Se você restaurar ao local original, os dados não serão refletidos nas mensagens do Teams. Esta não é uma restauração completa no local original, pois não é possível executar a restauração da pasta raiz.
- Se você restaurar um item de email no local original usando a opção Substituir duas vezes, após a restauração pela segunda vez, o item de

email da primeira restauração não será substituído. Como resultado, dois itens de email semelhantes serão exibidos no local original.

- Se você restaurar um item de email no local original usando a opção Ignorar, e na pasta original um item semelhante ao item restaurado já existir, a tarefa de backup exibirá o resultado incompleto.

Restaure em um local alternativo.

Restaura os dados de email em outra caixa de correio ou outra pasta na caixa de correio original. Ao selecionar essa opção, procure e selecione o destino.

2. Especifique uma das opções a seguir no menu suspenso **Se o item já existir no destino**:

Ignorar o item e não restaurar

Ignora os itens e não restaura.

Padrão: ignorar o item e não restaurar.

Substituir o item no destino

Substitui o item no destino.

Observação: a lista suspensa Se o item já existir no destino ficará disponível se você selecionar a opção **Restaurar no local original** na lista suspensa Restaurar o destino.

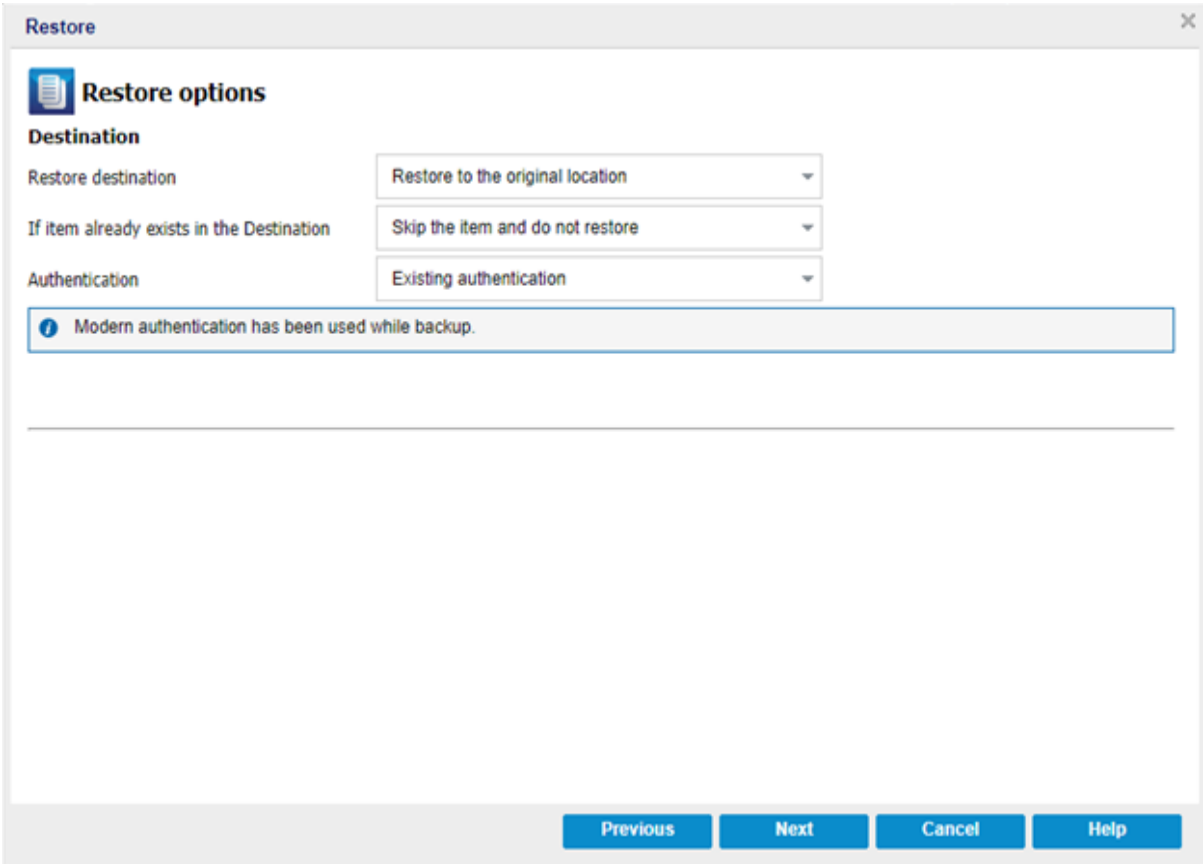
Autenticação

Valida e identifica a conta de usuário. Selecione uma das seguintes opções:

- **Autenticação existente**

  Quando você seleciona Autenticação existente, o tipo de autenticação que foi selecionado durante a criação do nó é usado.

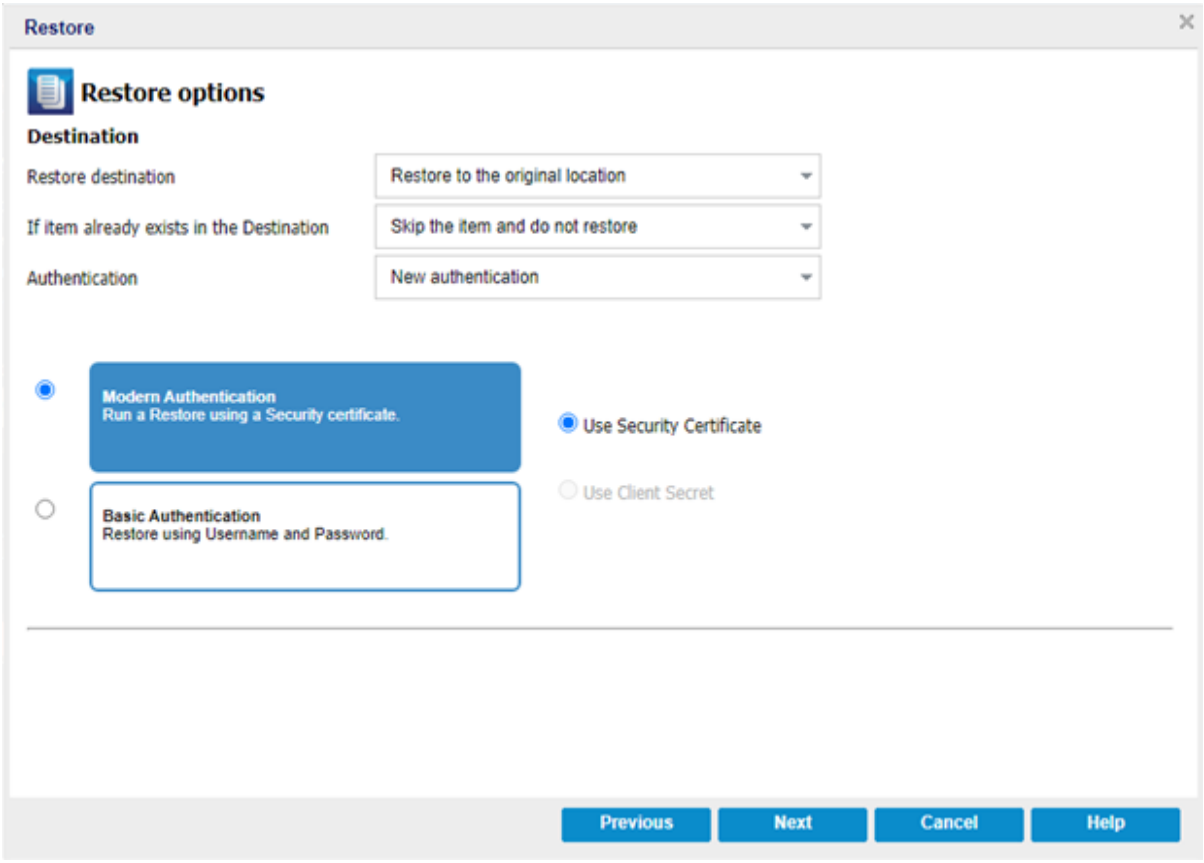
  - Se a autenticação do nó for básica, parâmetros como Nome de usuário, Senha e Criptografia de backup ou proteção por senha [se criptografada], serão carregados automaticamente para prosseguir com a restauração.
  - Se a autenticação do nó for moderna, parâmetros como Nome de usuário e Criptografia de backup ou proteção por senha [se criptografada], serão carregados automaticamente para prosseguir com a restauração.



- **Nova autenticação**

  Durante a restauração, é possível selecionar uma das seguintes opções para alterar o tipo de autenticação:

  - Autenticação moderna
  - Autenticação básica



3. Para aplicar a autenticação, siga um destes procedimentos:

   Autenticação moderna

   Para a autenticação moderna, é possível executar uma restauração usando o certificado de segurança.

   Usar certificado de segurança

   Observação: por padrão, o plano de backup seleciona **Usar certificado de segurança** para a autenticação moderna.

   Siga estas etapas:

   a. Para autenticar usando um certificado autoassinado, consulte Fazendo download do certificado do UDP e carregando-o no Azure.

   b. Digite a ID do aplicativo e o nome do usuário.

   c. Para aplicar as funções e permissões necessárias, marque a caixa de seleção **Permitir que o Arcserve UDP defina as funções e permissões necessárias do Azure para este aplicativo** e clique em **Avançar**.

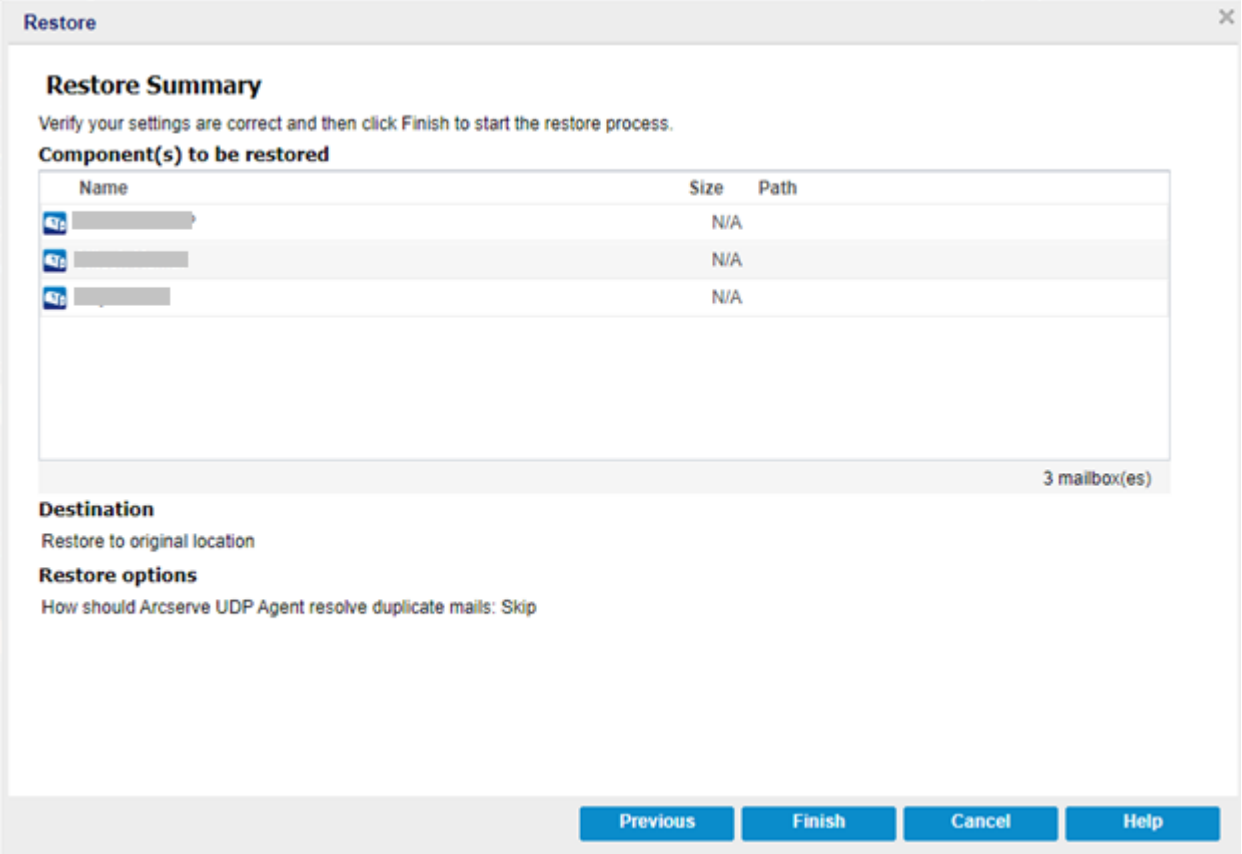
Autenticação básica

Para Autenticação básica, para continuar com a restauração, digite o nome do usuário e a senha.

Observação: essa opção falhará se a autenticação moderna estiver ativada no locatário ou na conta.

4. Clique em **Avançar**.

   A caixa de diálogo Resumo da restauração é exibida.



5. Na janela Resumo da restauração, verifique as configurações e clique em **Concluir**.

As opções de restauração são definidas para restaurar as informações do Exchange Online.

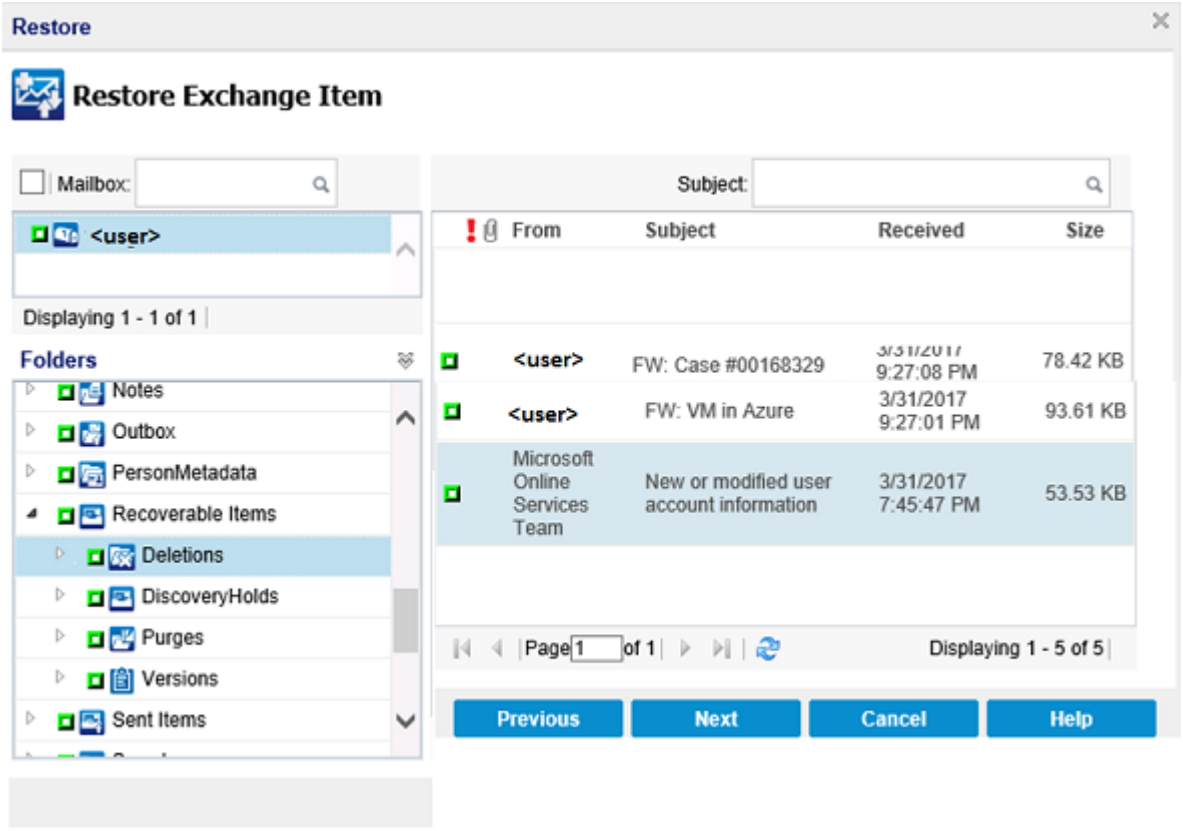
Restaurar os itens recuperáveis

Você pode restaurar os itens recuperáveis da caixa de correio que ativa o recurso Retenção local ou Retenção de litígio, pela IU do nó do Exchange Online, para procurar a sessão de backup. Para ativar esse recurso, consulte Especificar a origem.

Depois de ativar o recurso, usando o Assistente de restauração, é possível restaurar os itens recuperáveis.

Siga estas etapas:

1. Na caixa de diálogo Restaurar item do Exchange, selecione as pastas desejadas em **Itens recuperáveis** e clique em **Avançar**.



A tela Opção de restauração é exibida.

2. Na tela Opção de restauração, execute os seguintes detalhes e clique em **Avançar**:
   - Selecione o destino da restauração.
   - Caso o item já exista no destino, ignore-o ou substitua-o.

   Você pode executar uma restauração Original ou Alternativa.

   Restauração original

Os itens em Itens recuperáveis são restaurados na pasta *UDP_RecoverableItems_yyyyMMdd_HHmmssfff*, que é criada na caixa de correio de destino. As opções Ignorar e Substituir apresentadas para restauração não se aplicam a esses itens.

Restauração alternativa

Como ocorre com a caixa de correio do usuário, os itens selecionados são restaurados no caminho de destino em uma pasta exclusiva com carimbo de data/hora, como *titled /restore_yyyyMMdd-mmssff*.

- Forneça a ID de usuário e senha do destino onde você deseja restaurar os itens.

Os itens recuperáveis selecionados são restaurados.

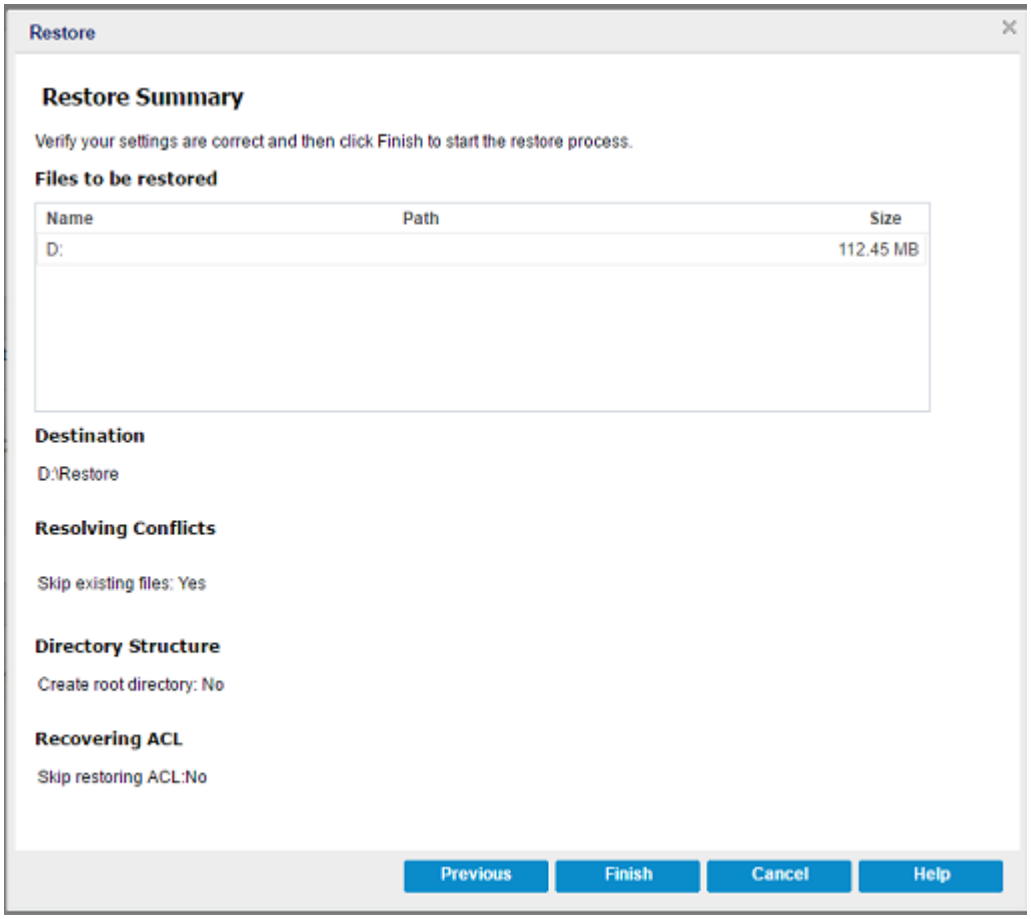
O ponto de recuperação do conteúdo é guardado.

Restaure o conteúdo do ponto de recuperação

Após definir as opções de restauração, verifique se suas configurações estão corretas e confirme o processo de restauração. O **Resumo da restauração** o auxilia a revisar todas as opções de restauração definidas e modificá-las se necessário.

Siga estas etapas:

1. Na caixa de diálogo Resumo da restauração, examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.



   - Se as informações do resumo não estiverem corretas, clique em **Anterior** e volte à caixa de diálogo em questão para alterar a configuração incorreta.
   - Se as informações de resumo estiverem corretas, clique em **Concluir** para iniciar a tarefa de restauração.

O ponto de recuperação do conteúdo é guardado.

Verificar se o conteúdo foi restaurado

Após a conclusão do processo de restauração, verifique se o conteúdo foi restaurado no destino especificado.

Siga estas etapas:

1. Efetue logon na caixa de correio de destino.
2. Verifique o item de caixa de correio que você restaurou.
3. Verifique o conteúdo restaurado.

   A restauração do conteúdo é verificada com êxito.

Como fazer backup e restaurar os arquivos do Microsoft Teams usando o SharePoint Online

Sempre que você cria um canal privado, público e de grupo no Microsoft Teams, um site do SharePoint Online é criado automaticamente para ele. Este site do SharePoint Online tem uma pasta de biblioteca de documentos padrão, na qual todos os arquivos compartilhados em todas as conversas são salvos automaticamente. Você também pode personalizar as permissões e as opções de segurança para informações confidenciais.

Quando você cria qualquer grupo no Microsoft Teams, um site do SharePoint Online com o nome **Team - Group_name** é criado automaticamente. Todos os arquivos compartilhados nos canais públicos são salvos neste site.

Quando você cria qualquer canal privado no grupo do Microsoft Teams, outro site do SharePoint Online com o nome **Teams_Group_name - Private_Channel_name** é criado para esse canal privado, além do site criado para o grupo Equipe.

Esta seção fornece informações sobre como fazer backup e restaurar os arquivos do Microsoft Teams usando o SharePoint Online.

Esta seção contém os seguintes tópicos:

Fazer backup de arquivos do Microsoft Teams usando o SharePoint Online

Esta seção fornece informações sobre como fazer backup de arquivos do Microsoft Teams usando o SharePoint Online.

Esta seção contém os seguintes tópicos:

Como criar um plano de backup do SharePoint Online

A proteção do SharePoint é usada para fazer backup e restaurar sites e itens de lista do Microsoft SharePoint Online. O SharePoint Online é um dos produtos principais do Microsoft Office 365. Para proteger seu conteúdo do SharePoint, é necessário criar um plano.

Esta seção contém os seguintes tópicos:

Verificar os pré-requisitos

Revise os seguintes pré-requisitos antes de criar um plano de backup do SharePoint Online.

Criando um plano de backup do SharePoint Online:

Pré-requisitos:

A conta de backup é integrante dos grupos de administradores da coleção do site ou é atribuída à função de *Administrador do SharePoint*.

Para adicionar uma conta ao grupo Administradores da coleção de sites, consulte o link.

Criando um plano de backup do SharePoint Online usando BA (Basic Authentication - Autenticação básica):

Revise os seguintes pré-requisitos:

- Instale o PowerShell versão 5.1 ou superior (parte da WMF, Windows Management Framework - Estrutura de Gerenciamento do Windows) no servidor proxy (computador de 64 bits).
- Instale os seguintes módulos do PowerShell no servidor proxy usando a janela do PowerShell:
  - Para instalar o módulo do Azure, execute o seguinte comando:

    Install-Module -Name AzureAD -Force
  - Para instalar o módulo ExchangeOnlineManagement, execute o seguinte comando:

    Install-Module -Name ExchangeOnlineManagement -Force

  Observação: ao instalar módulos do PowerShell usando os comandos acima, uma versão mais recente dos módulos poderá ser instalada dependendo da versão do GA do componente disponível no repositório da Microsoft.

Criando um plano de backup do SharePoint Online usando MA (Modern Authentication - Autenticação moderna):

Revise os Pré-requisitos antes de criar um plano usando a autenticação moderna.

Criar um plano de backup do SharePoint Online

Um plano de backup inclui uma tarefa **Backup: Office 365 SharePoint Online** que executa um backup de itens do SharePoint Online (listas, bibliotecas, documentos e assim por diante) e armazena os dados em um repositório de dados com redução de redundância ou sem redução de redundância. Além disso, esse plano de backup permite que o UDP detecte e especifique itens do SharePoint Online para os quais uma tarefa de backup é executada. Cada tarefa consiste em parâmetros que definem a origem, o destino, a programação e outros detalhes de backup.

Siga estas etapas:

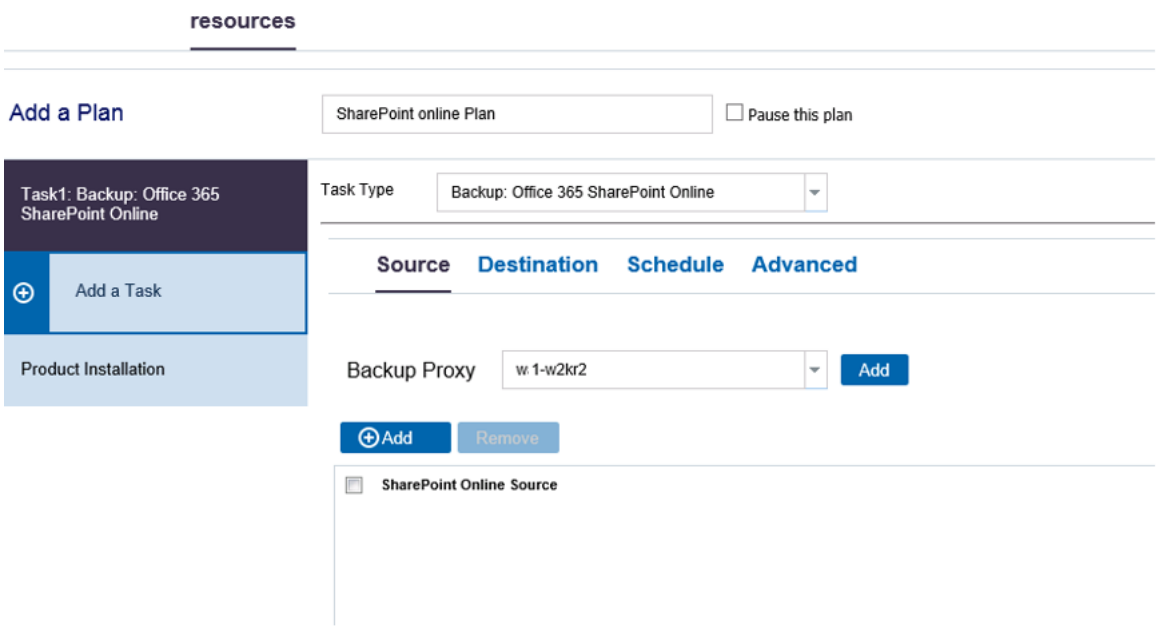
1. Clique na guia **Recursos** no Console.
2. No painel esquerdo, navegue para **Planos** e clique em **Todos os planos**.

   Se tiver criado os planos anteriores, esses planos serão exibidos no painel central.
3. No painel central, clique em **Adicionar um plano**.

   A caixa de diálogo Adicionar um plano abre.
4. Digite o nome do plano.
5. (Opcional) Selecione a caixa de seleção **Pausar este plano**.

   O plano não será executado até que você desmarque a caixa de seleção para retomar o plano.

   Observação: se um plano for pausado, nenhuma tarefa em andamento será pausada, mas todas as tarefas programadas correspondentes associadas a esse plano serão pausadas. No entanto, você pode executar uma tarefa manualmente. Por exemplo, você pode executar manualmente a tarefa de backup e a tarefa de replicação para um nó mesmo que o respectivo plano esteja pausado. Nesse caso, a tarefa seguinte da tarefa sob demanda (manual) não será executada. Por exemplo, há uma tarefa de replicação após uma tarefa de backup sob demanda, a tarefa de replicação não será executada para a tarefa de backup sob demanda. É necessário executar manualmente a tarefa de replicação. Quando você retomar o plano, as tarefas pendentes não são retomadas imediatamente. Depois de retomar o plano, as tarefas pendentes serão executadas no próximo horário programado.
6. Na lista suspensa Tipo de tarefa, selecione **Backup: Office 365 SharePoint Online**.



Agora especifique os detalhes de Origem, Destino, Programação e Avançado.

Especificar a origem

A página Origem permite especificar os nós de origem do SharePoint Online que você deseja proteger. É possível selecionar mais de um nó de origem do SharePoint Online em um plano.

Observação: é possível salvar um plano sem adicionar nós de origem, mas o plano só será implantado se você adicionar um nó.

Siga estas etapas:

1. Clique na guia **Origem**.
2. Selecione o **Proxy de Backup** na lista suspensa.
3. Adicione o nó do SharePoint Online usando um dos seguintes métodos:

   Método 1:

   a. Clique em **Adicionar** e em **Selecionar as origens a serem protegidas no Arcserve UDP**.

      A caixa de diálogo Adicionar nós ao plano é exibida.

      Observação: use essa opção somente se você já tiver adicionado o nó do SharePoint.

   b. Selecione um nó e clique em **Conectar**.

      Observação: para localizar os nós do SharePoint Online que você deseja proteger, use **Pesquisar**.

   Método 2:

   - Clique em **Adicionar** e, em seguida, clique em **Adicionar origem do SharePoint Online**.

     O diálogo Adicionar nós a um plano é exibido.

     Observação:

     - Use essa opção para detectar e especificar itens online para a origem do SharePoint Online.
     - Diferentemente de outros nós, não é possível adicionar o nó do SharePoint Online a partir da página Todos os nós. É possível adicionar um nó do SharePoint Online apenas durante a criação ou modificação de um plano.
4. Para aplicar a autenticação, siga um destes procedimentos:

Autenticação moderna

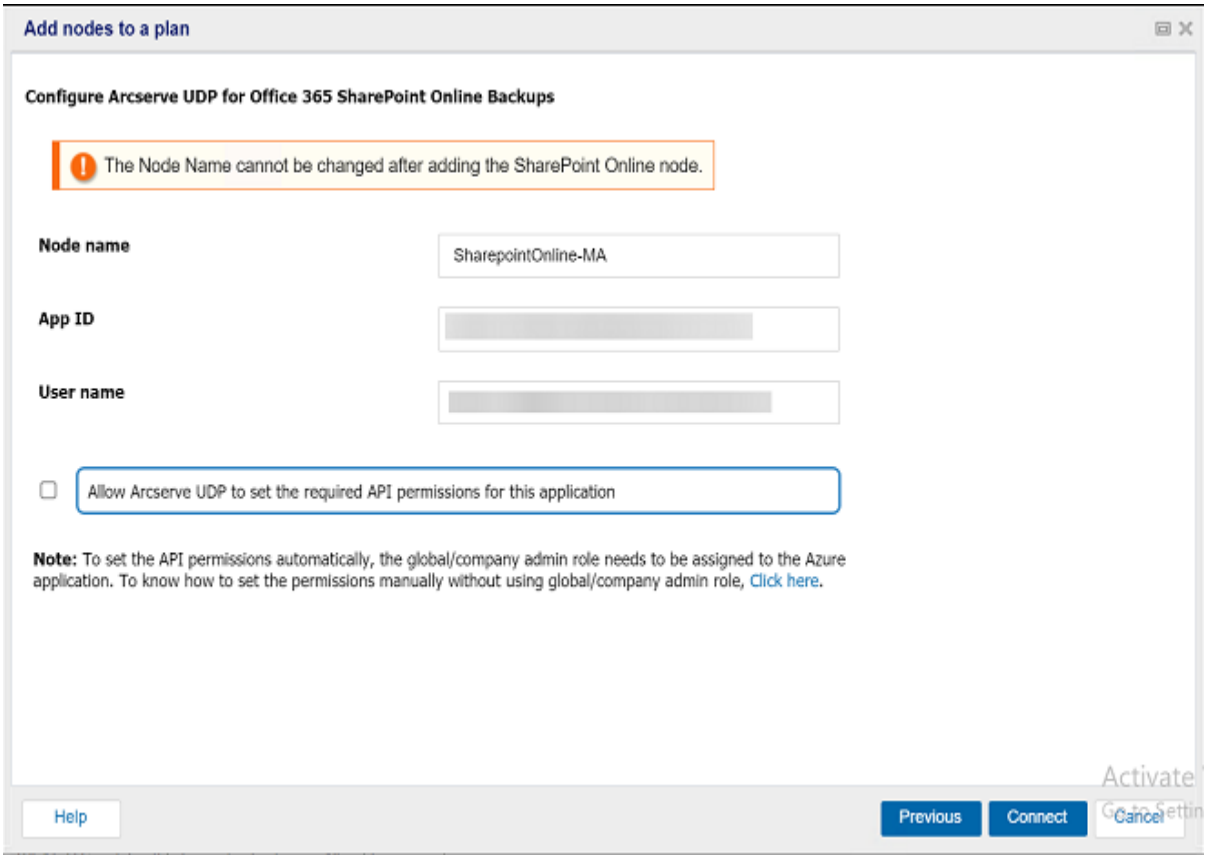
Para a autenticação moderna, você pode executar um backup usando o certificado de segurança.

Usar certificado de segurança

Observação: por padrão, o plano de backup seleciona **Usar certificado de segurança** para a autenticação moderna.

Siga estas etapas:

1. Para autenticar o aplicativo UDP com certificados de segurança, consulte Fazendo download do certificado do UDP e carregando-o no Azure.
2. Digite os seguintes detalhes:
   - Nome do nó
   - ID do aplicativo
   - Nome de usuário



c. Para aplicar as permissões de API automaticamente, marque a caixa de seleção **Permitir que o Arcserve UDP defina as permissões de API necessárias para este aplicativo**.

Observação: para aplicar as permissões manualmente sem usar a função de administrador global/de empresa, consulte Configurando as permissões da API manualmente sem usar a função de administrador global/de empresa.

d. Clique em **Conectar**.

Observações:

- Os nomes dos nós de origem do SharePoint Online não podem ser alterados após a criação do nó.
- Você pode usar uma única conta para proteger vários nós do SharePoint Online.
- Preencha a senha do aplicativo se a autenticação multifator estiver ativada e o locatário estiver definido para usar a autenticação básica.

Autenticação básica

Para a autenticação básica, para continuar com o backup, forneça as seguintes informações e clique em **Conectar**:

- Nome do nó
- URL da coleção de sites
- ID do usuário
- Senha

5. Para proteger os itens do SharePoint Online, faça o seguinte:
   - Na lista suspensa Tipo de site, selecione o tipo de site que deseja proteger, como sites do SharePoint ou sites pessoais.
   - Para Proteger todos os sites/subsites, faça o seguinte:

     Observações:

     - Esta opção é selecionada automaticamente por padrão quando a tela Selecionar conteúdo do SharePoint Online é exibida.
       - Para proteger todos os itens no tipo de site selecionado, marque a caixa de seleção **Proteger todos os sites/-subsites**.

- Para proteger itens específicos no tipo de site selecionado, desmarque a caixa de seleção **Proteger todos os sites/-subsites** e, em seguida, selecione os itens específicos que deseja proteger.

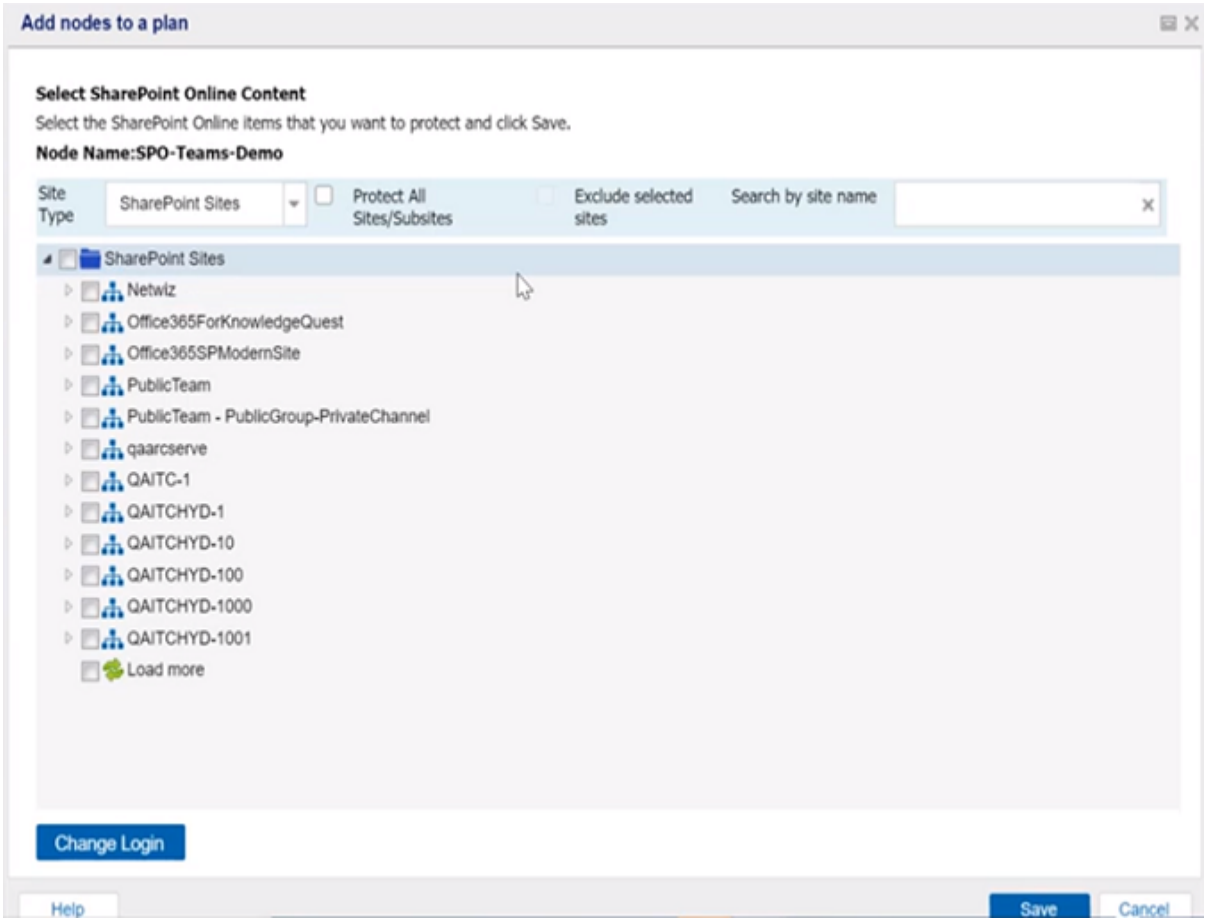
- Ao configurar o plano do SharePoint Online existente, se você selecionou sites manualmente para proteção e agora deseja marcar a caixa de seleção **Proteger todos os sites/subsites**, siga estas etapas:

  a. Modifique o plano do SharePoint Online existente.

  b. Limpe os sites do SharePoint selecionados manualmente para proteção.

  c. Marque a caixa de seleção **Proteger todos os sites/-subsites** e salve o plano.

- Para excluir itens específicos da proteção, marque a caixa de seleção **Excluir sites selecionados** e, em seguida, selecione itens específicos no tipo de site selecionado.



6. Clique em **Salvar**.

   As origens do SharePoint Online que você deseja proteger são adicionadas ao plano.

Especificar o destino

O destino é o local onde você armazena os dados de backup. É necessário, no mínimo, especificar o destino para salvar o plano.

Siga estas etapas:

1. Clique na guia **Destino**.

   O servidor de ponto de recuperação do Arcserve UDP especifica que o destino do backup é um servidor de ponto de recuperação.

   Não é possível armazenar dados como conjuntos de dados de recuperação.

2. Siga as seguintes etapas:

   a. Selecione um servidor de ponto de recuperação.

   b. Selecione um repositório de dados de redução de redundância ou de não redução de redundância.

      A lista exibe todos os repositórios de dados criados no servidor de ponto de recuperação especificado.

   c. Forneça uma senha da sessão.

      A senha da sessão é opcional quando o destino de backup é um repositório de dados do RPS não criptografado.

   d. Confirme a senha da sessão.

   O destino é especificado.

Especificar a programação

A página Programar permite definir uma programação para o backup e para que as funções Mesclar e Acelerar sejam repetidas em intervalos específicos. Após definir uma programação, as tarefas são executadas automaticamente de acordo com a programação. É possível adicionar várias programações e fornecer configurações de retenção.

Uma Programação de backup se refere a programação regular que é repetida várias vezes ao dia, com base no número de horas ou de minutos selecionado. Além da programação regular, uma programação de backup também fornece opções para adicionar programações diária, semanal e mensal.

Observação: para obter mais informações sobre as configurações de retenção e programação, consulte Entendendo a programação avançada e retenção.

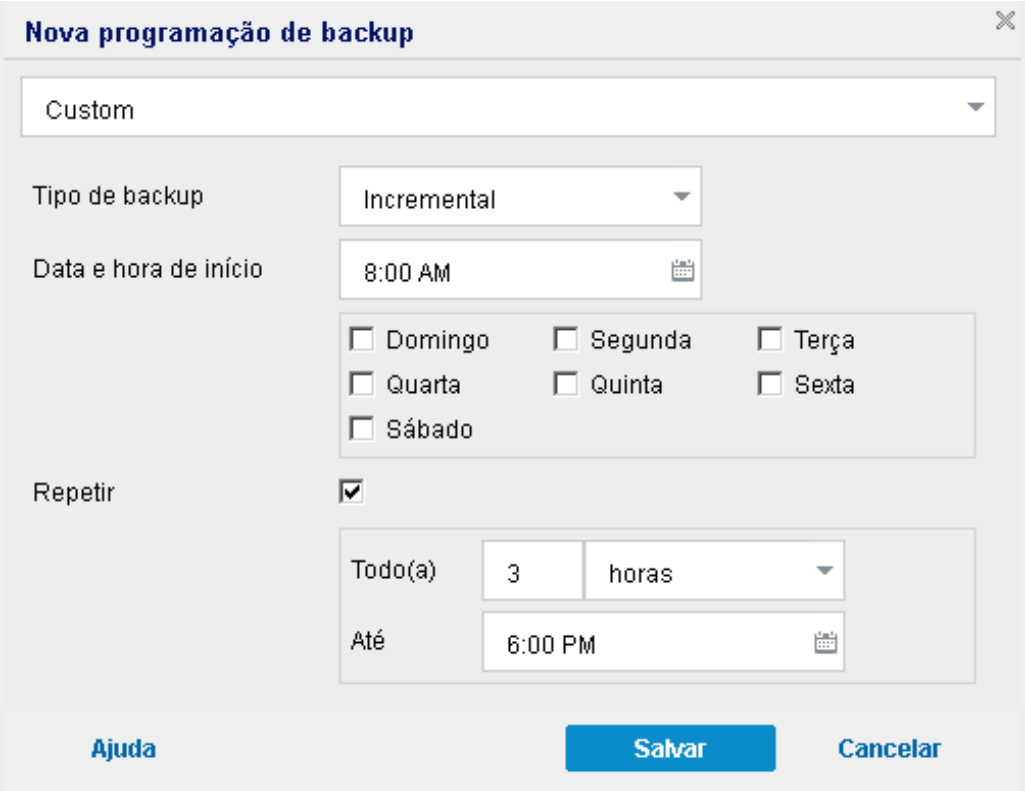
Siga estas etapas:

1. Adicionar programações de backup, mesclagem e acelerador.

   Adicionar programação de backup

   a. Clique em **Adicionar** e selecione **Adicionar programação de backups**.

      A caixa de diálogo **Nova programação de backup** é aberta.



   b. Selecione uma das seguintes opções:

Personalizado

Especifica a programação de backup que se repete várias vezes por dia.

Diário

Especifica a programação de backup que ocorre uma vez por dia. Por padrão, todos os dias da semana estão selecionados para o backup diário. Se não desejar executar a tarefa de backup em um dia específico, desmarque a caixa de seleção correspondente àquele dia da semana.

Semanal

Especifica a programação de backup que ocorre uma vez por semana.

Mensal

Especifica a programação de backup que ocorre uma vez por mês.

c. Selecione o tipo de backup.

Completo

Especifica a programação de backups para backups completos. Conforme programado, o Arcserve UDP executa um backup completo de todos os blocos usados do computador de origem. Um backup completo em geral, consome tempo, dependendo do tamanho do backup.

Incremental

Especifica a programação de backups para backups incrementais.

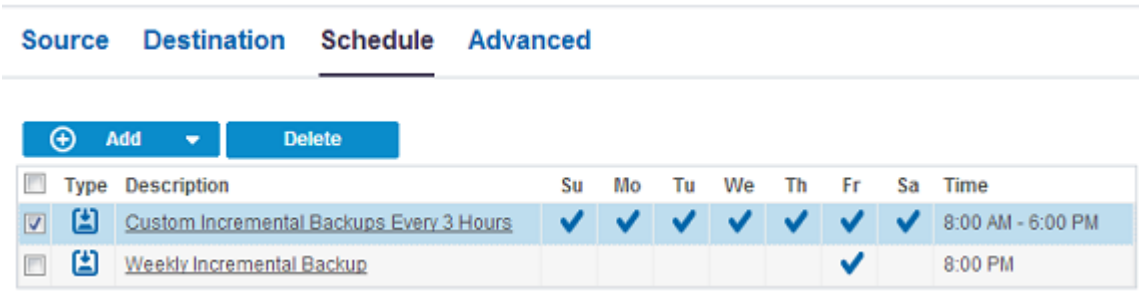
Conforme programado, o Arcserve UDP faz backup incremental apenas dos blocos que foram alterados após o último backup realizado com êxito. As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a executar um backup.

d. Especifique a hora de início do backup.

e. (Opcional) Marque a caixa de seleção de **Repetição** e especifique a programação a ser repetida.

f. Clique em **Salvar**.

A programação de backup é especificada e aparece na página **Programar**.



Adicionar Programação de mesclagem

a. Clique em **Adicionar** e selecione **Adicionar programação de mesclagem**.

   A caixa de diálogo **Adicionar nova programação de mesclagem** é aberta.

b. Especifique a hora de início da tarefa de mesclagem.

c. Especifique **Até** para fornecer uma hora de término para a tarefa de mesclagem.

d. Clique em **Salvar**.

A programação de mesclagem é especificada e aparece na página **Programar**.

Adicionar programação de acelerador

a. Clique em **Adicionar** e selecione **Adicionar programação de acelerador.**

   A caixa de diálogo **Adicionar nova programação do acelerador** é aberta.

b. Especifique o limite de taxa de transferência em unidades de MB por minuto.

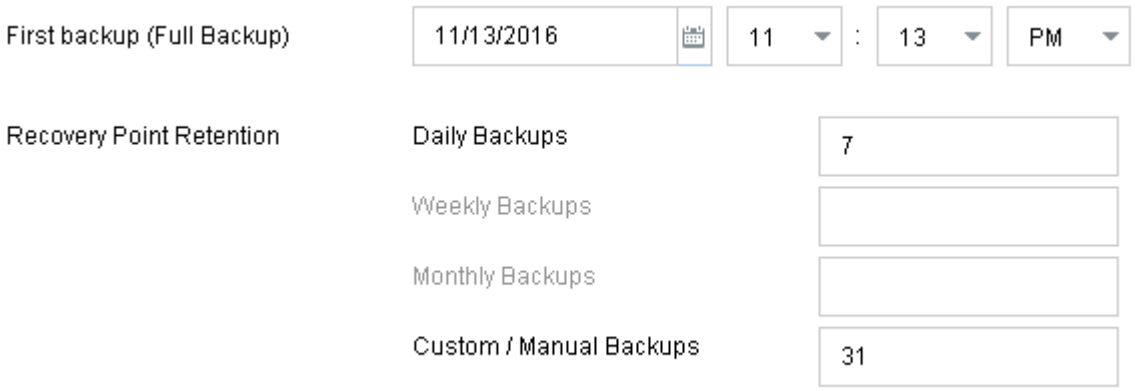
c. Especifique a hora de início da tarefa de taxa de transferência de backup.

d. Especifique **Até** para fornecer um horário de término para a tarefa de taxa de transferência.

e. Clique em **Salvar**.

A Programação de acelerador é especificada e exibida na página **Programar**.

2. Especifique a hora de início do backup programado.



3. Especifique as configurações de retenção de pontos de recuperação para programação diária, semanal e mensal.

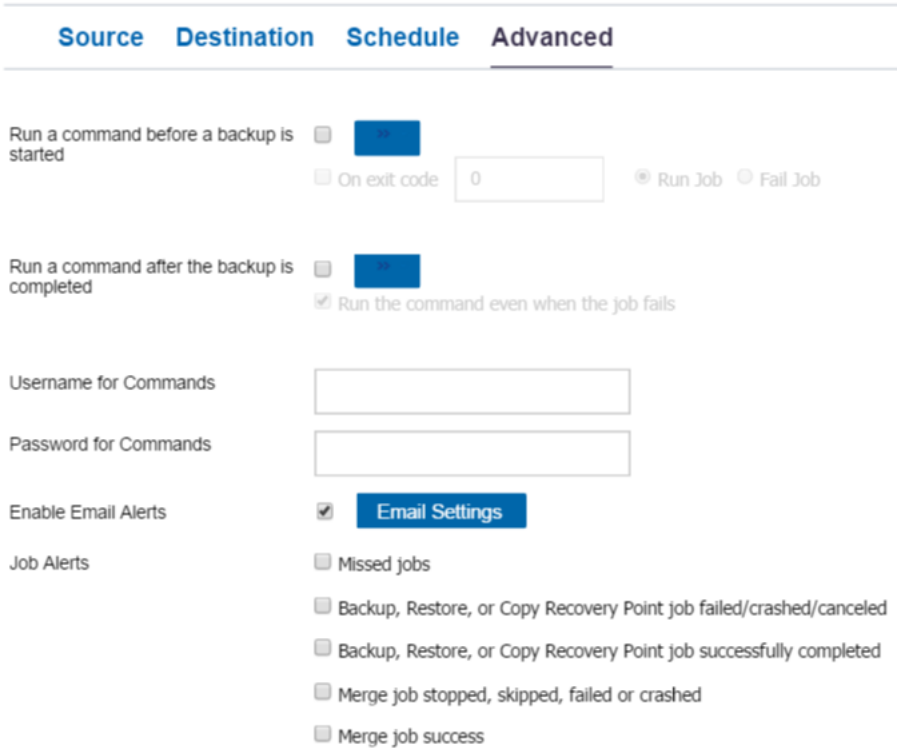
   As opções serão ativadas se tiver adicionado a programação de backup correspondente. Se você modificar as configurações de retenção desta página, as alterações serão refletidas na caixa de diálogo **Programação de backup**.

   A programação é especificada.

Especificar as configurações avançadas

A guia **Avançado** permite especificar algumas configurações avançadas para a tarefa de backup. As configurações avançadas incluem o fornecimento da localização dos scripts e as configurações de email.

A imagem a seguir mostra a guia **Avançado**:



Siga estas etapas:

1. Especifique os seguintes detalhes.

   Executar um comando antes do início do backup

   Permite a execução de um script antes de iniciar a tarefa de backup. Especifique o caminho em que o script está armazenado dentro do nó do proxy. Clique em **No código de saída** e especifique o código de saída para **Executar tarefa** ou **Tarefa com falha**. **Executar a tarefa** indica que a tarefa de backup continuará quando o script retornar o código de saída. **Tarefa com falha** indica que a tarefa de backup será interrompida quando o script retornar o código de saída.

   Executar um comando após a conclusão do backup

   Permite executar um script depois que a tarefa de backup foi concluída. Especifique o caminho completo onde o script está armazenado.

   Executar um comando, mesmo quando a tarefa falhar

Se essa caixa de seleção for selecionada, o script especificado em **Executar um comando após a conclusão do backup** é executado mesmo quando a tarefa de backup falha. Caso contrário, aquele script é executado somente quando a tarefa de backup é concluída com êxito.

Nome de usuário para comandos

Permite especificar o nome de usuário para executar os comandos.

Senha para comandos

Permite especificar a senha para executar os comandos.

Ativar alertas por email

Permite ativar alertas por email. É possível especificar configurações de email e os tipos de alertas que você deseja receber por email. Ao selecionar esta opção, as seguintes opções serão ativadas para a seleção.

Configurações de email

Permite configurar as definições de email. Clique em **Configurações de email** e configure o servidor de email e os detalhes do servidor proxy. Para obter mais informações sobre como definir as configurações de email, consulte Configuração de email e alerta.

Alertas de tarefa

Permite selecionar os tipos de emails de alerta de tarefas que deseja receber.

2. Clique em **Salvar**.

Observação: quando você seleciona um nó como origem de backup ou proxy de backup, o Arcserve UDP verifica se o agente está instalado no nó do proxy e se é a versão mais recente. Em seguida, o Arcserve UDP exibe uma caixa de diálogo de verificação que lista todos os nós que possuem uma versão antiga do agente ou que não tem o agente instalado. Para instalar/atualizar o agente nesses nós, selecione o método de instalação e clique em **Salvar**.

As alterações são salvas e uma marca de seleção verde aparece ao lado do nome da tarefa. A página do plano é fechada.

Observação: se precisar adicionar outra tarefa, deverá selecionar o plano na guia **Recursos** e modificar o plano. Para modificar o plano, clique no plano do painel central. O plano é exibido e será possível modificá-lo. É possível adicionar as tarefas **Copiar ponto de recuperação**, **Cópia em fita**, **Replicar** e **Replicar de um RPS remoto** como tarefas de acompanhamento.

O plano é automaticamente implantado ao nó do servidor proxy.

O plano de backup do SharePoint Online para o servidor proxy é criado. O backup é executado de acordo com a programação que você configurou na guia **Programar**. Também é possível fazer backup manual quando desejado.

(Opcional) Executar um backup manual

Normalmente, com base nas configurações de programação aplicadas, os backups são executados automaticamente. Além do backup programado, um backup manual fornece a opção de fazer backup dos nós de acordo com a necessidade. Por exemplo, se repetir a programação para backups completos e incrementais e desejar fazer grandes alterações em seu computador, você deverá executar um backup manual imediato sem esperar até que ocorra o próximo backup programado.

Para executar um backup manual dos nós do SharePoint Online, siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel esquerdo, navegue para **Nós** e clique em **Todos os nós**.

   Os nós do SharePoint Online são exibidos no painel central.
3. Selecione os nós do SharePoint Online (por exemplo, Caixa de correio@<nomedaorganização.com>) dos quais você deseja fazer backup e certifique-se de ter um plano atribuído a ele. O nome do nó é a conta usada durante a adição do nó do SharePoint Online e de sua conexão.
4. Clique com o botão direito do mouse no nó e selecione **Fazer backup agora**.

   A caixa de diálogo Fazer backup agora é exibida.
5. Selecione o tipo de backup que deseja executar e clique em **OK**.

   A caixa de diálogo Informações do andamento é exibida.
6. Aguarde até que a tarefa de backup seja concluída e clique em **OK**.
7. Para monitorar as tarefas de backup, navegue até **tarefas** > **Tarefas em andamento**.

   Aguarde até a conclusão da tarefa de backup.

   O backup manual é realizado com êxito.

Para executar um backup manual do plano do SharePoint Online, siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel esquerdo, navegue para **Planos** e clique em **Todos os planos**.

   Os planos de backup do SharePoint Online são exibidos no painel central.
3. Selecione o plano do qual você deseja fazer backup e certifique-se de que tenha um plano atribuído a ele.
4. Clique com o botão direito do mouse no plano e selecione **Fazer backup agora**.

A caixa de diálogo Fazer backup agora é exibida.

5. Selecione o tipo de backup que deseja executar e clique em **OK**.

   A caixa de diálogo Informações do andamento é exibida.

6. Aguarde até que a tarefa de backup seja concluída e clique em **OK**.

7. Para monitorar as tarefas de backup, navegue até **tarefas** > **Tarefas em andamento**.

   Aguarde até a conclusão da tarefa de backup.

   O backup manual é realizado com êxito.

Verificar o backup

Para verificar a tarefa de backup, confirme se você criou com êxito o plano de backup. Depois de verificar se o plano está criado com êxito, confirme se a tarefa de backup é executada conforme o programado. É possível verificar o status das tarefas de backup na guia **Tarefas**.

Siga estas etapas para verificar os planos:

1. Clique na guia **Recursos**.
2. No painel esquerdo, navegue para **Nós** e clique em **Todos os nós**.

   Uma lista de todos os nós é exibida no painel central.
3. Verifique se os planos são mapeados com nós.

Siga um destes métodos para verificar as tarefas de backup:

Método 1

1. Clique na guia **Tarefas**.
2. No painel à esquerda, clique em **Todas as tarefas concluídas**.

   O status de cada tarefa é incluído no painel central.
3. Verifique se a tarefa de backup é concluída com êxito.

   A tarefa de backup é verificada.

Método 2

1. Clique na guia **Tarefas**.
2. No painel esquerdo, clique em **Tarefas concluídas com êxito**.

   A lista de tarefas de backup concluídas é exibida no painel central.
3. Clique na tarefa que você deseja verificar.

   O painel direito é atualizado.
4. Em Detalhes da tarefa, clique no hiperlink **Exibir logs**.
5. Verifique se a tarefa de backup é concluída com êxito.

   A tarefa de backup é verificada.

Restaurar dados da coleção de sites do SharePoint Online

É possível restaurar lista/biblioteca ou item de lista do SharePoint Online no site. A coleção de sites e o site ainda não têm suporte no Arcserve UDP 8.0. Você pode restaurar os dados no site original com um novo nome, restaurar os dados no local original e exportar para o disco a partir dos pontos de recuperação.

Execute as seguintes tarefas para restaurar item de lista do SharePoint Online:

1. Selecionar itens de lista do site do SharePoint Online para restauração
2. Definir as opções de restauração
3. Verificar se o conteúdo foi restaurado

Selecionar itens de lista do site do SharePoint Online para restauração

É possível restaurar dados de itens de lista do SharePoint Online a partir de um ponto de recuperação. Ao selecionar uma data de recuperação e, em seguida, especificar a hora, todos os pontos de recuperação associados a esse período são exibidos. Você pode procurar e selecionar o conteúdo do backup (incluindo aplicativos) a ser restaurado.

Siga estas etapas:

1. Efetue logon no Arcserve UDP.
2. Clique na guia **Recursos**.
3. Selecione **Todos os nós** no painel esquerdo.

   Todos os nós do adicionados são exibidos no painel central.

   Ou

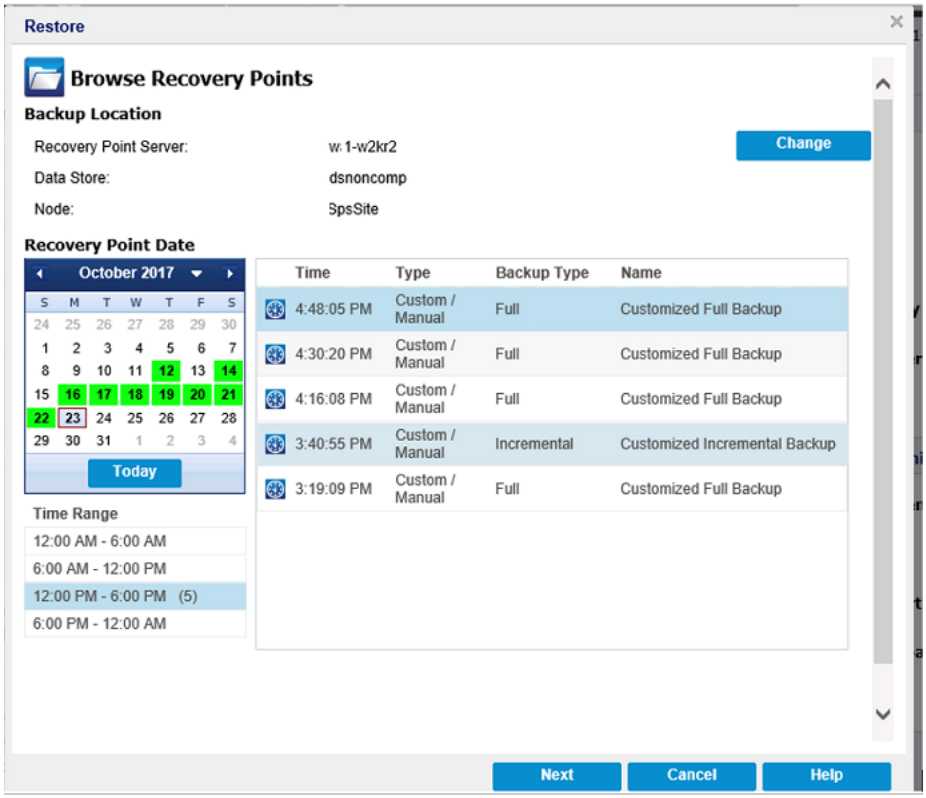
   Selecione o grupo **Nós do SharePoint Online**.

   Todos os nós do SharePoint adicionados são exibidos no painel central.
4. No painel central, selecione o nó do SharePoint Online e clique em **Ações**.
5. Clique em **Restaurar** no menu suspenso Ações.

   A caixa de diálogo Restaurar item do SharePoint é exibida.

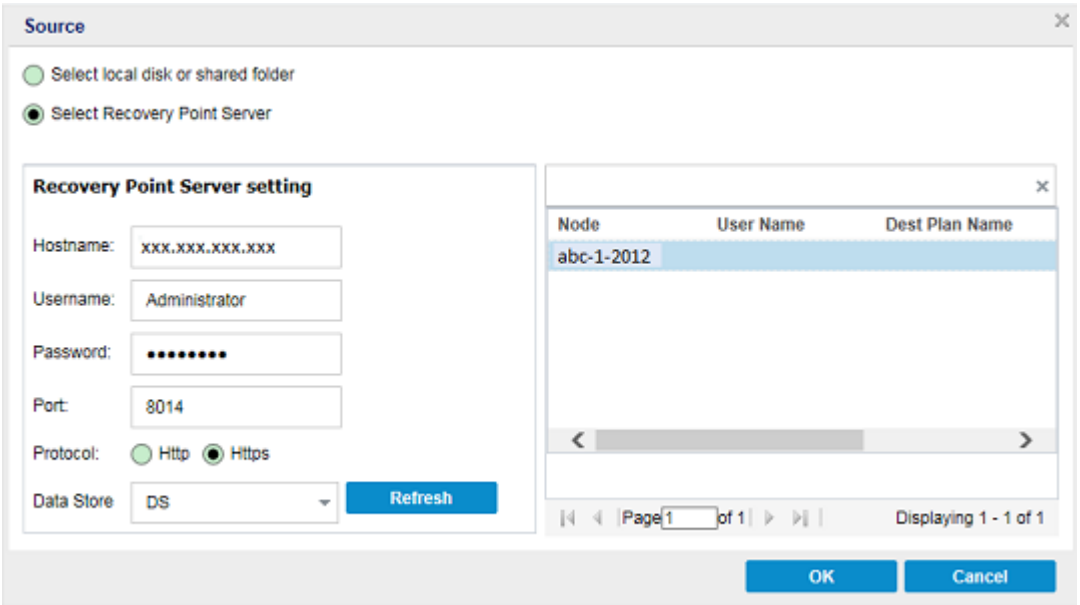
   Observação: você é automaticamente conectado ao nó do agente, e a caixa de diálogo Restaurar item do SharePoint é aberta.

   O Local do backup exibe os detalhes do Servidor de ponto de recuperação.



6. (Opcional) Clique em **Alterar** para modificar o local do backup.

   A caixa de diálogo Origem é exibida. É possível selecionar o local do backup na caixa de diálogo.



Observação: quando você adiciona uma tarefa de cópia em fita ao plano e deseja restaurar o ponto de recuperação de backup da cópia em fita, selecione o ponto de

recuperação no backup da cópia em fita. Para obter mais informações, consulte Procurar ponto de recuperação de cópia em fita para restauração.

7. Para especificar a origem, selecione uma das opções a seguir e clique em **OK**:

   Selecionar o disco local ou uma pasta compartilhada

   Observação: no Arcserve UDP, não recomendamos que você marque a opção **Selecionar o disco local ou a pasta compartilhada**.

   Selecionar servidor de ponto de recuperação

   a. Especifique os detalhes da configuração do servidor de ponto de recuperação e clique em **Atualizar**.

      Todos os agentes estão listados na coluna Agente de proteção de dados na caixa de diálogo Origem.

   b. Selecione o agente na lista/biblioteca exibida e clique em **OK**.

      Os pontos de recuperação são listados na caixa de diálogo Restaurar item do SharePoint.

8. Selecione a data do calendário para a imagem de backup a ser restaurada e clique em **Avançar**.

   Todas as datas que contém pontos de recuperação para a origem do backup especificado são realçadas em verde.

   Os pontos de recuperação correspondentes a essa data são exibidos, juntamente com a hora do backup, o tipo de backup que foi executado (completo ou incremental) e o nome do backup.

9. Na caixa de diálogo Restaurar itens do SharePoint Online, expanda a coleção de sites.

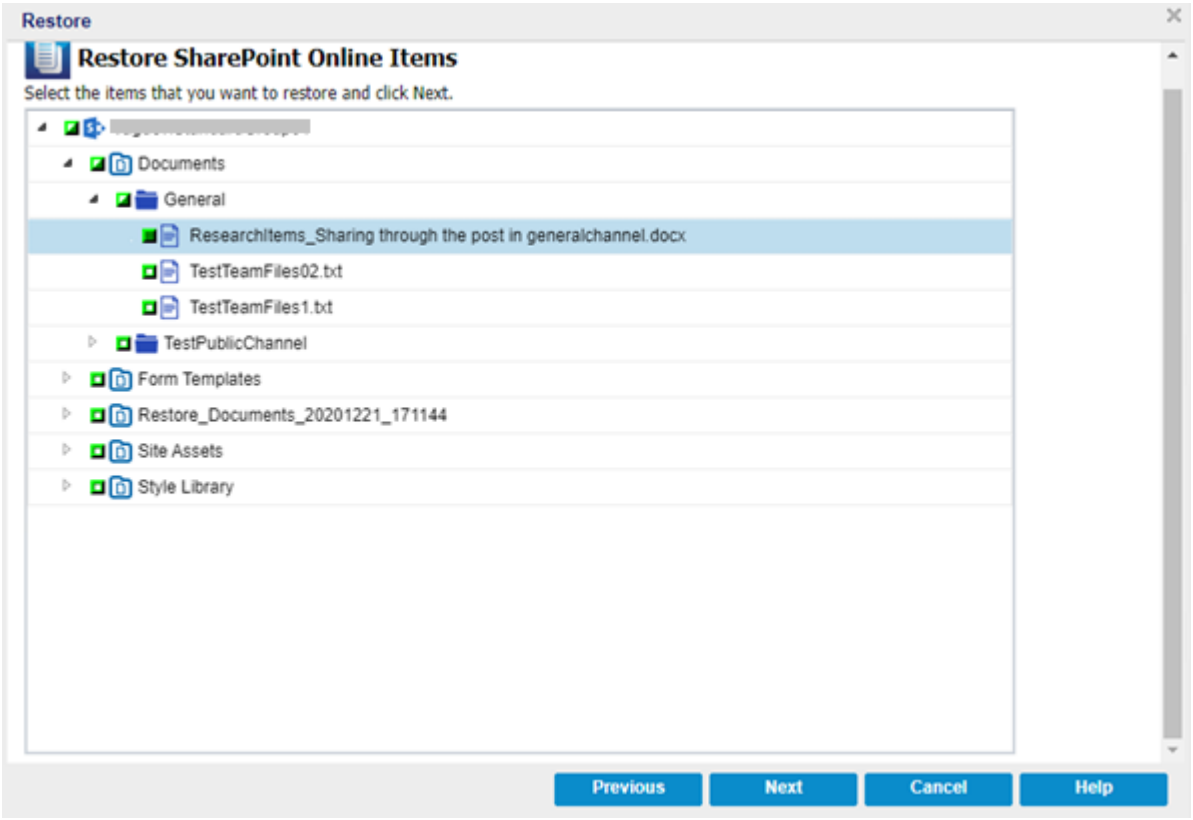
   Todas as listas/bibliotecas e os itens de lista são exibidos.

10. Selecione o site ou o canal específico na coleção de sites que você deseja restaurar da coleção de sites do SharePoint e clique em **Avançar**.

    Observações:

    - É possível selecionar parte ou todo o conteúdo do objeto do SharePoint a ser restaurado. Para selecionar o conteúdo parcial, expanda o objeto e clique na caixa de seleção do conteúdo.
    - É possível selecionar várias listas/bibliotecas ou itens de lista do SharePoint para restaurar.

    A caixa de diálogo Opções de restauração é exibida.



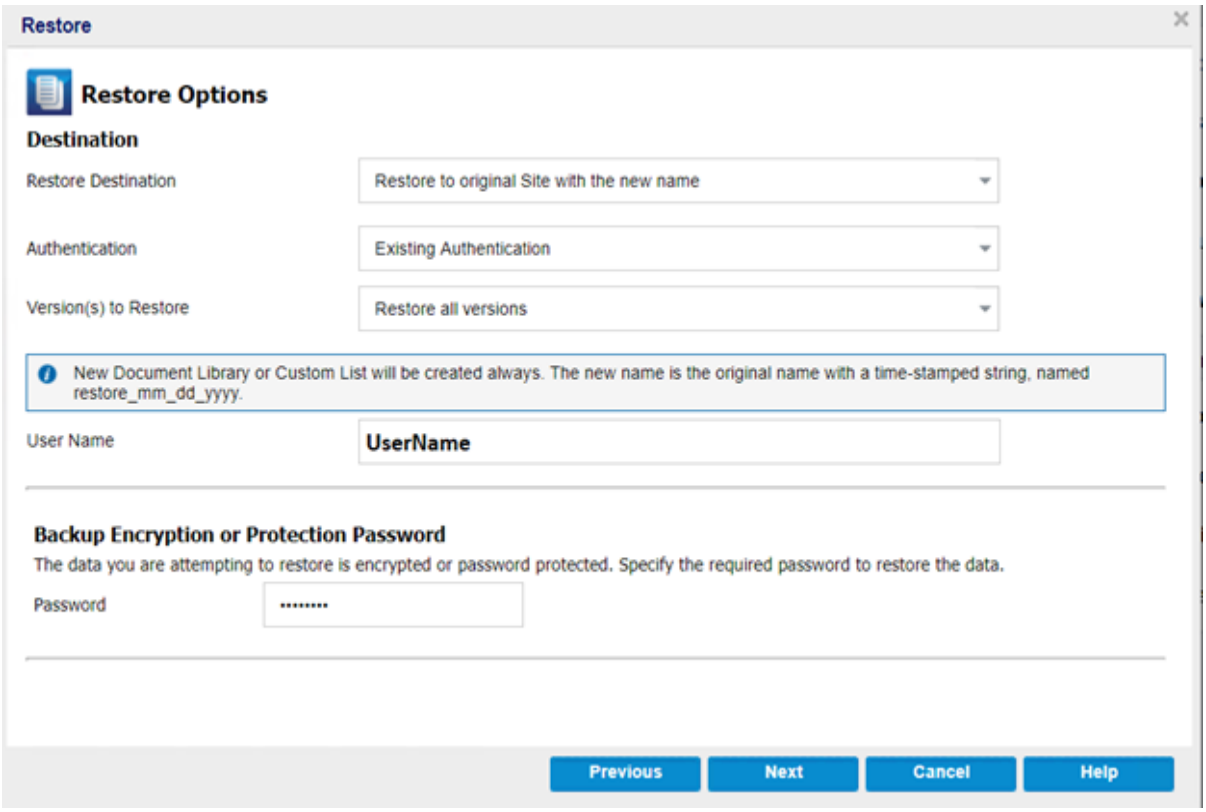
As listas/bibliotecas ou os itens de lista do SharePoint Online a serem restaurados são selecionados. Agora, você pode definir as opções de restauração.

Definir as opções de restauração

Depois de especificar as informações do SharePoint Online a serem restauradas, defina as opções de restauração do conteúdo selecionado.

Siga estas etapas:

1. Na caixa de diálogo Opções de restauração, selecione o destino da restauração.



As opções de destino disponíveis são:

Restaurar no site original com o novo nome

Restaura os dados da lista/biblioteca e dos itens de lista no mesmo site de onde você pegou um backup com um novo nome de lista.

Restaurar para o local original

Restaura os dados da lista/biblioteca e dos itens de lista no mesmo local de onde você pegou um backup.

2. Especifique uma das opções a seguir na lista suspensa Se o item já existir no destino:

Acrescentar como versão nova se o controle de versão estiver ativado

Essa opção funciona quando sua configuração de versão está ativada na configuração da biblioteca no site do SharePoint. Depois que você selecionar essa opção, a nova versão será acrescentada às versões atuais dos itens de lista se os itens de lista forem existentes.

Ignorar o item e não restaurar

Ignora os itens e não restaura.

Substituir o item no destino

Substitui o item no destino.

Exportar para o disco

Restaura as listas/bibliotecas ou os itens de lista da coleção de sites em uma pasta ou em uma pasta compartilhada no disco.

Observação: na restauração de listas quando a opção de restauração Exportar para o disco é selecionada, exporte somente o(s) anexo(s) da lista para o disco.

Autenticação

Valida e identifica a conta de usuário. Selecione uma das seguintes opções:

- **Autenticação existente**

  Quando você seleciona Autenticação existente, o tipo de autenticação que foi selecionado durante a criação do nó é usado.

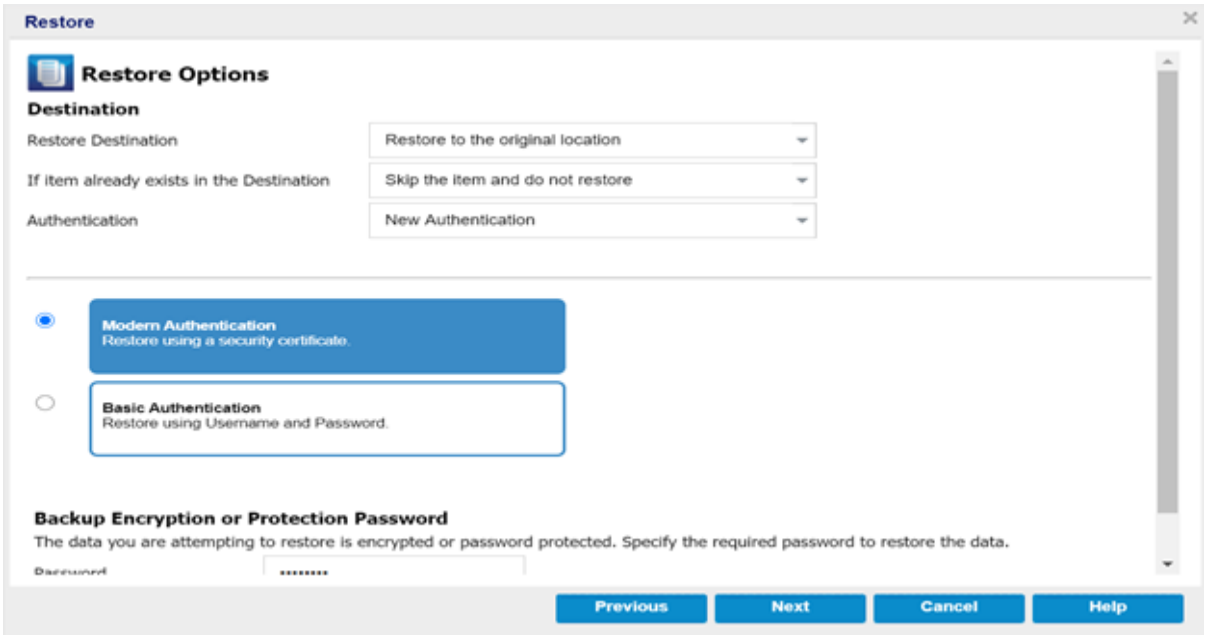
  - Se a autenticação do nó for básica, parâmetros como Nome de usuário, Senha e Criptografia de backup ou proteção por senha [se criptografada], serão carregados automaticamente para prosseguir com a restauração.
  - Se a autenticação do nó for moderna, parâmetros como Nome de usuário e Criptografia de backup ou proteção por senha [se criptografada], serão carregados automaticamente para prosseguir com a restauração.

- **Nova autenticação**

  Durante a restauração, é possível selecionar uma das seguintes opções para alterar o tipo de autenticação:

  - Autenticação moderna

- Autenticação básica



3. Para aplicar a autenticação, siga um destes procedimentos:

Autenticação moderna

Para a autenticação moderna, é possível executar uma restauração usando o certificado de segurança.

Usar certificado de segurança

Observação: por padrão, o plano de backup seleciona **Usar certificado de segurança** para a autenticação moderna.

Siga estas etapas:

a. Para autenticar usando um certificado autoassinado, consulte Fazendo download do certificado do UDP e carregando-o no Azure.

b. Digite a ID do aplicativo e o nome do usuário.

c. Para aplicar as funções e permissões necessárias, marque a caixa de seleção **Permitir que o Arcserve UDP defina as funções e permissões necessárias do Azure para este aplicativo** e clique em **Avançar**.

Autenticação básica

Na autenticação básica, para continuar com a restauração, digite o nome de usuário e a senha.

Observação: essa opção falhará se a autenticação moderna estiver ativada no locatário ou na conta.

4. Especifique as versões do item de lista que você quer restaurar quando sua configuração de versão estiver ativada na configuração da biblioteca no site do SharePoint.

   Restaurar todas as versões

   Restaura todas as versões do backup.

   Restaurar somente a versão mais recente

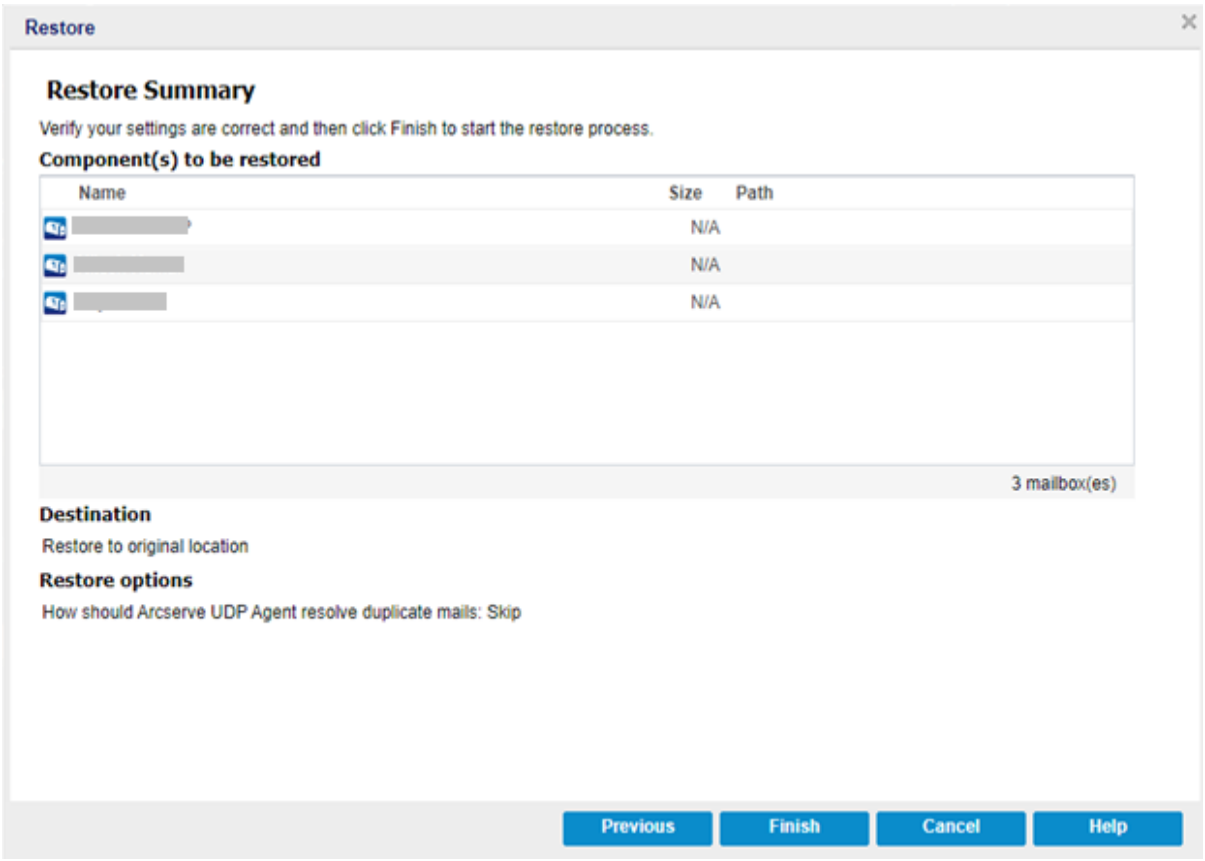
   Restaura somente a versão mais recente no backup.

   Restaurar somente a versão principal mais recente

   Restaura somente a versão principal mais recente no backup.

5. Especifique a senha da sessão, se houver.
6. Clique em **Avançar**.

   A caixa de diálogo Resumo da restauração é exibida.



   É possível verificar as informações da restauração na caixa de diálogo Resumo da restauração.

7. Clique em **Concluir** para enviar a tarefa de restauração.

As opções de restauração são definidas para restaurar as informações do SharePoint Online.

Verificar se o conteúdo foi restaurado

Após a conclusão do processo de restauração, verifique se o conteúdo foi restaurado no destino especificado.

Siga estas etapas:

1. Efetue logon na coleção de sites do SharePoint.
2. Verifique a lista/biblioteca e os itens de lista.
3. Verifique o conteúdo restaurado.

   A restauração do conteúdo é verificada com êxito.

Mapa de proteção de dados do Microsoft Teams

Importante:Os dados do Teams de uma organização inteira são protegidos automaticamente quando as tarefas do Exchange, do SharePoint e do OneDrive estão definidas para usar a opção *proteger todos* em contas e sites.

A tabela a seguir descreve o Mapa de proteção de dados do Microsoft Teams:

Item do Teams	Itens que devem ter backup no UDP	De onde restaurar
Registros de reuniões programadas	Conta do OneDrive do usuário que faz os registros	Interface do usuário do agente para conta do usuário do OneDrive
1-1 Bate-papos privados/postagens/conversas	Caixa de correio do usuário do Exchange	Interface do usuário do agente para usuário do Exchange
Arquivos enviados pelo bate-papo 1-1	Caixa de correio do Exchange/conta do usuário do OneDrive	Interface do usuário do agente para usuário do Exchange e conta do usuário do OneDrive
Itens no canal padrão do Teams		
Bate-papos/postagens/conversas	Caixa de correio de grupo do canal padrão	Interface do usuário do agente para caixa de correio do grupo
Calendário do Teams para o canal	Caixa de correio de grupo do canal padrão	Interface do usuário do agente para caixa de correio do grupo
Arquivos enviados em bate-papos	Selecionar o site do SharePoint do canal/*Proteger todos* os sites ou	Interface do usuário do agente para Sha-

	caixa de correio de grupo do canal	rePoint> Site para canal padrão> Biblioteca de documentos OU Interface do usuário do agente para Exchange> Caixa de correio do grupo
Arquivos/pastas carregados usando a guia Arquivos	Selecionar o site do SharePoint do canal/*Proteger todos* os sites.	Interface do usuário do agente para SharePoint> Site para canal padrão> Biblioteca de documentos
Itens no canal privado do Teams		
Bate-papos/postagens/conversas	Caixa de correio do usuário do Exchange	Interface do usuário do agente para caixa de correio do usuário
Arquivos enviados em bate-papos	Selecionar o site do SharePoint do canal/*Proteger todos* os sites ou caixa de correio do usuário	Interface do usuário do agente para SharePoint> Site para canal padrão > Biblioteca de documentos OU Interface do usuário do agente para Exchange > Caixa de correio do usuário
Arquivos/pastas carregados usando a guia Arquivos	Selecionar o site do SharePoint do canal/*Proteger todos* os sites.	Interface do usuário do agente para SharePoint> Site para canal padrão> Biblioteca de documentos

Como criar e configurar máquinas virtuais instantâneas simultâneas em vários hipervisores

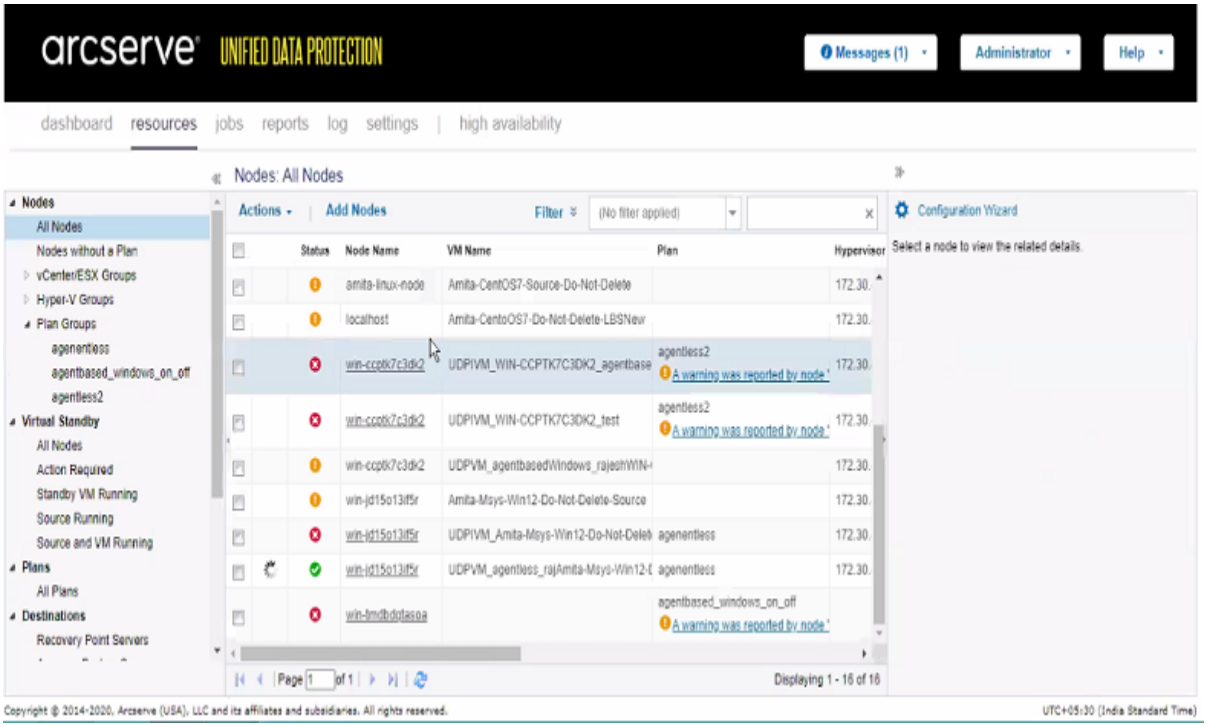
Esta seção fornece informações sobre como criar e configurar VMs instantâneas simultâneas em vários hipervisores, como Hyper-V, VMware, Nutanix AHV, Amazon EC2 e Microsoft Azure.

É possível criar VMs instantâneas simultâneas no console do Arcserve UDP usando o assistente de criação de uma VM instantânea.

Para abrir o assistente de criação de uma VM instantânea, siga estas etapas:

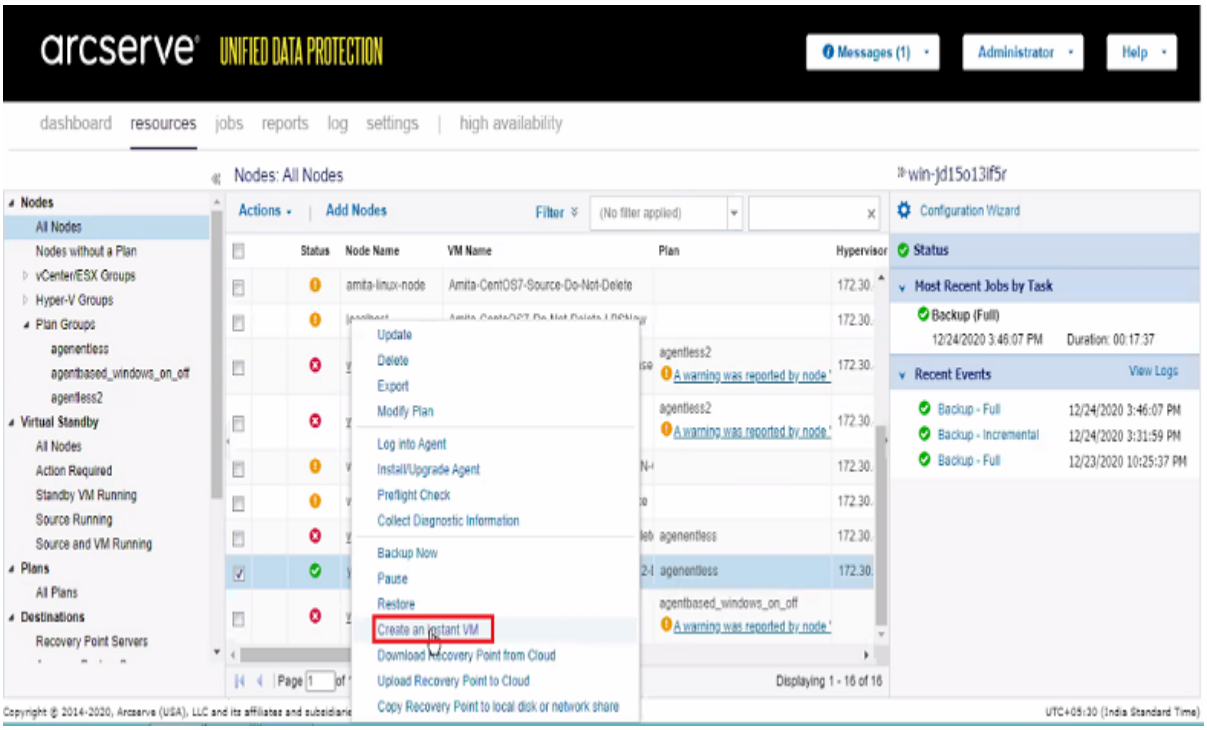
1. Efetue logon na conta do console do UDP.
2. Na página Console do UDP, clique na guia **recursos**.
3. No painel esquerdo, navegue para **Nós** > **Todos os nós**.

   A lista de nós existentes é exibida no painel central.



4. Selecione um ou mais nós que já estejam associados a um plano.

   Observação: se um nó não estiver associado a nenhum plano, a opção Criar uma VM instantânea não será exibida.



5. Clique com o botão direito do mouse nos nós selecionados e, em seguida, selecione a opção **Criar uma VM instantânea**.

O assistente de criação de uma VM instantânea é exibido. No assistente, você pode configurar VMs instantâneas simultâneas.

Para configurar as VMs instantâneas simultâneas, siga estas etapas:

1. Selecionar um servidor de ponto de recuperação de origem
2. Selecionar o local das VMs
3. Selecionar os servidores de recuperação
4. Definir as configurações das máquinas virtuais
5. Verificar o resumo

Selecionar um servidor de ponto de recuperação de origem

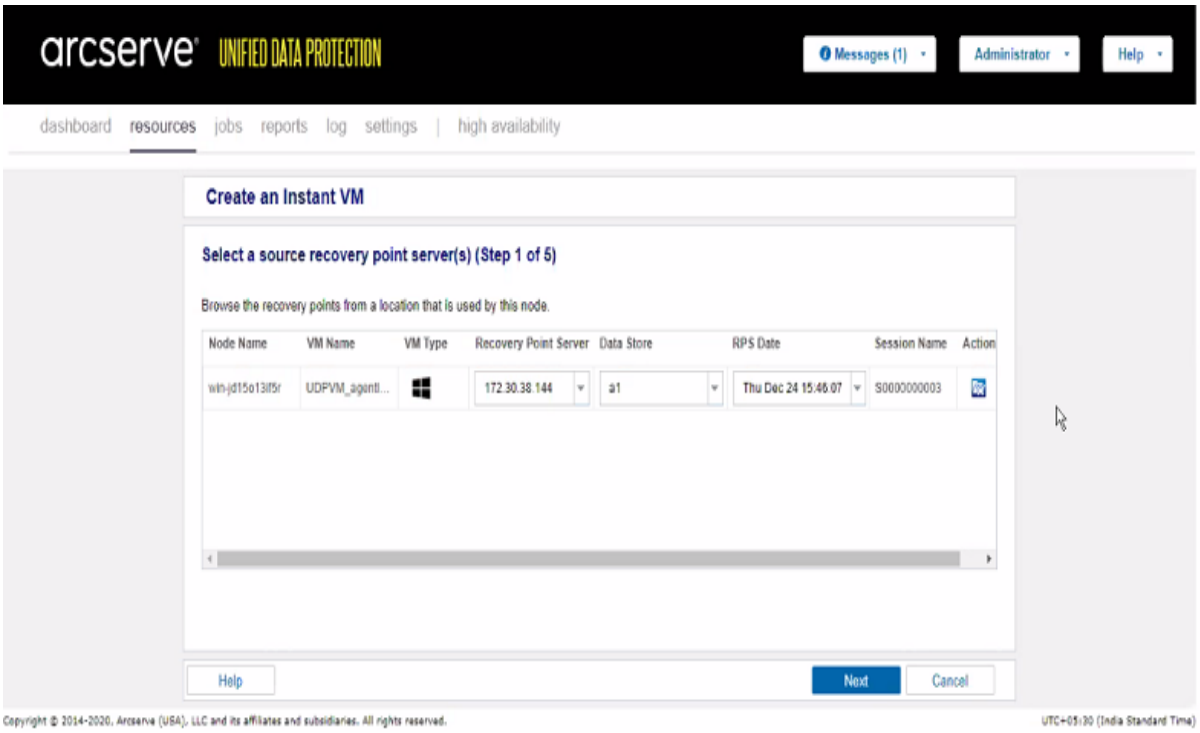
Esta seção fornece informações sobre como executar a primeira etapa de seleção de um ponto de recuperação de origem.

A tela Selecionar servidores de ponto de recuperação de origem exibe a lista de nós selecionados com detalhes como nome do nó, nome da VM, tipo de VM, servidor de ponto de recuperação, repositório de dados, data do RPS, nome da sessão e ação. Para cada nó na lista, o console seleciona automaticamente o servidor de

ponto de recuperação, o repositório de dados e os detalhes de data do RPS. Também é possível alterar esses detalhes se houver vários servidores de ponto de recuperação disponíveis em cada nó.

Siga estas etapas:

1. Na tela Selecionar servidores de ponto de recuperação de origem, em cada nó, faça o seguinte:



   - Para Servidor de ponto de recuperação, na lista suspensa, selecione o servidor de ponto de recuperação necessário.
   - Para Repositório de dados, na lista suspensa, selecione o repositório de dados necessário.
   - Para Data do RPS, na lista suspensa, selecione a data do RPS necessária.

2. Clique em **Avançar**.
3. (Opcional) Se a sessão de backup estiver criptografada para qualquer um dos nós selecionados, digite a senha.

   A tela Local das VMs é exibida.

Conclua a próxima etapa: Selecionar o local das VMs

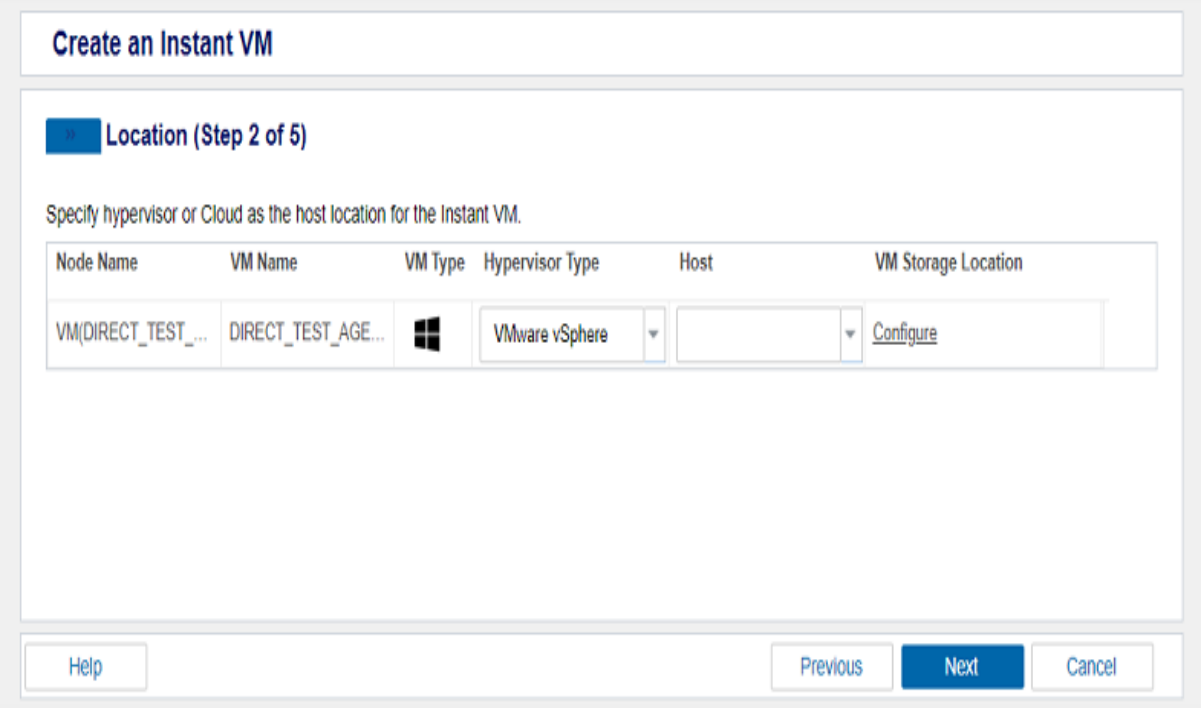
Selecionar o local das VMs

Esta seção fornece informações sobre como executar a segunda etapa de seleção de um local da máquina virtual para hospedar a VM instantânea.

A tela Local das VMs exibe a lista de nós selecionados com detalhes como nome da VM, tipo de VM, tipo de hipervisor e host. Para cada nó na lista, é possível selecionar o tipo de hipervisor e o local da máquina virtual para hospedar a VM instantânea.

Siga estas etapas:

1. Na tela Local das VMs, em cada nó, faça o seguinte:



Nó do Windows

- Para Tipo de hipervisor, na lista suspensa, selecione o tipo de hipervisor.

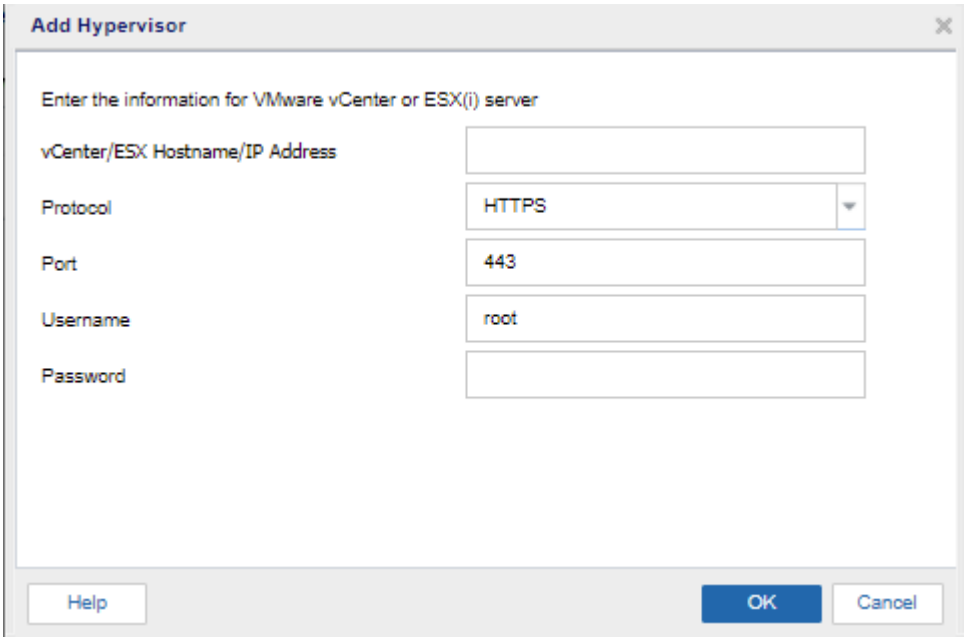
  Observação: o Arcserve UDP oferece suporte ao VMware e ao Hyper-V para hospedar os nós da VM instantânea para Windows.

- Para Host, na lista suspensa, selecione o hipervisor existente ou adicione um novo hipervisor.

  Para adicionar um novo hipervisor, siga estas etapas:

a. Na lista suspensa de Host, clique em **+Adicionar novo hipervisor**.

   A caixa de diálogo Adicionar hipervisor é exibida.



b. Na caixa de diálogo Adicionar hipervisor, forneça os seguintes detalhes, conforme necessário:

   - **Nome do host/endereço IP do vCenter/ESX:** digite o nome do host ou o endereço IP do vCenter.
   - **Protocolo:** selecione o protocolo como HTTP ou HTTPS.
   - **Porta:** digite o número da porta.
   - **Nome de usuário:** digite o nome de usuário.
   - **Senha:** digite a senha.

c. Clique em **OK**.

   O novo hipervisor é adicionado.

- Para Local de armazenamento da VM, para configurar a seleção do local de armazenamento de VMware, clique em **Configurado**.

Nó Linux

- Para Tipo de hipervisor, na lista suspensa, selecione o tipo de hipervisor.

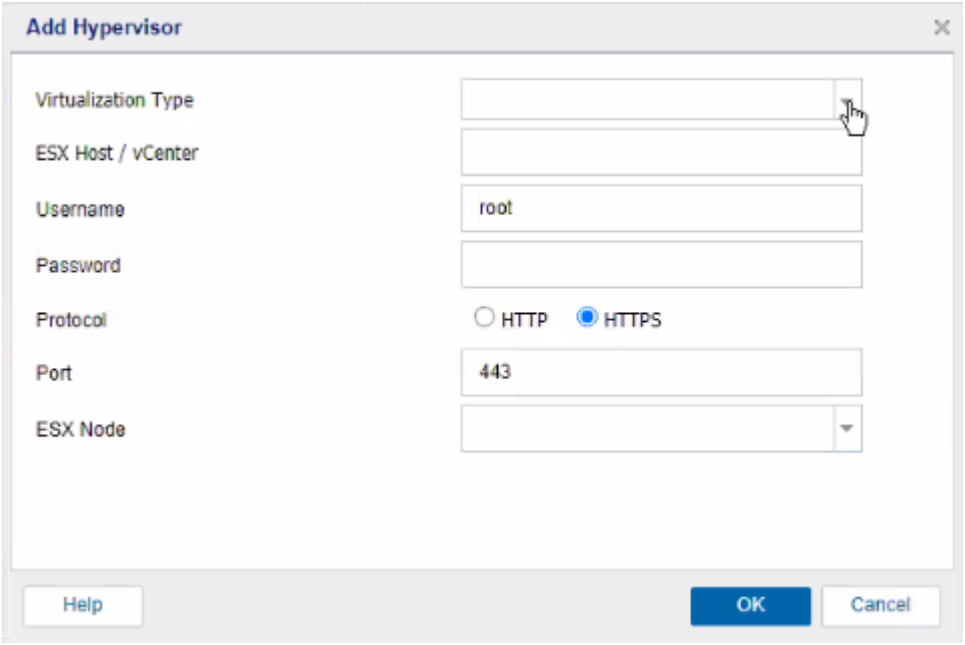
Observação: o Arcserve UDP oferece suporte a VMware, Hyper-V, Nutanix AHV, Amazon EC2 e Microsoft Azure para hospedar os nós da VM instantânea para Linux.

- Para Host, na lista suspensa, selecione o hipervisor existente ou adicione um novo hipervisor.

  Para adicionar um novo hipervisor, siga estas etapas:

  a. Na lista suspensa de Host, clique em **+Adicionar novo hipervisor**.

  A caixa de diálogo Adicionar hipervisor é exibida.



  b. Na caixa de diálogo Adicionar hipervisor, na lista suspensa Tipo de virtualização, selecione uma das seguintes opções:

  VMware

  Forneça os seguintes detalhes, conforme necessário:

  - **Host do ESX/vCenter:** digite o nome do host ou o endereço IP do vCenter.
  - **Nome de usuário:** digite o nome de usuário.
  - **Senha:** digite a senha.
  - **Protocolo:** selecione o protocolo como HTTP ou HTTPS.
  - **Porta:** digite o número da porta.

- **Nó ESX:** na lista suspensa, selecione um dos nós disponíveis.

Hyper-V

Forneça os seguintes detalhes, conforme necessário:

- **Nome do host do Hyper-V:** digite o nome do host para o hipervisor Hyper-V.
- **Nome de usuário:** digite o nome de usuário.
- **Senha:** digite a senha.

Nutanix AHV

Forneça os seguintes detalhes, conforme necessário:

- **Endereço IP virtual do agrupamento Nutanix AHV:** digite o endereço IP.
- **Nome de usuário:** digite o nome de usuário.
- **Senha:** digite a senha.
- **Porta:** digite o número da porta.

EC2

Forneça os seguintes detalhes, conforme necessário:

- **Nome da conta:** digite o nome da conta da nuvem. Se a conta da nuvem não for adicionada, clique em Adicionar. Para obter mais informações, consulte Adicionar uma conta da nuvem.
- **Região:** na lista suspensa, selecione a região disponível.

Azure

Forneça os seguintes detalhes, conforme necessário:

- **Nome da conta:** digite o nome da conta da nuvem. Se a conta da nuvem não for adicionada, clique em Adicionar. Para obter mais informações, consulte Adicionar uma conta da nuvem.
- **Grupo de recursos:** na lista suspensa, selecione o grupo de recursos disponível.

- **Região:** na lista suspensa, selecione a região disponível.

c. Clique em **OK**.

O novo hipervisor é adicionado.

- Para Local de armazenamento da VM, para configurar a seleção do local de armazenamento de VMware, clique em **Configurado**.

2. Clique em **Avançar**.

A tela dos servidores de recuperação é exibida.

Conclua a próxima etapa: Selecionar servidores de recuperação

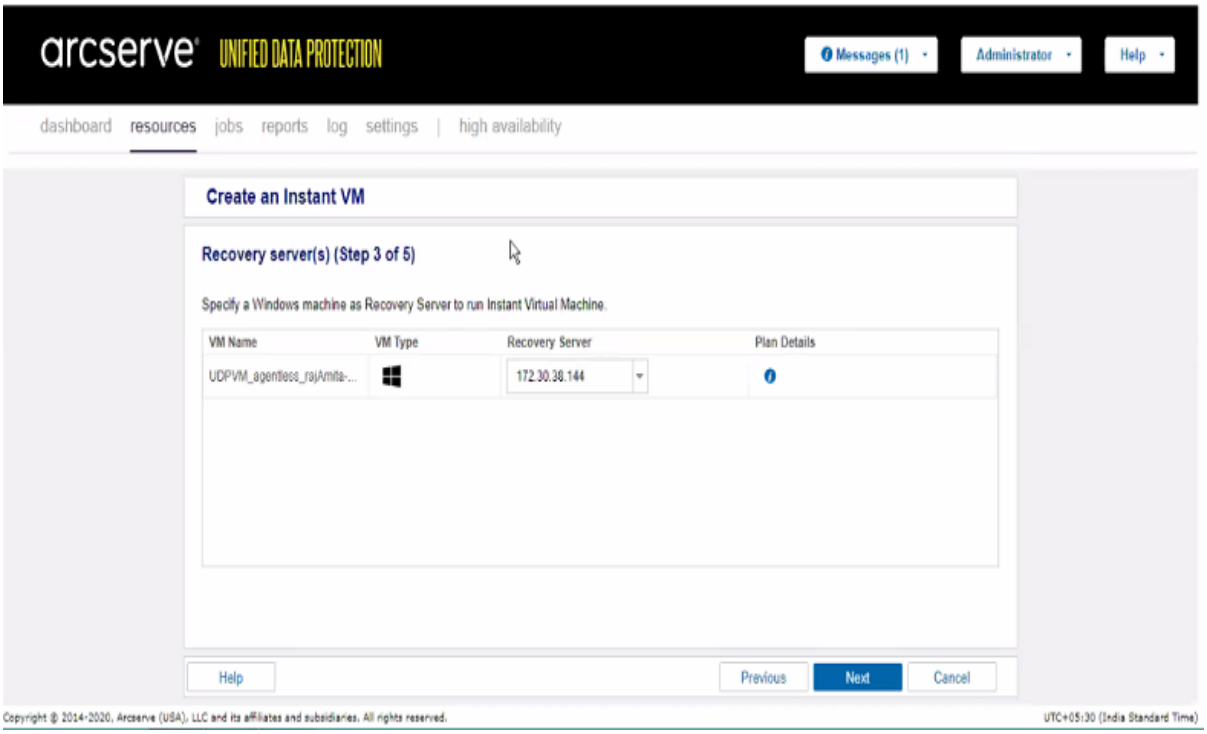
Selecionar os servidores de recuperação

Esta seção fornece informações sobre como executar a terceira etapa de seleção de um servidor de recuperação para executar a VM instantânea.

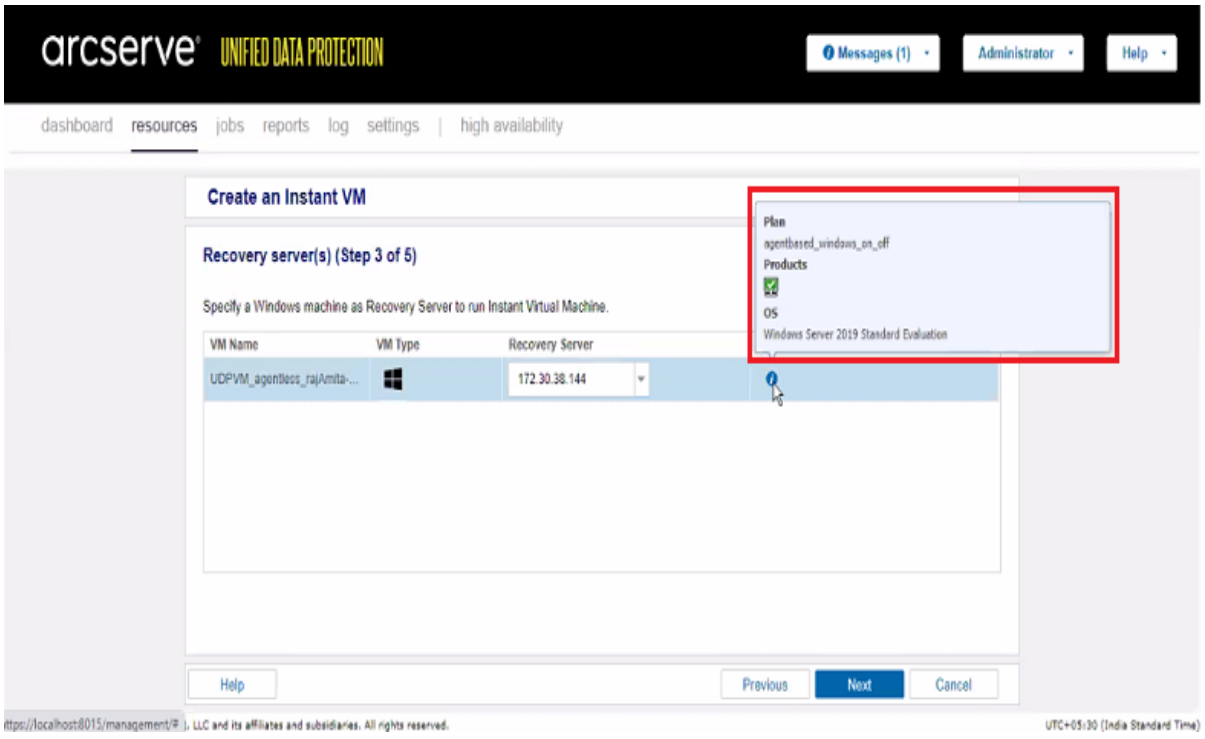
A tela dos servidores de recuperação exibe a lista de nós selecionados com detalhes como nome da VM, tipo de VM, servidor de recuperação e detalhes do plano. Para cada nó da lista, é possível selecionar o servidor de recuperação para executar a VM instantânea.

Siga estas etapas:

1. Na tela dos servidores de recuperação, em cada nó, faça o seguinte:



   - Para o servidor de recuperação, na lista suspensa, selecione o servidor de recuperação necessário.
   - Em Detalhes do plano, passe o mouse sobre o ícone de informações para verificar os detalhes do plano.



Observações:

- Em sessões de backup do Linux, o servidor de recuperação é um servidor de backup Linux.
- Quando o hipervisor é o VMware vSphere, a função NFS (Network File System - Sistema de arquivos da rede) do Windows deve ser instalada no servidor de ponto de recuperação. Ele é instalado automaticamente durante o processo da VM instantânea. Para instalar o sistema de arquivos de rede manualmente, consulte o tópico Como instalar manualmente o sistema de arquivos de rede em um servidor Windows.

2. Clique em **Avançar**.

   A tela Configurações das máquinas virtuais é exibida.

Conclua a próxima etapa: Definir as configurações das máquinas virtuais

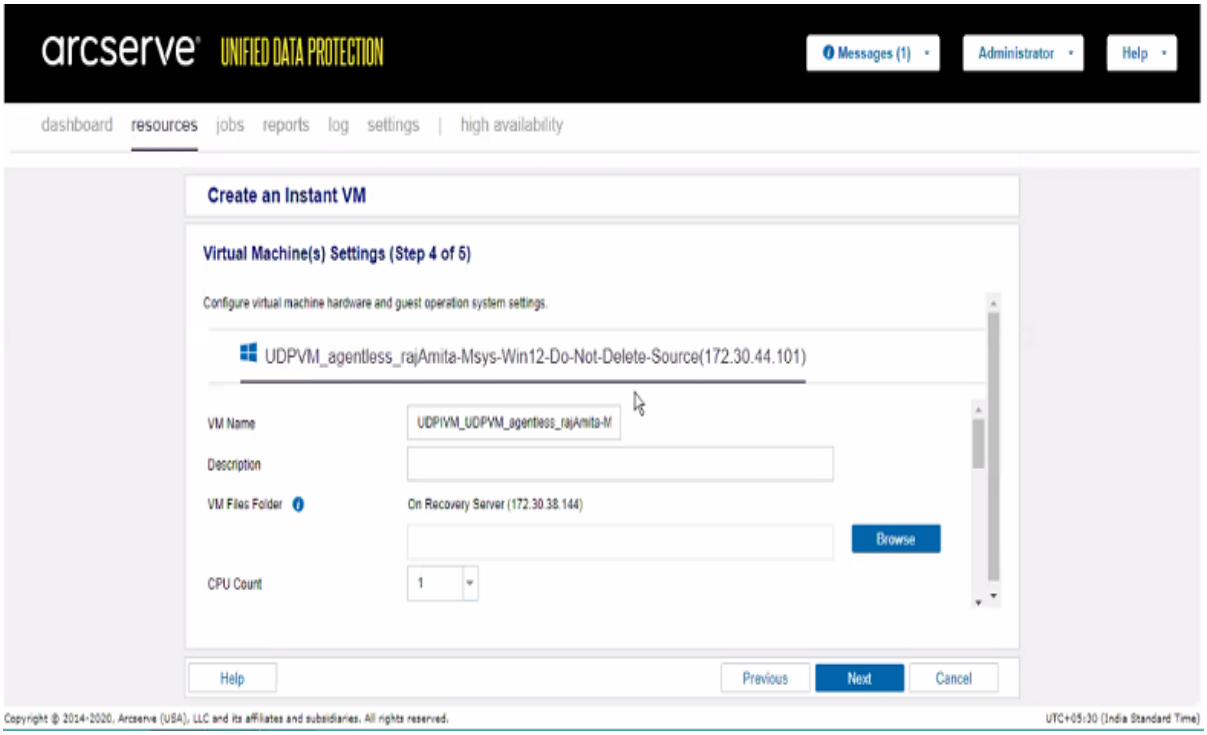
Definir as configurações das máquinas virtuais

Esta seção fornece informações sobre como definir as configurações da máquina virtual para criar uma VM instantânea.

A tela Configurações das máquinas virtuais exibe seções individuais para cada nó selecionado com os detalhes da configuração. Em cada seção, você pode fornecer os detalhes necessários para criar a VM instantânea.

Siga estas etapas:

1. Na tela Configurações das máquinas virtuais, clique no nó da VM que deseja configurar.



2. No nó da VM selecionado, faça o seguinte:
   - Em Nome da VM, digite o nome da VM instantânea. O nome do nó de origem com um prefixo é o nome padrão da VM instantânea.
   - (Opcional) Para Descrição, digite a descrição necessária à VM instantânea.
   - Para Pasta de arquivos da VM, clique no botão **Procurar** para selecionar o local da pasta no servidor de recuperação da VM instantânea. Você também pode criar uma nova pasta na caixa de diálogo Pasta de arquivos da VM.

     Observação: a opção Pasta de arquivos da VM está disponível apenas para os nós da VM do Windows. Para o nó da VM do Linux, é possível selecionar o repositório de dados disponível na lista suspensa do repositório de dados de arquivos da VM.
   - Para Contagem de CPU, selecione o número de CPUs para a VM instantânea.
   - Para Tamanho da memória, digite o tamanho da memória da VM instantânea.

Observação: também é possível usar o controle deslizante para fornecer o tamanho da memória para a VM instantânea.

- Para Adaptadores de rede, faça o seguinte:

  Adicionar um adaptador

  É possível adicionar vários adaptadores de rede. Depois de adicionar um adaptador de rede, é possível editar e excluir o adaptador de rede da coluna Ações.

  Observação: para uma VM instantânea do Linux, é possível usar pelo menos uma NIC virtual para se conectar ao servidor de backup Linux.

  Para adicionar um adaptador de rede, siga estas etapas:

  a. Na seção Adaptador de rede, clique em **Adicionar um adaptador**.

     A caixa de diálogo Adaptador de rede é exibida.

  b. Na caixa de diálogo Adicionar adaptador da rede, digite os seguintes detalhes e clique em **OK**.

     - **Rede virtual:** na lista suspensa Rede virtual, selecione a rede virtual necessária.
     - **Tipo de adaptador:** na lista suspensa Tipo de adaptador, selecione o tipo do adaptador.
     - **Configurações de TCP/IP:** na lista suspensa Configurações de TCP/IP, selecione **Origem (automático)** ou **Configurações de IP/gateway/DNS/WINS personalizadas**, conforme necessário.

       Observação: se você selecionar a opção Configurações de IP/gateway/DNS/WINS personalizadas, clique em Adicionar um endereço para fornecer os detalhes de TCP/IP manualmente.

  O adaptador de rede é adicionado.

  Atualize o DNS

  Se você já tiver fornecido um endereço IP e um endereço DNS no adaptador de rede e no computador de origem de um domínio, poderá atualizar o DNS usando as seguintes etapas:

Observação: esse recurso só está disponível para a VM instantânea do Windows.

a. Na seção Adaptador de rede, clique em **Atualizar DNS**.

b. Para adicionar um registro de atualização de DNS, clique em **Adicionar um endereço DNS**.

Observações:

- Você pode remover o registro de atualização de DNS. Para remover, clique em **Remover**.
- Para ajustar a sequência dos registros, clique no botão Para cima e Para baixo.

c. Selecione um endereço DNS e um endereço IP na lista suspensa e, em seguida, clique em **OK**.

d. Especifique o TTL (Time to Live - Tempo de Vida).

e. Especifique a autenticação de DNS.

Para o servidor DNS da Microsoft, digite o nome de usuário e a senha. Para o Servidor Bind, é necessário especificar o caminho completo, incluindo o nome de arquivo do arquivo de chave no servidor de recuperação.

- Para Configurações avançadas, faça o seguinte:
  - Verifique o espaço livre em disco da capacidade de Pasta de arquivos da VM.

    Observação: a caixa de seleção **Monitore o espaço livre em disco da capacidade da pasta de arquivos da VM** vem marcada por padrão. A barra de capacidade é exibida em amarelo na página Máquinas virtuais instantâneas quando o espaço livre da capacidade de Pasta de arquivos da VM é menor do que o valor-limite. O valor-limite padrão é 3%. Você pode alterar o valor conforme necessário.

  - Marque a caixa de seleção **Especificar o tipo de controlador de disco para a máquina virtual** e, na lista suspensa, selecione o tipo de controlador de disco da máquina virtual.

    Observação: a caixa de seleção **Especificar o tipo de controlador de disco para a máquina virtual** estará disponível se você tiver selecionado **VMware vSphere** como o local da VM. A

máquina virtual instantânea é criada aplicando-se o controlador do disco especificado na VMware.

- Para redirecionar as atualizações de disco virtual para o VMware Datastore, siga estas etapas:

  a. Marque a caixa de seleção **Redirecionar as atualizações de disco virtual para o Repositório de Dados VMware**.

     Observação: a caixa de seleção **Redirecionar as atualizações do disco virtual para o repositório de dados VMware** estará disponível se você tiver selecionado VMware vSphere como o local da VM.

  b. Na lista suspensa, selecione o repositório de dados VMware.

  As atualizações do disco virtual são redirecionadas para o repositório de dados VMware selecionado.

- Para alterar o nome de host da máquina virtual instantânea, siga estas etapas:

  a. Clique na caixa de seleção **Alterar nome do host**.

     A tela é atualizada com os novos campos.

  b. No campo Novo nome do host, digite o novo nome do host, conforme necessário.

  c. Se o computador de origem estiver em um domínio, forneça os seguintes detalhes, conforme necessário:

     - **Conta do usuário:** digite a conta do usuário.
     - **Senha:** digite a senha.
     - **Confirmar senha:** digite a senha novamente para confirmar.

     Observação: se o computador de origem estiver em um domínio, a conta deverá ter as permissões de conta para alterar o nome do host no domínio.

- (Opcional) Para a VM instantânea do Linux, selecione a opção **Recuperar dados automaticamente depois de iniciar a VM instantânea** para ativar a recuperação automática dos dados quando o destino da VM instantânea for iniciado.

  O comportamento padrão da VM instantânea do Linux é primeiro recuperar os dados necessários e, depois, iniciar a VM. Se

a opção não for selecionada, quando a VM iniciar, os dados restantes não serão recuperados, mesmo se ela for usada como uma VM normal. Se a opção for selecionada, os dados restantes serão recuperados no back-end ao usar a VM. Também é possível preservar o destino da VM instantânea permanentemente ao concluir a recuperação de dados.

Observação: quando o status do destino da VM instantânea do Linux estiver desligado, a tarefa de VM instantânea falhará. Se esse ponto de recuperação for mesclado, a VM instantânea do Linux falhará ao ligar.

3. Clique em **Avançar**.

   A tela Resumo é exibida.

Conclua a etapa final: Verificar resumo

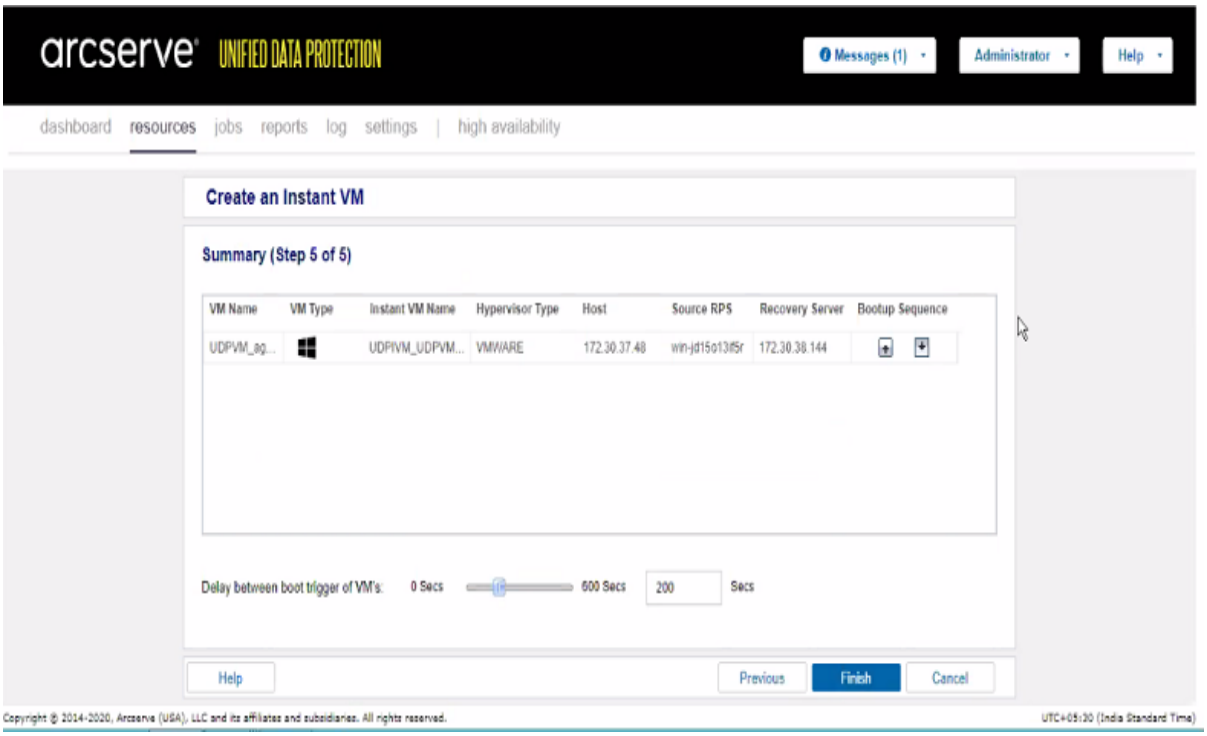
Verificar o resumo

Esta é a etapa final para criar VMs instantâneas simultâneas. Esta seção fornece informações sobre como verificar o resumo, ajustar a sequência de inicialização e fornecer atraso entre o acionamento da inicialização das VMs.

A tela Resumo exibe a lista de nós selecionados com detalhes como nome da VM, tipo de VM, nome da VM instantânea, tipo de hipervisor, host, RPS de origem, servidor de recuperação e sequência de inicialização. Você pode verificar os detalhes e priorizar as VMs na ordem que deseja inicializar.

Siga estas etapas:

1. Na tela Resumo, faça o seguinte:



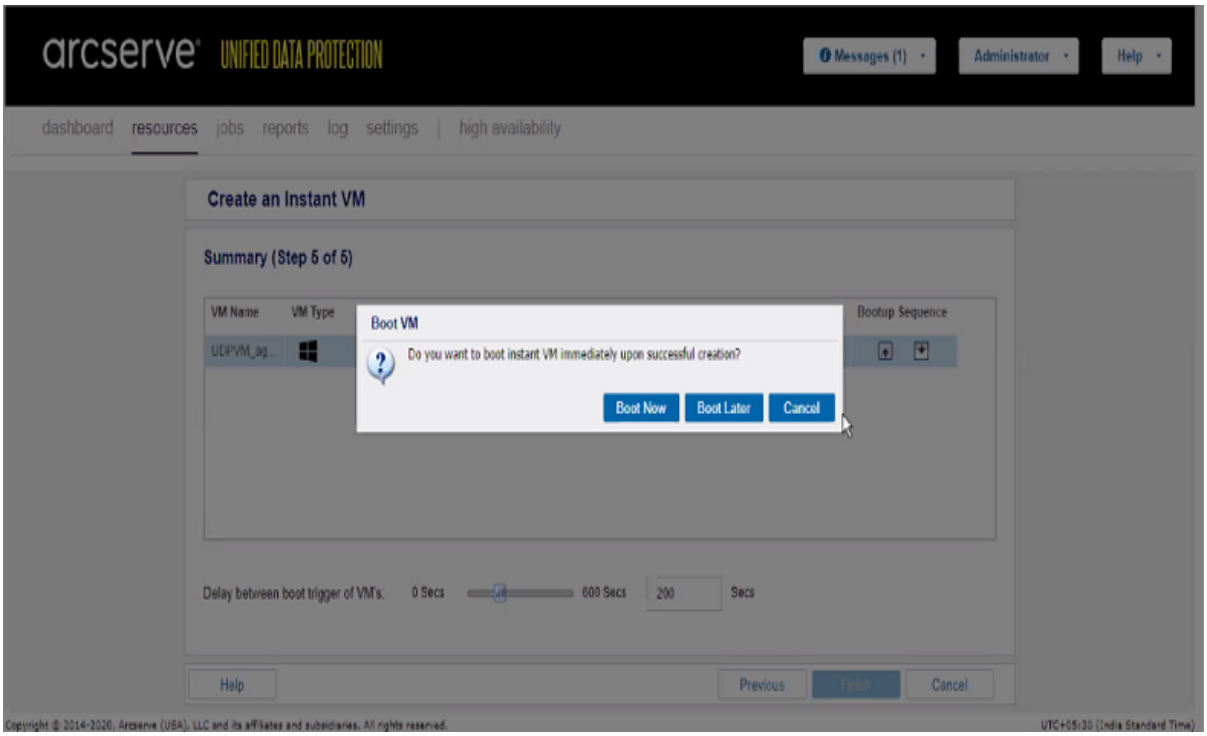
   - Na lista de nós, na sequência de inicialização de cada nó, clique no botão para cima ou para baixo para priorizar a sequência de inicialização da VM.
   - Para Atraso entre o acionamento da inicialização das VMs, digite o tempo de atraso no intervalo de 0 a 600 segundos.

     Observação: você também pode usar o controle deslizante para definir o tempo de atraso.

2. Clique em **Concluir**.

   A caixa de diálogo Inicializar VM é exibida.

3. Na caixa de diálogo VM de inicialização, selecione uma das seguintes opções:



- **Inicializar agora:** cria VMs instantâneas simultâneas. Depois que as VMs instantâneas simultâneas são criadas, o console inicia as VMs automaticamente.
- **Inicializar mais tarde:** cria VMs instantâneas simultâneas. Após a criação das VMs instantâneas simultâneas, é possível iniciá-las manualmente.
- **Cancelar:** você retorna à página Criar novas VMs instantâneas sem criar VMs instantâneas simultâneas.

As VMs instantâneas simultâneas são criadas.

Como configurar as máquinas simultâneas no modo de espera virtual

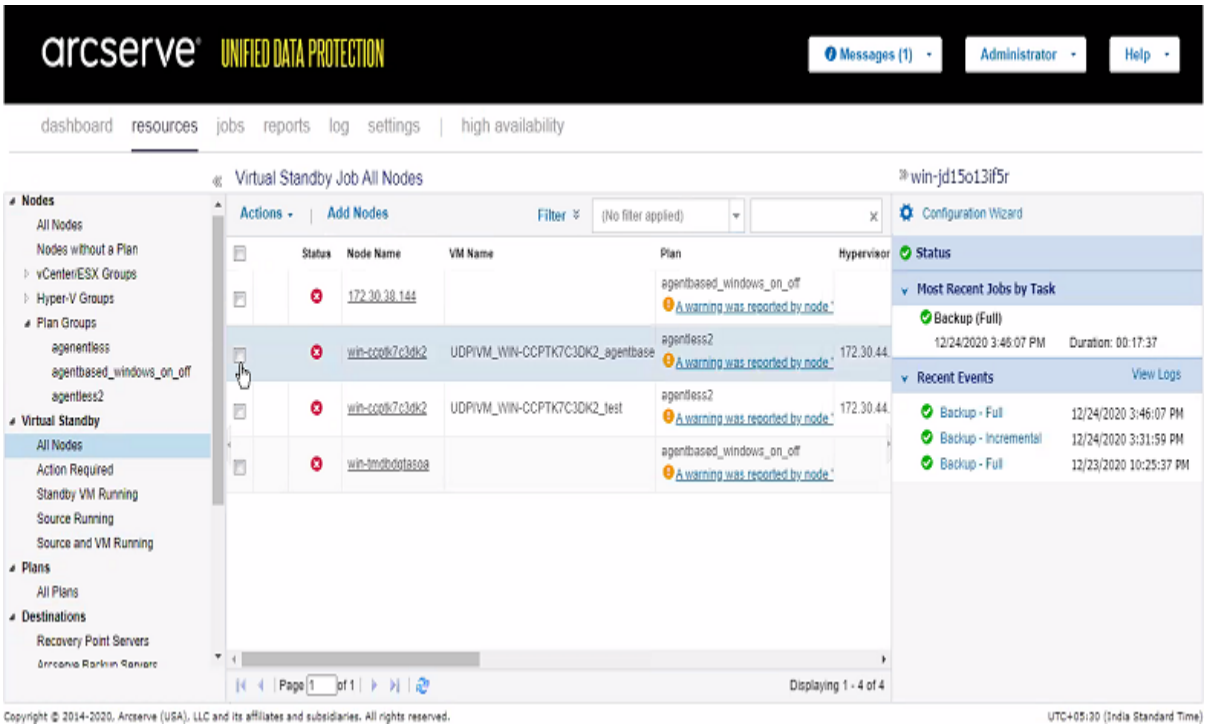
Esta seção fornece informações sobre como configurar as máquinas simultâneas no modo de espera virtual.

É possível configurar as máquinas simultâneas no modo de espera virtual no console do Arcserve UDP usando a caixa de diálogo VM em modo de espera.

Siga estas etapas:

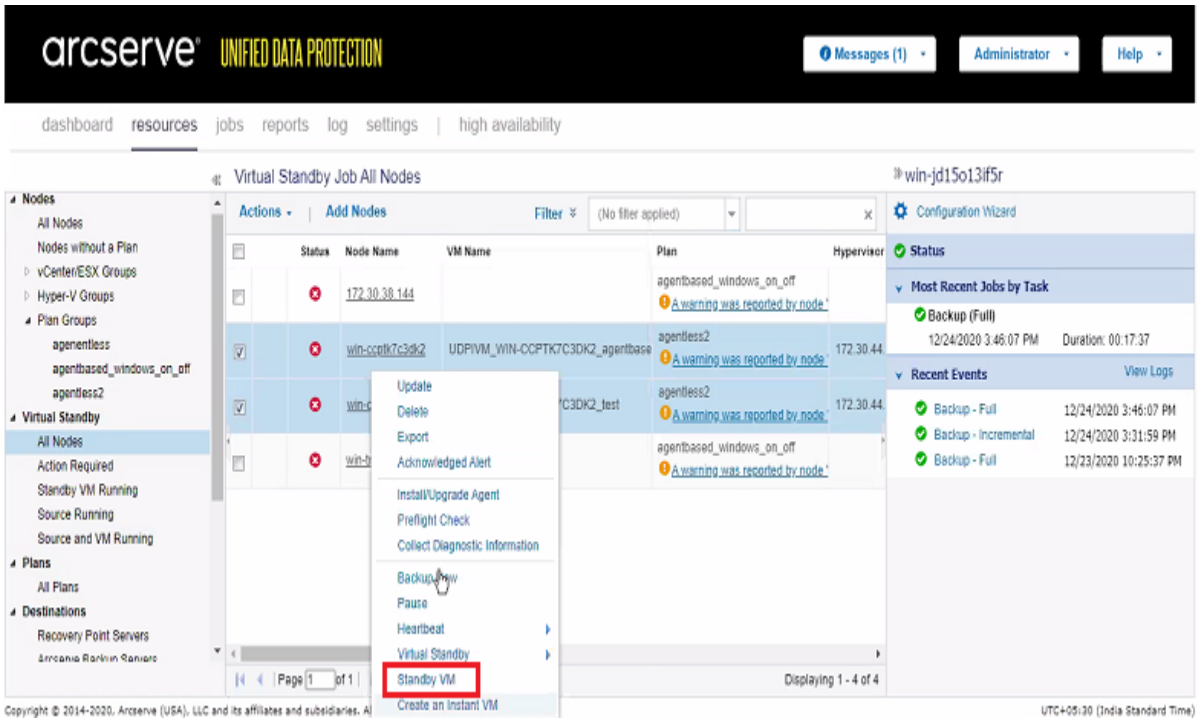
1. Efetue logon no Console do Arcserve UDP.
2. Na página Console do UDP, clique na guia **recursos**.
3. No painel esquerdo, navegue para **Nós** > **Todos os nós**.

   A lista de nós existentes é exibida no painel central.



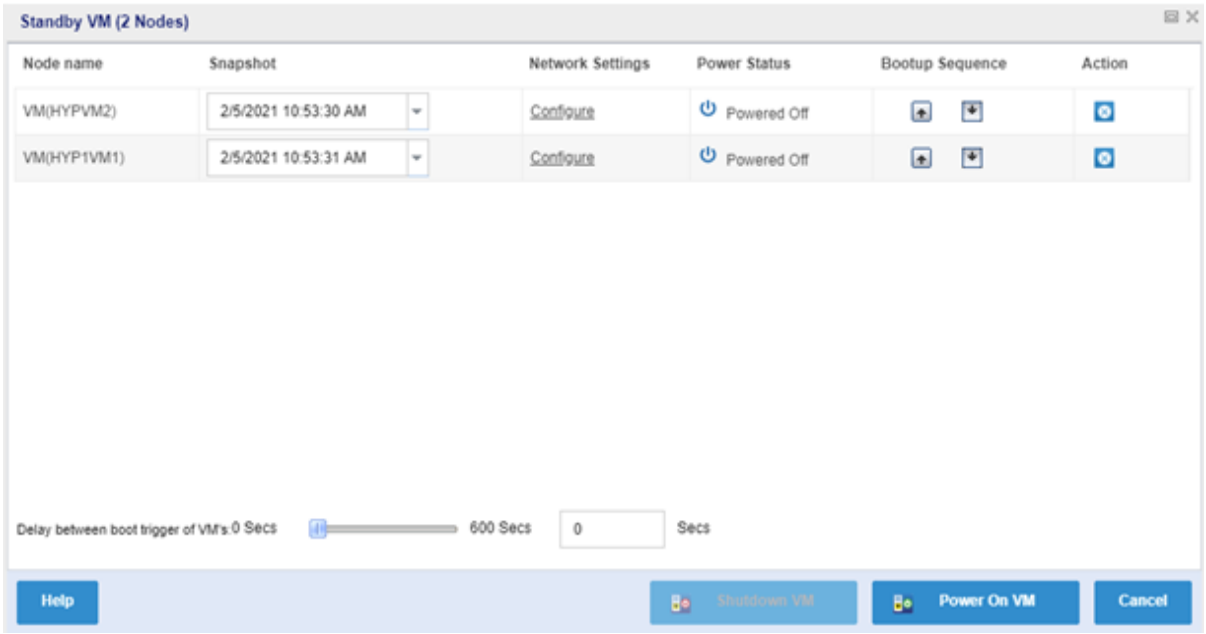
4. Selecione um ou mais nós que já estejam associados a um plano.

   Observação: se um nó não estiver associado a nenhum plano, a opção VM em modo de espera não será exibida.



5. Clique com o botão direito do mouse nos nós selecionados e, em seguida, selecione a opção **VM em modo de espera**.

   A caixa de diálogo VM em modo de espera é exibida com a lista de nós selecionados.



6. Na caixa de diálogo VM em modo de espera, execute as seguintes tarefas:

- **Ligar VM**

  Observação: essa opção é ativada apenas para máquinas virtuais em modo de espera desligadas.

  Para ligar as máquinas virtuais simultaneamente, siga estas etapas:

  a. Na lista de nós selecionados, para cada nó, faça o seguinte:

     - Para Instantâneo, na lista suspensa, selecione a data e a hora do instantâneo do ponto de recuperação.

       Observação: os detalhes de Instantâneo são exibidos somente quando a tarefa do VSB é concluída com êxito.

     - Para Configurações de rede, selecione o link Configurar. Para obter mais informações, consulte Configurar a rede da VM em espera.

     - Para Sequência de inicialização, clique no botão para cima ou para baixo para priorizar a sequência de inicialização da VM em modo de espera.

     - Em Ação, clique no ícone de cruz de cor azul para remover o nó.

  b. (Opcional) Para Atraso entre o acionamento da inicialização das VMs, digite o tempo de atraso no intervalo de 0 a 600 segundos.

     Observação: você também pode usar o controle deslizante para definir o tempo de atraso.

  c. Clique em **Ligar VM**.

     As VMs em modo de espera são ligadas simultaneamente usando os dados contidos no instantâneo do ponto de recuperação.

- **Desligar VM**

  Para desligar as máquinas virtuais em modo de espera simultaneamente, clique em **Desligar VM**.

  Observação: essa opção é ativada apenas para máquinas virtuais em modo de espera ativadas.

Capítulo 12: Usando o instantâneo de hardware para backup

Esta seção contém os seguintes tópicos:

Como usar o instantâneo de hardware para backup

O Arcserve UDP tem o recurso de utilizar instantâneos de armazenamento de hardware para backup. Você pode especificar se deseja que um instantâneo de hardware seja gerado durante a criação de uma tarefa de backup. Se você selecionar o instantâneo de hardware, o Arcserve UDP primeiro tenta criar um instantâneo de hardware. Se o instantâneo de hardware falhar, o Arcserve UDP reverte automaticamente para o instantâneo de software sem uma falha na tarefa de backup.

É possível usar o instantâneo de hardware para um backup com base em agente (máquinas físicas do Windows) ou backup sem agente com base em host (VMware e Hyper-V).

Matrizes de armazenamento com suporte:

- **Matriz de armazenamento NetApp:** o Arcserve UDP oferece suporte ao instantâneo de hardware para backups com base em agente (máquinas físicas do Windows) e backups sem agente com base em host (VMware e Hyper-V).
- **Matriz de armazenamento Nimble:** o Arcserve UDP oferece suporte ao instantâneo de hardware para backups com base em agente (máquinas físicas do Windows) e backups sem agente com base em host (VMware e Hyper-V).
- **Matriz de armazenamento HPE 3PAR storeserve:** o Arcserve UDP oferece suporte ao instantâneo de hardware para backups com base em agente (máquinas físicas do Windows) e backups sem agente com base em host (VMware e Hyper-V).
- **Matriz de armazenamento Dell EMC Unity VSA:** o Arcserve UDP oferece suporte ao instantâneo de hardware para backups com base em agente (máquinas físicas do Windows) e backups sem agente com base em host (Hyper-V).

O que fazer a seguir

- Usar o instantâneo de hardware para o backup sem agente da VMware
- Usar o instantâneo de hardware para o backup sem agente do Hyper-V
- Usar o instantâneo de hardware para o backup com base em agente
- Verificar se o backup usou o instantâneo de hardware

Usar o instantâneo de hardware para o backup sem agente da VMware

Siga estas etapas:

1. Verifique se os seguintes pré-requisitos foram atendidos:

   Para o instantâneo do NetApp

   - O Arcserve UDP oferece suporte a LUNs iSCSI//FC do NetApp e a exportações de volumes NFS do NetApp que foram configurados como armazenamentos de dados. O iSCSI, o FC e o NFS devem atender a determinadas condições para usar o instantâneo de hardware.

     Considerações sobre o suporte a iSCSI/FC do NetApp para VMware

     Considerações sobre o suporte a NFS da VMware

   - Para criar um instantâneo de hardware para a VMware, adicione a matriz de armazenamento ao console. Para obter mais informações sobre a adição de uma matriz de armazenamento, consulte o tópico Adicionar uma matriz de armazenamento.
   - Para usar o instantâneo de hardware, a licença Flexclone é recomendável para as matrizes de armazenamento do NetAapp com o Data ONTAP, operando no modo de 7 e no modo de agrupamento.

   Observação: para obter mais informações sobre como configurar o NetApp, consulte a documentação do NetApp ou entre em contato com a equipe de suporte da NetApp.

   Instantâneo de hardware do HPE 3PAR:

   - Para oferecer suporte ao instantâneo de hardware da VM da VMware, o HP RMC deve gerenciar a matriz de armazenamento do HPE 3PAR.
   - A matriz de armazenamento precisa ter a licença da cópia virtual.

     Protocolos suportados para o instantâneo de hardware do VMware: FC e iSCSI
   - Para criar um instantâneo de hardware para a VMware, adicione a matriz de armazenamento ao console. Para obter mais informações sobre a adição de uma matriz de armazenamento, consulte o tópico Adicionar uma matriz de armazenamento.

   Instantâneo de hardware Nimble:

- Protocolos suportados para o instantâneo de hardware do VMware: FC e iSCSI
- Para criar um instantâneo de hardware para a VMware, adicione a matriz de armazenamento ao console. Para obter mais informações sobre a adição de uma matriz de armazenamento, consulte o tópico Adicionar uma matriz de armazenamento

  Considerações sobre o armazenamento Nimble quando a autenticação CHAP está ativada

2. Efetue logon no Console e crie um plano para backup.

   Observação: para obter mais informações sobre como criar um plano de backup sem agente, consulte Como criar um plano de backup sem agente com base em host.

3. Verifique se você selecionou a opção **Usar instantâneo de hardware sempre que possível** na guia **Avançado**.

   Observação: para executar o backup somente a partir do instantâneo de hardware (e não do instantâneo de software), o Arcserve UDP fornece a seguinte chave de Registro: *FallbackToSWSnapshot =0(dword)*

   É possível aplicar essa chave de Registro para um nó específico, bem como para todos os nós.

   - Para aplicar a um nó específico, crie o Registro em HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\(Nodeid)

     Observação: (Nodeid) só é criado depois de um backup.

   - Para aplicar a todos os nós, crie o Registro em HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   Importante: se a subchave "AFBackupDll" não estiver disponível, então, você deverá adicionar manualmente a subchave *AFBackupDll* sob engine, como Engine\AFBackupDll\ e, em seguida, adicionar *DWORD FallbackToSWSnapshot* sob *AFBackupDll*.

4. **Salve o plano e envie a tarefa de backup.**

   A tarefa de backup é executada usando-se o instantâneo de hardware.

Considerações sobre o suporte a iSCSI/FC do NetApp para VMware

O Arcserve UDP oferece suporte a instantâneos de hardware para a máquina virtual da VMware somente quando a matriz de armazenamento subjacente for uma matriz de armazenamento do NetApp.

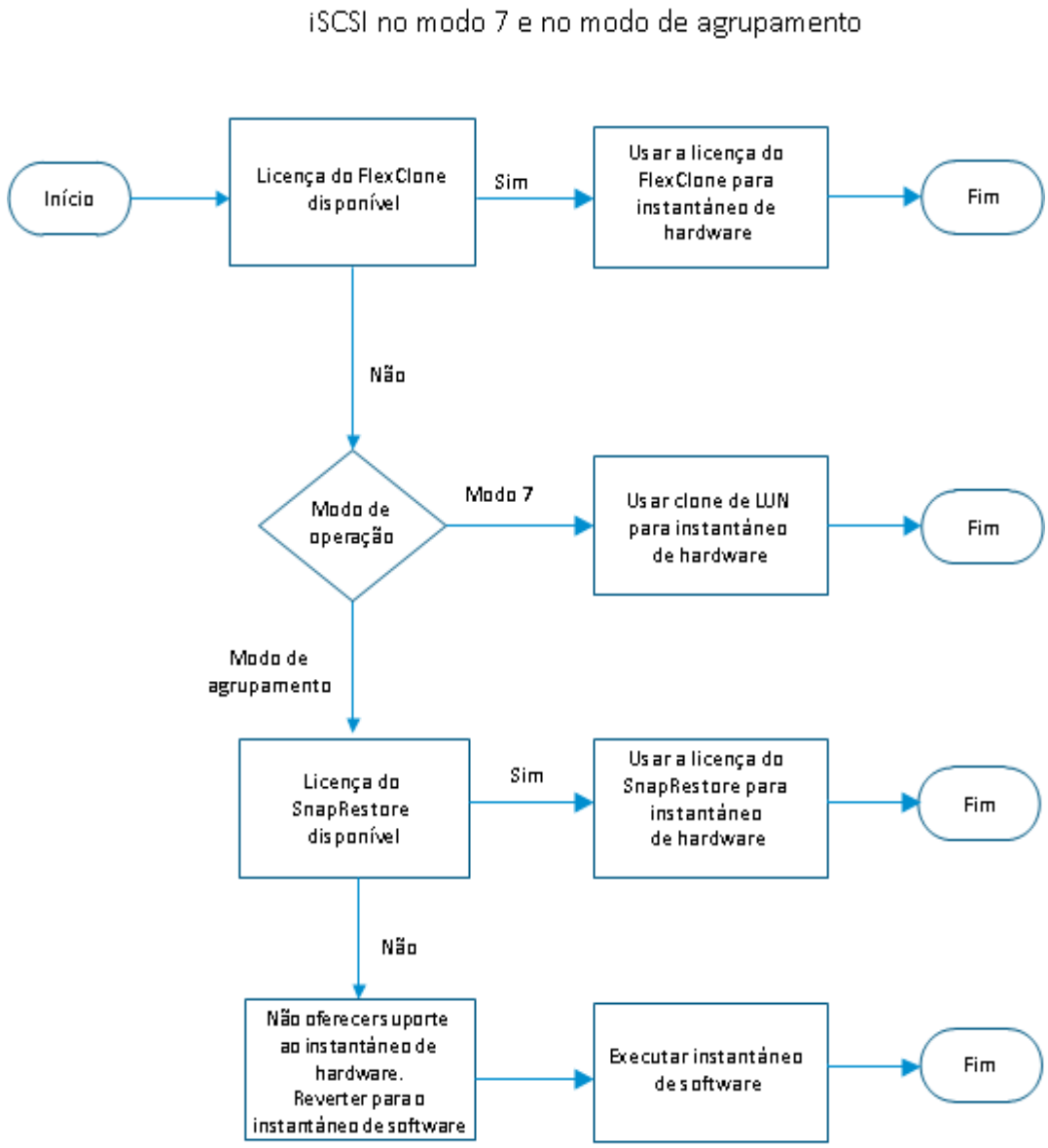
NetApp no modo 7

Se o sistema de armazenamento do NetApp opera no modo 7, não é obrigatório instalar quaisquer licenças adicionais para usar instantâneos de hardware. No entanto, é recomendável que a licença FlexClone esteja instalada.

NetApp no modo de agrupamento

Se o sistema de armazenamento do NetApp opera no modo de agrupamento (modo C), você deve ter uma licença FlexClone ou SnapRestore instalada para usar os instantâneos de hardware.

O fluxograma a seguir explica as condições aplicadas ao instantâneo de hardware para iSCSI/FC do NetApp VMware:



Limitação de um clone de LUN

Em um clone de LUN tradicional, às vezes, o instantâneo do backup não pode ser excluído durante as operações de limpeza. Em geral, um LUN existe como um arquivo no sistema de arquivos. Portanto, um instantâneo captura o arquivo. Quando você cria um clone de LUN, outro arquivo é criado no sistema de arquivos. Portanto, o próximo instantâneo captura o arquivo original e o arquivo duplicado. Quando vários instantâneos são capturados, o clone de LUN torna-se parte da cadeia de instantâneos. Agora, se você excluir um instantâneo, ele não será excluído porque ele se refere a um clone de LUN que, por sua vez, tem o apoio de outro instantâneo. Em tais casos, não é possível excluir um instantâneo até que você exclua o clone de LUN e todos os instantâneos que fazem referência a esse clone de LUN. Como resultado, sua política de retenção para os instantâneos programados pode ser interrompida.

Para evitar esse problema, instale a licença FlexClone no sistema de armazenamento do NetApp e o Arcserve UDP usará a tecnologia FlexClone para clonar o LUN.

Chaves de registro para o SnapRestore

Quando você usa a licença do SnapRestore, a restauração de LUNs demora mais dependendo do tamanho do LUN e do ambiente. Isso ocorre porque a exclusão de um instantâneo demora mais, pois o instantâneo está ocupado restaurando o LUN, o que leva mais tempo. O Arcserve UDP não tem um mecanismo para monitorar o progresso de restauração do LUN. Portanto, o Arcserve UDP usa o mecanismo de restauração para excluir o instantâneo.

O Arcserve UDP fornece duas chaves de registro (**DeleteRetryTimeoutInMins** e **DeleteRetryCount**) que você pode usar para melhorar o desempenho da exclusão de instantâneo dependendo do tamanho de LUN e do ambiente. As chaves de registro estão no seguinte local:

SOFTWARE\Arcserve\Unified Data Protection\Engine

DeleteRetryTimeoutInMins

Especifica a duração do tempo limite (em minutos) para excluir um instantâneo. Se você tiver apenas SnapRestore e você não tiver a licença FlexClone, é provável que a exclusão do instantâneo demore. É possível usar a chave de registro para especificar valores personalizados. No entanto, recomendamos que você use a licença FlexClone.

Por exemplo, se a duração do tempo limite for dois minutos, o agente de UDP aguardará dois minutos para o NetApp excluir o instantâneo antes de enviar o comando delete a matriz de armazenamento do NetApp em sua próxima tentativa. Esta chave de registro é usada em combinação com a chave **DeleteRetryCount**.

Valor padrão: 1 (em minutos)

Tipo: REG_SZ

DeleteRetryCount

Especifica a contagem de repetições para excluir um instantâneo.

Por exemplo, se a contagem de repetição for cinco, o agente de UDP tentará enviar cinco vezes o comando snapshot delete para a matriz de armazenamento do NetApp. Depois de tentar enviar cinco vezes o comando snapshot delete, se o instantâneo ainda existir, é necessário excluir manualmente o instantâneo e, também, aumentar a contagem de repetições para o valor apropriado para que o próximo backup não tenha esse problema.

Esta chave de registro é usada em associação com a chave **DeleteRetryTimeoutInMins**.

Valor padrão: 30

Tipo: REG_SZ

Chaves de registro para desativar a reserva de espaço de LUN

Quando o clone de LUN é executado durante o backup usando o instantâneo de hardware, por padrão, a reserva de espaço é herdada do LUN de origem. O Arcserve UDP fornece uma chave de registro que pode ser usada para desativar a reserva de espaço. A chave de registro está no seguinte local:

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

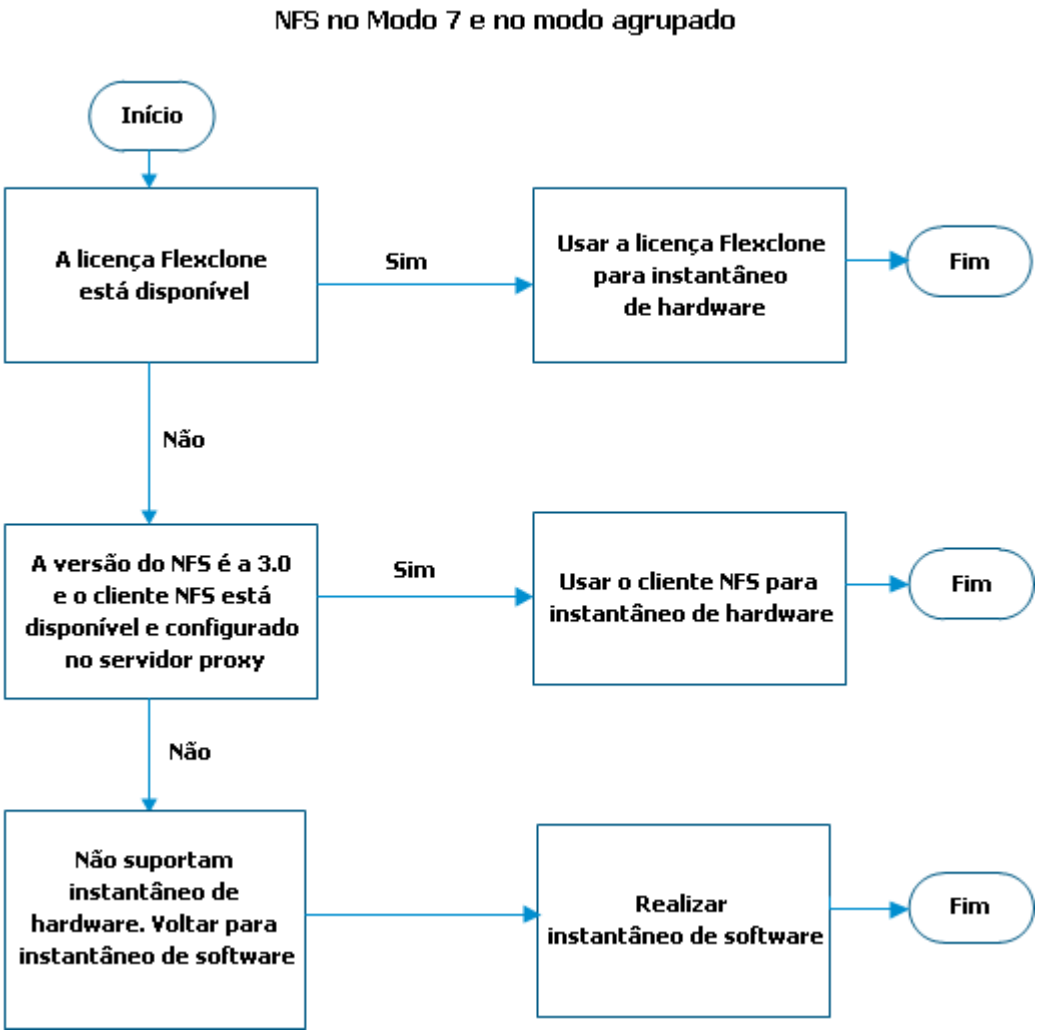
DisableLunSpaceReservation =1

Especifica que as reservas de espaço de LUN estão desativadas.

Observação: isso é aplicável somente quando a licença FlexClone é aplicada.

Considerações sobre o suporte a NFS da VMware

O fluxograma a seguir explica as condições aplicadas ao instantâneo de hardware para NFS do NetApp VMware:



O Arcserve UDP oferece suporte ao instantâneo de hardware para repositórios de dados do NFS versão 3.0. Para usar o instantâneo de hardware, o proxy de backup deve ter instalado e configurado o cliente Microsoft NFS.

A tabela a seguir exibe as versões NFS que oferecem suporte a VM VMware e ao Arcserve UDP. Certifique-se de que você tenha a versão correta do NFS com a versão correspondente do VMware.

Versões do VMware	Versões de NFS com suporte para VMware	Versões de NFS com suporte de Arcserve UDP para instantâneo de hardware para FlexClone	Versões de NFS com suporte de Arcserve UDP para instantâneo de hardware para o cliente de NFS Windows
VMware 6.0	Oferece	Oferece suporte a RHEL 3.0 e	Só oferece suporte ao NFS 3.0 e

e posterior	suporte a RHEL 3.0 e CentOS 4.1	CentOS 4.1	deve atender aos pré-requisitos
Versões de VMware anteriores a 6.0	Só oferece suporte ao NFS 3.0	Suporte ao NFS 3.0	Só oferece suporte ao NFS 3.0 e deve atender aos pré-requisitos

Pré-requisito do NFS 3.0

- Se a licença FlexClone não estiver presente, para oferecer suporte ao instantâneo de hardware de arquivos VMDK hospedados em um repositório de dados NFS 3.0, o aplicativo NetApp deve ter as seguintes versões do OnTAP instaladas:
  - Todos os sistemas de Data ONTAP modo 7 são suportados.
  - Releases agrupadas de Data ONTAP 8.2 começando com a release 8.2.3 são suportadas. Também, as releases agrupadas de Data ONTAP 8.3 começando com a release 8.3.1 são compatíveis
  - Por padrão, o suporte ao cliente do Windows NFS v3 está desativado. Para ativá-lo em SVM (Storage Virtual Machine - Máquina Virtual de Armazenamento), use o comando a seguir:

  vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled

- O proxy de backup, que faz backup da VM do VMware, deve ter instalado e configurado o cliente Microsoft NFS. O proxy de backup deve ter acesso ao compartilhamento de NFS. Para instalar manualmente o cliente NFS no servidor, consulte Como instalar manualmente o cliente do Microsoft NFS em um servidor Windows.
- Você precisará reiniciar o serviço de cliente do Microsoft NFS no servidor proxy depois de implantar o plano de backup sem agente. É necessário reiniciar o serviço apenas uma vez pela primeira vez, devido à implantação do plano de disparar algumas alterações sobre o cliente NFS no servidor proxy.

Como instalar manualmente o cliente Microsoft NFS em um servidor Windows

Siga estas etapas para instalar manualmente o cliente Microsoft NFS em um servidor Windows.

1. Efetue logon no servidor Windows.
2. Abra o Gerenciador de servidor e clique em Gerenciar.
3. Clique em Adicionar recursos e funções.
4. Na caixa de diálogo Antes de começar, clique em Avançar.
5. Na caixa de diálogo Selecionar tipo de instalação, selecione instalação com base em função ou com base em recurso e clique em Avançar.
6. Na caixa de diálogo Selecionar servidor de destino, se você estiver instalando no servidor local, clique em Avançar. De outra forma, selecione um servidor na lista Pool de servidores.
7. Na caixa de diálogo Selecionar funções de servidor, clique em Avançar.
8. Na caixa de diálogo Selecionar recursos, role a lista dos recursos disponíveis e selecione a caixa de diálogo Cliente para NFS.
9. Clique em Avançar.
10. Na caixa de diálogo Confirmar seleções de instalação, revise as seleções e, em seguida, clique em Instalar.
11. Após a conclusão da instalação, verifique os resultados e, em seguida, clique em Fechar.

Considerações sobre o armazenamento Nimble quando a autenticação CHAP está ativada

É possível fazer backup de instantâneo de hardware quando o armazenamento Nimble tem uma autenticação CHAP ativada.

Observação: não há suporte para a autenticação CHAP no ESXi 5.0, pois essa versão do ESXi não possui SQLite.

É preciso atender aos seguintes pré-requisitos:

Pré-requisitos

Importante: os pré-requisitos se aplicam somente se você desejar que a tarefa de backup sem agente com base em host use a SAN como o modo de transporte.

- Ative SSH no ESXi onde o armazenamento Nimble está configurado com a autenticação CHAP.
- Verifique se o computador Proxy tem a interface de linha de comando iscsicli necessária para configurar os dispositivos de destino iSCSI.
- Defina a diretiva de execução para RemoteSigned no computador Proxy para executar os scripts do Powershell. Use o seguinte comando:

  Set-ExecutionPolicy RemoteSigned
- Salve as credenciais do ESXi por meio de um script do Powershell para o qual o armazenamento Nimble está configurado com autenticação CHAP.

  Siga estas etapas para salvar as credenciais do ESXi:

  - Execute o script do Powershell "StoreESXCredentials.ps1" do Powershell no Proxy.

    Você será solicitado a inserir detalhes sobre IP, nome de usuário e senha.
  - Insira todos os três parâmetros.

    As credenciais são armazenadas em um arquivo CSV "ESXCredentials.csv" e a senha é criptografada.

  Para localizar o script do Powershell, siga estas etapas:

  - Efetue logon no computador proxy e abra o Powershell.
  - Vá até o seguinte diretório:

    Observação: o caminho muda com base no diretório de instalação.

    C:\Arquivos de programas\Arcserve\Unified Data Protection\Engine\BIN

- Execute o script do Powershell conforme abaixo:

  PS C:\Arquivos de programas\\Arcserve\Unified Data Protection\Engine\BIN> .\StoreESXCredentials.ps1

Usar o instantâneo de hardware para o backup sem agente do Hyper-V

Importante: o backup sem agente do Hyper-V usa o instantâneo de hardware somente quando todos os discos da VM estão em volumes compatíveis com o instantâneo de hardware. Caso contrário, o backup usa o instantâneo de software.

Siga estas etapas:

1. Verifique se os seguintes pré-requisitos foram atendidos:
   - Instale um provedor de hardware VSS (por exemplo, NetApp) nos servidores Hyper-V. Para oferecer suporte ao instantâneo transportável, instale o provedor de hardware VSS no servidor proxy de backup. A configuração típica de um provedor de hardware VSS inclui:
     - Especificação de um servidor que controla o LUN
     - Especificar as credenciais da matriz de disco para acessar a matriz de disco

     Observação: para obter mais informações sobre como configurar o provedor de hardware VSS, entre em contato com o fornecedor do provedor de hardware.
   - O servidor Hyper-V e o servidor proxy devem ter uma versão de sistema operacional semelhante.
   - Se o servidor Hyper-V pertencer a um agrupamento, o servidor proxy não deverá fazer parte do agrupamento do Hyper-V.
2. Efetue logon no console e crie um plano para backup.

   Observação: para obter mais informações sobre como criar um plano de backup sem agente, consulte Como criar um plano de backup sem agente com base em host.
3. Verifique se você selecionou a opção **Usar instantâneo de hardware sempre que possível** na guia **Avançado**.

   Observação: para executar o backup somente a partir do instantâneo de hardware (e não do instantâneo de software), o Arcserve UDP fornece a seguinte chave de Registro: *FallbackToSWSnapshot =0(dword)*

   É possível aplicar essa chave de Registro para um nó específico, bem como para todos os nós.
   - Para aplicar a um nó específico, crie o Registro em HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data

Protection\Engine\AFBackupDll\(Nodeid)

Observação: (Nodeid) só é criado depois de um backup.

- Para aplicar a todos os nós, crie o Registro em HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

Importante: se a subchave "AFBackupDll" não estiver disponível, então, você deverá adicionar manualmente a subchave *AFBackupDll* sob engine, como Engine\AFBackupDll\ e, em seguida, adicionar *DWORD FallbackToSWSnapshot* sob *AFBackupDll*.

4. **Salve** o plano e **envie** a tarefa de backup.

   A tarefa de backup é executada usando o instantâneo de armazenamento.

Usar o instantâneo de hardware para o backup com base em agente

Siga estas etapas:

1. Verifique se os seguintes pré-requisitos foram atendidos:
   - Instale um provedor de hardware VSS que oferece suporte ao instantâneo de hardware em agentes do Arcserve UDP. A configuração típica de um provedor de hardware VSS inclui:
     - Especificação de um servidor que controla o LUN.
     - Especificação das credenciais da matriz de disco para acessar a matriz de disco.

     Observação: Para obter mais informações sobre como configurar o provedor de hardware VSS, entre em contato com o fornecedor do provedor de hardware.
2. Efetue logon no console e crie um plano para backup.

   Observação: para obter mais informações sobre a criação de um plano com base em agente para Windows, consulte Como criar um plano de backup Windows.
3. Verifique se você selecionou a opção **Usar instantâneo de hardware sempre que possível** na guia **Avançado**.
4. Salve o plano e envie a tarefa de backup.

   A tarefa de backup é executada usando o instantâneo de armazenamento.

Verificar se o backup usou o instantâneo de hardware

Se os pré-requisitos para um instantâneo de hardware não forem atendidos, o Arcserve UDP alternará automaticamente para um instantâneo de software sem uma falha na tarefa de backup. Se o instantâneo de hardware falhar, o evento será registrado nos logs de atividades.

Verifique as mensagens de log para garantir que o backup usou o instantâneo de hardware.

Siga estas etapas:

1. Navegue até o seguinte caminho:

   <Pasta de instalação>\Arcserve\Unified Data Protection\Engine\Logs

2. Abra o arquivo correspondente à respectiva ID da tarefa.

   Por exemplo, se a ID da tarefa é JW002, vá para a pasta **Logs** e abra o arquivo JW002.

3. Examine as mensagens no arquivo para confirmar se o backup usou o instantâneo de armazenamento.

   Você usou com êxito o instantâneo de armazenamento para um backup.

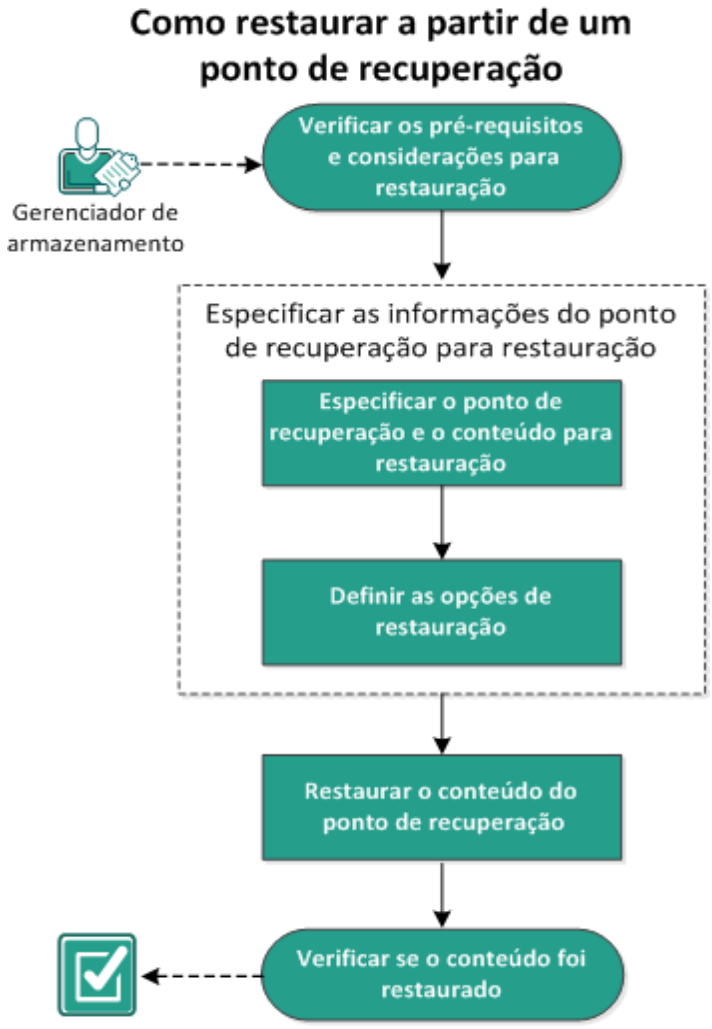
Capítulo 13: Restaurando dados protegidos

Esta seção contém os seguintes tópicos:

Como restaurar a partir de um ponto de recuperação

Cada vez que o Arcserve UDP executa um backup com êxito, também é criada uma imagem de instantâneo pontual de seu backup (ponto de recuperação). Essa coleta de pontos de recuperação permite localizar e especificar exatamente qual imagem de backup deve ser restaurada. Posteriormente, se você suspeitar que as informações de backup estão ausentes, corrompidas ou não são confiáveis, é possível localizar e restaurar a partir de uma versão anterior válida.

O diagrama seguinte ilustra o processo para restaurar um ponto de recuperação:



Execute as tarefas a seguir para restaurar um ponto de recuperação:

1. Verificar os pré-requisitos e as considerações para restauração
2. Especifique as informações do ponto de recuperação para restauração
    a. Especifique o ponto de recuperação e o conteúdo para restauração
    b. Definir as opções de restauração

3. Restaure o conteúdo do ponto de recuperação
4. Verificar se o conteúdo foi restaurado

Verificar os pré-requisitos e as considerações para restauração

Verifique se os pré-requisitos a seguir existem antes de executar uma restauração:

- Você tem pelo menos um ponto de recuperação para restauração.
- Você tem um destino válido e acessível de ponto de recuperação para do qual restaurar o ponto de recuperação de conteúdo.
- Você tem um local de destino válido e acessível para o qual restaurar o ponto de recuperação de conteúdo.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Revise as seguintes considerações de restauração:

- Se a restauração para um destino remoto e se todas as letras de unidade (A - Z) estiverem ocupadas, a restauração de dados para um caminho remoto não serão bem-sucedidas. O Agente do Arcserve UDP (Windows) precisa usar uma letra de unidade para montar o caminho do destino remoto.
- (Opcional) Compreenda como funciona o processo de restauração. Para obter mais informações, consulte Como a restauração em nível de arquivo funciona.
- (Opcional) Examine os arquivos ignorados durante a restauração. Para obter mais informações, consulte o tópico Arquivos ignorados durante a restauração.
- Ao tentar restaurar uma sessão de backup otimizada em um volume que não esteja vazio (restauração não otimizada), a tarefa de restauração pode levar mais tempo do que o exibido no tempo estimado do monitor de tarefas. A quantidade de dados que é processada e o tempo decorrido pode aumentar com base nos dados que são otimizados no volume.

Exemplo:

O tamanho do volume de backup é de 100 GB e, após a otimização, o tamanho do volume é reduzido para 50 GB.

Ao executar uma restauração não otimizada desse volume, o monitor de tarefas de restauração exibe 100% após restaurar 50 GB, mas levará mais tempo para restaurar todos os 100 GB.

- A mensagem do log de atividades a seguir será exibida durante a restauração de arquivos do sistema:

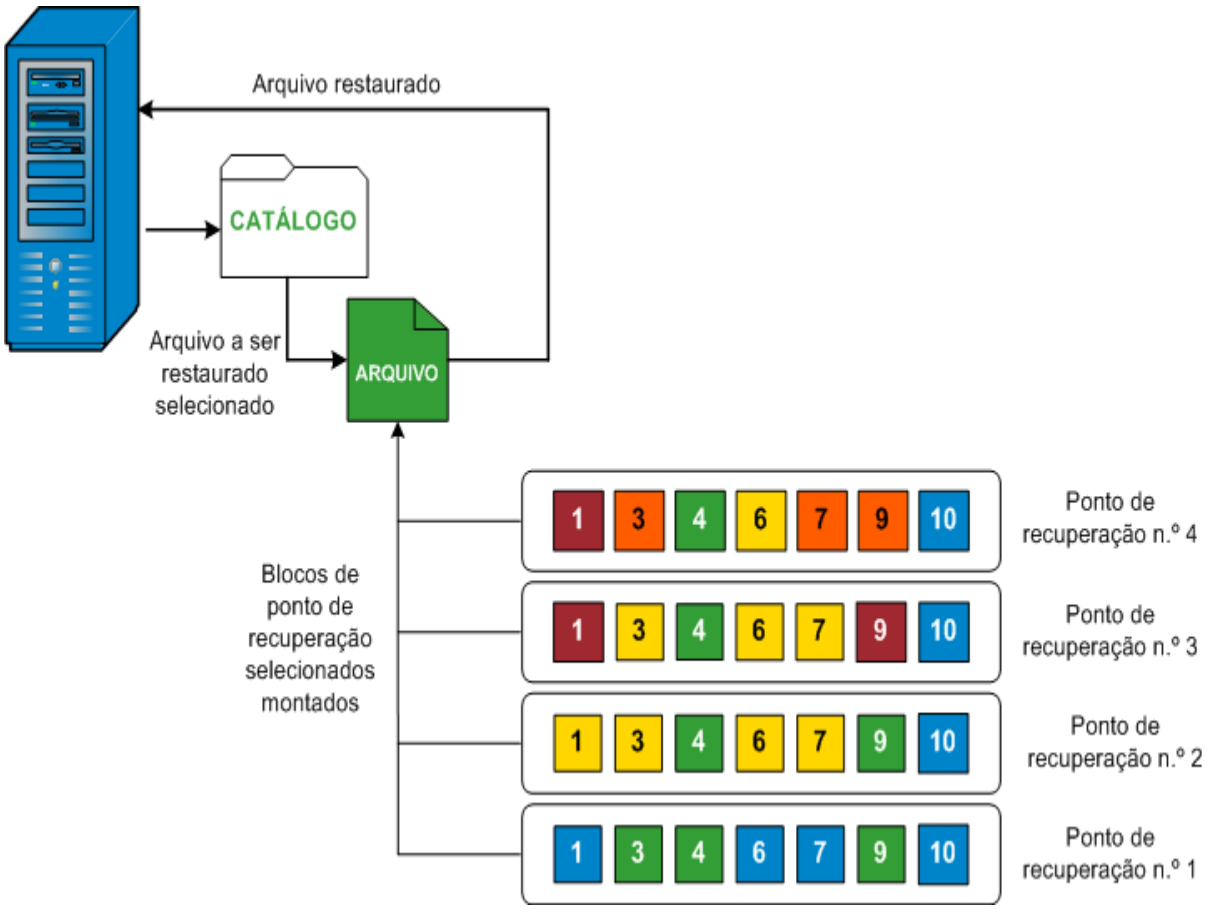
  "Os arquivos do sistema foram ignorados. Se necessário, é possível usar a opção Recuperação bare metal (BMR) para restaurá-los."

Como a restauração em nível de arquivo funciona

Durante um backup em nível de bloco, cada arquivo de backup é composto de um conjunto de blocos que definem aquele arquivo específico. Um arquivo de catálogo é criado contendo uma lista dos arquivos de backup, juntamente com os blocos individuais que foram usados para cada arquivo e os pontos de recuperação disponíveis para esses arquivos. Se precisar restaurar um arquivo específico, é possível pesquisar o backup e selecionar o arquivo que deseja restaurar e o ponto de recuperação de onde deseja restaurar. O Arcserve UDP coleta a versão dos blocos que foram usados para o ponto de recuperação do arquivo especificado, monta novamente o arquivo e o restaura.

Observação: também é possível executar uma restauração sem um arquivo de catálogo de um ponto de recuperação do backup sem catálogo.

O diagrama de fluxo a seguir mostra o processo de como o Arcserve UDP restaura um arquivo específico:



Arquivos ignorados durante a restauração

Durante a execução de uma restauração pelo agente do Arcserve UDP (Windows), alguns arquivos podem ser ignorados propositalmente.

Os arquivos e as pastas na tabela a seguir são ignorados durante uma restauração se as duas condições a seguir existirem:

- Os arquivos são ignorados quando tais arquivos existirem antes da restauração e a opção de conflito for "Ignorar arquivos existentes".
- As pastas e os arquivos listados na tabela a seguir são ignorados porque são um componente importante para o Windows ou o agente do Arcserve UDP (Windows).

Sistema operacional	Pasta ou local	Nome do arquivo ou pasta	Observações
Todos	Pasta raiz de cada volume	CAVolTrc.dat	Usado pelo driver de rastreamento do Arcserve UDP.
		cavoltrcsnapshot.dat	
		Informações de volume do sistema*	Usado para salvar arquivos/pastas por um sistema Windows, por exemplo, arquivos de cópia de sombra de volume.
		RECYCLER*	Usado apenas em partições NTFS. Contém uma lixeira para cada usuário que efetua logon no computador, classificadas por seu SID (Security Identifier – Identificador de Segurança).
		$Recycle.Bin*	Ao excluir um arquivo no Windows NT Explorer ou Meu computador, o arquivo é armazenado na Lixeira até que você a esvazie ou restaure o arquivo.
	Qualquer pasta contém arquivos de imagem	Thumbs.db	Armazena imagens em miniatura para o modo de exibição de miniatura do Windows Explorer.
	Pasta raiz do volume	PageFile.Sys	Arquivo de troca de memória virtual do Windows.
		Hiberfil.sys	Arquivo Hibernate usado para salvar os dados do sistema quando o computador entra no modo de hibernação.

As pastas e os arquivos a seguir são ignorados apenas quando você restaura no local original ou alternativo:

Sistema operacional	Pasta ou local	Nome do arquivo ou pasta	Observação
Todos	Pasta especificada no registro de valor em: HKLM\Software\Microsoft\Windows NT\CurrentVersion\WinLogon\SfcDllCache	Todos os arquivos/pastas (de maneira recursiva)	A pasta contém um arquivo DLL em cache que é usado para o SFC (System File Checker – Verificador de Arquivos do Sistema) e o conteúdo do diretório de cache da DLL do sistema é recriado usando SFC.
	%SystemRoot%\SYSTEM32\dllCache		
	Pasta raiz do quorum_device	MSCS*	Usado para o Microsoft Cluster Server.

	%SystemRoot%\SYSTEM32\	perf?00?.dat	Dados de desempenho usados pelo contador de desempenho do Windows.

		perf?00?.bak	
		CATROOT*	Usado para Proteção de arquivos do Windows (WFP) registra as assinaturas digitais das instalações do sistema operacional (como EXE, DLL, SYS, OCX e assim por diante) para protegê-las contra exclusão ou de substituição por versões mais antigas.
	%SystemRoot%\inetsrv\	metabase.bin	O arquivo binário de metabase de versões do IIS anteriores ao 6.0.
	Arquivo ou pasta especificada no valor diferente de "Armazenamento comum do SIS" em HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup	Todos os arquivos/pastas (de maneira recursiva)	Arquivos e pastas não devem ser copiados para backup e restaurados. Para obter mais informações, consulte o link.
XP	Volume do sistema	NTLDR	O principal

W2003			carregador de inicialização.
		BOOT.INI	Contém a configuração de inicialização (se a configuração estiver ausente, como padrão, o NTLDR usará \Windows na primeira partição do primeiro disco rígido).
		NTDETECT.COM	Obrigatório para inicializar um sistema operacional com base em NT. Detecta informações de hardware básicas necessárias para uma inicialização bem-sucedida.
Vista e posterior	Pasta raiz do volume do sistema	boot*	Pasta de inicialização para Windows.
		bootmgr	Arquivo do gerenciador de inicialização do

			Windows.
		EFI\Microsoft\Boot*	Usado para inicialização de EFI.
	%SystemRoot%\SYSTEM32\	LogFiles\WMI\RTBackup*	Armazena os arquivos de rastreamento de ETW (extension .etl) para as sessões de rastreamento de eventos em tempo real.
		config\RegBack*	Backup da tabela do registro atual.
Win8 e posterior	Volume do sistema	swapfile.sys	Arquivo do controlador de sistema, normalmente cerca de 256 MB. Ele é usado pelos aplicativos do Metro style que não podem se encaixar nas características de paginação tradicional (como padrões de uso, crescimento, reserva de

			espaço) do pagefile.sys.
		BOOTNXT	Usado para inicializar a partir do sistema operacional, que não seja o Windows 8. Criado ao ativar as opções de inicialização e atualizado pelo Windows.

O Log de atividades fornece as seguintes informações:

- Informações de data e hora: arquivos de sistema jobxxxx ignorados. Você pode usar a BMR (Recuperação Bare Metal) para restaurá-los.
- Informações de data e hora: arquivos ou diretórios de sistema jobxxxx ignorados. Arquivos ou diretórios ignorados estão disponíveis em: C:\Arquivos de programas\Arcserve\Unified Data Protection\Engine\Logs\Restore-<YYYYMMDD>-<hhmmss>-<Process ID>-<Job ID>.log.

Especifique as informações do ponto de recuperação para restauração

O Arcserve UDP fornece uma opção para restaurar os dados a partir de um ponto de recuperação. A meta de executar uma tarefa de restauração com êxito é identificar rapidamente os dados necessários e recuperá-los do local de backup adequado. Cada tarefa de restauração requer uma origem e um destino.

O processo envolvido na restauração de um ponto de recuperação é como se segue:

1. Especifique o ponto de recuperação e o conteúdo para restauração
2. Definir as opções de restauração

Especifique o ponto de recuperação e o conteúdo para restauração

Esta seção fornece informações sobre como especificar o ponto de recuperação e o conteúdo a ser restaurado.

Siga estas etapas:

1. Acesse a caixa de diálogo de seleção de método de restauração de uma das seguintes maneiras:

   No console do Arcserve UDP:

   a. Efetue logon no Console do Arcserve UDP.

   b. Navegue até **recursos** > **Nó** > **Todos os nós**.

      Todos os nós do adicionados são exibidos no painel central.

   c. Clique com o botão direito do mouse no nó e clique em **Restaurar**.

      Você é conectado automaticamente ao console do nó do agente e a caixa de diálogo Restaurar é aberta.

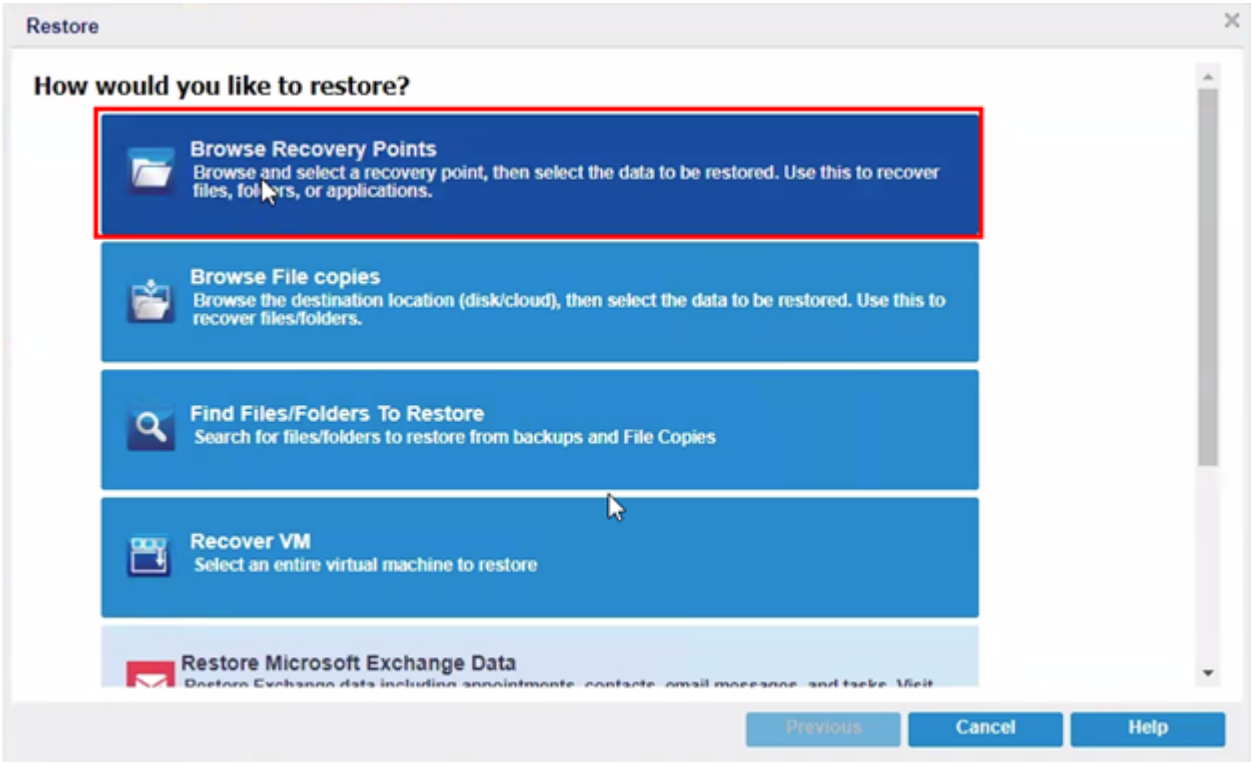
   No agente do Arcserve UDP (Windows):

   a. Efetue logon no Agente do Arcserve UDP (Windows).

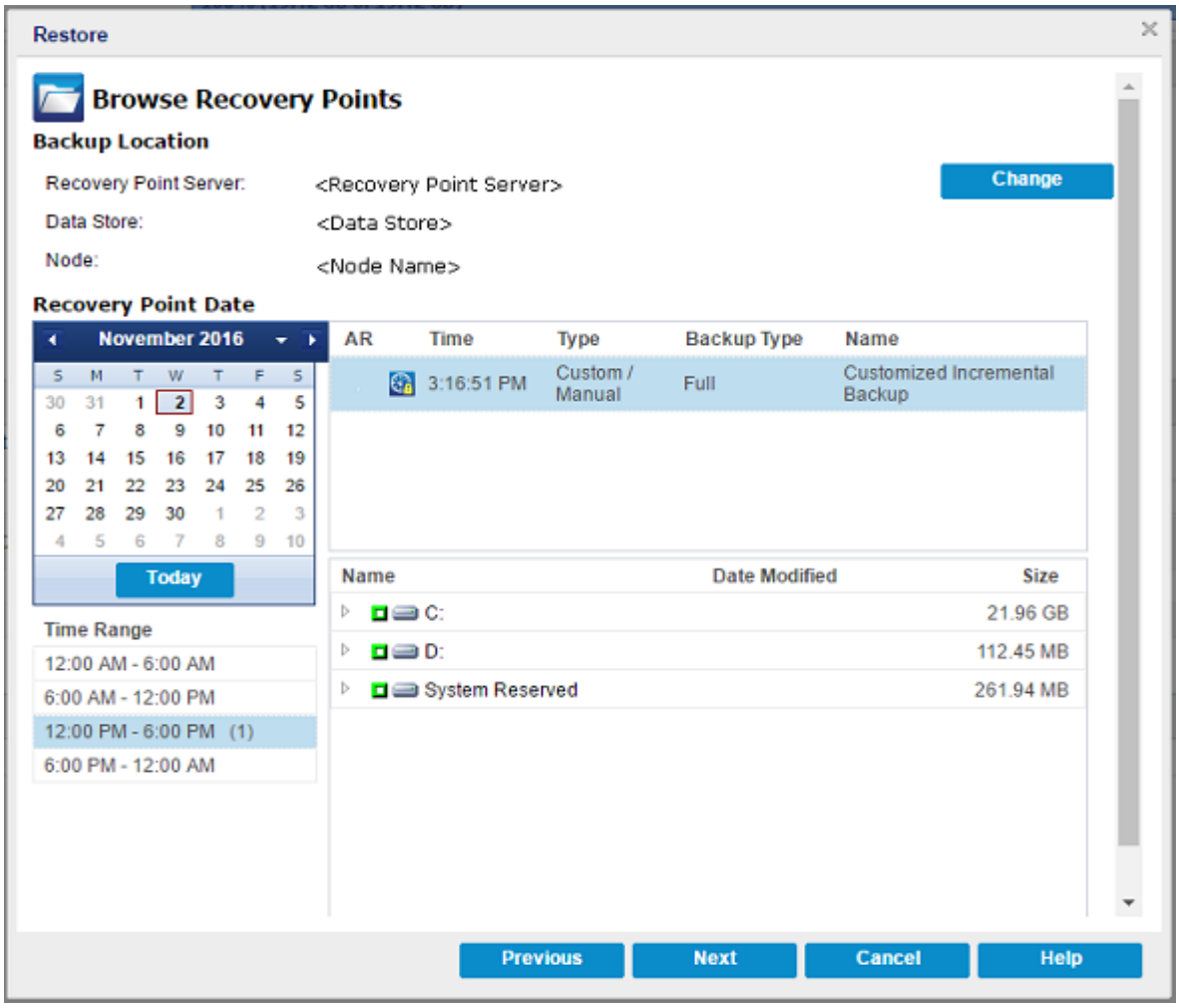
   b. Na página inicial, selecione **Restaurar**.

      A caixa de diálogo Restaurar é exibida.

2. Na caixa de diálogo Restaurar, clique na opção **Procurar os pontos de recuperação**.



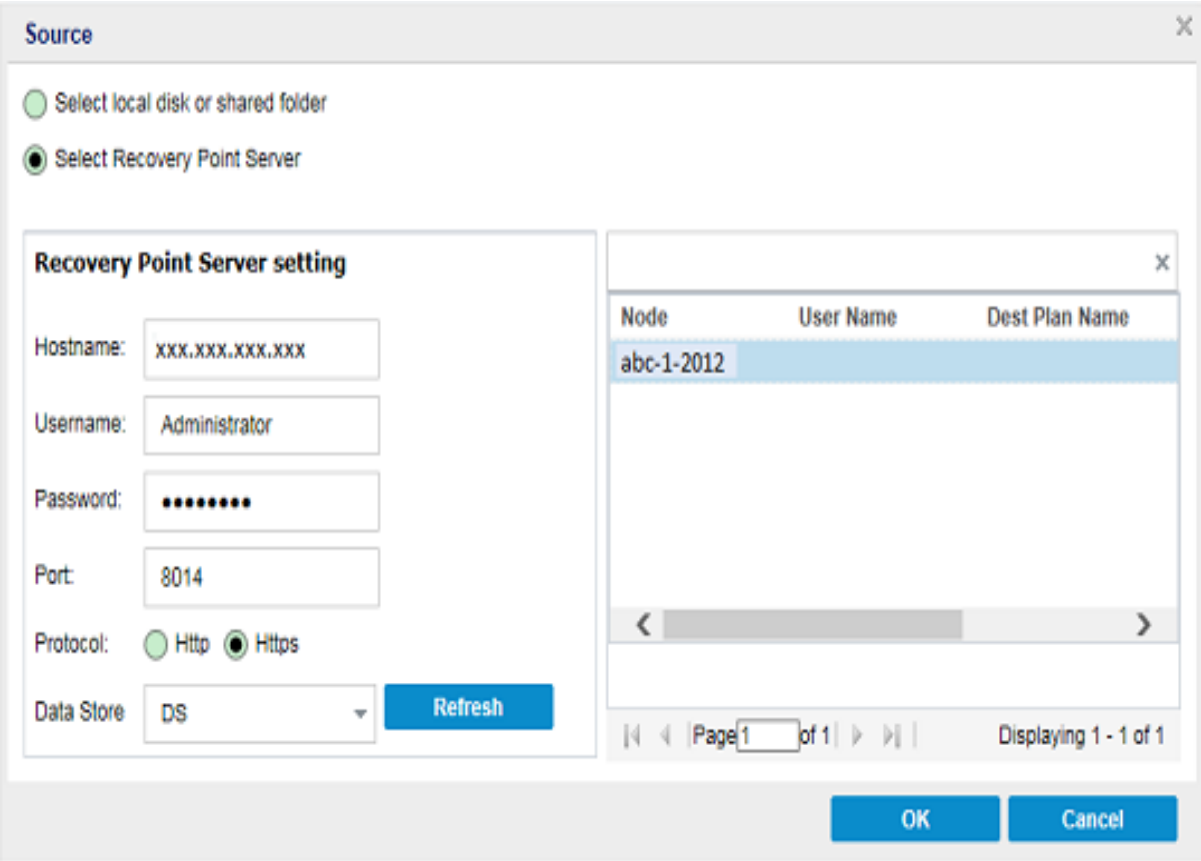
3. Na página Procurar os pontos de recuperação, faça o seguinte:



a. Para atualizar o local do backup, clique em **Alterar**.

   A caixa de diálogo Origem é exibida.

b. Na caixa de diálogo Origem, selecione um dos seguintes locais de backup e clique em **OK**:



Selecionar o disco local ou uma pasta compartilhada

1. Especifique ou procure o local onde as suas imagens de backup estão armazenadas e selecione o backup de origem adequado.
2. Para verificar a conexão com o local especificado, clique no botão de seta verde. Se necessário, forneça o nome de usuário e a senha para acessar esse local de origem.

   A caixa de diálogo Selecionar o local do backup é exibida.
3. Selecione a pasta onde estão armazenados os pontos de recuperação e clique em **OK**.

   A caixa de diálogo Selecione o local do backup será fechada, e você poderá ver o local do backup na caixa de diálogo Origem.

   Os pontos de recuperação são listados na caixa de diálogo Procurar pontos de recuperação.

Selecionar servidor de ponto de recuperação

1. Especifique os detalhes da configuração do servidor de ponto de recuperação e clique em **Atualizar**.

Todos os agentes estão listados na coluna Agente de proteção de dados na caixa de diálogo Origem.

2. Selecione o agente na lista exibida.

   Os pontos de recuperação são listados na caixa de diálogo Procurar pontos de recuperação.

c. Selecione a data no calendário para a imagem de backup para restaurar.

   Todas as datas que contém pontos de recuperação para a origem do backup especificado são realçadas em verde.

   Os pontos de recuperação correspondentes a essa data são exibidos, juntamente com a hora do backup, o tipo de backup que foi executado (completo, incremental ou de verificação) e o nome do backup.

d. Selecione um ponto de recuperação para restaurar.

   O conteúdo do backup (incluindo aplicativos) para o ponto de recuperação selecionado é exibida.

   Observação: um ícone de relógio com um símbolo de cadeado indica que o ponto de recuperação contém informações criptografadas e que pode ser necessária uma senha para restaurar.

e. Selecione o conteúdo para restaurar.

   - Para uma restauração de nível de volume, pode-se especificar a restauração do volume inteiro ou de arquivos/pastas selecionados no volume.
   - Para uma restauração de nível do aplicativo, pode-se especificar a restauração do aplicativo inteiro ou de itens selecionados no aplicativo, como componentes, bancos de dados, instâncias e assim por diante.

4. Clique em **Avançar**.

   A caixa de diálogo Opções de restauração é exibida.

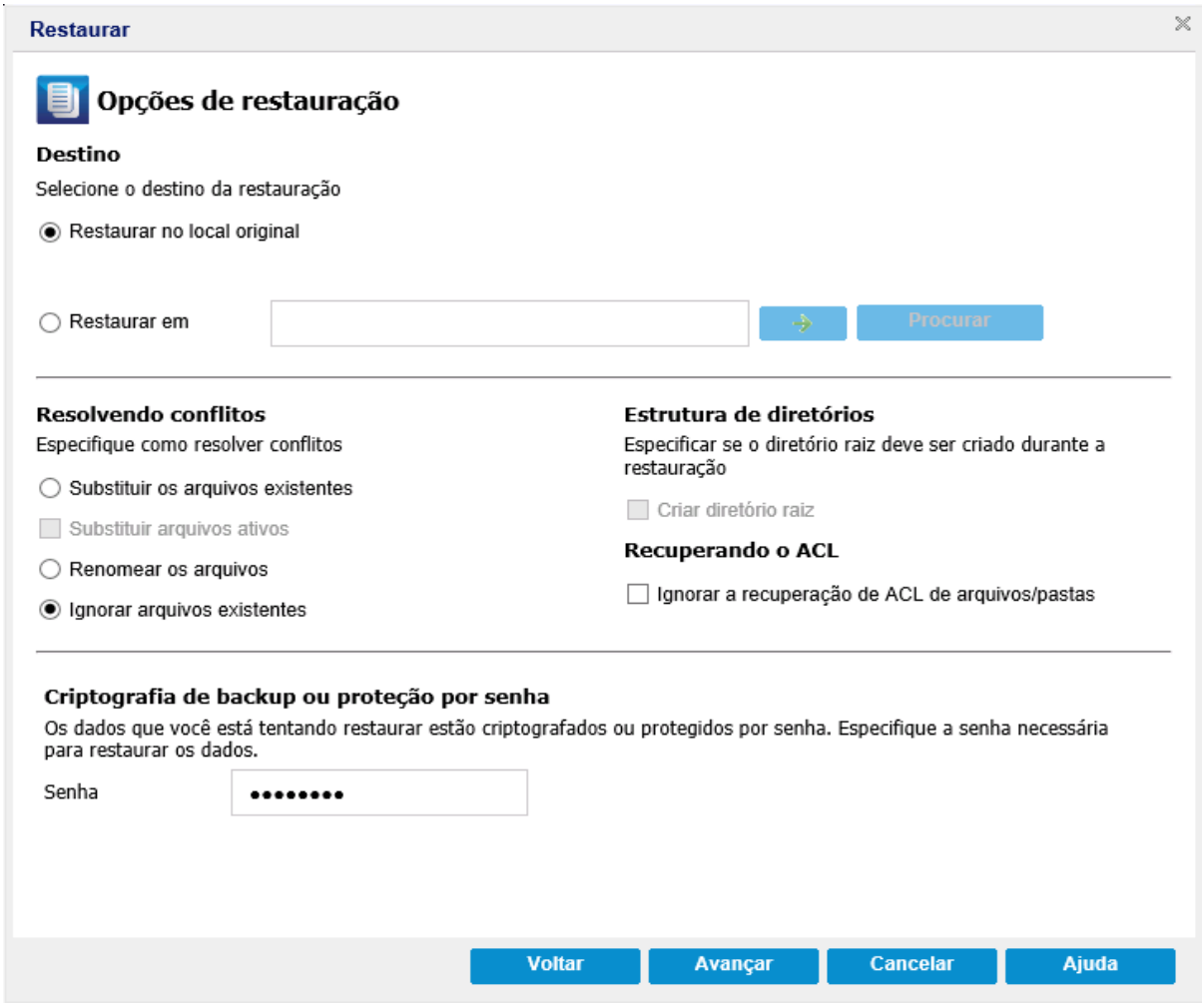
   O ponto de recuperação e o conteúdo para restauração é especificado.

Definir as opções de restauração

Depois de especificar um ponto de recuperação e conteúdo para restauração, defina as opções de cópia do ponto de recuperação selecionado. Esta seção explica como definir as opções de restauração para o ponto de recuperação selecionado.

Siga estas etapas:

1. Na caixa de diálogo Opções de restauração, selecione o destino da restauração.



As opções de destino disponíveis são:

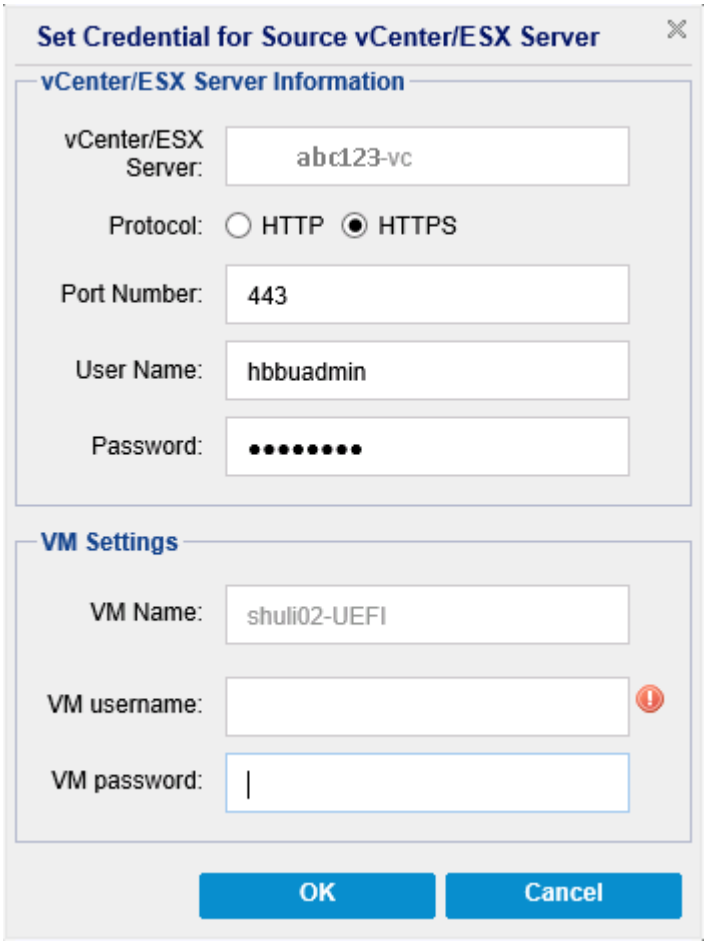
Restaurar no local original

Restaura no local original a partir do qual a imagem de backup foi capturada.

Observação: se você tiver feito backup do ponto de recuperação usando o backup sem agente com base em host, a opção Restaurar no local original restaurará o arquivo na máquina virtual. Nesse caso, uma caixa de diálogo abre.

Você pode digitar as credenciais do hipervisor e do sistema operacional da máquina virtual.

Para a VM do VMware:



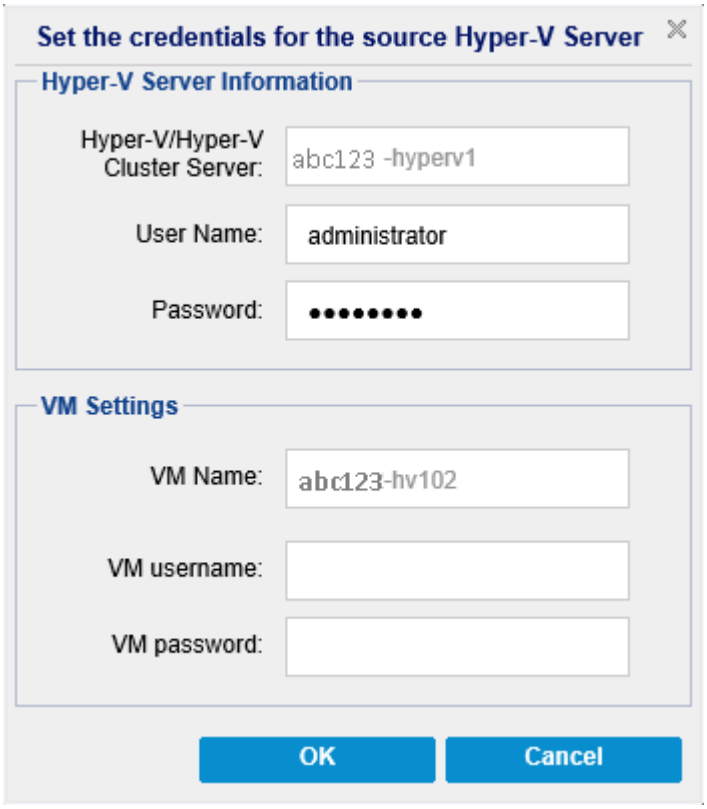
Observação: para criar ou gravar arquivos na VM, considere os seguintes requisitos de configuração e permissão de conta da máquina virtual:

- o VMware Tools está instalado e em execução.
- o Firewall deve permitir que o compartilhamento de arquivo e de impressora.
- A conta é o administrador local internos, o administrador de domínio interno ou conta de domínio que é integrante do grupo de administradores locais. Se outras contas forem usadas, faça o seguinte:
  - Desative o acesso remoto ao UAC. Para desativar o acesso remoto de UAC, consulte Importar máquina virtual usando a conta administrativa adicional.

- Desative o UAC na Diretiva de Segurança Local, desativando a configuração Executar todos os administradores no modo de aprovação de administrador em secpol.msc -> Diretivas Locais -> Opções de Segurança. (Secpol.msc é editor da diretiva de segurança da Microsoft).

  Importante: não tente desativar o UAC na caixa de diálogo Configurações de controle de conta do usuário, que é aberta no painel de controle.

Para a VM do Hyper-V:



Observação: para criar ou gravar arquivos na VM, considere os seguintes requisitos de configuração e permissão de conta da máquina virtual:

- os serviços de integração do Hyper-V estão instalados e em execução.
- o Firewall deve permitir que o compartilhamento de arquivo e de impressora.
- A conta é o administrador local internos, o administrador de domínio interno ou conta de domínio que é integrante do grupo de administradores locais. Se outras contas forem usadas, desative o

acesso remoto do UAC. Para desativar o acesso remoto de UAC, consulte Importar máquina virtual usando a conta administrativa adicional.

- Se o sistema operacional convidado da máquina virtual for a versão de cliente do Windows (por exemplo, o Windows 10), será necessário configurar manualmente o firewall para permitir a WMI (Windows Management Instrumentation - Instrumentação de Gerenciamento do Windows).

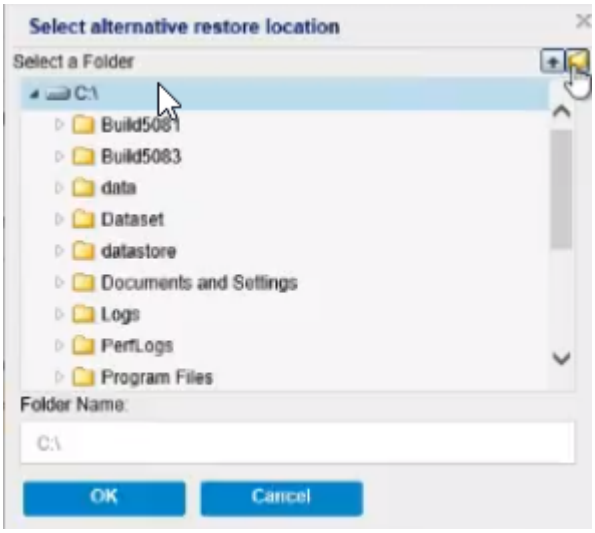
Restaurar para

Restaura no local especificado. Para restaurar para o local original, faça o seguinte:

- Para fornecer o destino, clique em **Procurar**.

  A caixa de diálogo Selecionar local de restauração alternativo é exibida.

- Selecione a pasta existente ou crie uma nova pasta, conforme necessário, e clique em **OK**.



- Para verificar a conexão com o local especificado, clique no botão de seta verde. Se necessário, digite o nome de usuário e a senha para acessar esse local.

2. (Opcional) Para ativar a comunicação entre o agente do Windows e o servidor de ponto de recuperação, marque a caixa de seleção **Usar a rede selecionada para tráfego de restauração** e selecione a rede na lista suspensa.

   Observações:

   - Se a rede de backup selecionada não estiver acessível e, para continuar a tarefa de backup com a rede disponível ou com a rede padrão, clique na

caixa de seleção **Continuar a executar a tarefa, mesmo que não seja possível estabelecer conexão com a rede de backup selecionada**.

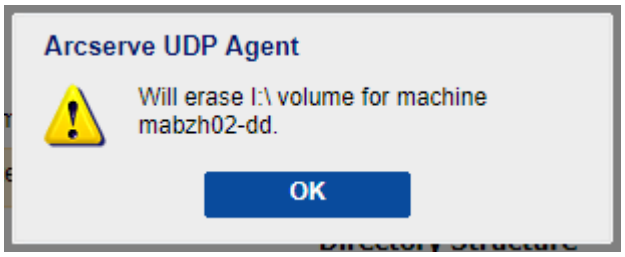
- Para definir a restrição no SMB Multichannel para que as transferências de dados sejam realizadas somente pela rede selecionada, marque a caixa de seleção **Usar Ethernet dedicada se o computador atual permitir o SMB multicanal**.

  Essa opção não está disponível por padrão. Para ativar essa opção, crie o registro da sequência de caracteres *UseDedicatedEthernet* no seguinte caminho e, em seguida, defina o valor do registro como 1:

  SOFTWARE\Arcserve\Unified Data Protection\Engine

  - Ao executar uma tarefa de restauração na página Nós, crie uma chave do Registro no proxy de backup.
  - Ao executar uma tarefa de restauração do agente normal usando a sessão de backup RPS, crie uma chave do Registro no agente normal.

3. Para melhorar a taxa de transferência ao restaurar um volume grande com muitos arquivos pequenos, selecione um volume e, em Restaurar nível de bloco, marque a caixa de seleção **Executar restauração de bloco**. Outras opções são desativadas, e uma notificação é exibida. Para continuar com a restauração de nível de bloco clique em **OK**.



Observação: os dados são restaurados na máquina atual que possui o agente do UDP, e o volume de destino é substituído. O volume de destino não está acessível durante a tarefa de restauração.

4. Especifique a opção Resolvendo conflitos que o Arcserve UDP executará se forem encontrados conflitos durante o processo de restauração.

   As opções disponíveis são:

   Substituir arquivos existentes

   Sobrescreve (substitui) qualquer arquivo existente que está localizado no destino da restauração. Todos os objetos serão restaurados dos arquivos de backup, independentemente da presença atual deles no computador.

   Substituir os arquivos ativos

Substitui todos os arquivos ativos ao reinicializar. Se, durante a tentativa de restauração, o agente do Arcserve UDP (Windows) detectar que o arquivo existente está em uso ou sendo acessado, para evitar erros, ele não substituirá o arquivo imediatamente, só depois que o computador for reinicializado. (A restauração ocorrerá imediatamente, mas a substituição de arquivos ativos é feita durante a próxima reinicialização).

Essa opção só estará disponível se você selecionar a opção **Substituir os arquivos existentes**.

Observação: se essa opção não estiver selecionada, qualquer arquivo ativo será ignorado na restauração.

Renomear arquivos

Cria um novo arquivo se o nome de arquivo já existir. A seleção desta opção copia o arquivo de origem no destino com o mesmo nome de arquivo, mas com uma extensão diferente. Os dados serão restaurados no novo arquivo.

Ignorar arquivos existentes

Ignora e não substitui (sobrescreve) os arquivos localizados no destino da restauração. Apenas os objetos inexistentes em seu computador no momento serão restaurados dos arquivos de backup.

Padrão: Ignorar arquivos existentes.

5. Para Estrutura de diretórios, se desejar criar um diretório raiz durante a restauração, marque a caixa de seleção **Criar diretório raiz**.

   A caixa de seleção **Criar o diretório raiz** especifica que se uma estrutura de diretórios raiz existir na imagem de backup capturada, o Arcserve UDP recriará a mesma estrutura de diretórios raiz no caminho de destino da restauração.

   Se essa opção não for selecionada, o arquivo ou a pasta será restaurado diretamente para a pasta de destino.

   Por exemplo, se durante o backup você capturou os arquivos "C:\Folder1\SubFolder2\A.txt" e "C:\Folder1\SubFolder2\B.txt" e, durante a restauração, você especificou o destino da restauração como "D:\Restore".

   - Se você optar por restaurar os arquivos "A.txt" e "B.txt" individualmente, o destino dos arquivos restaurados será "D:\Restore\A.txt" e "D:\Restore\B.txt" (o diretório raiz acima do nível de arquivo especificado não será recriado).
   - Se você optar por restaurar a partir do nível da "Subpasta2", o destino dos arquivos restaurados será "D:\Restore\Subpasta2\A.txt" e "D:\Restore\Subpasta2\B.txt" (o diretório acima do nível de pasta especificado não será recriado).

Se esta opção for selecionada, todo o caminho do diretório raiz para os arquivos/pastas (incluindo o nome de volume) será recriado para a pasta de destino. Se os arquivos/pastas a serem restaurados tiverem o mesmo nome de volume, o caminho do diretório raiz de destino não incluirá esse nome de volume. No entanto, se os arquivos/pastas a serem restaurados forem de nomes de volume diferentes, o caminho do diretório raiz do destino incluirá o nome do volume.

Por exemplo, se durante o backup você capturou os arquivos "C:\Folder1\SubFolder2\A.txt", "C:\Folder1\SubFolder2\B.txt", e também E:\Folder3\SubFolder4\C.txt" e, durante a restauração, especificou o destino de restauração como "D:\Restore".

- Se você optar por restaurar apenas o arquivo "A.txt", o destino do arquivo restaurado será "D:\Restore\Pasta1\Subpasta2\A.txt" (o diretório raiz inteiro, sem o nome do volume, será recriado).
- Se você optar por restaurar tanto o arquivo "A.txt" como o "C.txt", o destino dos arquivos restaurados será "D:\Restore\C\Pasta1\Subpasta2\A.txt" e "D:\Restore\E\Pasta3\Subpasta4\C.txt" (o diretório raiz inteiro, com o nome do volume, será recriado).

6. Para a recuperação de ACL, para ignorar a permissão original para os arquivos/pastas restaurados, marque a caixa de seleção **Ignorar a recuperação de ACL de arquivos/pastas**. Selecionar essa opção permite, em vez disso, herdar as permissões da pasta de destino. Se a opção não for selecionada, as permissões originais serão mantidas.

7. Para **Criptografia de backup ou proteção por senha**, se necessário, especifique a senha de criptografia de backup quando os dados que você está tentando restaurar estiverem criptografados.

   A senha não será necessária se você estiver tentando fazer a restauração a partir do mesmo computador do agente do Arcserve UDP (Windows) em que o backup criptografado foi executado. No entanto, se você estiver tentando fazer a restauração a partir de um computador diferente do Agente do Arcserve UDP (Windows), a senha será necessária.

   Observação: um ícone de relógio com um símbolo de cadeado indica que o ponto de recuperação contém informações criptografadas e que pode ser necessária uma senha para restaurar.

8. Clique em **Avançar**.

   A página Resumo da restauração é exibida.

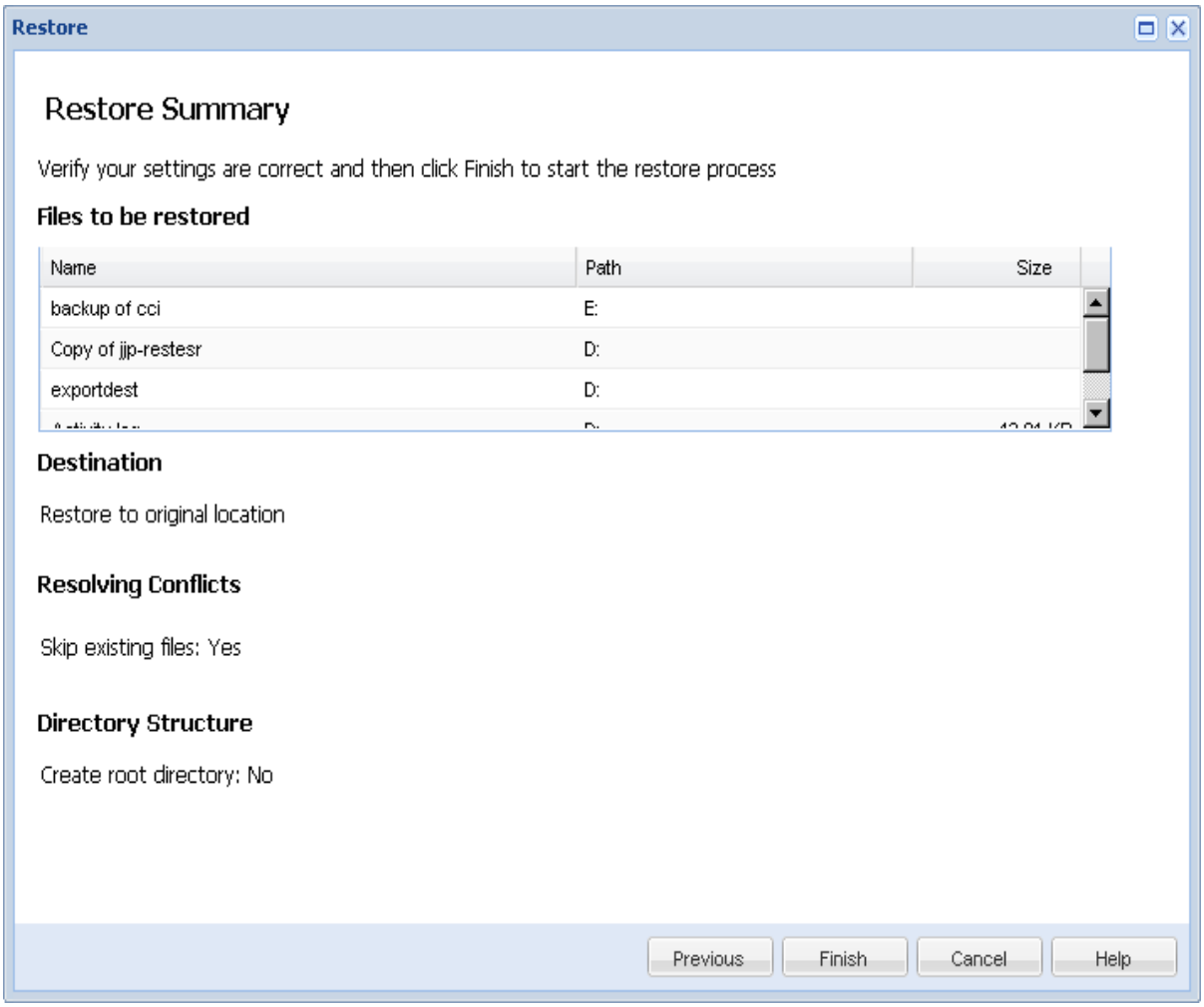
   As opções de restauração são definidas para restaurar a partir de um ponto de recuperação.

Restaure o conteúdo do ponto de recuperação

Após definir as opções de restauração, verifique se suas configurações estão corretas e confirme o processo de restauração. A página Resumo da restauração o auxilia a revisar todas as opções de restauração definidas e modificá-las se necessário.

Siga estas etapas:

1. Na caixa de diálogo Resumo da restauração, examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.



2. Siga um destes procedimentos:
   - Se as informações do resumo não estiverem corretas, clique em **Anterior** e volte à caixa de diálogo em questão para alterar a configuração incorreta.

- Se as informações de resumo estiverem corretas, clique em **Concluir** para iniciar o processo de restauração.

O ponto de recuperação do conteúdo é restaurado.

Verificar se o conteúdo foi restaurado

Depois que o processo de restauração estiver concluído, verifique se o conteúdo foi restaurado para o destino especificado.

Siga estas etapas:

1. No console do Arcserve UDP, navegue até **tarefas** > **Tarefas concluídas com êxito**.

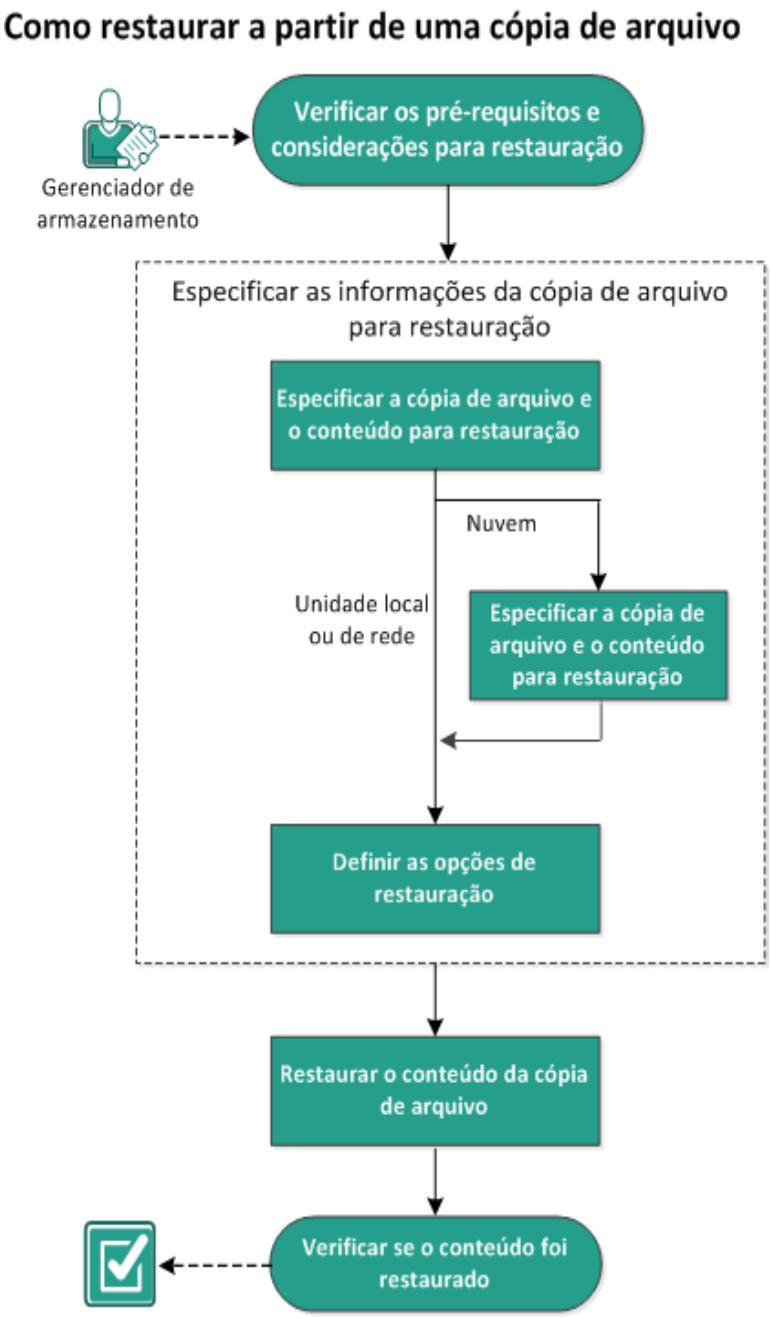
   A lista de tarefas de backup concluídas é exibida no painel central.
2. Clique na tarefa de replicação inversa concluída. O painel direito é atualizado.
3. Em Detalhes da tarefa, clique no hiperlink **Exibir logs**.
4. Verifique o conteúdo para confirmar a tarefa de restauração.

   A restauração do conteúdo é verificada com êxito.

Como restaurar a partir de uma cópia de arquivo

Toda vez que o Arcserve UDP executa uma tarefa de cópia de arquivo com êxito, ele faz backup de todos os arquivos que foram alterados desde a última tarefa de cópia de arquivo com êxito. Este método de restauração permite procurar os dados copiados do arquivo e especificar exatamente qual arquivo deseja restaurar.

O diagrama seguinte ilustra o processo para restaurar a partir de uma cópia de arquivo:



Execute as tarefas a seguir para restaurar a partir de uma cópia de arquivo:

1. Verificar os pré-requisitos e as considerações para restauração
2. Especificar as informações de cópia de arquivo para restauração
    a. Especifique a cópia do arquivo e o conteúdo para restauração
        - Especificar configuração de nuvem para restauração
    b. Definir as opções de restauração
3. Restaurar o conteúdo do ponto de recuperação
4. Verificar se o conteúdo foi restaurado

Revisar os pré-requisitos e as considerações para restauração

Verifique se os pré-requisitos a seguir existem antes de executar uma restauração:

- Você tem pelo menos uma cópia de arquivo para restauração.
- Você tem um destino válido e acessível da cópia de arquivo do qual restaurar o conteúdo da cópia do arquivo.
- Você tem um local de destino válido e acessível para o qual restaurar o conteúdo da cópia do arquivo.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Revise as seguintes considerações de restauração:

- O Arcserve UDP permite que apenas uma tarefa de restauração seja executada ao mesmo tempo. Se você tentar iniciar manualmente uma tarefa de restauração, enquanto outra tarefa de restauração estiver em execução, uma mensagem de alerta será exibida informando sobre a outra tarefa está em execução e solicita que você tente novamente mais tarde.
- Se a restauração para um destino remoto e se todas as letras de unidade (A - Z) estiverem ocupadas, a restauração de dados para um caminho remoto não serão bem-sucedidas. O Agente do Arcserve UDP (Windows) precisa usar uma letra de unidade para montar o caminho do destino remoto.
- Aprimore a cópia do arquivo para otimizar o desempenho:
  - A cópia de arquivo pode enviar vários fragmentos simultaneamente para o destino (ArchMultChunkIO)
  - A cópia de arquivo pode copiar mais de um arquivo por vez (ThreadsForArchive).
  - A restauração a partir da cópia de arquivo pode fazer download de mais de um arquivo por vez (ThreadsForRestore).
  - A sincronização de catálogo usa vários segmentos (ThreadForCatalogSync).

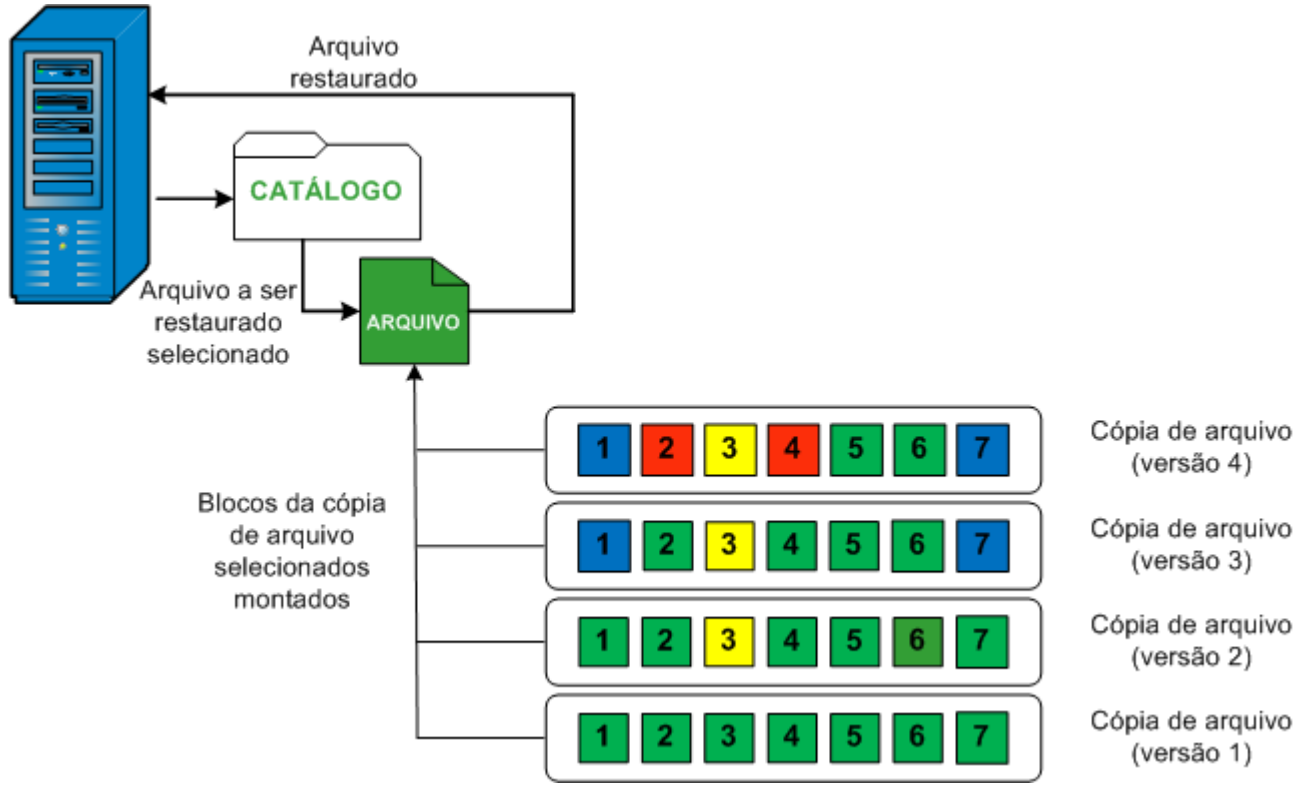
  É possível alterar os valores do registro de cópia de arquivo padrão modificando o valor DWORD. Para obter mais informações, consulte Configurar definições da cópia de arquivo para otimizar o desempenho na *ajuda online do Agente para Windows*.

- (Opcional) Compreenda como funciona o processo de restauração. Para obter mais informações, consulte Como a restauração em nível de arquivo funciona.

Como a restauração em nível de arquivo funciona

Durante uma Cópia de arquivo, cada arquivo de backup é composto de um conjunto de blocos que definem o arquivo específico. Um arquivo de catálogo é criado para cada versão do arquivo com backup, juntamente com os blocos individuais que foram usados para esses arquivos. Se precisar restaurar um arquivo específico, é possível pesquisar e selecionar o arquivo que deseja restaurar e as versões das cópias do arquivo de onde deseja restaurar. Posteriormente, o Arcserve UDP coleta a versão dos blocos de dados que foram usados para a cópia do arquivo especificado, que monta novamente o arquivo e o restaura.

O diagrama de fluxo a seguir mostra o processo de como o Arcserve UDP restaura um arquivo específico:



Especificar as informações de cópia de arquivo para restauração

O Arcserve UDP oferece a opção de restaurar os dados a partir de uma cópia de arquivo. O objetivo de executar uma tarefa de restauração com êxito é identificar rapidamente os dados necessários e recuperá-los do local de backup adequado. Cada tarefa de restauração requer uma origem e um destino.

O processo envolvido na restauração de uma cópia de arquivo é como se segue:

- Especificar a cópia do arquivo e o conteúdo para restauração
- Definir as opções de restauração

Especificar a cópia do arquivo e o conteúdo para restauração

Use a opção **Procurar cópias de arquivo** para restaurar a partir de uma cópia do arquivo. Este método de restauração permite procurar os dados copiados do arquivo e especificar exatamente qual arquivo deseja restaurar.

Siga estas etapas:

1. Acesse a caixa de diálogo de seleção de método de restauração de uma das seguintes maneiras:

   No Arcserve UDP:

   a. Efetue logon no Arcserve UDP.

   b. Clique na guia **Recursos**.

   c. Selecione **Todos os nós** no painel esquerdo.

      Todos os nós adicionados são exibidos no painel central.

   d. No painel central, selecione o nó do e clique em **Ações**.

   e. Clique em **Restaurar** no menu suspenso **Ações**.

      A caixa de diálogo de seleção do método de restauração é exibida.

      Observação: você é automaticamente conectado ao nó do agente e a caixa de diálogo de seleção do método de restauração é exibida no nó do agente.

   No agente do Arcserve UDP (Windows):

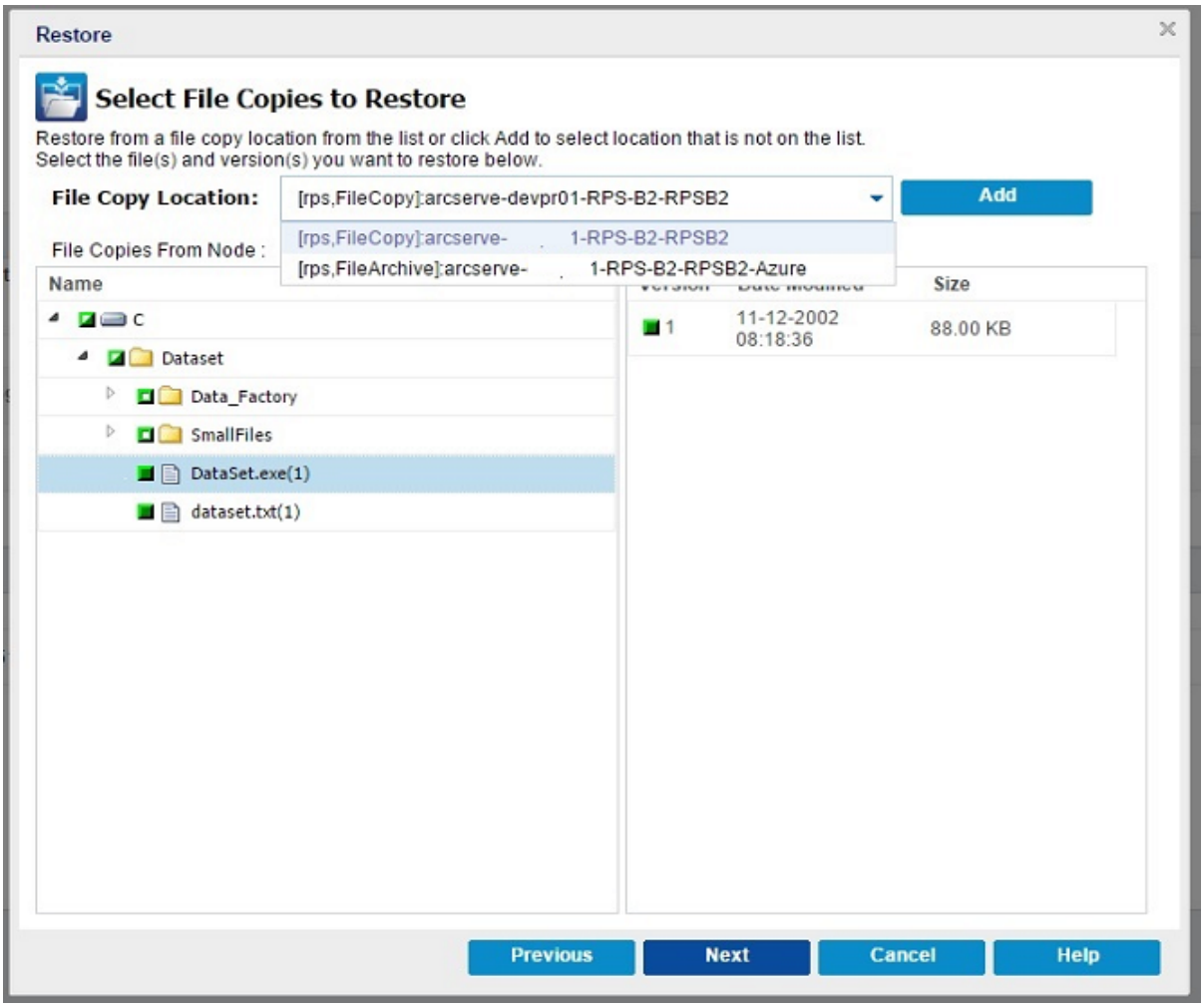
   a. Efetue logon no Agente do Arcserve UDP (Windows).

   b. Na página inicial, selecione **Restaurar**.

   A caixa de diálogo de seleção do método de restauração é exibida.

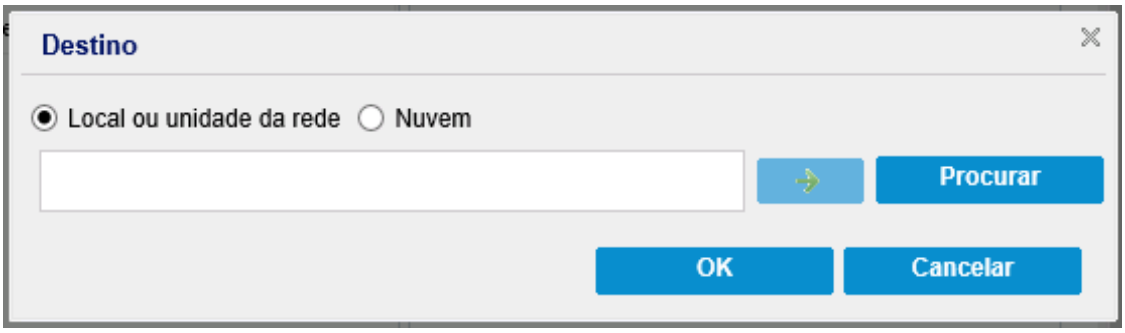
2. Clique na opção **Procurar cópias de arquivo**.

   A caixa de diálogo **Restaurar** é exibida. O destino em exibição no momento, no campo **Restaurar a partir de**, é o destino padrão configurado em **Cópia de arquivo**.



3. Se necessário, é possível clicar em **Adicionar** para procurar um local alternativo onde as imagens da cópia de arquivo estão armazenadas.

   A caixa de diálogo **Destino** é aberta exibindo as outras opções de destino disponíveis.



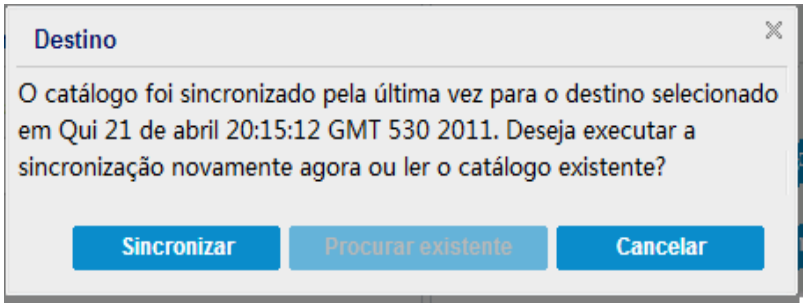
Local ou unidade da rede

A caixa de diálogo **Selecionar um local de backup** é exibida, permitindo procurar e selecionar um local alternativo ou o local da unidade de rede.

Nuvem

A caixa de diálogo **Configuração de nuvem** é exibida, permitindo acessar e selecionar um local de nuvem alternativo. Para obter mais informações sobre essa caixa de diálogo, consulte Especificar configuração de nuvem para restauração.

Independentemente de você ter selecionado a restauração na **Unidade local ou de rede** ou na **Nuvem**, ao alterar o destino para um local alternativo, uma caixa de diálogo pop-up será exibida perguntando se deseja executar uma nova sincronização do catálogo ou ler o catálogo existente.



- Se você estiver executando a sincronização do catálogo pela primeira vez, o botão **Procurar existente** estará desativado porque o catálogo de cópia de arquivo não existe localmente.
- Se a sincronização do catálogo já foi executada, a caixa de diálogo exibirá detalhes sobre a última vez o catálogo foi sincronizado no destino. Caso outras tarefas de cópia de arquivo tenham sido executadas após a hora exibida, talvez seu catálogo não esteja sincronizado. Você pode selecionar a opção **Sincronizar** para garantir que seu catálogo de cópia de arquivo contenha dados atualizados.

1. Clique em **Sincronizar** para fazer download do catálogo de cópia de arquivo do destino da cópia de arquivo especificado para o computador local para obter uma busca mais rápida.

2. Clique em **Procurar existente** para usar o catálogo de cópia de arquivo que está disponível localmente e para não o baixar/sincronizar novamente.

4. No painel à esquerda, especifique os dados da cópia de arquivo a serem restaurados. É possível selecionar pastas de cópia de arquivos ou arquivos a serem restaurados.

   Ao selecionar um arquivo individual a ser restaurado, todas as versões de cópia de arquivo de tal arquivo são exibidas no painel direito. Se várias versões estiverem disponíveis, é necessário selecionar qual versão da cópia de arquivo deseja restaurar.

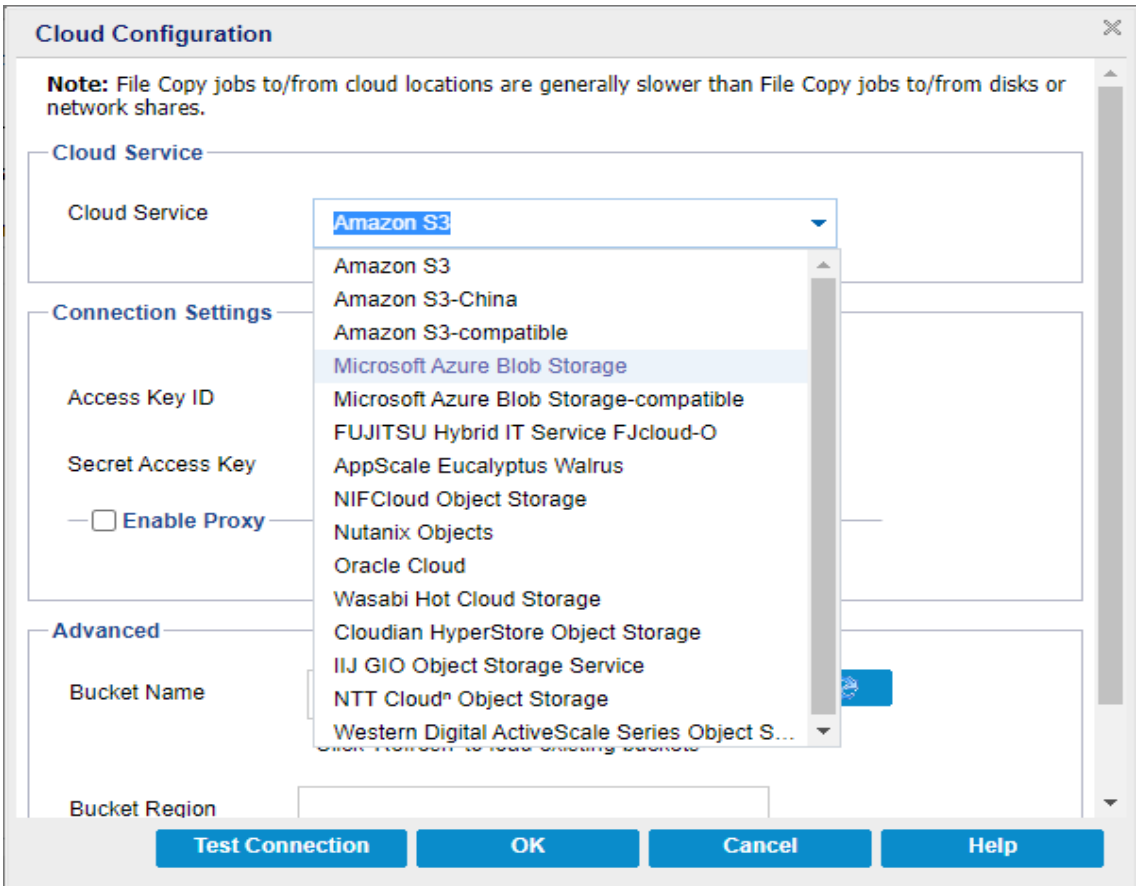
5. Depois de selecionar uma pasta do arquivo copiado ou versão do arquivo para restauração, clique em **Avançar**.

   A caixa de diálogo **Opções de restauração** é exibida.

   A **Cópia do arquivo e o Conteúdo para restauração** são especificados.

Especificar configuração de nuvem para restauração

Observação: o procedimento a seguir só se aplica se você está restaurando um arquivo/uma pasta a partir de um local na nuvem de cópia de arquivo ou de arquivo morto.



As opções disponíveis são Amazon S3, compatível com Amazon S3, Windows Azure, compatível com Windows Azure, FUJITSU Hybrid IT Service FJcloud-O e Eucalyptus-Walrus. (Amazon S3 é o fornecedor padrão).

Observação: se estiver usando o Eucalyptus-Walrus como seu fornecedor da nuvem de cópia de arquivo, não será possível copiar arquivos cujo tamanho de caminho total excede 170 caracteres.

As opções de configuração para cada fornecedor da nuvem são semelhantes (com algumas terminologias distintas), e nenhuma diferença é descrita.

1. A partir da opção **Procurar cópias de arquivo** ou **Localizar arquivos/pastas para restauração**, clique em **Adicionar**.

   A caixa de diálogo **Destino** será aberta.

2. Selecione **Nuvem** e clique em **Procurar**.

A caixa de diálogo **Configuração da nuvem** é aberta.

3. Digite os seguintes detalhes:

Nome do armazenamento

Especifica o nome do armazenamento na nuvem. Esse nome será adicionado ao console para identificar a conta da nuvem. Cada conta de nuvem deve ter um nome de armazenamento exclusivo.

Serviço de armazenamento

Selecione o serviço na lista suspensa. A opção de configuração varia de acordo com o serviço de armazenamento selecionado.

ID da chave de acesso/nome da conta/ID de consulta

Identifica o usuário que está solicitando acesso a este local.

Para esse campo, o Amazon S3 usa a ID da chave de acesso. O Windows Azure e FUJITSU Hybrid IT Service FJcloud-O usam o nome da conta, e o Eucalyptus-Walrus usa a ID da consulta.

Chave de acesso secreta/chave secreta

Uma vez que a chave de acesso não está criptografada, esta chave de acesso secreta será uma senha usada para verificar a autenticidade da solicitação para acessar este local.

Importante: esta chave de acesso secreta é fundamental para manter a segurança de suas contas. É necessário manter as chaves e as credenciais da conta em um local seguro. Não incorpore a chave de acesso secreta em uma página da web ou em outro código-fonte de acesso público e não a transmita em canais não seguros.

Para esse campo, o Amazon S3 usa a chave de acesso secreta. O Windows Azure, o FUJITSU Hybrid IT Service FJcloud-O e o Eucalyptus-Walrus usam a chave secreta.

Configurações de proxy

Especifica as configurações do servidor proxy. Selecione **Conectar usando um servidor proxy** para ativar essa opção. Caso selecione esta opção, será necessário incluir também o endereço IP (ou nome do computador) do servidor proxy e o número da porta correspondente, usado pelo servidor proxy em conexões com a internet. Pode-se também selecionar esta opção se o servidor proxy exigir autenticação. Será necessário fornecer as informações de autenticação correspondentes (Nome de domínio/nome de usuário e senha) para usar o servidor proxy.

Observação: o recurso Proxy não está disponível para Eucalyptus-Walrus.

Nome do compartimento de memória/Contêiner

Todos os arquivos e as pastas movidos ou copiados para o fornecedor da nuvem são armazenados e organizados nos compartimentos de memória (ou contêineres). Os compartimentos de memória são como um contêiner para os arquivos e são usados para agrupar e organizar objetos. Cada objeto armazenado no fornecedor da nuvem é colocado em um compartimento de memória.

Para esse campo, o Amazon S3 e Eucalyptus-Walrus usam o Nome do compartimento de memória. O Windows Azure e o FUJITSU Hybrid IT Service FJcloud-O usam o recipiente.

Observação: para o restante desta etapa, todas as referências a compartimentos de memória também podem ser aplicadas aos recipientes, contanto que seja especificado.

Região de compartimento de memória

Refere-se à região de compartimento de memória no Amazon e no FUJITSU Hybrid IT Service FJcloud-O.

Número do contrato

Refere-se ao número do contrato que o FUJITSU Hybrid IT Service FJcloud-O fornece.

ID do projeto

Refere-à ID do projeto que o FUJITSU Hybrid IT Service FJcloud-O gera.

Ativar a redução de armazenamento de dados redundantes

Para Amazon S3 apenas, esta opção permite ativar a RRS (Reduced Redundancy Storage). RRS é uma opção de armazenamento no Amazon S3 que ajuda você a reduzir o custo por meio do armazenamento de dados reproduzíveis não essenciais em níveis de redundância mais baixos do que aqueles do armazenamento padrão do Amazon S3s. As opções de armazenamento padrão e de redução de armazenamento de dados redundantes armazenam dados em vários recursos e dispositivos, mas com a RRS os dados são replicados menos vezes e o custo é menor. Deve-se esperar a mesma latência e taxa de transferência usando o armazenamento padrão ou RRS do Amazon S3. Por padrão, esta opção não está selecionada (o Amazon S3 usa a opção de armazenamento padrão).

4. Clique em **Testar conexão** para verificar a conexão com o local na nuvem especificado.
5. Clique em **OK**.

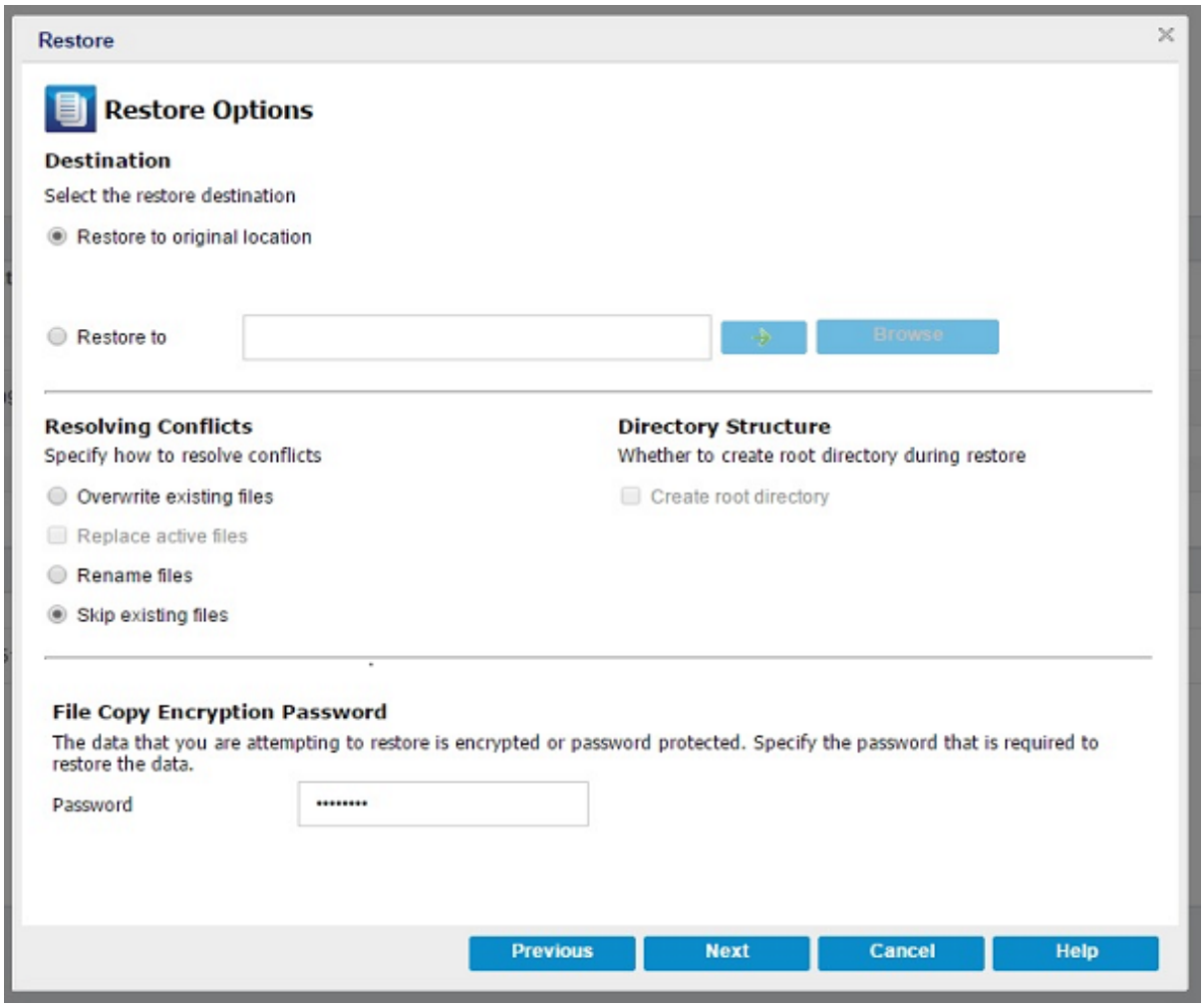
A conta de nuvem é adicionada ao console.

Definir as opções de restauração

Depois de especificar as informações de cópia de arquivo para restauração, defina as opções de cópia para a cópia do arquivo e conteúdo selecionado.

Siga estas etapas:

1. Na caixa de diálogo **Opções de restauração**, selecione o destino da restauração.



As opções de destino disponíveis são:

Restaurar no local original

Restaura no local original a partir do qual a imagem de backup foi capturada.

Restaurar para

Restaura no local especificado. É possível clicar no botão com a seta verde para verificar a conexão com o local especificado. Se necessário, forneça as credenciais de nome de usuário e senha para acessar esse local.

2. Especifique a opção **Resolvendo conflitos** que o Arcserve UDP executará se forem encontrados conflitos durante o processo de restauração.

   As opções disponíveis são:

   Substituir arquivos existentes

   Sobrescreve (substitui) qualquer arquivo existente que está localizado no destino da restauração. Todos os objetos serão restaurados dos arquivos de backup, independentemente da presença atual deles no computador.

   Substituir os arquivos ativos

   Substitui todos os arquivos ativos ao reinicializar. Se, durante a tentativa de restauração, o agente do Arcserve UDP (Windows) detectar que o arquivo existente está em uso ou sendo acessado, para evitar erros, ele não substituirá o arquivo imediatamente, só depois que o computador for reinicializado. (A restauração ocorrerá imediatamente, mas a substituição de arquivos ativos é feita durante a próxima reinicialização).

   Essa opção só estará disponível se você selecionar a opção **Substituir os arquivos existentes**.

   Observação: se essa opção não estiver selecionada, qualquer arquivo ativo será ignorado na restauração.

   Renomear arquivos

   Cria um novo arquivo se o nome de arquivo já existir. A seleção desta opção copia o arquivo de origem no destino com o mesmo nome de arquivo, mas com uma extensão diferente. Os dados serão restaurados no novo arquivo.

   Ignorar arquivos existentes

   Ignora e não substitui (sobrescreve) os arquivos localizados no destino da restauração. Apenas os objetos inexistentes em seu computador no momento serão restaurados dos arquivos de backup.

   Padrão: Ignorar arquivos existentes.

3. Especifique a **Estrutura de diretórios** para criar um diretório raiz durante a restauração.

   Criar diretório raiz

Especifica que se uma estrutura de diretórios raiz existir na imagem de backup capturada, o Arcserve UDP recriará a mesma estrutura de diretórios raiz no caminho de destino de restauração.

Se essa opção não for selecionada, o arquivo ou pasta será restaurado diretamente para a pasta de destino.

Por exemplo, se durante o backup você capturou os arquivos "C:\Pasta1\Subpasta2\A.txt" e "C:\Pasta1\Subpasta2\B.txt" e durante a restauração foi especificado como destino o local "D:\Restore".

- Se você optar por restaurar os arquivos "A.txt" e "B.txt" individualmente, o destino dos arquivos restaurados será "D:\Restore\A.txt" e "D:\Restore\B.txt" (o diretório raiz acima do nível de arquivo especificado não será recriado).
- Se você optar por restaurar a partir do nível da "Subpasta2", o destino dos arquivos restaurados será "D:\Restore\Subpasta2\A.txt" e "D:\Restore\Subpasta2\B.txt" (o diretório acima do nível de pasta especificado não será recriado).

Com esta opção selecionada, todo o caminho de diretório raiz para os arquivos / pastas (incluindo o nome de volume) é recriado até a pasta de destino. Se os arquivos/pastas a serem restaurados tiverem o mesmo nome de volume, o caminho do diretório raiz de destino não incluirá esse nome de volume. No entanto, se os arquivos/pastas a serem restaurados forem de nomes de volume diferentes, o caminho do diretório raiz do destino incluirá o nome do volume.

Por exemplo, se durante o backup você capturou os arquivos "C:\Pasta1\Subpasta2\A.txt", "C:\Pasta1\Subpasta2\B.txt" e também "E:\Pasta3\Subpasta4\C.txt" e durante a restauração foi especificado como destino de restauração o local "D:\Restore".

- Se você optar por restaurar apenas o arquivo "A.txt", o destino do arquivo restaurado será "D:\Restore\Pasta1\Subpasta2\A.txt" (o diretório raiz inteiro, sem o nome do volume, será recriado).
- Se você optar por restaurar tanto o arquivo "A.txt" como o "C.txt", o destino dos arquivos restaurados será "D:\Restore\C\Pasta1\Subpasta2\A.txt" e "D:\Restore\E\Pasta3\Subpasta4\C.txt" (o diretório raiz inteiro, com o nome do volume, será recriado).

4. Especifique a senha de criptografia em **Senha de criptografia da cópia de arquivo**.
5. Clique em **Avançar**.

   A caixa de diálogo **Resumo da restauração** é exibida.

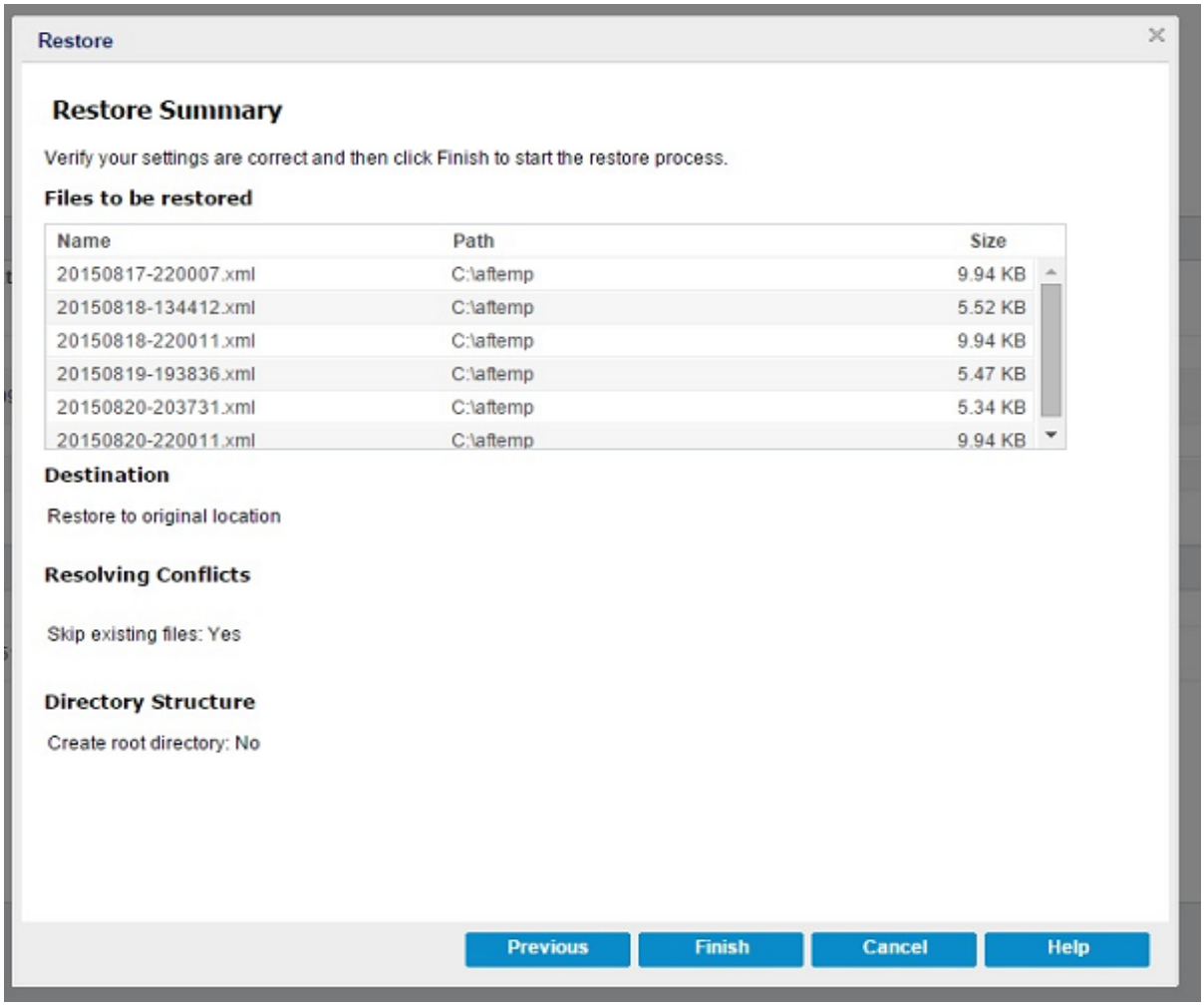
As opções de restauração são definidas para restaurar a partir de uma cópia de arquivo.

Restaurar o conteúdo da cópia de arquivo

Após definir as opções de restauração, verifique se suas configurações estão corretas e confirme o processo de restauração. O **Resumo da restauração** o auxilia a revisar todas as opções de restauração definidas e modificá-las se necessário.

Siga estas etapas:

1. Na caixa de diálogo **Resumo da restauração**, examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.



- Se as informações do resumo não estiverem corretas, clique em **Anterior** e volte à caixa de diálogo em questão para alterar a configuração incorreta.
- Se as informações de resumo estiverem corretas, clique em **Concluir** para iniciar o processo de restauração.

O conteúdo da cópia do arquivo é restaurado.

Verificar se o conteúdo foi restaurado

Após a conclusão do processo de restauração, verifique se o conteúdo foi restaurado no destino especificado.

Siga estas etapas:

1. Navegue até o destino de restauração especificado.

   É exibida uma lista de pastas.

2. Localize o arquivo para o qual tiver restaurado o conteúdo.

   Por exemplo, se selecionar restaurar o arquivo **A.txt** para o destino de restauração como "D:\Restore, vá até o seguinte local:

   D:\Restore\A.txt

3. Verifique o conteúdo para confirmar a tarefa de restauração.

   A restauração do conteúdo é verificada com êxito.

Como restaurar a partir de um arquivo morto

Cada vez que o Arcserve UDP executa uma tarefa de arquivo morto com êxito, ele arquiva todos os arquivos que foram alterados desde a última tarefa de arquivo morto bem-sucedida. Esse método de restauração permite procurar os dados arquivados e especificar exatamente qual arquivo deseja restaurar.

O processo de restauração de arquivo morto é idêntico à restauração de cópia de arquivo.

Execute as tarefas a seguir para restaurar de um arquivo morto:

1. Verificar os pré-requisitos e as considerações para restauração
2. Especificar as informações de cópia de arquivo para restauração
    a. Especifique a cópia do arquivo e o conteúdo para restauração
        - Especificar configuração de nuvem para restauração
    b. Definir as opções de restauração
3. Restaure o conteúdo do ponto de recuperação
4. Verificar se o conteúdo foi restaurado

Revisar os pré-requisitos e as considerações para restauração

Verifique se os pré-requisitos a seguir existem antes de executar uma restauração:

- Você tem pelo menos uma cópia de arquivo para restauração.
- Você tem um destino válido e acessível da cópia de arquivo do qual restaurar o conteúdo da cópia do arquivo.
- Você tem um local de destino válido e acessível para o qual restaurar o conteúdo da cópia do arquivo.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Revise as seguintes considerações de restauração:

- O Arcserve UDP permite que apenas uma tarefa de restauração seja executada ao mesmo tempo. Se você tentar iniciar manualmente uma tarefa de restauração, enquanto outra tarefa de restauração estiver em execução, uma mensagem de alerta será exibida informando sobre a outra tarefa está em execução e solicita que você tente novamente mais tarde.
- Se a restauração para um destino remoto e se todas as letras de unidade (A - Z) estiverem ocupadas, a restauração de dados para um caminho remoto não serão bem-sucedidas. O Agente do Arcserve UDP (Windows) precisa usar uma letra de unidade para montar o caminho do destino remoto.
- Aprimore a cópia do arquivo para otimizar o desempenho:
  - A cópia de arquivo pode enviar vários fragmentos simultaneamente para o destino (ArchMultChunkIO)
  - A cópia de arquivo pode copiar mais de um arquivo por vez (ThreadsForArchive).
  - A restauração a partir da cópia de arquivo pode fazer download de mais de um arquivo por vez (ThreadsForRestore).
  - A sincronização de catálogo usa vários segmentos (ThreadForCatalogSync).

  É possível alterar os valores do registro de cópia de arquivo padrão modificando o valor DWORD. Para obter mais informações, consulte Configurar definições da cópia de arquivo para otimizar o desempenho na *ajuda online do Agente para Windows*.

- (Opcional) Compreenda como funciona o processo de restauração. Para obter mais informações, consulte Como a restauração em nível de arquivo funciona.

Especificar as informações de cópia de arquivo para restauração

O Arcserve UDP oferece a opção de restaurar os dados a partir de uma cópia de arquivo. O objetivo de executar uma tarefa de restauração com êxito é identificar rapidamente os dados necessários e recuperá-los do local de backup adequado. Cada tarefa de restauração requer uma origem e um destino.

O processo envolvido na restauração de uma cópia de arquivo é como se segue:

- Especificar a cópia do arquivo e o conteúdo para restauração
- Definir as opções de restauração

Especificar a cópia do arquivo e o conteúdo para restauração

Use a opção **Procurar cópias de arquivo** para restaurar a partir de uma cópia do arquivo. Este método de restauração permite procurar os dados copiados do arquivo e especificar exatamente qual arquivo deseja restaurar.

Siga estas etapas:

1. Acesse a caixa de diálogo de seleção de método de restauração de uma das seguintes maneiras:

   No Arcserve UDP:

   a. Efetue logon no Arcserve UDP.

   b. Clique na guia **Recursos**.

   c. Selecione **Todos os nós** no painel esquerdo.

      Todos os nós adicionados são exibidos no painel central.

   d. No painel central, selecione o nó do e clique em **Ações**.

   e. Clique em **Restaurar** no menu suspenso **Ações**.

      A caixa de diálogo de seleção do método de restauração é exibida.

      Observação: você é automaticamente conectado ao nó do agente e a caixa de diálogo de seleção do método de restauração é exibida no nó do agente.

   No agente do Arcserve UDP (Windows):

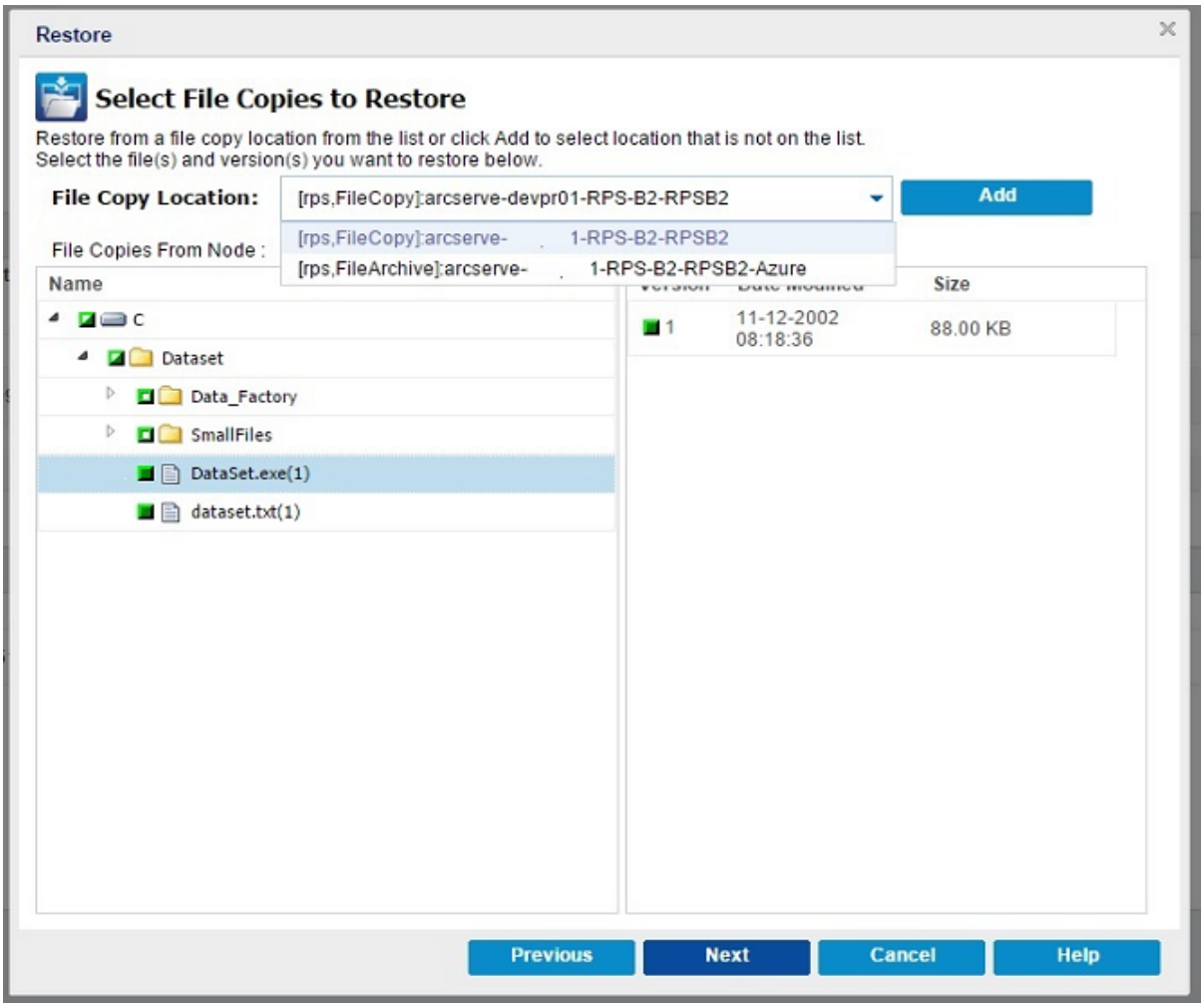
   a. Efetue logon no Agente do Arcserve UDP (Windows).

   b. Na página inicial, selecione **Restaurar**.

   A caixa de diálogo de seleção do método de restauração é exibida.

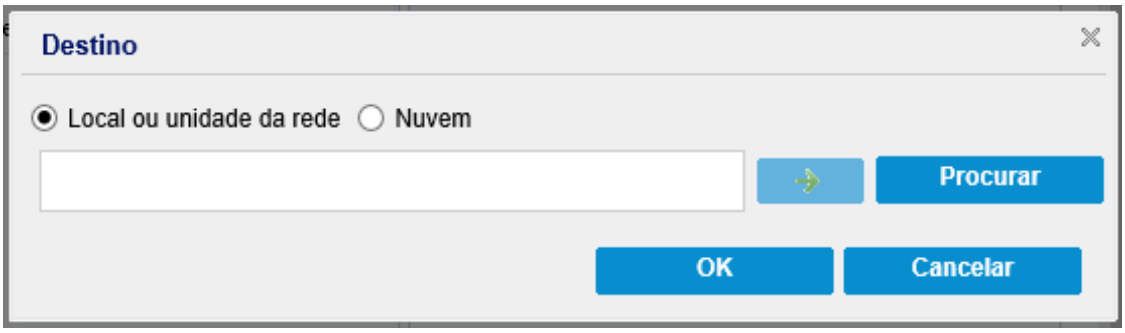
2. Clique na opção **Procurar cópias de arquivo**.

   A caixa de diálogo **Restaurar** é exibida. O destino em exibição no momento, no campo **Restaurar a partir de**, é o destino padrão configurado em **Cópia de arquivo**.



3. Se necessário, é possível clicar em **Adicionar** para procurar um local alternativo onde as imagens da cópia de arquivo estão armazenadas.

   A caixa de diálogo **Destino** é aberta exibindo as outras opções de destino disponíveis.



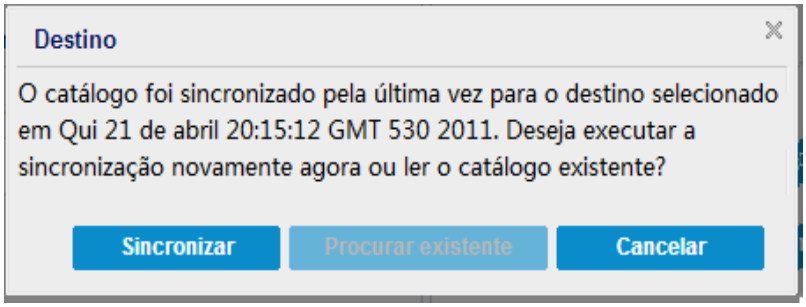
Local ou unidade da rede

A caixa de diálogo **Selecionar um local de backup** é exibida, permitindo procurar e selecionar um local alternativo ou o local da unidade de rede.

Nuvem

A caixa de diálogo **Configuração de nuvem** é exibida, permitindo acessar e selecionar um local de nuvem alternativo. Para obter mais informações sobre essa caixa de diálogo, consulte Especificar configuração de nuvem para restauração.

Independentemente de você ter selecionado a restauração na **Unidade local ou de rede** ou na **Nuvem**, ao alterar o destino para um local alternativo, uma caixa de diálogo pop-up será exibida perguntando se deseja executar uma nova sincronização do catálogo ou ler o catálogo existente.



- Se você estiver executando a sincronização do catálogo pela primeira vez, o botão **Procurar existente** estará desativado porque o catálogo de cópia de arquivo não existe localmente.
- Se a sincronização do catálogo já foi executada, a caixa de diálogo exibirá detalhes sobre a última vez o catálogo foi sincronizado no destino. Caso outras tarefas de cópia de arquivo tenham sido executadas após a hora exibida, talvez seu catálogo não esteja sincronizado. Você pode selecionar a opção **Sincronizar** para garantir que seu catálogo de cópia de arquivo contenha dados atualizados.

1. Clique em **Sincronizar** para fazer download do catálogo de cópia de arquivo do destino da cópia de arquivo especificado para o computador local para obter uma busca mais rápida.

2. Clique em **Procurar existente** para usar o catálogo de cópia de arquivo que está disponível localmente e para não o baixar/sincronizar novamente.

4. No painel à esquerda, especifique os dados da cópia de arquivo a serem restaurados. É possível selecionar pastas de cópia de arquivos ou arquivos a serem restaurados.

   Ao selecionar um arquivo individual a ser restaurado, todas as versões de cópia de arquivo de tal arquivo são exibidas no painel direito. Se várias versões estiverem disponíveis, é necessário selecionar qual versão da cópia de arquivo deseja restaurar.

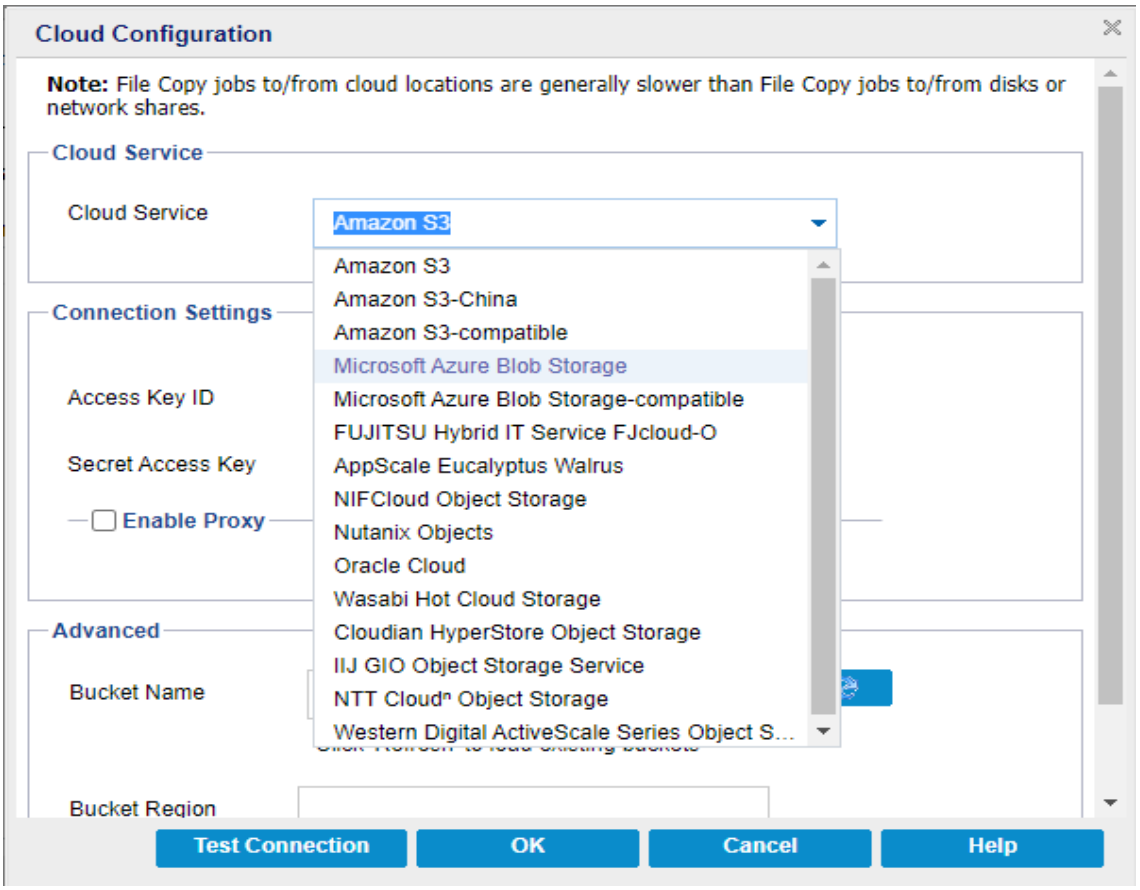
5. Depois de selecionar uma pasta do arquivo copiado ou versão do arquivo para restauração, clique em **Avançar**.

   A caixa de diálogo **Opções de restauração** é exibida.

   A **Cópia do arquivo e o Conteúdo para restauração** são especificados.

Especificar configuração de nuvem para restauração

Observação: o procedimento a seguir só se aplica se você está restaurando um arquivo/uma pasta a partir de um local na nuvem de cópia de arquivo ou de arquivo morto.



As opções disponíveis são Amazon S3, compatível com Amazon S3, Windows Azure, compatível com Windows Azure, FUJITSU Hybrid IT Service FJcloud-O e Eucalyptus-Walrus. (Amazon S3 é o fornecedor padrão).

Observação: se estiver usando o Eucalyptus-Walrus como seu fornecedor da nuvem de cópia de arquivo, não será possível copiar arquivos cujo tamanho de caminho total excede 170 caracteres.

As opções de configuração para cada fornecedor da nuvem são semelhantes (com algumas terminologias distintas), e nenhuma diferença é descrita.

1. A partir da opção **Procurar cópias de arquivo** ou **Localizar arquivos/pastas para restauração**, clique em **Adicionar**.

   A caixa de diálogo **Destino** será aberta.

2. Selecione **Nuvem** e clique em **Procurar**.

A caixa de diálogo **Configuração da nuvem** é aberta.

3. Digite os seguintes detalhes:

Nome do armazenamento

Especifica o nome do armazenamento na nuvem. Esse nome será adicionado ao console para identificar a conta da nuvem. Cada conta de nuvem deve ter um nome de armazenamento exclusivo.

Serviço de armazenamento

Selecione o serviço na lista suspensa. A opção de configuração varia de acordo com o serviço de armazenamento selecionado.

ID da chave de acesso/nome da conta/ID de consulta

Identifica o usuário que está solicitando acesso a este local.

Para esse campo, o Amazon S3 usa a ID da chave de acesso. O Windows Azure e FUJITSU Hybrid IT Service FJcloud-O usam o nome da conta, e o Eucalyptus-Walrus usa a ID da consulta.

Chave de acesso secreta/chave secreta

Uma vez que a chave de acesso não está criptografada, esta chave de acesso secreta será uma senha usada para verificar a autenticidade da solicitação para acessar este local.

Importante: esta chave de acesso secreta é fundamental para manter a segurança de suas contas. É necessário manter as chaves e as credenciais da conta em um local seguro. Não incorpore a chave de acesso secreta em uma página da web ou em outro código-fonte de acesso público e não a transmita em canais não seguros.

Para esse campo, o Amazon S3 usa a chave de acesso secreta. O Windows Azure, o FUJITSU Hybrid IT Service FJcloud-O e o Eucalyptus-Walrus usam a chave secreta.

Configurações de proxy

Especifica as configurações do servidor proxy. Selecione **Conectar usando um servidor proxy** para ativar essa opção. Caso selecione esta opção, será necessário incluir também o endereço IP (ou nome do computador) do servidor proxy e o número da porta correspondente, usado pelo servidor proxy em conexões com a internet. Pode-se também selecionar esta opção se o servidor proxy exigir autenticação. Será necessário fornecer as informações de autenticação correspondentes (Nome de domínio/nome de usuário e senha) para usar o servidor proxy.

Observação: o recurso Proxy não está disponível para Eucalyptus-Walrus.

Nome do compartimento de memória/Contêiner

Todos os arquivos e as pastas movidos ou copiados para o fornecedor da nuvem são armazenados e organizados nos compartimentos de memória (ou contêineres). Os compartimentos de memória são como um contêiner para os arquivos e são usados para agrupar e organizar objetos. Cada objeto armazenado no fornecedor da nuvem é colocado em um compartimento de memória.

Para esse campo, o Amazon S3 e Eucalyptus-Walrus usam o Nome do compartimento de memória. O Windows Azure e o FUJITSU Hybrid IT Service FJcloud-O usam o recipiente.

Observação: para o restante desta etapa, todas as referências a compartimentos de memória também podem ser aplicadas aos recipientes, contanto que seja especificado.

Região de compartimento de memória

Refere-se à região de compartimento de memória no Amazon e no FUJITSU Hybrid IT Service FJcloud-O.

Número do contrato

Refere-se ao número do contrato que o FUJITSU Hybrid IT Service FJcloud-O fornece.

ID do projeto

Refere-à ID do projeto que o FUJITSU Hybrid IT Service FJcloud-O gera.

Ativar a redução de armazenamento de dados redundantes

Para Amazon S3 apenas, esta opção permite ativar a RRS (Reduced Redundancy Storage). RRS é uma opção de armazenamento no Amazon S3 que ajuda você a reduzir o custo por meio do armazenamento de dados reproduzíveis não essenciais em níveis de redundância mais baixos do que aqueles do armazenamento padrão do Amazon S3s. As opções de armazenamento padrão e de redução de armazenamento de dados redundantes armazenam dados em vários recursos e dispositivos, mas com a RRS os dados são replicados menos vezes e o custo é menor. Deve-se esperar a mesma latência e taxa de transferência usando o armazenamento padrão ou RRS do Amazon S3. Por padrão, esta opção não está selecionada (o Amazon S3 usa a opção de armazenamento padrão).

4. Clique em **Testar conexão** para verificar a conexão com o local na nuvem especificado.
5. Clique em **OK**.

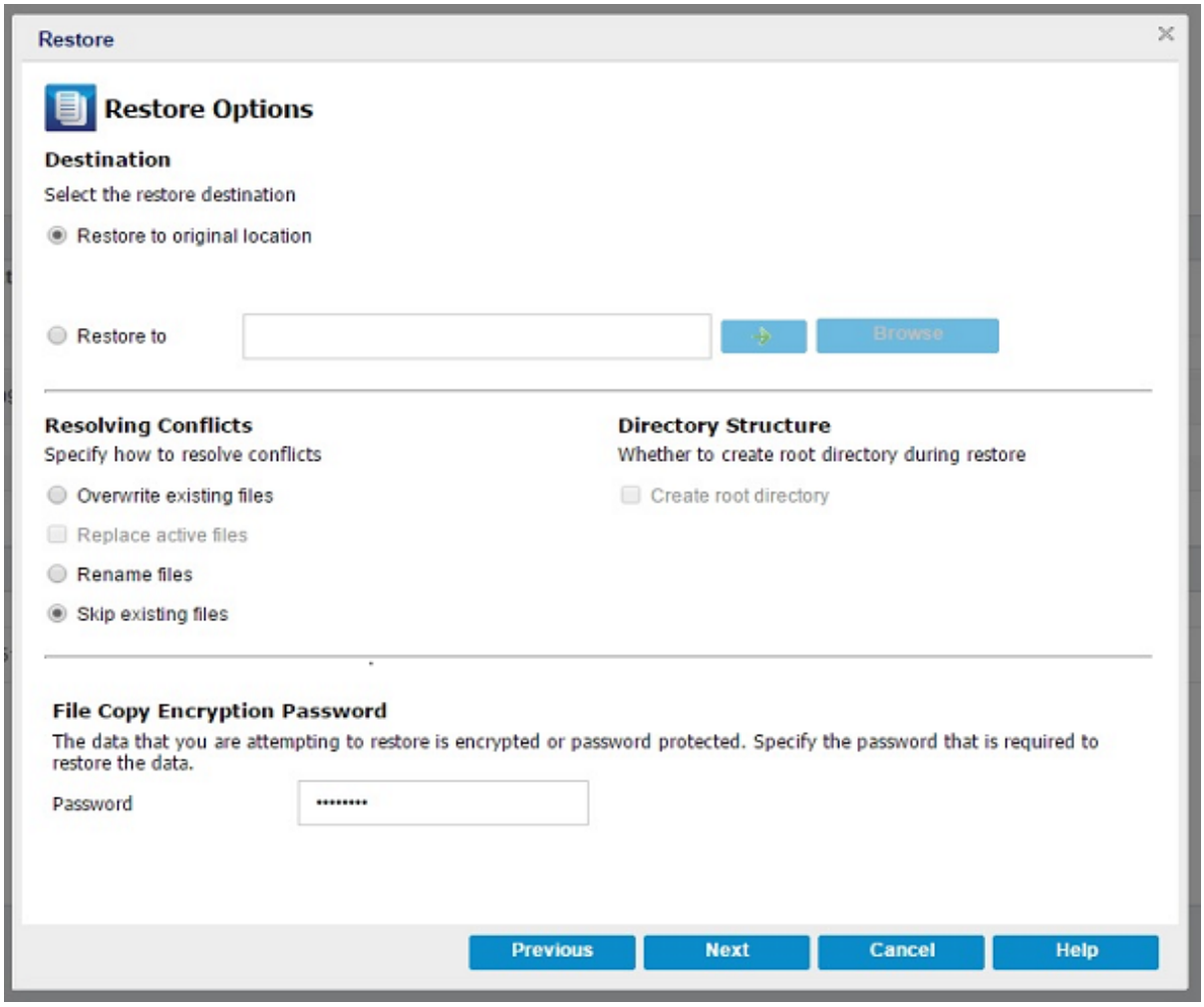
A conta de nuvem é adicionada ao console.

Definir as opções de restauração

Depois de especificar as informações de cópia de arquivo para restauração, defina as opções de cópia para a cópia do arquivo e conteúdo selecionado.

Siga estas etapas:

1. Na caixa de diálogo **Opções de restauração**, selecione o destino da restauração.



As opções de destino disponíveis são:

Restaurar no local original

Restaura no local original a partir do qual a imagem de backup foi capturada.

Restaurar para

Restaura no local especificado. É possível clicar no botão com a seta verde para verificar a conexão com o local especificado. Se necessário, forneça as credenciais de nome de usuário e senha para acessar esse local.

2. Especifique a opção **Resolvendo conflitos** que o Arcserve UDP executará se forem encontrados conflitos durante o processo de restauração.

   As opções disponíveis são:

   Substituir arquivos existentes

   Sobrescreve (substitui) qualquer arquivo existente que está localizado no destino da restauração. Todos os objetos serão restaurados dos arquivos de backup, independentemente da presença atual deles no computador.

   Substituir os arquivos ativos

   Substitui todos os arquivos ativos ao reinicializar. Se, durante a tentativa de restauração, o agente do Arcserve UDP (Windows) detectar que o arquivo existente está em uso ou sendo acessado, para evitar erros, ele não substituirá o arquivo imediatamente, só depois que o computador for reinicializado. (A restauração ocorrerá imediatamente, mas a substituição de arquivos ativos é feita durante a próxima reinicialização).

   Essa opção só estará disponível se você selecionar a opção **Substituir os arquivos existentes**.

   Observação: se essa opção não estiver selecionada, qualquer arquivo ativo será ignorado na restauração.

   Renomear arquivos

   Cria um novo arquivo se o nome de arquivo já existir. A seleção desta opção copia o arquivo de origem no destino com o mesmo nome de arquivo, mas com uma extensão diferente. Os dados serão restaurados no novo arquivo.

   Ignorar arquivos existentes

   Ignora e não substitui (sobrescreve) os arquivos localizados no destino da restauração. Apenas os objetos inexistentes em seu computador no momento serão restaurados dos arquivos de backup.

   Padrão: Ignorar arquivos existentes.

3. Especifique a **Estrutura de diretórios** para criar um diretório raiz durante a restauração.

   Criar diretório raiz

Especifica que se uma estrutura de diretórios raiz existir na imagem de backup capturada, o Arcserve UDP recriará a mesma estrutura de diretórios raiz no caminho de destino de restauração.

Se essa opção não for selecionada, o arquivo ou pasta será restaurado diretamente para a pasta de destino.

Por exemplo, se durante o backup você capturou os arquivos "C:\Pasta1\Subpasta2\A.txt" e "C:\Pasta1\Subpasta2\B.txt" e durante a restauração foi especificado como destino o local "D:\Restore".

- Se você optar por restaurar os arquivos "A.txt" e "B.txt" individualmente, o destino dos arquivos restaurados será "D:\Restore\A.txt" e "D:\Restore\B.txt" (o diretório raiz acima do nível de arquivo especificado não será recriado).
- Se você optar por restaurar a partir do nível da "Subpasta2", o destino dos arquivos restaurados será "D:\Restore\Subpasta2\A.txt" e "D:\Restore\Subpasta2\B.txt" (o diretório acima do nível de pasta especificado não será recriado).

Com esta opção selecionada, todo o caminho de diretório raiz para os arquivos / pastas (incluindo o nome de volume) é recriado até a pasta de destino. Se os arquivos/pastas a serem restaurados tiverem o mesmo nome de volume, o caminho do diretório raiz de destino não incluirá esse nome de volume. No entanto, se os arquivos/pastas a serem restaurados forem de nomes de volume diferentes, o caminho do diretório raiz do destino incluirá o nome do volume.

Por exemplo, se durante o backup você capturou os arquivos "C:\Pasta1\Subpasta2\A.txt", "C:\Pasta1\Subpasta2\B.txt" e também "E:\Pasta3\Subpasta4\C.txt" e durante a restauração foi especificado como destino de restauração o local "D:\Restore".

- Se você optar por restaurar apenas o arquivo "A.txt", o destino do arquivo restaurado será "D:\Restore\Pasta1\Subpasta2\A.txt" (o diretório raiz inteiro, sem o nome do volume, será recriado).
- Se você optar por restaurar tanto o arquivo "A.txt" como o "C.txt", o destino dos arquivos restaurados será "D:\Restore\C\Pasta1\Subpasta2\A.txt" e "D:\Restore\E\Pasta3\Subpasta4\C.txt" (o diretório raiz inteiro, com o nome do volume, será recriado).

4. Especifique a senha de criptografia em **Senha de criptografia da cópia de arquivo**.
5. Clique em **Avançar**.

   A caixa de diálogo **Resumo da restauração** é exibida.

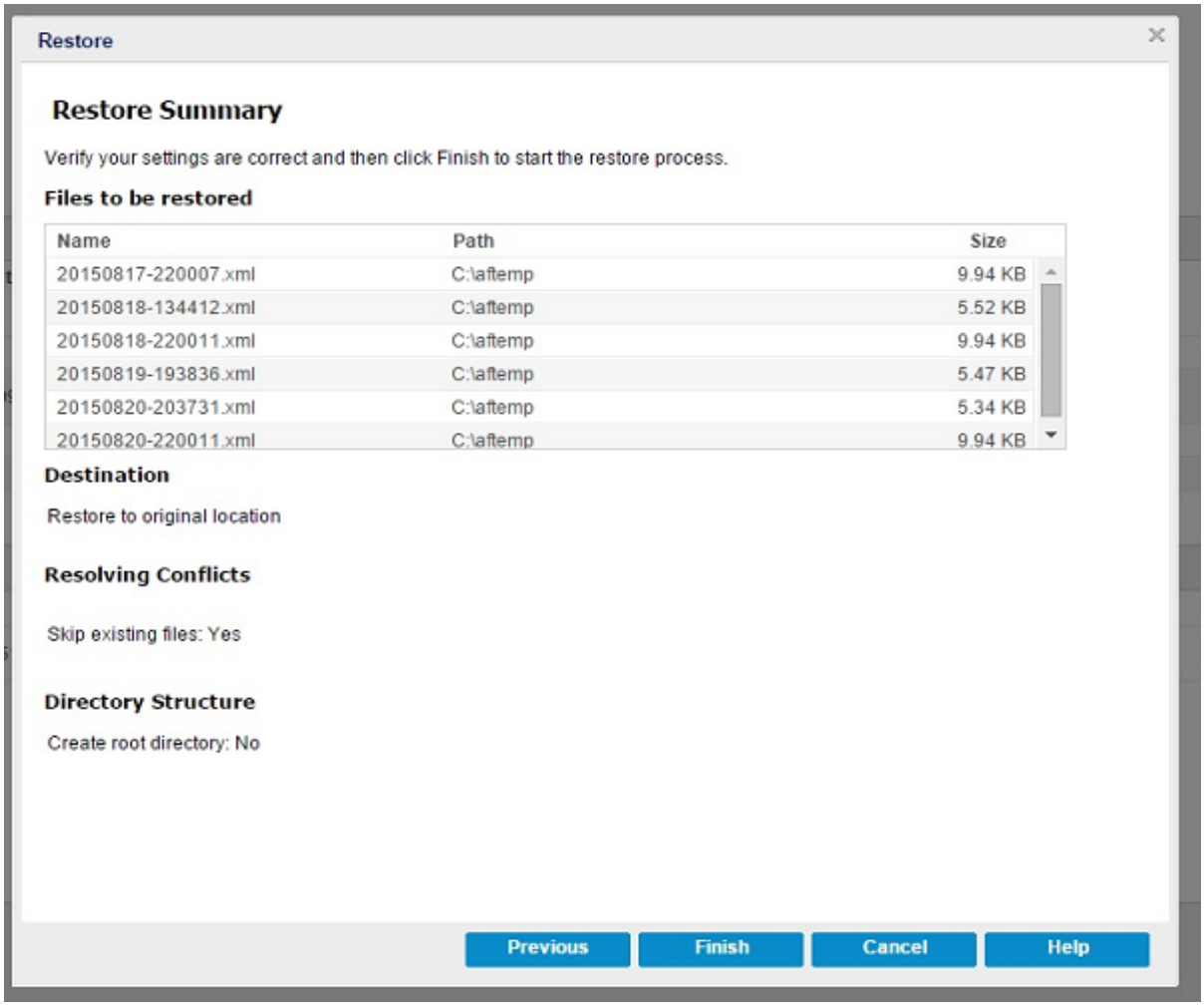
As opções de restauração são definidas para restaurar a partir de uma cópia de arquivo.

Restaure o conteúdo do ponto de recuperação

Após definir as opções de restauração, verifique se suas configurações estão corretas e confirme o processo de restauração. O **Resumo da restauração** o auxilia a revisar todas as opções de restauração definidas e modificá-las se necessário.

Siga estas etapas:

1. Na caixa de diálogo **Resumo da restauração**, examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.



- Se as informações do resumo não estiverem corretas, clique em **Anterior** e volte à caixa de diálogo em questão para alterar a configuração incorreta.
- Se as informações de resumo estiverem corretas, clique em **Concluir** para iniciar o processo de restauração.

O conteúdo da cópia do arquivo é restaurado.

Verificar se o conteúdo foi restaurado

Após a conclusão do processo de restauração, verifique se o conteúdo foi restaurado no destino especificado.

Siga estas etapas:

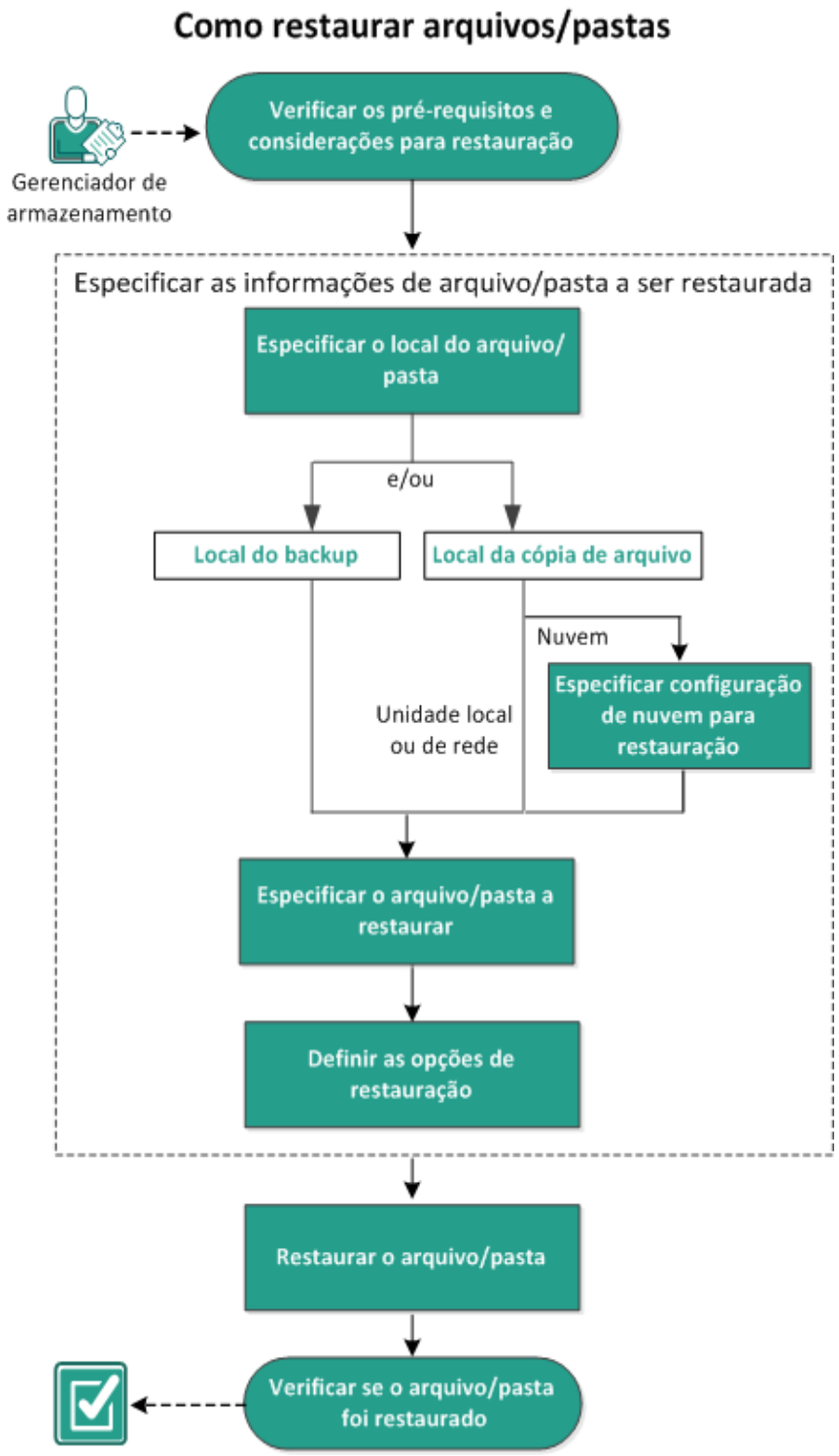
1. Efetue logon na caixa de correio de destino.
2. Verifique o item de caixa de correio que você restaurou.
3. Verifique o conteúdo restaurado.

   A restauração do conteúdo é verificada com êxito.

Como restaurar arquivos/pastas

Sempre que o Arcserve UDP executar um backup com êxito, todas as pastas/arquivos com backup serão incluídos na imagem de instantâneo do seu backup. Este método de restauração permite especificar exatamente qual arquivo/pasta deve ser restaurado.

O seguinte diagrama ilustra o processo para restaurar arquivos/pastas específicos:



Execute as seguintes tarefas para restaurar arquivos/pastas:

1. Verificar os pré-requisitos e as considerações para restauração
2. Especificar as informações de arquivo/pasta a serem restauradas

a. Especificar o local do arquivo/pasta
    - Especificar configuração de nuvem para restauração
b. Especificar o arquivo/pasta a ser restaurado
c. Definir as opções de restauração

3. Restaurar o arquivo/pasta
4. Verificar se o arquivo/pasta foi restaurado

Verificar os pré-requisitos e as considerações para restauração

Verifique se os pré-requisitos a seguir existem antes de executar uma restauração:

- Você tem pelo menos um backup ou versão da cópia do arquivo disponível para restauração.
- Você tem um destino válido e acessível do backup ou da cópia de arquivo a partir do qual restaurar o conteúdo do backup ou da cópia do arquivo.
- Você tem um local de destino válido e acessível para o qual restaurar o conteúdo do backup ou da cópia do arquivo.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Revise as seguintes considerações de restauração:

- Para um ponto de recuperação sem um catálogo do sistema de arquivos criado, para garantir que você possa navegar e selecionar arquivos/pastas para restaurar da IU, deve ser concedido acesso à conta/grupo para todas as pastas/arquivos em todos os volumes com acesso de leitura/lista antes de realizar o backup.

  O sistema local (SYSTEM) ou o grupo de administradores internos (BUILTIN\Administrators) precisa ser adicionado à ACL das pastas para que o Agente do Arcserve UDP (Windows) consiga procurar um backup sem um catálogo do sistema de arquivos criado. Caso contrário, o Agente do Arcserve UDP (Windows) não poderá procurar as pastas na IU de restauração.

- (Opcional) Compreenda como funciona o processo de restauração. Para obter mais informações, consulte Como a restauração em nível de arquivo funciona.

  Observação: o processo para restaurar a partir de um local de cópia de arquivo é semelhante à restauração a partir de um local de backup.

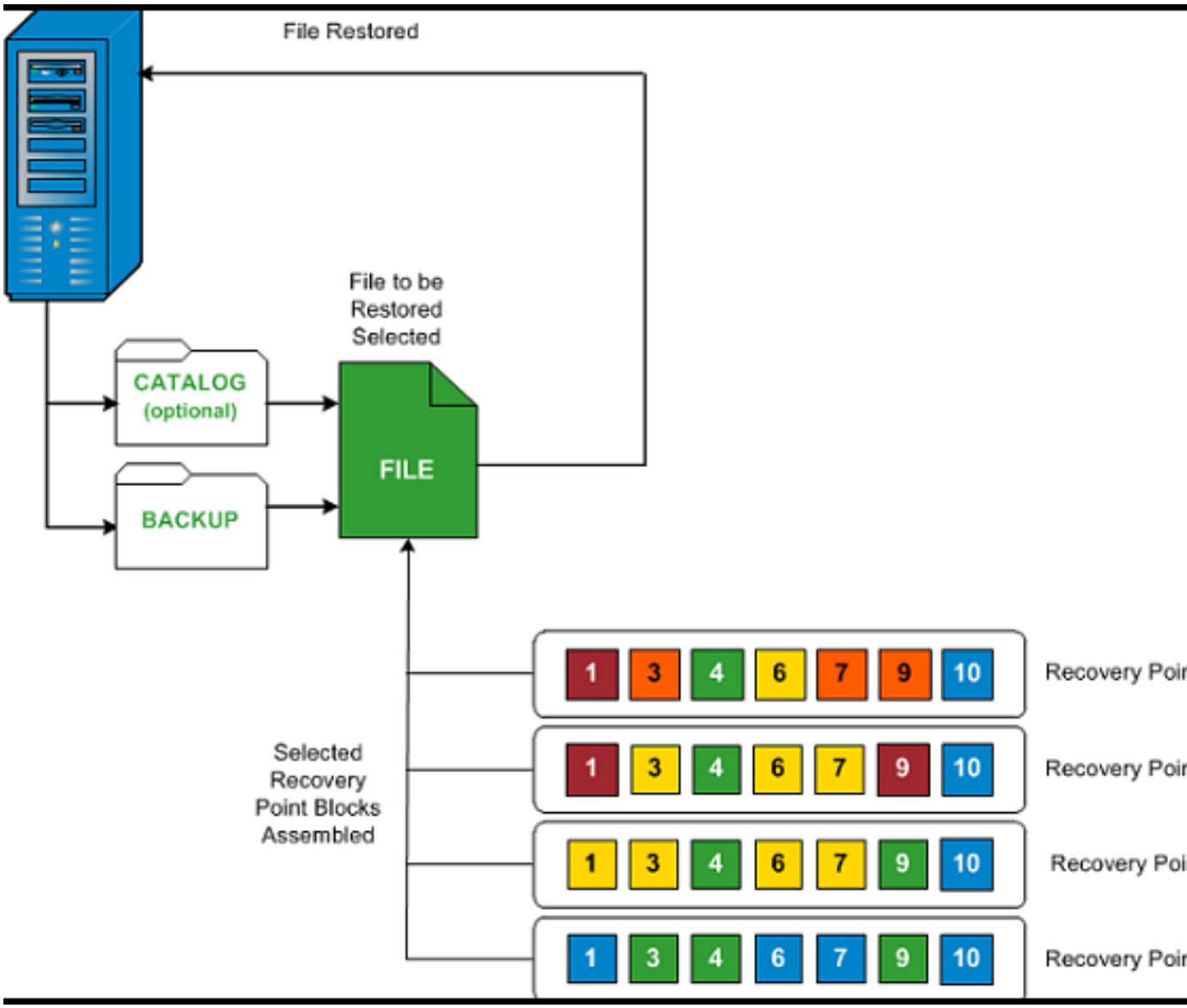
- (Opcional) Examine os arquivos ignorados durante a restauração. Para obter mais informações, consulte o tópico Arquivos ignorados durante a restauração.

Como a restauração em nível de arquivo funciona

Durante um backup em nível de bloco, cada arquivo de backup é composto de um conjunto de blocos que definem aquele arquivo específico. Se precisar restaurar um arquivo específico, é possível pesquisar o backup e selecionar o arquivo que deseja restaurar e o ponto de recuperação de onde deseja restaurar. Em seguida, o Agente do Arcserve UDP (Windows) coleta a versão dos blocos que foram usados para o ponto de recuperação do arquivo especificado, monta novamente e restaura o arquivo.

Observação: ao especificar as configurações de backup, você tem a opção de criar um catálogo de arquivos durante o backup. Esse catálogo de arquivos permite que você procure por sessões de backup mais rapidamente durante a restauração. Se você optar por não criar o catálogo durante o backup, ele poderá ser criado posteriormente.

O diagrama de fluxo a seguir mostra o processo de como o Arcserve UDP restaura um arquivo específico.


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

Arquivos ignorados durante a restauração

Durante a execução de uma restauração pelo agente do Arcserve UDP (Windows), alguns arquivos podem ser ignorados propositalmente.

Os arquivos e as pastas na tabela a seguir são ignorados durante uma restauração se as duas condições a seguir existirem:

- Os arquivos são ignorados quando tais arquivos existirem antes da restauração e a opção de conflito for "Ignorar arquivos existentes".
- As pastas e os arquivos listados na tabela a seguir são ignorados porque são um componente importante para o Windows ou o agente do Arcserve UDP (Windows).

Sistema operacional	Pasta ou local	Nome do arquivo ou pasta	Observações
Todos	Pasta raiz de cada volume	CAVolTrc.dat	Usado pelo driver de rastreamento do Arcserve UDP.
		cavoltrcsnapshot.dat	
		Informações de volume do sistema*	Usado para salvar arquivos/pastas por um sistema Windows, por exemplo, arquivos de cópia de sombra de volume.
		RECYCLER*	Usado apenas em partições NTFS. Contém uma lixeira para cada usuário que efetua logon no computador, classificadas por seu SID (Security Identifier – Identificador de Segurança).
		$Recycle.Bin*	Ao excluir um arquivo no Windows NT Explorer ou Meu computador, o arquivo é armazenado na Lixeira até que você a esvazie ou restaure o arquivo.
	Qualquer pasta contém arquivos de imagem	Thumbs.db	Armazena imagens em miniatura para o modo de exibição de miniatura do Windows Explorer.
	Pasta raiz do volume	PageFile.Sys	Arquivo de troca de memória virtual do Windows.
		Hiberfil.sys	Arquivo Hibernate usado para salvar os dados do sistema quando o computador entra no modo de hibernação.

As pastas e os arquivos a seguir são ignorados apenas quando você restaura no local original ou alternativo:

Sistema operacional	Pasta ou local	Nome do arquivo ou pasta	Observação
Todos	Pasta especificada no registro de valor em: HKLM\Software\Microsoft\Windows NT\CurrentVersion\WinLogon\SfcDllCache	Todos os arquivos/pastas (de maneira recursiva)	A pasta contém um arquivo DLL em cache que é usado para o SFC (System File Checker – Verificador de Arquivos do Sistema) e o conteúdo do diretório de cache da DLL do sistema é recriado usando SFC.
	%SystemRoot%\SYSTEM32\dllCache		
	Pasta raiz do quorum_device	MSCS*	Usado para o Microsoft Cluster Server.

	%SystemRoot%\SYSTEM32\	perf?00?.dat	Dados de desem-penho usa-dos pelo contador de desem-penho do Windows.

		perf?00?.bak	
		CATROOT*	Usado para Proteção de arquivos do Windows (WFP) registra as assinaturas digitais das instalações do sistema operacional (como EXE, DLL, SYS, OCX e assim por diante) para protegê-las contra exclusão ou de substituição por versões mais antigas.
	%SystemRoot%\inetsrv\	metabase.bin	O arquivo binário de metabase de versões do IIS anteriores ao 6.0.
	Arquivo ou pasta especificada no valor diferente de "Armazenamento comum do SIS" em HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup	Todos os arquivos/pastas (de maneira recursiva)	Arquivos e pastas não devem ser copiados para backup e restaurados. Para obter mais informações, consulte o link.
XP	Volume do sistema	NTLDR	O principal

W2003			carregador de inicialização.
		BOOT.INI	Contém a configuração de inicialização (se a configuração estiver ausente, como padrão, o NTLDR usará \Windows na primeira partição do primeiro disco rígido).
		NTDETECT.COM	Obrigatório para inicializar um sistema operacional com base em NT. Detecta informações de hardware básicas necessárias para uma inicialização bem-sucedida.
Vista e posterior	Pasta raiz do volume do sistema	boot*	Pasta de inicialização para Windows.
		bootmgr	Arquivo do gerenciador de inicialização do

			Windows.
		EFI\Microsoft\Boot*	Usado para inicialização de EFI.
	%SystemRoot%\SYSTEM32\	LogFiles\WMI\RTBackup*	Armazena os arquivos de rastreamento de ETW (extension .etl) para as sessões de rastreamento de eventos em tempo real.
		config\RegBack*	Backup da tabela do registro atual.
Win8 e posterior	Volume do sistema	swapfile.sys	Arquivo do controlador de sistema, normalmente cerca de 256 MB. Ele é usado pelos aplicativos do Metro style que não podem se encaixar nas características de paginação tradicional (como padrões de uso, crescimento, reserva de

			espaço) do pagefile.sys.
		BOOTNXT	Usado para inicializar a partir do sistema operacional, que não seja o Windows 8. Criado ao ativar as opções de inicialização e atualizado pelo Windows.

O Log de atividades fornece as seguintes informações:

- Informações de data e hora: arquivos de sistema jobxxxx ignorados. Você pode usar a BMR (Recuperação Bare Metal) para restaurá-los.
- Informações de data e hora: arquivos ou diretórios de sistema jobxxxx ignorados. Arquivos ou diretórios ignorados estão disponíveis em: C:\Arquivos de programas\Arcserve\Unified Data Protection\Engine\Logs\Restore-<YYYYMMDD>-<hhmmss>-<Process ID>-<Job ID>.log.

Especificar as informações de arquivo/pasta a serem restauradas

O Arcserve UDP fornece uma opção de localizar e restaurar um arquivo ou uma pasta específica. A meta de executar uma tarefa de restauração com êxito é identificar rapidamente os dados necessários e recuperá-los do local de backup adequado. Cada tarefa de restauração requer uma origem e um destino.

O processo envolvido na restauração de localização de arquivos/pastas é o seguinte:

1. Especificar o local do arquivo/pasta
   - Especificar configuração de nuvem para restauração
2. Especificar o arquivo/pasta a ser restaurado
3. Definir as opções de restauração

Especificar o local do arquivo/pasta

Use a opção **Localizar arquivos/pastas** para restaurar arquivos e pastas. Este método de restauração permite especificar exatamente qual arquivo ou pasta deve ser restaurado.

Siga estas etapas:

1. Acesse a caixa de diálogo de seleção de método de restauração de uma das seguintes maneiras:

   No Arcserve UDP:

   a. Efetue logon no Arcserve UDP.

   b. Clique na guia **Recursos**.

   c. Selecione **Todos os nós** no painel esquerdo.

      Todos os nós adicionados são exibidos no painel central.

   d. No painel central, selecione o nó do e clique em **Ações**.

   e. Clique em **Restaurar** no menu suspenso **Ações**.

      A caixa de diálogo de seleção do método de restauração é exibida.

      Observação: você é automaticamente conectado ao nó do agente e a caixa de diálogo de seleção do método de restauração é exibida no nó do agente.

   No agente do Arcserve UDP (Windows):

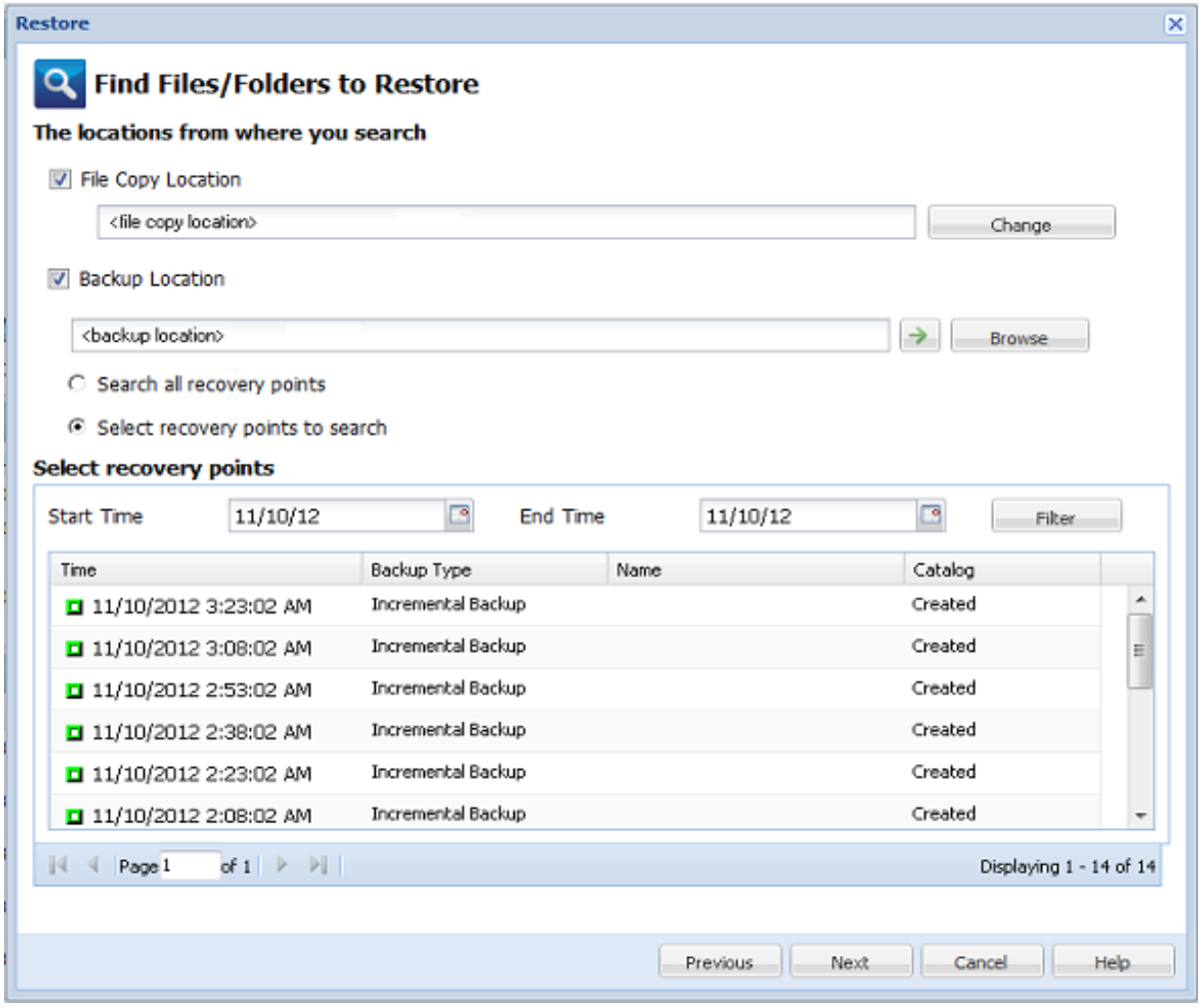
   a. Efetue logon no Agente do Arcserve UDP (Windows).

   b. Na página inicial, selecione **Restaurar**.

   A caixa de diálogo de seleção do método de restauração é exibida.

2. Clique na opção **Localizar arquivos/pastas para restauração**.

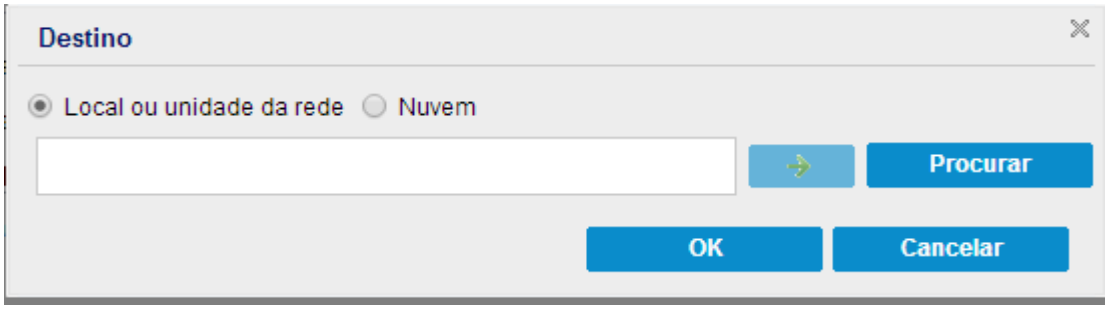
   A caixa de diálogo **Localizar arquivos/pastas para restauração** é exibida.



3. Marque a caixa de seleção **Local da cópia de arquivo** ou clique em **Alterar** para modificar o local de destino em que as imagens de cópia de arquivo estão armazenadas.

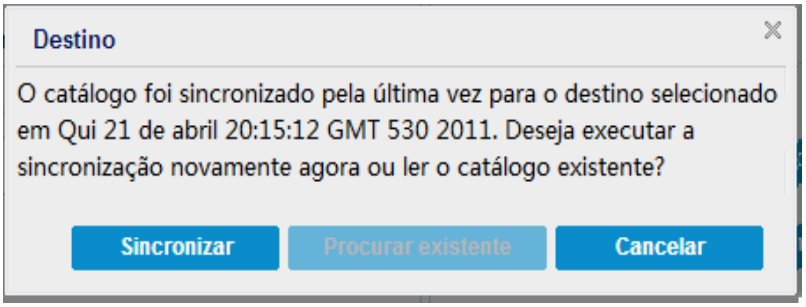
   A caixa de diálogo **Destino** é exibida e será possível selecionar **Local ou unidade da rede** ou **Nuvem**.

   Observação: por padrão, os campos **Local do backup** e **Local da cópia de arquivo** exibem o caminho correspondente usado para o mais recentes destinos de backup/-cópia de arquivo.



- Se selecionar um **Local ou unidade da rede**, será possível especificar ou procurar um local onde as suas imagens de cópia de arquivo estão armazenadas.
- Pode-se clicar no ícone de validação em forma de seta verde para confirmar o devido acesso ao local de origem.
- Se selecionar **Nuvem**, será possível especificar um local na nuvem ou clicar no botão **Configurar** para exibir a caixa de diálogo **Configuração de nuvem**. Para obter mais informações, consulte o tópico Especificar configuração de nuvem para restauração.

  Independentemente de você ter selecionado a restauração na **Unidade local ou de rede** ou na **Nuvem**, ao alterar o destino para um local alternativo, uma caixa de diálogo pop-up será exibida perguntando se deseja executar uma nova sincronização do catálogo ou ler o catálogo existente.



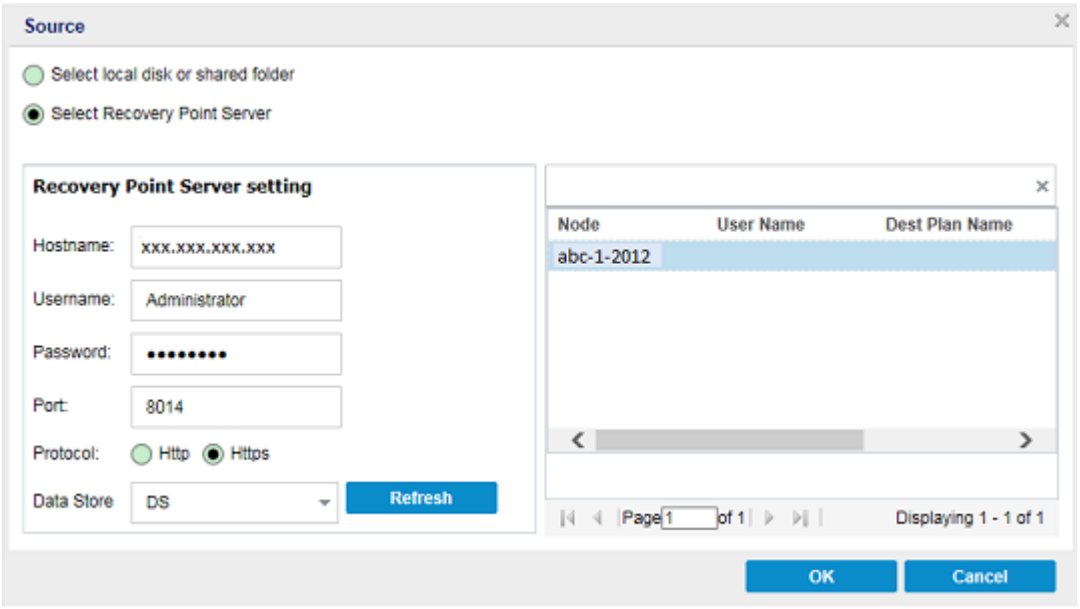
  - Se você estiver executando a sincronização do catálogo pela primeira vez, o botão **Procurar existente** estará desativado porque o catálogo de cópia de arquivo não existe localmente.
  - Se a sincronização do catálogo já foi executada, a caixa de diálogo exibirá detalhes sobre a última vez o catálogo foi sincronizado no destino. Caso outras tarefas de cópia de arquivo tenham sido executadas após a hora exibida, talvez seu catálogo não esteja sincronizado. Você pode selecionar a opção **Sincronizar** para garantir que seu catálogo de cópia de arquivo contenha dados atualizados.

    1. Clique em **Sincronizar** para fazer download do catálogo de cópia de arquivo do destino da cópia de arquivo especificado para o computador local para obter uma busca mais rápida.

    2. Clique em **Procurar existente** para usar o catálogo de cópia de arquivo que está disponível localmente e para não o baixar/sincronizar novamente.

4. Marque a caixa de diálogo **Local do backup** e clique em **Alterar** para modificar o local do backup.

   A caixa de diálogo **Origem** é exibida e será possível selecionar o local do backup.



5. Selecione uma das opções abaixo na caixa de diálogo **Origem**:

   Selecionar o disco local ou uma pasta compartilhada

   a. Especifique ou procure o local onde as suas imagens de backup estão armazenadas e selecione o backup de origem adequado.

      É possível clicar no botão com a seta verde para verificar a conexão com o local especificado. Se necessário, forneça as credenciais de Nome de usuário e Senha para acessar esse local de origem.

      A caixa de diálogo **Selecionar o local do backup** é exibida.

   b. Selecione a pasta onde estão armazenados os pontos de recuperação e clique em **OK**.

      A caixa de diálogo **Selecione o local do backup** é fechada e é possível ver o local do backup na caixa de diálogo **Origem.**

   c. Clique em **OK**.

      Os pontos de recuperação são listados na caixa de diálogo **Localizar arquivos/pastas para restauração**.

   Selecionar servidor de ponto de recuperação

   a. Especifique os detalhes da configuração do servidor de ponto de recuperação e clique em **Atualizar**.

      Todos os agentes estão listados na coluna **Agente de proteção de dados** na caixa de diálogo **Origem**.

   b. Selecione o agente na lista exibida e clique em **OK**.

Os pontos de recuperação são listados na caixa de diálogo **Localizar arquivos/pastas para restauração**.

Observação: se você selecionar um agente diferente e se os pontos de recuperação estão criptografados, é necessário fornecer a senha de criptografia quando solicitado.

6. Selecione uma das opções a seguir para pesquisar pontos de recuperação:

Pesquisar em todos os pontos de recuperação

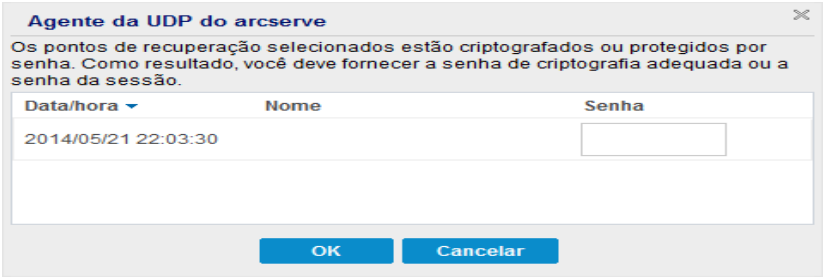
Procura o arquivo ou a pasta em todos os pontos de recuperação armazenados no local indicado. É necessário especificar o arquivo ou a pasta que você deseja pesquisar na caixa de diálogo **Localizar arquivos/pastas para restauração**.

Selecionar pontos de recuperação para pesquisa

Exibe os pontos de recuperação entre o período especificado. É possível especificar a hora de início e de término e, em seguida, selecionar o ponto de recuperação a partir do período especificado.

7. Selecione o ponto de recuperação e clique em **Avançar**.

Observação: se você selecionou um agente diferente na caixa de diálogo **Origem** e se os pontos de recuperação estiverem criptografados, será exibida a caixa de diálogo da criptografia. Digite a senha e clique em **OK**.



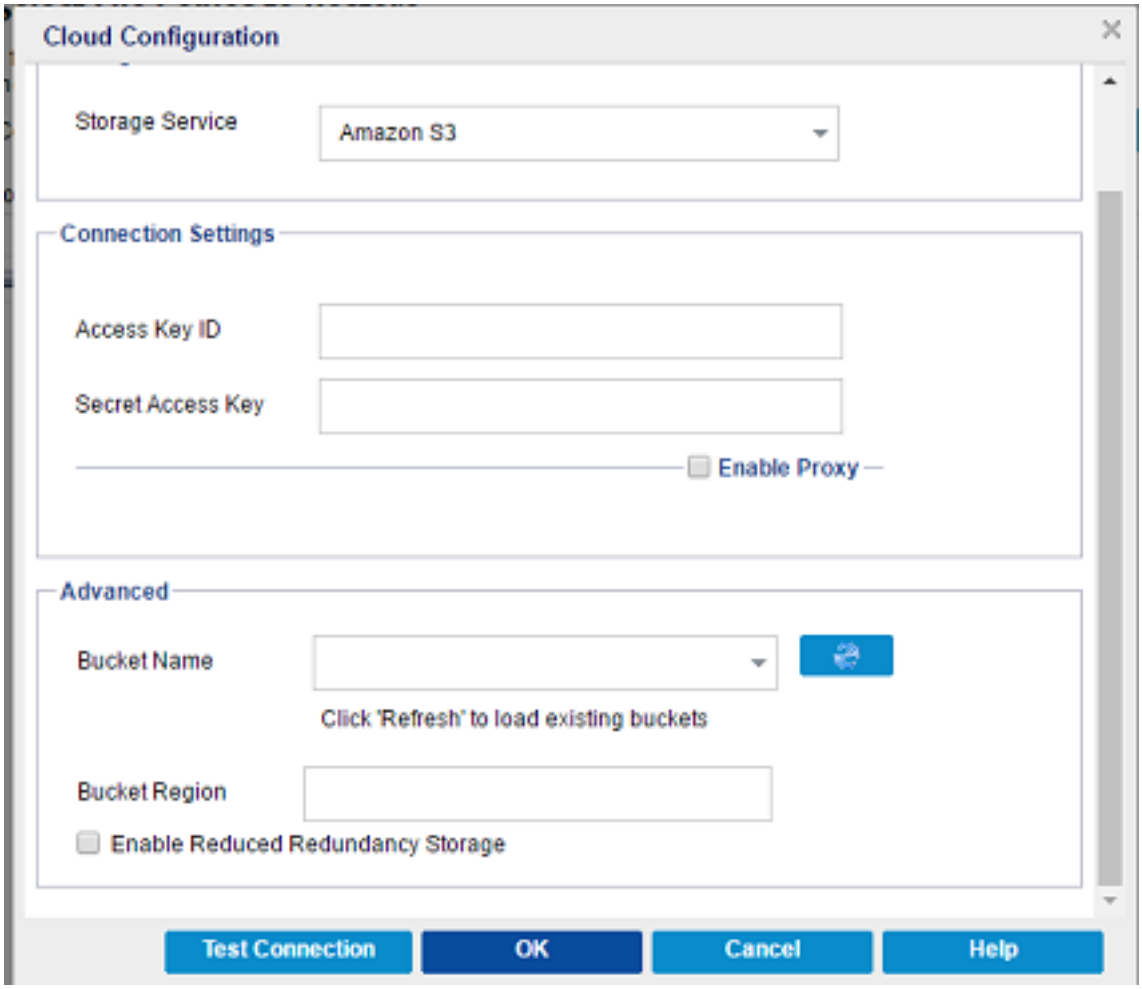
A caixa de diálogo **Localizar arquivos/pastas para restauração** é exibida.

O local do **Backup ou da cópia do arquivo** é especificado.

Especificar configuração de nuvem para restauração

Observação: o procedimento a seguir aplica-se apenas se você estiver restaurando um arquivo/pasta em um local de cópia de arquivo na nuvem.

Na opção **Procurar cópias de arquivo** ou **Localizar arquivos/pastas para restauração**, clique no botão **Configurar** para exibir a caixa de diálogo **Configuração de nuvem**.



Siga estas etapas:

1. Na caixa de diálogo **Configuração da nuvem**, use o menu suspenso para selecionar o tipo de fornecedor de nuvem a partir do qual você deseja restaurar. As opções disponíveis são **Amazon S3**, **Windows Azure**, **FUJITSU Hybrid IT Service FJcloud-O** e **Eucalyptus-Walrus**. (**Amazon S3** é o fornecedor padrão). Para obter mais informações sobre o Fujitsu Cloud (Windows Azure) e o FUJITSU Hybrid IT Service FJcloud-O, consulte Visão geral e Registro.

Observação: após a codificação do nome do compartimento de memória, se o comprimento do caminho for superior a 170 caracteres, o Eucalyptus-Walrus não poderá copiar os arquivos.

2. Especifique as **Opções de configuração**.

   As opções de configuração para cada fornecedor da nuvem são semelhantes (com algumas terminologias distintas), e nenhuma diferença é descrita.

   a. Especifique as **Configurações de conexão**:

      URL do fornecedor

      Identifica o endereço URL do provedor da nuvem.

      Para Amazon S3 e Windows Azure, o URL do fornecedor é pré-preenchido automaticamente. Para Eucalyptus-Walrus, o URL do fornecedor deve ser inserido manualmente usando o formato especificado.

      ID da chave de acesso/nome da conta/ID de consulta

      Identifica o usuário que está solicitando acesso a este local.

      Para esse campo, o Amazon S3 usa a ID da chave de acesso. O Windows Azure e FUJITSU Hybrid IT Service FJcloud-O usam o nome da conta, e o Eucalyptus-Walrus usa a ID da consulta.

      Chave de acesso secreta/chave secreta

      Uma vez que a chave de acesso não está criptografada, esta chave de acesso secreta será uma senha usada para verificar a autenticidade da solicitação para acessar este local.

      Importante: esta chave de acesso secreta é fundamental para manter a segurança de suas contas. É necessário manter as chaves e as credenciais da conta em um local seguro. Não incorpore a chave de acesso secreta em uma página da web ou em outro código-fonte de acesso público e não a transmita em canais não seguros.

      Para esse campo, o Amazon S3 usa a chave de acesso secreta. O Windows Azure, o FUJITSU Hybrid IT Service FJcloud-O e o Eucalyptus-Walrus usam a chave secreta.

      Ativar proxy

      Caso selecione esta opção, será necessário incluir também o endereço IP (ou nome do computador) do servidor proxy e o número da porta correspondente, usado pelo servidor proxy em conexões com a internet. Pode-se também selecionar esta opção se o servidor proxy exigir auten-

ticação. Será necessário fornecer as informações de autenticação correspondentes (nome de usuário e senha) para usar o servidor proxy.

(O recurso proxy não está disponível para Eucalyptus-Walrus).

b. Especifique as **Configurações avançadas**:

Nome do compartimento de memória/Contêiner

Todos os arquivos e as pastas movidos ou copiados para o fornecedor da nuvem são armazenados e organizados nos compartimentos de memória (ou contêineres). Os compartimentos de memória são como um contêiner para os arquivos e são usados para agrupar e organizar objetos. Cada objeto armazenado no fornecedor da nuvem é colocado em um compartimento de memória.

Selecione um nome de compartimento de memória na lista suspensa. Se necessário, você pode clicar no botão **Atualizar** para atualizar a lista de compartimentos de memória disponíveis.

Para esse campo, o Amazon S3 e Eucalyptus-Walrus usam o Nome do compartimento de memória. O Windows Azure e o FUJITSU Hybrid IT Service FJcloud-O usam o recipiente.

Região de compartimento de memória

Refere-se à região de compartimento de memória no Amazon e no FUJITSU Hybrid IT Service FJcloud-O.

Número do contrato

Refere-se ao número do contrato que o FUJITSU Hybrid IT Service FJcloud-O fornece.

ID do projeto

Refere-à ID do projeto que o FUJITSU Hybrid IT Service FJcloud-O gera.

Ativar a redução de armazenamento de dados redundantes

Para Amazon S3 apenas, esta opção permite ativar a RRS (Reduced Redundancy Storage). RRS é uma opção de armazenamento no Amazon S3 que ajuda você a reduzir o custo por meio do armazenamento de dados reproduzíveis não essenciais em níveis de redundância mais baixos do que aqueles do armazenamento padrão do Amazon S3s. As opções de armazenamento padrão e de redução de armazenamento de dados redundantes armazenam dados em vários recursos e dispositivos, mas com a RRS os dados são replicados menos vezes e o custo é menor. Deve-se esperar a mesma latência e taxa de transferência usando o arma-

zenamento padrão ou RRS do Amazon S3. Por padrão, esta opção não está selecionada (o Amazon S3 usa a opção de armazenamento padrão).

3. Clique em **Testar conexão** para verificar a conexão com o local na nuvem especificado.
4. Clique em **OK** para sair da caixa de diálogo **Configuração de nuvem**.

Especificar o arquivo/pasta a ser restaurado

Depois de especificar o local do backup ou da cópia do arquivo, procure o nome do arquivo ou pasta a ser restaurado. Se um arquivo tiver várias versões de cópia, todas as versões serão listadas e classificadas por data (com a mais recente listada primeiro).

Siga estas etapas:

1. Na caixa de diálogo **Localizar arquivos/pastas para restauração**, especifique o que procurar (nome de arquivo ou pasta para restaurar).

   Observação: o campo **Nome do arquivo** oferece suporte à pesquisa de nome completo e à pesquisa com caracteres curinga. Se não souber o nome do arquivo completo, é possível simplificar os resultados da pesquisa especificando os caracteres curinga "*" e "?" no campo Nome de arquivo.

   Os caracteres curinga suportados para o nome de arquivo ou pasta são os seguintes:

   - Use o asterisco para substituir zero ou mais caracteres em um nome de arquivo ou pasta.
   - Use o ponto de interrogação para substituir um único caractere em um nome de arquivo ou pasta.

   Por exemplo, se *.txt for especificado, todos os arquivos com uma extensão de arquivo .txt serão exibidos nos resultados da pesquisa.

2. (Opcional) Especifique um caminho para filtragem adicional de pesquisa e selecione se deseja incluir ou não os subdiretórios.

3. Clique em **Localizar** para iniciar a pesquisa.

   Os resultados da pesquisa são exibidos. Se o arquivo pesquisado possuir várias versões de cópia de arquivo, todas as versões serão listadas e classificadas por data (com a mais recente listada primeiro). Também será indicado se foi feito backup ou cópia do arquivo pesquisado.

4. Selecione a versão (ocorrência) do arquivo/pasta que deseja restaurar e clique em **Avançar**.

   A caixa de diálogo **Opções de restauração** é exibida.

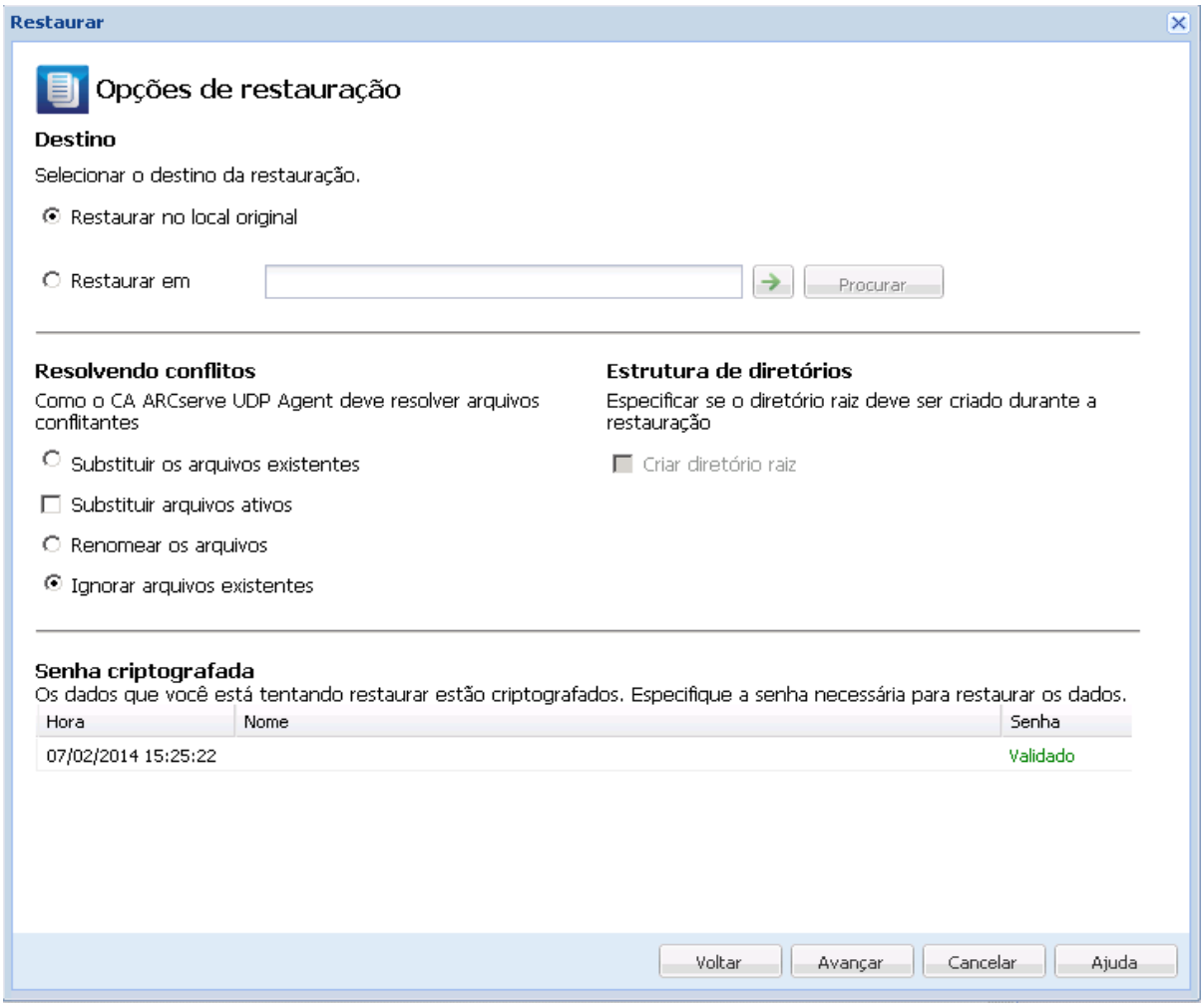
   O nome do arquivo/pasta a ser restaurado é especificado.

Definir as opções de restauração

Depois de especificar o arquivo ou pasta para restaurar, defina as opções de restauração do arquivo ou da pasta selecionada.

Siga estas etapas:

1. Na caixa de diálogo **Opções de restauração**, selecione o destino da restauração.



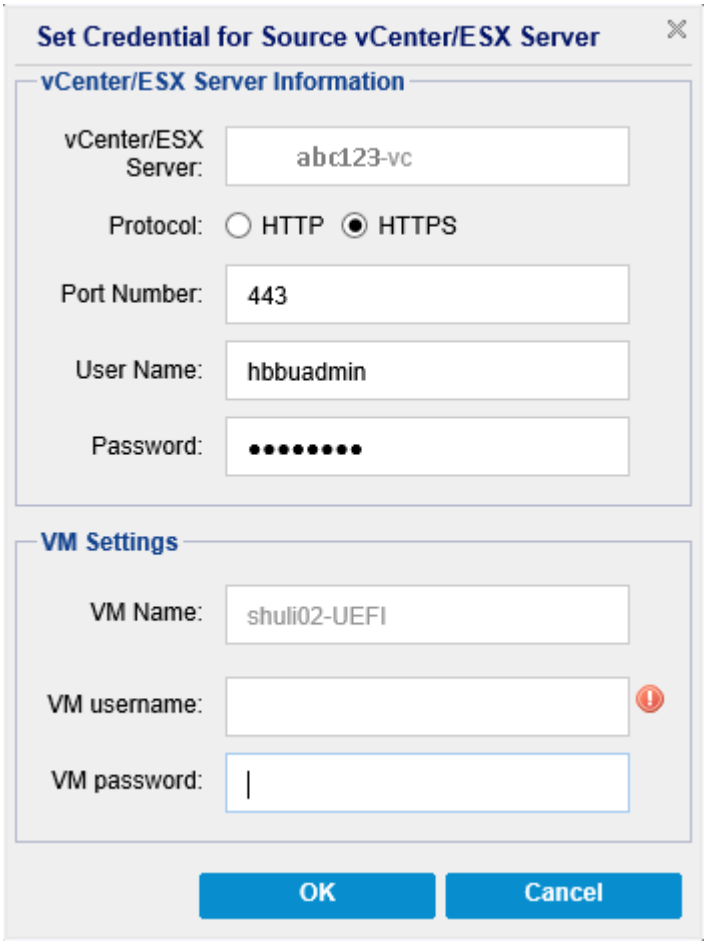
As opções de destino disponíveis são:

Restaurar no local original

Restaura no local original a partir do qual a imagem de backup foi capturada.

Observação: se você tiver feito backup do ponto de recuperação usando o backup sem agente com base em host, a opção Restaurar no local original restaurará o arquivo na máquina virtual. Nesse caso, uma caixa de diálogo abre. Você pode digitar as credenciais do hipervisor e do sistema operacional da máquina virtual.

Para a VM do VMware:



Observação: para criar ou gravar arquivos na VM, considere os seguintes requisitos de configuração e a permissão de conta da máquina virtual:

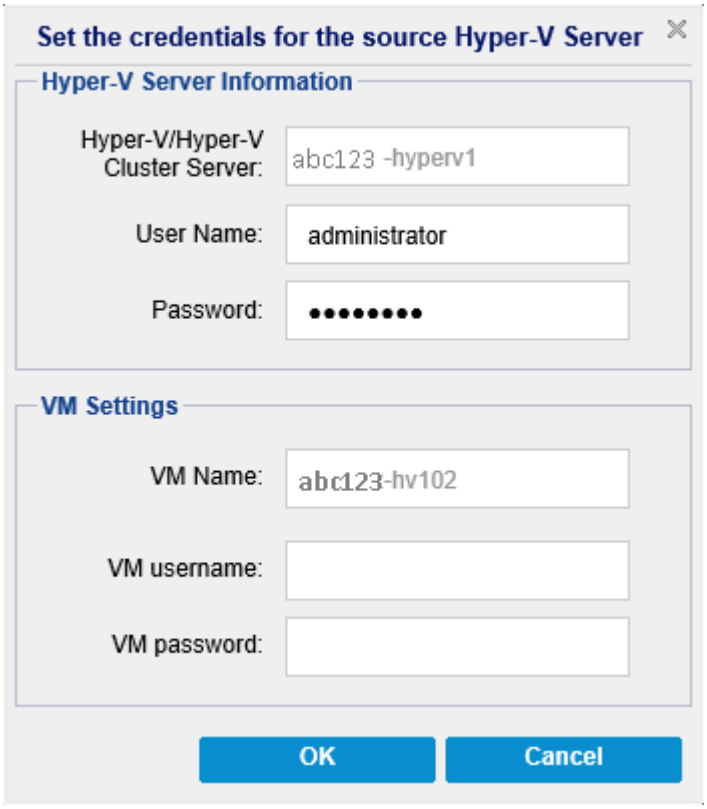
- o VMware Tools está instalado e em execução.
- o Firewall deve permitir que o compartilhamento de arquivo e de impressora.
- A conta é o administrador local internos, o administrador de domínio interno ou conta de domínio que é integrante do grupo de administradores locais. Se forem usadas outras contas:
  - Desative o acesso remoto ao UAC. Para desativar o acesso remoto de UAC, consulte Importar máquina virtual usando a conta

administrativa adicional.

- Desative o UAC na Diretiva de Segurança Local, desativando a configuração Executar todos os administradores no modo de aprovação de administrador em secpol.msc -> Diretivas Locais -> Opções de Segurança. (Secpol.msc é editor da diretiva de segurança da Microsoft).

  Importante: não tente desativar o UAC na caixa de diálogo Configurações de controle de conta do usuário, que é aberta no painel de controle.

Para a VM do Hyper-V:



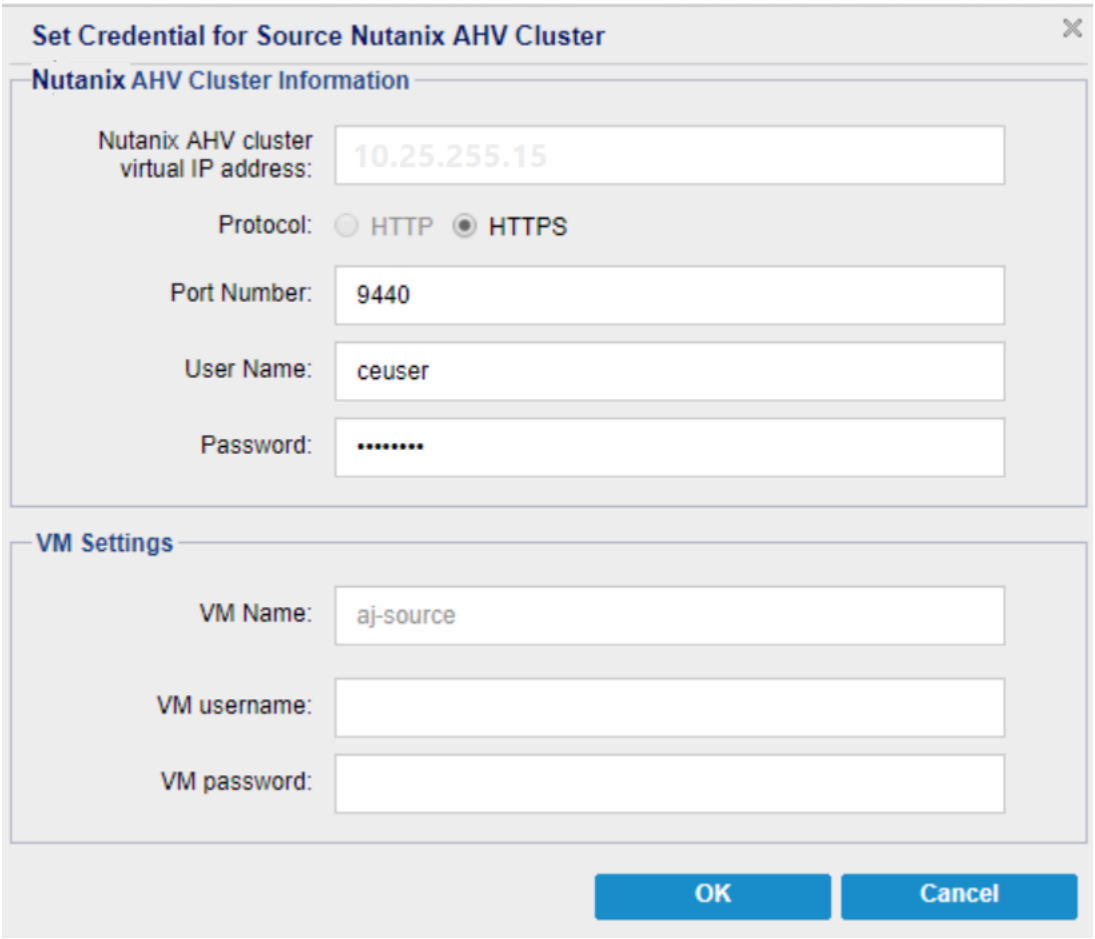
Observação: para criar ou gravar arquivos na VM, considere os seguintes requisitos de configuração e a permissão de conta da máquina virtual:

- os serviços de integração do Hyper-V estão instalados e em execução.
- o Firewall deve permitir que o compartilhamento de arquivo e de impressora.
- A conta é o administrador local internos, o administrador de domínio interno ou conta de domínio que é integrante do grupo de administradores locais. Se forem usadas outras contas:

Desative o acesso remoto ao UAC. Para desativar o acesso remoto de UAC, consulte Importar máquina virtual usando a conta administrativa adicional.

- Se o sistema operacional convidado da máquina virtual for a versão de cliente do Windows (por exemplo, o Windows 10), será necessário configurar manualmente o firewall para permitir a WMI (Windows Management Instrumentation - Instrumentação de Gerenciamento do Windows).

Para a VM do Nutanix



Observações: para conseguir criar ou gravar arquivos na VM, considere os seguintes requisitos de configuração e permissão de conta da máquina virtual:

- o Firewall deve permitir que o compartilhamento de arquivo e de impressora.
- A conta é o administrador local internos, o administrador de domínio interno ou conta de domínio que é integrante do grupo de administradores locais. Se forem usadas outras contas:

Desative o acesso remoto ao UAC. Para desativar o acesso remoto de UAC, consulte Importar máquina virtual usando a conta administrativa adicional.

- O firewall deve permitir a WMI (Windows Management Instrumentation - Instrumentação de Gerenciamento do Windows).

Restaurar para

Restaura no local especificado. É possível clicar no botão com a seta verde para verificar a conexão com o local especificado. Se necessário, forneça as credenciais de nome de usuário e senha para acessar esse local.

2. Especifique a opção **Resolvendo conflitos** que o Arcserve UDP executará se forem encontrados conflitos durante o processo de restauração.

   As opções disponíveis são:

   Substituir arquivos existentes

   Sobrescreve (substitui) qualquer arquivo existente que está localizado no destino da restauração. Todos os objetos serão restaurados dos arquivos de backup, independentemente da presença atual deles no computador.

   Substituir os arquivos ativos

   Substitui todos os arquivos ativos ao reinicializar. Se, durante a tentativa de restauração, o agente do Arcserve UDP (Windows) detectar que o arquivo existente está em uso ou sendo acessado, para evitar erros, ele não substituirá o arquivo imediatamente, só depois que o computador for reinicializado. (A restauração ocorrerá imediatamente, mas a substituição de arquivos ativos é feita durante a próxima reinicialização).

   Essa opção só estará disponível se você selecionar a opção **Substituir os arquivos existentes**.

   Observação: se essa opção não estiver selecionada, qualquer arquivo ativo será ignorado na restauração.

   Renomear arquivos

   Cria um novo arquivo se o nome de arquivo já existir. A seleção desta opção copia o arquivo de origem no destino com o mesmo nome de arquivo, mas com uma extensão diferente. Os dados serão restaurados no novo arquivo.

   Ignorar arquivos existentes

   Ignora e não substitui (sobrescreve) os arquivos localizados no destino da restauração. Apenas os objetos inexistentes em seu computador no momento serão restaurados dos arquivos de backup.

   Padrão: Ignorar arquivos existentes.

3. Especifique a **Estrutura de diretórios** para criar um diretório raiz durante a restauração.

   Criar diretório raiz

   Especifica que se uma estrutura de diretórios raiz existir na imagem de backup capturada, o Arcserve UDP recriará a mesma estrutura de diretórios raiz no caminho de destino de restauração.

   Se essa opção não for selecionada, o arquivo ou pasta será restaurado diretamente para a pasta de destino.

   Por exemplo, se durante o backup você capturou os arquivos "C:\Pasta1\Subpasta2\A.txt" e "C:\Pasta1\Subpasta2\B.txt" e durante a restauração foi especificado como destino o local "D:\Restore".

   - Se você optar por restaurar os arquivos "A.txt" e "B.txt" individualmente, o destino dos arquivos restaurados será "D:\Restore\A.txt" e "D:\Restore\B.txt" (o diretório raiz acima do nível de arquivo especificado não será recriado).
   - Se você optar por restaurar a partir do nível da "Subpasta2", o destino dos arquivos restaurados será "D:\Restore\Subpasta2\A.txt" e "D:\Restore\Subpasta2\B.txt" (o diretório acima do nível de pasta especificado não será recriado).

   Com esta opção selecionada, todo o caminho de diretório raiz para os arquivos / pastas (incluindo o nome de volume) é recriado até a pasta de destino. Se os arquivos/pastas a serem restaurados tiverem o mesmo nome de volume, o caminho do diretório raiz de destino não incluirá esse nome de volume. No entanto, se os arquivos/pastas a serem restaurados forem de nomes de volume diferentes, o caminho do diretório raiz do destino incluirá o nome do volume.

   Por exemplo, se durante o backup você capturou os arquivos "C:\Pasta1\Subpasta2\A.txt", "C:\Pasta1\Subpasta2\B.txt" e também "E:\Pasta3\Subpasta4\C.txt" e durante a restauração foi especificado como destino de restauração o local "D:\Restore".

   - Se você optar por restaurar apenas o arquivo "A.txt", o destino do arquivo restaurado será "D:\Restore\Pasta1\Subpasta2\A.txt" (o diretório raiz inteiro, sem o nome do volume, será recriado).
   - Se você optar por restaurar tanto o arquivo "A.txt" como o "C.txt", o destino dos arquivos restaurados será "D:\Restore\C\Pasta1\Subpasta2\A.txt" e "D:\Restore\E\Pasta3\Subpasta4\C.txt" (o diretório raiz inteiro, com o nome do volume, será recriado).

4. A **Senha criptografada** para o destino da cópia de arquivo é carregada automaticamente. Caso selecione um destino alternativo para a restauração, é necessário digitar a senha manualmente.
5. Clique em **Avançar**.

   A caixa de diálogo **Resumo da restauração** é exibida.

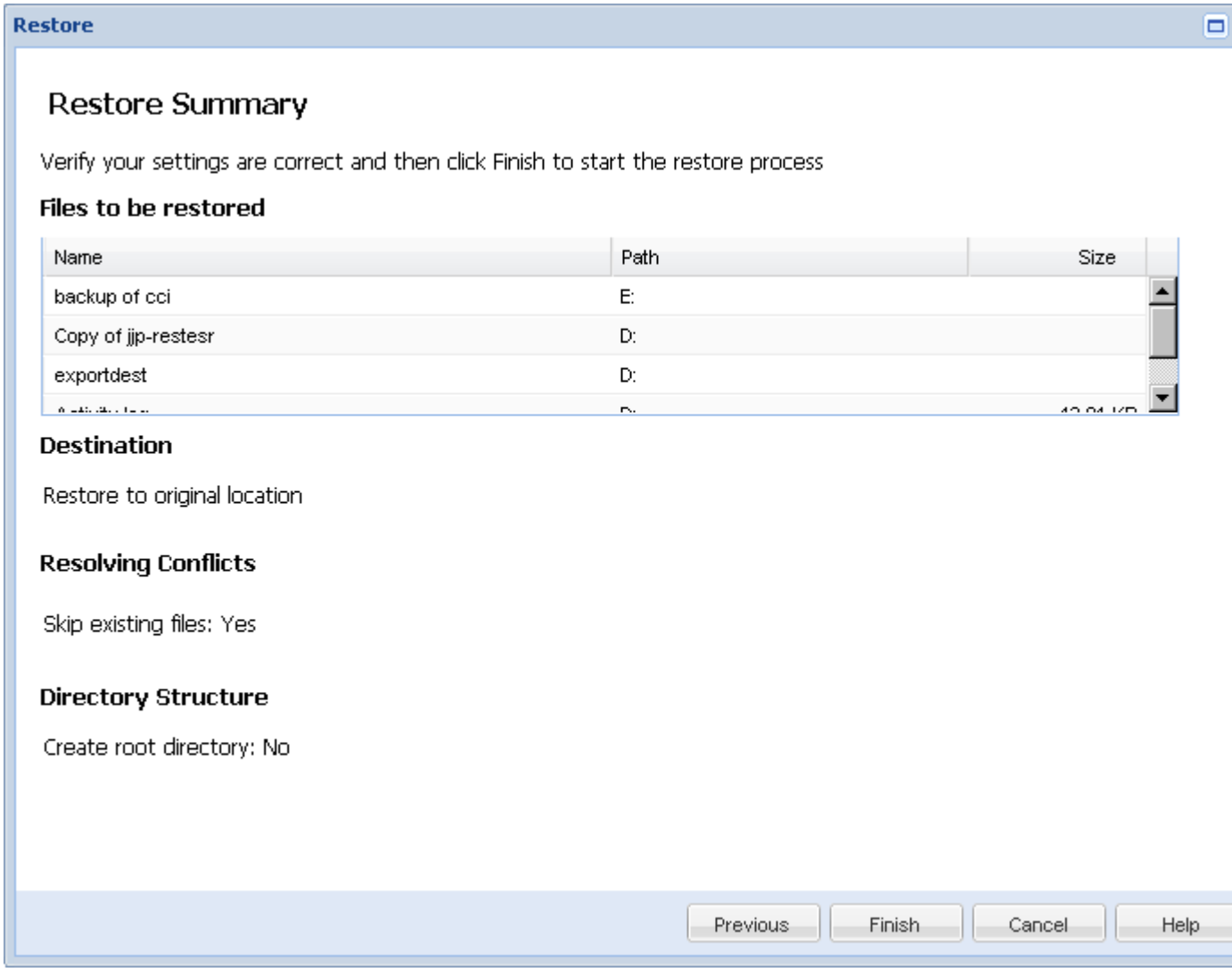
   As opções de restauração são definidas para restaurar o arquivo/pasta especificado.

Restaurar o arquivo/pasta

O **Resumo da restauração** ajuda a examinar todas as opções de restauração definidas anteriormente e permite modificá-las, se necessário.

Siga estas etapas:

1. Na caixa de diálogo **Resumo da restauração**, examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.



- Se as informações do resumo não estiverem corretas, clique em **Anterior** e volte à caixa de diálogo em questão para alterar a configuração incorreta.
- Se as informações de resumo estiverem corretas, clique em **Concluir** para iniciar o processo de restauração.

O arquivo/pasta especificado é restaurado.

Verificar se o arquivo/pasta foi restaurado

Após a conclusão do processo de restauração, verifique se o arquivo/pasta foi restaurado no destino especificado.

Siga estas etapas:

1. Navegue até o destino de restauração especificado.

   É exibida uma lista de pastas.

2. Localize o arquivo para o qual tiver restaurado o conteúdo.

   Por exemplo, se você selecionar para restaurar o arquivo A.txt no destino de restauração como D:\Restore, navegue até o seguinte local:

   D:\Restore\A.txt.

3. Verifique o conteúdo do arquivo/pasta restaurado.

   A restauração do conteúdo é verificada com êxito.

Como executar uma recuperação bare metal usando uma VM no modo de espera virtual ou VM instantânea

A BMR (Bare Metal Recovery - Recuperação Bare Metal) é o processo de restauração de um sistema de computador a partir do estado bare metal, incluindo a reinstalação do sistema operacional e dos aplicativos de software e, em seguida, a restauração dos dados e das configurações. O processo de BMR permite a restauração completa de um computador com o mínimo de esforço, até mesmo para um hardware diferente. A BMR é possível porque durante o processo de backup em nível de bloco, o agente do Arcserve UDP (Windows) não captura apenas os dados, mas também todas as informações relacionadas aos seguintes aplicativos:

- Sistema operacional
- Aplicativos instalados
- Configurações
- Drivers necessários

  Para todas as informações relevantes, necessárias à execução de uma recompilação completa do sistema a partir do estado bare metal, é feito backup em uma série de blocos, os quais são armazenados no local do backup.

Para executar uma BMR a partir de uma máquina virtual, siga um destes procedimentos:

- Estabelecer conexão com o servidor ESX usando diretamente o endereço IP
- Adicionar a configuração correta de DNS em seu computador de BMR e resolver o nome do host para o endereço IP

Conclua as tarefas a seguir para executar uma BMR usando uma VM de espera virtual ou VM instantânea:

1. Rever os pré-requisitos e considerações da BMR
2. Definir as opções da BMR
   - Recuperar usando uma VM no modo de espera virtual do Hyper-V ou uma VM instantânea
   - Recuperar usando uma VM no modo de espera virtual do VMware ou uma VM instantânea
   - Executar a BMR em modo expresso
   - Executar a BMR em modo avançado

3. Verificar se a BMR foi bem-sucedida
4. Informações de referência da BMR
5. Solução de problemas da BMR

Rever os pré-requisitos e considerações da BMR

Verifique se os pré-requisitos a seguir existem antes de executar uma BMR:

- Você deve possuir uma das seguintes imagens:
  - Uma imagem ISO criada da BMR gravada em um CD/DVD
  - Uma imagem ISO criada da BMR gravada em um dispositivo USB portátil

  Observação: o agente do Arcserve UDP (Windows) utiliza um Utilitário do kit de Inicialização para combinar uma imagem do WinPE e uma imagem do agente do Arcserve UDP (Windows) para criar uma imagem ISO da BMR. Em seguida, essa imagem ISO é gravada em uma mídia inicializável. Dessa maneira, você pode usar qualquer uma dessas mídias inicializáveis (CD/DVD ou dispositivo USB) para inicializar o novo sistema do computador e permitir que o processo de recuperação bare metal seja iniciado. Para garantir que a imagem salva seja sempre a versão mais atualizada, crie uma nova imagem ISO sempre que você atualizar o agente do Arcserve UDP (Windows).
- Ao menos um backup completo disponível.
- Uma RAM de ao menos 1 GB instalada na máquina virtual e o servidor de origem que se está recuperando.
- Para recuperar máquinas virtuais VMware para máquinas virtuais VMware configuradas para se comportarem como servidores físicos, verifique se o VMware Tools está instalado na máquina virtual de destino.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Revise as seguintes considerações de restauração:

- Independentemente do método usado para criar a imagem do kit de inicialização, o processo de BMR é basicamente o mesmo.

  Observação: Não é possível criar espaços de armazenamento por meio do processo de BMR. Se o computador de origem tinha espaço de armazenamento, não será possível criar espaços de armazenamento no computador de destino durante a BMR. Você pode restaurar os volumes em discos/volumes regulares ou criar manualmente espaços de armazenamento antes de executar a BMR e, em seguida, restaurar os dados nesses espaços de armazenamento criados.
- Discos dinâmicos serão restaurados somente no nível do disco. Se o backup dos dados for feito no volume local de um disco dinâmico, você não poderá restaurar este disco durante a BMR. Nesse cenário, para fazer uma restauração durante uma BMR, é preciso executar uma das tarefas abaixo e, em seguida,

realizar a BMR a partir do ponto de recuperação copiado:

- Faça backup em um volume em outra unidade.
- Faça backup em um compartilhamento remoto.
- Copie um ponto de recuperação em outro local.

Observação: se executar uma BMR com vários discos dinâmicos, ela pode falhar devido a alguns erros inesperados (como falha na inicialização, volumes dinâmicos não reconhecidos e assim por diante). Se isso ocorrer, será necessário restaurar somente o disco do sistema usando a BMR e, em seguida, após a reinicialização do computador, será possível restaurar os outros volumes dinâmicos em um ambiente normal.

- Se você tentar executar uma BMR em uma VM do Hyper-V com um disco de 4 KB, adicione esse disco de 4 KB ao controlador SCSI. Se você adicioná-lo ao controlador IDE, o disco não será detectado no sistema do Windows PE.
- (Opcional) Rever as informações de referência da BMR. Para obter mais informações, consulte os tópicos a seguir:
  - Como a recuperação bare metal funciona
  - Sistemas operacionais que oferecem suporte à conversão de UEFI/BIOS
  - Gerenciando o menu de operações de BMR

Revise as seguintes considerações:

- Se você atualizar para uma versão ou atualização mais recente do Arcserve UDP, deve recriar o ISO da BMR usando o nível do Windows AIK ou ADK apropriado para incluir suporte para os recursos e as correções de erro mais recentes. No entanto, depois que BMR ISO é criado, o arquivo ISO pode ser usado para o mesmo nível de sistema operacional. Os seguintes níveis de sistema operacional podem usar o mesmo ISO:
  - ISO criado usando o Windows 7 WAIK – funciona para o Windows 2003, Vista, 2008, 2008 R2
  - ISO criado usando o Windows 8/8.1 ADK – funciona para o Windows 8, 8.1, Server 2012, Server 2012 R2
  - ISO criado usando o Windows 10 ADK – funciona para o Windows 10

Definir as opções da BMR

Antes de iniciar o processo da BMR, especifique algumas opções preliminares da BMR.

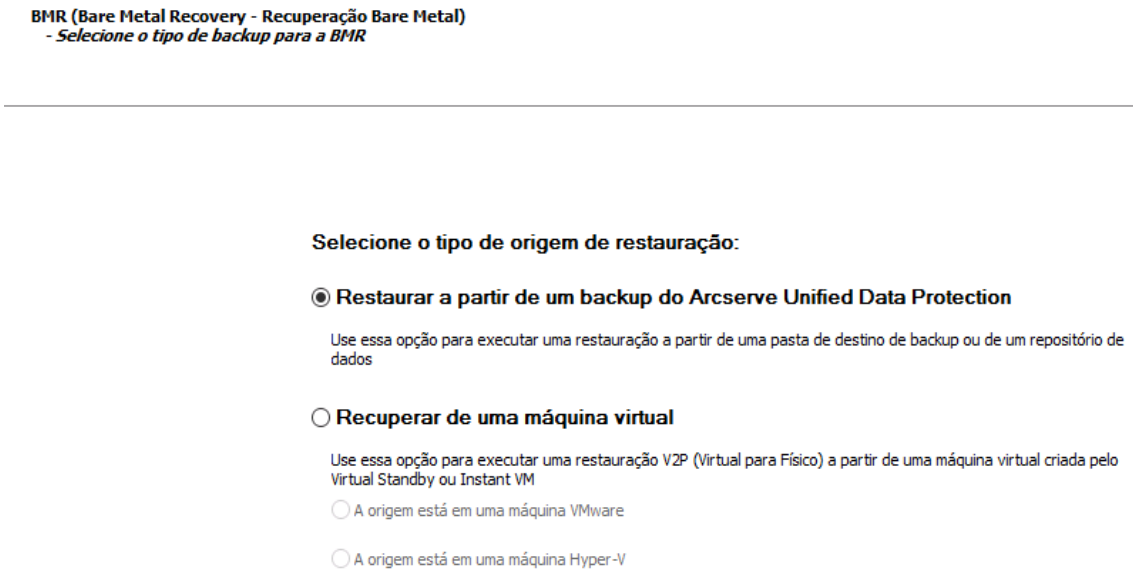
Siga estas etapas:

1. Insira a mídia da imagem do kit de inicialização salva e inicialize o computador.
   - Se estiver usando uma imagem ISO da BMR gravada em um CD/DVD, insira o CD/DVD.
   - Se estiver usando uma imagem ISO da BMR gravada em um dispositivo USB, insira o dispositivo USB.

   A tela do **Utilitário de instalação do BIOS** é exibida.
2. Na tela do **Utilitário de instalação do BIOS**, selecione a opção da unidade de CD-ROM ou a opção de USB para iniciar o processo de inicialização. Selecione uma arquitetura (x86/x64) e pressione **Enter** para continuar.

   A tela de seleção de idioma do Agente do Arcserve UDP (Windows) é exibida.
3. Selecione um idioma e clique em **Avançar** para continuar.

O processo de recuperação bare metal é iniciado, e a tela do assistente da BMR inicial é exibida.



A tela do assistente da BMR permite que você selecione o tipo de BMR que deseja executar:

- **Restaurar a partir de um backup do Arcserve Unified Data Protection**

  Use essa opção para executar uma restauração a partir de uma pasta de destino do backup ou de um repositório de dados.

  Essa opção permite recuperar dados cujo backup foi feito usando o Agente do Arcserve UDP (Windows). Essa opção é usada junto com sessões de backup realizadas com o Agente do Arcserve UDP (Windows) ou com o aplicativo de backup de VM com base em host do Arcserve UDP.

  Para obter mais informações, consulte Como executar uma recuperação bare metal usando um backup na ajuda online.

- **Recuperação de uma VM no modo de espera virtual**

  Use essa opção para executar uma restauração V2P (Virtual-to-Physical – Virtual para Física) a partir de uma VM no modo de espera virtual ou VM instantânea. V2P (Virtual-to-Physical) é um termo que se refere à migração de um SO (Sistema Operacional), aplicativos e dados de uma de máquina virtual ou partição de disco para o disco rígido principal de um computador. O destino pode ser um único computador ou vários computadores.

- **A origem está em uma máquina VMware**

  Permite recuperar dados de uma máquina cuja conversão virtual é executada em uma máquina virtual do VMware. Essa opção é usada junto com o aplicativo de VM no modo de espera virtual ou VM instantânea do Arcserve Central.

  Observação: nessa opção, só é possível recuperar dados se a conversão virtual para um arquivo VMDK (para VMware) foi executada usando uma VM no modo de espera virtual ou VM instantânea do Arcserve Central.

  Se você selecionar essa opção, consulte o tópico Recuperação usando-se uma VM instantânea ou no modo de espera virtual da VMware para continuar com este procedimento.

- **A origem está em uma máquina Hyper-V**

  Permite recuperar dados de uma máquina virtual cuja conversão é executada em uma máquina virtual do Hyper-V. Essa opção é usada junto com o aplicativo de VM no modo de espera virtual ou VM instantânea do Arcserve Central.

  Observação: nessa opção, só é possível recuperar dados se a conversão virtual para um arquivo VHD (para Hyper-V) foi executada usando uma VM no modo de espera virtual ou VM instantânea do Arcserve Central.

  Se você selecionar essa opção, consulte o tópico Recuperação usando-se uma VM instantânea ou no modo de espera virtual do Hyper-V para continuar com este procedimento.

4. Selecione **Recuperação de uma VM no modo de espera virtual**. Em seguida, selecione uma das origens a seguir.

   Se selecionar a opção **Origem está em um computador VMware**, consulte Recuperar usando uma VM no modo de espera virtual do VMware ou VM instantânea para continuar este procedimento.

   Se selecionar a opção **Origem está em um computador Hyper-V**, consulte Recuperar usando uma VM instantânea e no modo de espera virtual do Hyper-V para continuar este procedimento.

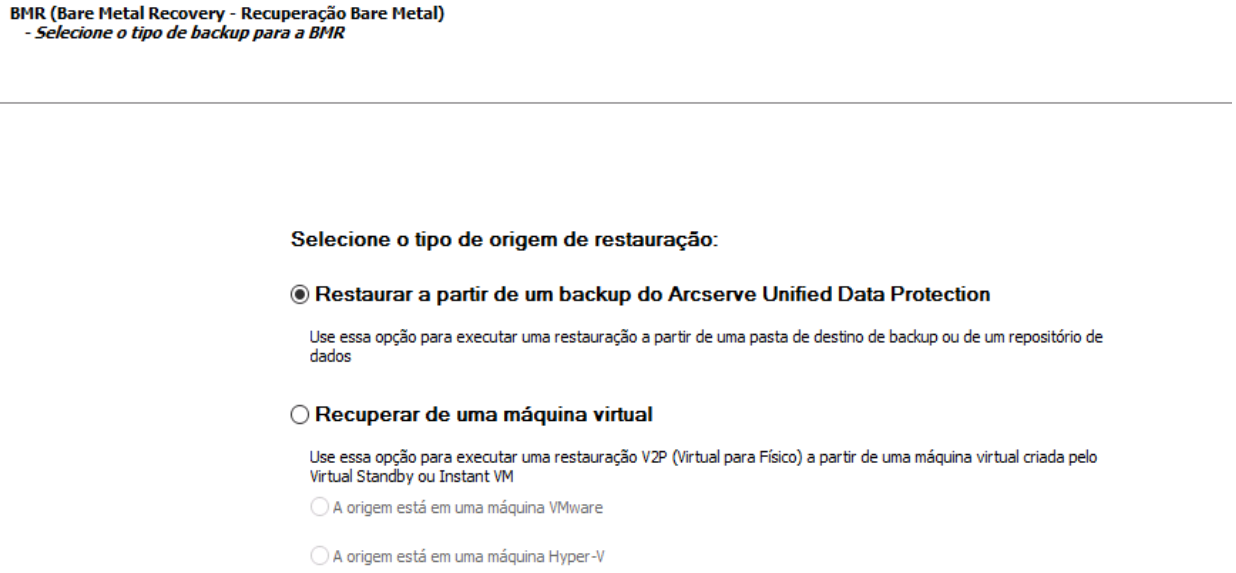
Recuperar usando uma VM no modo de espera virtual do Hyper-V ou uma VM instantânea

O agente do Arcserve UDP (Windows) oferece o recurso de executar a recuperação bare metal de computadores V2P (Virtual to Physical – Virtual para Físico). Este recurso permite executar recuperação virtual para física a partir do último estado de uma máquina virtual instantânea ou no modo de espera e ajuda a reduzir a perda de produção de sua máquina.

Siga estas etapas:

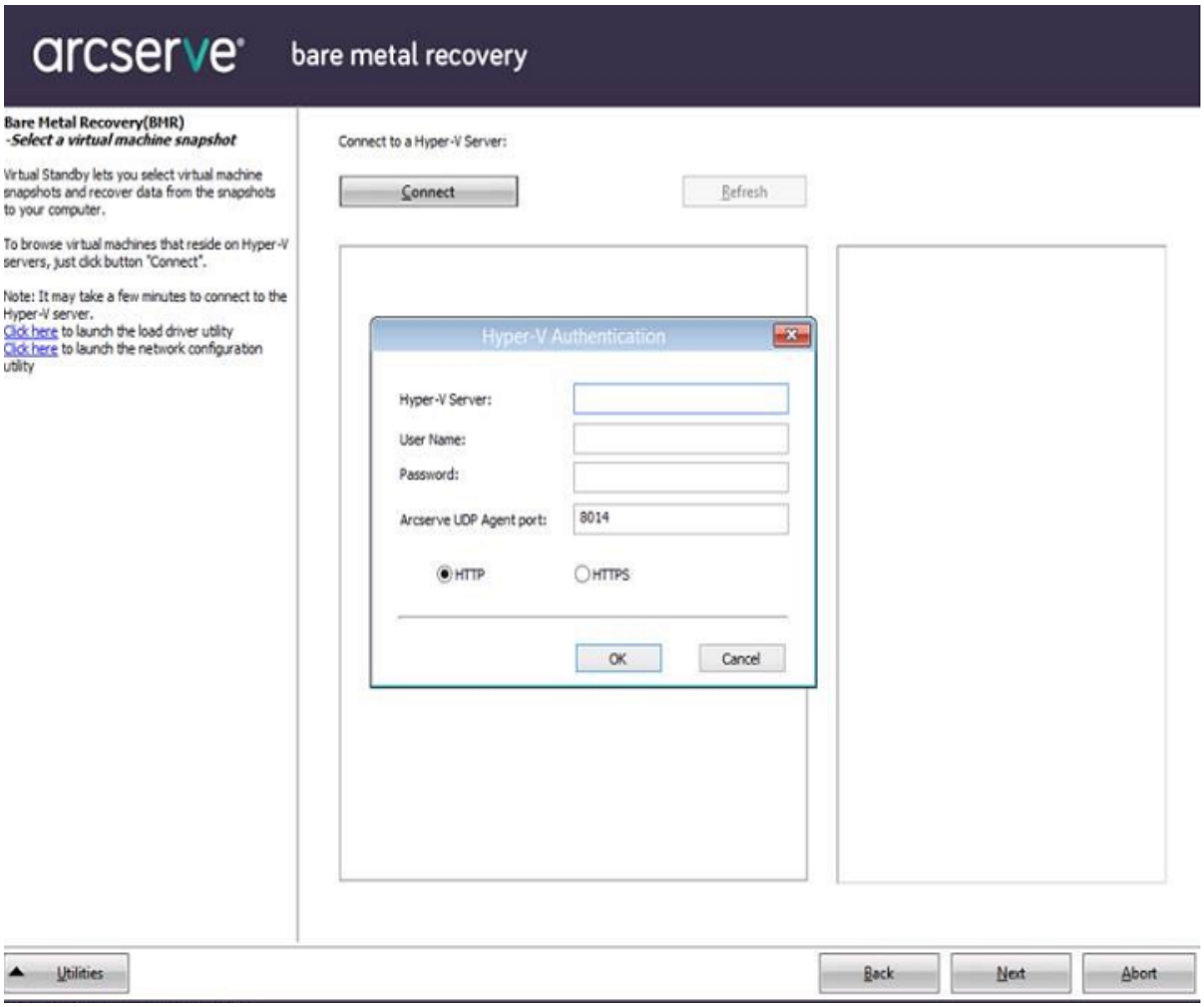
1. Na tela do assistente, selecione o tipo de BMR (Bare-Metal Recovery – Recuperação Bare Metal), selecione **Recuperação de uma VM no modo de espera virtual** e, em seguida, selecione a opção **A origem está em uma máquina Hyper-V**.

   Use essa opção para executar uma restauração V2P (Virtual-to-Physical – Virtual para Física) de uma VM instantânea ou VM no modo de espera virtual. O termo virtual para físico se refere à migração de um SO (Sistema Operacional), programas de aplicativos e dados de uma de máquina virtual ou partição de disco para um disco rígido principal de um computador. O destino pode ser um único computador ou vários computadores.



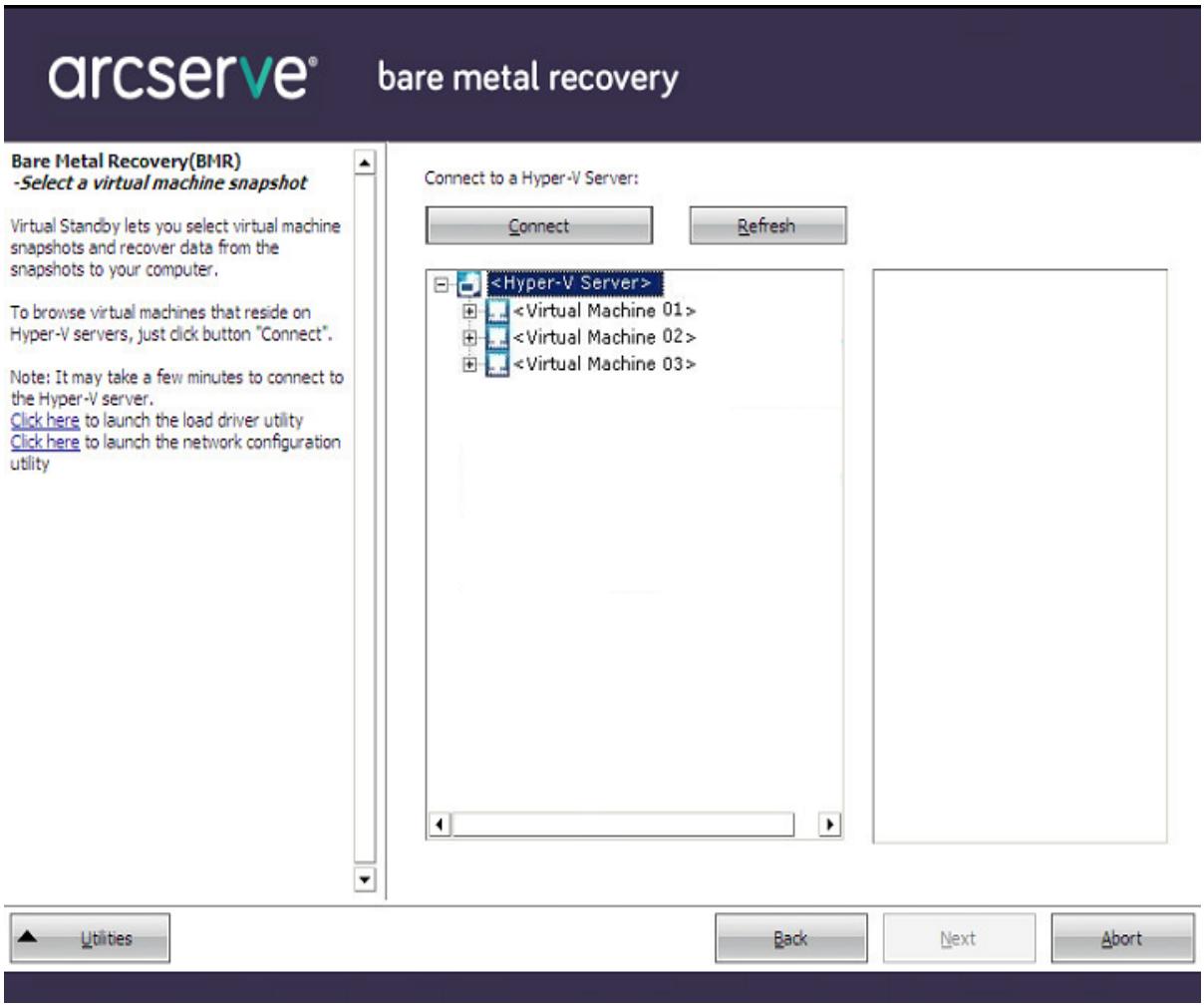
2. Clique em **Avançar**.

   A tela Selecione o instantâneo de uma máquina virtual é exibida, com a caixa de diálogo autenticação do Hyper-V, solicitando detalhes do servidor do Hyper-V.



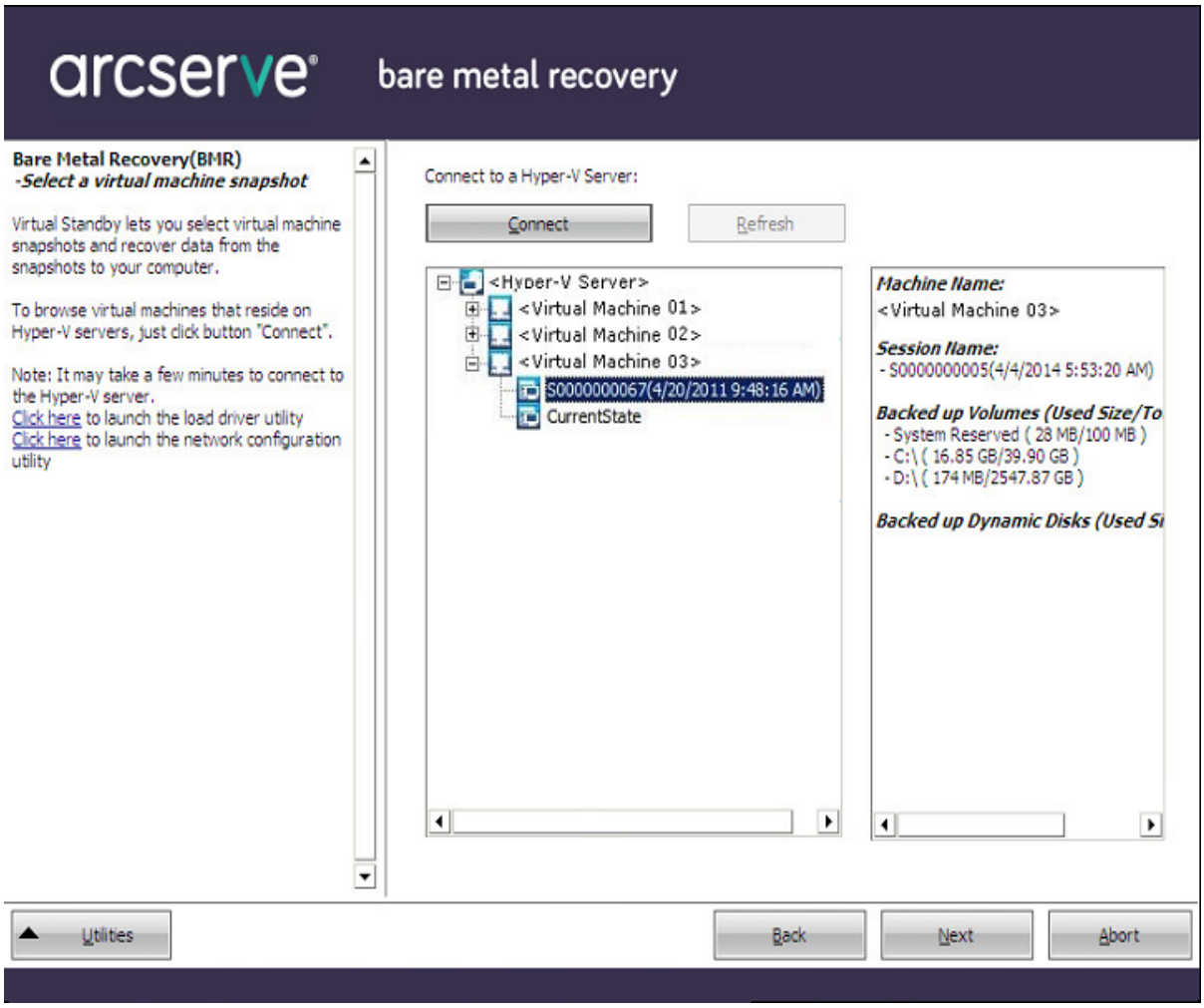
3. Digite as informações de autenticação e clique em **OK**.

   O Agente do Arcserve Unified Data Protection para Windows detecta e exibe o servidor do Hyper-V com uma lista de todas as máquinas virtuais que são convertidas no servidor do Hyper-V especificado usando o Arcserve Central Virtual Standby ou uma VM instantânea.



4. Selecione a máquina virtual que contém os instantâneos do ponto de recuperação para a imagem de backup.

   As sessões de backup (instantâneos do ponto de recuperação) da máquina virtual selecionada são exibidas.



5. Selecione a sessão de backup da máquina virtual (instantâneo do ponto de recuperação) que deseja recuperar.

   Os detalhes correspondentes do instantâneo do ponto de recuperação selecionado (nome da máquina virtual, nome da sessão de backup, volumes armazenados em backup) são exibidos no painel direito.

   Além disso, para selecionar um dos pontos de recuperação relacionados, também é possível selecionar o ponto de recuperação **Estado atual** ou **Estado mais recente**.

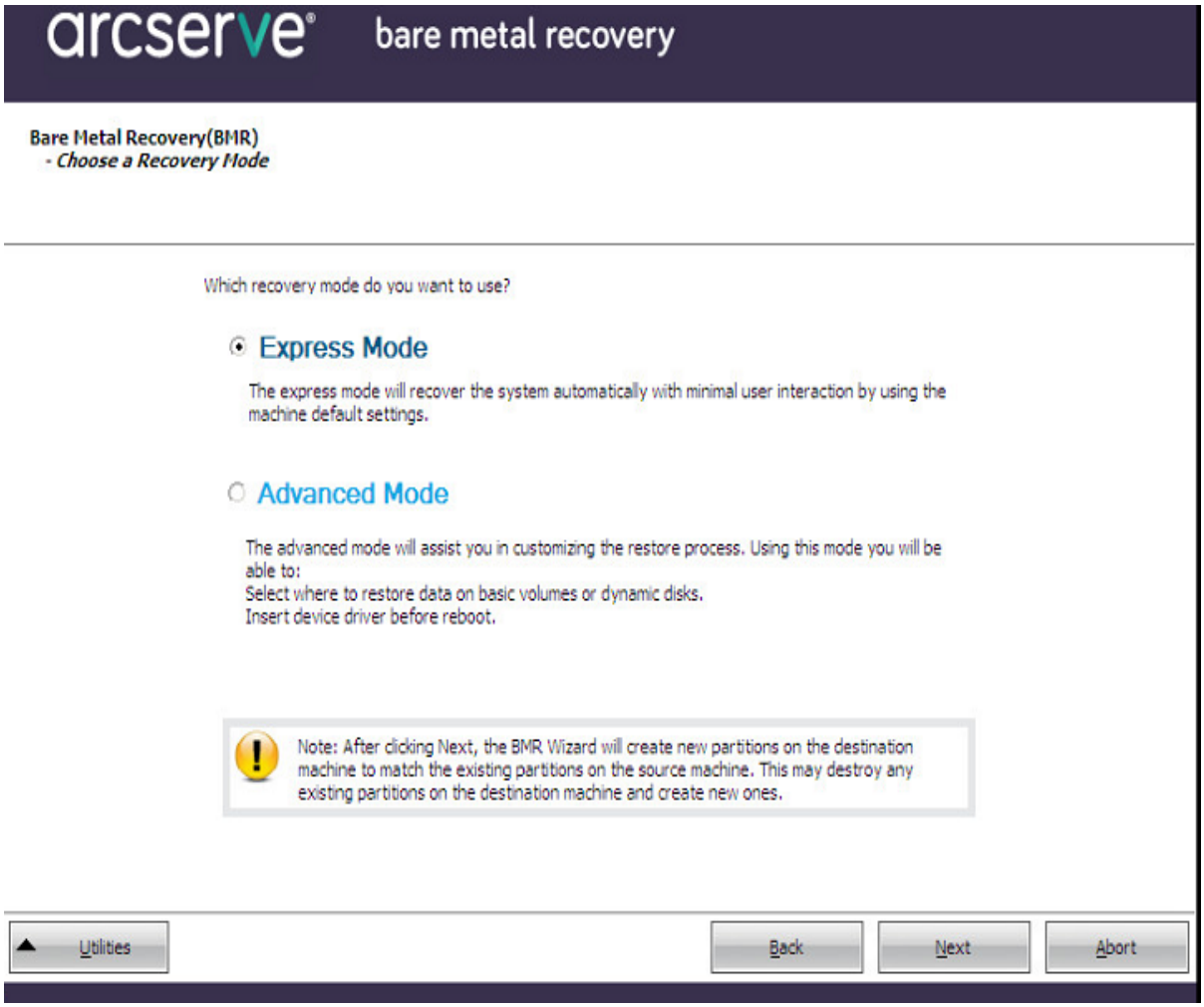
   - Se a máquina virtual que está recuperando estiver ligada, o ponto de recuperação **Estado atual** será exibido.

     Observação: se a máquina virtual estiver ligada, as alterações de dados feitas na máquina virtual após o início do processo de BMR não serão recuperadas.

   - Se a máquina virtual que está recuperando estiver desligada, o ponto de recuperação **Estado mais recente** será exibido.

6. Verifique se este é o ponto de recuperação que deseja restaurar e clique em **Avançar**.

   Uma tela do assistente de BMR é exibida com as opções disponíveis do modo de recuperação.



   As opções disponíveis são **Modo avançado** e **Modo expresso**.

   - Selecione **Modo expresso** se desejar o mínimo de interação durante o processo de recuperação. Para obter mais informações, consulte Executar BMR no modo expresso.
   - Selecione **Modo avançado** se desejar personalizar o processo de recuperação. Para obter mais informações, consulte Executar BMR no modo avançado.

   Padrão: Modo expresso.

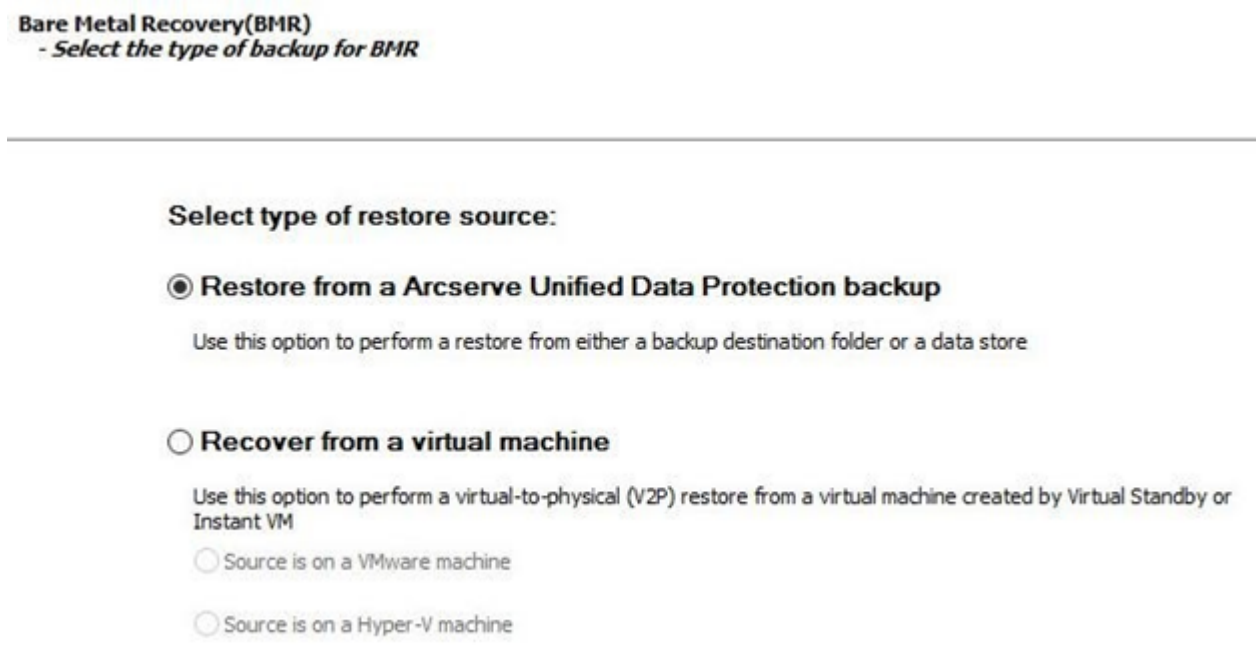
Recuperar usando uma VM no modo de espera virtual do VMware ou uma VM instantânea

O agente do Arcserve UDP (Windows) oferece o recurso de executar a recuperação bare metal de computadores V2P (Virtual to Physical – Virtual para Físico). Este recurso permite executar recuperação virtual para física a partir do último estado de uma máquina virtual no modo de espera e ajuda a reduzir a perda de produção de sua máquina.

Siga estas etapas:

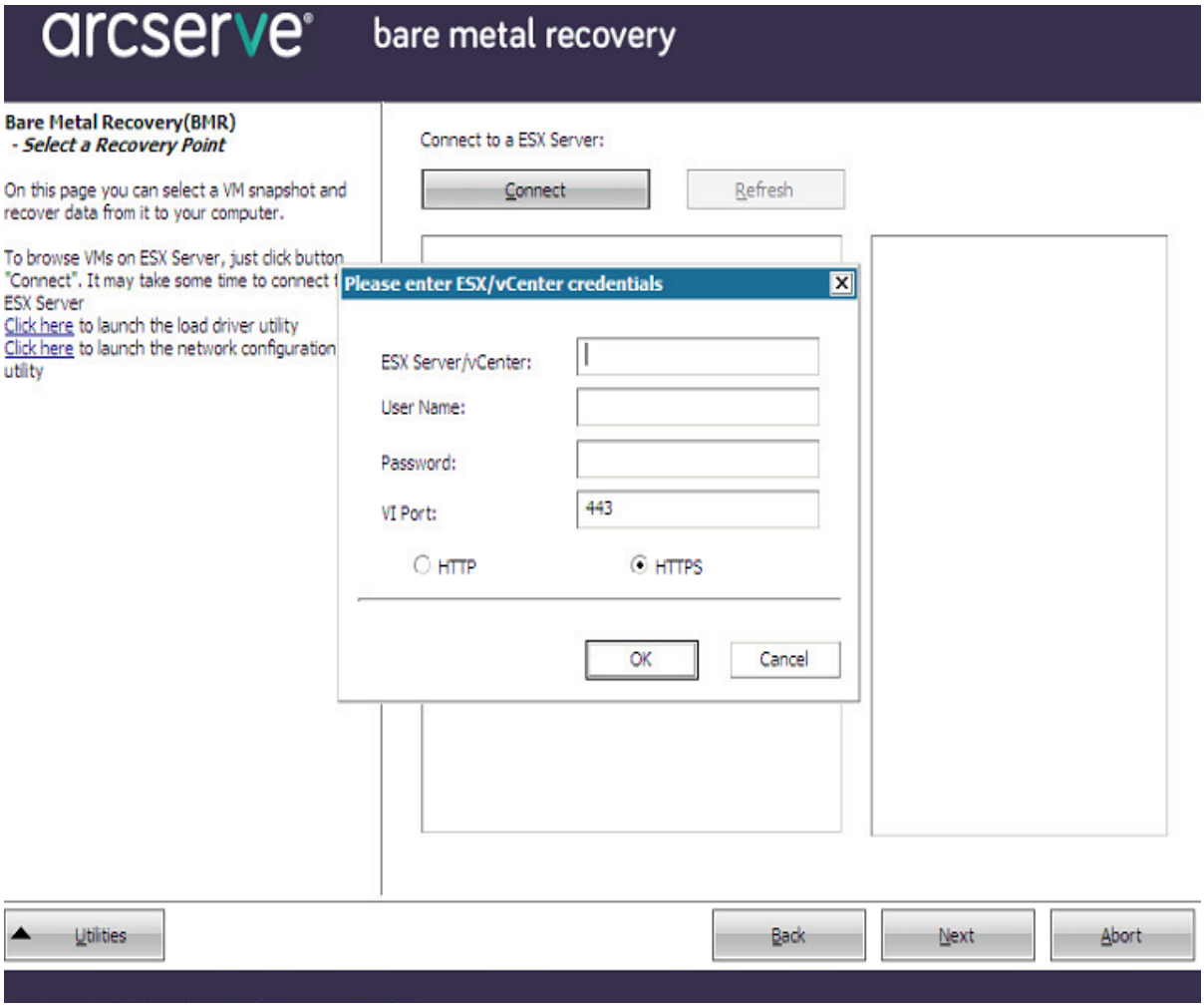
1. Na tela do assistente, selecione o tipo de BMR (Bare-Metal Recovery – Recuperação Bare Metal), selecione **Recuperação de uma máquina virtual** e, em seguida, selecione a opção **A origem está em um computador VMware**.

   Use essa opção para executar uma restauração V2P (Virtual-to-Physical – Virtual para Física) de uma VM instantânea ou VM no modo de espera virtual. O termo virtual para físico se refere à migração de um SO (Sistema Operacional), programas de aplicativos e dados de uma de máquina virtual ou partição de disco para um disco rígido principal de um computador. O destino pode ser um único computador ou vários computadores.



2. Clique em **Avançar**.

   A tela **Selecionar um ponto de recuperação** é exibida com a caixa de diálogo **Credenciais do ESX/VC**.



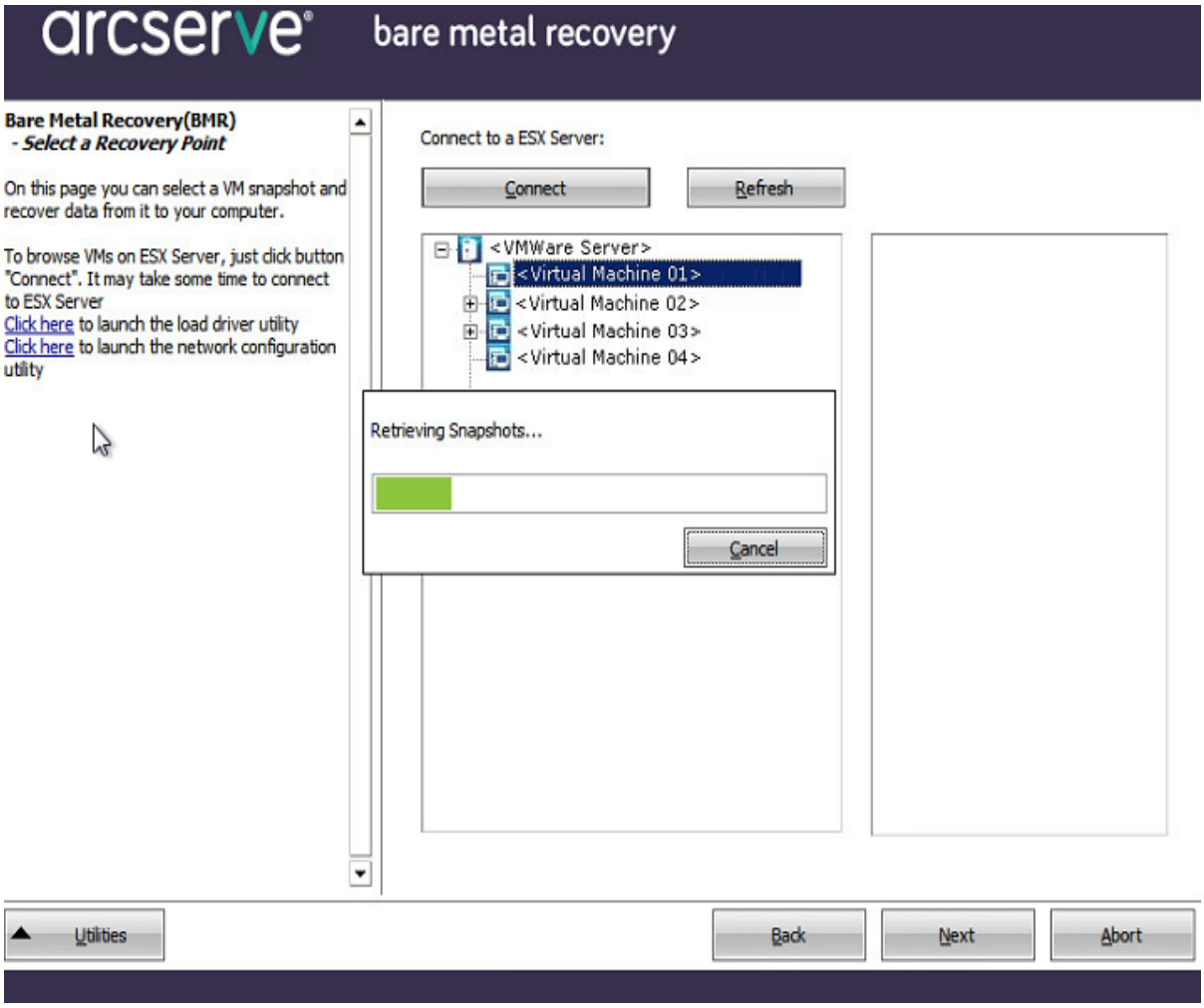
3. Digite as informações da credencial e clique em **OK**.

   Observação: se estiver se conectando a um vCenter, não precisará de permissão no nível do vCenter Server, mas deverá ter a permissão Administrator no nível do Datacenter. Além disso, você deve ter as seguintes permissões no nível do vCenter Server:

   - Global, DisableMethods e EnableMethods
   - Global, License

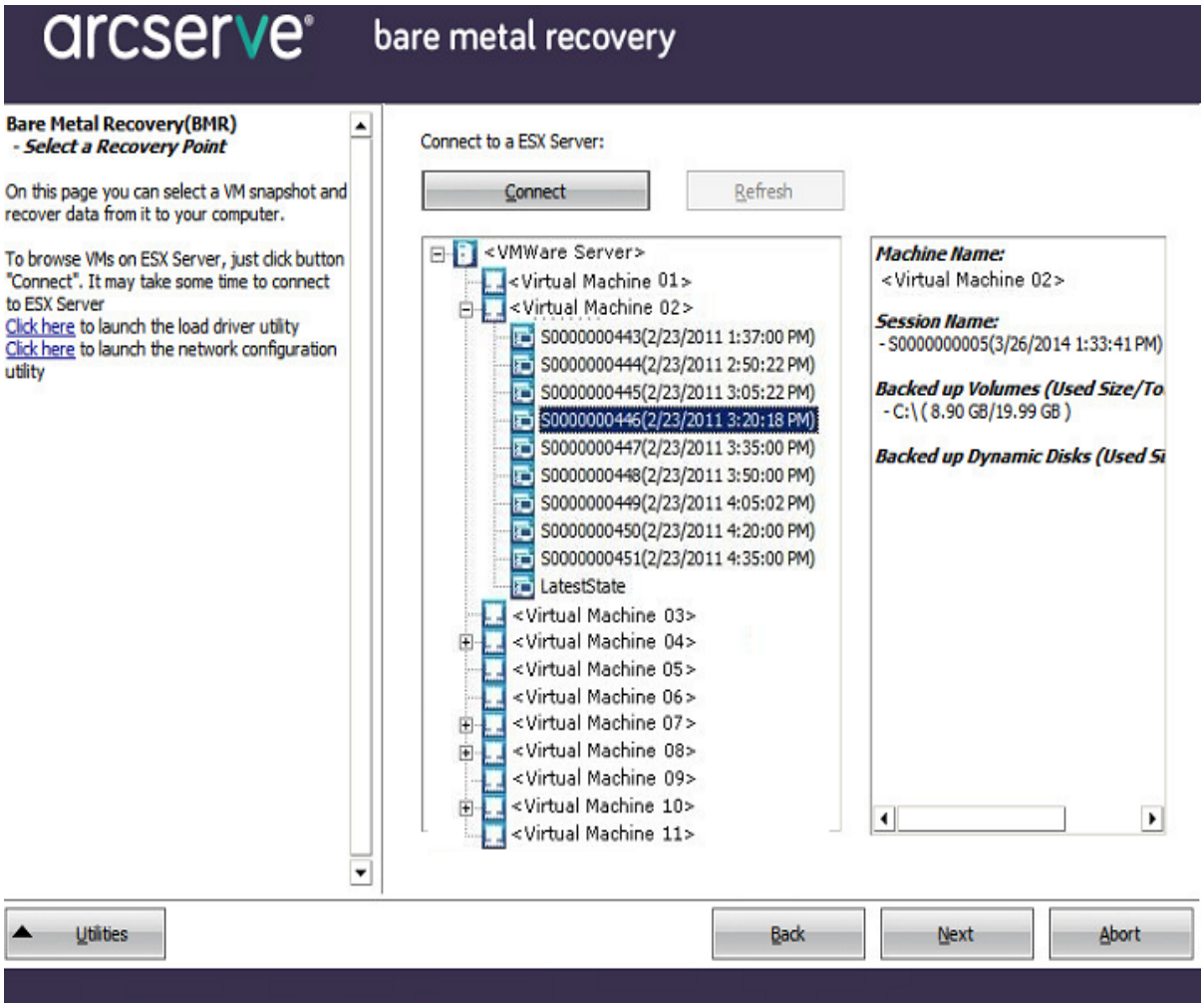
   A tela **Selecionar ponto de recuperação** é exibida.

   O Agente do Arcserve Unified Data Protection para Windows recupera todos os instantâneos do ponto de recuperação do servidor VMware selecionado e exibe o servidor VMware no painel à esquerda, com uma lista de todas as máquinas virtuais hospedadas no servidor VMware selecionado.



4. Selecione a máquina virtual que contenha pontos de recuperação da imagem de backup.

   As sessões de backup (instantâneos do ponto de recuperação) da máquina virtual selecionada são exibidas.



5. Selecione a sessão de backup da máquina virtual (instantâneos do ponto de recuperação) que deseja recuperar.

   Os detalhes correspondentes do instantâneo do ponto de recuperação selecionado (nome da máquina virtual, nome da sessão de backup, volumes armazenados em backup, discos dinâmicos com backup realizado) são exibidos no painel direito.

   Além disso, para selecionar um dos pontos de recuperação relacionados, também é possível selecionar o ponto de recuperação **Estado atual** ou **Estado mais recente**.

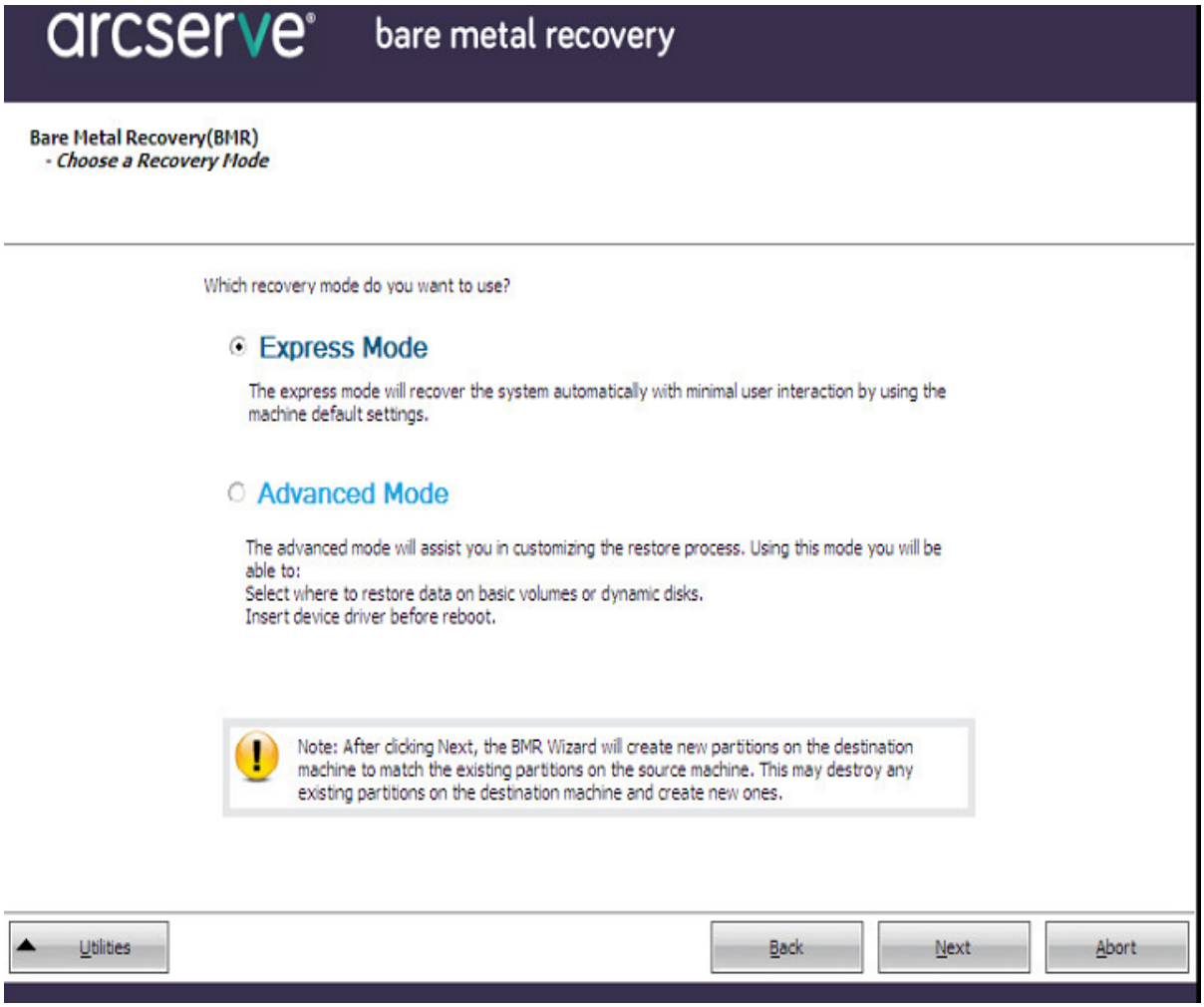
   - Se a máquina virtual que está recuperando estiver ligada, o ponto de recuperação **Estado atual** será exibido.

     Observação: se a máquina virtual estiver ligada, as alterações de dados feitas na máquina virtual após o início do processo de BMR não serão recuperadas.

   - Se a máquina virtual que está recuperando estiver desligada, o ponto de recuperação **Estado mais recente** será exibido.

6. Verifique se este é o ponto de recuperação que deseja restaurar e clique em **Avançar**.

   Uma tela do assistente de BMR é exibida com as opções disponíveis do modo de recuperação.



   As opções disponíveis são **Modo avançado** e **Modo expresso**.

   - Selecione **Modo expresso** se desejar o mínimo de interação durante o processo de recuperação. Para obter mais informações, consulte Executar BMR no modo expresso.
   - Selecione **Modo avançado** se desejar personalizar o processo de recuperação. Para obter mais informações, consulte Executar BMR no modo avançado.

   Padrão: Modo expresso.

Executar a BMR em modo expresso

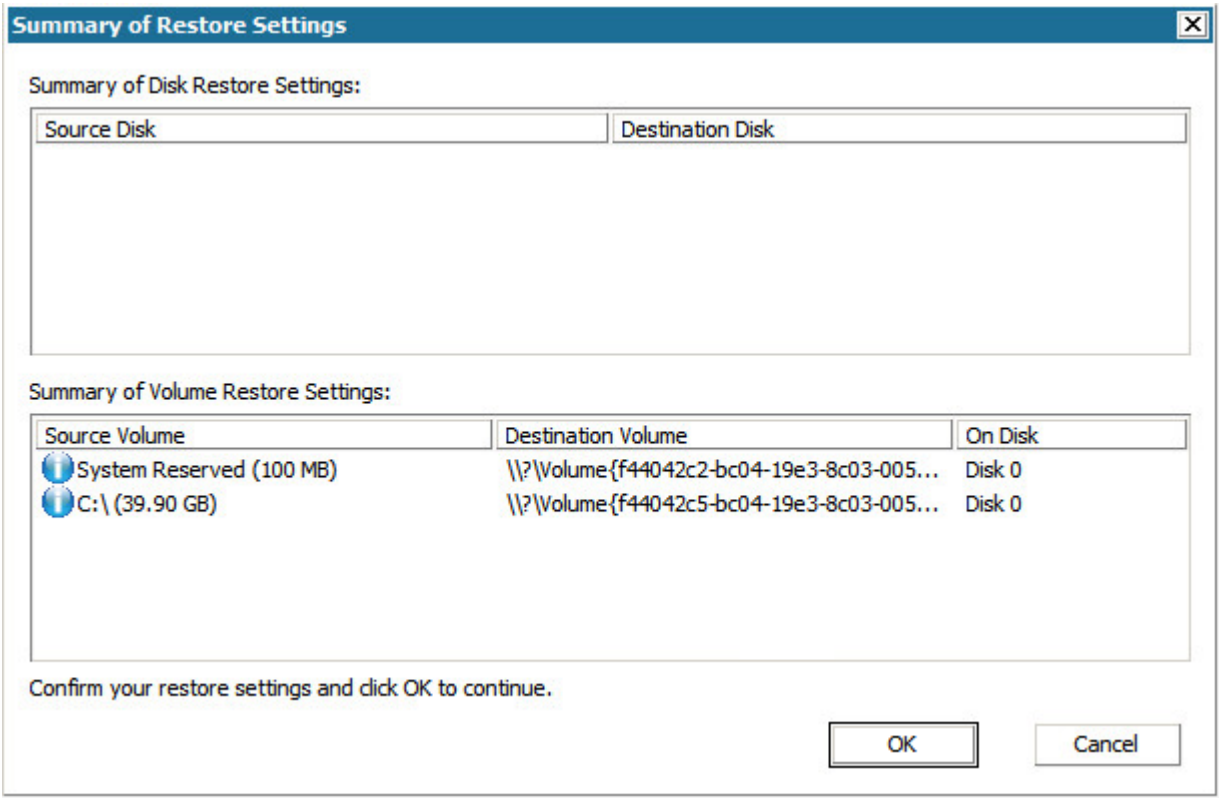
O **Modo expresso** requer pouca interação durante o processo de recuperação.

Siga estas etapas:

1. Na caixa de diálogo **Selecionar um modo de recuperação**, selecione o **Modo expresso** e clique em **Avançar**.

   A tela **Resumo das configurações de restauração do disco** é exibida, mostrando um resumo dos volumes a serem restaurados.

   Observação: na parte inferior da janela de resumo da restauração, as letras de unidade listadas na coluna **Volume de destino** são geradas automaticamente do WinPE (Windows Preinstallation Environment – Ambiente de Pré-Instalação do Windows). Elas podem ser diferentes das letras das unidades listadas na coluna **Volume de origem**. No entanto, os dados serão restaurados no volume apropriado, mesmo quando as letras forem diferentes.



2. Após verificar se as informações de resumo estão corretas, clique em **OK**.

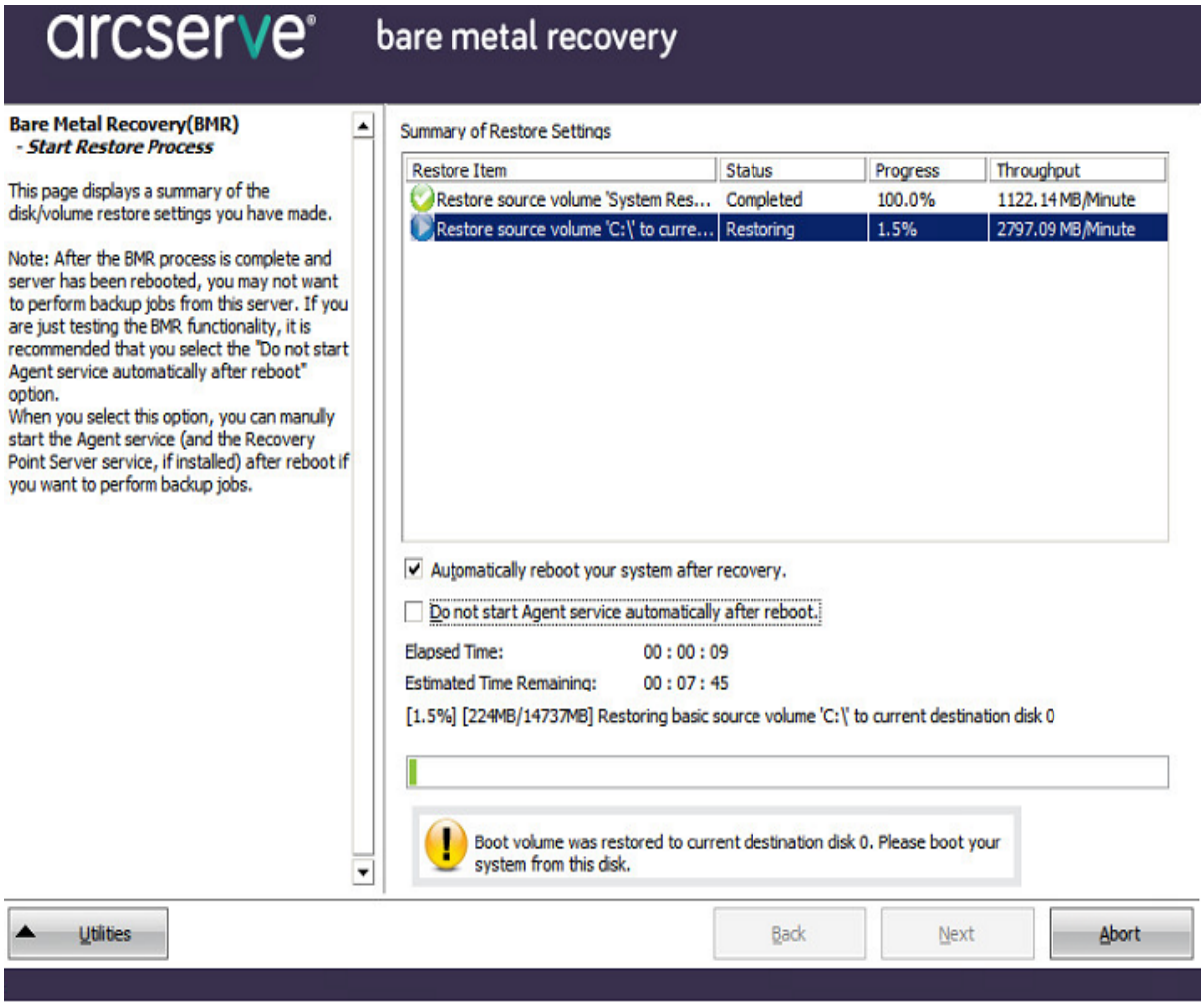
   O processo de restauração é iniciado. A tela do assistente de BMR exibe o status da restauração para cada volume.

   - Dependendo do tamanho do volume sendo restaurado, essa operação pode levar algum tempo

- Durante este processo, você estará restaurando bloco por bloco tudo o que tiver sido armazenado em backup para esse ponto de recuperação e criando uma réplica do computador de origem no computador de destino.
- Por padrão, a opção que permite reiniciar o sistema automaticamente depois da recuperação é selecionada. Se necessário, você pode desmarcar esta opção e reinicializar manualmente mais tarde.

  Importante: Se estiver executando uma restauração autoritativa de um Active Directory após BMR, é necessário desmarcar a opção **Reiniciar o sistema automaticamente depois da recuperação** e, para obter mais informações, consulte Como realizar uma restauração autoritativa de um Active Directory após BMR.

  - Se necessário, é possível selecionar Do not start Agent service automatically after reboot.
  - Se necessário, é possível cancelar ou anular a operação a qualquer momento.



3. No menu **Utilitários**, é possível acessar o **Log de atividades** da BMR e usar a opção **Salvar** para salvar o Log de atividades.

   Por padrão, o log de atividades será salvo no seguinte local:

   X:\windows\system32\dr\log.

   Observação: para evitar um erro gerado pelo Windows, não salve o Log de atividades na área de trabalho ou crie uma pasta na área de trabalho usando a opção **Salvar como**, na janela Log de atividades da BMR.

4. Caso esteja restaurando em diferentes tipos de hardware (o adaptador SCSI/FC usado para conectar unidades de disco rígido pode ter sido alterado) e nenhum driver compatível tenha sido detectado no sistema original, uma página de injeção de drivers será exibida para permitir o fornecimento de drivers a esses dispositivos.

   Procure e selecione os drivers a serem injetados no sistema recuperado de forma que, mesmo se estiver fazendo a recuperação em um computador com tipos diferentes de hardware, ainda seja possível trazer o computador de volta após a BMR.

5. Quando o processo de BMR for concluído, uma notificação de confirmação é exibida.

Executar a BMR em modo avançado

O **Modo Avançado** permite personalizar o processo de recuperação.

Siga estas etapas:

1. Na caixa de diálogo **Selecionar um modo de recuperação**, selecione **Modo avançado** e clique em **Avançar**.

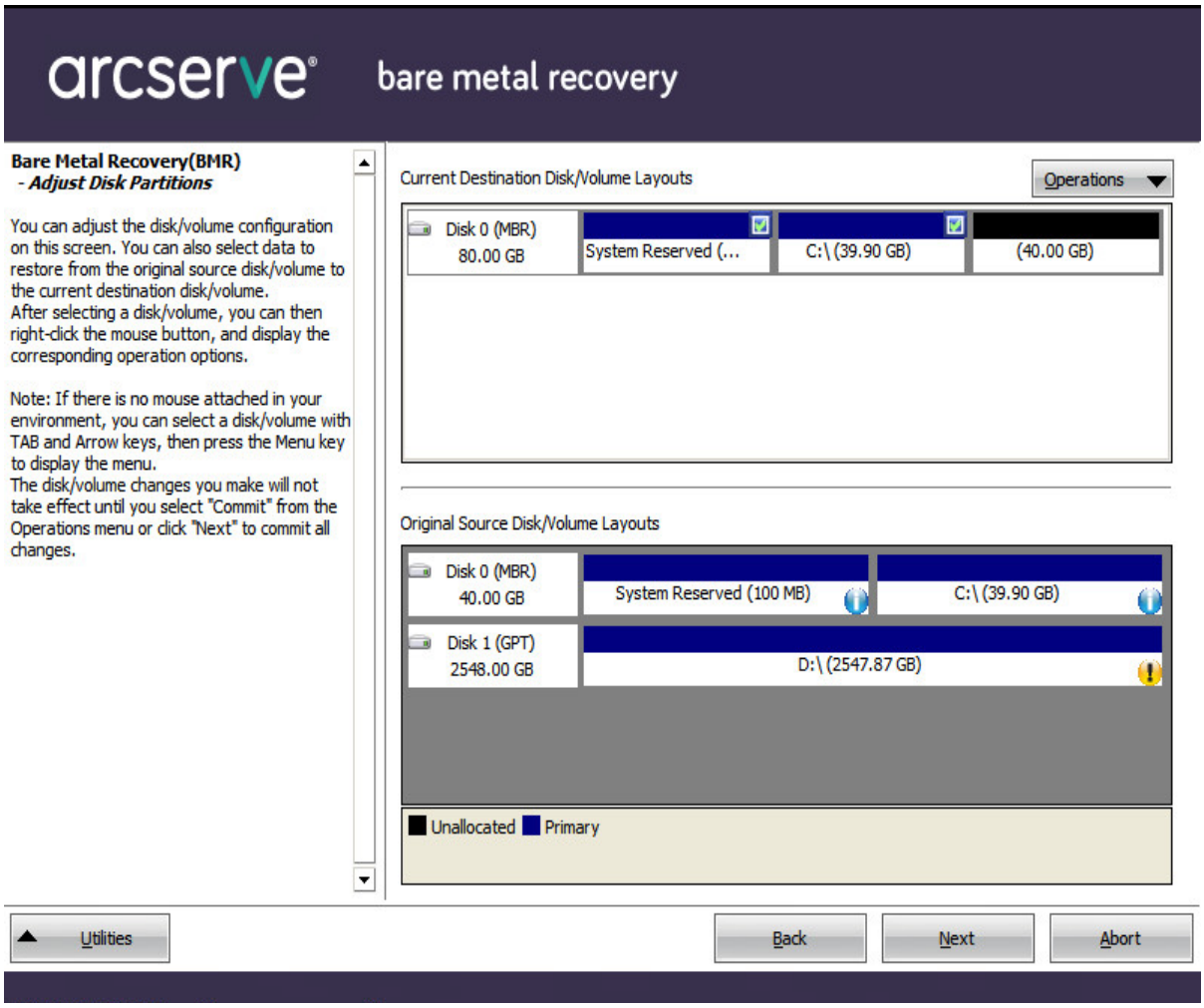
   O utilitário BMR inicia localizando o computador a ser recuperado e exibe as informações da partição de disco correspondente.

   O painel superior mostra a configuração de disco que você possui no computador atual (destino) e o painel inferior mostra as informações da partição de disco que havia no computador original (origem).

   Importante: um ícone vermelho em forma de X exibido para um volume de origem no painel inferior indica que o volume contém informações do sistema e não foi atribuído (mapeado) ao volume de destino. O volume contendo informações do sistema do disco de origem deve ser atribuído ao disco de destino e restaurado durante a BMR, caso contrário, haverá falha na reinicialização.

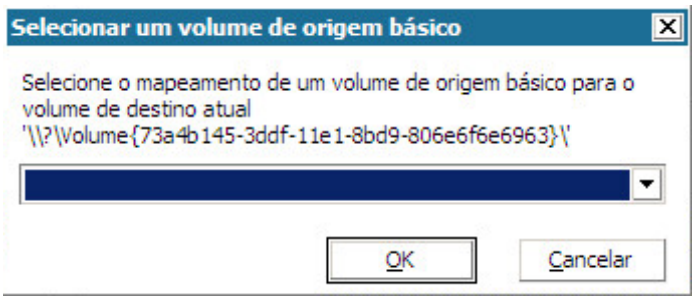
   Observação: se executar a BMR e restaurar o volume do sistema em um disco que não está configurado como disco de inicialização, haverá falha ao iniciar o computador após o término da BMR. Verifique se está restaurando o volume do sistema em um disco de inicialização configurado corretamente.

   Observação: ao restaurar em outro disco/volume, a capacidade do novo disco/volume deve ser do mesmo tamanho ou maior do que o disco/volume original. Além disso, o redimensionamento do disco destina-se somente a discos básicos, não a discos dinâmicos.



2. Se as informações do disco atual que você estiver vendo não parecerem corretas, acesse o menu **Utilitários** e verifique se há drivers ausentes.
3. Se necessário, no painel de disco/volume de destino, é possível clicar no menu suspenso **Operações** para exibir as opções disponíveis. Para obter mais informações sobre essas opções, consulte Gerenciando o menu operações de BMR.
4. Clique em cada volume de destino e, no menu pop-up, selecione a opção **Mapear volume de** para atribuir um volume de origem a esse volume de destino.

   A caixa de diálogo **Selecionar um volume de origem básico** é exibida.

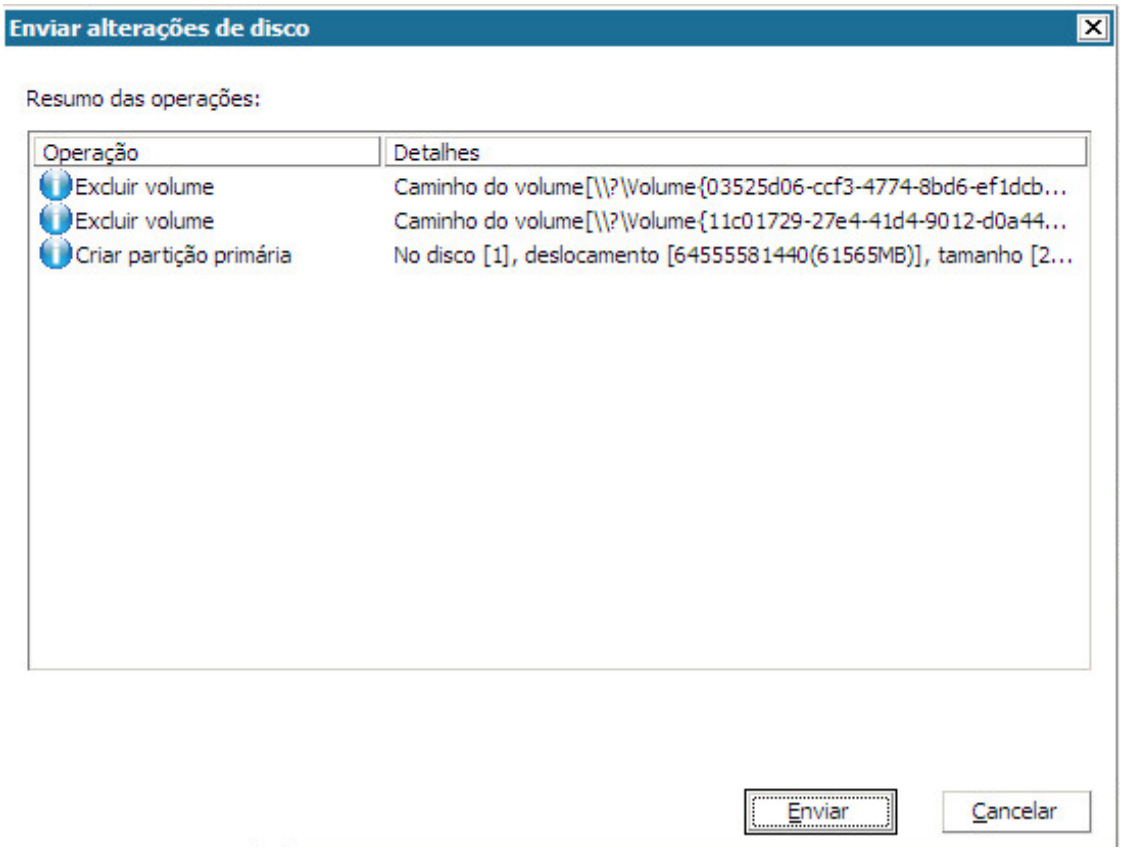


5. Na caixa de diálogo **Selecionar um volume de origem básico**, clique no menu suspenso e selecione o volume de origem disponível para atribuí-lo ao volume de destino selecionado. Clique em **OK**.

   - No volume de destino, um ícone de marca de seleção é exibido, indicando que o volume de destino foi mapeado.
   - No volume de origem, o ícone em forma de X vermelho muda para verde, indicando que o volume de origem foi atribuído a um volume de destino.

6. Quando tiver certeza de que todos os volumes que desejar restaurar e todos os volumes que contêm informações do sistema foram atribuídos a um volume de destino, clique em **Avançar**.

   A tela Enviar alterações de disco é exibida, mostrando um resumo das operações selecionadas. Para cada novo volume criado, são exibidas as informações correspondentes.



7. Ao confirmar se as informações de resumo estão corretas, clique em **Enviar**. (Se as informações não estiverem corretas, clique em **Cancelar**).

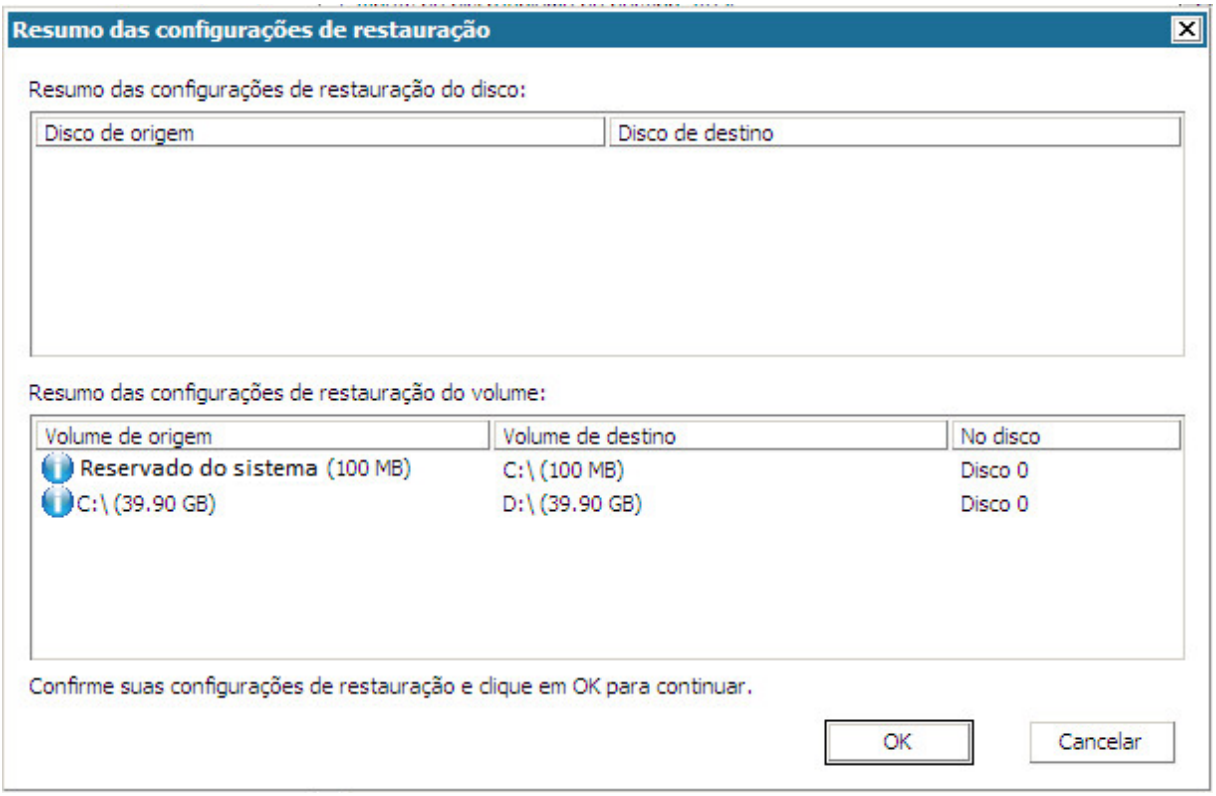
   Observação: as operações no disco rígido não entrarão em vigor até que sejam enviadas.

   No computador de destino, os novos volumes são criados e mapeados para o computador de origem correspondente.

8. Quando as alterações forem concluídas, clique em **OK**.

   A tela Resumo das configurações de restauração do disco é exibida, mostrando um resumo dos volumes a serem restaurados.

   Observação: na parte inferior da janela de resumo da restauração, as letras de unidade listadas na coluna Volume de destino são geradas automaticamente no WinPE (Windows Preinstallation Environment - Ambiente de Pré-Instalação do Windows). Elas podem ser diferentes das listadas na coluna Volume de origem. No entanto, os dados serão restaurados no volume apropriado, mesmo quando as letras forem diferentes.

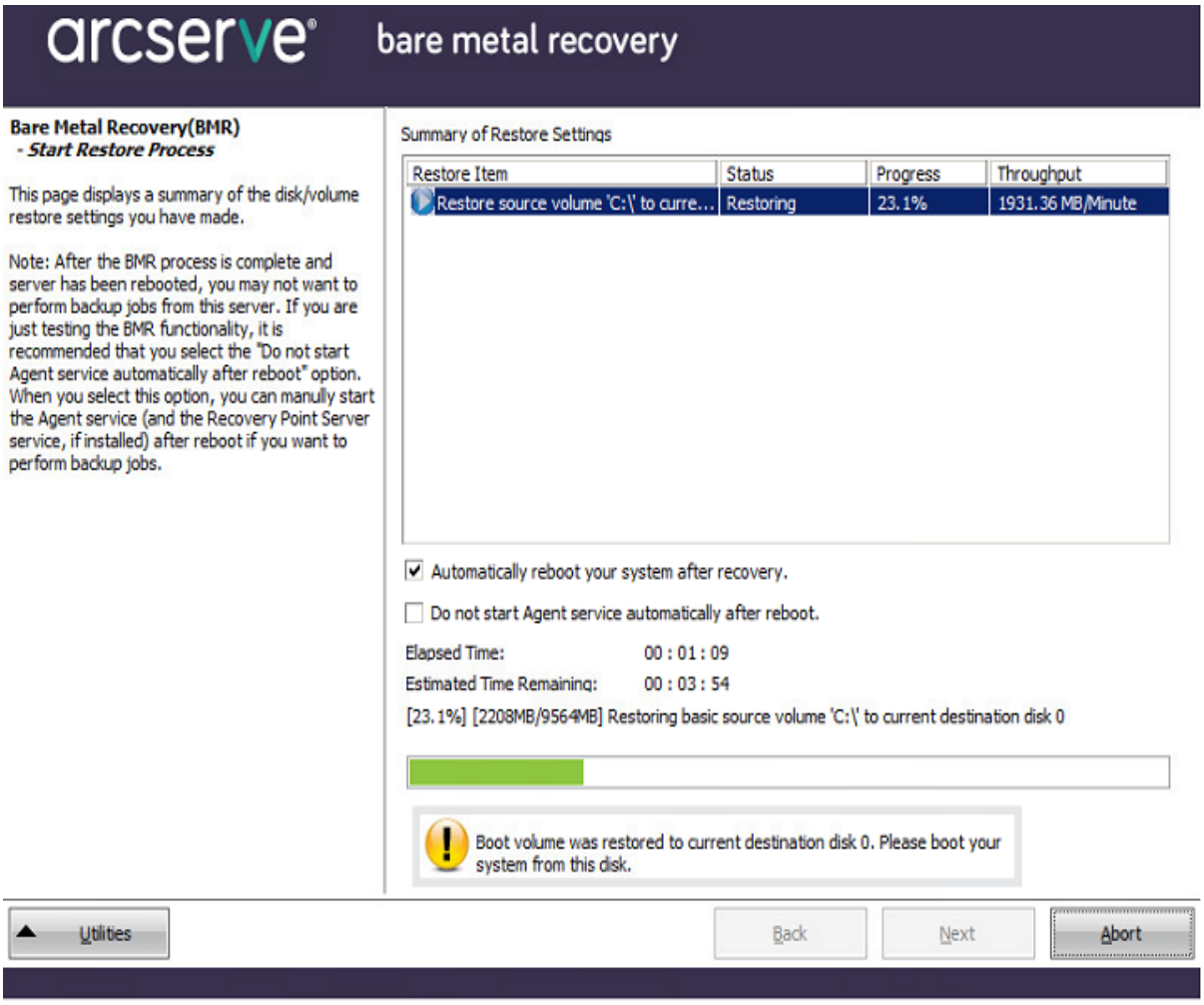


9. Após verificar se as informações de resumo estão corretas, clique em **OK**.

   O processo de restauração é iniciado. A tela do assistente de BMR exibe o status da restauração para cada volume.

- Dependendo do tamanho do volume sendo restaurado, essa operação pode levar algum tempo.
- Durante este processo, você estará restaurando bloco por bloco tudo o que tiver sido armazenado em backup para esse ponto de recuperação e criando uma réplica do computador de origem no computador de destino.
- Por padrão, a opção que permite reiniciar o sistema automaticamente depois da recuperação é selecionada. Se necessário, você pode desmarcar esta opção e reinicializar manualmente mais tarde.

  Importante: se estiver executando uma restauração autoritativa de um Active Directory após uma BMR, é necessário desmarcar a opção **Reiniciar o sistema automaticamente após a recuperação** e, para obter mais informações, consulte Como executar uma restauração autoritativa de um Active Directory após BMR.
- Se necessário, é possível selecionar Do not start Agent service automatically after reboot.
- Se necessário, é possível cancelar ou anular a operação a qualquer momento.



10. No menu **Utilitários**, é possível acessar o **Log de atividades** da BMR e usar a opção **Salvar** para salvar o Log de atividades.

    Por padrão, o log de atividades será salvo no seguinte local:

    X:\windows\system32\dr\log

    Observação: para evitar um erro gerado pelo Windows, não salve o Log de atividades na área de trabalho ou crie uma pasta na área de trabalho usando a opção **Salvar como**, na janela Log de atividades da BMR.

11. Caso esteja restaurando em diferentes tipos de hardware (o adaptador SCSI/FC usado para conectar unidades de disco rígido pode ter sido alterado) e nenhum driver compatível tenha sido detectado no sistema original, uma página de injeção de drivers será exibida para permitir o fornecimento de drivers a esses dispositivos.

    Procure e selecione os drivers a serem injetados no sistema recuperado de forma que, mesmo se estiver fazendo a recuperação em um computador com tipos diferentes de hardware, ainda seja possível trazer o computador de volta após a BMR.

12. Quando o processo de BMR for concluído, uma notificação de confirmação é exibida.

Verificar se a BMR foi bem-sucedida

Para verificar se a BMR foi concluída com êxito, execute as seguintes tarefas:

- Reinicie o sistema operacional.
- Verifique se todos os sistemas e aplicativos funcionam corretamente.
- Verifique se todas as configurações de rede foram configuradas corretamente.
- Verifique se a BIOS está configurada para inicializar a partir do disco no qual o volume de inicialização foi restaurado.
- Quando a BMR for concluída lembre-se das seguintes condições:
  - O primeiro backup realizado depois da BRM é um backup de verificação.
  - Após a reinicialização do computador, talvez seja necessário configurar os adaptadores de rede manualmente caso você tenha restaurado em um hardware diferente.

    Observação: Quando o computador for reinicializado, uma tela de recuperação de erro do Windows pode ser exibida indicando que o Windows não foi desligado corretamente. Se isso ocorrer, você poderá ignorar esse aviso com segurança e continuar para iniciar o Windows normalmente.
  - Para discos dinâmicos, se o status do disco for offline, é possível alterá-lo manualmente para online na interface de gerenciamento de disco (acessado executando o utilitário de controle Diskmgmt.msc).
  - Para discos dinâmicos, se os volumes dinâmicos estiverem em um status de falha de redundância, é possível sincronizar novamente os volumes na interface de gerenciamento de disco (acessado usando o utilitário de controle Diskmgmt.msc).

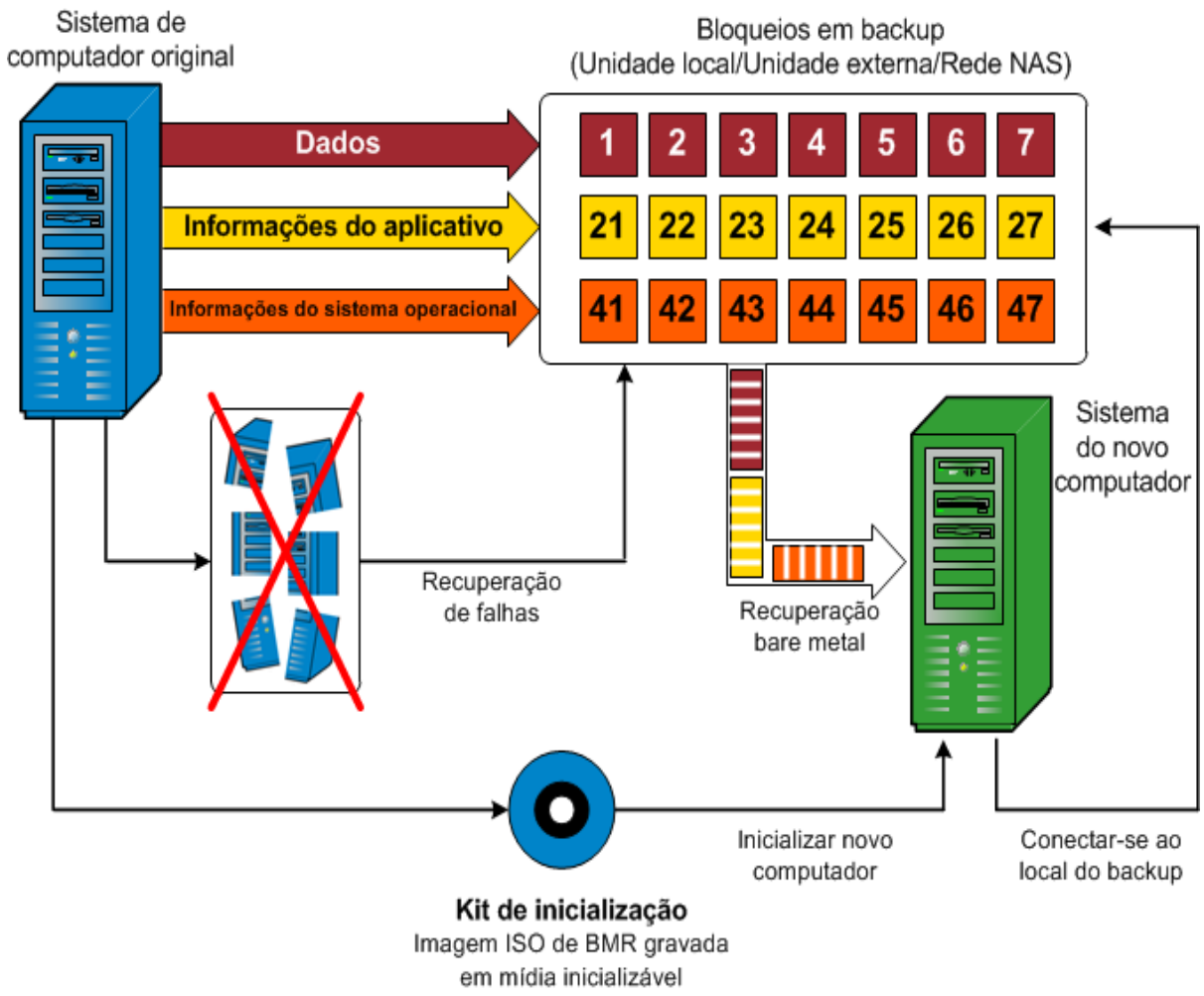
Informações de referência da BMR

- Como a recuperação bare metal funciona
- Sistemas operacionais que oferecem suporte à conversão de UEFI/BIOS
- Gerenciando o menu de operações de BMR

Como a recuperação bare metal funciona

A Recuperação bare metal é o processo de restauração de um sistema de computador a partir do estado “bare metal”, por meio da reinstalação do sistema operacional e dos aplicativos de software e, em seguida, da restauração dos dados e das configurações. Os motivos mais comuns para a execução de uma recuperação bare metal são a falha ou enchimento completo do disco rígido e você deseja atualizar (migrar) para uma unidade maior ou migrar para um hardware mais recente. A recuperação bare metal é possível porque, durante o processo de backup em nível de bloco, o agente do Arcserve UDP (Windows) não só captura os dados, mas também todas as informações relacionadas ao sistema operacional, aplicativos instalados, configurações, drivers necessários, e assim por diante. Para todas as informações relevantes, necessárias à execução de uma recompilação completa do sistema a partir do estado bare metal, é feito backup em uma série de blocos, os quais são armazenados no local do backup.

Observação: os discos dinâmicos serão restaurados somente no nível do disco. Se o backup dos dados for feito no volume de um disco dinâmico, não será possível restaurar este disco (incluindo todos os volumes) durante a BMR.



Ao executar uma recuperação bare metal, o disco de inicialização do agente do Arcserve UDP (Windows) é usado para inicializar o novo sistema do computador e permitir que o processo de recuperação bare metal seja iniciado. Ao iniciar a recuperação bare metal, o agente do Arcserve UDP (Windows) solicitará que você selecione ou forneça um local válido para recuperar esses blocos armazenados em backup, como também o ponto de recuperação para restauração. Caso seja necessário, também pode ser solicitado que você forneça drivers válidos para o novo sistema do computador. Quando essas informações de configuração e conexão forem fornecidas, o agente do Arcserve UDP (Windows) começa a receber a imagem de backup especificada do local do backup e restaura todos os blocos armazenados em backup no novo sistema (blocos vazios não são restaurados). Após a recuperação bare metal, a imagem é totalmente restaurada em um novo sistema de computador, o computador voltará ao estado que era quando o último backup foi realizado e os backups do agente do Arcserve UDP (Windows) poderão continuar conforme programado. (Após a conclusão da BMR, o primeiro backup será um Backup de verificação).

Sistemas operacionais que oferecem suporte à conversão de UEFI/BIOS

Se for detectado que o sistema operacional do computador de origem não é o mesmo firmware de seu sistema, você será questionado se deseja converter a UEFI em um sistema compatível com o BIOS ou o BIOS em um sistema compatível com a UEFI. A tabela a seguir lista cada sistema operacional e o tipo de conversão com suporte:

Sistema operacional (SO)	CPU	uEFI para BIOS	BIOS para uEFI
Windows Vista (nenhum SP)	x86	Não	Não
Windows Vista (nenhum SP)	x64	Não	Não
Windows Vista SP1	x86	Não	Não
Windows Vista SP1	x64	Sim	Sim
Windows Server 2008	x86	Não	Não
Windows Server 2008	x64	Sim	Sim
Windows Server 2008 R2	x64	Sim	Sim
Windows 7	x86	Não	Não
Windows 7	x64	Sim	Sim
Windows 8	x86	Não	Não
Windows 8	x64	Sim	Sim
Windows Server 2012	x64	Sim	Sim
Windows 8.1	x86	Não	Não
Windows 8.1	x64	Sim	Sim
Windows 10	x86	Não	Não
Windows 10	x64	Sim	Sim
Windows Server 2012 R2	x64	Sim	Sim
Windows Server 2016	x64	Sim	Sim
Windows Server 2019	x64	Sim	Sim

Gerenciando o menu de operações de BMR

O menu de operações de BMR consiste nos três seguintes tipos de operações:

- Operações específicas de disco
- Operações específicas de volume/partição
- Operação específica da BMR

Operações específicas de disco:

Para executar as operações de disco específicas, selecione o cabeçalho do disco e clique em **Operações**.

Limpar o disco

Essa operação é usada para limpar todas as partições de um disco e é:

- Um método alternativo para excluir todos os volumes de um disco. Com a operação **Limpar o disco**, não é necessário excluir os volumes um a um.
- Usada para excluir as partições que não sejam Windows. Devido a uma limitação do VDS, as partições que não são Windows não podem ser excluídas da IU, mas você pode usar esta operação para limpar todas elas.

  Observação: durante a BMR, quando o disco de destino possui partições não Windows ou partições OEM, não é possível selecionar essa partição e excluí-la da UI da BMR. Geralmente isso pode ocorrer se você nunca instalou o Linux/Unix no disco de destino. Para solucionar o problema, execute uma das seguintes tarefas:
- Selecione o cabeçalho do disco na IU da BMR, clique em **Operações** e use a operação **Limpar o disco** para apagar todas as partições no disco.
- Abra um prompt de comando e digite **Diskpart** para abrir o console do comando Diskpart. Em seguida, digite "select disk x", em que 'x' é o número de disco e "clean" para apagar todas as partições no disco.

Converter em MBR

Essa operação é usada para converter um disco em MBR (Master Boot Record – Registro mestre de inicialização). Ela está disponível apenas quando o disco selecionado é um disco GPT (GUID Partition Table – Tabela de partição GUID) e não há volumes nesse disco.

Converter em GPT

Essa operação é usada para converter um disco em GPT. Ela está disponível apenas quando o disco selecionado é um disco MBR e não há volumes nesse disco.

Converter em básico

Essa operação é usada para converter um disco em disco básico. Ela está disponível apenas quando o disco selecionado é um disco dinâmico e não há volumes nesse disco.

Converter em dinâmico

Essa operação é usada para converter um disco em disco dinâmico. Ela está disponível apenas quando o disco selecionado é um disco básico.

Disco online

Essa operação é usada para colocar um disco online. Ela está disponível apenas quando o disco selecionado está no status offline.

Propriedades do disco

Essa operação é usada para exibir detalhes sobre as propriedades do disco. Está sempre disponível e quando você seleciona essa operação, uma caixa de diálogo **Propriedades do disco** é exibida.

Operações específicas de volume/partição:

Para executar operações de volume/partição, selecione a área de corpo do disco e clique em **Operações**. Nesse menu, é possível criar novas partições que correspondam às partições do disco no volume de origem.

Criar partição primária

Essa operação é usada para criar uma partição em um disco básico. Ela está disponível somente quando a área selecionada é um espaço em disco não alocado.

Criar partição lógica

Essa operação é usada para criar uma partição lógica em um disco MBR básico. Está disponível somente quando a área selecionada é uma partição estendida.

Criar partição estendida

Essa operação é usada para criar uma partição estendida em um disco MBR básico. Está disponível apenas quando o disco é um disco MBR e a área selecionada é um espaço em disco não alocado.

Criar partição reservada do sistema

Essa operação é usada para criar a partição reservada do sistema em um sistema de firmware do BIOS e compilar um relacionamento de mapeamento com a partição de sistema EFI de origem. Está disponível apenas quando você restaura um sistema UEFI para um sistema BIOS.

Observação: se você tiver feito a conversão de UEFI para um sistema compatível com o BIOS anteriormente, use a operação Criar partição reservada do sistema para redimensionamento do disco de destino.

Criar partição de sistema EFI

Essa operação é usada para criar a partição de sistema EFI em um disco GPT básico. Está disponível apenas quando o firmware do computador de destino é UEFI e o disco selecionado é um disco GPT básico.

Observação: se tiver feito a conversão de BIOS para um sistema compatível com UEFI anteriormente, use a operação Criar partição de sistema EFI para o redimensionamento do disco de destino.

Observação: os sistemas que oferecem suporte à UEFI também exigem que a partição de inicialização resida em um disco GPT (GUID Partition Table - Tabela de Partição do GUID). Se estiver usando um disco MBR (Master Boot Record), você deverá converter esse disco em um disco GPT e, em seguida, usar a operação Criar partição de sistema EFI para redimensionamento do disco.

Redimensionar volume

Essa operação é usada para redimensionar um volume. Ela é um método alternativo do Windows "Ampliar volume/Reduzir volume". Está disponível somente quando a área selecionada é uma partição de disco válida.

Excluir volume

Essa operação é usada para excluir um volume. Está disponível somente quando a área selecionada é um volume válido.

Excluir partição estendida

Essa operação é usada para excluir a partição estendida. Está disponível somente quando a área selecionada é a partição estendida.

Propriedades do volume

Essa operação é usada para exibir propriedades de volume detalhadas. Quando você seleciona essa operação, uma caixa de diálogo **Propriedades do volume** é exibida.

Operações específicas de BMR:

Essas operações são específicas para a BMR. Para executar operações de BMR, selecione o cabeçalho do disco ou a área de corpo do disco e clique em **Operações**.

Mapear disco de

Essa operação é usada para compilar um mapeamento de relacionamento entre os discos dinâmicos de origem e de destino. Está disponível apenas quando o disco selecionado é um disco dinâmico.

Observação: ao fazer o mapeamento para outro disco, a capacidade de cada volume de destino mapeado deve ser do mesmo tamanho ou maior do que o volume de origem correspondente.

Mapear volume a partir de

Essa operação é usada para compilar um relacionamento de mapeamento entre o volume básico de origem e de destino. Ela está disponível apenas quando o volume selecionado é um volume básico.

Observação: ao fazer o mapeamento para outro disco, a capacidade de cada volume de destino mapeado deve ser do mesmo tamanho ou maior do que o volume de origem correspondente.

Confirmar

Essa operação está sempre disponível. Todas as operações são armazenadas em cache na memória e não modificam os discos de destino até que você selecione a operação de **Confirmação**.

Redefinir

Essa operação está sempre disponível. A operação **Redefinir** é usada para abandonar suas operações e restaurar o layout do disco para o status padrão. Essa operação limpará todas as operações em cache. Redefinir significa recarregar as informações de layout do disco de origem e de destino a partir do arquivo de configuração e do sistema operacional atual, e descartar quaisquer informações de layout de disco alteradas pelo usuário.

Solução de problemas da BMR

Quando um problema é detectado, o agente do Arcserve UDP (Windows) gera uma mensagem para ajudá-lo a identificar e solucionar o problema. Essas mensagens estão contidas no **Log de atividades** do Agente do Arcserve UDP (Windows), que é acessado pela opção **Exibir logs** na IU da página inicial. Além disso, ao tentar uma ação incorreta, o Agente do Arcserve UDP (Windows) em geral exibe uma mensagem pop-up para ajudá-lo a identificar e resolver o problema rapidamente.

- Baixo desempenho da taxa de transferência durante a BMR
- Volumes dinâmicos não são reconhecidos pelo sistema operacional após a BMR
- Não é possível reinicializar a VM Hyper-V após a BMR
- Não é possível reinicializar a VM VMware após a BMR
- Não é possível inicializar o servidor após executar uma BMR
- Falha ao enviar a tarefa BMR para o Servidor do ponto de recuperação

Baixo desempenho da taxa de transferência durante a BMR

Esse problema pode ser causado por controladores SATA com "AHCI" ativado.

Durante a BMR, o agente do Arcserve UDP (Windows) instalará drivers para dispositivos desconhecidos importantes. Se o dispositivo já tiver um driver instalado, o agente do Arcserve UDP (Windows) não atualizará o driver novamente. Para alguns dispositivos, o Windows 7PE pode conter os drivers, mas tais drivers podem não ser os melhores, e fazer com que a BMR seja executada de maneira muito lenta.

Para solucionar o problema, execute uma das seguintes tarefas:

- Verifique se a pasta do pool de drivers contém os drivers de disco mais novos. Caso contenha, e você esteja restaurando para a máquina original, instale o novo driver a partir da pasta do pool de drivers. Caso esteja restaurando para uma máquina alternativa, faça download dos drivers de disco mais recentes a partir da internet e carregue-os antes de iniciar a recuperação dos dados. Para carregar o driver, pode-se usar o utilitário "drvload.exe" que está incluído no Windows PE.
- Altere o modo de operação do dispositivo de AHCI (Advanced Host Controller Interface) para o modo de compatibilidade. (O modo de compatibilidade fornece uma melhor taxa de transferência).

Se o problema persistir, use o Bate-papo ao vivo para entrar em contato com o suporte da Arcserve. O Bate papo ao vivo permite viabilizar uma comunicação inteligente entre você e a equipe do suporte técnico, de modo que suas dúvidas e preocupações sejam atendidas imediatamente, sem interromper o acesso ao produto.

Volumes dinâmicos não são reconhecidos pelo sistema operacional após a BMR

Para manter os discos dinâmicos em um estado consistente, o sistema operacional Windows sincroniza automaticamente o metadados do LDM (Logical Disk Manager - Gerenciador de discos lógicos) em cada disco dinâmico. Assim, quando a BMR restaura um disco dinâmico e coloca-o online, o metadados do LDM neste disco será atualizado automaticamente pelo sistema operacional. Isso pode resultar em um volume dinâmico não reconhecido pelo sistema operacional e ausente após a reinicialização.

Para corrigir este problema, ao executar a BMR com vários discos dinâmicos, você não deve executar operações de disco antes da BMR, como limpeza, exclusão de volume, etc.

Se o problema persistir, use o Bate-papo ao vivo para entrar em contato com o suporte da Arcserve. O Bate papo ao vivo permite viabilizar uma comunicação inteligente entre você e a equipe do suporte técnico, de modo que suas dúvidas e preocupações sejam atendidas imediatamente, sem interromper o acesso ao produto.

Não é possível reinicializar a VM Hyper-V após a BMR

Se você executou a BMR em um computador Hyper-V que consiste em mais de um disco conectado a um controlador IDE (Integrated Drive Electronics), e o servidor não está reinicializando, execute o seguinte procedimento para solucionar o problema:

1. Verifique se o disco que contém o volume do sistema é o disco mestre.

   O BIOS do Hyper-V procura o volume do sistema no disco mestre (disco 1) que está conectado ao canal mestre. Se o volume do sistema não estiver localizado no disco mestre, a VM não será reinicializada.

   Observação: verifique se o disco que contém o volume do sistema está conectado a um controlador IDE. O Hyper-V não consegue inicializar a partir de um disco SCSI.

2. Se necessário, modifique as configurações do Hyper-V para conectar o disco que contém o volume do sistema ao canal mestre de IDE e reinicialize o computador virtual novamente.

   Se o problema persistir, use o Bate-papo ao vivo para entrar em contato com o suporte da Arcserve. O Bate papo ao vivo permite viabilizar uma comunicação inteligente entre você e a equipe do suporte técnico, de modo que suas dúvidas e preocupações sejam atendidas imediatamente, sem interromper o acesso ao produto.

Não é possível reinicializar a VM VMware após a BMR

Caso tenha executado a BMR em um computador VMware que consiste em mais de um disco conectado a um controlador IDE (Integrated Drive Electronics) ou a um adaptador SCSI, e o servidor não está reinicializando, execute o seguinte procedimento para solucionar o problema:

1. Verifique se o disco que contém o volume do sistema é o disco mestre.

   O BIOS do VMware procura o volume do sistema no disco mestre (disco 0) que está conectado ao canal mestre. Se o volume do sistema não estiver localizado no disco mestre, a VM não será reinicializada.

2. Se necessário, modifique as configurações do VMware para conectar o disco que contém o volume do sistema ao canal mestre de IDE e reinicialize o computador virtual novamente.

3. Se o disco for SCSI, certifique-se de que o disco contendo o volume de inicialização seja o primeiro a estabelecer conexão com o adaptador SCSI. Caso contrário, atribua o disco de inicialização do BIOS da VMware.

4. Verifique se o disco que contém o volume de inicialização está entre os oito discos anteriores, pois o BIOS da VMware detecta apenas oito discos durante a inicialização. Se houver mais de sete discos à frente do disco que contém os volumes do sistema conectados ao adaptador SCSI, a VM não poderá executar a inicialização.

   Se o problema persistir, use o Bate-papo ao vivo para entrar em contato com o suporte da Arcserve. O Bate papo ao vivo permite viabilizar uma comunicação inteligente entre você e a equipe do suporte técnico, de modo que suas dúvidas e preocupações sejam atendidas imediatamente, sem interromper o acesso ao produto.

Não é possível inicializar o servidor após executar uma BMR

Sintoma

Quando o computador de origem for um servidor Active Directory executando uma BMR para uma máquina física com um hardware diferente ou para uma máquina virtual em um servidor Hyper-V, o servidor não será inicializado e uma tela azul será exibida com a seguinte mensagem:

INTERROMPER: não foi possível iniciar os serviços de diretório c00002e2 devido ao seguinte erro: um dispositivo conectado ao sistema não está funcionando. Status do erro: 0xc0000001.

Solução

Reinicialize o sistema para o ambiente do Windows PE da BMR, renomeie todos os arquivos *.log na pasta C:\Windows\NTDS e reinicie o sistema. Por exemplo, renomeie o arquivo edb.log como edb.log.old e reinicie o sistema.

Se o problema persistir, use o Bate-papo ao vivo para entrar em contato com o suporte da Arcserve. O Bate papo ao vivo permite viabilizar uma comunicação inteligente entre você e a equipe do suporte técnico, de modo que suas dúvidas e preocupações sejam atendidas imediatamente, sem interromper o acesso ao produto.

Falha ao enviar a tarefa BMR para o Servidor do ponto de recuperação

Apenas uma tarefa de BMR é suportada quando a restauração do mesmo servidor de RPS para o mesmo nó (Backup do agente ou Backup com base em host). Isso é controlado pelo monitor de tarefas no servidor de RPS.

Se a máquina em que a tarefa BMR está em execução estiver desligada ou for reiniciada de forma inesperada, o monitor de tarefas no servidor de RPS aguardará 10 minutos e, em seguida, o tempo limite. Durante esse tempo, não será possível iniciar outra BMR para o mesmo nó do mesmo servidor de RPS.

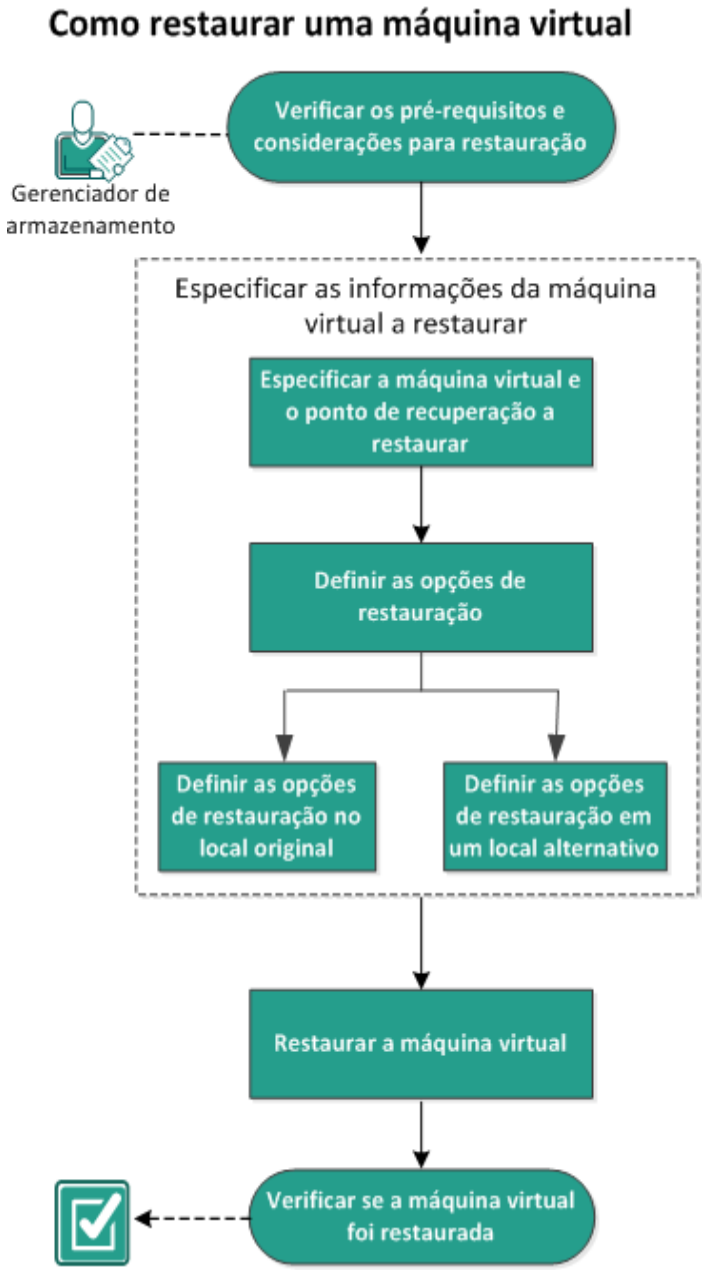
Se anular a BMR na IU da BMR, esse problema não existirá.

Se o problema persistir, use o Bate-papo ao vivo para entrar em contato com o suporte da Arcserve. O Bate papo ao vivo permite viabilizar uma comunicação inteligente entre você e a equipe do suporte técnico, de modo que suas dúvidas e preocupações sejam atendidas imediatamente, sem interromper o acesso ao produto.

Como restaurar uma máquina virtual

O Arcserve UDP permite usar a opção **Recuperar VM** para restaurar uma VM (Virtual Machine – Máquina Virtual) cujo backup foi feito anteriormente usando o backup sem agente com base em host. Esse método ajuda a restaurar a máquina virtual inteira no local original ou em um local ESX ou Hyper-V alternativo. É possível procurar os pontos de recuperação de máquina virtual a partir de uma exibição de calendário e selecionar o ponto de recuperação que você deseja restaurar.

O seguinte diagrama ilustra o processo para restaurar a partir de uma máquina virtual:



Execute as seguintes tarefas para restaurar uma máquina virtual:

1. Verificar os pré-requisitos e as considerações para restauração
2. Especificar as informações da máquina virtual a ser restaurada
    a. Especificar a máquina virtual e o ponto de recuperação para restaurar
    b. Definir as opções de restauração
        - Definir as opções de restauração do local original
        - Definir as opções de restauração no local alternativo
3. Restaurar a máquina virtual
4. Verificar se a máquina virtual foi restaurada

Revisar os pré-requisitos e as considerações para restauração

Verifique se os pré-requisitos a seguir existem antes de executar uma restauração:

- Você tem um ponto de recuperação válido para restauração.
- Existe um servidor de destino Virtual Center/ESX ou Hyper-V válido e acessível para recuperar a máquina virtual.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Revise as seguintes considerações de restauração:

- Se o destino de Recuperar VM for o Windows Server 2008 R2, então, a VM do backup de origem não deverá conter discos VHDx, que não são suportados no servidor Hyper-V (Windows Server 2008 R2).
- Se o destino de Recuperar VM for o Windows Server 2008 R2 ou Win2012, então, o tipo de subsistema da VM de backup de origem não deverá ser da geração 2 (introduzido no Windows Server 2012 R2) e não será suportado no servidor Hyper-V (Windows Server 2012/2008 R2).

Especificar as informações da máquina virtual a ser restaurada

É possível recuperar uma máquina virtual inteira a partir de um ponto de recuperação.

O processo envolvido na restauração de máquina virtual é o seguinte:

1. Especificar a máquina virtual e o ponto de recuperação para restaurar
2. Definir as opções de restauração
   - Definir as opções de restauração do local original
   - Definir as opções de restauração no local alternativo

Especificar a máquina virtual e o ponto de recuperação para restaurar

Use a opção **Restaurar VM** para restaurar uma máquina virtual cujo backup tenha sido feito anteriormente. Este método cria de maneira rápida e consistente uma máquina virtual a partir de um ponto de recuperação do Arcserve UDP em um servidor ESX ou Hyper-V. A máquina virtual recuperada então pode ser simplesmente iniciada para concluir o processo de recuperação.

Siga estas etapas:

1. Acesse a caixa de diálogo de seleção de método de restauração de uma das seguintes maneiras:

   No Arcserve UDP:

   a. Efetue logon no Arcserve UDP.

   b. Clique na guia **Recursos**.

   c. Selecione **Todos os nós** no painel esquerdo.

      Todos os nós adicionados são exibidos no painel central.

   d. No painel central, selecione o nó do e clique em **Ações**.

   e. Clique em **Restaurar** no menu suspenso **Ações**.

      A caixa de diálogo de seleção do método de restauração é exibida.

      Observação: você é automaticamente conectado ao nó do agente e a caixa de diálogo de seleção do método de restauração é exibida no nó do agente.

   No agente do Arcserve UDP (Windows):

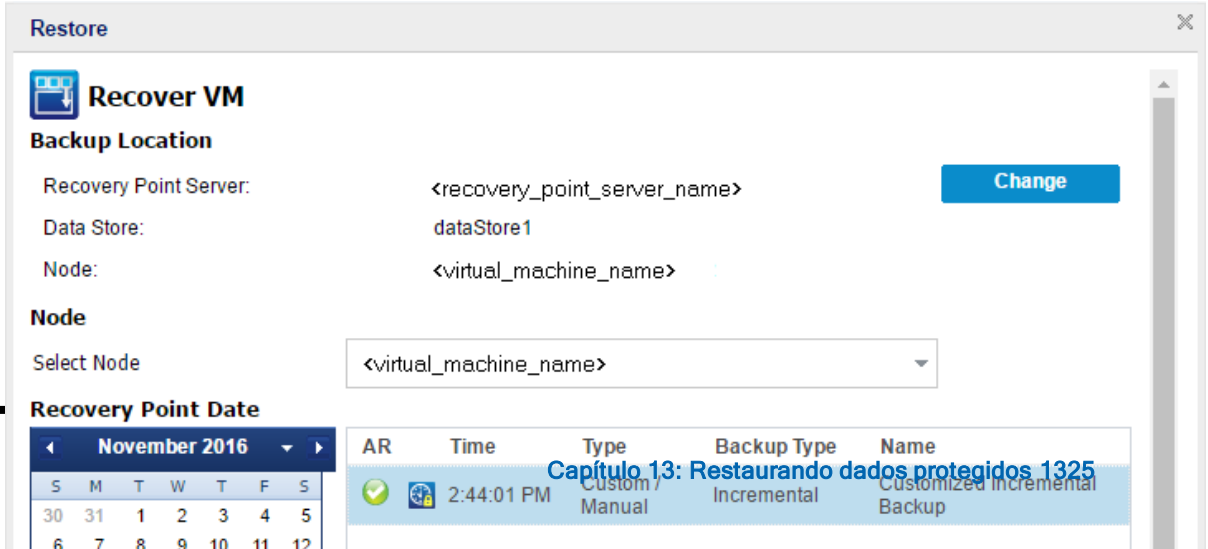
   a. Efetue logon no Agente do Arcserve UDP (Windows).

   b. Na página inicial, selecione **Restaurar**.

   A caixa de diálogo de seleção do método de restauração é exibida.

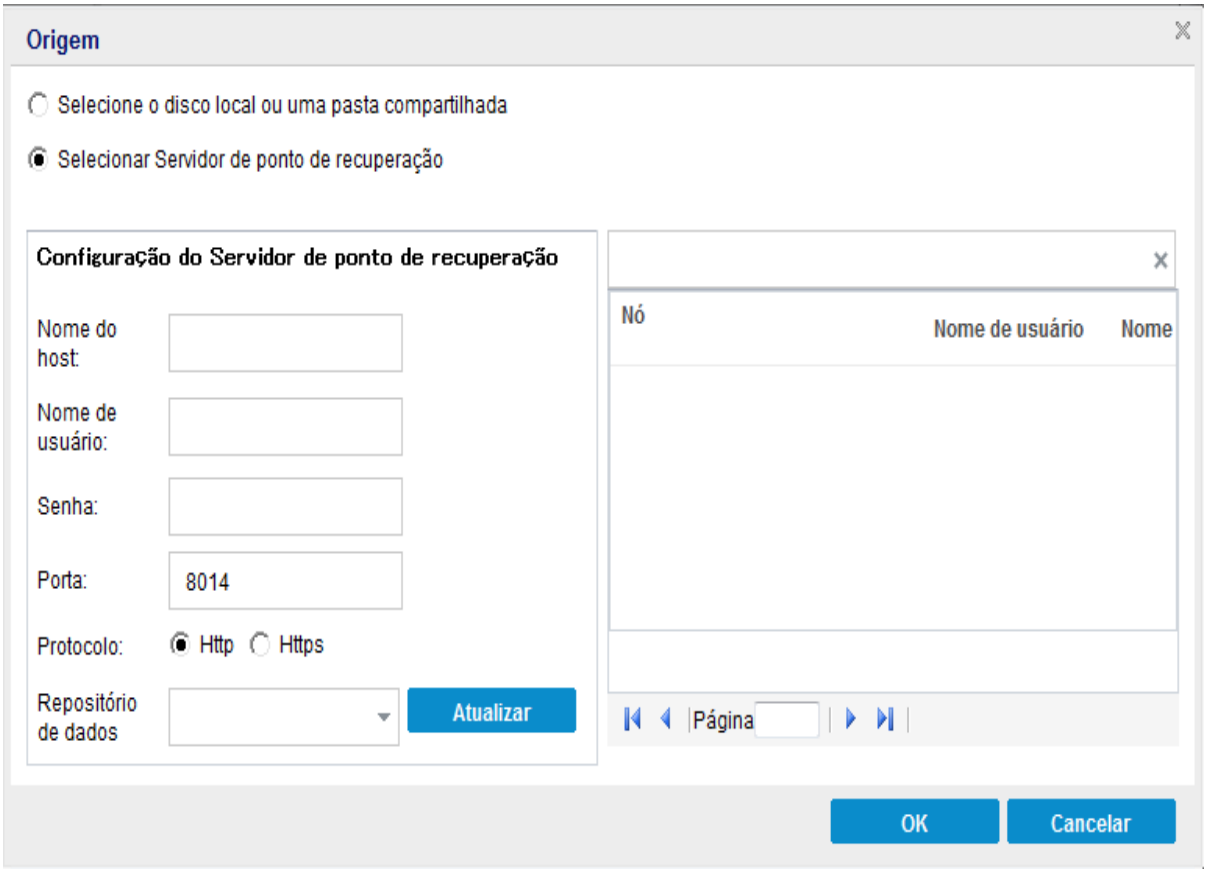
2. Clique na opção **Restaurar VM**.

   A caixa de diálogo **Recuperar VM** é exibida.



3. Clique em **Alterar** para alterar o local do backup.

   A caixa de diálogo **Origem** é exibida. É possível selecionar o local do backup na caixa de diálogo.



4. Selecione uma das seguintes opções:

   Selecionar o disco local ou uma pasta compartilhada

   a. Especifique ou procure o local onde as suas imagens de backup estão armazenadas e selecione o backup de origem adequado.

      É possível clicar no botão com a seta verde para verificar a conexão com o local especificado. Se necessário, forneça as credenciais de Nome de usuário e Senha para acessar esse local de origem.

      A caixa de diálogo **Selecionar o local do backup** é exibida.

   b. Selecione a pasta onde estão armazenados os pontos de recuperação e clique em **OK**.

      A caixa de diálogo **Selecione o local do backup** é fechada e é possível ver o local do backup na caixa de diálogo **Origem.**

   c. Clique em **OK**.

Os pontos de recuperação são listados na caixa de diálogo **Recuperar VM**.

Selecionar servidor de ponto de recuperação

a. Especifique os detalhes da configuração do servidor de ponto de recuperação e clique em **Atualizar**.

   Todos os nós (agentes/máquinas virtuais) são listados na coluna do nó na caixa de diálogo **Origem**.

b. Selecione o nó (agente/máquina virtual) da lista exibida e clique em **OK**.

   Os pontos de recuperação são listados na caixa de diálogo **Recuperar VM**.

5. Na lista suspensa **Máquina virtual**, selecione a máquina virtual a recuperar.

   O calendário é exibido e todas as datas que contém pontos de recuperação para o backup de origem especificado são realçadas em verde.

6. Selecione a data do calendário da imagem da máquina virtual a ser restaurada.

   Os pontos de recuperação correspondentes a essa data são exibidos, juntamente com a hora do backup, o tipo de backup que foi executado e o nome do backup.

7. Selecione um ponto de recuperação para restaurar.

   O conteúdo do backup (incluindo quaisquer aplicativos) para o ponto de recuperação selecionado é exibido. Ao restaurar uma máquina virtual, o sistema inteiro é restaurado. Como resultado, é possível exibir, mas não selecionar volumes, pastas ou arquivos individuais da máquina virtual selecionada.

   Observação: um ícone de relógio com um símbolo de cadeado indica que o ponto de recuperação contém informações criptografadas e pode ser necessária uma senha para restaurar.

8. Clique em **Avançar**.

   A caixa de diálogo **Opções de restauração** é exibida.

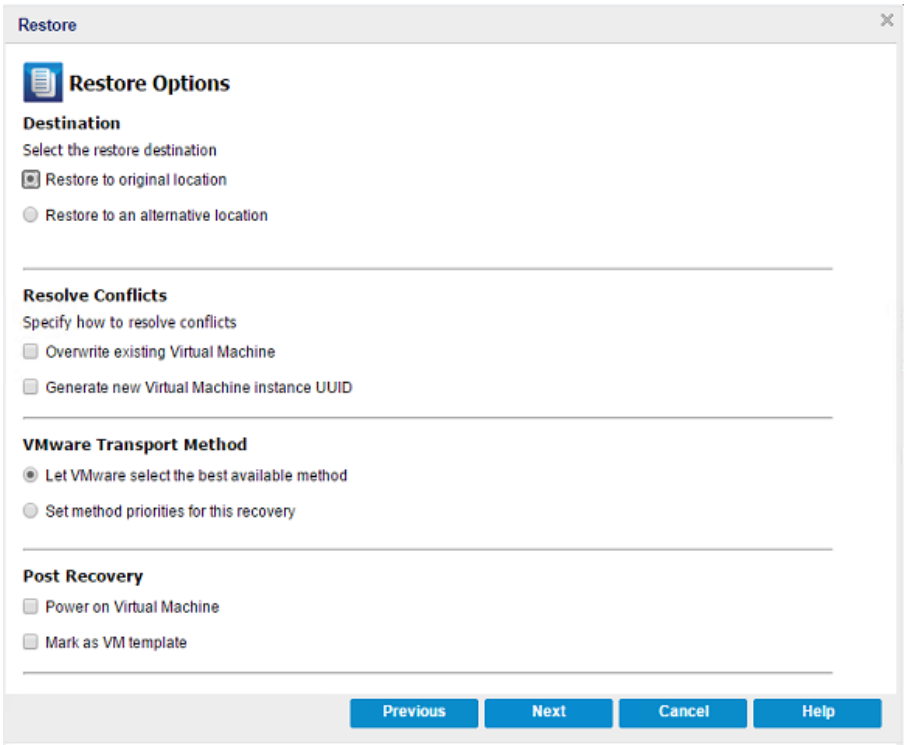
   A máquina virtual e o ponto de recuperação para restaurar são especificados.

Definir as opções de restauração

Depois de especificar a máquina virtual e o ponto de recuperação para restauração, defina as opções de restauração da máquina virtual selecionada.

Siga estas etapas:

1. Na caixa de diálogo Opções de restauração, selecione o destino da restauração.



As opções de destino disponíveis são:

Restaurar no local original

Restaura a máquina virtual no local original em que a imagem de backup foi capturada. Por padrão, esta opção está ativada.

Para obter mais informações, consulte Definir as opções de restauração do local original.

Restaurar em um local alternativo

Restaura para a máquina virtual em outro local em que a imagem de backup foi capturada.

Para obter mais informações, consulte Definir as opções de restauração do local alternativo.

2. (Opcional) Marque a caixa de seleção **Usar a rede do servidor RPS selecionado para restaurar o tráfego** e faça o seguinte:

a. Para ativar a comunicação entre o servidor proxy do Windows e o servidor de ponto de recuperação, selecione a rede CIDR na lista suspensa.

b. Para definir a restrição no SMB Multichannel para que as transferências de dados sejam realizadas somente pela rede selecionada, marque a caixa de seleção **Usar Ethernet dedicada se o computador atual permitir o SMB multicanal**.

Observações:

- Essa opção não está disponível por padrão. Para ativar essa opção, crie o registro da sequência de caracteres *UseDedicatedEthernet* no seguinte caminho e, em seguida, defina o valor do registro como 1:

  SOFTWARE\Arcserve\Unified Data Protection\Engine

- Ao executar uma tarefa de restauração na página Nós, crie uma chave do Registro no proxy de backup.
- Ao executar uma tarefa de restauração do agente normal usando a sessão de backup RPS, crie uma chave do Registro no agente normal.

3. (Opcional) Marque a caixa de seleção **Usar a rede do servidor proxy selecionado para restaurar o tráfego** e faça o seguinte:

a. Para ativar a comunicação entre o servidor proxy do Windows e o hipervisor, selecione a rede CIDR na lista suspensa.

b. Para definir a restrição no SMB Multichannel para que as transferências de dados sejam realizadas somente pela rede selecionada, marque a caixa de seleção **Usar Ethernet dedicada se o computador atual permitir o SMB multicanal**.

Observações:

- Essa opção não está disponível por padrão. Para ativar essa opção, crie o registro da sequência de caracteres *UseDedicatedEthernet* no seguinte caminho e, em seguida, defina o valor do registro como 1:

  SOFTWARE\Arcserve\Unified Data Protection\Engine

- Ao executar uma tarefa de restauração na página Nós, crie uma chave do Registro no proxy de backup.
- Ao executar uma tarefa de restauração do agente normal usando a sessão de backup RPS, crie uma chave do Registro no agente normal.

4. Especifique as opções Resolvendo conflitos que o Arcserve UDP executará se forem encontrados conflitos durante o processo de restauração

Substituir a máquina virtual existente

Essa opção serve para especificar se você deseja substituir a máquina virtual existente. Por padrão, essa opção de substituição não está selecionada.

Observação: para a opção Substituir a máquina virtual existente, uma "máquina virtual existente" é definida como uma VM que tem o mesmo nome da VM e reside no mesmo host ESXi (para a VM da VMware), ou uma VM que tem o mesmo nome de VM e a UUID da instância e reside no mesmo host do Hyper-V (para a VM do Hyper-V). Para a VM da VMware, se houver uma VM que tenha o mesmo nome de VM, mas resida em um host ESXi diferente (sob o mesmo vCenter), a opção de substituição não funcionará. Nesse caso, a GUI de recuperação da VM detecta essa VM e exibe uma mensagem de erro e impede que você prossiga de forma que a VM não seja substituída por engano. Como solução alternativa, é necessário renomear a VM existente ou usar a opção Restaurar em um local alternativo e especificar um outro nome de VM.

- Se você selecionar esta opção, o processo de restauração substituirá todas as imagens existentes dessa máquina virtual que estiverem no destino de restauração especificado. A imagem da máquina virtual é restaurada dos arquivos de backup, independentemente de sua presença atual no destino da restauração.
- Se você não selecionar essa opção, a GUI de recuperação da VM exibe uma mensagem de erro e impede que você prossiga se a VM original ainda existir no local original. Como solução alternativa, é necessário renomear a VM existente ou usar a opção Restaurar em um local alternativo e especificar um outro nome de VM.

Gerar novo UUID de instância da máquina virtual

Essa opção destina-se a especificar se você deseja gerar um novo UUID de instância para a VM restaurada ou manter o UUID de instância original.

Observação: se você não selecionar essa opção, a UUID da instância original será definida como a VM restaurada. No entanto, caso o host de destino do vCenter/ESX ou Hyper-V já tenha uma VM com a mesma UUID de instância, a nova UUID será usada e uma mensagem de aviso será exibida no log de atividades da tarefa de recuperação da VM.

5. Marque a opção Após a recuperação.

Ligar máquina virtual

Selecione se a máquina virtual deve ser ligada no final do processo de restauração. Por padrão, essa opção não é selecionada.

Marcar como modelo de VM (disponível somente para VM da VMware)

Selecione se deseja converter a VM restaurada para o modelo. Se o nó de origem for VM em backup, essa opção não será selecionada por padrão. Se o nó de origem for modelo em backup, essa opção será selecionada por padrão.

As opções de restauração são definidas para restaurar uma máquina virtual.

Definir as opções de restauração do local original

Durante o processo de configuração para recuperar a VM, é necessário selecionar a opção de onde deseja restaurá-la. As seleções disponíveis são **Restaurar no local original** e **Restaurar em um local alternativo**.

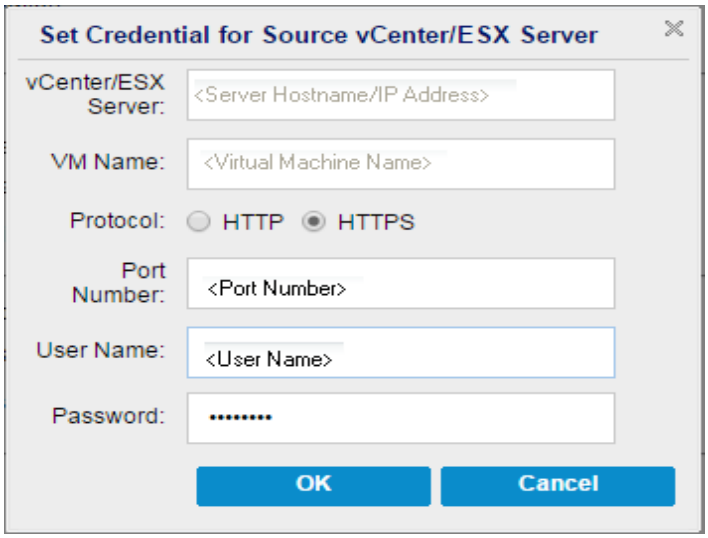
Este procedimento explica como restaurar uma máquina virtual no local original.

Siga estas etapas:

1. Na caixa de diálogo **Opções de restauração**, após marcar as opções **Resolver conflitos** e **Após a recuperação**, selecione **Restaurar no local original** e clique em **Avançar**.

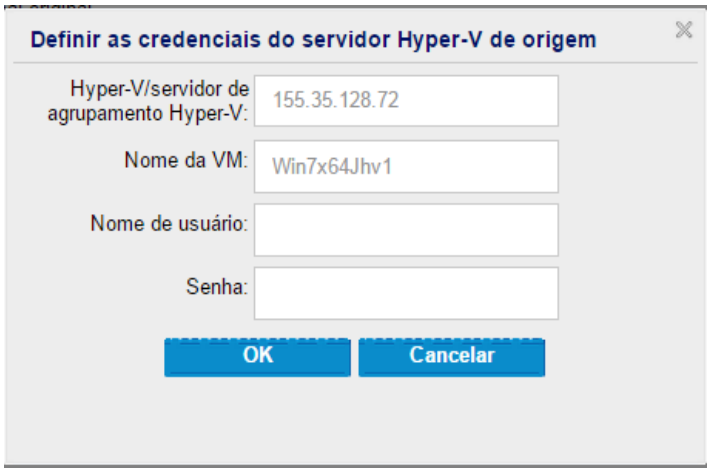
   A devida caixa de diálogo para VMware ou Hyper-V é exibida.

   - A caixa de diálogo **Definir credencial para o Servidor vCenter/ESX de origem** é exibida.



   - Para Hyper-V, a caixa de diálogo **Definir as credenciais para o Servidor**

Hyper-V de origem é exibida.



2. Especifique as credenciais para acessar a máquina virtual.
   - Para VMware, preencha os campos a seguir.

     vCenter/ESX Server

     Exibe o nome do host ou o endereço IP do sistema do servidor vCenter ou ESX de destino.

     Observação: não é possível editar este campo. É possível somente exibir os detalhes.

     Nome da VM

     Exibe o nome da máquina virtual que você está restaurando.

     Observação: não é possível editar este campo. É possível somente exibir os detalhes.

     Protocolo

     Especifica o protocolo que você deseja usar para comunicação com o servidor de destino. As seleções disponíveis são HTTP e HTTPS.

     Número da porta

     Especifica a porta que você deseja usar para a transferência de dados entre o servidor de origem e o de destino.

     Padrão: 443.

     Nome de usuário

     Especifica o nome de usuário que tem direitos de acesso para efetuar logon no servidor vCenter/ESX onde você planeja restaurar a máquina virtual.

     Senha

Especifica a senha correspondente ao Nome de usuário.

- Para Hyper-V, preencha os campos a seguir.

  Servidor do Hyper-V/Hyper-V Cluster

  Exibe o nome do host ou o endereço IP do sistema do servidor Hyper-V de destino ou servidor do Hyper-V cluster.

  Observação: não é possível editar este campo. É possível somente exibir os detalhes.

  Nome da VM

  Exibe o nome da máquina virtual que você está restaurando.

  Observação: não é possível editar este campo. É possível somente exibir os detalhes.

  Nome de usuário

  Especifica o nome de usuário que tem direitos de acesso para efetuar logon no servidor vHyper-V onde planeja restaurar a máquina virtual. Para a VM do cluster do Hyper-V, especifique a conta de domínio que tem privilégios administrativos do cluster.

  Senha

  Especifica a senha correspondente ao Nome de usuário.

3. Clique em **OK**.

   A caixa de diálogo **Resumo da restauração** é exibida.

   As opções de restauração para o local original são definidas.

Definir as opções de restauração no local alternativo

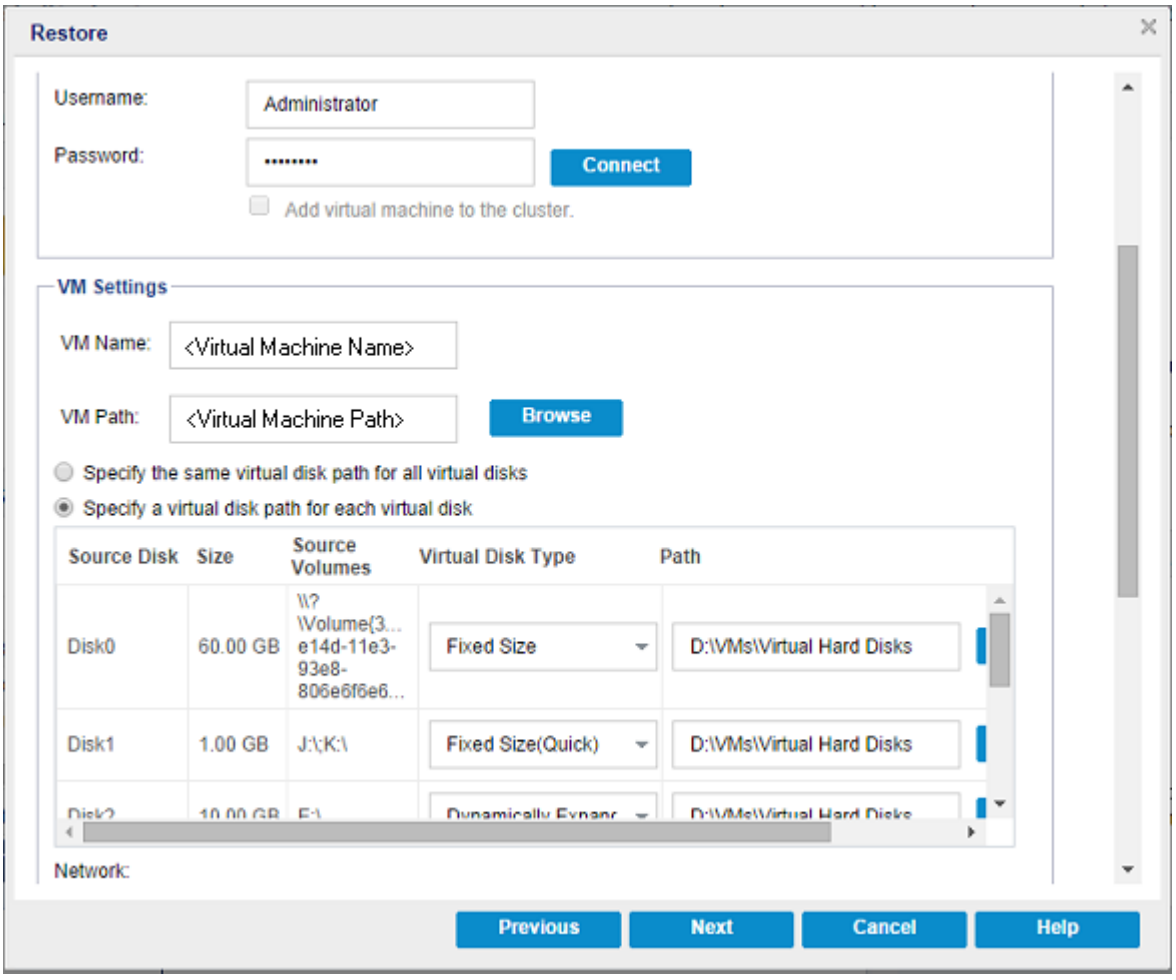
Durante o processo de configuração da VM, especifique onde a máquina virtual recuperada deve ser armazenada. As seleções disponíveis são **Restaurar no local original** e **Restaurar em um local alternativo**.

Este procedimento explica como restaurar uma máquina virtual para um local alternativo ou outro armazenamento de dados.

Siga estas etapas:

1. Na caixa de diálogo **Opções de restauração**, após marcar as opções **Resolver conflitos** e **Após a recuperação**, selecione **Restaurar em um local diferente**.
   - Para VMware, a caixa de diálogo **Opções de restauração** se expande para exibir restauração adicional em opções alternativas.
   - Para Hyper-V, a caixa de diálogo **Opções de restauração** se expande para exibir restauração adicional em opções alternativas.

   Se você selecionar a opção **Especificar o caminho para cada disco virtual**, a seguinte caixa de diálogo será exibida:



2. Especifique as informações do servidor apropriado.

   - Para VMware, preencha os campos a seguir:

     vCenter/ESX Server

     Especifica o nome do host ou o endereço IP do sistema do servidor vCenter ou ESX de destino.

     Nome de usuário

     Especifica o nome de usuário que tem direitos de acesso para efetuar logon no servidor vCenter/ESX onde você planeja restaurar a máquina virtual.

     Senha

     Especifica a senha correspondente ao Nome de usuário.

     Protocolo

     Especifica o protocolo que você deseja usar para comunicação com o servidor de destino. As seleções disponíveis são HTTP e HTTPS.

     Padrão: HTTPS.

     Observação: o VDDK 6.x.x da VMware vem integrado ao Arcserve UDP 6.5, mas o VDDK 6.x.x não oferece suporte a HTTP. Certifique-se de selecionar HTTPS, a menos que você substitua manualmente o VDDK 6.x.x integrado por outra versão do VDDK.

     Número da porta

     Especifica a porta que você deseja usar para a transferência de dados entre o servidor de origem e o de destino.

     Padrão: 443.

   - Para Hyper-V, preencha os campos a seguir:

     Servidor Hyper-V

     Exibe o nome do host ou o endereço IP do sistema do servidor Hyper-V de destino.

     Nome de usuário

     Especifica o nome de usuário que tem direitos de acesso para efetuar logon no servidor vHyper-V onde planeja restaurar a máquina virtual. Para a VM do agrupamento do Hyper-V, especifique a conta de domínio que tem privilégios administrativos do agrupamento.

     Senha

     Especifica a senha correspondente ao Nome de usuário.

Adicionar máquina virtual no agrupamento

Selecione a opção se desejar adicionar a máquina virtual que restaura o Arcserve UDP, no agrupamento. Considere as seguintes opções:

- Se você fornecer um nome de nó de agrupamento como o nome do servidor Hyper-V, a caixa de seleção é desativada e selecionada por padrão. Como resultado, a máquina virtual será automaticamente adicionada ao agrupamento.
- Se você fornecer o nome de host de um servidor Hyper-V que faz parte do agrupamento, a caixa de seleção é ativada e você pode optar por adicionar a máquina virtual ao agrupamento.
- Se você fornecer o nome de host de um servidor Hyper-V autônomo que não faz parte do agrupamento, a caixa de seleção é desativada e desmarcada.

3. Quando as informações do Servidor vCenter/ESX ou as informações do Servidor Hyper-V são especificadas, clique no botão **Estabelecer conexão com este servidor vCenter/ESX** ou clique no botão **Estabelecer conexão com este servidor Hyper-V**.

   Se as informações de credenciais de acesso do servidor alternativo estiverem corretas, os campos **Configurações da VM** serão ativados.

4. Especifique as **Configurações da VM**.

   - Para VMware, preencha os campos a seguir.

     Nome da VM

     Especifica o nome da máquina virtual que você está restaurando.

     ESX Server

     Especifica o servidor ESX de destino. O menu suspenso contém uma lista de todos os servidores ESX associados ao servidor vCenter.

     Pool de recursos

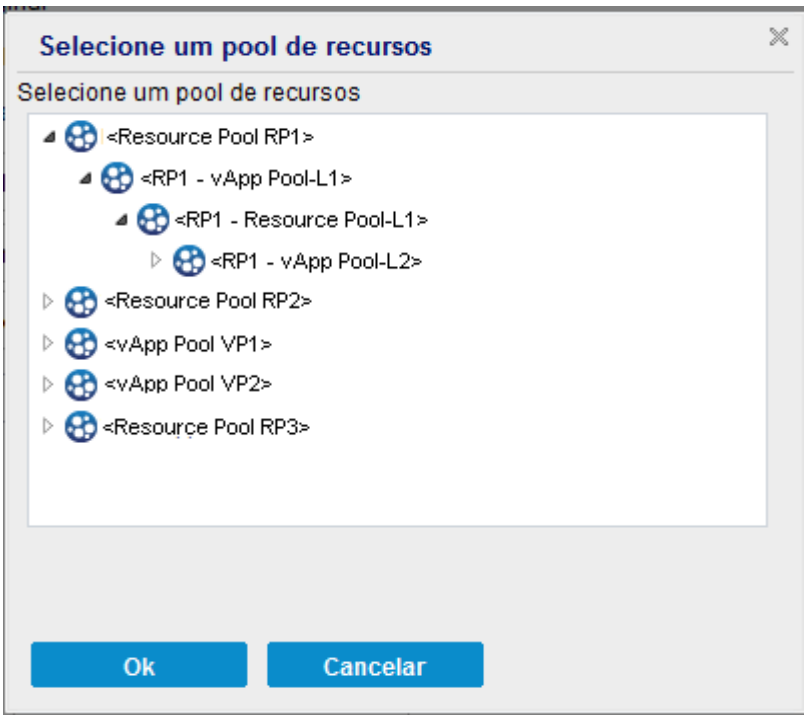
     Seleciona o **Pool de recursos** ou o **Pool de vApp** a ser usado para a recuperação da máquina virtual.

     Observação: um pool de recursos é uma coleção configurada de recursos de CPU e memória. Um pool de vApp é uma coleção de uma ou mais máquinas virtuais que podem ser gerenciadas como um único objeto.

     Padrão: em branco.

     Clique no botão **Procurar pool de recursos** para exibir a caixa de diálogo **Selecionar um pool de recursos**. Essa caixa de diálogo contém uma

lista de todos os pools de recursos e pools de vApp disponível para o destino do servidor ESX. Selecione o pool a ser usado para a recuperação da máquina virtual. Você pode deixar este campo em branco se não quiser atribuir um pool de recursos ou de vApp à recuperação dessa máquina virtual.



Diretiva de armazenamento

Especifique a diretiva de armazenamento da VM que é aplicada ao início da VM da VM restaurada. Selecione o padrão de repositório de dados se você não deseja aplicar a diretiva de armazenamento de VM.

Observação: se você pode ver apenas o padrão de repositório de dados, mas, na verdade, há outras diretivas de armazenamento definidas no vCenter, a conta usada para conectar o vCenter não tem permissão suficiente para obter a diretiva de armazenamento do vCenter. Verifique se a conta tem o privilégio de exibição de armazenamento orientado por perfil no nível do vCenter.

Armazenamento de dados em VM

Especifique o repositório de dados de destino para o início da VM da VM restaurada.

Observação: por padrão, somente os repositórios de dados que são compatíveis com a diretiva de armazenamento selecionada são listados. Se você quiser ver todos os repositórios de dados, desmarque a caixa de seleção **Mostrar apenas repositórios de dados compatíveis para a**

diretiva de armazenamento selecionada que fica sob a tabela Repositório de dados do disco.

Repositório de dados do disco

Especifique o tipo de disco virtual, diretiva de armazenamento e repositório de dados de destino para cada disco virtual da VM, respectivamente.

- Tipo de disco virtual: selecione uma das opções a seguir: Fina, Thick Lazy Zeroed ou Thick Eager Zeroed.
- Diretiva de armazenamento: selecione a diretiva de armazenamento da VM que é aplicada a este disco virtual. Selecione o padrão de repositório de dados se você não deseja aplicar a diretiva de armazenamento de VM.
- Repositório de dados de destino: selecione o repositório de dados em que o disco virtual é restaurado.

Observação: por padrão, somente os repositórios de dados que são compatíveis com a diretiva de armazenamento selecionada são listados. Se você quiser ver todos os repositórios de dados, desmarque a caixa de seleção **Mostrar apenas repositórios de dados compatíveis para a diretiva de armazenamento selecionada** que fica sob a tabela Repositório de dados do disco.

Rede

Especifica os detalhes da configuração de vSphere Standard Switch/vSphere Distributed Switch.

- Para Hyper-V, preencha os campos a seguir.

Nome da VM

Especifica o nome da máquina virtual que você está restaurando.

Caminho da VM

Especifica o caminho de destino (no servidor Hyper-V) onde salvar o arquivo de configuração da VM do Hyper-V. A pasta padrão do arquivo de configuração de VM para o servidor Hyper-V é exibida por padrão. É possível modificar o caminho diretamente no campo ou clicar em **Procurar** para selecionar um caminho.

Observação: se estiver restaurando a máquina virtual no agrupamento do Hyper-V e desejar que a máquina virtual migre entre os nós do agrupamento, especifique o CSV (Cluster Shared Volume – Volume Com-

partilhado do Agrupamento) para o caminho da VM e o caminho do disco virtual.

Especifique o mesmo caminho do disco virtual para todos os discos virtuais

Especifique um caminho (no servidor Hyper-V) onde salvar todos os discos virtuais da VM juntos. A pasta padrão do arquivo de disco de VM para o servidor Hyper-V é exibida por padrão. É possível modificar o caminho diretamente no campo ou clicar em **Procurar** para selecionar um caminho.

Observação: se estiver restaurando a máquina virtual no agrupamento do Hyper-V e desejar que a máquina virtual migre entre os nós do agrupamento, especifique o CSV (Cluster Shared Volume – Volume Compartilhado do Agrupamento) para o caminho da VM e o caminho do disco virtual.

Especifique um caminho do disco virtual para cada disco virtual

Especifique o caminho (no servidor Hyper-V) de cada um dos discos virtuais da VM, respectivamente. A pasta padrão do arquivo de disco de VM para o servidor Hyper-V é exibida por padrão. É possível modificar o caminho diretamente no campo ou clicar em **Procurar** para selecionar um caminho. Para atribuir o tipo de disco virtual, selecione uma das seguintes opções: Tamanho fixo, Tamanho fixo (Rápido), Expandindo dinamicamente e Manter o mesmo que o disco de origem.

Observações:

- Se estiver restaurando a máquina virtual no agrupamento do Hyper-V e desejar que a máquina virtual migre entre os nós do agrupamento, especifique o CSV (Cluster Shared Volume – Volume Compartilhado do Agrupamento) para o caminho da VM e o caminho do disco virtual.
- Não use a opção Tamanho fixo (Rápido), a menos que tenha certeza de que anteriormente você não tenha salvado informações importantes sobre o dispositivo de armazenamento no qual o arquivo de disco virtual reside.

Tamanho fixo (Rápido)

Com essa opção, é possível restaurar um disco de tamanho fixo de maneira mais rápida. Você não precisa limpar blocos de disco não utilizados como zero ao restaurar o disco. Entretanto, por isso, alguns fragmentos de dados originais permanecem no armazenamento subjacentes. Essa situação cria riscos de vazamento de informações. Depois que o

disco for montado na máquina virtual, o usuário da máquina virtual pode usar algumas ferramentas de disco para analisar os dados brutos no disco e obter os dados originais no dispositivo de armazenamento do servidor Hyper-V em que o arquivo de disco virtual reside.

Rede

Especifica os detalhes de configuração da rede para a VM.

5. Clique em **OK**.

   A caixa de diálogo **Resumo da restauração** é exibida.

   As opções de restauração para o local alternativo são definidas.

Restaurar a máquina virtual

O **Resumo da restauração** ajuda você a revisar todas as opções de restauração definidas e modificá-las se necessário.

Na caixa de diálogo **Resumo da restauração**, examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.

- Se as informações do resumo não estiverem corretas, clique em **Anterior** e volte à caixa de diálogo em questão para alterar a configuração incorreta.
- Se as informações de resumo estiverem corretas, clique em **Concluir** para iniciar o processo de restauração.

A máquina virtual é restaurada.

Verificar se a máquina virtual foi restaurada

Após a conclusão do processo de restauração, verifique se a máquina virtual foi restaurada no destino especificado.

Siga estas etapas:

1. Navegue até o destino de restauração especificado.

   Por exemplo, se selecionar para restaurar a máquina virtual para o destino de restauração como local original, efetue logon no vCenter/ESX ou no Hyper-V Server e verifique se a máquina virtual existe.

   Se selecionar para restaurar a máquina virtual no local alternativo, efetue logon no vCenter/ESX ou no Hyper-V Server alternativo fornecido nas opções de restauração e verifique se a máquina virtual existe.

2. Verifique se a máquina virtual foi restaurada.

   A máquina virtual é restaurada com êxito.

Como restaurar o Filestream SQL

Esta seção contém os seguintes tópicos:

Como aplicar o patch T00002266

Esta seção fornece informações sobre como aplicar o patch T00002266.

Antes de instalar o patch *T00002266*, verifique se o arquivo *SqlRestore.ini* está em *C:\Arquivos de programas\Arcserve\Unified Data Protection\Engine\Configuration* para executar as restaurações.

Para instalar o patch, faça o seguinte:

1. Faça download e extraia o arquivo **T00002266.zip**.
2. Para instalar, clique no arquivo **T00002266.exe**.

Para abrir e editar o arquivo SqlRestore.ini, faça o seguinte:

1. Na máquina de origem, navegue até o seguinte local:

   C:\Arquivos de programas\Arcserve\Unified Data Protection\Engine\Configuration
2. Abra o arquivo *SqlRestore.ini* em um editor de texto e inclua as seguintes informações:

   RestoreInstanceName = {nome da instância do servidor SQL de destino}

   MDF-restore-folder = {local do arquivo MDF}

   LDF-restore-folder = {local do arquivo LDF}

   NDF-restore-folder = {local do arquivo NDF}

   FILESTREAM-restore-folder = {local do arquivo FileStreams}
3. Com base no local onde deseja restaurar os bancos de dados, edite o conteúdo entre chaves com os locais das pastas.

   Por exemplo, substitua:

   MDF-restore-folder = {local do arquivo MDF}

   com

   MDF-restore-folder = C:\Rest\MDF1

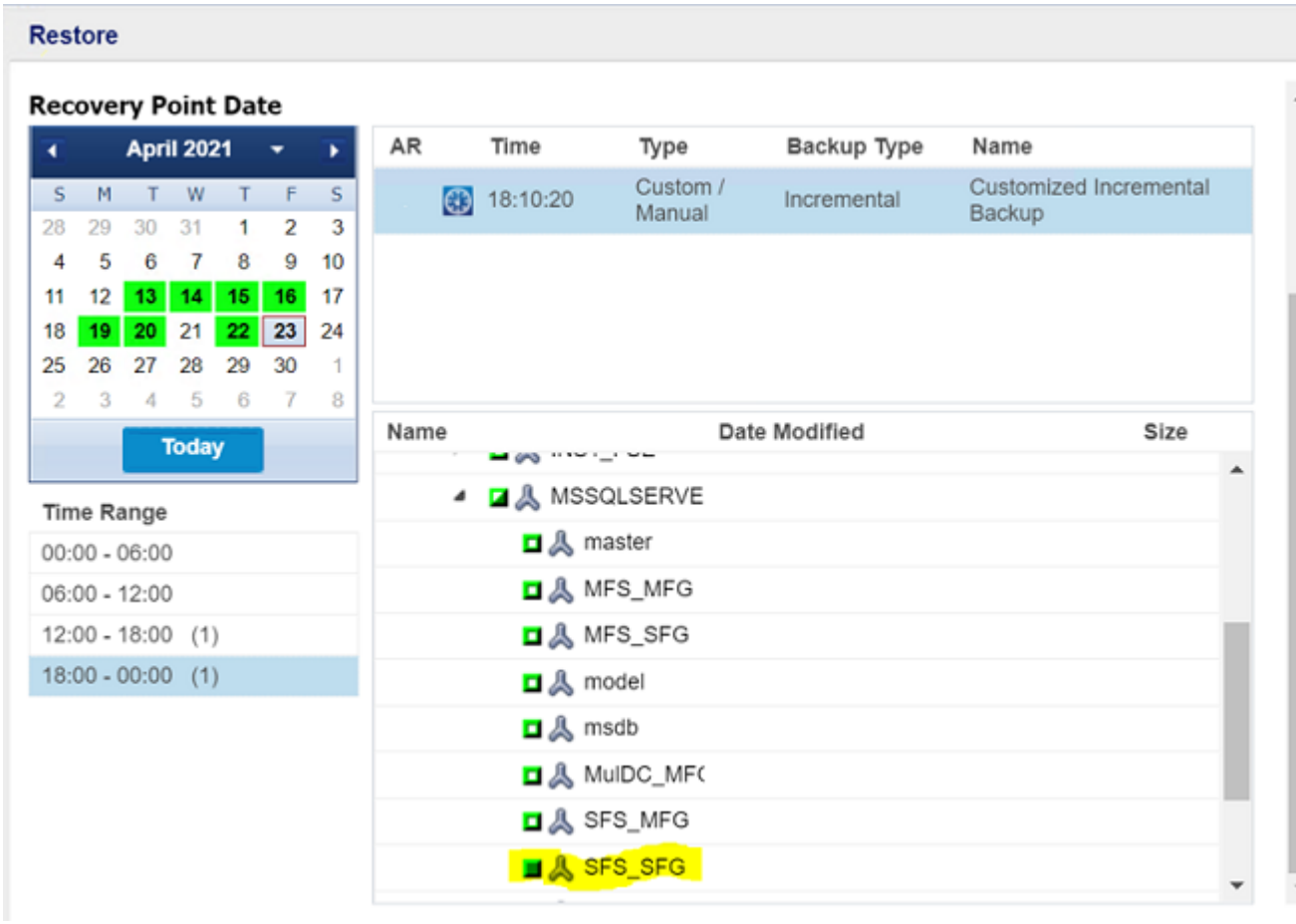
   Observação: o conteúdo entre chaves indica espaços reservados para o nome e os locais, e as chaves não são necessárias ao usar dados reais.
4. Execute a restauração de um banco de dados SQL, conforme necessário.

Restaurar o banco de dados SQL no local original

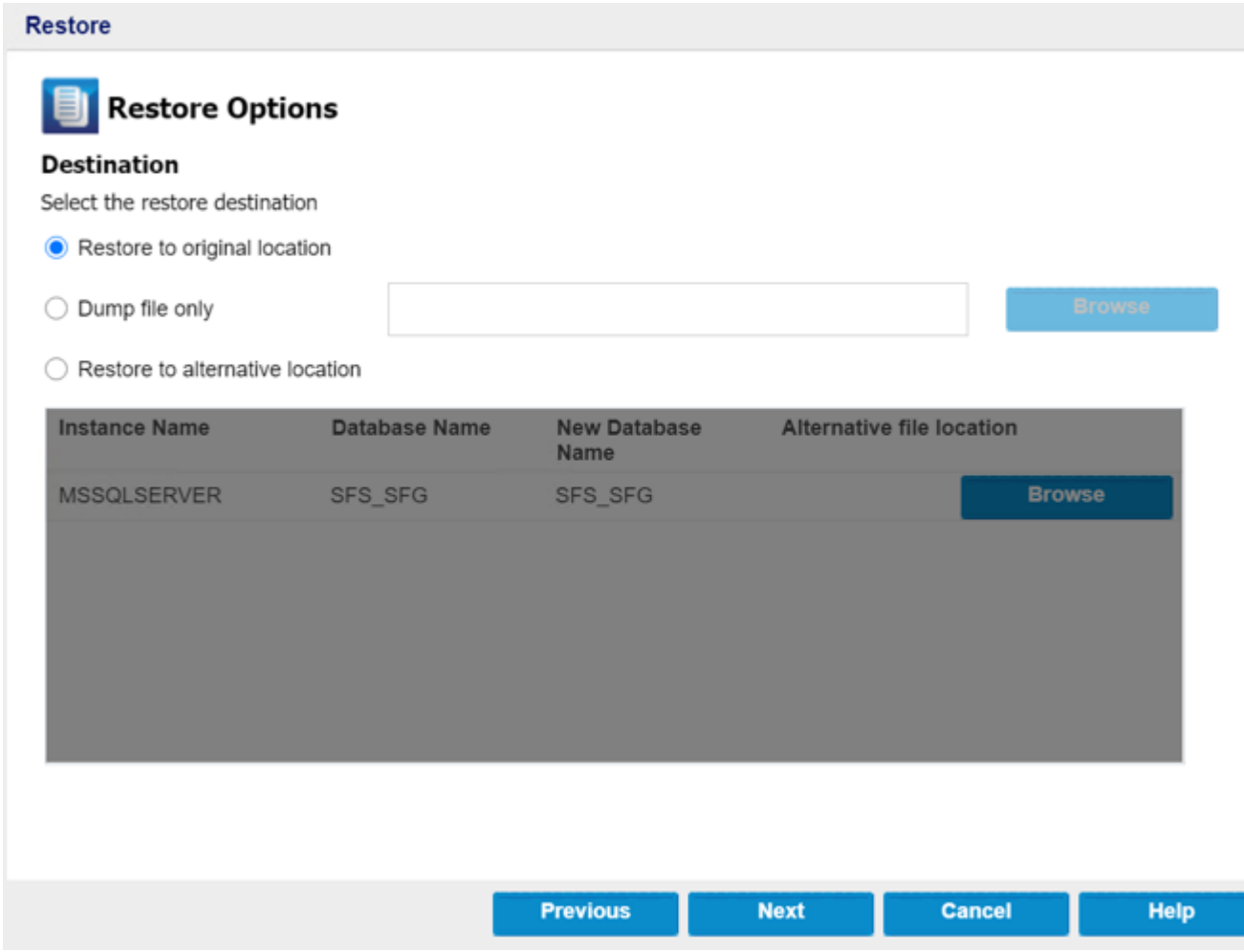
Esta seção fornece informações sobre como restaurar o banco de dados SQL com o Filestream ativado em um local original.

Siga estas etapas:

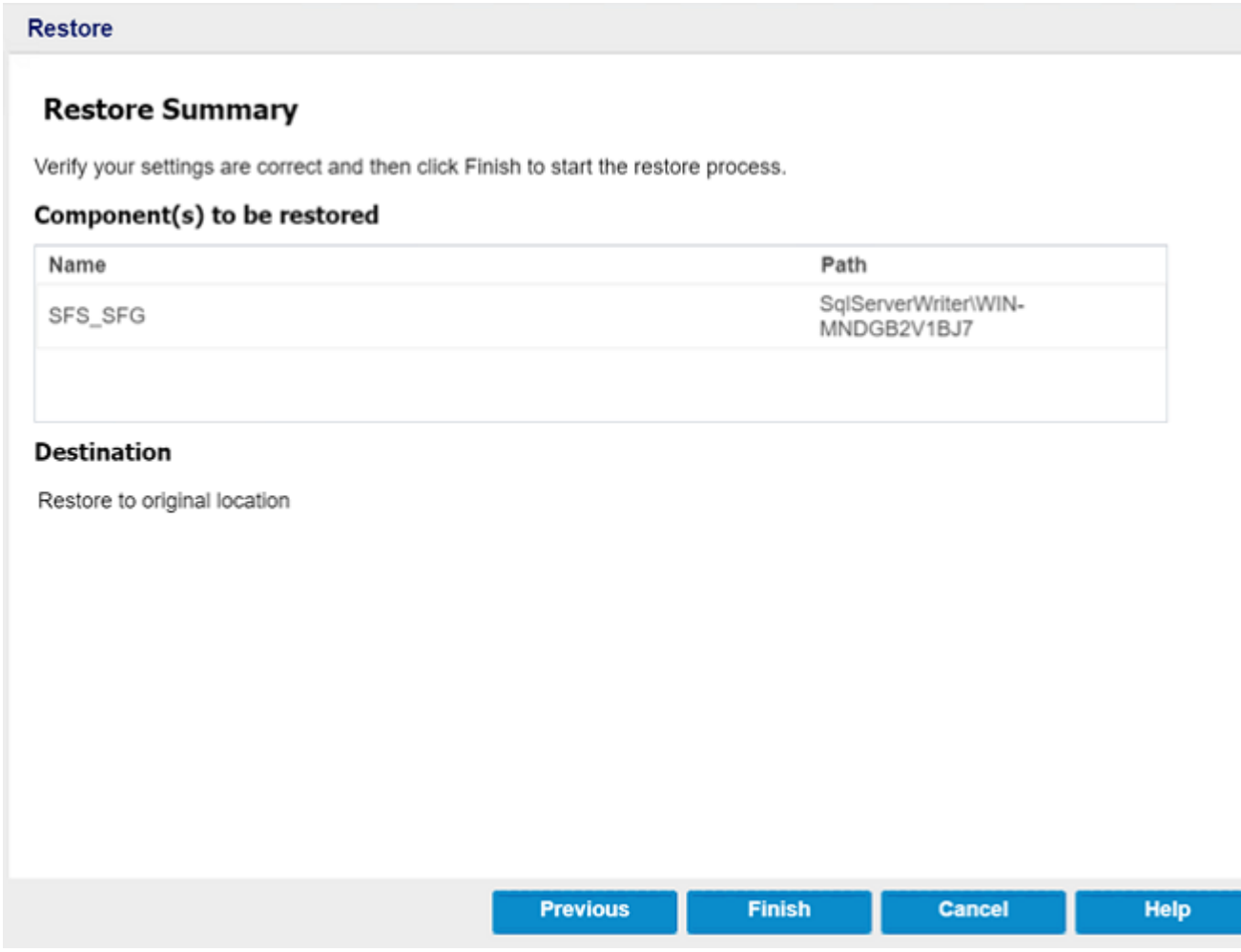
1. Na tela Restaurar, selecione Data do ponto de recuperação, Intervalo de tempo e banco de dados SQL e, em seguida, clique em **Avançar**.



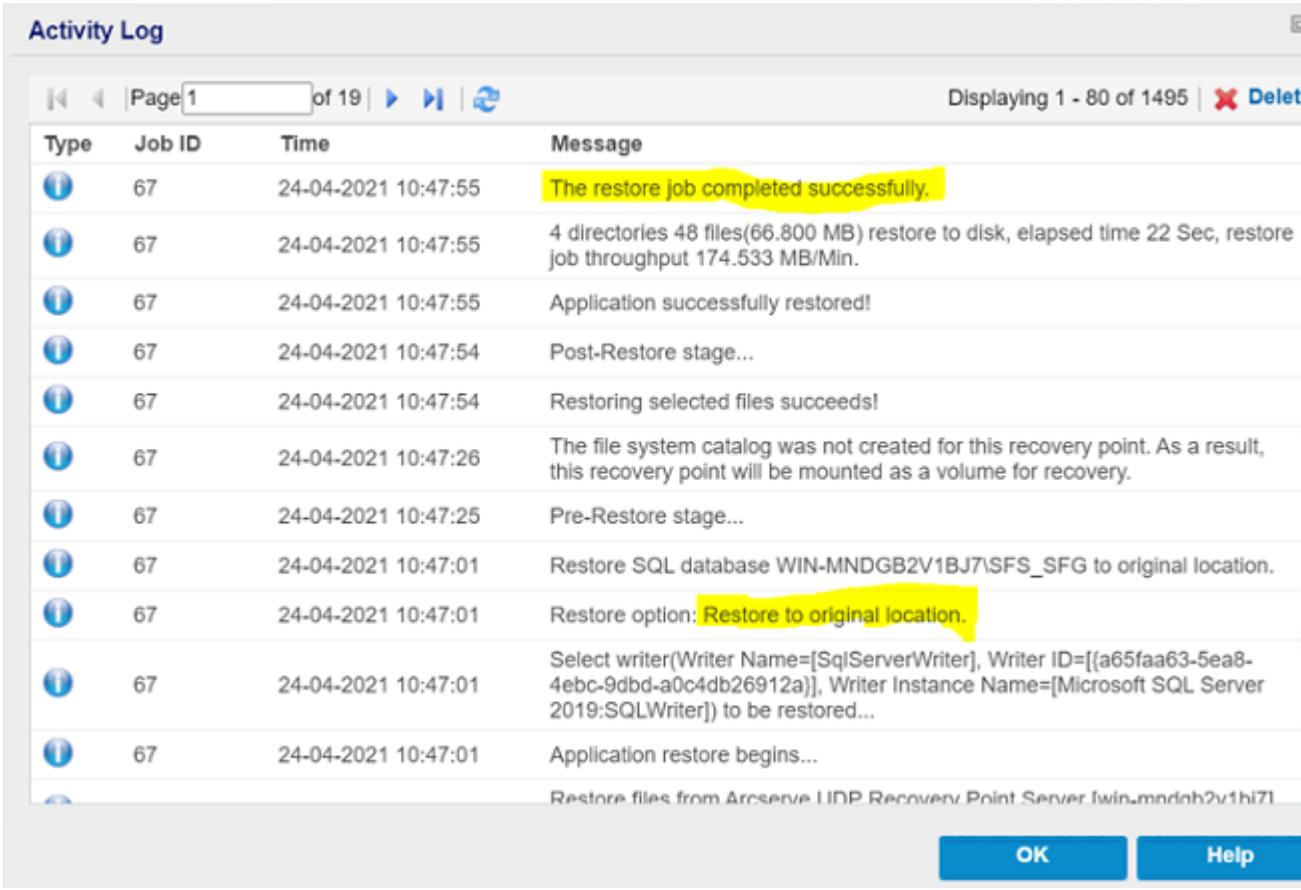
2. Na tela Opções de restauração, em Destino, selecione **Restaurar no local original** e, em seguida, clique no botão **Procurar** para selecionar a instância.



3. Selecione a instância e clique em **Avançar**.
4. Verifique se as configurações estão corretas e clique em **Concluir** para iniciar o processo de restauração no local original.



Exiba os logs de atividades para verificar se o status da restauração foi bem-sucedido.



Restaurar o banco de dados SQL em uma instância alternativa no mesmo servidor

Esta seção fornece informações sobre como restaurar o banco de dados SQL com o Filestream ativado para uma instância alternativa do banco de dados de Filestream ativado, em que as duas instâncias estão no mesmo servidor SQL.

Siga estas etapas:

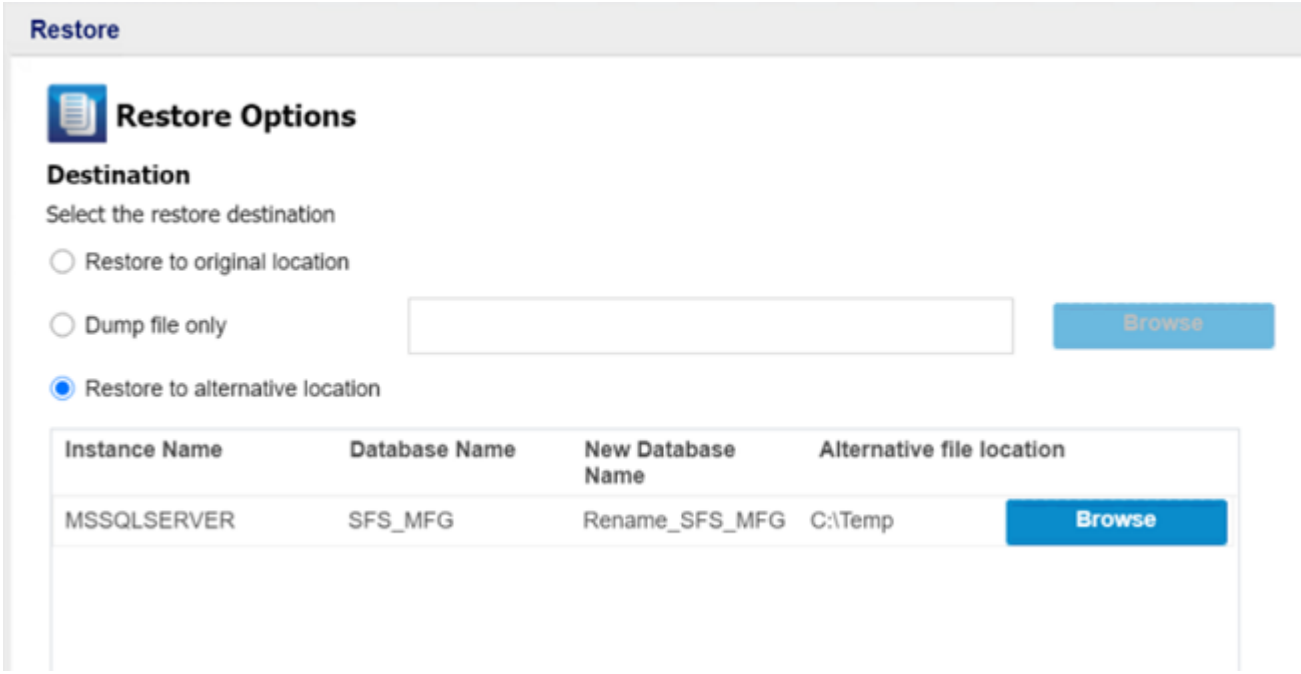
1. Para alterar o nome da instância, abra o arquivo **SqlRestore.ini** e edite **RestoreInstanceName**.

   Por exemplo, altere o nome da instância de *WIN-MNDGB2V1BJ7\MSSQLSERVER* para *WIN-MNDGB2V1BJ7\INS1_FSE*.

   Observação: WIN-MNDGB2V1BJ7 indica o servidor SQL.

Observação: também é possível fornecer o campo *RestoreInstanceName* sem o servidor SQL. Por exemplo, *RestoreInstanceName = INS1_FSE*.

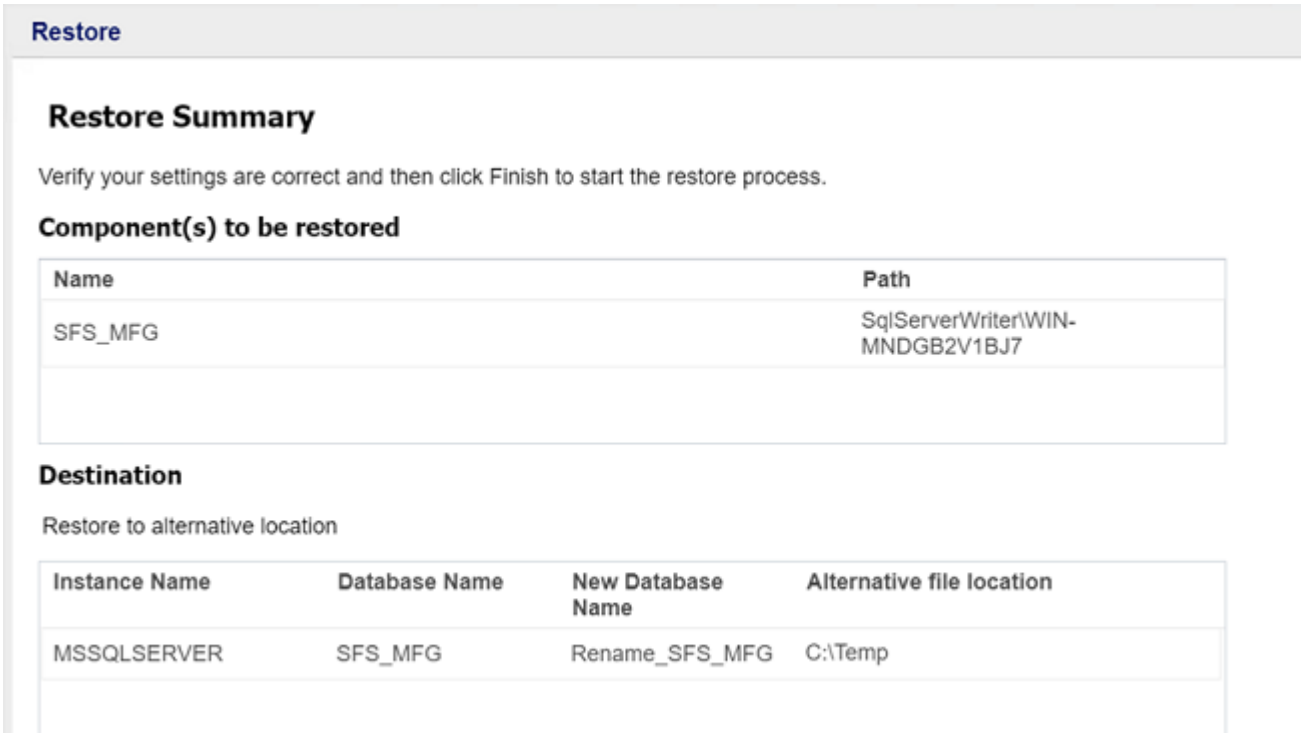
2. No agente, na página Restaurar, selecione o banco de dados que deseja restaurar e clique em **Avançar**.
3. Na tela Opções de restauração, selecione **Restaurar em um local alternativo** e procure a instância.



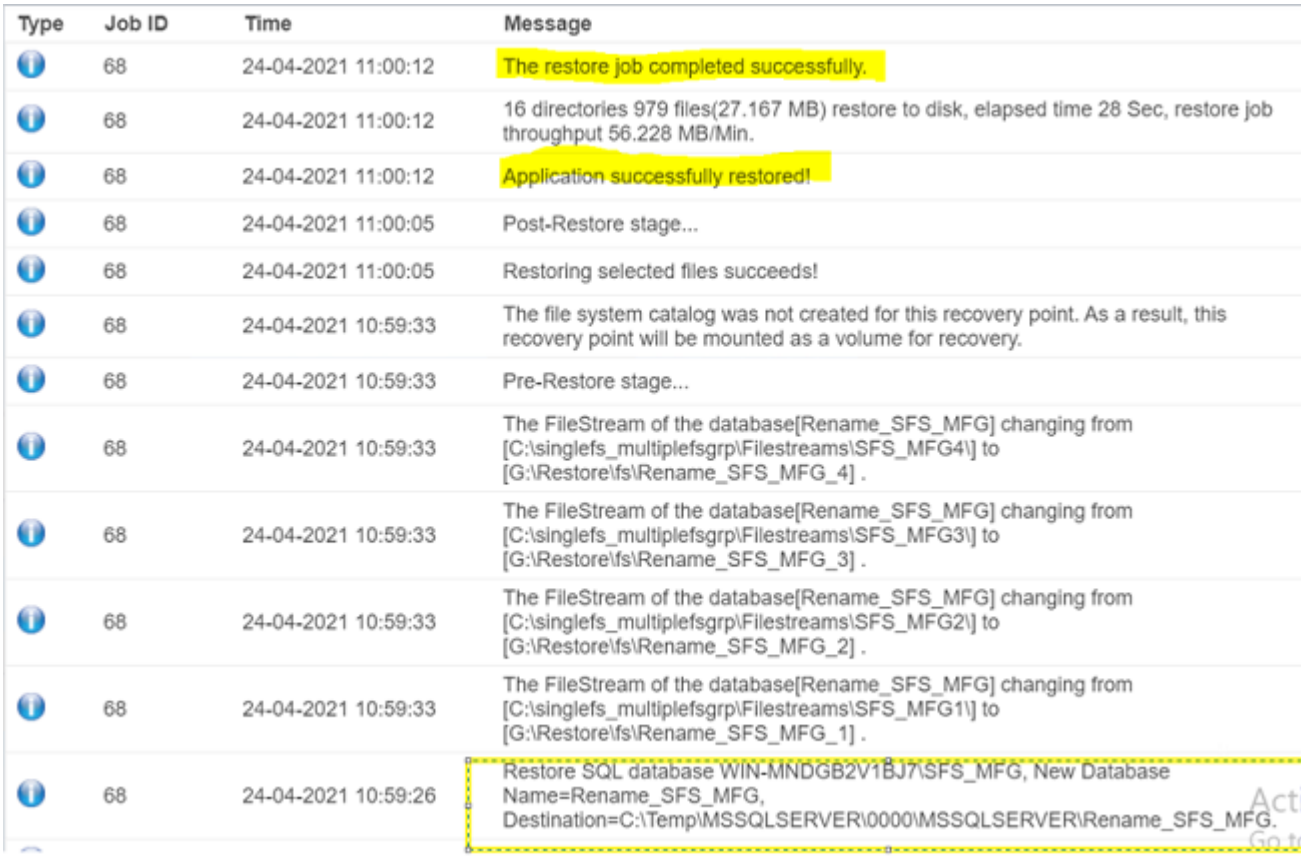
Para renomear o nome do banco de dados, clique na área de texto **Novo nome do banco de dados** e digite o novo nome. Por exemplo, *SFS_MFG* é renomeado como *Rename_SFS_MFG*.

Observação: em Local alternativo de arquivo, uma pasta temporária é selecionada. Este local processa a restauração dos arquivos no local definido no arquivo SqlRestore.ini.

4. Verifique se as configurações estão corretas e clique em **Concluir** para iniciar o processo de restauração.

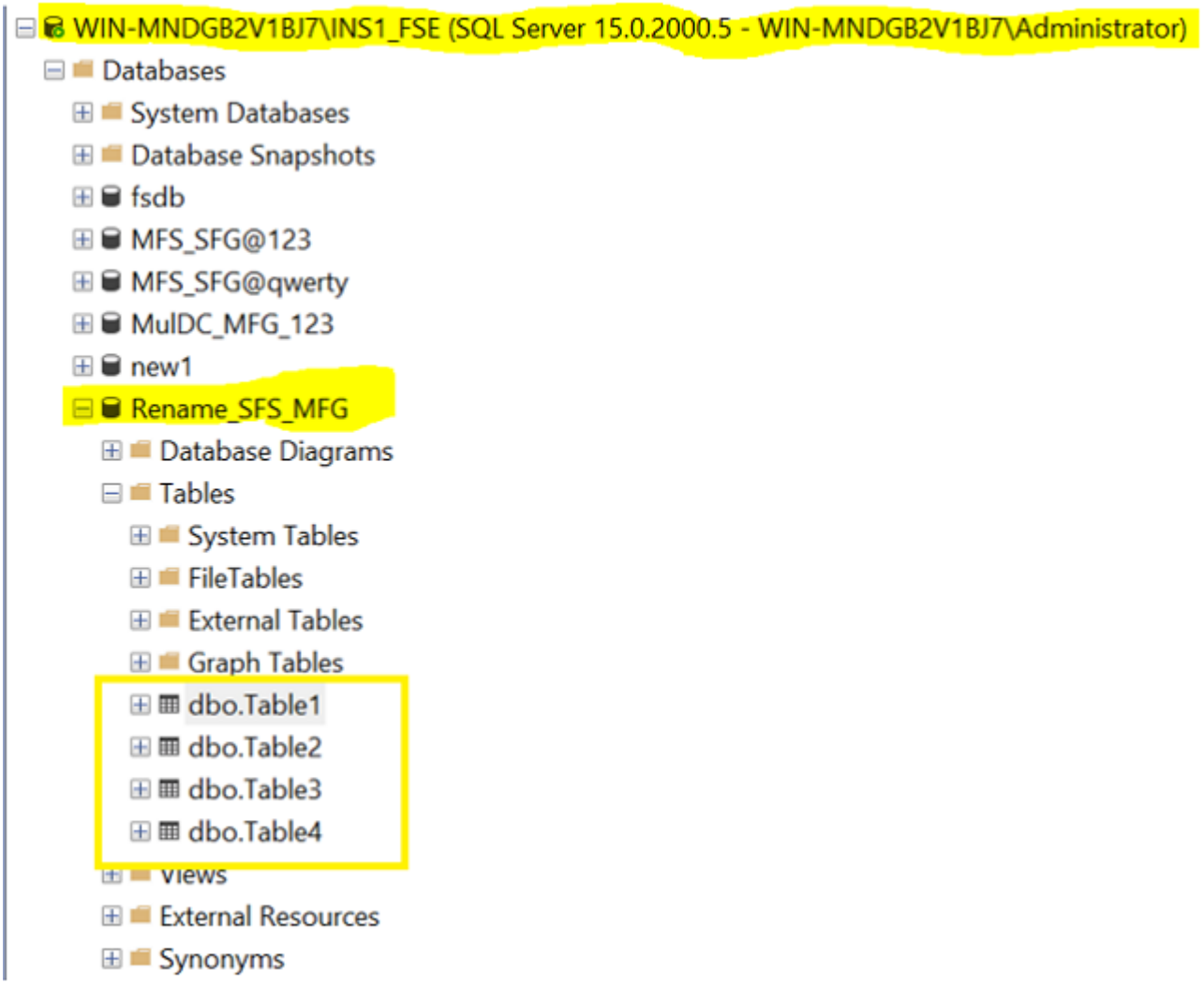


O log de atividades exibe o status da restauração juntamente com a renomeação do banco de dados.

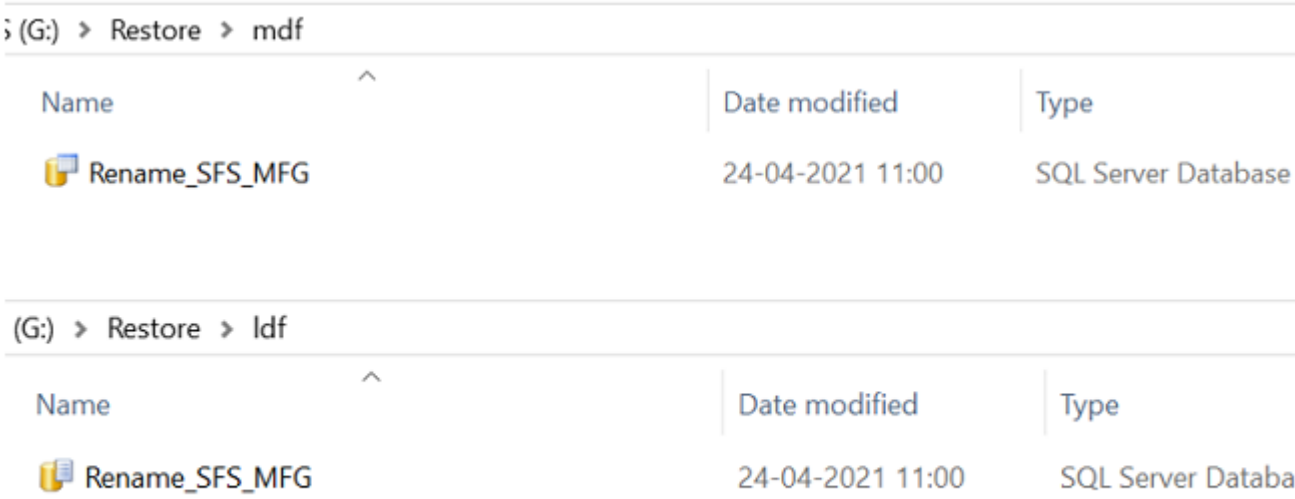


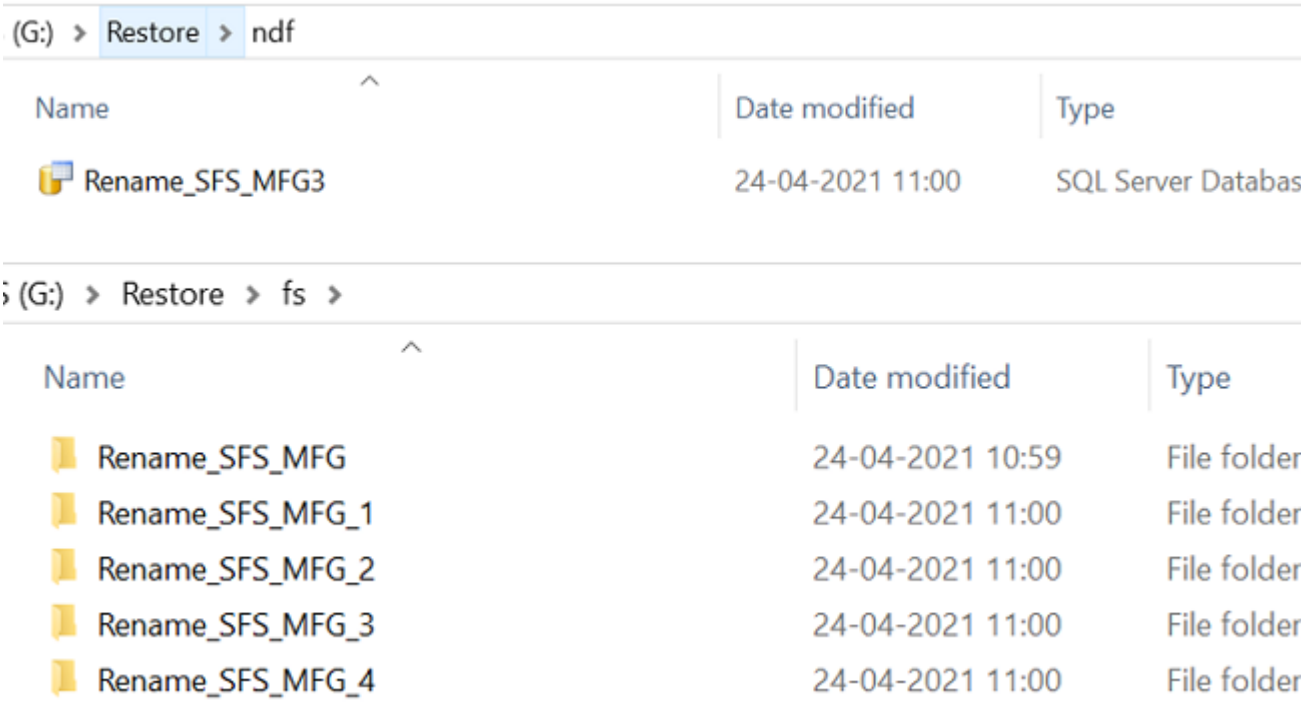
Type	Job ID	Time	Message
	68	24-04-2021 11:00:12	The restore job completed successfully.
	68	24-04-2021 11:00:12	16 directories 979 files(27.167 MB) restore to disk, elapsed time 28 Sec, restore job throughput 56.228 MB/Min.
	68	24-04-2021 11:00:12	Application successfully restored!
	68	24-04-2021 11:00:05	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.

As alterações no nome da instância e do banco de dados são refletidas no SQL Management Studio.



Conforme definido no arquivo SqlRestore.ini, os arquivos LDF, MDF e Files-tream são armazenados em suas respectivas pastas.



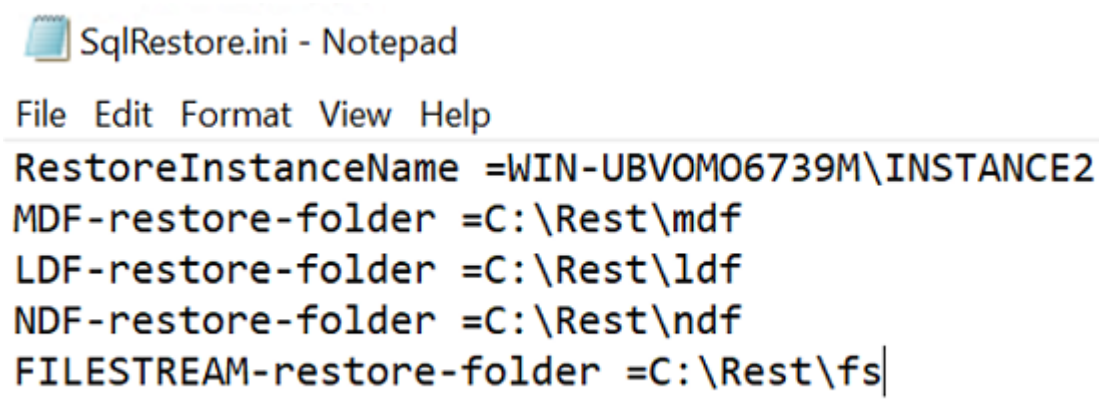


Restaurar o banco de dados SQL em uma instância alternativa em um servidor diferente

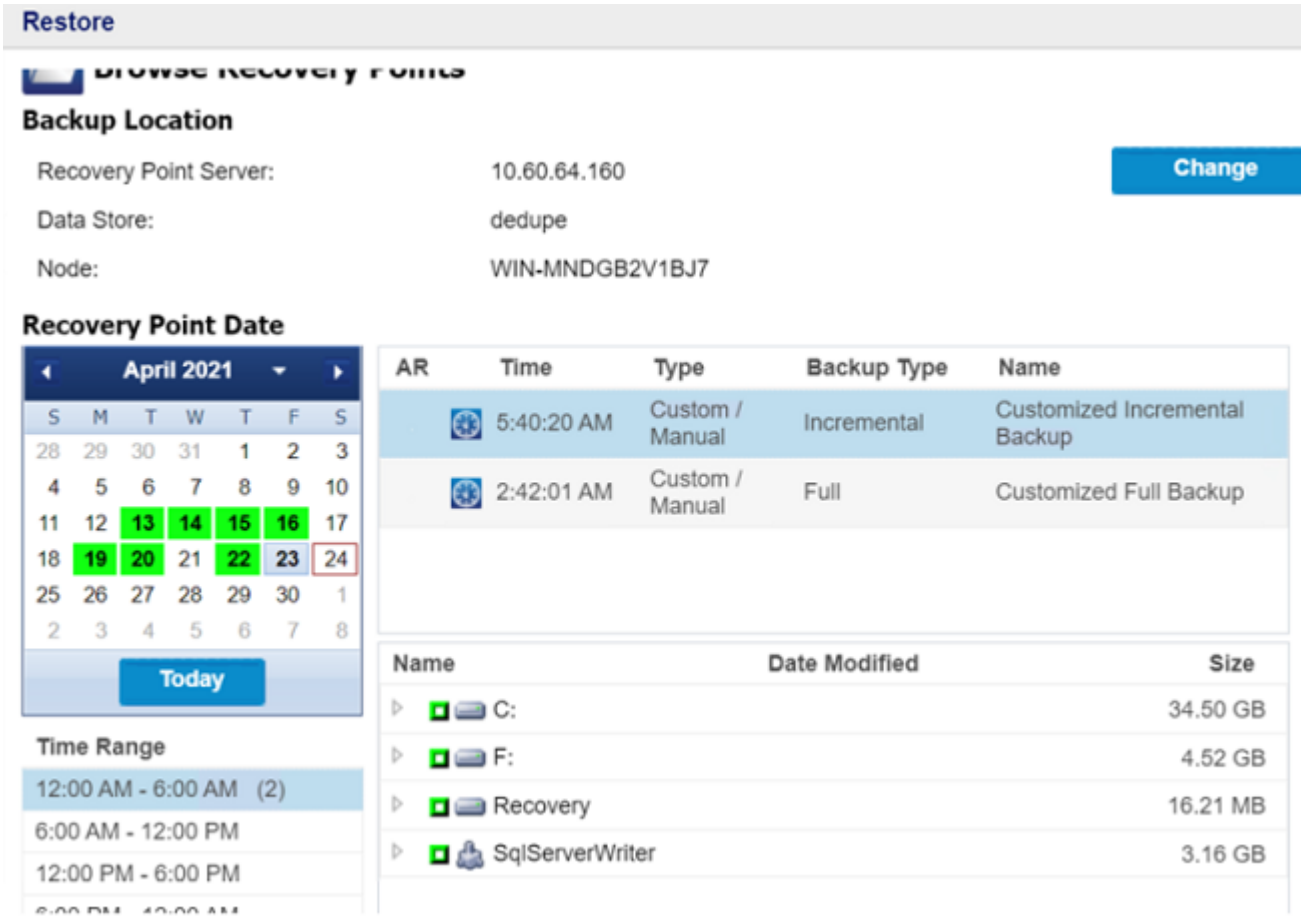
Esta seção fornece informações sobre como restaurar o banco de dados SQL com o Filestream ativado para uma instância alternativa do banco de dados de Filestream ativado, em que as duas instâncias estão em um servidor SQL diferente. Por exemplo, se o banco de dados estiver no servidor de origem WIN- MNDGB2V1BJ7 e na instância de origem MSSQLSERVER, ele poderá ser restaurado no servidor de destino WIN-UBVOMO6739M e na instância de destino INSTANCE2.

Siga estas etapas:

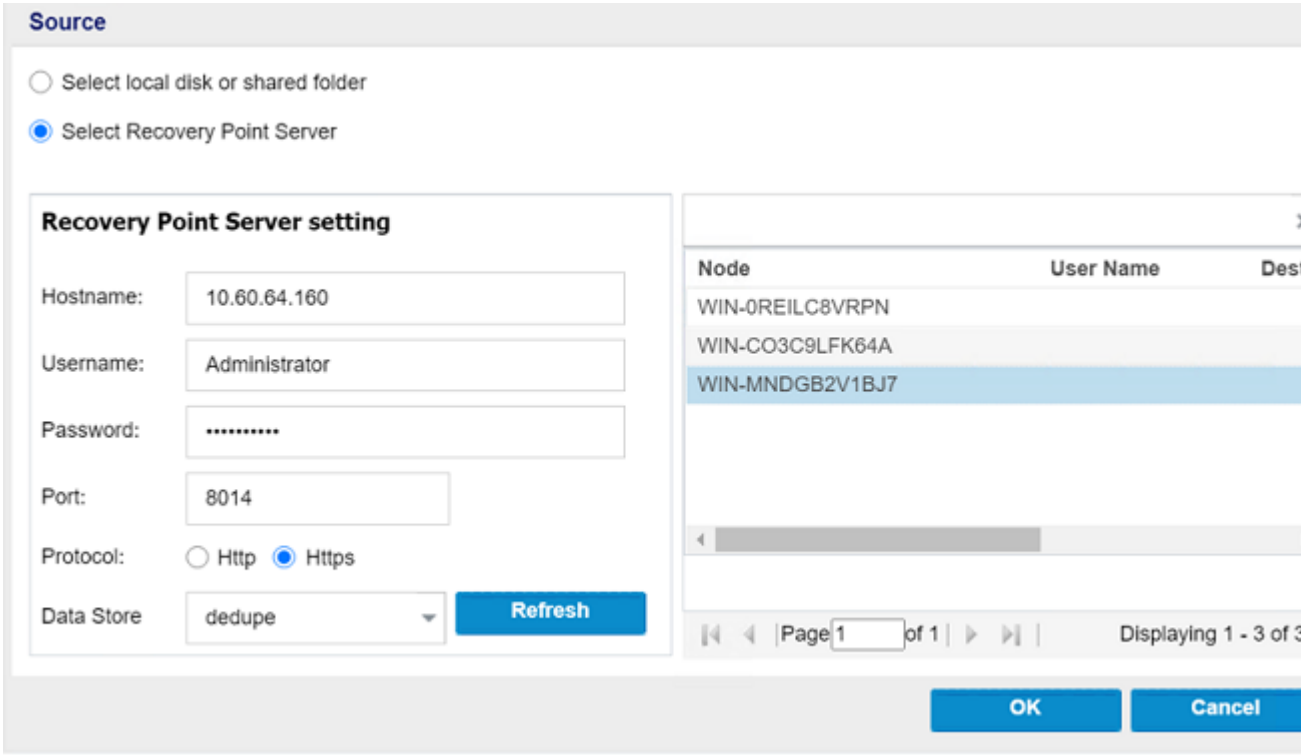
1. Para restaurar o banco de dados para o servidor (WIN-UBVOMO6739M) e para a instância (INSTANCE2) alternativos, modifique o arquivo SqlRestore.ini.



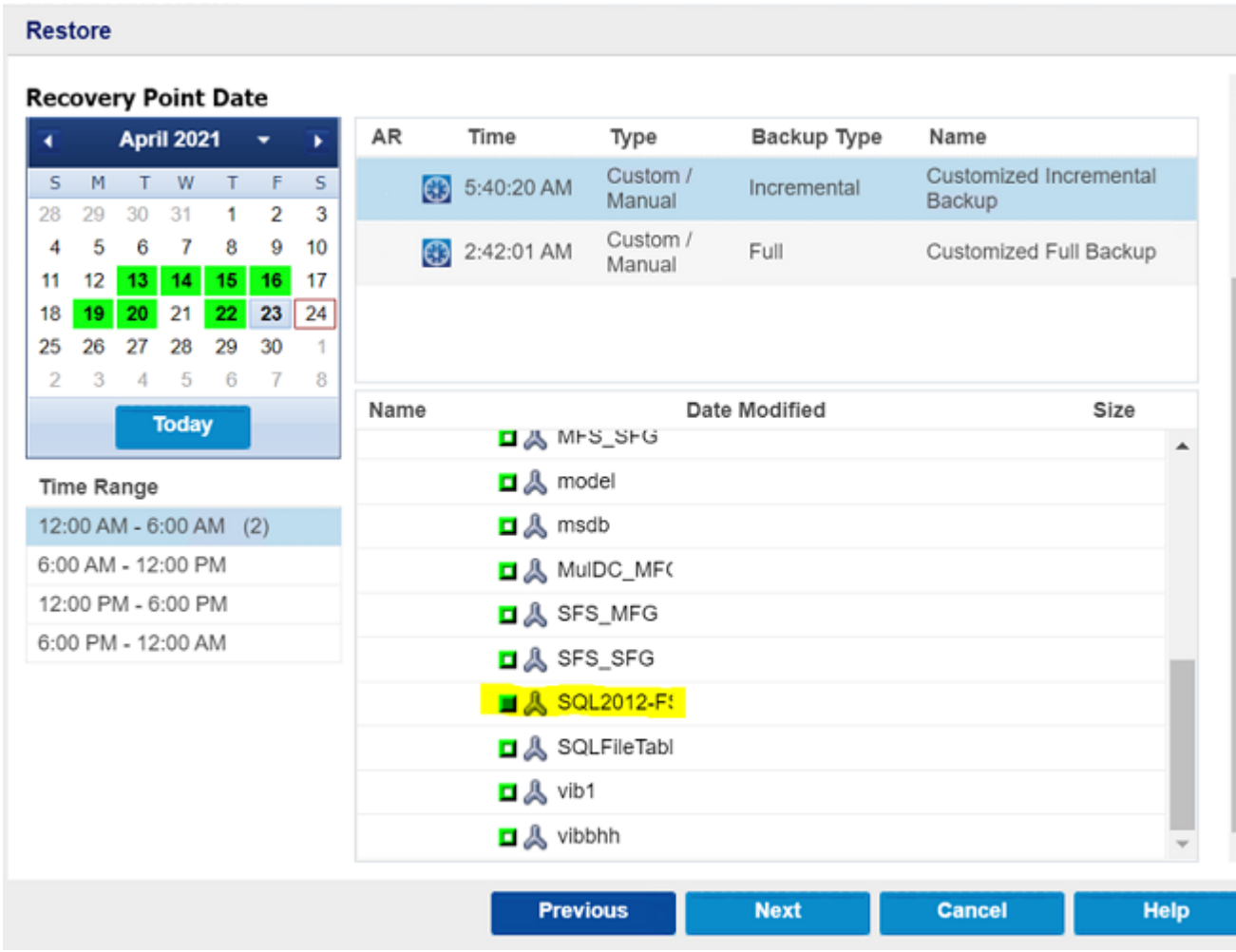
2. Para alterar o local do RPS (Recovery Point Server - Servidor de Ponto de Recuperação) para restaurar os servidores e as instâncias no servidor alternativo, clique no botão **Alterar** e forneça os novos detalhes do RPS.



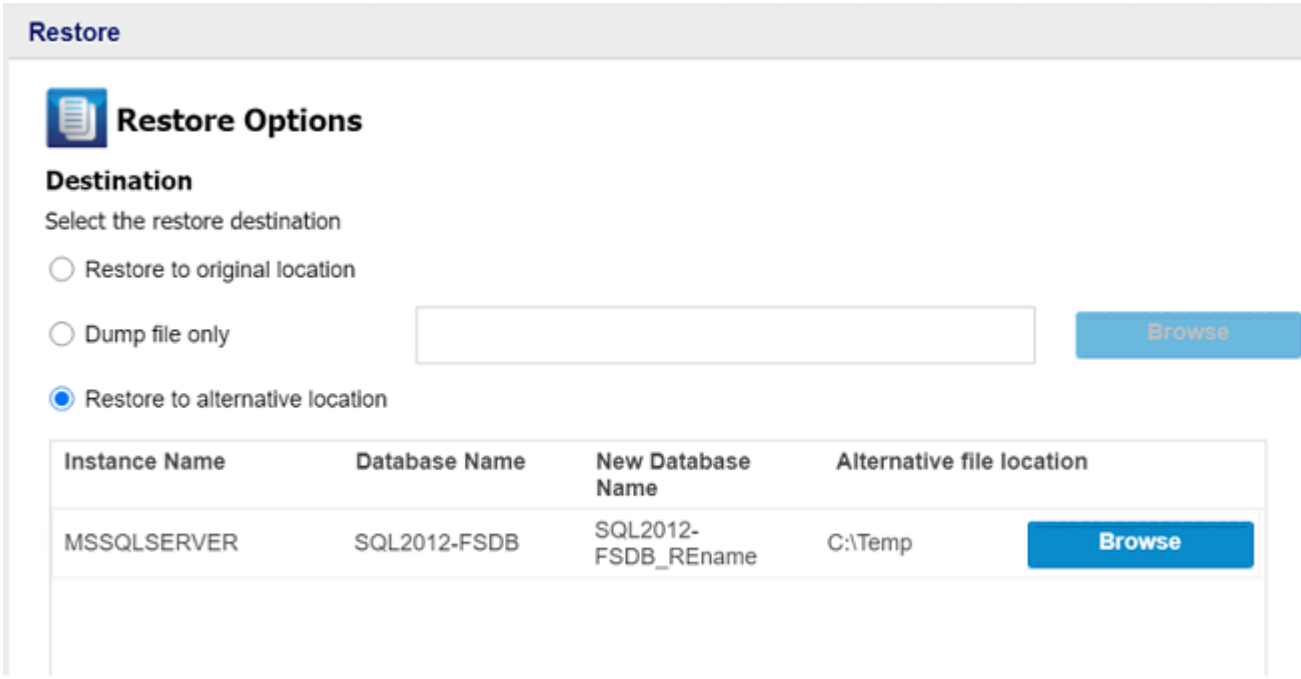
3. Para selecionar o RPS de origem, clique em **Selecionar servidor de ponto de recuperação**, selecione o servidor de origem (WIN-MNDGB2V1BJ7) e clique em **OK**.



4. Para restaurar em um servidor alternativo, selecione o banco de dados (SQL2012-FSDB) e clique em **Avançar**.



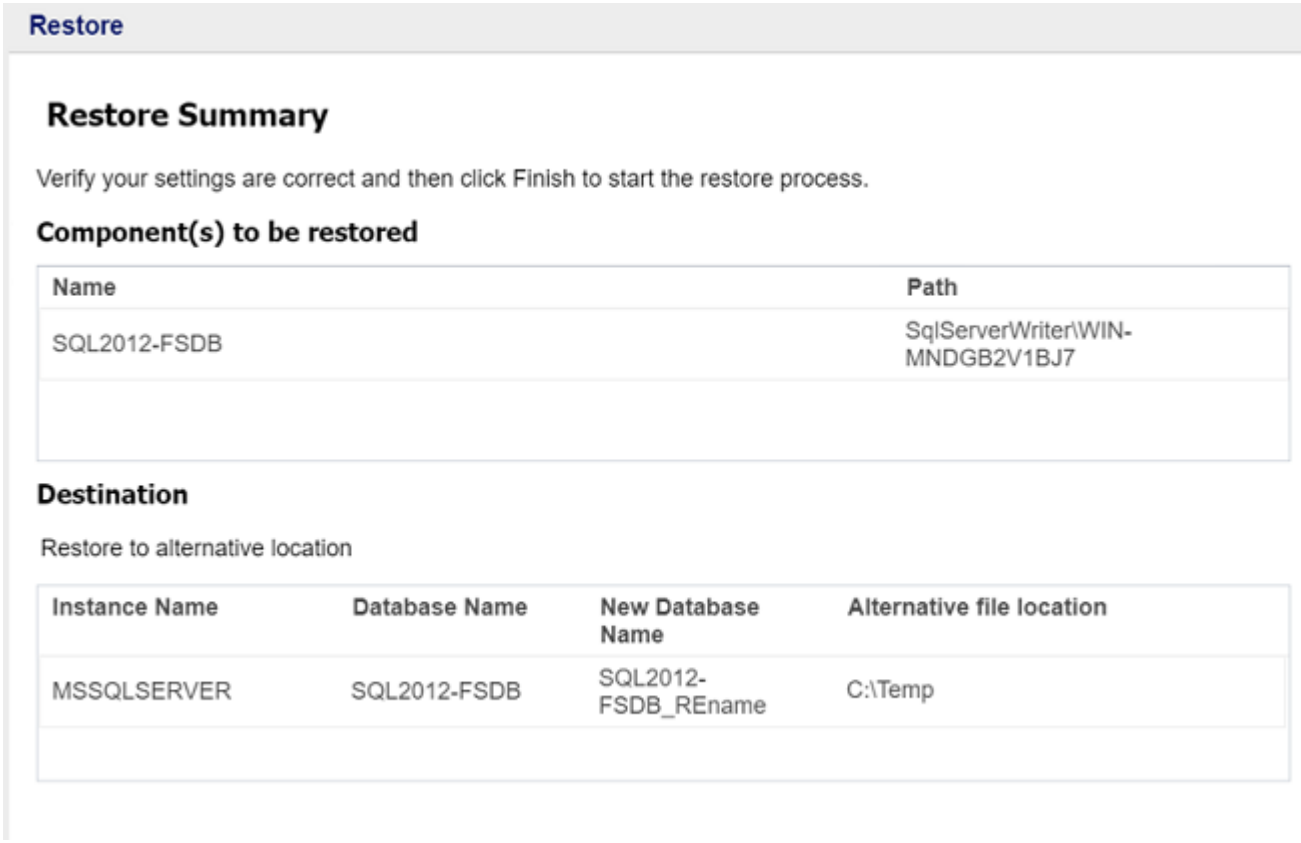
5. Na tela Opções de restauração, selecione **Restaurar em um local alternativo** e procure a instância.



Para renomear o nome do banco de dados, clique na área de texto **Novo nome do banco de dados** e digite o novo nome. Por exemplo, SQL2012-FSDB é renomeado como SQL2012-FSDB-REname.

Observação: em Local alternativo de arquivo, uma pasta temporária é selecionada. Este local processa a restauração dos arquivos no local definido no arquivo SqlRestore.ini.

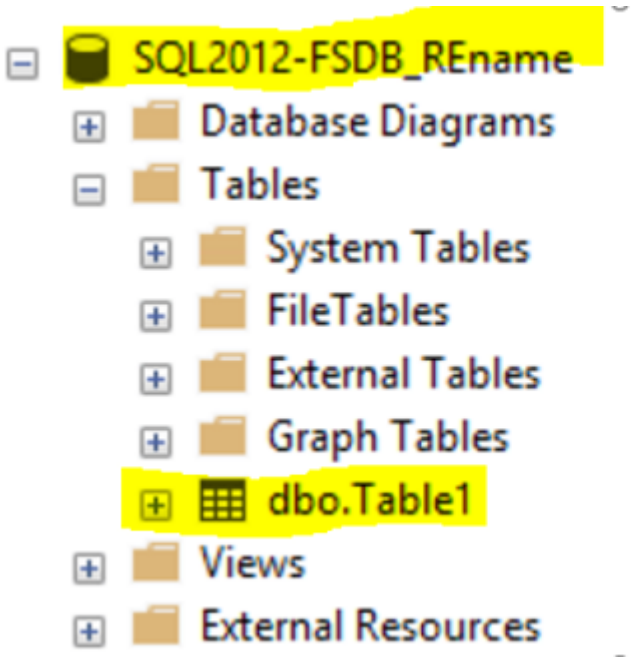
6. Verifique se as configurações estão corretas e clique em **Concluir** para iniciar o processo de restauração.



O log de atividades exibe o status da restauração juntamente com a renomeação do banco de dados.

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.

A alteração no nome do banco de dados é refletida no SQL Management Studio.



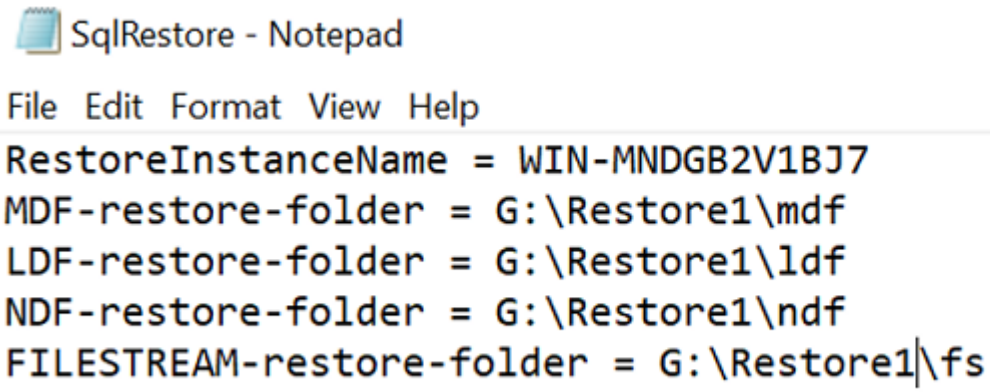
Restaurar o banco de dados SQL em um local alternativo na mesma instância

Esta seção fornece informações sobre como restaurar o banco de dados SQL com o Filestream ativado em um local alternativo, mas na mesma instância, ao renomear o banco de dados.

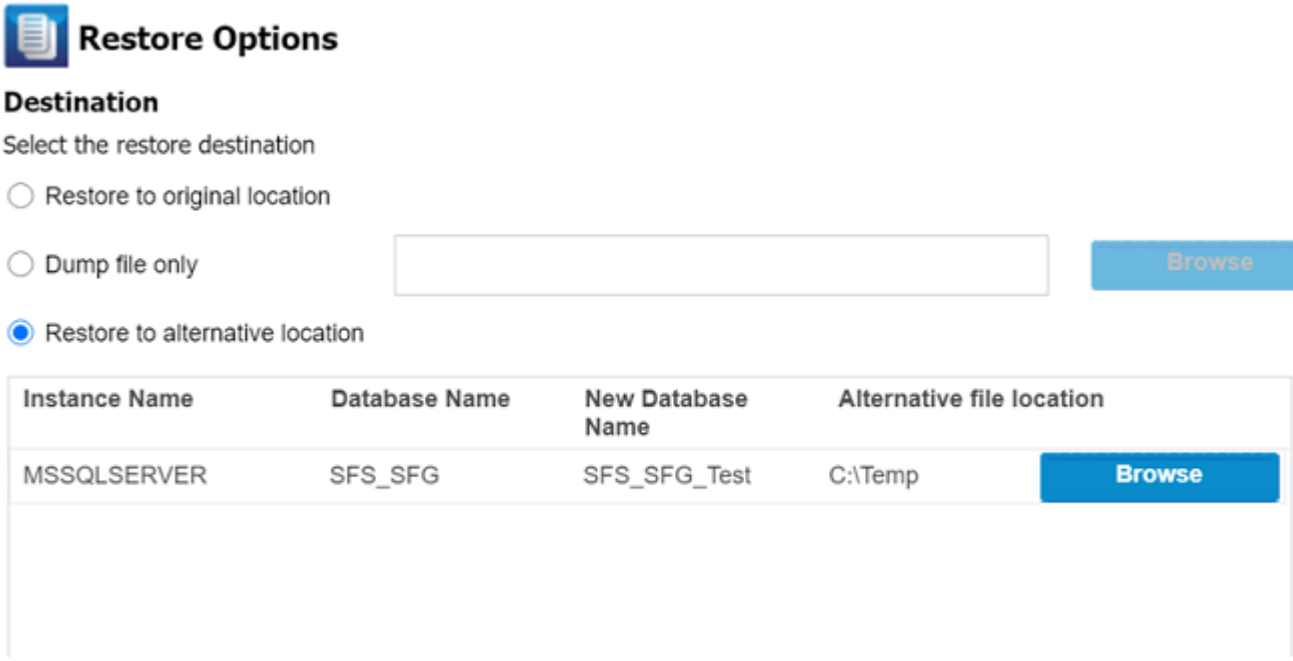
Siga estas etapas:

1. Para modificar o banco de dados de restauração em um local alternativo, abra o arquivo SqlRestore.ini e altere os locais da pasta conforme necessário.

   Por exemplo, altere os locais da pasta de *C:\singlefs_singlefsgrp\ SFS_SFG1* para *G:\Restore1\fs1*.



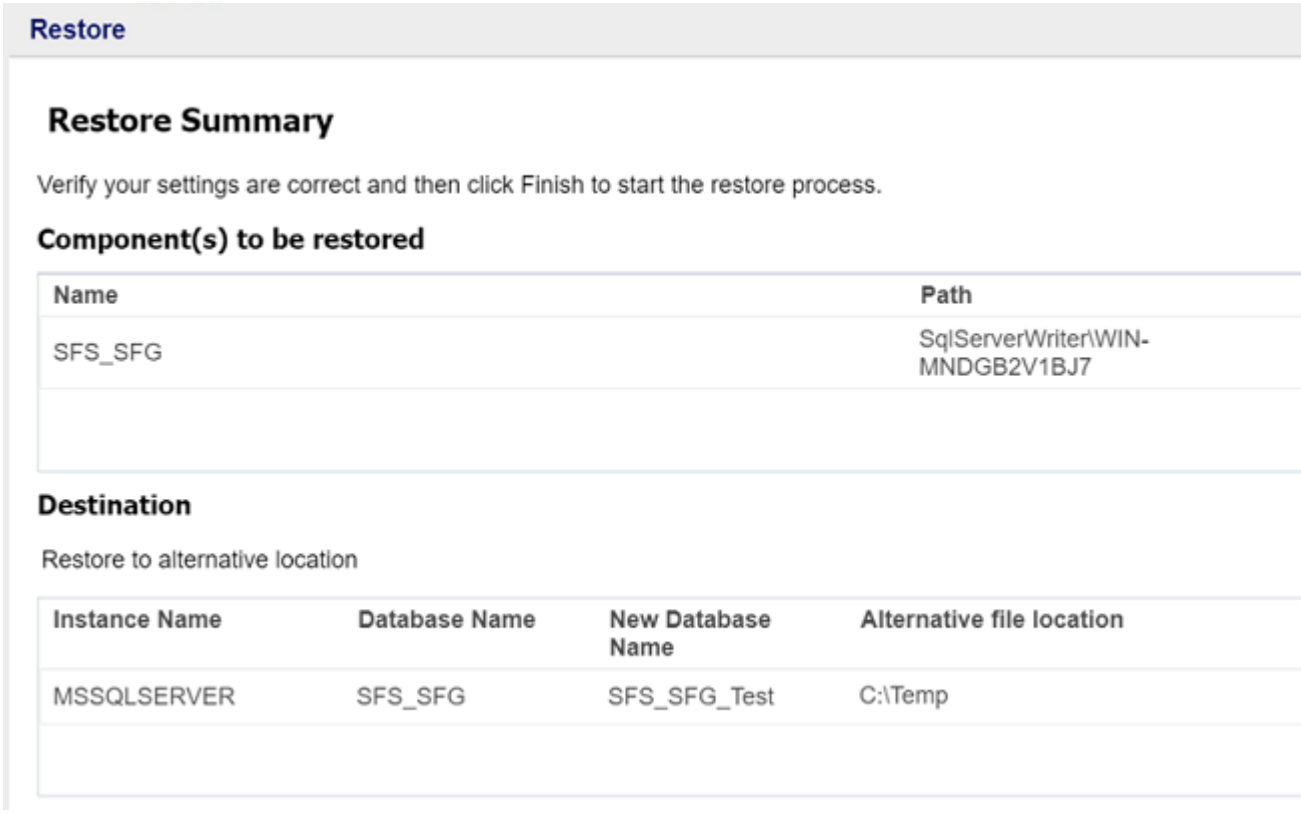
2. No agente, na página Restaurar, selecione o banco de dados que deseja restaurar e clique em **Avançar**.
3. Na tela Opções de restauração, selecione **Restaurar em um local alternativo** e procure a instância.



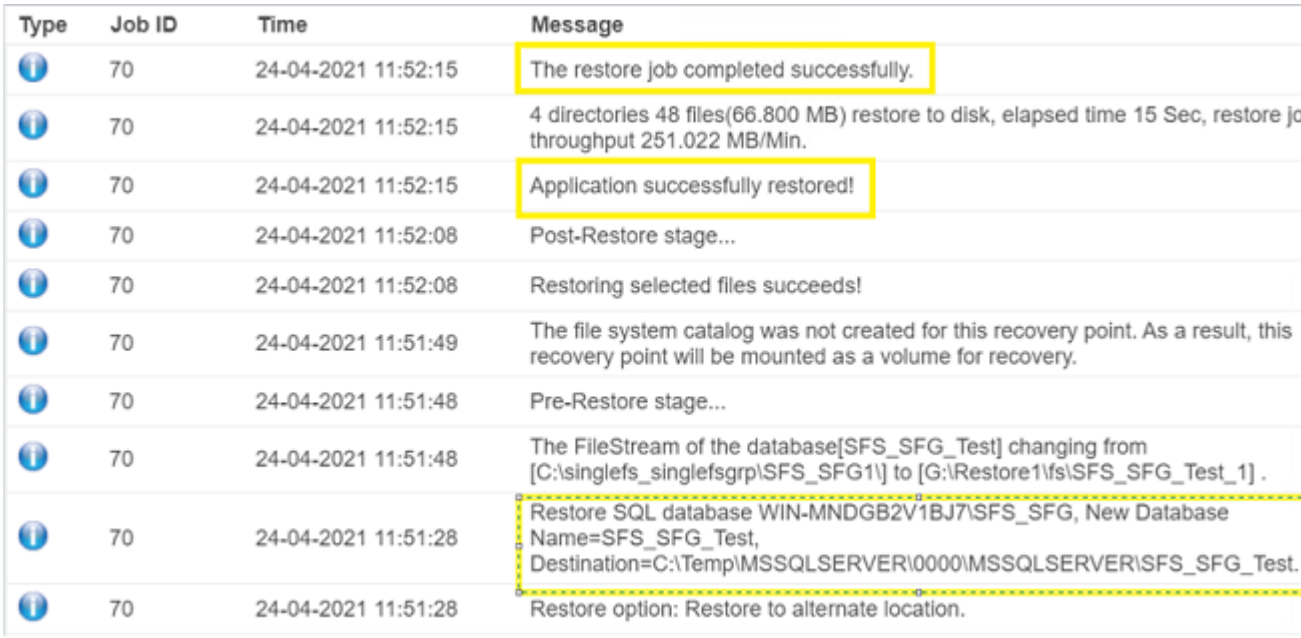
Para renomear o nome do banco de dados, clique na área de texto **Novo nome do banco de dados** e digite o novo nome. Por exemplo, *SFS_SFG* é renomeado como *SFS_SFG_Test*.

Observação: em Local alternativo de arquivo, uma pasta temporária é selecionada. Este local processa a restauração dos arquivos no local definido no arquivo SqlRestore.ini.

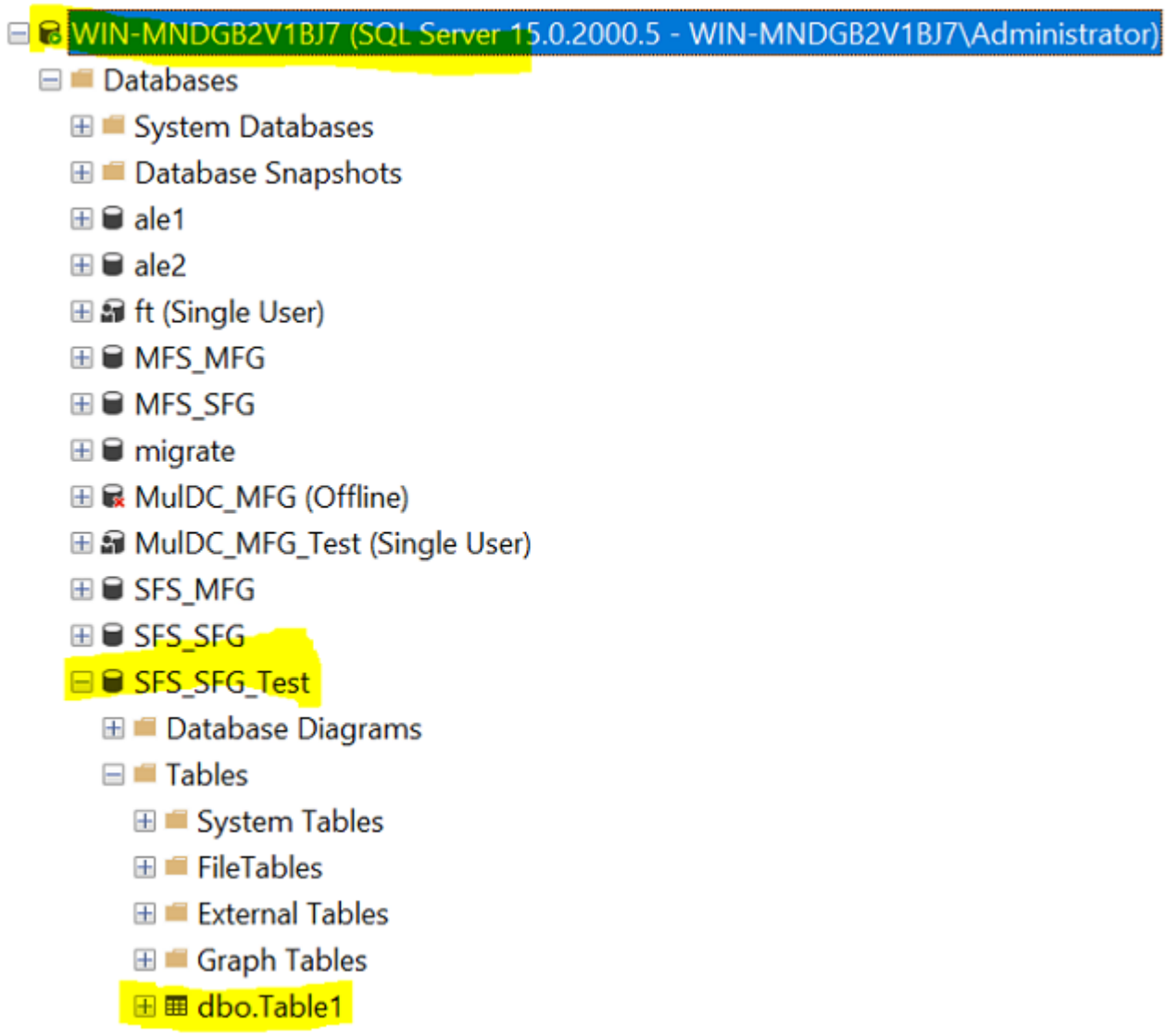
4. Verifique se as configurações estão corretas e clique em **Concluir** para iniciar o processo de restauração.



O log de atividades exibe o status da restauração juntamente com a renomeação do banco de dados.



A alteração no nome do banco de dados é refletida no SQL Management Studio.

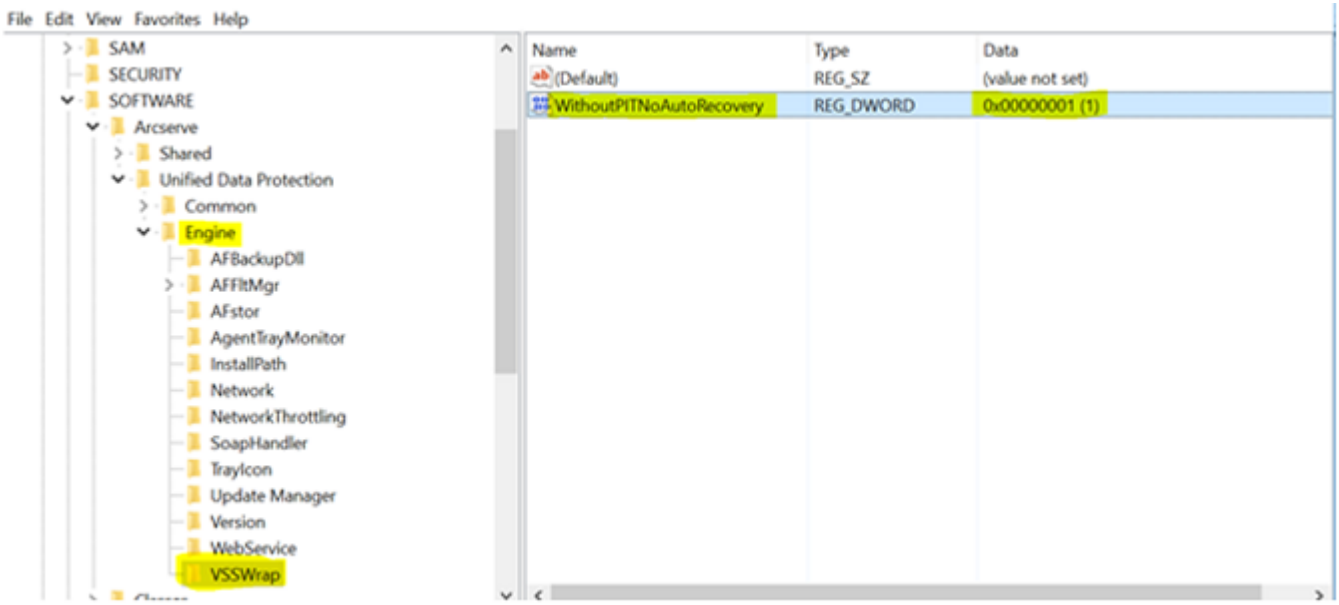


Modo de restauração por meio da chave do Registro

Esta seção fornece informações sobre como usar o modo de restauração usando a chave do Registro. Este método restaura o banco de dados do Filestream ativado para a instância alternativa (INS1_FSE).

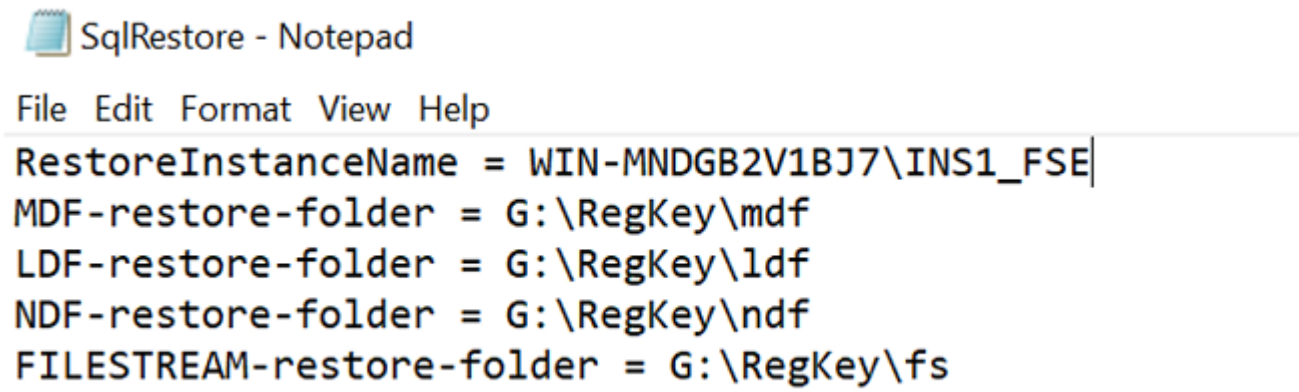
Depois que o backup for bem-sucedido, adicione a chave do Registro à pasta VSSW-rap com o valor DWORD de 32 bits: *WithoutPITNoAutoRecovery* e defina o valor como 1.

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\VSSWrap\

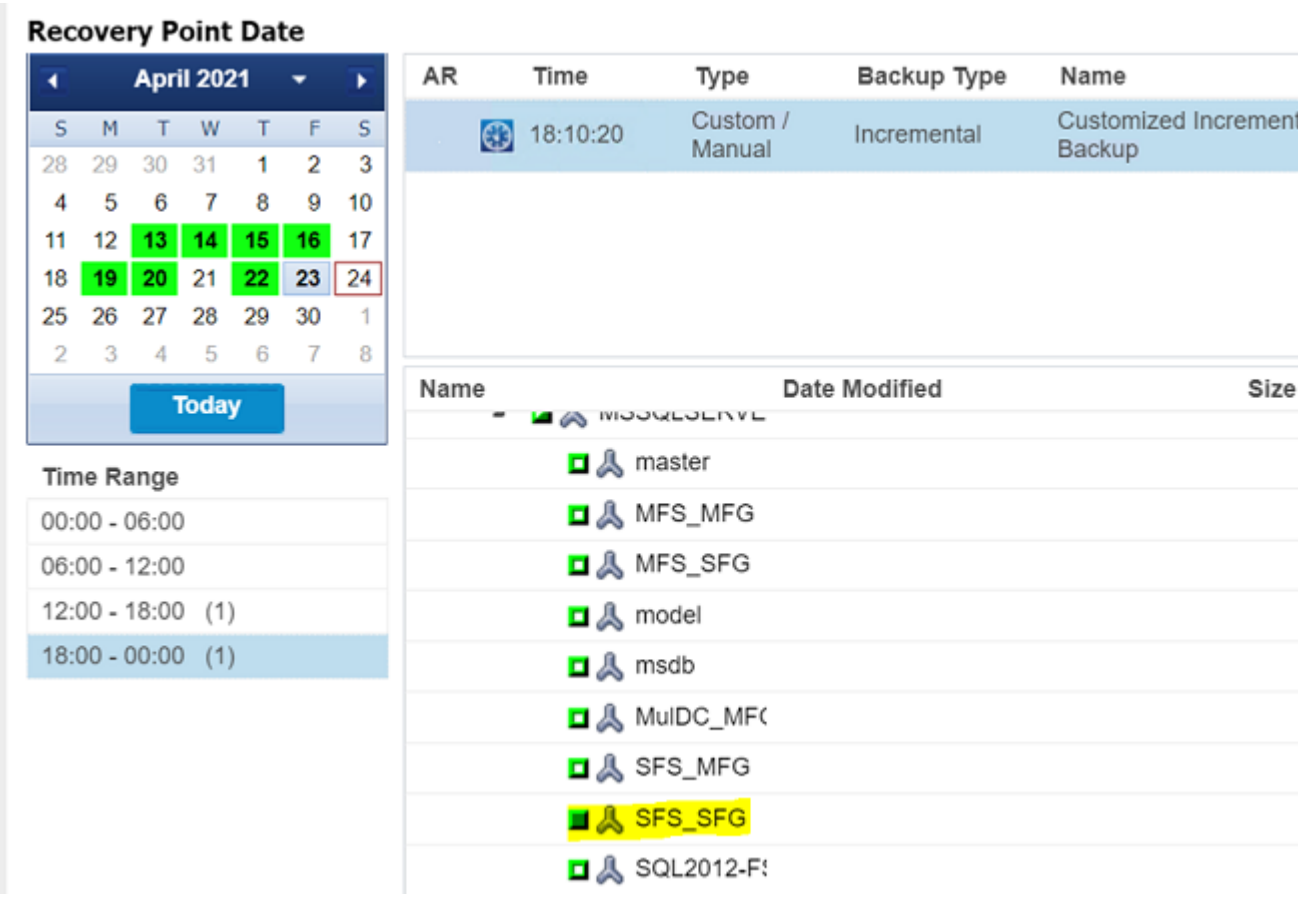


Siga estas etapas:

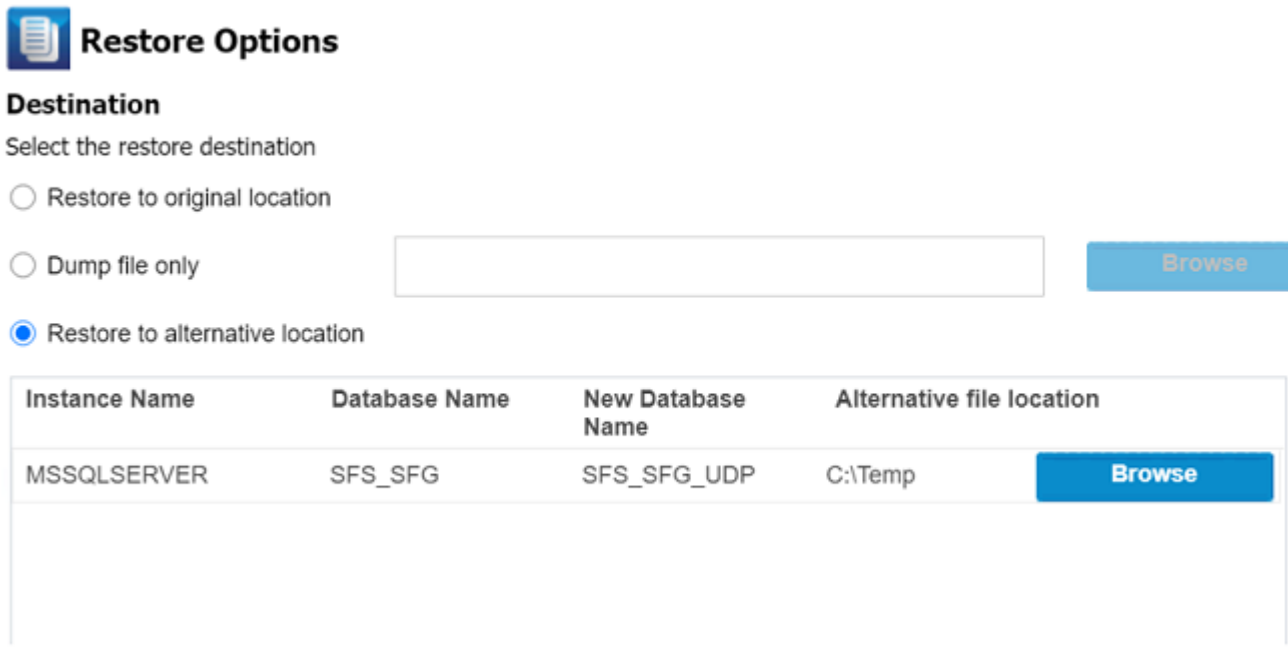
1. Para restaurar o banco de dados para uma instância alternativa, abra o arquivo SqlRestore.ini e altere os locais da pasta conforme necessário.



2. No agente, na página Restaurar, selecione o banco de dados que deseja restaurar e clique em **Avançar**.



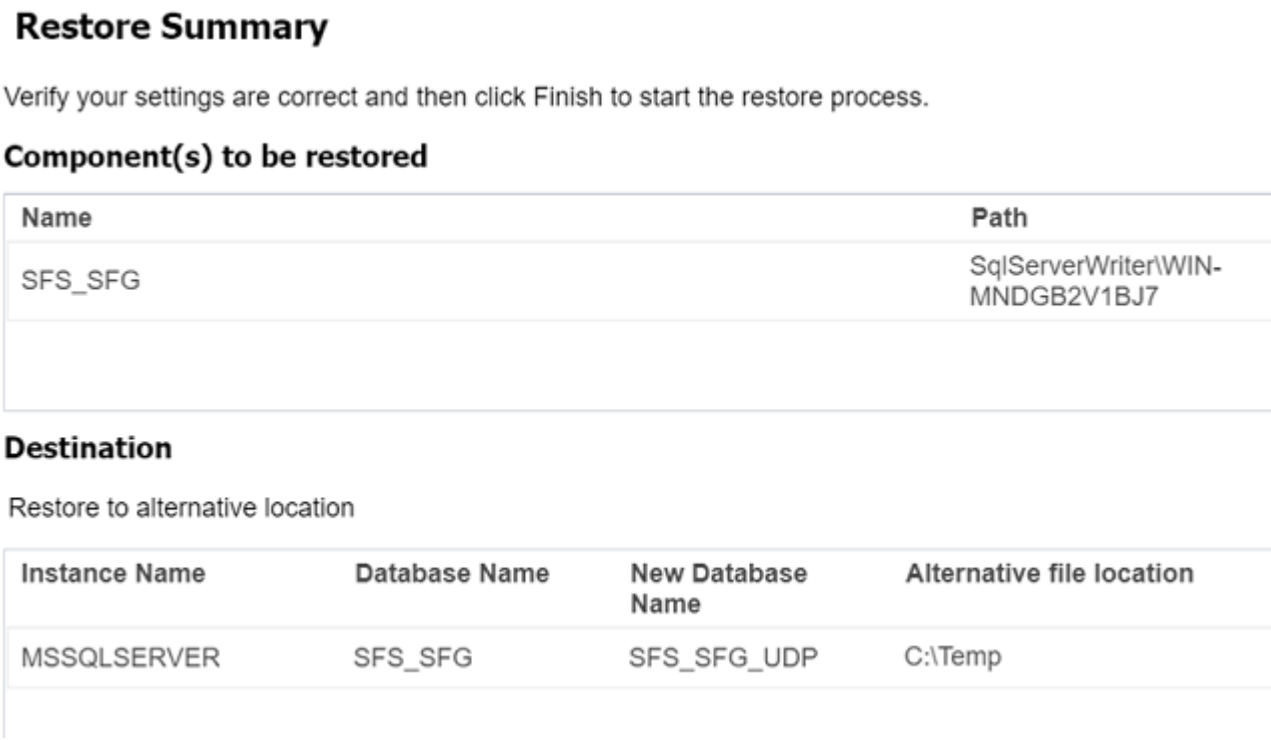
3. Na tela Opções de restauração, selecione **Restaurar em um local alternativo** e procure a instância.



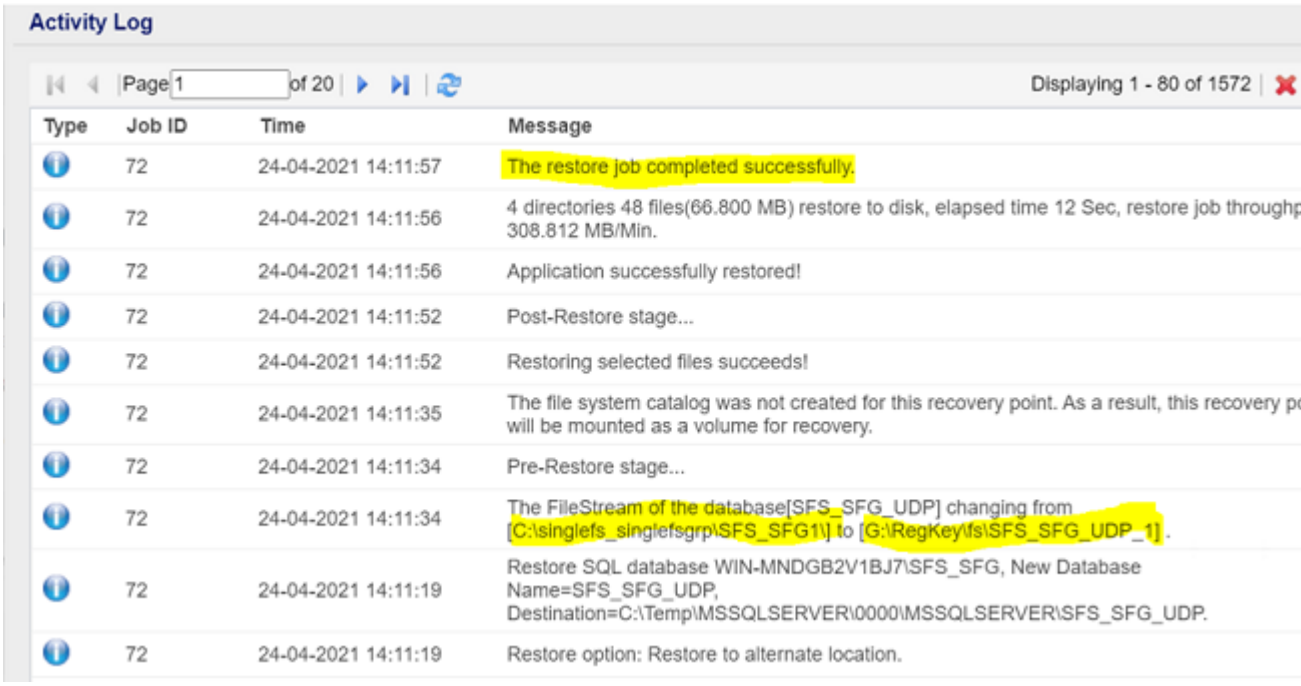
Para renomear o nome do banco de dados, clique na área de texto **Novo nome do banco de dados** e digite o novo nome. Por exemplo, *SFS_SFG* é renomeado como *SFS_SFG_UDP*.

Observação: em Local alternativo de arquivo, uma pasta temporária é selecionada. Este local processa a restauração dos arquivos no local definido no arquivo SqlRestore.ini.

4. Verifique se as configurações estão corretas e clique em **Concluir** para iniciar o processo de restauração.



O log de atividades exibe o status da restauração juntamente com a renomeação do banco de dados.

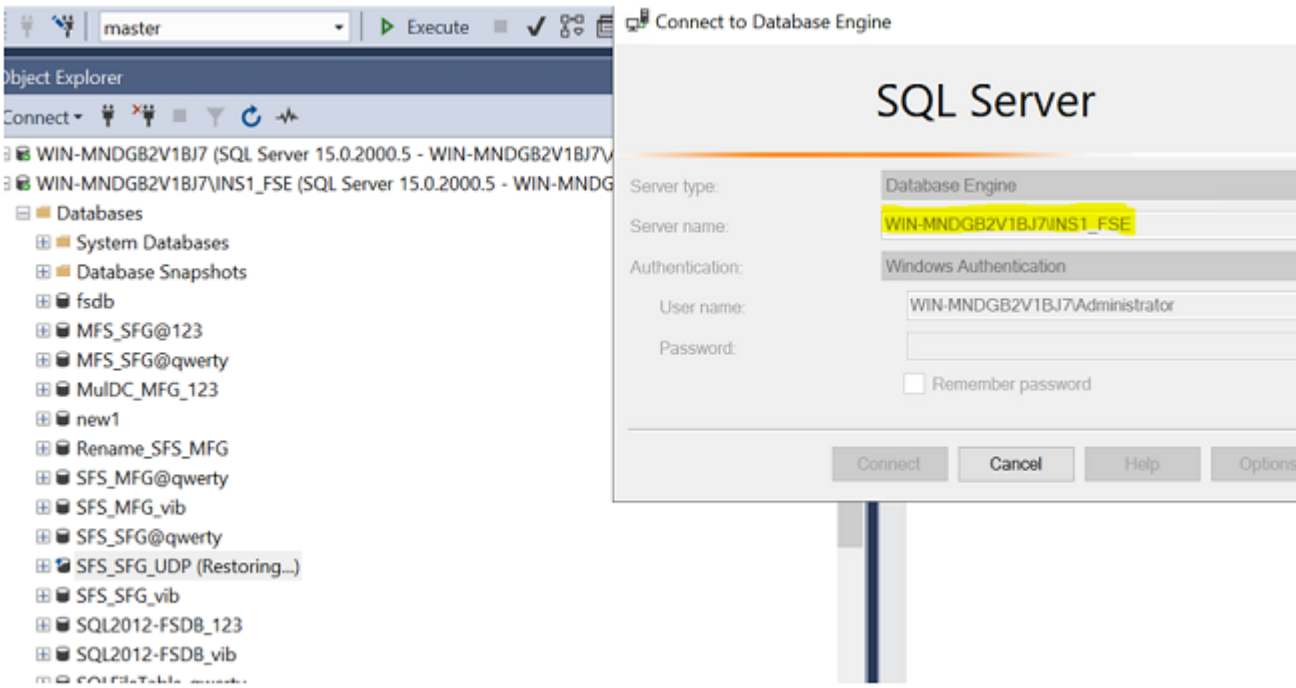


Em alguns casos, o banco de dados ainda é mostrado como uma restauração, mesmo após a conclusão bem-sucedida da tarefa.

Para remover o banco de dados do modo de restauração, faça o seguinte:

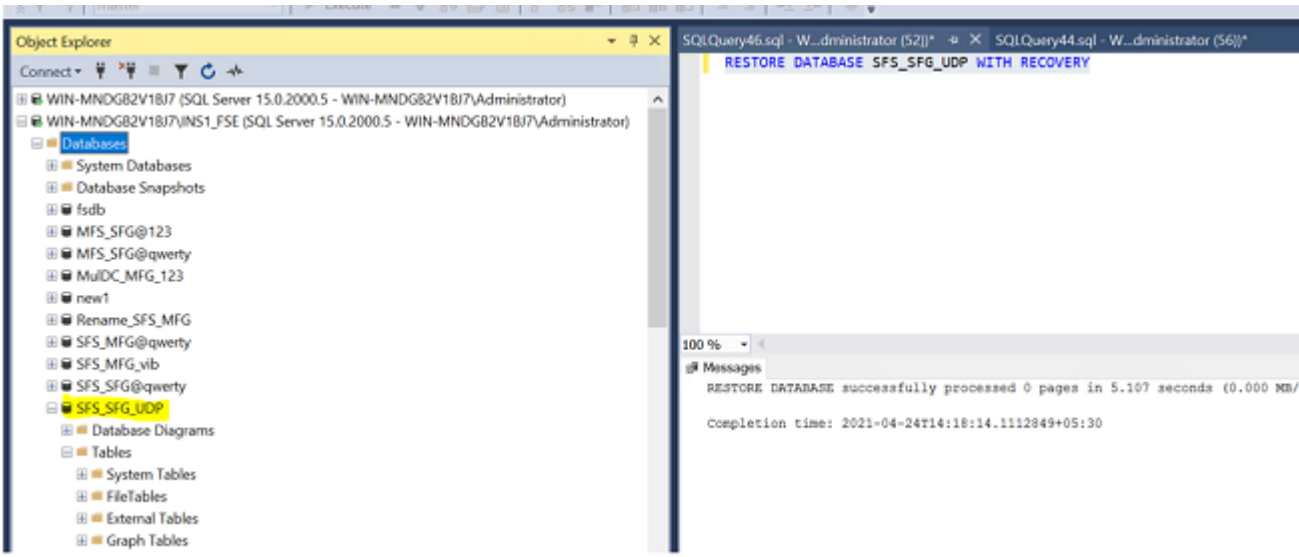
1. Clique com o botão direito do mouse no banco de dados e selecione **Nova consulta**.

   A janela é exibida e se conecta à instância restaurada.



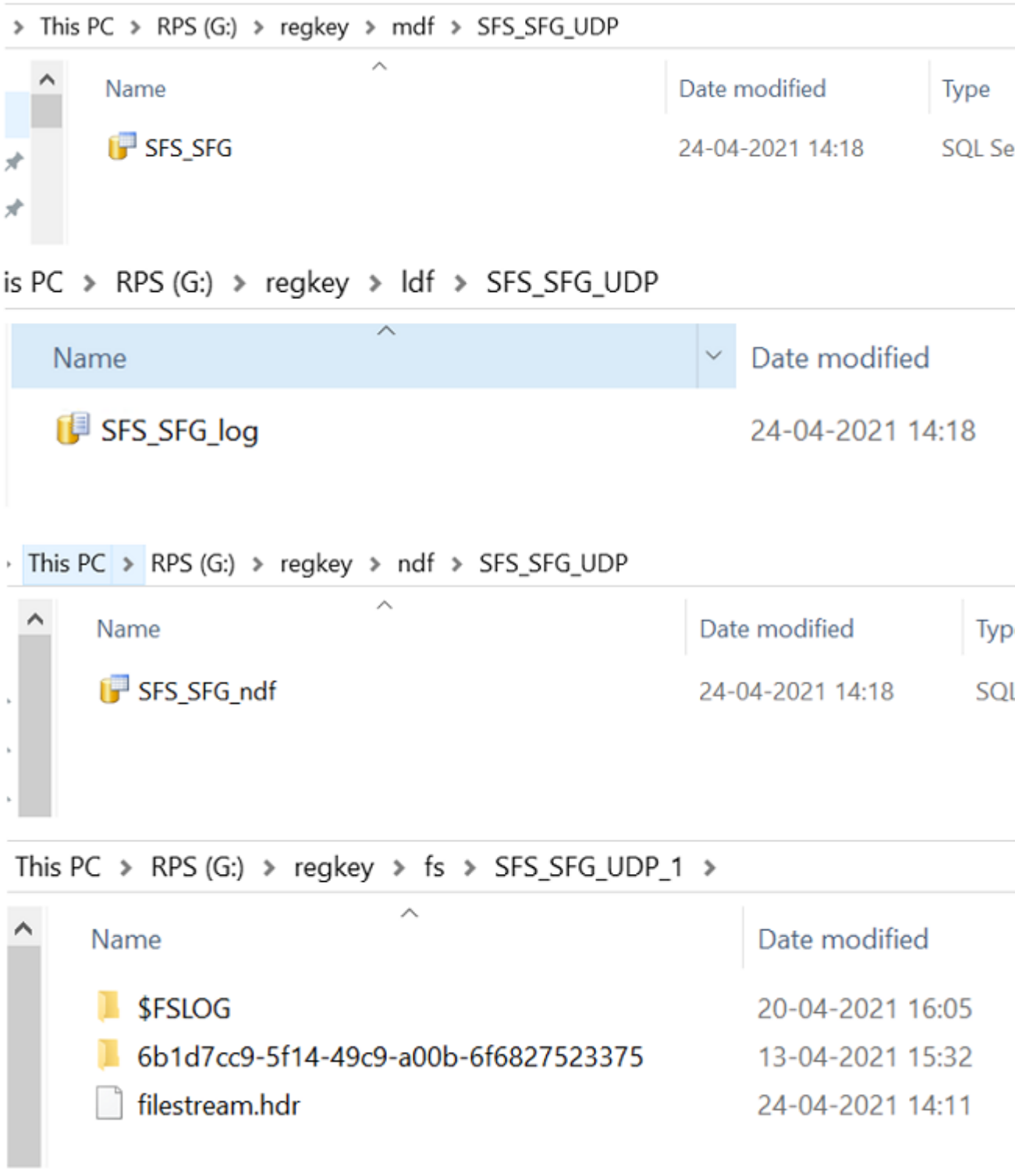
2. Na janela de consulta, execute a consulta a seguir.

   RESTAURAR BANCO DE DADOS [NOME DO BANCO DE DADOS] COM RECUPERAÇÃO



   O modo de restauração é removido do banco de dados.

   Observação: quando a renomeação de um arquivo de banco de dados não é bem-sucedida durante o registro, a pasta principal exibe o novo nome, no entanto, os arquivos do banco de dados, como MDF, NDF e LDF, exibem o nome do banco de dados original.


This PC › RPS (G:) › regkey › mdf › SFS_SFG_UDP
Name
Date modified
Type
SFS_SFG
24-04-2021 14:18
SQL Se
is PC › RPS (G:) › regkey › ldf › SFS_SFG_UDP
Name
Date modified
SFS_SFG_log
24-04-2021 14:18
This PC › RPS (G:) › regkey › ndf › SFS_SFG_UDP
Name
Date modified
Typ
SFS_SFG_ndf
24-04-2021 14:18
SQL
This PC › RPS (G:) › regkey › fs › SFS_SFG_UDP_1 ›
Name
Date modified
$FSLOG
20-04-2021 16:05
6b1d7cc9-5f14-49c9-a00b-6f6827523375
13-04-2021 15:32
filestream.hdr
24-04-2021 14:11

Como usar o utilitário GRT (Exchange Granular Restore- Restauração granular do Exchange)

Esta seção contém as seguintes informações sobre o utilitário GRT (Exchange Granular Restore- Restauração granular do Exchange):

Introdução

Verificar os pré-requisitos e as considerações

Como restaurar dados do Microsoft Exchange usando o utilitário GRT (Exchange Granular Restore - Restauração granular do Exchange)

Introdução

O utilitário Exchange Granular Restore é usado para restaurar objetos de email e não email do Microsoft Exchange. O utilitário inclui o recurso de injeção de itens, como emails, bancos de dados offline (*.EDB) e arquivos de log para bancos de dados dinâmicos originais do Exchange, bem como a descompactação de dados granular para arquivos PST (Personal Storage File - Arquivo de armazenamento pessoal).

Esse utilitário inclui os seguintes benefícios principais:

- Suporte a itens que não são de email (por exemplo, calendário, contatos, tarefas) e a pastas públicas.
- Também pode funcionar com apenas um arquivo de banco de dados. Os logs não são obrigatórios, mas tê-los garante que os dados mais recentes estejam disponíveis para restauração.
- Não precisa gerar um catálogo e restaura o email diretamente do ponto de recuperação montado.
- Leva um tempo mínimo para restaurar um item de nível de caixa de correio a partir de um banco de dados ou uma caixa de correio de usuário de qualquer tamanho.
- Oferece suporte às opções de linha de comando para processar vários bancos de dados.

Observação: para obter mais detalhes sobre as especificações, funcionalidades e outros recursos suportados, consulte o Guia do Usuário da Restauração Granular do Exchange (esr.pdf).

Verificar os pré-requisitos e as considerações

Verifique se os pré-requisitos a seguir existem antes de executar uma restauração:

- O utilitário de Restauração Granular do Exchange está disponível no seguinte local:

  A ferramenta está instalada com o agente do Arcserve UDP no seguinte diretório:

  ```
  X:\Arquivos de programas\Arcserve\Unified Data Protection\Engine\Exchange GRT
  ```

  Observação: A ferramenta está instalada com o agente do Arcserve UDP.

- A tarefa de restauração está definida para execução no computador do Exchange ou máquina proxy HBBU.

  Observação: se você deseja executar a tarefa de restauração em qualquer outro computador, procure o ponto de recuperação a partir do destino de backup.

- O nome do banco de dados, nome do servidor, caminho do banco de dados (.edb) e os arquivos de log do usuário são identificados para executar a tarefa de restauração.

  Para identificar, use o EMC (Exchange Management Console - Console de Gerenciamento do Exchange), o ECP (Exchange Control Panel - Painel de Controle do Exchange (ECP) ou o Shell de gerenciamento do Exchange.

  Por exemplo:

  ```
  Get-Mailbox -identity "username" | fl Database
  ```

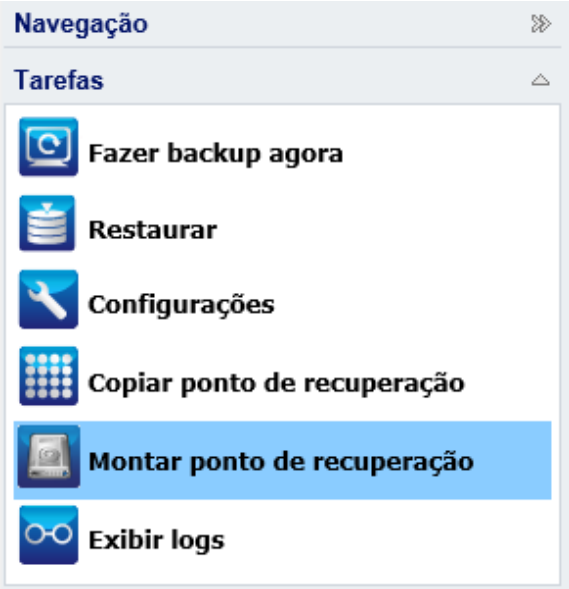
  ```
  Get-MailboxDatabase -identity "Databasename" | fl Name, Server, EdbFilePath,LogFolderPath
  ```

Como restaurar dados do Microsoft Exchange usando o utilitário GRT (Exchange Granular Restore - Restauração granular do Exchange)

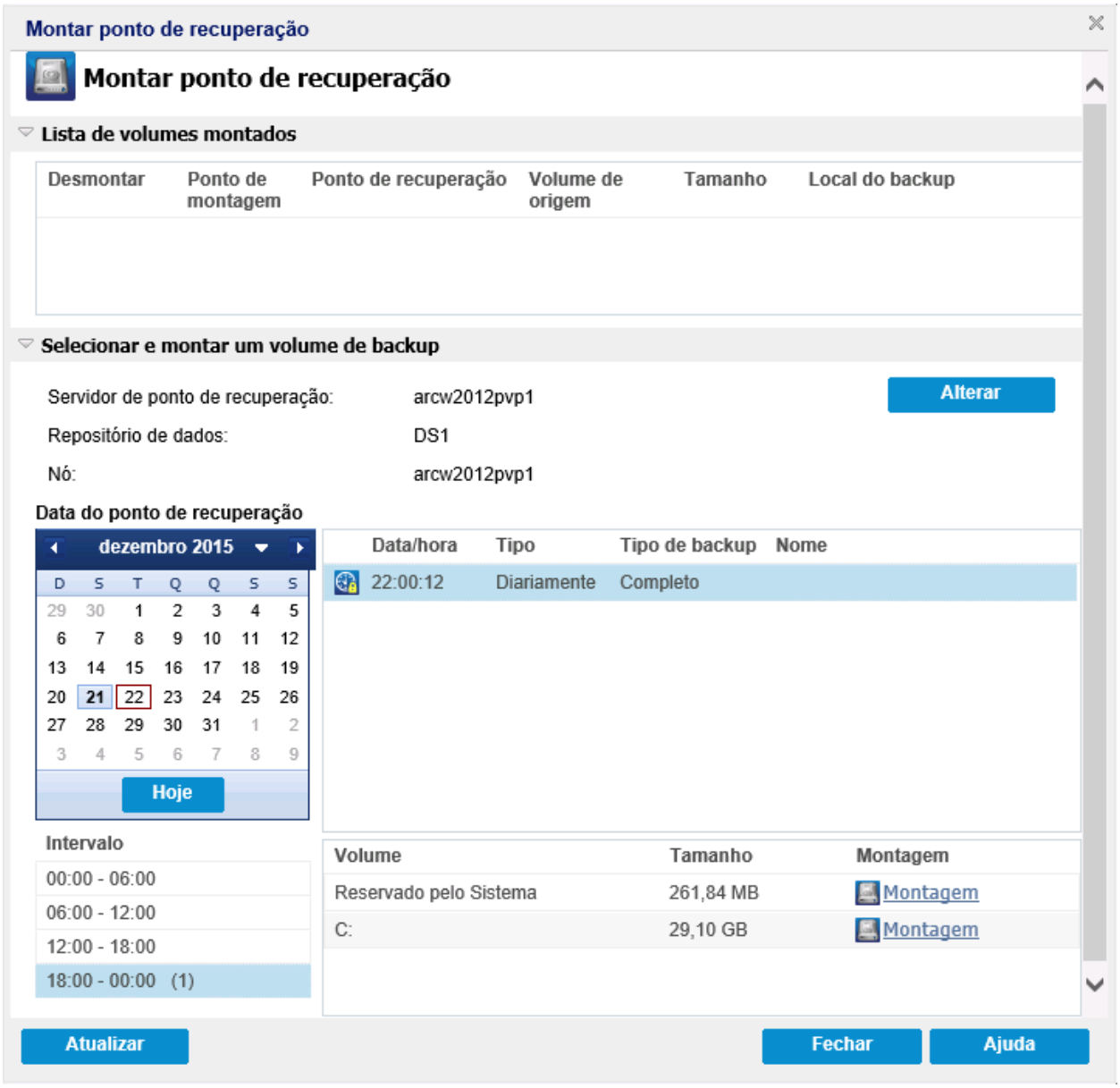
Antes de começar, Verifique os pré-requisitos e as considerações.

Execute as seguintes tarefas para restaurar itens da caixa de correio do Microsoft Exchange usando o utilitário de Restauração granular do Exchange:

1. No console do agente do Arcserve UDP, selecione a tarefa Montar ponto de recuperação (recomendada) ou Restaurar o banco de dados do Exchange para uma unidade local. A caixa de diálogo Montar ponto de recuperação é exibida.

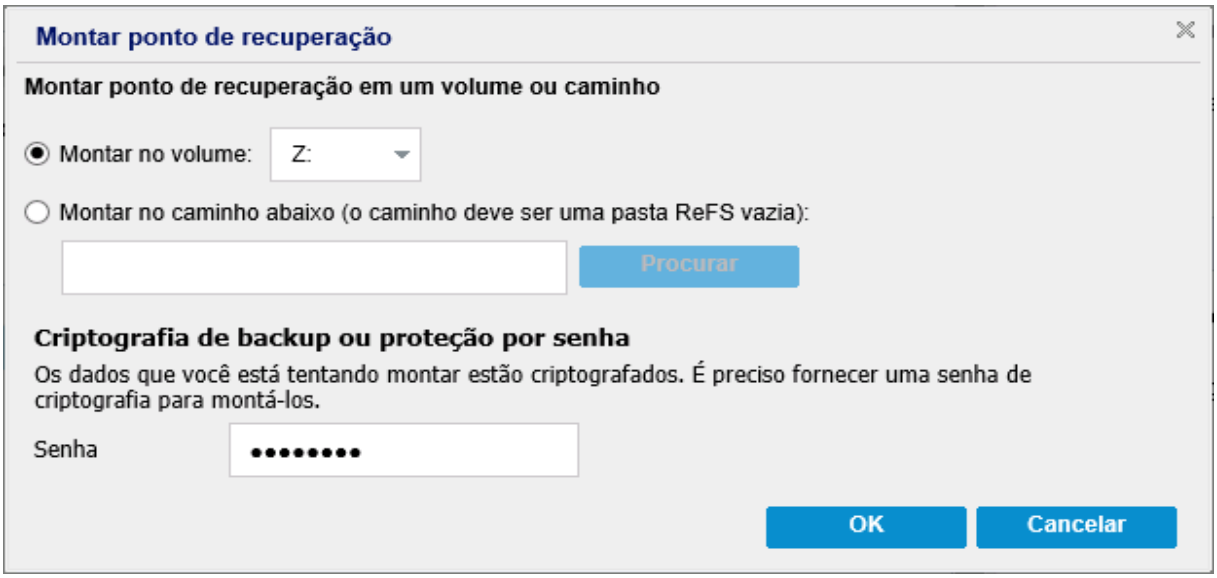


2. Selecione a data no ponto de recuperação e clique em **Montar** para os volumes que contêm o banco de dados do Exchange e logs.



Observação: se o servidor que está executando a tarefa de restauração não for o Exchange ou proxy HBBU, clique em **Alterar** para selecionar o servidor de ponto de recuperação apropriado, o repositório de dados e o Exchange Server.

3. Selecione a letra da unidade onde o volume deve ser montado e clique em **OK**.



4. Inicie o utilitário de Restauração Granular do Exchange em um dos seguintes locais:

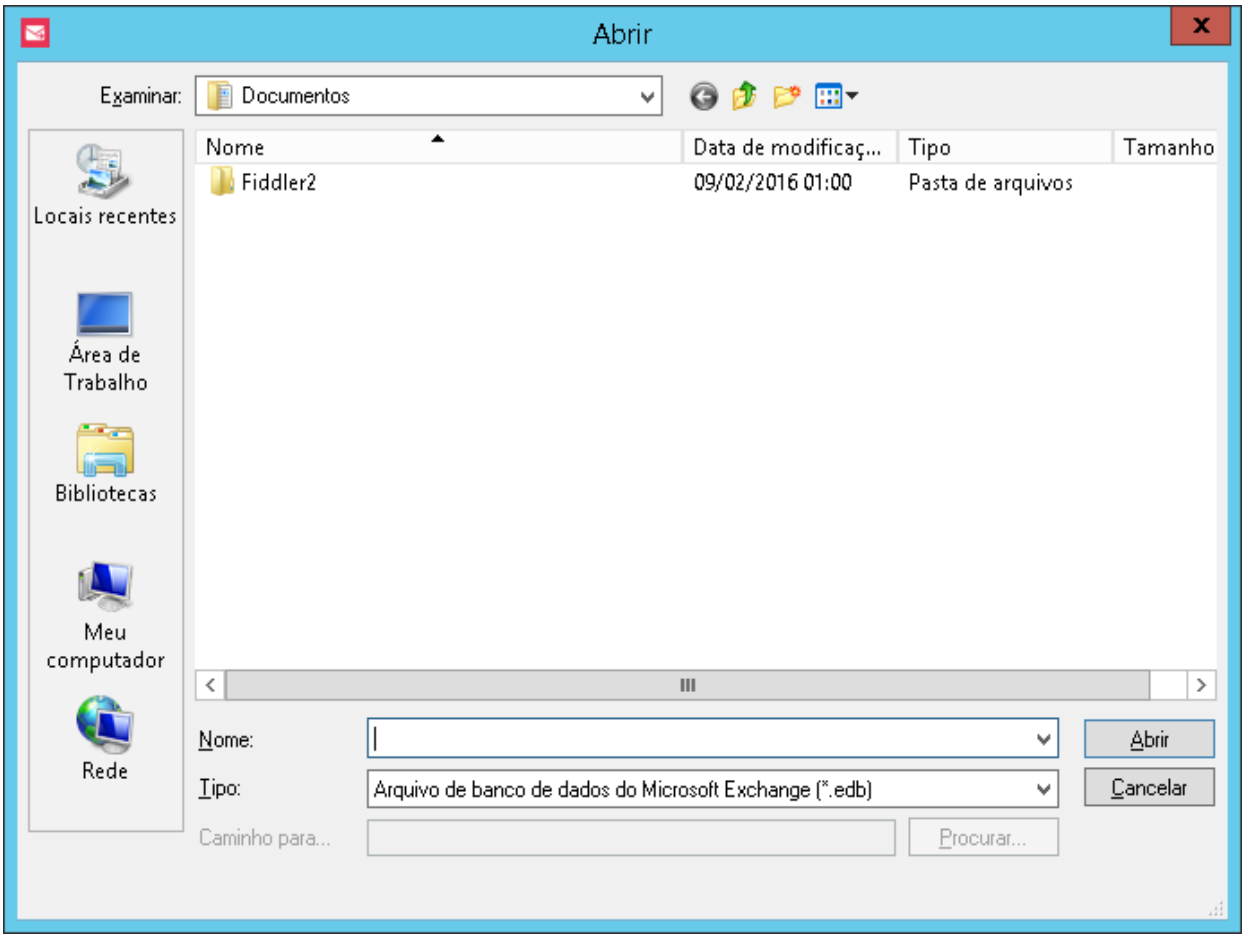
   Iniciar > Todos os programas > Arcserve > Unified Data Protection > Arcserve UDP Exchange Granular Restore

   ou

   X:\Arquivos de programas\Arcserve\Unified Data Protection\Engine\Exchange GRT\esr.exe

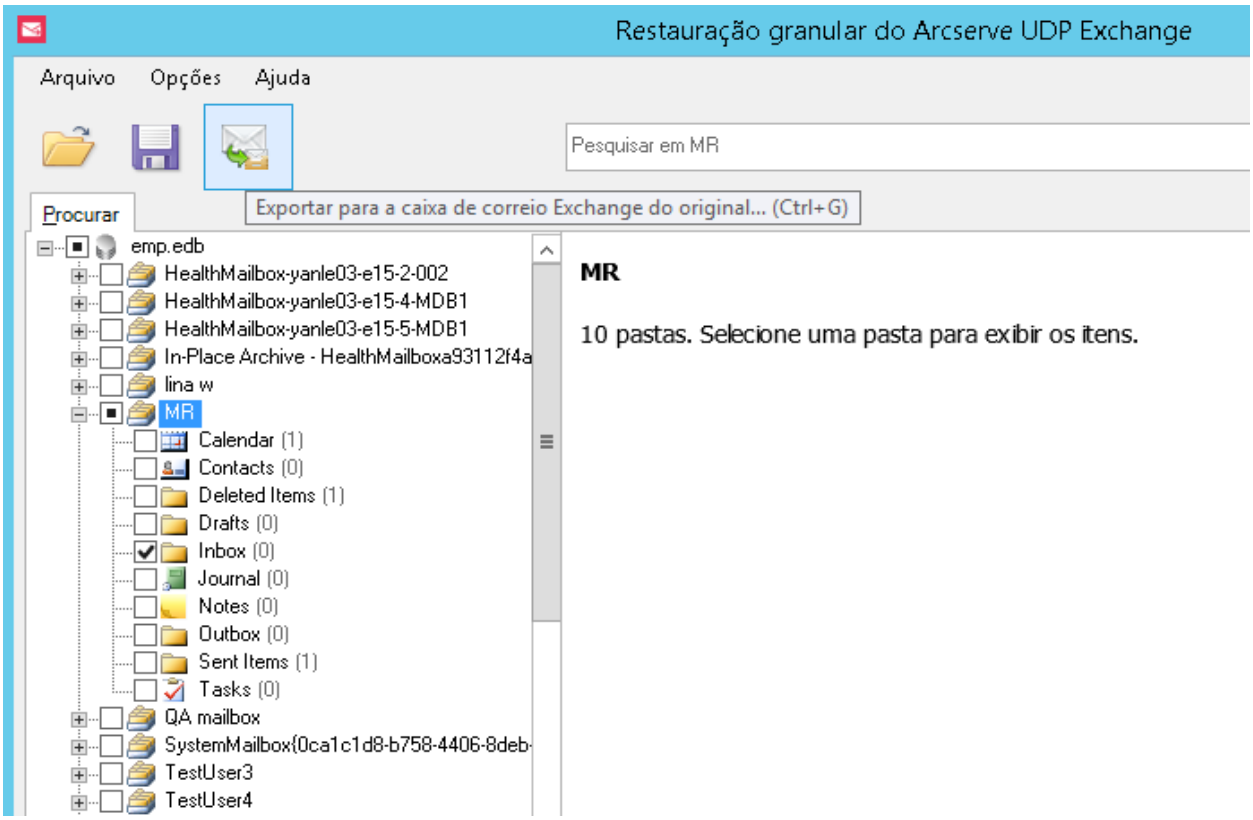
   É exibida uma caixa de diálogo para especificar o caminho para os arquivos de banco de dados e log.

5. Especifique o caminho para o volume montado e clique em **Abrir**.



O utilitário de Restauração Granular do Exchange do Arcserve UDP abre.

6. Selecione os dados do usuário para restaurar e clique em **Exportar na caixa de correio original** ou **Exportar em. PST**.



Observações:

- Para obter mais detalhes sobre as especificações suportadas, recursos, opções do usuário e limitações, consulte o guia do usuário da Restauração granular do Exchange (esr.pdf), localizado em:

  %ProgramFiles%\Arcserve\Unified Data Protection\Engine\Exchange GRT ou Biblioteca.

- Por padrão, o utilitário usa o usuário atual que está conectado ao Windows para estabelecer a conexão. Se o usuário atual não tiver permissões para personificar o usuário selecionado, uma mensagem de erro será exibida no painel de **Detalhes**.

  Se um erro for relatado, a ação recomendada é efetuar logon no computador com uma conta que tenha direitos de representação para o usuário selecionado ou a conta do usuário selecionado.

7. Quando a tarefa de restauração é concluída, desmonte o volume que foi usado para a recuperação.

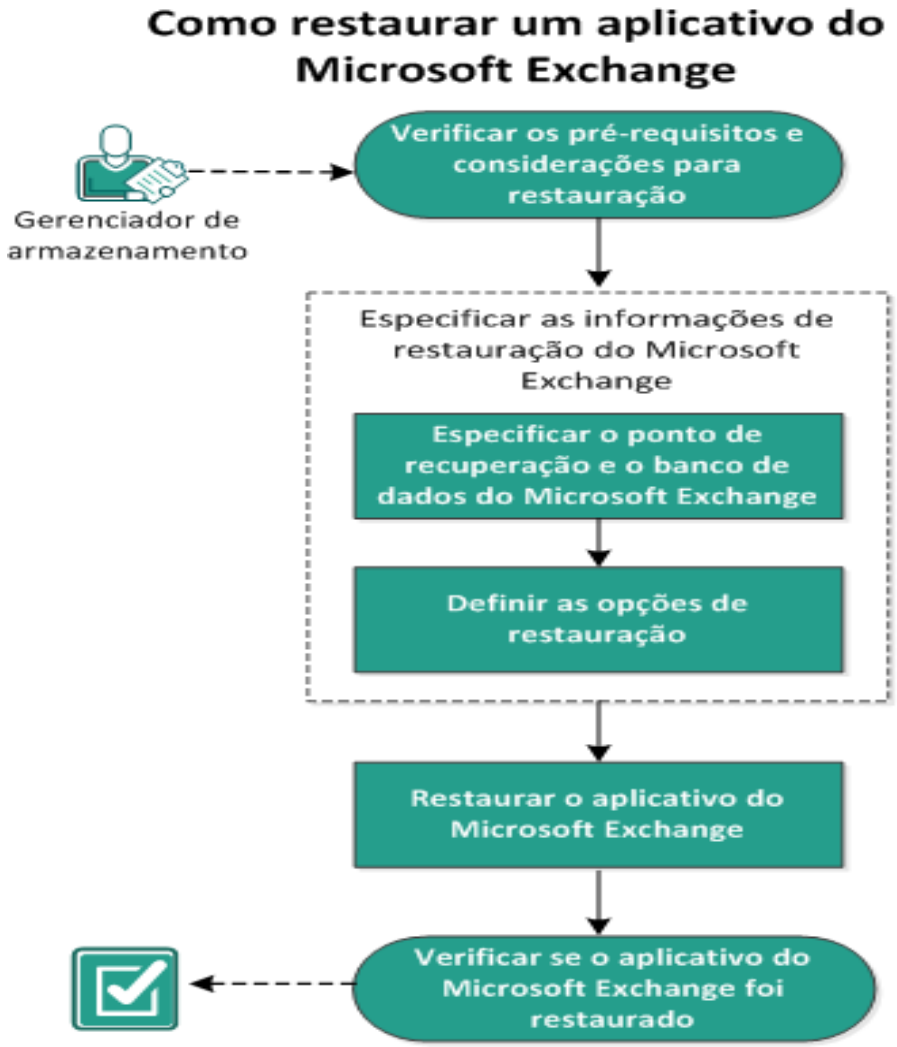
   Para desmontar o volume no console do agente do Arcserve UDP, clique em **Montar ponto de recuperação** e, em seguida, clique em **Desmontar**.

Montar ponto de recuperação
Montar ponto de recuperação
Lista de volumes montados
Desmontar
Ponto de montagem
Ponto de recuperação
Volume de origem
Tamanho
Local do backup
Desmontar
Z:
21/12/2015 22:00:12
C:
29,10 GB
\\arcw2012pvp1\CA_UDP_D...

Como restaurar um aplicativo do Microsoft Exchange

O Agente do Arcserve UDP (Windows) permite não só proteger e recuperar seus dados, como também fazer com que os aplicativos que irão usar tais dados voltem a funcionar. As recuperações de aplicativos só podem ser feitas com o uso do método Restore by Recovery Point. Durante uma recuperação de aplicativo, o Agente do Arcserve UDP (Windows) aproveita o VSS (Volume Shadow Copy Service - Serviço de Cópia de Sombra de Volume) do Windows para garantir a consistência dos dados de qualquer aplicativo que reconheça VSS. Com o Agente do Arcserve UDP (Windows), é possível recuperar o aplicativo do Microsoft Exchange Server sem executar uma recuperação de falhas completa.

O diagrama a seguir ilustra o processo para restaurar um aplicativo do Microsoft Exchange:



Execute as tarefas a seguir para restaurar um aplicativo do Microsoft Exchange:

1. Verificar os pré-requisitos e as considerações para restauração
2. Especificar as informações de restauração do Microsoft Exchange
    a. Especificar o ponto de recuperação e o banco de dados do Microsoft Exchange
    b. Definir as opções de restauração
3. Restaurar o aplicativo do Microsoft Exchange
4. Verificar se o aplicativo do Microsoft Exchange foi restaurado

Revisar os pré-requisitos e as considerações para restauração

O Agente do Arcserve UDP (Windows) suporta as seguintes versões do Microsoft Exchange Server:

- Microsoft Exchange 2010 – ambiente de servidor único e ambiente DAG (Database Availability Group – Grupo de Disponibilidade do Banco de Dados).
- Microsoft Exchange 2013 e 2016 – ambiente de servidor único e ambiente de DAG (Database Availability Group – Grupo de Disponibilidade do Banco de Dados).

  Para o ambiente de DAG do Microsoft Exchange Server 2010, 2013 e 2016, o Agente do Arcserve UDP (Windows) precisa estar instalado em todos os servidores integrantes no DAG. A tarefa de backup também pode ser executada a partir de qualquer servidor integrante para cópias de bancos de dados ativas e passivas, contudo, a restauração só pode ser realizada para uma cópia de banco de dados ativa.
- Embora não seja necessário que todos os integrantes do DAG façam parte do mesmo plano de backup, recomendamos que você use o mesmo repositório de dados de redução de redundância para eliminar dados duplicados.

É possível restaurar o Microsoft Exchange Server para os seguintes níveis:

Nível do gravador do Microsoft Exchange

Caso queira restaurar todos os dados do Microsoft Exchange Server, é possível executar uma restauração no nível do gravador do Microsoft Exchange.

Nível de grupo de armazenamento

Caso queira restaurar um grupo de armazenamento específico, é possível executar uma restauração nesse nível.

Observação: o nível do grupo de armazenamento não se aplica ao Microsoft Exchange Server 2010, 2013 e 2016.

Nível do banco de dados da caixa de correio (Microsoft Exchange 2010, 2013 e 2016)

Caso queira restaurar um banco de dados de caixa de correio específico, é possível executar uma restauração nesse nível.

Nível de caixa de correio (Microsoft Exchange 2010, 2013, e 2016)

Defina se deseja restaurar uma caixa de correio ou um objeto correio específico.

Antes de executar uma restauração do Microsoft Exchange, verifique se os seguintes pré-requisitos foram atendidos:

Restauração de nível de banco de dados

- O computador de destino tem o mesmo nome e a mesma versão do Microsoft Exchange instalado.
- O banco de dados de destino tem o mesmo nome de banco de dados e o mesmo nome de grupo de armazenamento (Microsoft Exchange 200X) e faz parte da mesma organização do Microsoft Exchange.

Restauração de nível granular

- Para restaurar dados do Microsoft Exchange, use o Utilitário de Restauração Granular do Exchange.

Especificar as informações de restauração do Microsoft Exchange

O Agente do Arcserve UDP (Windows) permite que você não apenas proteja e recupere os dados, como também faz com que o aplicativo do Microsoft Exchange Server que usar tais dados volte a funcionar. A recuperação do Microsoft Exchange Server só pode ser feita usando o método de restauração por ponto de recuperação.

O processo envolvido na restauração de um aplicativo do Microsoft Exchange é o seguinte:

1. Especificar o ponto de recuperação e o banco de dados do Microsoft Exchange
2. Definir as opções de restauração

Especificar o ponto de recuperação e o banco de dados do Microsoft Exchange

Use a opção **Procurar pontos de recuperação** para restaurar a partir de um ponto de recuperação. Ao selecionar uma data de recuperação, todos os pontos de recuperação associados a essa data serão exibidos. Em seguida, você poderá procurar e selecionar o banco de dados do Microsoft Exchange a ser restaurado.

Siga estas etapas:

1. Acesse a caixa de diálogo de seleção de método de restauração de uma das seguintes maneiras:

   No Arcserve UDP:

   a. Efetue logon no Arcserve UDP.

   b. Clique na guia **Recursos**.

   c. Selecione **Todos os nós** no painel esquerdo.

      Todos os nós adicionados são exibidos no painel central.

   d. No painel central, selecione o nó do e clique em **Ações**.

   e. Clique em **Restaurar** no menu suspenso **Ações**.

      A caixa de diálogo de seleção do método de restauração é exibida.

      Observação: você é automaticamente conectado ao nó do agente e a caixa de diálogo de seleção do método de restauração é exibida no nó do agente.

   No agente do Arcserve UDP (Windows):

   a. Efetue logon no Agente do Arcserve UDP (Windows).

   b. Na página inicial, selecione **Restaurar**.

   A caixa de diálogo de seleção do método de restauração é exibida.

2. Clique na opção **Procurar pontos de recuperação**.

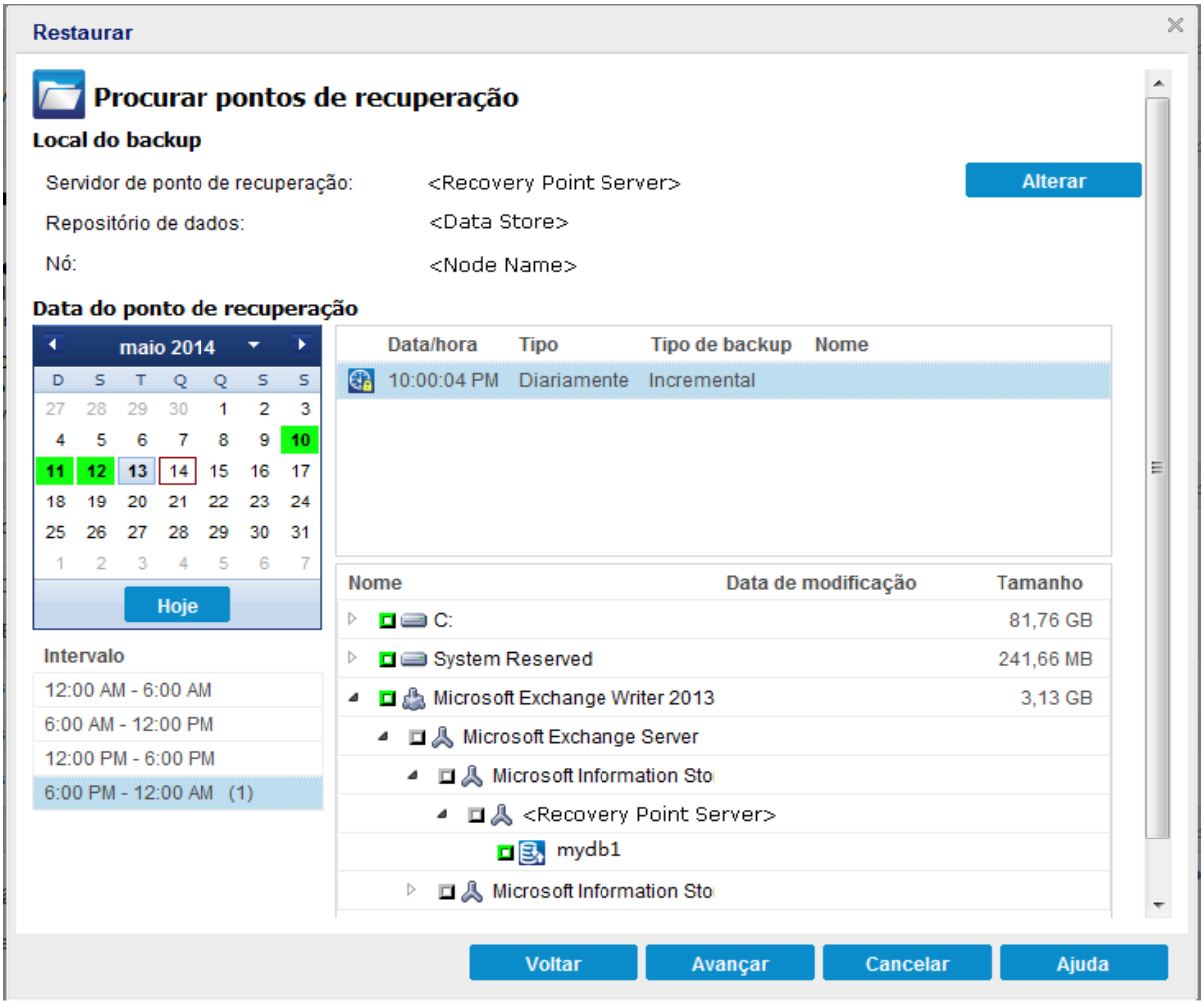
   A caixa de diálogo **Procurar pontos de recuperação** é exibida.

3. Selecione o ponto de recuperação (data e hora) e, em seguida, o banco de dados do Microsoft Exchange a ser restaurado.

   A caixa do marcador correspondente é preenchida (verde) para indicar que o banco de dados foi selecionado para restauração.

   Observação: se não desejar que os arquivos de log de transações sejam aplicados após a restauração, é necessário excluí-los manualmente antes de a restauração ser realizada. Para obter mais informações sobre como excluir manualmente

arquivos de log de transações, consulte a documentação do Microsoft Exchange Server.



4. Clique em **Avançar**.

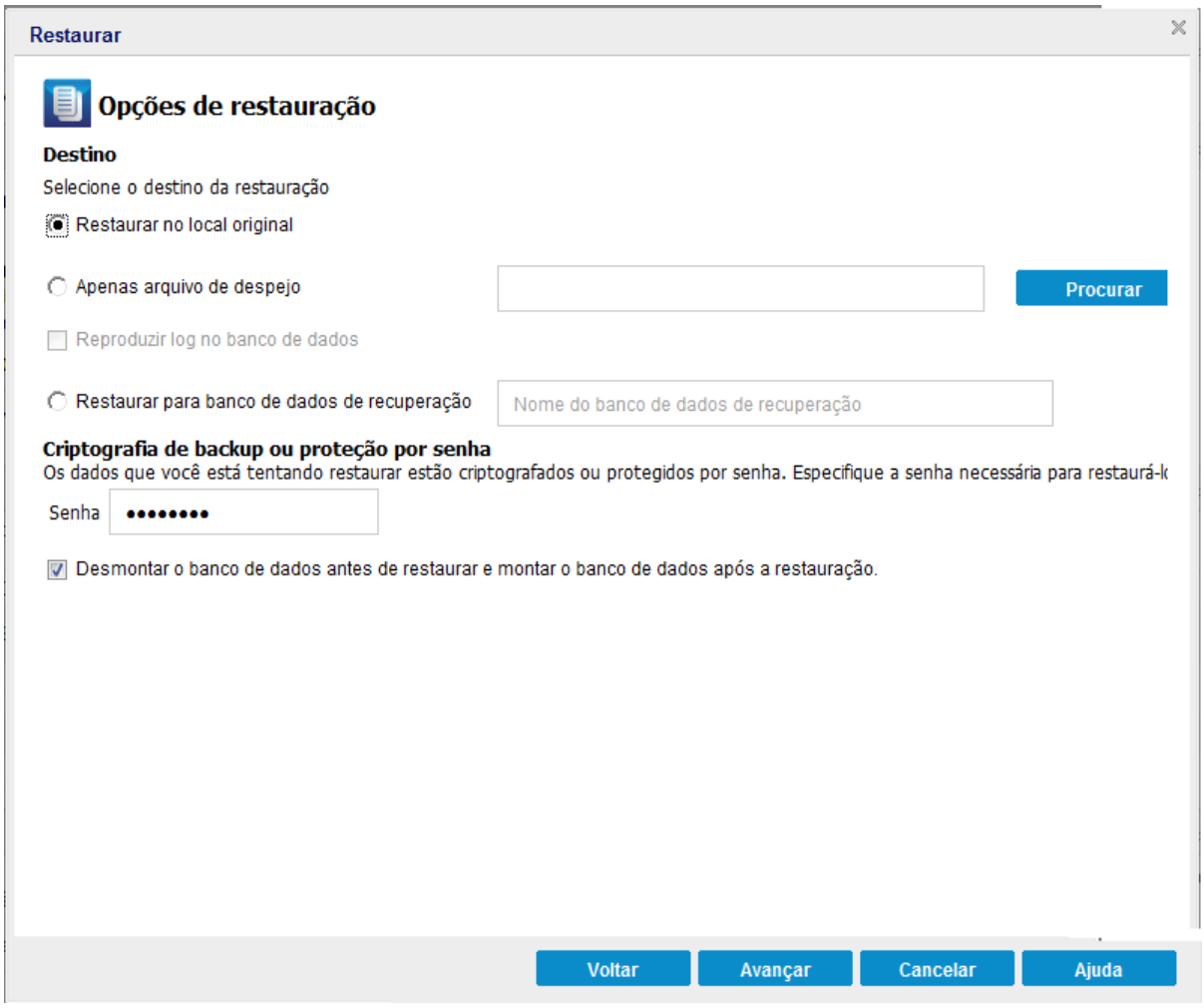
   A caixa de diálogo **Opções de restauração** é exibida.

Definir as opções de restauração

Depois de especificar um ponto de recuperação e conteúdo para restauração, defina as opções de cópia do ponto de recuperação selecionado.

Siga estas etapas:

1. Na caixa de diálogo **Opções de restauração**, selecione o destino da restauração.



2. Selecione o destino da restauração.

As opções disponíveis permitem restaurar no local original do backup, restaurar apenas o arquivo de despejo ou restaurar em um Grupo de armazenamento de recuperação/Banco de dados de caixa de correio de recuperação.

Restaurar no local original

Restaura no local original a partir do qual a imagem de backup foi capturada.

Somente arquivo de despejo

Restaura apenas os arquivos de despejo.

Para essa opção, o Agente do Arcserve UDP (Windows) restaurará o arquivo do banco de dados do Microsoft Exchange em uma pasta especificada e não o colocará online após a recuperação. Em seguida, você poderá usá-lo para a montagem manual no Microsoft Exchange Server.

Observação: quando há um Banco de dados de caixa de correio de recuperação, a restauração com a opção **Apenas arquivo de despejo** falhará.

Reproduzir log no banco de dados

Especifica que, quando os arquivos do banco de dados são despejados na pasta de destino, você pode reproduzir os arquivos de log de transações do Microsoft Exchange e confirmá-los para o banco de dados.

Desmontar o banco de dados antes de restaurar e montar o banco de dados após a restauração

Em geral, antes de uma restauração, o Microsoft Exchange executará algumas verificações para garantir:

- O banco de dados a ser restaurado está no status *Desmontado*.
- Que o banco de dados não seja restaurado de forma inesperada.

Para proteger um banco de dados de produção do Microsoft Exchange contra restauração inesperada, o switch é adicionado para permitir que o banco de dados seja substituído durante o processo de restauração. O Microsoft Exchange não fará a restauração de um banco de dados se essa opção não estiver definida.

Para o Agente do Arcserve UDP (Windows), essas duas opções são controladas pela opção "Desmontar o banco de dados antes de restaurar e montar o banco de dados após a restauração". Com essa opção, o Agente do Arcserve UDP (Windows) permite iniciar o processo de restauração automaticamente sem nenhuma operação manual. (É possível também especificar a desmontagem/montagem do banco de dados manualmente).

- Se estiver marcada, especifica que o processo de recuperação desmontará automaticamente o banco de dados do Microsoft Exchange antes do processo de restauração e, em seguida, montará o banco de dados após a conclusão do processo de restauração. Além disso, se estiver marcada, essa opção também permite que o banco de dados do Microsoft Exchange seja substituído durante a restauração.
- Se estiver desmarcada, essa opção especifica que o processo de recuperação não desmontará automaticamente o banco de dados do Microsoft Exchange antes da recuperação e que não o montará após a recuperação.

O administrador do Microsoft Exchange deverá executar algumas operações manuais, como desmontar o banco de dados do Microsoft Exchange, definir o sinalizador Permitir substituição no banco de dados e montar o banco de dados do Microsoft Exchange. (O procedimento de recuperação é realizado pelo Exchange durante a montagem do banco de dados).

Além disso, se não estiver marcada, essa opção não permite que o banco de dados do Microsoft Exchange seja substituído durante a restauração.

Restaurar no banco de dados de recuperação (Microsoft Exchange 2010 e 2013)

Restaura o banco de dados em um banco de dados de recuperação. Um banco de dados de recuperação é um banco de dados que pode ser usado para fins de recuperação. É possível restaurar um banco de dados da caixa de correio do Microsoft Exchange a partir de um backup em um banco de dados de recuperação, bem como recuperar e extrair seus dados, sem afetar o banco de dados de produção que estiver sendo acessado por usuários finais.

Antes de restaurar um banco de dados do Microsoft Exchange 2010 ou 2013 para um banco de dados de recuperação, você deve primeiro criar um banco de dados de recuperação.

3. Clique em **Avançar**.

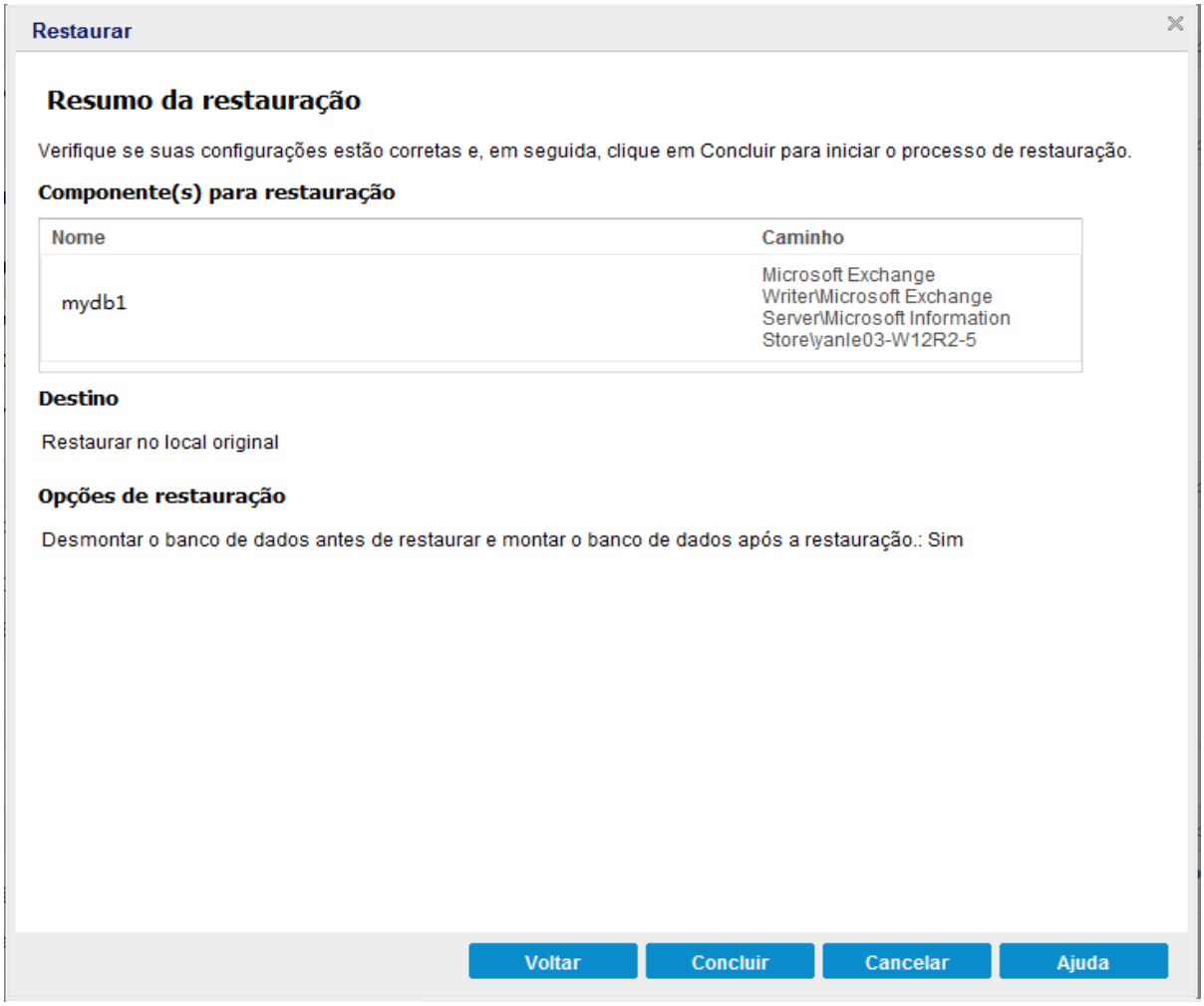
   A caixa de diálogo **Resumo da restauração** é exibida.

Restaurar o aplicativo do Microsoft Exchange

Após definir as opções de restauração, verifique se suas configurações estão corretas e confirme o processo de restauração. O **Resumo da restauração** o auxilia a revisar todas as opções de restauração definidas e modificá-las se necessário.

Siga estas etapas:

1. Na caixa de diálogo **Resumo da restauração**, examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.



- Se as informações de resumo não estiverem corretas, clique em **Anterior** e volte à caixa de diálogo em questão para alterar a configuração incorreta.
- Se as informações de resumo estiverem corretas, clique em **Avançar** e em **Concluir** para iniciar o processo de restauração.

O aplicativo do Microsoft Exchange é restaurado.

Verificar se o aplicativo do Microsoft Exchange foi restaurado

Siga estas etapas:

1. Navegue até o destino de restauração do Agente do Arcserve UDP (Windows) que você especificou.

   Por exemplo, se você optar por restaurar o banco de dados do Microsoft Exchange no local original, após a restauração ser concluída, vá até o local físico para verificar se os logs e o banco de dados do Microsoft Exchange foram restaurados.

   Se você optar por restaurar o banco de dados do Microsoft Exchange no local Apenas arquivo de despejo, o agente do Arcserve UDP (Windows) restaurará os logs e o banco de dados do Microsoft Exchange em um local especificado.

2. Verifique se o aplicativo do Microsoft Exchange foi restaurado e se o banco de dados está montado e acessível.

   O aplicativo do Microsoft Exchange é restaurado com êxito.

Como restaurar dados do Exchange em uma máquina virtual do VMware

Importante: para restaurar dados do Microsoft Exchange em uma máquina virtual VMware, é recomendável usar o Utilitário de restauração Granular do Exchange.

Como fazer download de arquivo/pastas sem restaurar

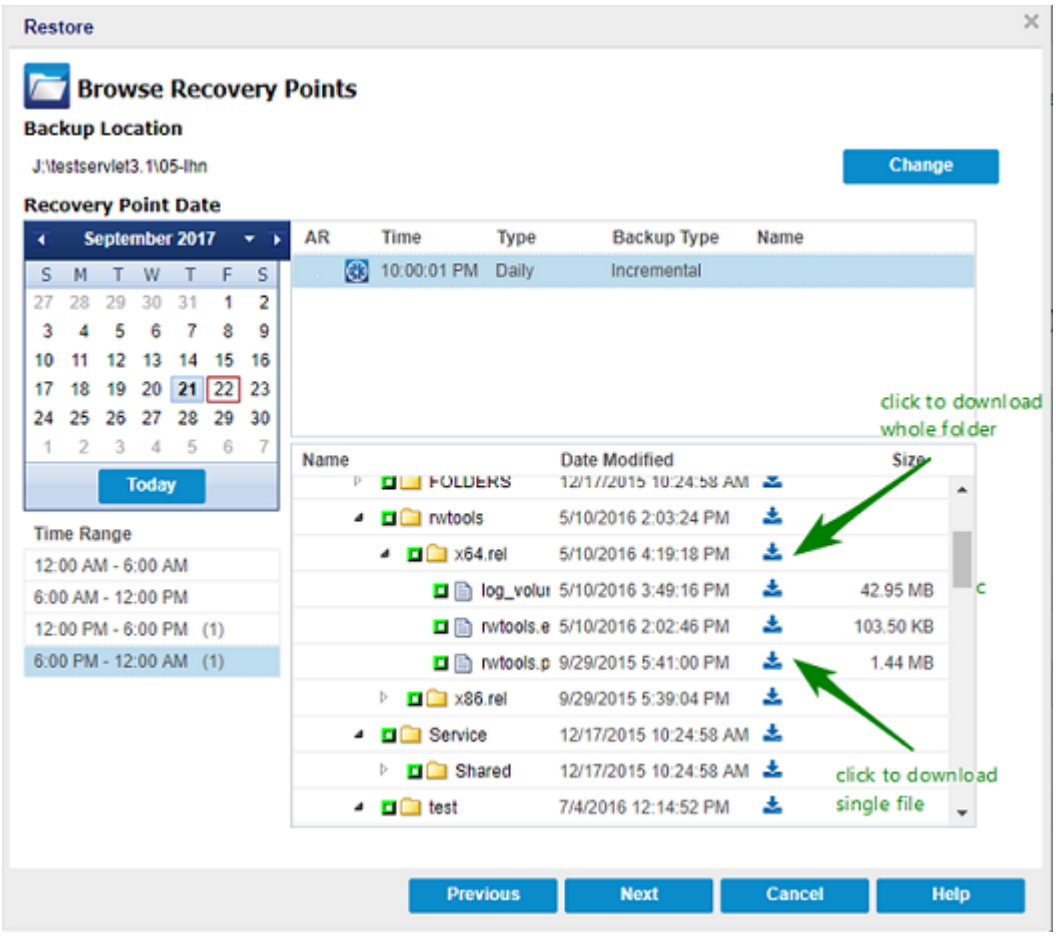
Arcserve UDP permite que você faça download de um arquivo ou uma pasta completa sem enviar para restauração. No Assistente de restauração, a tela Procurar pontos de recuperação permite fazer download diretamente de qualquer arquivo ou pasta completa com todos os arquivos. Fazer download antes da restauração pode ajudar a executar uma verificação rápida de arquivos para evitar que arquivos indesejados sejam restaurados.

Observação: fazer download dos arquivos não mantém as permissões dos arquivos ou das pastas.

Um único arquivo é transferido por download diretamente no mesmo formato, enquanto uma pasta é transferida por download como um arquivo zip. O arquivo zip tem o seguinte formato de nome:

[nodename]_[sessionid]_[timestamp].zip

Para fazer download, basta acessar a tela Procurar pontos de recuperação no Assistente de restauração. A seguinte captura de tela exibe como fazer download de um arquivo ou pasta:



Considerações para download:

- Fazer download ou compactar como arquivo zip não é possível para alguns arquivos de sistema. O serviço tomcat do agente não tem privilégios suficientes para acessar o arquivo de sistema ou arquivos do usuário de outro nó protegido.
- Para evitar o consumo excessivo de memória do Tomcat e uso da CPU, é recomendável enviar uma tarefa de restauração para o caminho alternativo durante o download de um arquivo grande ou uma pasta.
- Usar as ferramentas de pastas compactadas do Windows para procurar os arquivos zip baixado pode falhar, pois alguns nomes de entrada zip são longos demais para a ferramenta procurar. É recomendável usar outras ferramentas zip para abrir o arquivo. Por exemplo, WinZip, WinRAR, 7-Zip.
- Um usuário do IE9 usando Https no IE9 e agente de serviço da web para fornecer serviço não poderá fazer download dos arquivos. Um problema conhecido do IE9 de download de recursos de uma página dinâmica, por meio de https, impede esse download. Para obter mais informações e soluções, clique no link para o artigo da Microsoft.

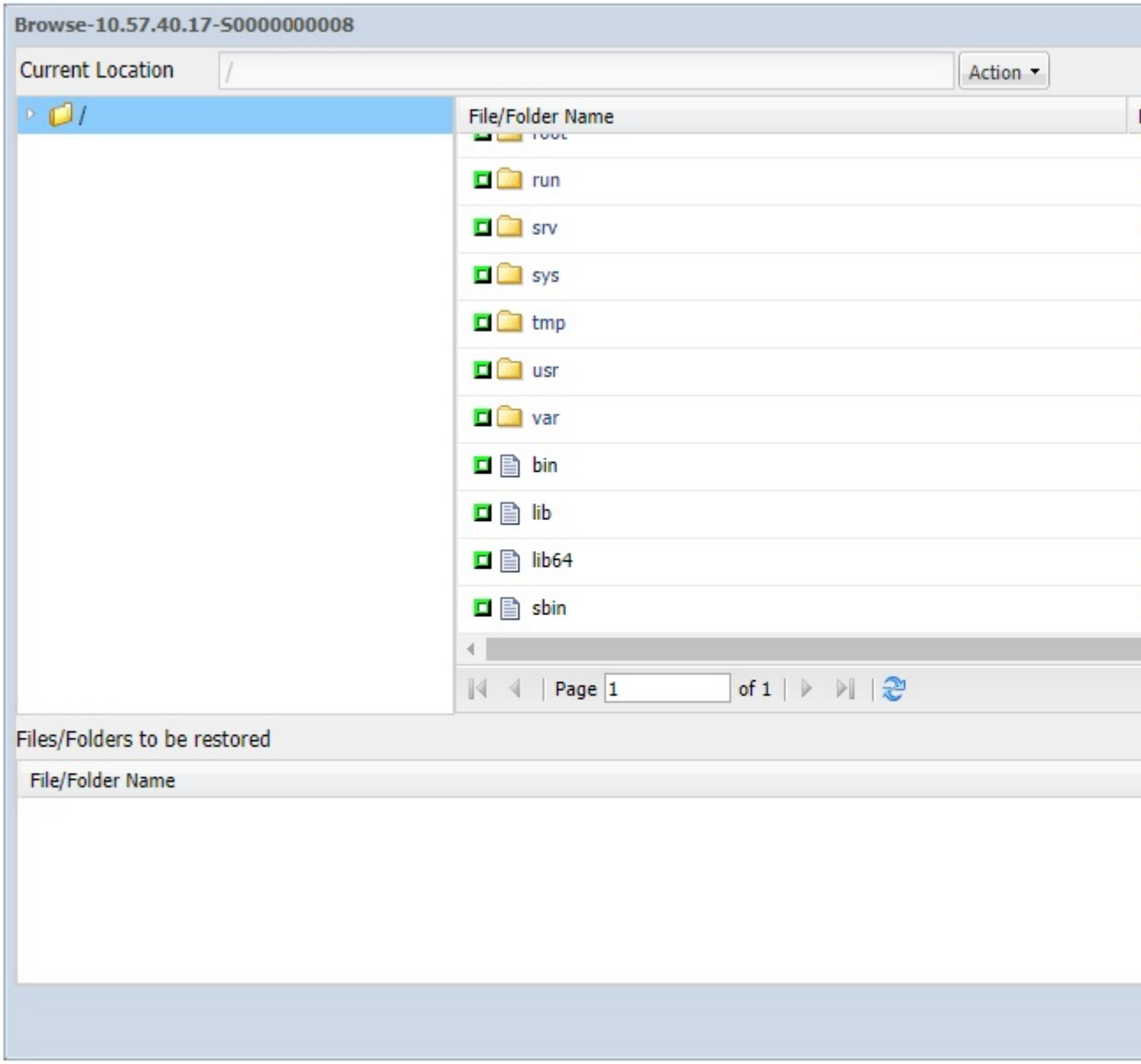
Como fazer download de arquivos/pastas sem restaurar para nós do Linux

Arcserve UDP permite que você faça download de um arquivo ou uma pasta completa sem enviar para restauração. No Assistente de restauração, a tela Procurar pontos de recuperação permite fazer download diretamente de qualquer arquivo ou pasta completa com todos os arquivos. Fazer download antes da restauração pode ajudar a executar uma verificação rápida de arquivos para evitar que arquivos indesejados sejam restaurados.

Um único arquivo é transferido por download diretamente no mesmo formato, enquanto uma pasta é transferida por download como um arquivo zip. O arquivo zip tem o seguinte formato de nome:

[nodename]_[sessionid]_[timestamp].zip

Para fazer download, basta acessar a tela Procurar pontos de recuperação no Assistente de restauração. A captura de tela a seguir mostra como fazer download de um arquivo ou pasta para nós do Linux:

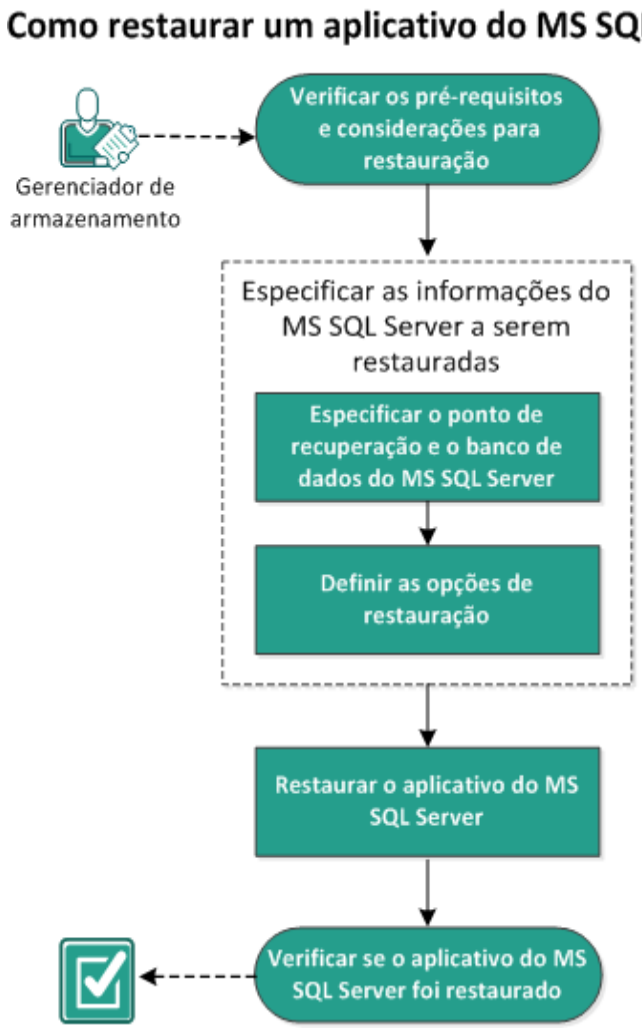


Para abrir os arquivos baixados, use ferramentas de compactação como WinZip, WinRAR, 7-Zip, etc.

Como restaurar um aplicativo do Microsoft SQL Server

O Agente do Arcserve UDP (Windows) permite não só proteger e recuperar seus dados, como também ajuda a fazer com que os aplicativos que irão usar tais dados voltem a funcionar. As recuperações de aplicativos só podem ser feitas com o uso do método Restore by Recovery Point. Durante uma recuperação de aplicativo, o Agente do Arcserve UDP (Windows) aproveita o VSS (Volume Shadow Copy Service - Serviço de Cópia de Sombra de Volume) do Windows para garantir a consistência dos dados de qualquer aplicativo que reconheça VSS. Com o Agente do Arcserve UDP (Windows), é possível recuperar o aplicativo do Microsoft SQL Server sem executar uma recuperação de falhas completa.

O diagrama seguinte ilustra o processo de restauração de um aplicativo do Microsoft SQL Server:



Execute as tarefas a seguir para restaurar um aplicativo do Microsoft SQL Server:

1. Verificar os pré-requisitos e as considerações para restauração
2. Especificar as informações do Microsoft SQL Server a serem restauradas
    a. Especificar o ponto de recuperação e o banco de dados do Microsoft SQL Server
    b. Definir as opções de restauração
3. Restaurar o aplicativo do Microsoft SQL Server
4. Verificar se o aplicativo do Microsoft SQL Server foi restaurado

Revisar os pré-requisitos e as considerações para restauração

Verifique se os pré-requisitos a seguir existem antes de executar uma restauração:

- É necessário ter uma instância do Microsoft SQL Server para poder executar uma restauração de aplicativo do Exchange.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Revise as seguintes considerações de restauração:

- Não é possível restaurar bancos de dados em uma instância. A restauração em um local alternativo no Agente do Arcserve UDP (Windows) significa que é possível restaurar o banco de dados e alterar o nome dele, bem como o local do arquivo. Para obter mais informações, consulte o tópico Considerações sobre a restauração do Microsoft SQL Server em um local alternativo.
- Se as tarefas não forem para a mesma VM, o Arcserve UDP permitirá que várias tarefas de restauração sejam executadas ao mesmo tempo. Se você tentar iniciar uma tarefa de restauração enquanto outra tarefa de restauração estiver em execução para a mesma VM, uma mensagem de alerta aparece informando que outra tarefa está em execução e solicitando que você tente novamente mais tarde.
- O Arcserve UDP_agt_windows> permite que apenas uma tarefa de restauração seja executada ao mesmo tempo. Se você tentar iniciar uma tarefa de restauração manualmente enquanto outra tarefa de restauração estiver em execução, uma mensagem de alerta será exibida informando que outra tarefa está em execução e solicitando que você tente novamente mais tarde.

Considerações sobre a restauração do Microsoft SQL Server em um local diferente

Ao especificar a restauração de um aplicativo do Microsoft SQL Server em um local diferente, é possível restaurá-lo em um local diferente no mesmo computador ou em outro.

Antes de executar uma restauração de um aplicativo do Microsoft SQL Server de um Agente do Arcserve UDP (Windows) em um local diferente, considere o seguinte:

Se o local diferente está no mesmo computador

Para esta opção, é possível restaurar um banco de dados para um novo local (com o mesmo nome) ou restaurar com um novo nome (para o mesmo local):

- **Mesmo nome - Novo local**

  Por exemplo, se o banco de dados A está instalado no SQL Server atual em C:\DB_A e foi feito backup. É possível usar esta opção e especificar Local de arquivo alternativo para restaurar o banco de dados A em um local diferente como D:\Alternate_A.

  Depois que o banco de dados tiver sido restaurado, o arquivo de banco de dados localizado no novo local D:\Alternate_A será usado.

  Importante: durante a restauração, se você alterar o local do banco de dados, mas mantiver seu nome, o banco de dados anterior será excluído depois que a restauração for concluída. O arquivo de banco de dados restaurado será apontado para o novo local.

  Ao restaurar em um local alternativo, a seção Nome da instância não estará disponível porque o Nome da instância sempre deve ser igual e não pode ser alterado. Portanto, você não pode restaurar um banco de dados em uma instância alternativa presente no mesmo MS SQL Server.

- **Mesmo local - Novo nome**

  Por exemplo, se tiver dois bancos de dados (Banco de dados A e Banco de dados B) instalados no SQL Server e o backup de ambos foi feito. É possível usar esta opção e especificar Novo nome do banco de dados para restaurar o banco de dados A no mesmo local como Banco de dados A_New.

  Depois que o banco de dados tiver sido restaurado, esse local terá agora três bancos de dados (Bancos de dados A, banco de dados B, e banco de dados A_ New).

Se o local diferente estiver em outro computador

- O caminho de instalação do SQL Server deve ser o mesmo que o caminho de quando o backup foi realizado.

  Por exemplo, se o backup do SQL Server foi instalado em C:\SQLServer, o SQL Server no novo servidor do agente do Arcserve UDP (Windows) também deve ser instalado em C:\SQLServer.

- O mesmo nome de instância do banco de dados existente quando o backup foi realizado deve ser instalado no servidor do Agente do Arcserve UDP (Windows), caso contrário, o banco de dados associado àquela instância será ignorado durante a restauração.

Por exemplo, se o backup do SQL Server continha "Instance_1" com banco de dados A e B e "Instance_2" com banco de dados C, mas o servidor do Agente do Arcserve UDP (Windows) tem apenas a "Instance_1". Depois que a restauração for concluída, o banco de dados A e B serão restaurados, mas o banco de dados C não será restaurado.

- A versão do SQL Server no servidor do Agente do Arcserve UDP (Windows) deve ser compatível com a versão anterior do SQL Server usada durante a sessão de backup.

  Por exemplo, é possível restaurar um computador do SQL Server 2008 em um computador do SQL Server 2010; no entanto, não é possível restaurar um computador do SQL Server 2010 em um computador do SQL Server 2008.

- A restauração de um banco de dados de uma instância de 64 bits em instâncias de 32 bits não é suportada.

Considerações sobre a restauração do Microsoft SQL Server 2012/2014 AAG

Ao restaurar um banco de dados do Microsoft SQL Server 2012/2014 que faz parte de um Grupo de Disponibilidade AlwaysOn (AAG), há algumas considerações a serem feitas.

Se o banco de dados do MS SQL 2012/2014 for parte do Grupo de Disponibilidade AlwaysOn (AAG) e a restauração para o local original falhar, execute as seguintes tarefas:

1. Remova o banco de dados a ser restaurado do Grupo de disponibilidade. Para obter mais informações, consulte o link.
2. Compartilhe a sessão de backup no Agente do Arcserve UDP (Windows) em cada nó do Grupo de disponibilidade e, em seguida, restaure a sessão pelo Agente do Arcserve UDP (Windows) também em cada nó.
3. Adicione o banco de dados de volta a um Grupo de disponibilidade. Para obter mais informações, consulte o link.

Especificar as informações do Microsoft SQL Server a serem restauradas

O Agente do Arcserve UDP (Windows) permite que você não apenas proteja e recupere os dados, como também faz com que o aplicativo do Microsoft SQL Server que usar tais dados volte a funcionar. A recuperação do Microsoft SQL Server só pode ser feita usando o método Restore by Recovery Point.

O processo envolvido na restauração de um aplicativo do Microsoft SQL Server é o seguinte:

1. Especificar o ponto de recuperação e o banco de dados do Microsoft SQL Server
2. Definir as opções de restauração

Especificar o ponto de recuperação e o banco de dados do Microsoft SQL Server

Use a opção **Procurar pontos de recuperação** para restaurar a partir de um ponto de recuperação. Ao selecionar uma data de recuperação, todos os pontos de recuperação associados a essa data serão exibidos. Em seguida, você poderá procurar e selecionar o banco de dados do Microsoft SQL Server a ser restaurado.

Siga estas etapas:

1. Acesse a caixa de diálogo de seleção de método de restauração de uma das seguintes maneiras:

   - No Arcserve UDP:

     a. Efetue logon no Arcserve UDP.

     b. Clique na guia **Recursos**.

     c. Selecione **Todos os nós** no painel esquerdo.

        Todos os nós adicionados são exibidos no painel central.

     d. No painel central, selecione o nó do e clique em **Ações**.

     e. Clique em **Restaurar** no menu suspenso do nome do servidor.

        A caixa de diálogo de seleção do método de restauração é exibida.

        Observação: você é automaticamente conectado ao nó do agente e a caixa de diálogo de seleção do método de restauração é exibida no nó do agente.

   - No agente do Arcserve UDP (Windows):

     a. Efetue logon no Agente do Arcserve UDP (Windows).

     b. Na página inicial, selecione **Restaurar**.

     A caixa de diálogo de seleção do método de restauração é exibida.

2. Clique na opção **Procurar pontos de recuperação**.

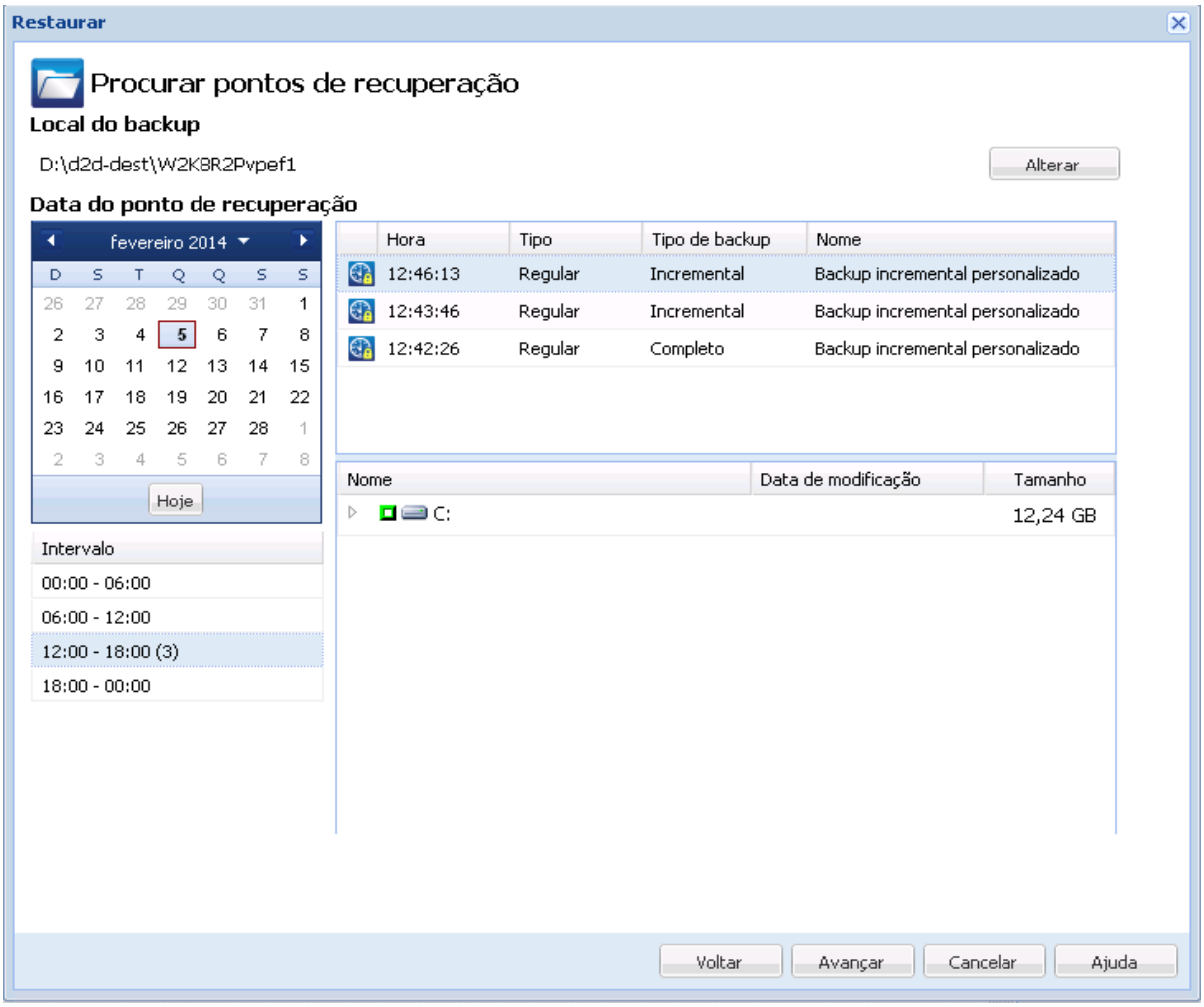
   A caixa de diálogo **Procurar pontos de recuperação** é exibida.

3. Selecione o ponto de recuperação (data e hora) e, em seguida, o banco de dados do Microsoft SQL Server a ser restaurado.

4. A caixa do marcador correspondente é preenchida (verde) para indicar que o banco de dados foi selecionado para restauração.

   Observação: se não desejar que os arquivos de log de transações sejam aplicados após a restauração, é necessário excluí-los manualmente antes de a

restauração ser realizada. Para obter mais informações sobre como excluir arquivos de log de transações manualmente, consulte a documentação do Microsoft SQL Server.



5. Clique em **Avançar**.

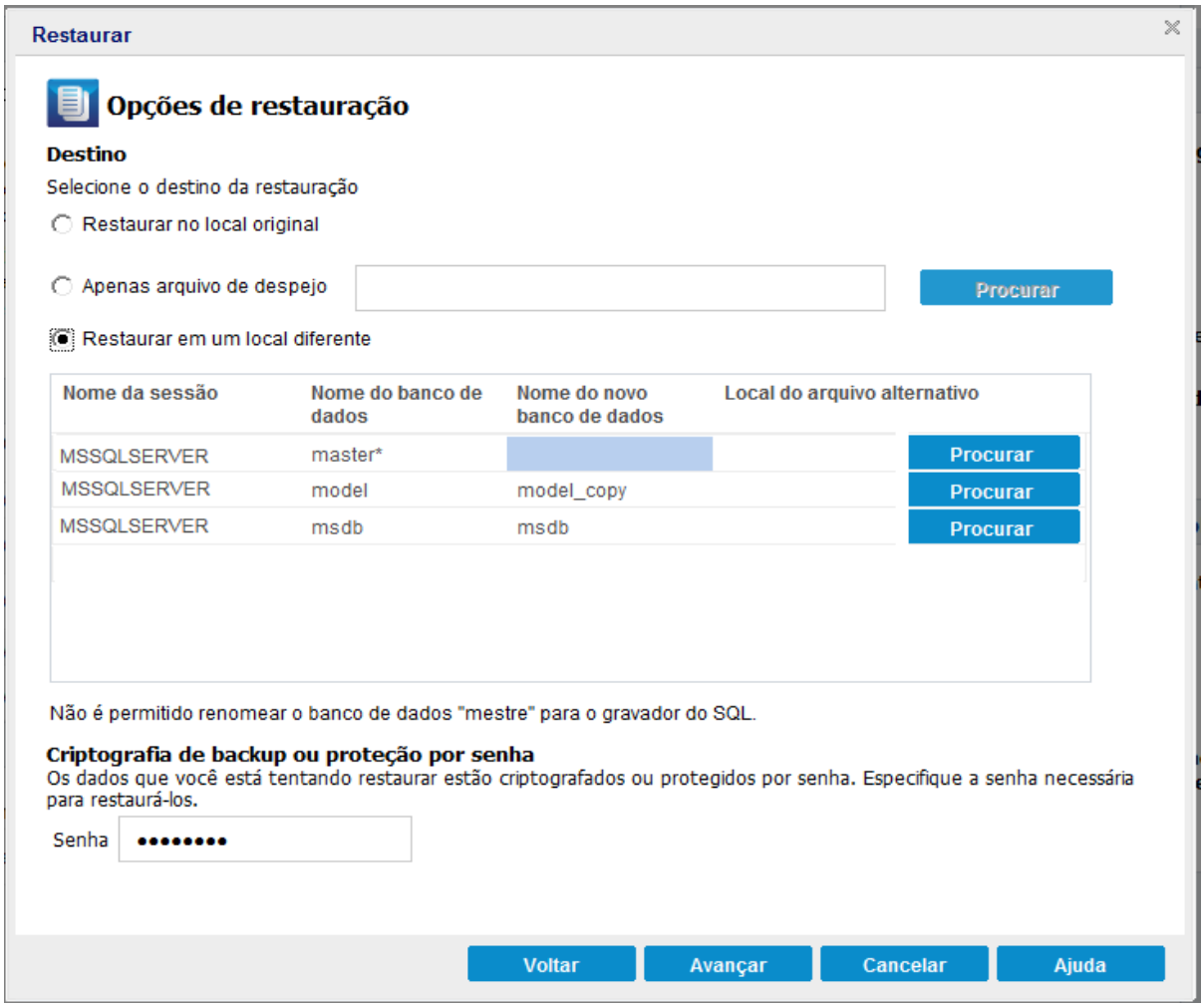
   A caixa de diálogo **Opções de restauração** é exibida.

Definir as opções de restauração

Depois de especificar um ponto de recuperação e conteúdo para restauração, defina as opções de cópia do ponto de recuperação selecionado.

Siga estas etapas:

1. Na caixa de diálogo **Opções de restauração**, selecione o destino da restauração.



2. Selecione o destino da restauração.

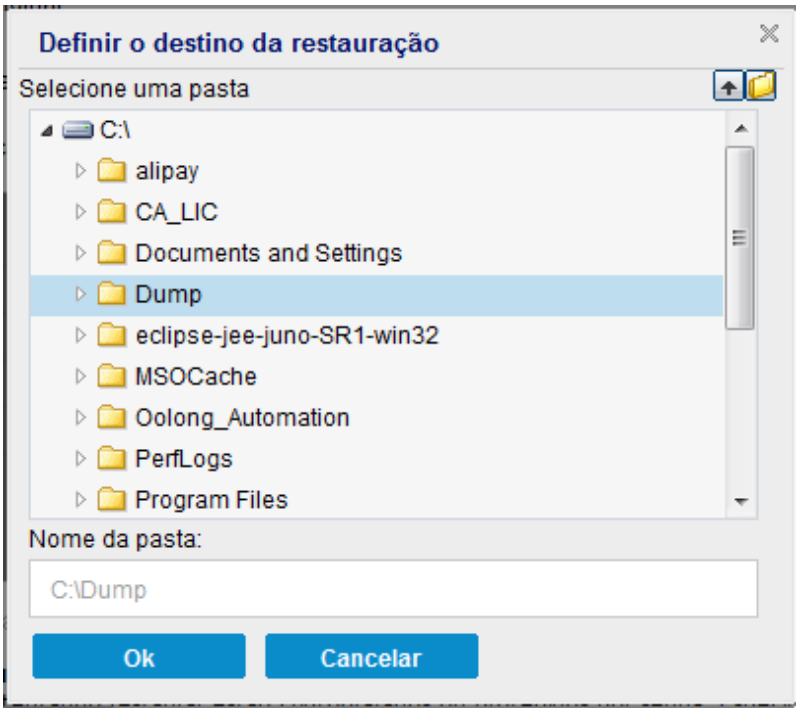
   As opções disponíveis permitem restaurar no local original do backup, restaurar somente o arquivo de despejo ou restaurar em um local alternativo.

Restaurar no local original

Restaura no local original a partir do qual a imagem de backup foi capturada.

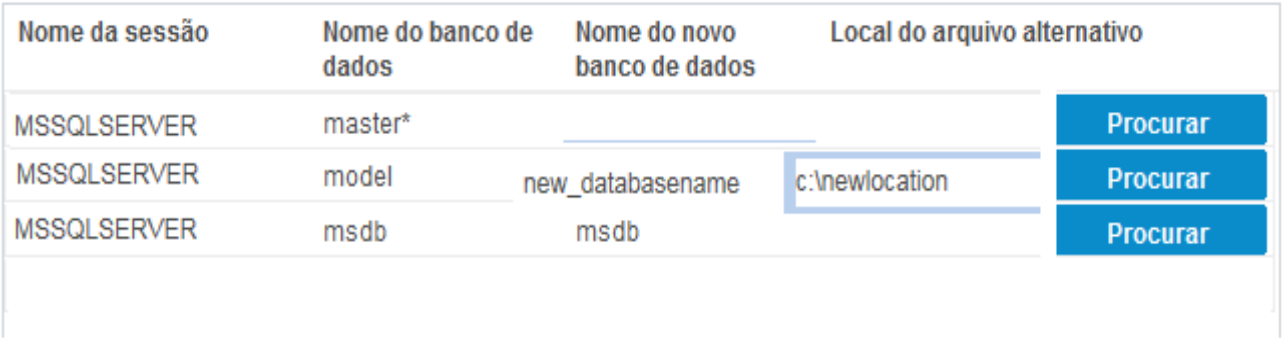
Somente arquivo de despejo

Para essa opção, o Agente do Arcserve UDP (Windows) despeja os arquivos selecionados do banco de dados do Microsoft SQL na pasta especificada. Ao selecionar essa opção, você pode especificar ou procurar o local da pasta onde o arquivo de despejo será restaurado.



Restaurar em um local diferente

Restaura em um local diferente que não o local original.



Os backups podem ser copiados em locais de rede e podem ser usados por várias instâncias do SQL Server. É possível executar uma restauração de vários bancos de dados (simultaneamente) no nível de instância. Nesta

listagem, você pode selecionar a instância do banco de dados e especificar um novo nome de banco de dados e o local alternativo onde restaurá-lo. Além disso, pode também ir até o local alternativo em que o banco de dados será restaurado.

A restauração de um aplicativo Microsoft SQL Server para um local diferente tem algumas limitações que você deve estar ciente. Para obter mais informações, consulte a seção **Considerações da restauração do Microsoft SQL Server para um local diferente** no tópico Verificar os pré-requisitos e as considerações da restauração.

3. Clique em **Avançar**.

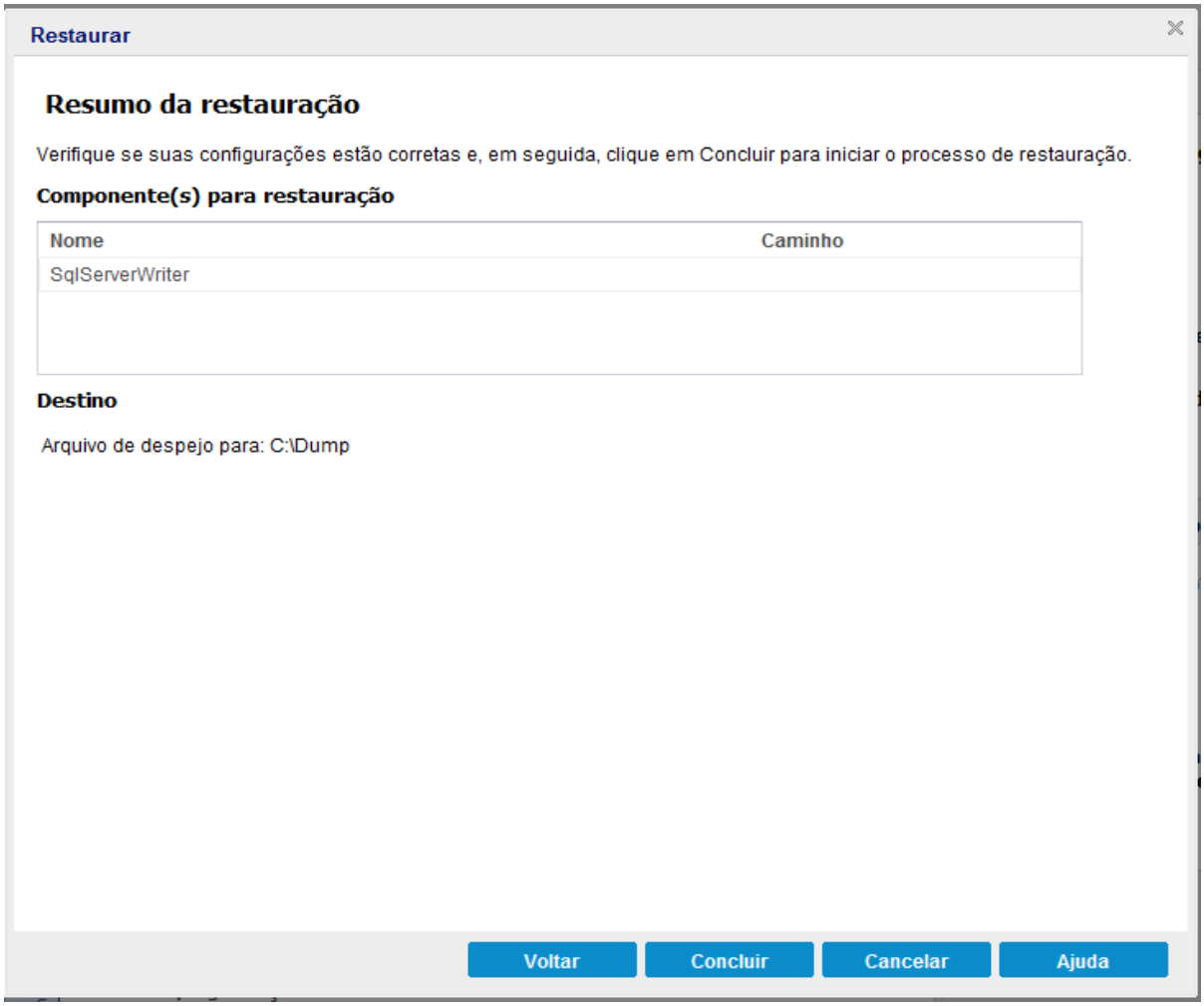
   A caixa de diálogo **Resumo da restauração** é exibida.

Restaurar o aplicativo do Microsoft SQL Server

Após definir as opções de restauração, verifique se suas configurações estão corretas e confirme o processo de restauração. O **Resumo da restauração** o auxilia a revisar todas as opções de restauração definidas e modificá-las se necessário.

Siga estas etapas:

1. Na caixa de diálogo **Resumo da restauração**, examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.



- Se as informações de resumo não estiverem corretas, clique em **Anterior** e volte à caixa de diálogo em questão para alterar a configuração incorreta.
- Se as informações de resumo estiverem corretas, clique em **Concluir** para iniciar o processo de restauração.

O aplicativo do Microsoft SQL Server é restaurado.

Verificar se o aplicativo do Microsoft SQL Server foi restaurado

Siga estas etapas:

1. Navegue até o destino de restauração do Agente do Arcserve UDP (Windows) que você especificou.

   Por exemplo, se você optar por restaurar o banco de dados do Microsoft SQL Server no local original, após a restauração ser concluída, vá até o local físico para verificar se os logs e o banco de dados do Microsoft SQL Server foram restaurados.

   Se você optar por restaurar o banco de dados do Microsoft SQL Server no local Apenas arquivo de despejo, o agente do Arcserve UDP (Windows) restaurará os logs e o banco de dados do Microsoft SQL Server em um local especificado.

2. Verifique se o aplicativo do Microsoft SQL Server foi restaurado e se o banco de dados está montado e acessível.

   O aplicativo do Microsoft SQL Server é restaurado com êxito.

Como restaurar a partir de um caminho UNC/NFS

Sempre que o Arcserve UDP obtém sucesso no backup de caminho UNC/NFS, ele faz backup de todos os arquivos e todas as pastas alterados após a última tarefa bem-sucedida. Esse método de restauração permite procurar os arquivos/pastas arquivados e especificar exatamente qual arquivo você deseja restaurar.

Execute as tarefas a seguir para restaurar um ponto de recuperação:

1. Revisar os pré-requisitos e as considerações para restauração
2. Especificar os arquivos/diretórios em um caminho UNC/NFS a ser restaurado
    a. Especificar os arquivos e o conteúdo a serem restaurados
    b. Definir as opções de restauração
3. Restaurar os arquivos e o conteúdo
4. Verificar se o conteúdo foi restaurado

Verificar os pré-requisitos e as considerações para restauração

Verifique se os pré-requisitos a seguir existem antes de executar uma restauração:

- Você tem pelo menos um ponto de recuperação para restauração.
- Você tem um destino válido e acessível de ponto de recuperação para do qual restaurar o ponto de recuperação de conteúdo.
- Você tem um local de destino válido e acessível para o qual restaurar o ponto de recuperação de conteúdo.

Especificar as informações de caminho UNC/NFS a serem restauradas

O Arcserve UDP fornece uma opção para restaurar os dados a partir de um caminho UNC/NFS. O objetivo de executar uma tarefa de restauração com êxito é identificar rapidamente os dados necessários e recuperá-los do local de backup adequado. Cada tarefa de restauração requer uma origem e um destino.

O processo envolvido na restauração de um caminho UNC/NFS ocorre da seguinte maneira:

1. Especificar os arquivos/pastas e o conteúdo a ser restaurado
2. Definir as opções de restauração

Especificar os arquivos/as pastas UNC/NFS e o conteúdo a ser restaurado

Esta seção fornece informações sobre como especificar os arquivos/pastas UNC/NFS e o conteúdo a ser restaurado.

Siga estas etapas:

1. Acesse a caixa de diálogo de seleção de método de restauração de uma das seguintes maneiras:

   No console do Arcserve UDP:

   a. Efetue logon no Console do Arcserve UDP.

   b. Navegue até **recursos** > **Nó** > **Todos os nós**.

      Todos os nós do adicionados são exibidos no painel central.

   c. Clique com o botão direito do mouse no nó e clique em **Restaurar**.

      Você é conectado automaticamente ao console do nó do agente e a caixa de diálogo Restaurar é aberta.

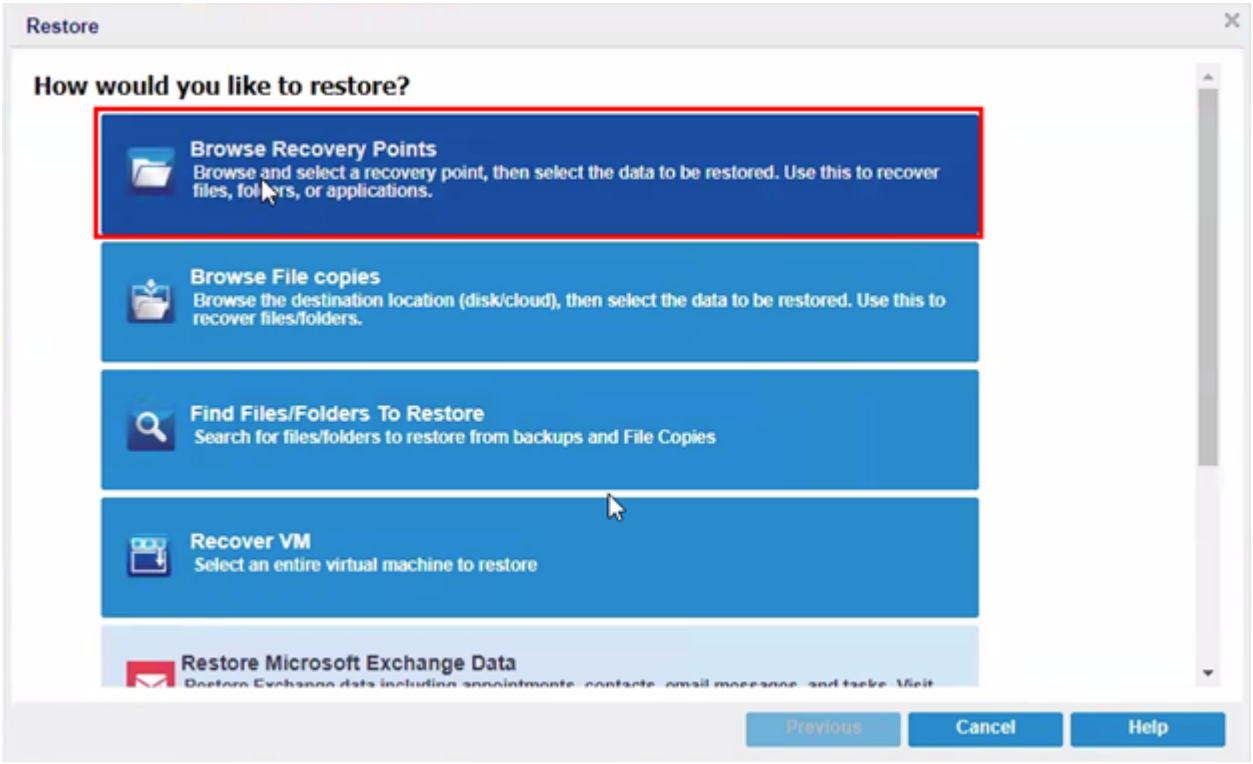
   No agente do Arcserve UDP (Windows):

   a. Efetue logon no Agente do Arcserve UDP (Windows).

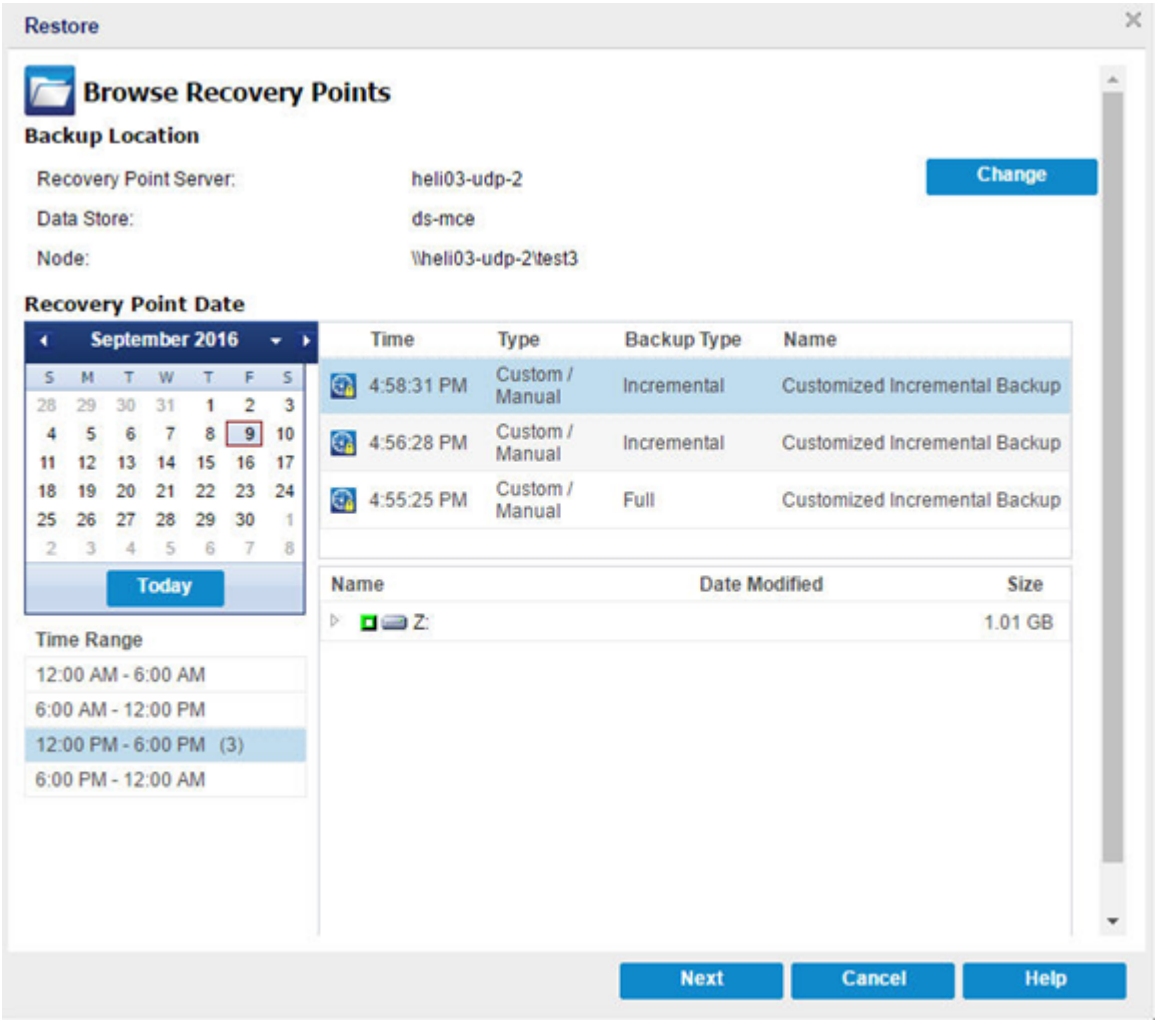
   b. Na página inicial, selecione **Restaurar**.

      A caixa de diálogo Restaurar é exibida.

2. Na caixa de diálogo Restaurar, clique na opção **Procurar os pontos de recuperação**.



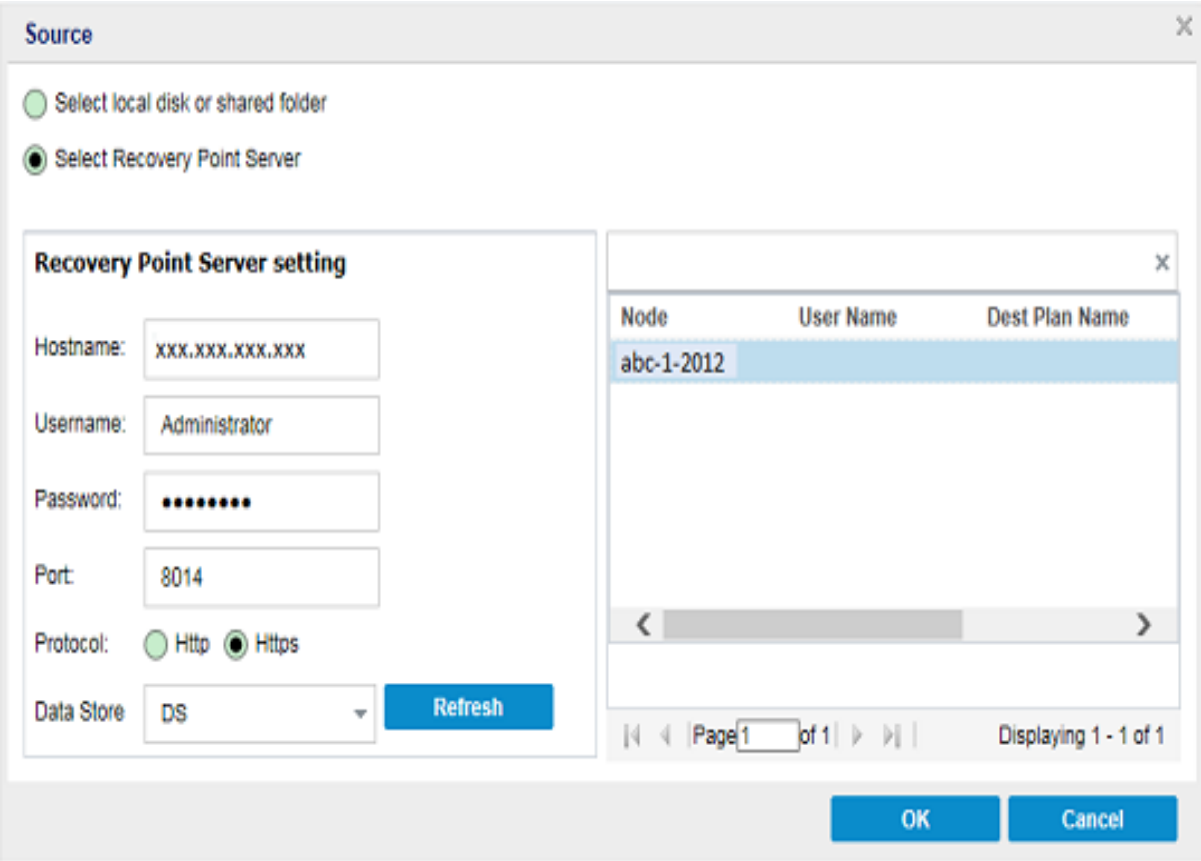
3. Na página Procurar os pontos de recuperação, faça o seguinte:



a. Para atualizar o local do backup, clique em **Alterar**.

   A caixa de diálogo Origem é exibida.

b. Na caixa de diálogo Origem, selecione um dos seguintes locais de backup e clique em **OK**:



Selecionar o disco local ou uma pasta compartilhada

1. Especifique ou procure o local onde as suas imagens de backup estão armazenadas e selecione o backup de origem adequado.
2. Para verificar a conexão com o local especificado, clique no botão de seta verde. Se necessário, forneça o nome de usuário e a senha para acessar esse local de origem.

   A caixa de diálogo Selecionar o local do backup é exibida.
3. Selecione a pasta onde estão armazenados os pontos de recuperação e clique em **OK**.

   A caixa de diálogo Selecione o local do backup será fechada, e você poderá ver o local do backup na caixa de diálogo Origem.

   Os pontos de recuperação são listados na caixa de diálogo Procurar pontos de recuperação.

Selecionar servidor de ponto de recuperação

1. Especifique os detalhes da configuração do servidor de ponto de recuperação e clique em **Atualizar**.

Todos os agentes estão listados na coluna Agente de proteção de dados na caixa de diálogo Origem.

2. Selecione o agente na lista exibida.

   Os pontos de recuperação são listados na caixa de diálogo Procurar pontos de recuperação.

c. Selecione a data no calendário para a imagem de backup para restaurar.

   Todas as datas que contém pontos de recuperação para a origem do backup especificado são realçadas em verde.

   Os pontos de recuperação correspondentes a essa data são exibidos, juntamente com a hora do backup, o tipo de backup que foi executado (completo, incremental ou de verificação) e o nome do backup.

d. Selecione um ponto de recuperação para restaurar.

   O conteúdo do backup (incluindo aplicativos) para o ponto de recuperação selecionado é exibida.

   Observação: um ícone de relógio com um símbolo de cadeado indica que o ponto de recuperação contém informações criptografadas e que pode ser necessária uma senha para restaurar.

e. Selecione o conteúdo para restaurar.

   - Para uma restauração de nível de volume, pode-se especificar a restauração do volume inteiro ou de arquivos/pastas selecionados no volume.
   - Para uma restauração de nível do aplicativo, pode-se especificar a restauração do aplicativo inteiro ou de itens selecionados no aplicativo, como componentes, bancos de dados, instâncias e assim por diante.

4. Clique em **Avançar**.

   A caixa de diálogo Opções de restauração é exibida.

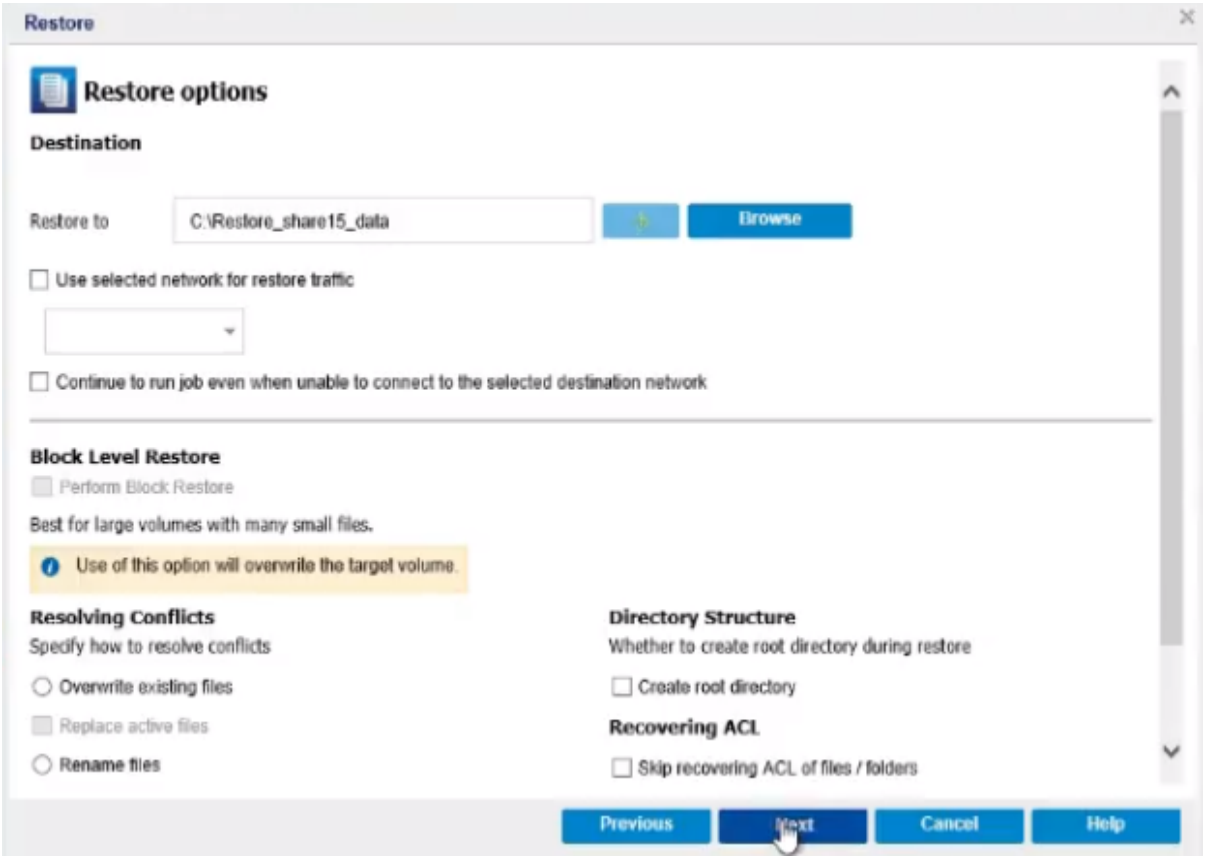
   O ponto de recuperação e o conteúdo para restauração é especificado.

Definir as opções de restauração

Depois de especificar um ponto de recuperação e conteúdo para restauração, defina as opções de cópia do ponto de recuperação selecionado.

Siga estas etapas:

1. Na caixa de diálogo Opções de restauração, selecione o destino da restauração.



A opção de destino é:

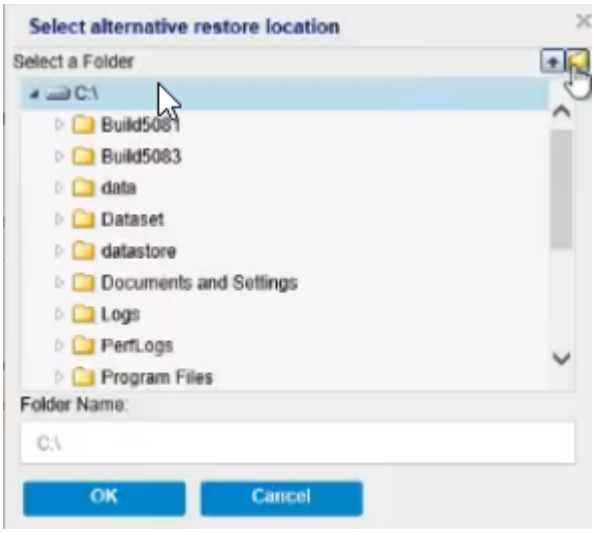
Restaurar para

Restaura no local especificado. Para restaurar para o local original, faça o seguinte:

a. Para fornecer o destino, clique em **Procurar**.

   A caixa de diálogo Selecionar local de restauração alternativo é exibida.

b. Selecione a pasta existente ou crie uma nova pasta, conforme necessário, e clique em **OK**.



c. Para verificar a conexão com o local especificado, clique no botão de seta verde. Se necessário, digite o nome de usuário e a senha para acessar esse local.

Observação: a restauração em um compartilhamento NFS a partir de um plano de proteção do NFS não é permitida.

2. Para ativar a comunicação entre a rede selecionada e o servidor de ponto de recuperação, marque a caixa de seleção **Usar a rede selecionada para restaurar o tráfego** e, em seguida, selecione a rede na lista suspensa.

   Observação: se a rede de backup selecionada não estiver acessível e para continuar a tarefa de backup com a rede disponível ou com a rede padrão, clique na caixa de seleção **Continuar a executar a tarefa mesmo quando não for possível se conectar à rede de backup selecionada**.

3. Especifique a opção **Resolvendo conflitos** que o Arcserve UDP executará se forem encontrados conflitos durante o processo de restauração.

   As opções disponíveis são:

   Substituir arquivos existentes

   Sobrescreve (substitui) qualquer arquivo existente que está localizado no destino da restauração. Todos os objetos serão restaurados dos arquivos de backup, independentemente da presença atual deles no computador.

   Substituir os arquivos ativos

   Substitui todos os arquivos ativos ao reinicializar. Se, durante a tentativa de restauração, o agente do Arcserve UDP (Windows) detectar que o arquivo existente está em uso ou sendo acessado, para evitar erros, ele não substituirá o arquivo imediatamente, só depois que o computador for reinicializado. (A res-

tauração ocorrerá imediatamente, mas a substituição de arquivos ativos é feita durante a próxima reinicialização).

Essa opção só estará disponível se você selecionar a opção **Substituir os arquivos existentes**.

Observação: se essa opção não estiver selecionada, qualquer arquivo ativo será ignorado na restauração.

Renomear arquivos

Cria um novo arquivo se o nome de arquivo já existir. A seleção desta opção copia o arquivo de origem no destino com o mesmo nome de arquivo, mas com uma extensão diferente. Os dados serão restaurados no novo arquivo.

Ignorar arquivos existentes

Ignora e não substitui (sobrescreve) os arquivos localizados no destino da restauração. Apenas os objetos inexistentes em seu computador no momento serão restaurados dos arquivos de backup.

Padrão: Ignorar arquivos existentes.

4. Para criar um diretório raiz durante a restauração, especifique a **Estrutura de diretórios**.

Criar diretório raiz

Especifica que, se uma estrutura de diretório raiz existir na imagem de backup capturada, o Arcserve UDP recriará a mesma estrutura no caminho de destino de restauração.

Se essa opção não for selecionada, o arquivo ou pasta será restaurado diretamente para a pasta de destino.

Por exemplo, se durante o backup você capturou os arquivos "C:\Pasta1\Subpasta2\A.txt" e "C:\Pasta1\Subpasta2\B.txt" e durante a restauração foi especificado como destino o local "D:\Restore".

- Se você optar por restaurar os arquivos "A.txt" e "B.txt" individualmente, o destino dos arquivos restaurados será "D:\Restore\A.txt" e "D:\Restore\B.txt" (o diretório raiz acima do nível de arquivo especificado não será recriado).
- Se você optar por restaurar a partir do nível da "Subpasta2", o destino dos arquivos restaurados será "D:\Restore\Subpasta2\A.txt" e "D:\Restore\Subpasta2\B.txt" (o diretório acima do nível de pasta especificado não será recriado).

Com esta opção selecionada, todo o caminho de diretório raiz para os arquivos / pastas (incluindo o nome de volume) é recriado até a pasta de destino. Se os arquivos/pastas a serem restaurados tiverem o mesmo nome de volume, o

caminho do diretório raiz de destino não incluirá esse nome de volume. No entanto, se os arquivos/pastas a serem restaurados forem de nomes de volume diferentes, o caminho do diretório raiz do destino incluirá o nome do volume.

Por exemplo, se durante o backup você capturou os arquivos "C:\Pasta1\Subpasta2\A.txt", "C:\Pasta1\Subpasta2\B.txt" e também "E:\Pasta3\Subpasta4\C.txt" e durante a restauração foi especificado como destino de restauração o local "D:\Restore".

- Se você optar por restaurar apenas o arquivo "A.txt", o destino do arquivo restaurado será "D:\Restore\Pasta1\Subpasta2\A.txt" (o diretório raiz inteiro, sem o nome do volume, será recriado).
- Se você optar por restaurar tanto o arquivo "A.txt" como o "C.txt", o destino dos arquivos restaurados será "D:\Restore\C\Pasta1\Subpasta2\A.txt" e "D:\Restore\E\Pasta3\Subpasta4\C.txt" (o diretório raiz inteiro, com o nome do volume, será recriado).

5. Especifique se deseja que a ação Recuperando o ACL ignore a recuperação de ACL de arquivos/pastas.

   Se a opção **Ignorar a recuperação de ACL de arquivos/pastas** estiver selecionada, somente arquivos/pastas de origem serão restaurados. O atributo de pastas/arquivos não é restaurado para que todos possam acessar.

   Padrão: restaura arquivos/pastas de origem com o atributo - lista de controle de acesso.

6. Se necessário, digite a **Senha de criptografia de backup** se os dados que está tentando restaurar estiverem criptografados.

   A senha não será necessária se você estiver tentando fazer a restauração a partir do mesmo computador do agente do Arcserve UDP (Windows) em que o backup criptografado foi executado. No entanto, se você estiver tentando fazer a restauração a partir de um computador diferente do Agente do Arcserve UDP (Windows), a senha será necessária.

   Observação: um ícone de relógio com um símbolo de cadeado indica que o ponto de recuperação contém informações criptografadas e que pode ser necessária uma senha para restaurar.

7. Clique em **Avançar**.

   A caixa de diálogo Resumo da restauração é exibida.

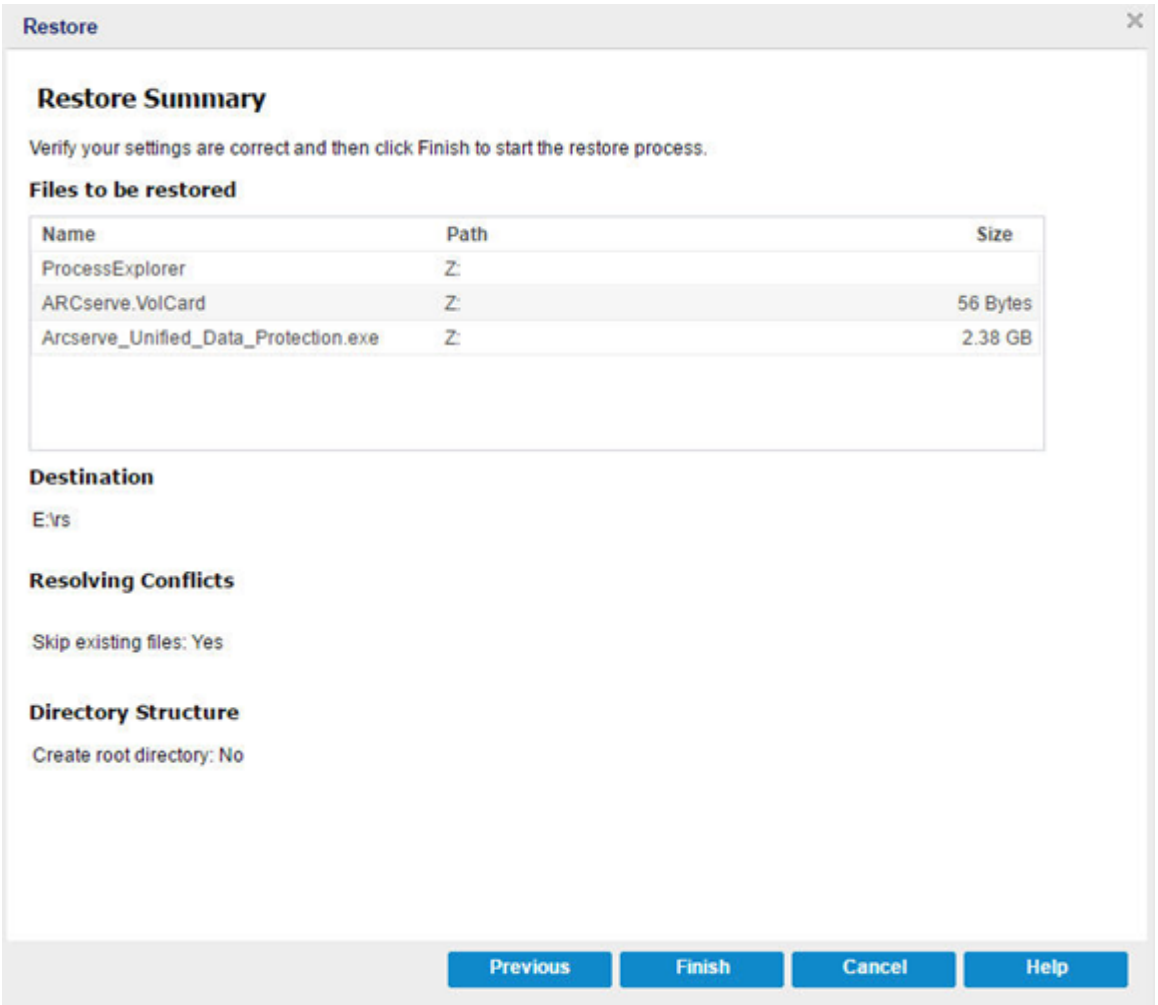
   As opções de restauração são definidas para restaurar a partir de um ponto de recuperação.

Restaurar arquivos/pastas e o conteúdo localizados no caminho UNC/NFS

Após definir as opções de restauração, verifique se suas configurações estão corretas e confirme o processo de restauração. A página Resumo da restauração o auxilia a revisar todas as opções de restauração definidas e modificá-las se necessário.

Siga estas etapas:

1. Na caixa de diálogo Resumo da restauração, examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.



2. Siga um destes procedimentos:
   - Se as informações do resumo não estiverem corretas, clique em **Anterior** e volte à caixa de diálogo em questão para alterar a configuração incorreta.

- Se as informações de resumo estiverem corretas, clique em **Concluir** para iniciar o processo de restauração.

O ponto de recuperação do conteúdo é restaurado.

Verificar se o conteúdo foi restaurado

Após a conclusão da tarefa de restauração, certifique-se de que todos os arquivos estejam restaurados no nó de destino. Verifique as guias **Histórico da tarefa** e **Log de atividades** no painel Status para monitorar o andamento do processo de restauração.

Siga estas etapas:

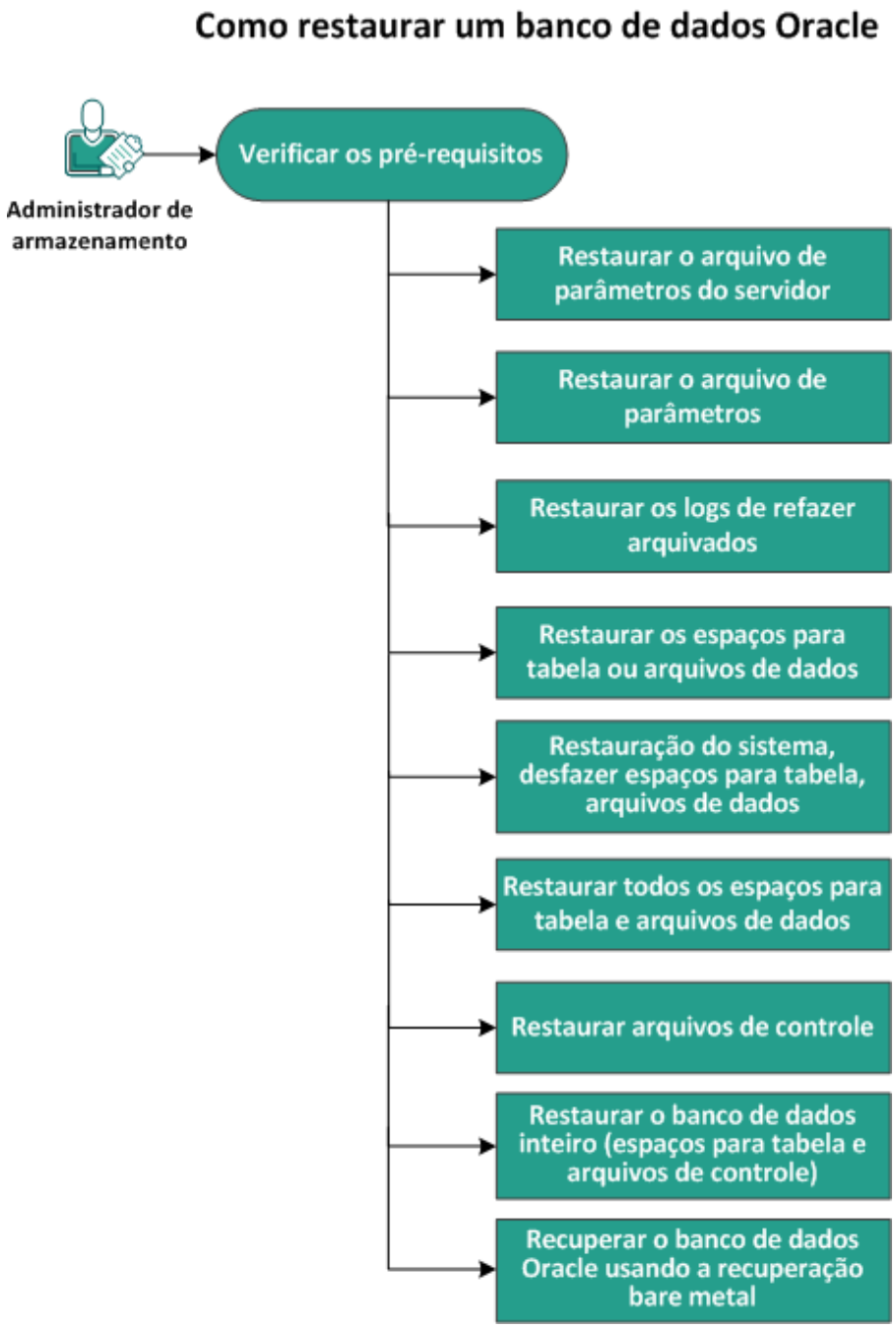
1. Navegue para o computador de destino em que você restaurou os dados.
2. Verifique se os dados necessários do ponto de recuperação foram restaurados.

   A restauração do conteúdo é verificada com êxito.

Como restaurar um banco de dados Oracle

É possível restaurar determinados arquivos e espaços para tabelas ou todo o banco de dados Oracle usando o assistente de restauração. Para restaurar um banco de dados Oracle, localize os arquivos ou espaços para tabelas no nó de destino. Em seguida, restaure os arquivos ou espaços para tabelas usando o assistente de restauração.

O seguinte diagrama ilustra o processo para restaurar um banco de dados Oracle:



Execute as tarefas a seguir para restaurar um banco de dados Oracle:

- Verificar os pré-requisitos
- Restaurar o arquivo de parâmetros do servidor
- Restaurar o arquivo de parâmetros
- Restaurar os logs de repetição arquivados
- Restaurar os espaços para tabelas ou arquivos de dados
- Restaurar o sistema, desfazer espaços para tabelas, arquivos de dados
- Restaurar todos os espaços para tabelas e arquivos de dados
- Restaurar arquivos de controle
- Restaurar todo o banco de dados (espaços para tabelas e arquivos de controle)
- Recuperar o banco de dados Oracle usando recuperação bare metal

Verificar os pré-requisitos e as considerações

Verifique os pré-requisitos a seguir antes de restaurar o banco de dados Oracle:

- O gravador Oracle VSS no nó de backup está funcionando corretamente. Se o gravador Oracle VSS não funcionar corretamente, será exibida uma mensagem de aviso no Log de atividades associadas à tarefa de backup.
- Você tem um ponto de recuperação válido.
- Para evitar qualquer problema de falha na restauração, salve uma cópia duplicada dos arquivos do sistema antes de substituir os arquivos originais.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Restaurar o arquivo de parâmetros do servidor

O arquivo de parâmetros do servidor é um repositório para parâmetros de inicialização. Antes de restaurar, você deve localizar o arquivo. Quando você localizar os arquivos, verifique se o banco de dados está no estado Aberto.

Siga estas etapas:

1. Efetue logon no computador no qual deseja restaurar os arquivos.
2. Abra o arquivo de parâmetros do servidor usando o seguinte comando:

   SQL> SHOW PARAMETER SPFILE;
3. Encerre o banco de dados ou a instância do Oracle antes de iniciar o processo de restauração:

   SQL> SHUTDOWN IMMEDIATE;
4. Efetue logon no Console do Arcserve UDP.
5. Restaure o arquivo de parâmetros do servidor usando o Assistente de restauração. Para obter mais informações sobre o processo de restauração, consulte Como restaurar de um ponto de recuperação.
6. Efetue logon no computador de destino.
7. Navegue até a pastas específicas e verifique se os arquivos foram restaurados.
8. Conecte-se ao SQL*Plus para reiniciar a instância do Oracle com o arquivo de parâmetros do servidor restaurado.

   O arquivo de parâmetros do servidor é restaurado.

Restaurar o arquivo de parâmetros

O arquivo de parâmetros inclui uma lista de parâmetros de inicialização e os valores para cada parâmetro. Antes de restaurar, você deve localizar o arquivo. Quando você localizar os arquivos, verifique se o banco de dados está no estado Aberto.

Siga estas etapas:

1. Efetue logon no computador no qual deseja restaurar os arquivos.
2. Localize o arquivo de parâmetros (pfile).

   Normalmente, o pfile (INIT<SID>.ORA) está localizado no diretório %ORACLE_HOME/database. Você pode digitar "INIT<SID>.ORA" para localizar o pfile.
3. Encerre o banco de dados ou a instância do Oracle antes de iniciar o processo de restauração:

   SQL> SHUTDOWN IMMEDIATE;
4. Efetue logon no Console do Arcserve UDP.
5. Restaure o arquivo de parâmetros usando o Assistente de restauração. Para obter mais informações sobre o processo de restauração, consulte Como restaurar de um ponto de recuperação.
6. Efetue logon no computador de destino.
7. Navegue até a pastas específicas e verifique se os arquivos foram restaurados.
8. Conecte-se ao SQL*Plus para reiniciar a instância do Oracle com o arquivo de parâmetros restaurado.

   O arquivo de parâmetros é restaurado.

Restaurar os logs de repetição arquivados

Os logs de repetição arquivados são usados para recuperar um banco de dados ou atualizar um banco de dados em espera. Antes de restaurar, você deve localizar o arquivo. Quando você localizar os arquivos, verifique se o banco de dados está no estado Aberto.

Siga estas etapas:

1. Efetue logon no computador no qual deseja restaurar os arquivos.
2. Localize os logs de repetição arquivados usando o seguinte comando.

   SQL> ARCHIVE LOG LIST;

   SQL> SHOW PARAMETER DB_RECOVERY_FILE_DEST;
3. Efetue logon no Console do Arcserve UDP.
4. Restaurar os logs de repetição arquivados usando o Assistente de restauração. Para obter mais informações sobre o processo de restauração, consulte Como restaurar de um ponto de recuperação.
5. Efetue logon no computador de destino.
6. Navegue até a pastas específicas e verifique se os logs de repetição arquivados foram restaurados.

   Os logs de repetição arquivados são restaurados.

Restaurar os espaços para tabelas ou arquivos de dados

Você pode restaurar o espaço para tabelas ou os arquivos de dados. Antes de restaurar, você deve localizar o arquivo. Quando você localizar os arquivos, verifique se o banco de dados está no estado Aberto. Se o banco de dados estiver aberto, use a ALTER TABLESPACE. OFFLINE instrui para tornar os espaços para tabelas ou arquivos de dados offline antes de iniciar o processo de restauração.

Siga estas etapas:

1. Efetue logon no computador no qual deseja restaurar os arquivos de dados ou espaços para tabelas.
2. Localize os espaços para tabelas de usuário ou arquivos de dados usando o seguinte comando:

   SQL> SELECT FILE_NAME, TABLESPACE_NAME FROM DBA_DATA_FILES;
3. Altere o estado do banco de dados para montar, não montar ou encerre antes de restaurar espaços para tabelas ou arquivos de dados.

   SQL> STARTUP MOUNT;

   SQL> STARTUP NOMOUNT;

   SQL> SHUTDOWN IMMEDIATE;
4. Efetue logon no Console do Arcserve UDP.
5. Restaure os espaços para tabelas ou arquivos de dados usando o Assistente de restauração. Para obter mais informações sobre o processo de restauração, consulte Como restaurar de um ponto de recuperação.
6. Efetue logon no computador de destino.
7. Navegue até a pastas específicas e verifique se os espaços para tabelas ou arquivos de dados foram restaurados.
8. Recuperar o espaço para tabelas ou arquivos de dados.
   - Para recuperar um espaço para tabelas, insira o seguinte comando na tela de prompt do SQL*PLUS:

     SQL> RECOVER TABLESPACE "tablespace_name";
   - Para recuperar um arquivo de dados, insira o seguinte comando na tela de prompt do SQL*PLUS:

     SQL> RECOVER DATAFILE 'path';

O Oracle verifica os arquivos de repetição de log arquivados dos quais necessita para aplicar e exibir os nomes dos arquivos em uma sequência.

9. Digite AUTO na tela de prompt do SQL*PLUS para aplicar os arquivos.

   O Oracle aplica os arquivos de log para restaurar os arquivos de dados. Depois que o Oracle terminar de aplicar o arquivo de repetição de log, ele exibirá as seguintes mensagens:

   Aplicando arquivo de log sugerido

   Log aplicado

   Após a aplicação de cada log, o Oracle continuará a aplicar o arquivo de redo log seguinte até que a recuperação esteja completa.

10. Insira o comando a seguir para colocar o espaço para tabelas online:

    SQL> ALTER TABLESPACE "tablespace_name" ONLINE;

    Agora, o espaço para tabelas está recuperado para o último arquivo de log disponível.

Restaurar sistema, desfazer espaços para tabelas ou arquivos de dados

Você pode restaurar o sistema, desfazer espaços para tabelas ou arquivos de dados. Antes de restaurar, você deve localizar o arquivo. Quando você localizar os arquivos, verifique se o banco de dados está no estado Aberto.

Siga estas etapas:

1. Efetue logon no computador no qual deseja restaurar o sistema ou desfazer espaços para tabelas ou arquivos de dados.
2. Localize os espaços para tabelas de usuário ou arquivos de dados usando o seguinte comando:

   SQL> SELECT TABLESPACE_NAME, FILE_NAME FROM DBA_DATA_FILES;
3. Altere o estado do banco de dados para montar, não montar ou encerre antes de restaurar espaços para tabelas ou arquivos de dados.

   SQL> STARTUP MOUNT;

   SQL> STARTUP NOMOUNT;

   SQL> SHUTDOWN IMMEDIATE;
4. Efetue logon no Console do Arcserve UDP.
5. Restaure os espaços para tabelas ou arquivos de dados usando o Assistente de restauração. Para obter mais informações sobre o processo de restauração, consulte Como restaurar de um ponto de recuperação.
6. Efetue logon no computador de destino.
7. Navegue até as pastas específicas e verifique se o sistema, os espaços para tabelas ou arquivos de dados desfeitos foram restaurados.
8. Recuperar o espaço para tabelas ou arquivos de dados.
   - Para recuperar um espaço para tabelas, insira o seguinte comando na tela de prompt do SQL*PLUS:

     SQL> RECOVER TABLESPACE "tablespace_name";
   - Para recuperar um arquivo de dados, insira o seguinte comando na tela de prompt do SQL*PLUS:

     SQL> RECOVER DATAFILE 'path';

   O Oracle verifica os arquivos de repetição de log arquivados dos quais necessita para aplicar e exibir os nomes dos arquivos em uma sequência.
9. Digite AUTO na tela de prompt do SQL*PLUS para aplicar os arquivos.

O Oracle aplica os arquivos de log para restaurar os arquivos de dados. Depois que o Oracle terminar de aplicar o arquivo de repetição de log, ele exibirá as seguintes mensagens:

Aplicando arquivo de log sugerido

Log aplicado

Após a aplicação de cada log, o Oracle continua a aplicar o arquivo de repetição de log seguinte até que a recuperação seja concluída.

10. Insira o comando a seguir para colocar o espaço para tabelas online:

    SQL> ALTER TABLESPACE "tablespace_name" ONLINE;

    Agora, o espaço para tabelas está recuperado para o último arquivo de log disponível.

Restaurar todos os espaços para tabelas e arquivos de dados

É possível restaurar todos os espaços para tabelas e os arquivos de dados. Antes de restaurar, você deve localizar o arquivo. Quando você localizar os arquivos, verifique se o banco de dados está no estado Aberto. Se o banco de dados estiver aberto, use a ALTER TABLESPACE. OFFLINE instrui para tornar os espaços para tabelas ou arquivos de dados offline antes de iniciar o processo de restauração.

Siga estas etapas:

1. Efetue logon no computador no qual deseja restaurar os arquivos de dados ou espaços para tabelas.
2. Localize os espaços para tabelas de usuário ou arquivos de dados usando o seguinte comando:

   SQL> SELECT FILE_NAME, TABLESPACE_NAME FROM DBA_DATA_FILES;
3. Altere o estado do banco de dados para montar, não montar ou encerre antes de restaurar espaços para tabelas ou arquivos de dados.

   SQL> STARTUP MOUNT;

   SQL> STARTUP NOMOUNT;

   SQL> SHUTDOWN IMMEDIATE;
4. Efetue logon no Console do Arcserve UDP.
5. Restaure os espaços para tabelas ou arquivos de dados usando o Assistente de restauração. Para obter mais informações sobre o processo de restauração, consulte Como restaurar de um ponto de recuperação.
6. Efetue logon no computador de destino.
7. Navegue até a pastas específicas e verifique se os espaços para tabelas ou arquivos de dados foram restaurados.
8. Recuperar o banco de dados do.

   SQL> RECOVER DATABASE;

   O Oracle verifica os arquivos de repetição de log arquivados dos quais necessita para aplicar e exibir os nomes dos arquivos em uma sequência.
9. Digite AUTO na tela de prompt do SQL*PLUS para aplicar os arquivos.

   O Oracle aplica os arquivos de log para restaurar os arquivos de dados. Depois que o Oracle terminar de aplicar o arquivo de repetição de log, ele exibirá as seguintes mensagens:

   Aplicando arquivo de log sugerido

Log aplicado

Após a aplicação de cada log, o Oracle continua a aplicar o arquivo de repetição de log seguinte até que a recuperação seja concluída.

Observação: se o Oracle exibir um erro indicando que o arquivo de log não pode ser aberto, talvez esse arquivo não esteja disponível. Nesses casos, execute a recuperação de mídia incompleta para recuperar o banco de dados novamente. Depois que todos os arquivos de log forem aplicados, a recuperação do banco de dados estará completa. Para obter mais informações sobre recuperação incompleta de mídia, consulte a documentação do Oracle.

10. Insira o comando a seguir para colocar o banco de dados online:

    SQL> ALTER DATABASE OPEN;

    Agora, o espaço para tabela está recuperado para o último arquivo de log disponível.

    Observação: se você executar uma recuperação incompleta de mídia, digite o seguinte comando para alterar o banco de dados para o estado aberto:

    SQL> ALTER DATABASE OPEN RESETLOGS;

Restaurar arquivos de controle

É possível restaurar os arquivos de controle que armazenam a estrutura física do banco de dados. Antes de restaurar, você deve localizar o arquivo. Quando você localizar os arquivos, verifique se o banco de dados está no estado Aberto.

Siga estas etapas:

1. Efetue logon no computador no qual deseja restaurar os arquivos de controle.
2. Localize os arquivos de controle, usando o seguinte comando:

   SQL> SHOW PARAMETER CONTROL FILES;
3. Alterar o estado do banco de dados para não montado ou encerrado antes de restaurar os arquivos de controle.

   SQL> STARTUP NOMOUNT;

   SQL> SHUTDOWN IMMEDIATE;
4. Efetue logon no Console do Arcserve UDP.
5. Restaure o arquivo de controle usando o Assistente de restauração. Para obter mais informações sobre o processo de restauração, consulte Como restaurar de um ponto de recuperação.
6. Efetue logon no computador de destino.
7. Navegue até a pastas específicas e verifique se os arquivos de controle foram restaurados.
8. Monte o banco de dados para iniciar a recuperação do banco de dados:

   SQL> STARTUP MOUNT
9. Digite o comando RECOVER com a cláusula USING BACKUP CONTROLFILE.

   SQL> RECOVER DATABASE USING BACKUP CONTROLFILE

   O processo de recuperação do banco de dados é iniciado.
10. (Opcional) Especifique a cláusula UNTIL CANCEL para executar uma recuperação incompleta.

    SQL> RECOVER DATABASE USING BACKUP CONTROLFILE UNTIL CANCEL
11. Aplique os logs arquivados solicitados.

    Observação: se o log arquivado necessário estiver ausente, isso indica que um registro de repetição necessário está localizado nos logs de repetição online. Isso ocorre porque as alterações não arquivadas estão localizadas nos logs online quando a instância falha. É possível especificar o caminho completo de um arquivo

de log de repetição online e pressionar Enter (pode ser necessário executar isso algumas vezes até localizar o log correto).

12. Digite o seguinte comando para retornar as informações sobre o arquivo de controle sobre o log de repetição de um banco de dados:

    SQL>SELECT * FROM V$LOG;

13. (Opcional) Insira o comando a seguir para ver os nomes de todos os integrantes de um grupo:

    SQL>SELECT * FROM V$LOGFILE;

    Exemplo: após aplicar os logs arquivados solicitados, você poderá ver as seguintes mensagens:

    ORA-00279: alterar 55636 gerado em 24/06/2014 16:59:47 necessário para o segmento 1

    ORA-00289: sugestão 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

    Especificar log: {<RET>=suggested | filename | AUTO | CANCEL}

14. Especifique o caminho completo do arquivo de log de repetição online e pressione Enter.

    Exemplo: E:\app\Administrator\oradata\orcl\redo01.log

    Observação: é necessário especificar o caminho completo várias vezes até obter o log correto.

    As seguintes mensagens são exibidas:

    Log aplicado

    Completa recuperação de mídia

15. Abra o banco de dados com a cláusula RESETLOGS após concluir o processo de recuperação.

    SQL> ALTER DATABASE OPEN RESETLOGS;

    Os arquivos de controle perdidos foram recuperados.

Restaurar todo o banco de dados (espaços para tabelas e arquivos de controle)

É possível restaurar todo o banco de dados (todos os espaços para tabelas e arquivos de controle). Antes de restaurar, você deve localizar o arquivo. Quando você localizar os arquivos, verifique se o banco de dados está no estado Aberto. Se o banco de dados estiver aberto, use a ALTER TABLESPACE. OFFLINE instrui para tornar os espaços para tabelas ou arquivos de dados offline antes de iniciar o processo de restauração.

Siga estas etapas:

1. Efetue logon no computador no qual deseja restaurar os arquivos de dados ou espaços para tabelas.
2. Localize os espaços para tabelas de usuário ou arquivos de dados usando o seguinte comando:

   SQL> SELECT TABLESPACE_NAME, FILE_NAME from DBA_DATA_FILES;

   SQL> SHOW PARAMETER CONTROL FILES;
3. Altere o estado do banco de dados para não montar ou encerre antes de restaurar espaços para tabelas ou arquivos de dados.

   SQL> STARTUP NOMOUNT;

   SQL> SHUTDOWN IMMEDIATE;
4. Efetue logon no Console do Arcserve UDP.
5. Restaure os espaços para tabelas ou arquivos de dados usando o Assistente de restauração. Para obter mais informações sobre o processo de restauração, consulte Como restaurar de um ponto de recuperação.
6. Efetue logon no computador de destino.
7. Navegue até a pastas específicas e verifique se os espaços para tabelas ou arquivos de dados foram restaurados.
8. Recuperar o banco de dados do.

   SQL> RECOVER DATABASE USING BACKUP CONTROLFILE UNTIL CANCEL;
9. Aplique os logs arquivados solicitados.

   Observação: se o log arquivado necessário estiver ausente, isso indica que um registro de repetição necessário está localizado nos logs de repetição online. Isso ocorre porque as alterações não arquivadas estão localizadas nos logs online quando a instância falha. É possível especificar o caminho completo de um arquivo

de log de repetição online e pressionar Enter (pode ser necessário executar isso algumas vezes até localizar o log correto).

10. Digite o seguinte comando para retornar as informações sobre o arquivo de controle sobre o log de repetição de um banco de dados:

    SQL>SELECT * FROM V$LOG;

11. (Opcional) Insira o comando a seguir para ver os nomes de todos os integrantes de um grupo:

    SQL>SELECT * FROM V$LOGFILE;

    Exemplo: após aplicar os logs arquivados solicitados, você poderá ver as seguintes mensagens:

    ORA-00279: alterar 55636 gerado em 24/06/2014 16:59:47 necessário para o segmento 1

    ORA-00289: sugestão 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

    Especificar log: {<RET>=suggested | filename | AUTO | CANCEL}

12. Especifique o caminho completo do arquivo de log de repetição online e pressione Enter.

    Exemplo: E:\app\Administrator\oradata\orcl\redo01.log

    Observação: é necessário especificar o caminho completo várias vezes até obter o log correto.

    As seguintes mensagens são exibidas:

    Log aplicado

    Completa recuperação de mídia

13. Abra o banco de dados com a cláusula RESETLOGS após concluir o processo de recuperação.

    SQL> ALTER DATABASE OPEN RESETLOGS;

    Observação: para bancos de dados de vários locatários (CDB/PDB), também é necessário abrir todos os bancos de dados conectáveis.

    SQL> ALTER PLUGGABLE DATABASE <PDB_NAME> OPEN;

    Todo o banco de dados é restaurado.

14. Reinicie o servidor Oracle depois de executar as etapas 1 a 13 para os bancos de dados de vários locatários.

    Observação: essa etapa não é necessária para o servidor que esteja executando somente bancos de dados autônomos.

Recuperar o banco de dados Oracle usando recuperação bare metal

A recuperação bare metal permite recuperar e recriar todo o sistema de computador durante uma falha. Você pode restaurar o computador original ou outro computador.

Siga estas etapas:

1. Restaurar o computador usando um dos seguintes métodos:
   - Se os pontos de recuperação forem de um backup com base em agente, execute uma BMR para restaurar o computador.
   - Se os pontos de recuperação forem de um backup sem agente com base em host, use a opção Recuperar VM para restaurar o computador.
2. Efetue logon no computador restaurado.
3. Abra o prompt de comando e conecte-se à instância do Oracle (por exemplo, ORCL) como sysdba.
4. Verifique o status da instância do Oracle.

   SQL> SELECT STATUS FROM V$INSTANCE;
5. Execute uma das seguintes etapas de acordo com o status da instância do Oracle:
   - Se o status for Encerrar, inicie e abra a instância.

     SQL> STARTUP;

     SQL> ALTER DATABASE OPEN;
   - Se o status for Não montar, monte e abra a instância.

     SQL> ALTER DATABASE MOUNT;

     SQL> ALTER DATABASE OPEN;
   - Se o status for Montar, abra a instância do Oracle.

     SQL> ALTER DATABASE OPEN;
6. Recuperação por meio da execução do comando RECOVER se o banco de dados precisar de recuperação de mídia

   SQL> RECOVER DATABASE;
7. Abra a instância do Oracle após a recuperação de mídia ser concluída.

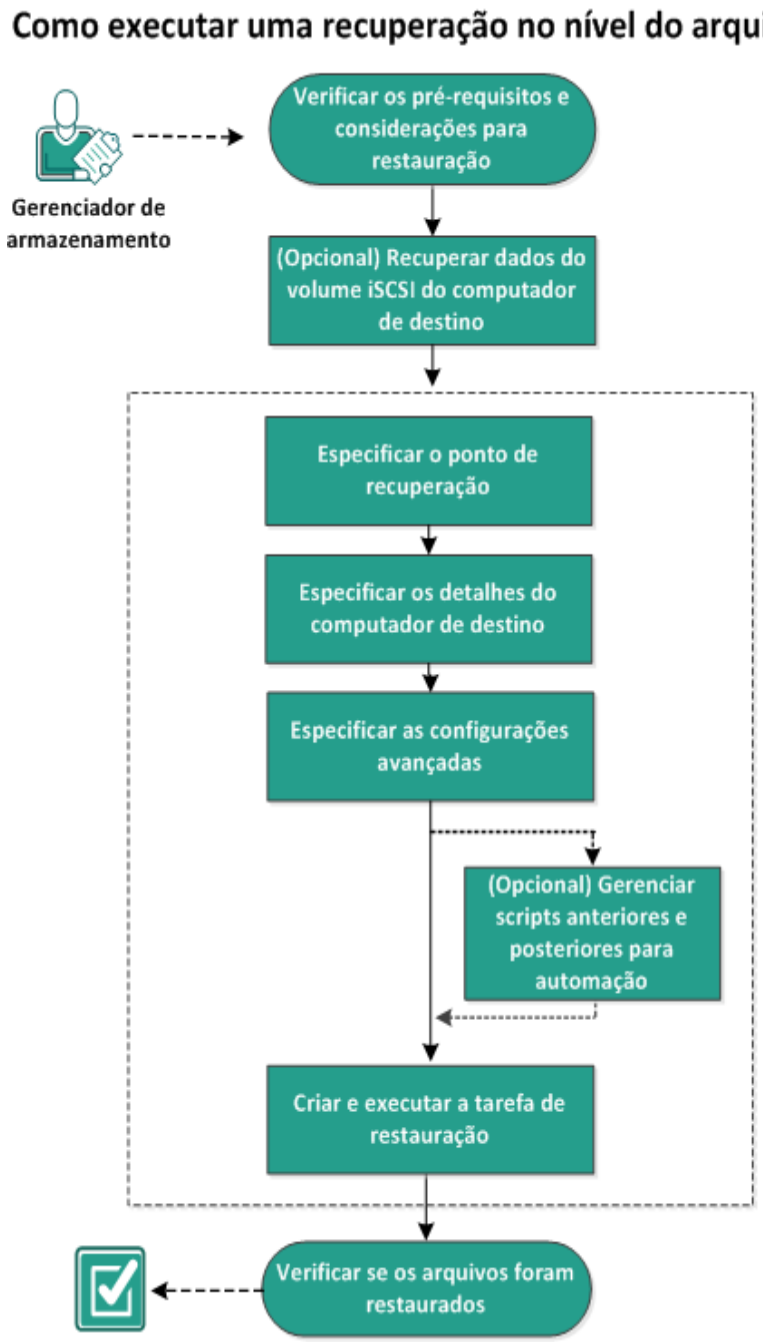
   SQL> ALTER DATABASE OPEN;

   O banco de dados Oracle foi recuperado usando a recuperação bare metal.

Como executar uma recuperação em nível de arquivo em nós Linux

Uma recuperação em nível de arquivo restaura os arquivos e as pastas individuais a partir de um ponto de recuperação. É possível restaurar um mínimo de um arquivo a partir do ponto de recuperação. Essa opção é útil se você deseja restaurar os arquivos selecionados e não todo o ponto de recuperação.

O diagrama a seguir exibe o processo para executar uma recuperação em nível de arquivo:



Execute essas tarefas para uma recuperação em nível de arquivo:

- Verificar os pré-requisitos da restauração
- (Opcional) Recuperar dados do volume iSCSI para o computador de destino
- Especificar o ponto de recuperação
- Especificar os detalhes do computador de destino
- Especificar as configurações avançadas
- (Opcional) Gerenciar scripts anteriores e posteriores para automação
- Criar e executar a tarefa de restauração
- Verificar se os arquivos foram restaurados

Verificar os pré-requisitos

Considere as seguintes opções antes de executar uma recuperação em nível de arquivo:

- Você tem um ponto de recuperação válido e a senha de criptografia, se houver.
- Você tem um nó de destino válido para recuperar os dados.
- Você verificou se o servidor de backup do Linux oferece suporte ao sistema de arquivos que deseja restaurar.

  Por exemplo, o RedHat 7.x não oferece suporte para o sistema de arquivos *reiserfs*. Se o sistema operacional do servidor de backup for RedHat 7.x e você desejar restaurar o sistema de arquivos reiserfs, instale o driver do sistema de arquivos para oferecer suporte ao reiserfs. Também é possível usar o Live CD do Agente do Arcserve Unified Data Protection para Linux para executar a restauração em nível de arquivo já que o Live CD oferece suporte a todos os tipos de sistema de arquivos.
- Você instalou os seguintes pacotes de software no servidor de backup Linux:
  - mdadm
  - kpartx
  - lvm2
  - Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

(Opcional) Recuperar dados do volume iSCSI para o computador de destino

Se você tiver armazenado os dados em um volume de destino iSCSI, é possível conectar o volume iSCSI e recuperar os dados. O volume iSCSI permite gerenciar dados e transferi-los por uma rede.

Verifique se você tem a release mais recente do software iniciador iSCSI instalada no servidor de backup. O software iniciador em sistemas RHEL é empacotado como iscsi-initiator-utils. O iniciador de software em sistemas SLES é empacotado como open-iscsi.

Siga estas etapas:

1. Efetue logon no ambiente do servidor de backup.
2. Execute um dos comandos a seguir para iniciar o daemon do iniciador iSCSI.
   - Para sistemas RHEL:

     /etc/init.d/iscsid start

     O serviço em sistemas RHEL é denominado iscsid.
   - Para sistemas SLES:

     /etc/init.d/open-iscsi start

     O serviço em sistemas SLES é denominado open-iscsi.
3. Execute um script de detecção para detectar o host de destino iSCSI.

   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>

   O valor da porta padrão do host de destino iSCSI é 3260.
4. Anote o IQN (iSCSI Qualified Name – Nome Qualificado iSCSI) do host de destino iSCSI encontrado pelo script de detecção antes de efetuar logon manualmente no destino detectado.
5. Liste o dispositivo de bloqueio disponível do servidor de backup.

   #fdisk -l
6. Efetue logon no destino detectado.

   iscsiadm -m node -T <iSCSI Target IQN name> -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number> -l

   É possível ver um dispositivo de bloqueio no diretório /dev do servidor de backup.
7. Execute o comando a seguir para obter o novo nome do dispositivo:

#fdisk -l

É possível ver um dispositivo adicional nomeado /dev/sd<x> no nó servidor de backup.

Por exemplo, considere que o nome do dispositivo é /dev/sdc. Esse nome de dispositivo é usado para criar uma partição e um sistema de arquivos nas etapas a seguir.

8. Monte o volume iSCSI usando os seguintes comandos:

   # mkdir /iscsi

   # mount /dev/sdc1 /iscsi

   Observação: ao especificar o local da sessão no Assistente de restauração, é necessário selecionar Local e digitar o caminho /iscsi.

   Exemplo: <caminho>/iscsi

9. (Opcional) Adicione o seguinte registro ao arquivo /etc/fstab de maneira que o volume iSCSI se conecte automaticamente ao servidor de backup após reiniciar o servidor.

   /dev/sdc1 /iscsi ext3 _netdev 0 0

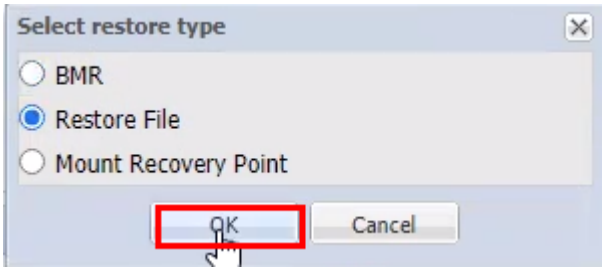
   O servidor de backup agora pode se conectar ao volume iSCSI e pode recuperar os dados do volume iSCSI.

Especifique o ponto de recuperação para o backup com base em agente

Cada vez que você executa um backup, um ponto de recuperação é criado. Especifique as informações do ponto de recuperação no Assistente de restauração de forma que seja possível recuperar exatamente os dados desejados. É possível restaurar arquivos específicos ou todos os arquivos de acordo com as suas necessidades.

Siga estas etapas:

1. Acesse o Assistente de restauração com um dos seguintes procedimentos:
   - **A partir do Arcserve UDP :**
     a. Efetue logon no Arcserve UDP.
     b. Navegue até **recursos** > **Nó** > **Todos os nós**.
        Todos os nós adicionados são exibidos no painel central.
     c. Clique com o botão direito do mouse no nó e clique em **Restaurar**.
        A interface da web do agente do Arcserve UDP (Linux) é aberta e exibe a caixa de diálogo Selecionar tipo de restauração.
     d. Na caixa de diálogo Selecionar tipo de restauração, clique na opção **Restaurar arquivo** e, em seguida, clique em **OK**.



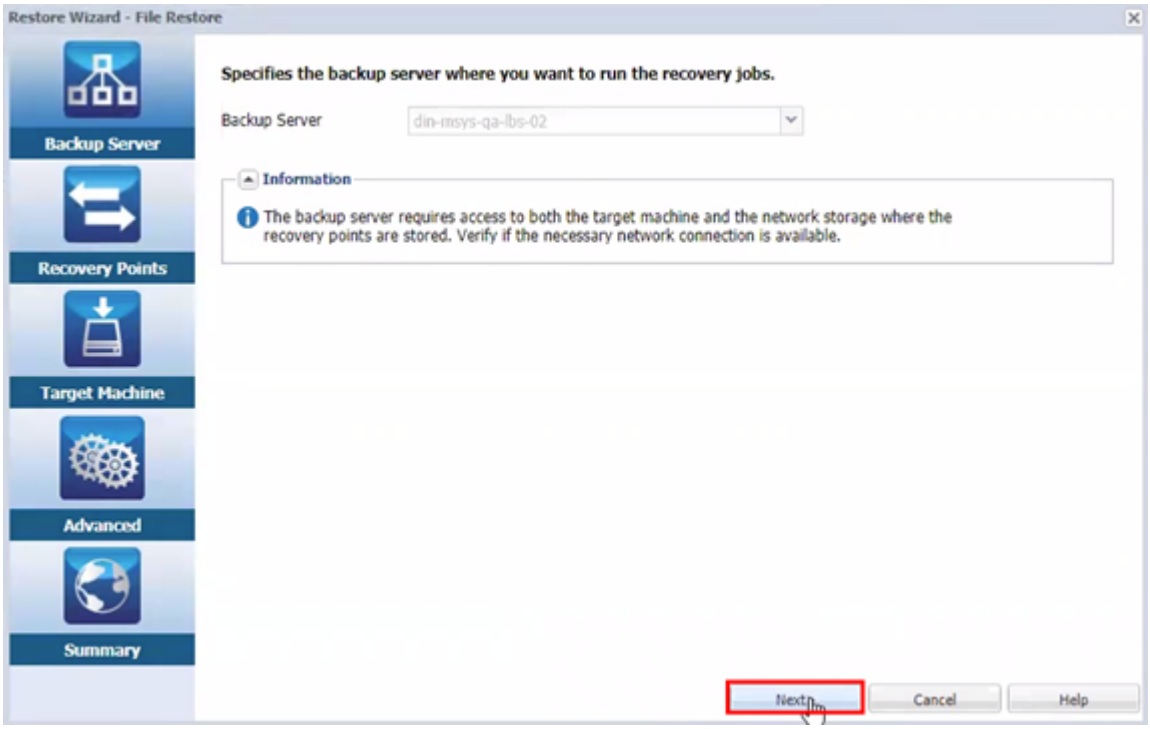
        Observação: você será automaticamente conectado ao nó do agente e o Assistente de restauração será exibido a partir do nó do agente.
   - **A partir do Agente do Arcserve Unified Data Protection para Linux :**
     a. Abra a interface da web do Agente do Arcserve Unified Data Protection para Linux.

Observação: durante a instalação do Agente do Arcserve Unified Data Protection para Linux, você recebeu o URL para acessar e gerenciar o servidor. Efetue logon no Agente do Arcserve Unified Data Protection para Linux.

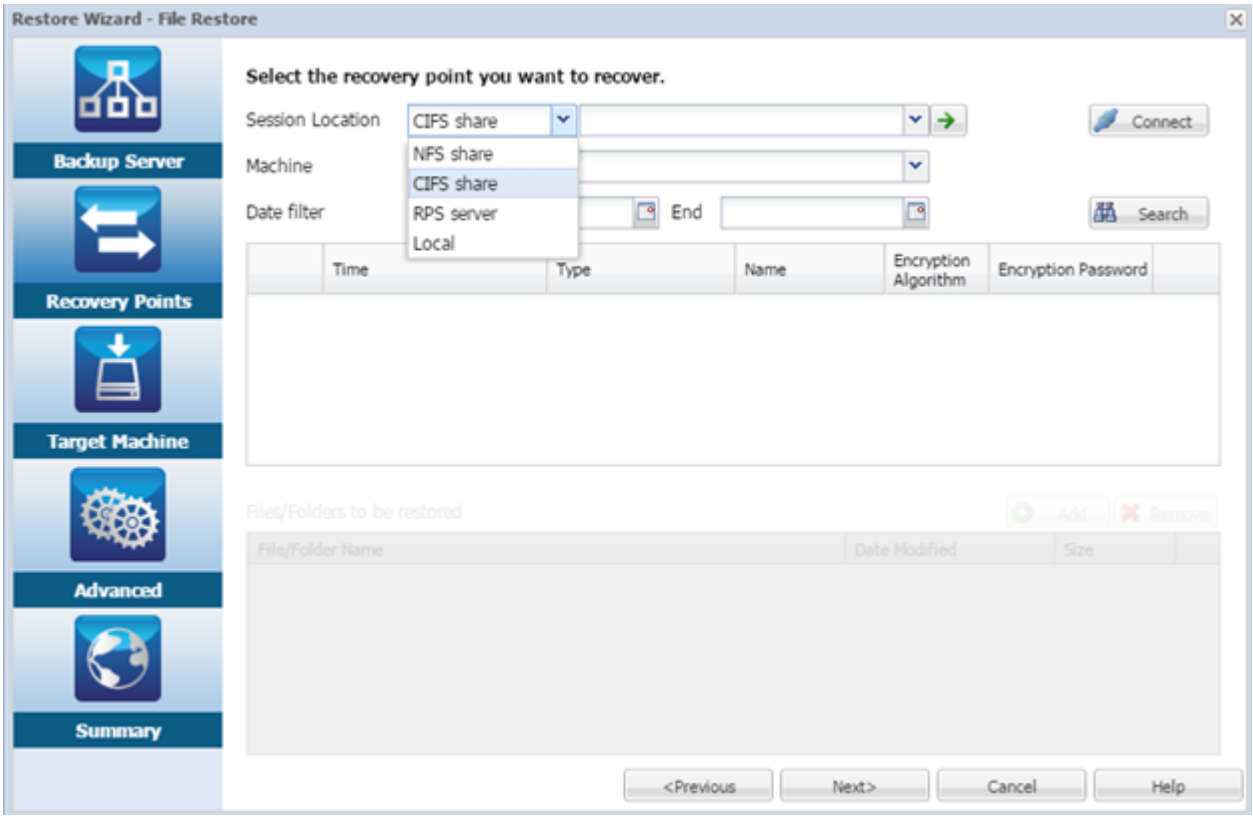
b. No menu Assistente, clique em **Restaurar** e selecione **Restaurar arquivo**.

A caixa de diálogo Assistente de restauração - restauração de arquivo é aberta.

2. Na página Servidor de backup do Assistente de restauração, é possível ver o servidor de backup. Não é possível selecionar nenhuma opção na lista suspensa Servidor de backup. Clique em **Avançar**.



3. Na página Pontos de recuperação do Assistente de restauração, faça o seguinte:



Importante: Se você abrir o Assistente a partir do Console, as informações sobre a máquina e o local da sessão são exibidas automaticamente. Pule para a Etapa 4.

a. Selecione o **compartilhamento CIFS/compartilhamento NFS/servidor RPS/Local** na lista suspensa Local da sessão.

b. Execute uma das seguintes etapas, dependendo do local da sessão:

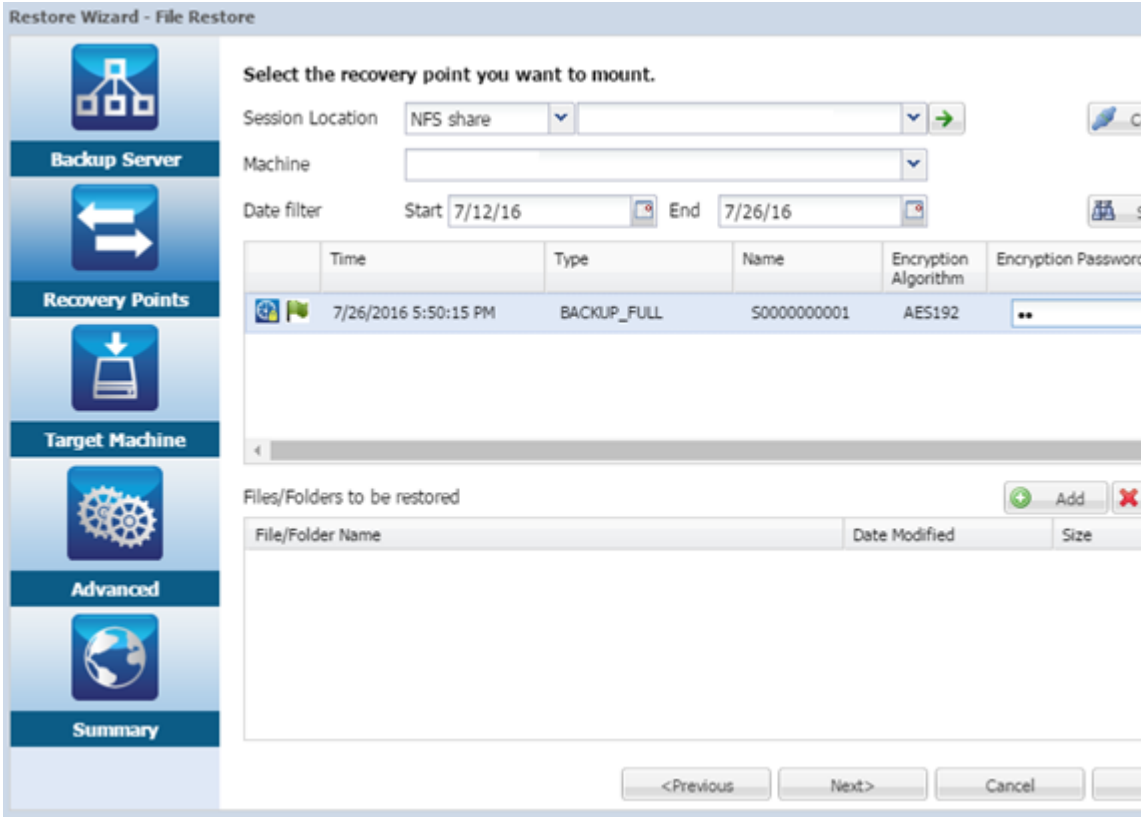
Para compartilhamento de CIFS/compartilhamento de NFS/Local

Especifique o caminho completo do compartilhamento CIFS/-compartilhamento NFS/Local e clique em **Conectar**.

Todas as máquinas são listadas na lista suspensa Computador.

Observação: se você selecionar a opção **Compartilhamento**

CIFS, especifique o nome de usuário e a senha.



Para o servidor RPS

a. Selecione o servidor RPS e clique em **Adicionar**.

   A caixa de diálogo Informações do servidor de ponto de recuperação abre.

b. Forneça os detalhes do RPS e clique em **Sim**.

c. Selecione o repositório de dados na lista suspensa.

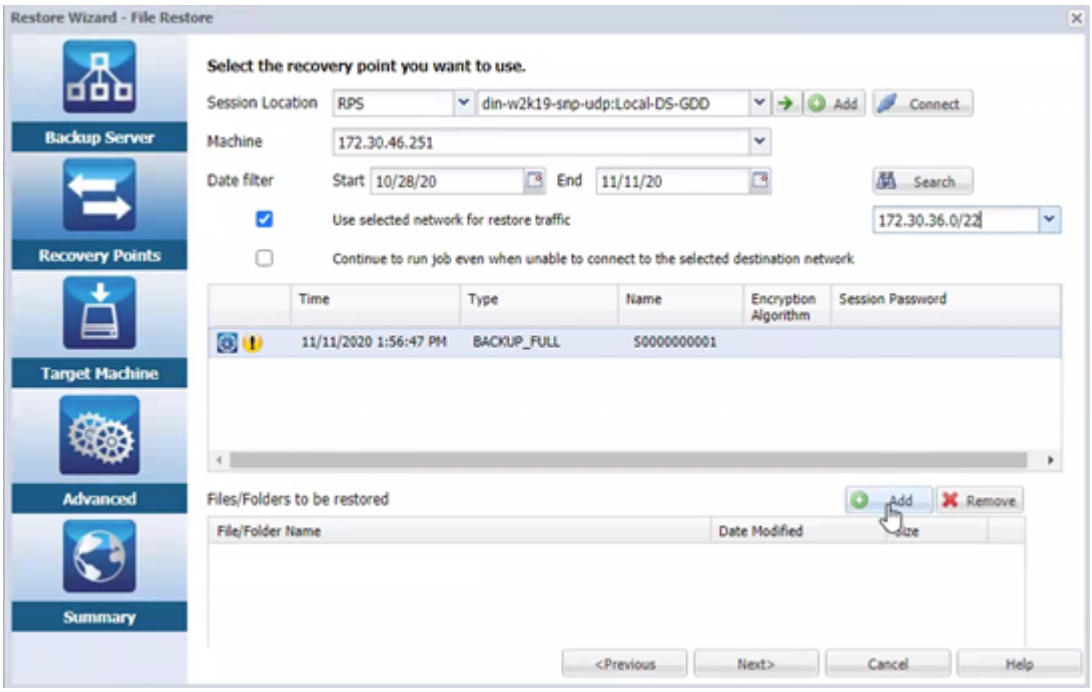
   A caixa de diálogo Informações do servidor de ponto de recuperação fecha e você vê o assistente.

d. Clique em **Conectar**.

   Todos os nós que foram copiados para backup nesse local são listados na lista suspensa Computador.

e. Na lista suspensa Computador, selecione o nó que deseja restaurar.

Todos os pontos de recuperação do nó selecionado são listados.



4. Aplique o filtro de datas para exibir os pontos de recuperação que são gerados entre a data especificada e clique em **Pesquisar**.

   Padrão: últimas duas semanas.

   Todos os pontos de recuperação disponíveis entre as datas especificadas serão exibidos.

5. Para ativar a comunicação entre o agente Linux e o servidor de ponto de recuperação, marque a caixa de seleção **Usar a rede selecionada para restaurar o tráfego** e, em seguida, selecione a rede na lista suspensa.

   Observação: se a rede de backup selecionada não estiver acessível e para continuar a tarefa de backup com a rede disponível ou com a rede padrão, clique na caixa de seleção **Continuar a executar a tarefa mesmo quando não for possível se conectar à rede de backup selecionada**.

6. Selecione o ponto de recuperação que deseja restaurar. Se o ponto de recuperação estiver criptografado, insira a senha de criptografia para restaurar os dados.

7. Para que os arquivos/pastas sejam restaurados, clique em **Adicionar**.

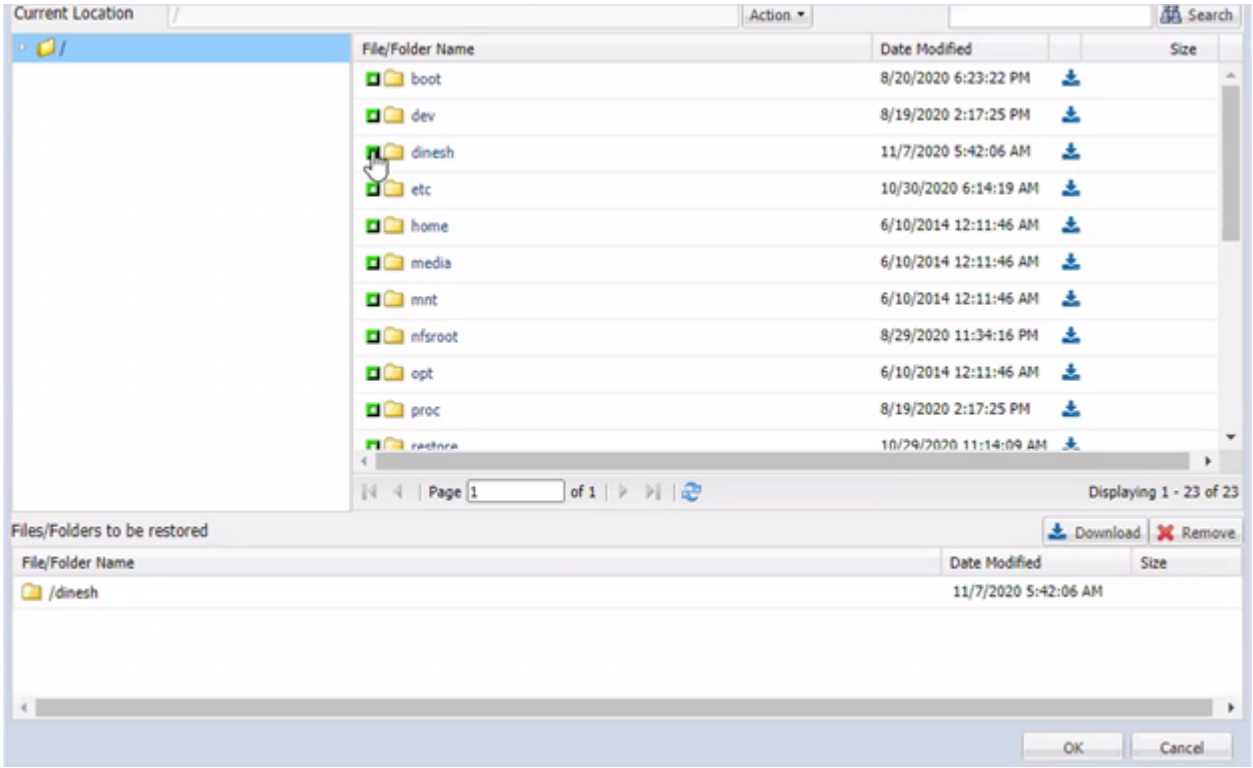
   A caixa de diálogo Procurar-<nome do nó> é aberta.

   Importante: caso você encontre a mensagem de aviso, "os arquivos/pastas são exibidos no arquivo do dispositivo. Clique em Ajuda para obter mais infor-

mações." No console, consulte a seguinte observação para obter uma resolução.

Observação: para alguns layouts de disco complexos, o sistema de arquivos é exibido pelo arquivo do dispositivo. A alteração no comportamento de exibição do sistema de arquivos não afeta a função de restauração de nível de arquivo da VM Linux com base em host. É possível procurar o sistema de arquivos sob o arquivo do dispositivo. Além disso, é possível usar a função de pesquisa para procurar um arquivo ou diretório específico.

8. Na caixa de diálogo Procurar-<nome do nó>, selecione o arquivo ou a pasta que deseja restaurar e clique em **OK**.



Observação: se você tentar localizar um arquivo ou pasta usando o campo **Pesquisar**, certifique-se de que tenha selecionado a pasta de nível mais alto na hierarquia. A pesquisa é conduzida em todas as pastas filhas da pasta selecionada.

A caixa de diálogo Procurar-<nome de nó> é fechada e você retorna à página Pontos de recuperação. Os arquivos e pastas selecionados são listados em Arquivos/pastas para restauração.

9. Clique em **Avançar**.

   A página Computador de destino é exibida.

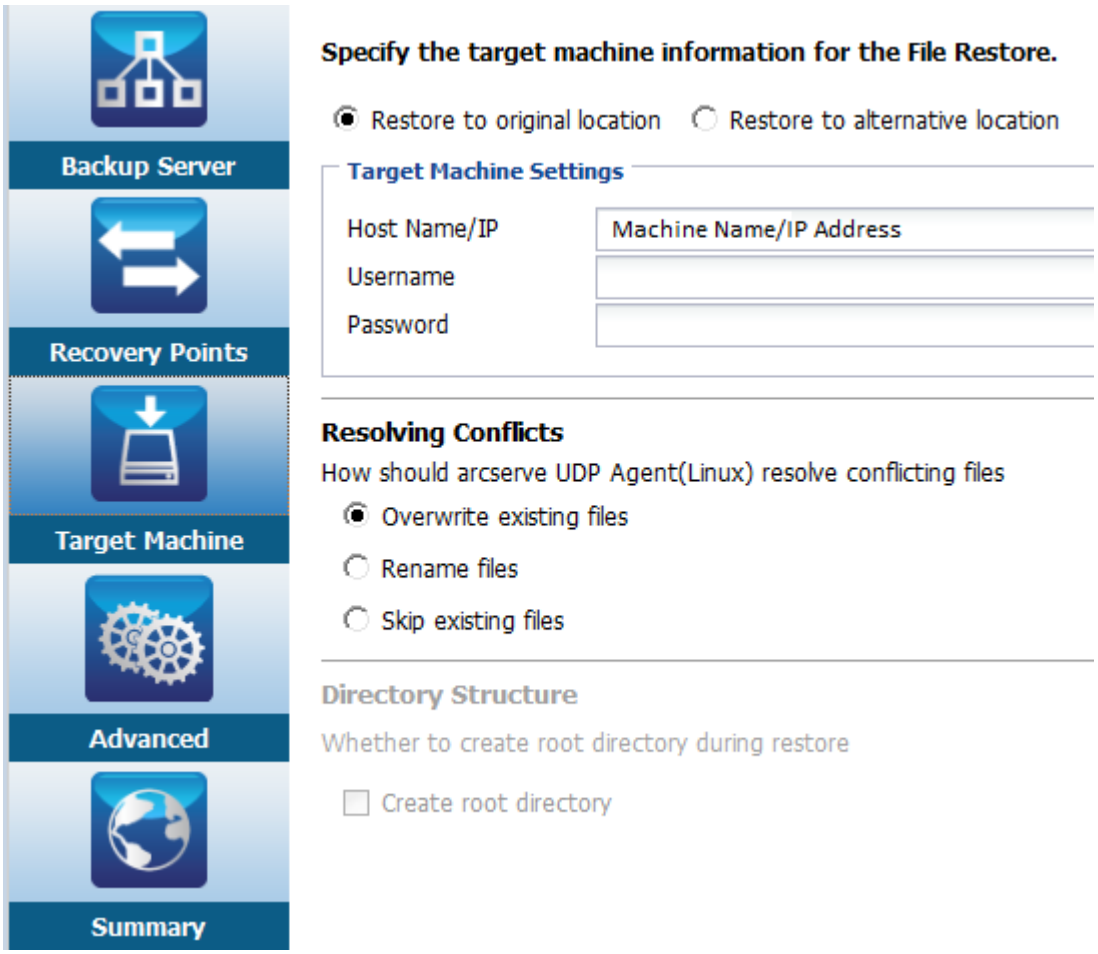
O ponto de recuperação é especificado.

Especificar os detalhes da máquina de destino

Especifique os detalhes do nó de destino, de modo que os dados sejam restaurados para esse nó. É possível restaurar os arquivos ou pastas selecionados no nó de origem ou para um novo nó.

Para fazer a restauração para o nó a partir do qual o backup dos dados foi realizado, siga estas etapas:

1. Na página Computador de destino, selecione **Restaurar ao local original**.



2. Digite o nome de usuário e a senha do nó.
3. Selecione uma das seguintes opções para resolver arquivos conflitantes:

   Substituir arquivos existentes

   Especifica que, se o arquivo existe no computador de destino, o arquivo de backup do ponto de recuperação substituirá o arquivo existente.

   Renomear arquivos

Especifica que, se o arquivo existir no computador de destino, será criado um novo arquivo com o mesmo nome de arquivo e extensão de arquivo *.d2dduplicate<x>*. <x> especifica o número de vezes que o arquivo é restaurado. Todos os dados serão restaurados para o novo arquivo.

Ignorar arquivos existentes

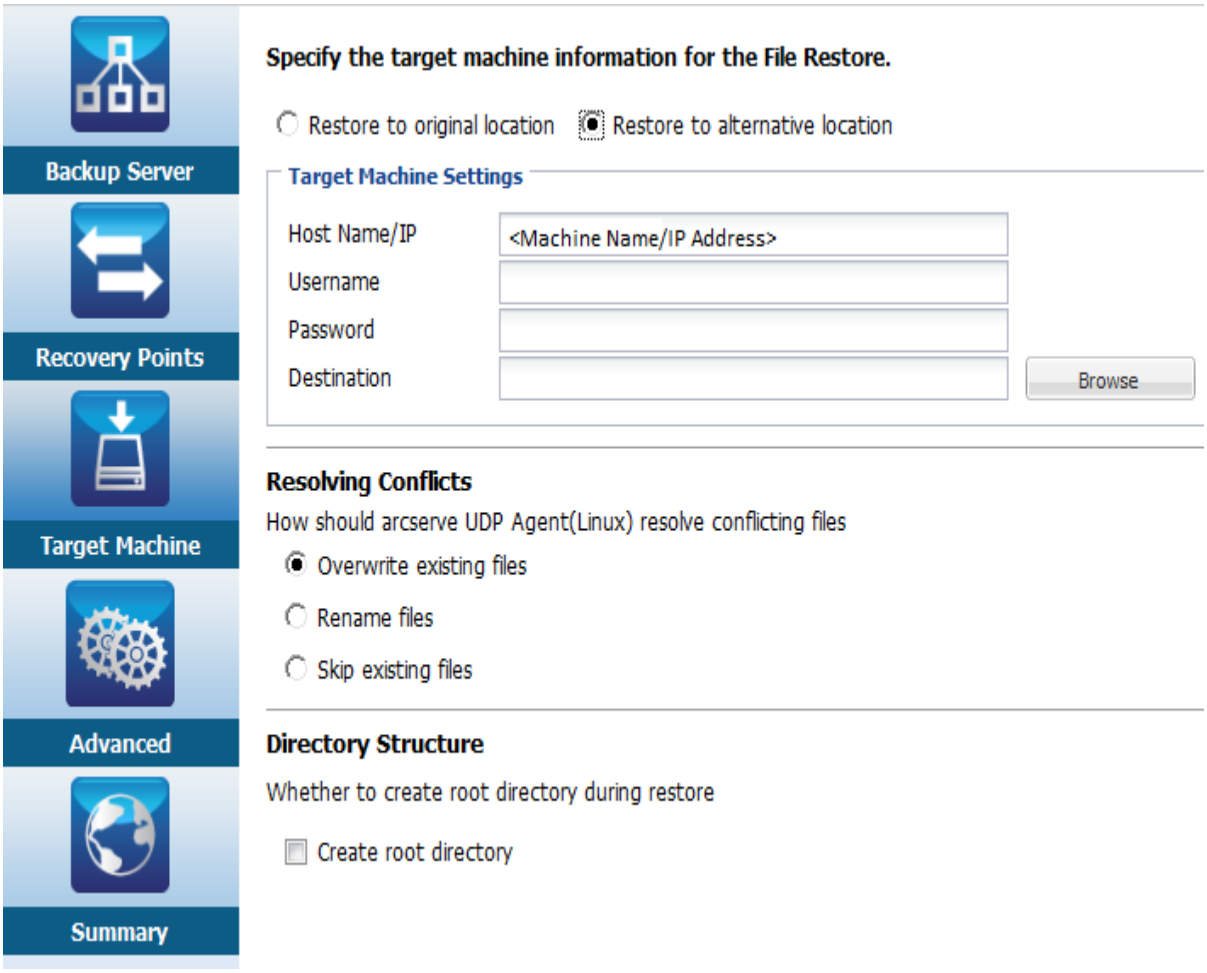
Especifica que, se o mesmo arquivo existe no computador de destino, esses arquivos não serão restaurados a partir do ponto de recuperação.

4. (Opcional) Selecione **Criar diretório raiz**.
5. Clique em **Avançar**.

   A página Avançado é exibida.

Para restaurar em um novo nó, siga estas etapas:

1. Na página Computador de destino, selecione **Restaurar em um local alternativo**.



2. Digite o nome do host ou o endereço IP do nó de destino.

3. Digite o nome de usuário e a senha do nó.
4. Digite o caminho onde os dados são restaurados ou clique em **Procurar** para selecionar a pasta na qual os dados serão restaurados e clique em **OK**.
5. Selecione uma das seguintes opções para resolver arquivos conflitantes:

   Substituir arquivos existentes

   Especifica que, se o arquivo existe no computador de destino, o arquivo de backup do ponto de recuperação substituirá o arquivo existente.

   Renomear arquivos

   Especifica que, se o arquivo existir no computador de destino, será criado um novo arquivo com o mesmo nome de arquivo e extensão de arquivo *.d2dduplicate<x>*. <x> especifica o número de vezes que o arquivo é restaurado. Todos os dados serão restaurados para o novo arquivo.

   Ignorar arquivos existentes

   Especifica que, se o mesmo arquivo existe no computador de destino, esses arquivos não serão restaurados a partir do ponto de recuperação.
6. (Opcional) Selecione **Criar diretório raiz**.
7. Clique em **Avançar**.

   A página Avançado é exibida.

Os detalhes do computador de destino são especificados.

Especificar as configurações avançadas

Especifique as configurações avançadas para executar uma recuperação programada de seus dados. A recuperação programada assegura que os dados sejam recuperados no horário especificado, mesmo em sua ausência.

Siga estas etapas:

1. Defina a hora e data de início, selecionando uma das seguintes opções:

   Executar agora

   Inicia a tarefa de restauração em nível de arquivo assim que você enviar a tarefa.

   Definir data e hora de início

   Inicia a tarefa de restauração em nível de arquivo na data e hora especificadas, após enviar a tarefa.

2. (Opcional) Selecione **Estimativa de tamanho do arquivo**.
3. (Opcional) Selecione um script a partir da opção **Configurações de scripts anteriores e posteriores**.

   Esses scripts executam os comandos de script para as ações a serem realizadas antes do início da tarefa e/ou após a conclusão da tarefa.

   Observação: os campos **Configurações de scripts anteriores e posteriores** serão preenchidos apenas se já tiver criado um arquivo de script e o tiver colocado no seguinte local:

   /opt/Arcserve/d2dserver/usr/prepost

   Observação: para obter mais informações sobre como criar scripts anteriores e posteriores, consulte o tópico *Gerenciar scripts anteriores e posteriores para automação*.

4. Clique em **Avançar**.

   A página **Resumo** é exibida.

   As configurações avançadas são especificadas.

(Opcional) Gerenciar scripts anteriores e posteriores para automação

Os scripts anteriores e posteriores permitem executar sua própria lógica de negócios em estágios específicos de uma tarefa em execução. É possível especificar quando executar os scripts em **Configurações de scripts anteriores e posteriores** do **Assistente de backup** e do **Assistente de restauração** na interface do usuário. Dependendo da sua programação, é possível executar os scripts no servidor de backup.

O gerenciamento dos scripts anteriores e posteriores é um processo em duas etapas, que consiste em criar os scripts anteriores e posteriores e em colocar o script na pasta prepost.

Criar scripts anteriores e posteriores

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Crie um arquivo de script usando as variáveis de ambiente em sua linguagem de scripts de preferência.

   Variáveis de ambiente de script anterior e posterior

   Para criar seu script, use as seguintes variáveis de ambiente:

   D2D_JOBNAME

   Identifica o nome da tarefa.

   D2D_JOBID

   Identifica a ID da tarefa. A ID da tarefa é um número fornecido para a tarefa durante a execução da tarefa. Se você executar novamente a mesma tarefa, receberá um novo número de tarefa.

   D2D_TARGETNODE

   Identifica o nó cujo backup está sendo feito ou restaurado.

   D2D_JOBTYPE

   Identifica o tipo da tarefa em execução. Os valores a seguir identificam a variável D2D_JOBTYPE:

   backup.full

   Identifica a tarefa como um backup completo.

   backup.incremental

Identifica a tarefa como um backup incremental.

backup.verify

Identifica a tarefa como um backup de verificação.

restore.bmr

Identifica a tarefa como uma BMR (Bare-Metal Recovery – Recuperação Bare Metal). Esta é uma tarefa de restauração.

restore.file

Identifica a tarefa como uma restauração em nível de arquivo. Esta é uma tarefa de restauração.

D2D_SESSIONLOCATION

Identifica o local onde os pontos de recuperação estão armazenados.

D2D_PREPOST_OUTPUT

Identifica um arquivo temporário. O conteúdo da primeira linha do arquivo temporário é exibido no log de atividades.

D2D_JOBSTAGE

Identifica o estágio da tarefa. Os valores a seguir identificam a variável D2D_JOBSTAGE:

pre-job-server

Identifica o script que é executado no servidor de backup antes do início da tarefa.

post-job-server

Identifica o script que é executado no servidor de backup após a conclusão da tarefa.

pre-job-target

Identifica o script que é executado no computador de destino antes do início da tarefa.

post-job-target

Identifica o script que é executado no computador de destino após a conclusão da tarefa.

pre-snapshot

Identifica o script que é executado no computador de destino antes de capturar o instantâneo.

post-snapshot

Identifica o script que é executado no computador de destino depois de capturar o instantâneo.

D2D_TARGETVOLUME

Identifica o volume cujo backup foi feito durante uma tarefa de backup. Essa variável é aplicável a scripts de instantâneo anteriores e posteriores para uma tarefa de backup.

D2D_JOBRESULT

Identifica o resultado de um script de tarefa posterior. Os valores a seguir identificam a variável D2D_JOBRESULT:

success

Identifica o resultado realizado com êxito.

fail

Identifica o resultado realizado sem êxito.

D2DSVR_HOME

Identifica a pasta onde o servidor de backup está instalado. Essa variável é aplicável a scripts que são executados no servidor de backup.

O script é criado.

Observação: para todos os scripts, um valor de retorno zero indica êxito e um valor de retorno diferente de zero indica falha.

Colocar o script na pasta Prepost e verificar

Todos os scripts anteriores e posteriores de um servidor de backup são gerenciados na pasta prepost no seguinte local:

/opt/Arcserve/d2dserver/usr/prepost

Siga estas etapas:

1. Coloque o arquivo no seguinte local do servidor de backup:

   /opt/Arcserve/d2dserver/usr/prepost
2. Forneça a permissão de execução para o arquivo de script.
3. Efetue logon na interface da web do Agente do Arcserve Unified Data Protection para Linux.
4. Abra o **Assistente de backup** ou o **Assistente de restauração** e navegue até à guia **Avançado**.
5. Selecione o arquivo de script na lista suspensa **Configurações de scripts anteriores/posteriores** e, em seguida, envie a tarefa.

6. Clique em **Log de atividades** e verifique se o script é executado para a tarefa de backup especificada.

   O script é executado.

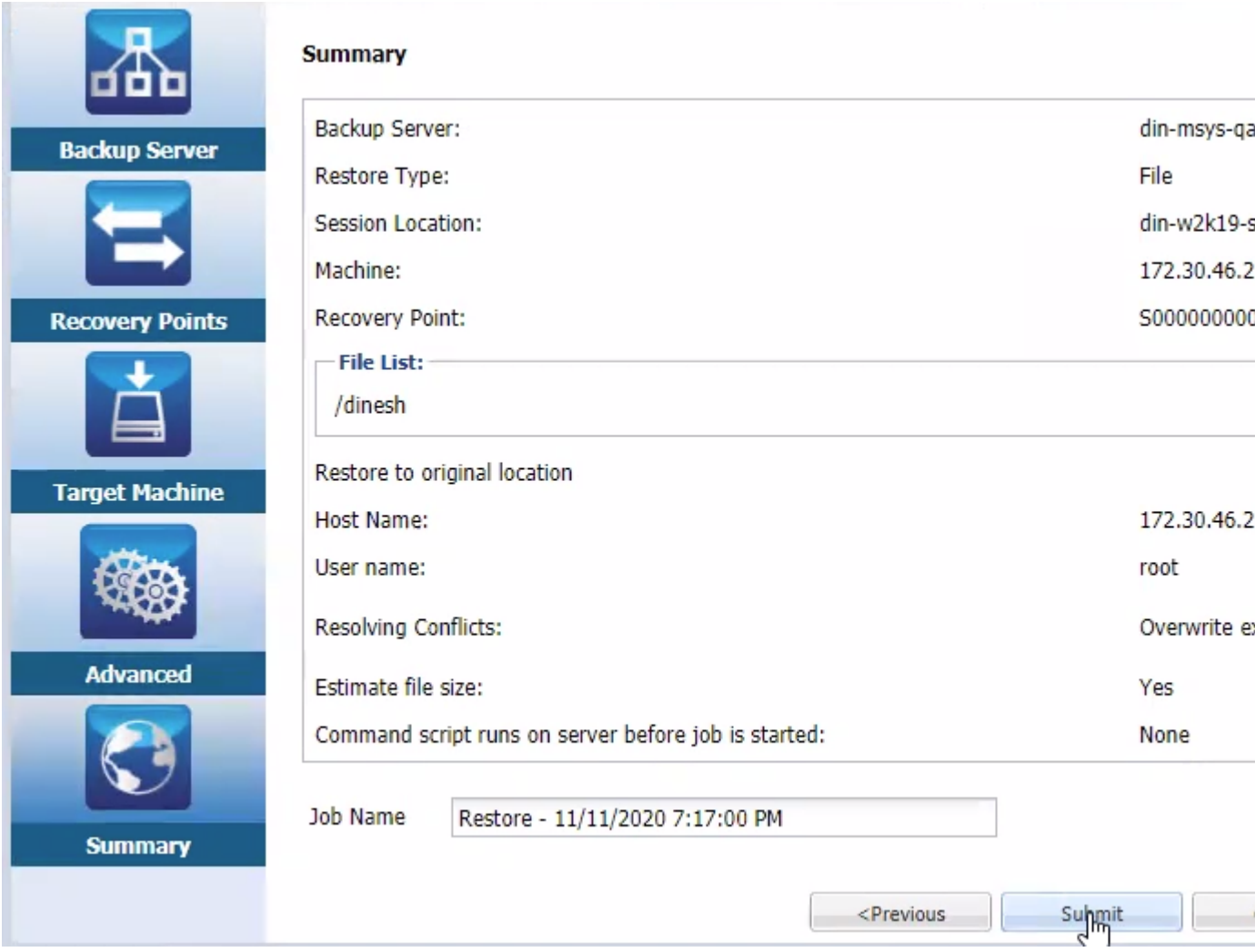
   Os scripts anteriores e posteriores são criados com êxito e colocados na pasta pre-post.

Criar e executar a tarefa de restauração

Crie e execute a tarefa de restauração, para poder iniciar a recuperação de nível de arquivo. Verifique as informações do ponto de recuperação antes de restaurar os arquivos. Se necessário, volte e altere as configurações de restauração no assistente.

Siga estas etapas:

1. Na página Resumo do Assistente de restauração, verifique os detalhes da restauração.



2. Siga um destes procedimentos:
   - Se as informações do resumo não estiverem corretas, clique em **Anterior** e volte à caixa de diálogo em questão para alterar a configuração incorreta.
   - Se as informações de resumo estiverem corretas, digite um nome de tarefa e clique em **Enviar** para iniciar o processo de restauração.

Observação: o campo Nome da tarefa tem um nome padrão inicialmente. É possível digitar um novo nome de tarefa de sua escolha, mas não é possível deixar esse campo em branco.

O Assistente de restauração é fechado. É possível ver o status da tarefa na página Status da tarefa.

A tarefa de restauração é criada e executada com êxito.

Verificar se os arquivos foram restaurados

Após a conclusão da tarefa de restauração, certifique-se de que todos os arquivos estejam restaurados no nó de destino. Verifique as guias **Histórico da tarefa** e **Log de atividades** no painel **Status** para monitorar o andamento do processo de restauração.

Siga estas etapas:

1. Navegue para o computador de destino em que você restaurou os dados.
2. Verifique se os dados necessários do ponto de recuperação foram restaurados.

   Os arquivos são verificados com êxito.

   A recuperação em nível de arquivo é executada com êxito.

Como executar uma recuperação em nível de arquivo de backup sem agente com base em host para nós do Linux

Uma recuperação em nível de arquivo restaura os arquivos e as pastas individuais a partir de um ponto de recuperação. É possível restaurar um mínimo de um arquivo a partir do ponto de recuperação. Essa opção é útil se você deseja restaurar os arquivos selecionados e não todo o ponto de recuperação.

Execute essas tarefas para uma recuperação em nível de arquivo:

- Verificar os pré-requisitos da restauração
- Especificar o ponto de recuperação
- Especificar os detalhes do computador de destino
- Especificar as configurações avançadas
- (Opcional) Gerenciar scripts anteriores e posteriores para automação
- Criar e executar a tarefa de restauração
- Verificar se os arquivos foram restaurados

Verificar os pré-requisitos

Considere as seguintes opções antes de executar uma recuperação em nível de arquivo:

- Você tem um ponto de recuperação válido e a senha de criptografia, se houver.
- Você tem um nó de destino válido para recuperar os dados.
- Você verificou se o servidor de backup do Linux oferece suporte ao sistema de arquivos que deseja restaurar.

  Por exemplo, o RedHat 7.x não oferece suporte para o sistema de arquivos *reiserfs*. Se o sistema operacional do servidor de backup for RedHat 7.x e você desejar restaurar o sistema de arquivos reiserfs, instale o driver do sistema de arquivos para oferecer suporte ao reiserfs. Também é possível usar o Live CD do Agente do Arcserve Unified Data Protection para Linux para executar a restauração em nível de arquivo já que o Live CD oferece suporte a todos os tipos de sistema de arquivos.
- Você instalou os seguintes pacotes de software no servidor de backup Linux:
  - mdadm
  - kpartx
  - lvm2
  - Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Especificar o ponto de recuperação

Cada vez que você executar um backup com êxito, um ponto de recuperação é criado. Especifique as informações do ponto de recuperação no **Assistente de restauração** de forma que seja possível recuperar exatamente os dados desejados. É possível restaurar arquivos específicos ou todos os arquivos de acordo com as suas necessidades.

Siga estas etapas:

1. Acesse o assistente de restauração com um dos seguintes procedimentos:

   A partir do Arcserve UDP :

   a. Efetue logon no Arcserve UDP.

   b. Clique na guia **Recursos**.

   c. Selecione **Todos os nós** no painel esquerdo.

      Todos os nós do adicionados são exibidos no painel central.

   d. No painel central, selecione o nó do e clique em **Ações**.

   e. Clique em **Restaurar** no menu suspenso **Ações**.

      A interface da web do Agente do Arcserve Unified Data Protection para Linux é exibida. A caixa de diálogo Selecionar tipo de restauração é exibida na interface de usuário do agente.

   f. Selecione o tipo de restauração e clique em **OK**.

      Observação: você será automaticamente conectado ao nó do agente e o **Assistente de restauração** será exibido do nó do agente.

   A partir do Agente do Arcserve Unified Data Protection para Linux :

   a. Abra a interface da web do Agente do Arcserve Unified Data Protection para Linux.

      Observação: durante a instalação do Agente do Arcserve Unified Data Protection para Linux, você recebeu o URL para acessar e gerenciar o servidor. Efetue logon no Agente do Arcserve Unified Data Protection para Linux.

   b. Clique em **Restaurar** no menu **Assistente** e selecione **Restaurar arquivo**.

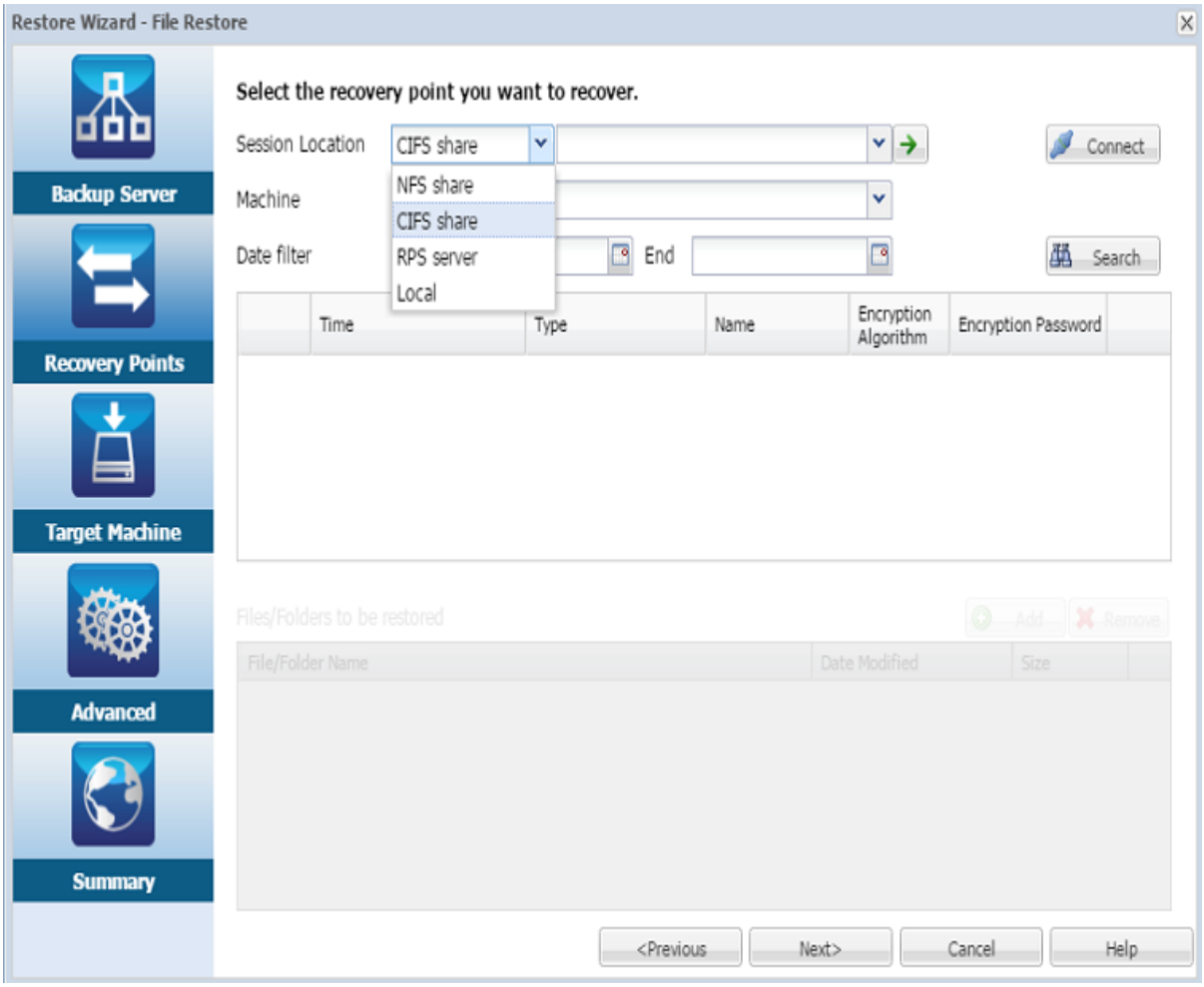
      O **Assistente de restauração - restauração de arquivo** é exibido.

      É possível ver o servidor de backup na página **Servidor de backup** do **Assistente de restauração**. Não é possível selecionar nenhuma opção na lista suspensa **Servidor de backup**.

2. Clique em **Avançar**.

   A página **Pontos de recuperação** do **Assistente de restauração** é exibida.

   Importante: Se você abrir o Assistente a partir do Console, as informações sobre a máquina e o local da sessão são exibidas automaticamente. Pule para a Etapa 5.



3. Selecione um **Compartilhamento CIFS** ou um **Servidor RPS** na lista suspensa **Local da sessão**.

   Observação: é possível selecionar Local ou compartilhamento de NFS para a restauração de sessões de backup sem agente com base em host.

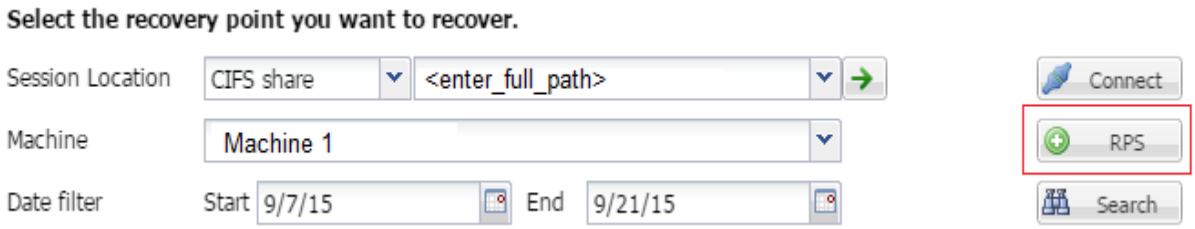
4. Siga uma das seguintes etapas, dependendo do local da sessão:

   Para o compartilhamento CIFS

   a. Especifique o caminho completo do compartilhamento CIFS e clique em **Conectar**.

   b. Especifique o nome de usuário e a senha para se conectar ao compartilhamento CIFS e clique em **OK**.

Todos os computadores são listados na lista suspensa Computador e um botão RPS aparece ao lado de Computador.



c. Selecione o computador na lista suspensa e clique em RPS.

A caixa de diálogo Informações do **servidor de ponto de recuperação** abre.

d. Forneça os detalhes do RPS e clique em Sim.

A caixa de diálogo **Informações do servidor de ponto de recuperação** fecha. Todos os pontos de recuperação do computador selecionado são exibidos abaixo da opção **Filtro de data**.

Para o servidor RPS

a. Selecione o servidor RPS e clique em Adicionar.

A caixa de diálogo Informações do **servidor de ponto de recuperação** abre.

b. Forneça os detalhes do RPS e clique em Carregar

c. Selecione o repositório de dados na lista suspensa e clique em **Sim**.

A caixa de diálogo **Informações do servidor de ponto de recuperação** fecha e você vê o assistente.

d. Clique em **Conectar**.

Todas as máquinas são listadas na lista suspensa Computador.

e. Selecione o computador na lista suspensa.

Todos os pontos de recuperação do computador selecionado são exibidos abaixo da opção **Filtro de data**.

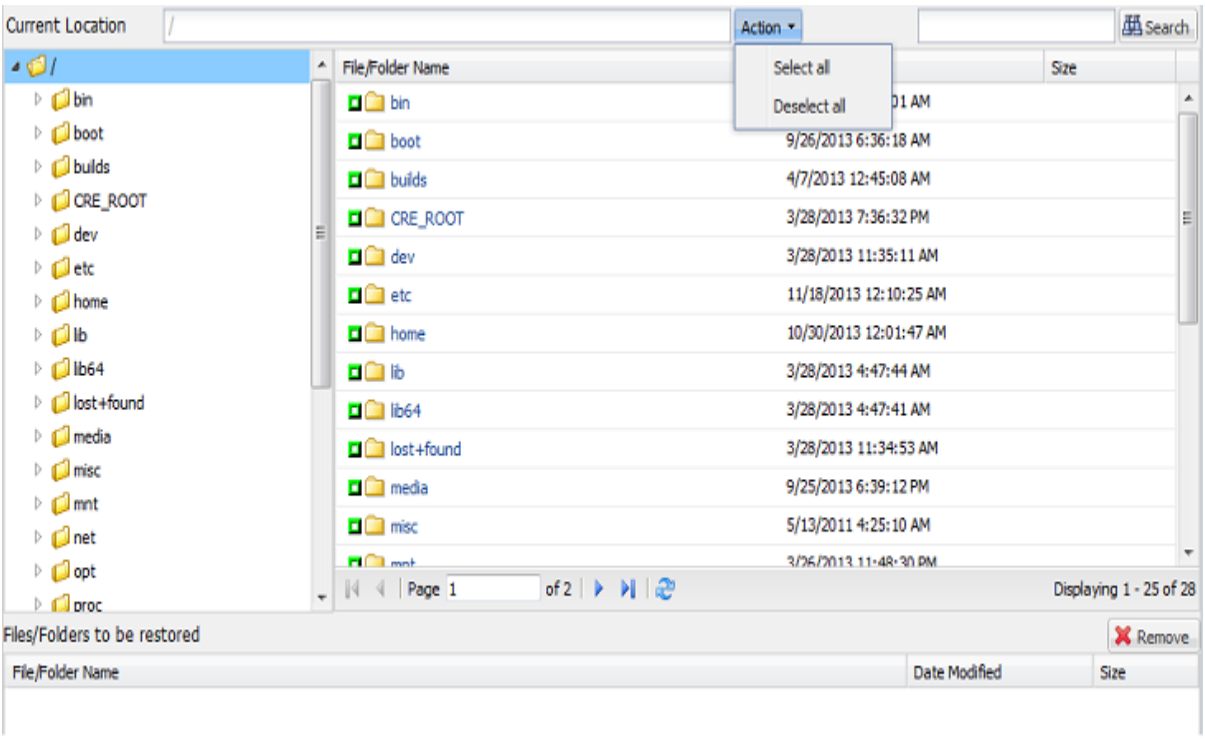
5. Aplique o filtro de datas para exibir os pontos de recuperação que são gerados entre a data especificada e clique em **Pesquisar**.

Padrão: últimas duas semanas.

Todos os pontos de recuperação disponíveis entre as datas especificadas serão exibidos.

6. Selecione o ponto de recuperação que deseja restaurar e clique em **Adicionar**. Se o ponto de recuperação estiver criptografado, insira a senha de criptografia para restaurar os dados.

A caixa de diálogo **Procurar-<nome do nó>** é aberta.



Importante: caso você encontre a mensagem de aviso, "os arquivos/pastas são exibidos no arquivo do dispositivo. Clique em Ajuda para obter mais informações." no console, consulte a seguinte Observação para obter uma resolução.

Observação: para alguns layouts de disco complexos, o sistema de arquivos é exibido pelo arquivo do dispositivo. A alteração no comportamento de exibição do sistema de arquivos não afeta a função de restauração de nível de arquivo da VM Linux com base em host. É possível procurar o sistema de arquivos sob o arquivo do dispositivo. Além disso, é possível usar a função de pesquisa para procurar um arquivo ou diretório específico.

7. Selecione os arquivos e as pastas que deseja restaurar e clique em **OK**.

   Observação: se você tentar localizar um arquivo ou pasta usando o campo **Pesquisar**, certifique-se de que tenha selecionado a pasta de nível mais alto na hierarquia. A pesquisa é conduzida em todas as pastas filhas da pasta selecionada.

   A caixa de diálogo **Procurar-<nome de nó>** é fechada e você retorna à página **Pontos de recuperação.** Os arquivos e pastas selecionados são listados em **Arquivos/pastas para restauração**.

8. Clique em **Avançar**.

   A página **Computador de destino** é exibida.

   O ponto de recuperação é especificado.

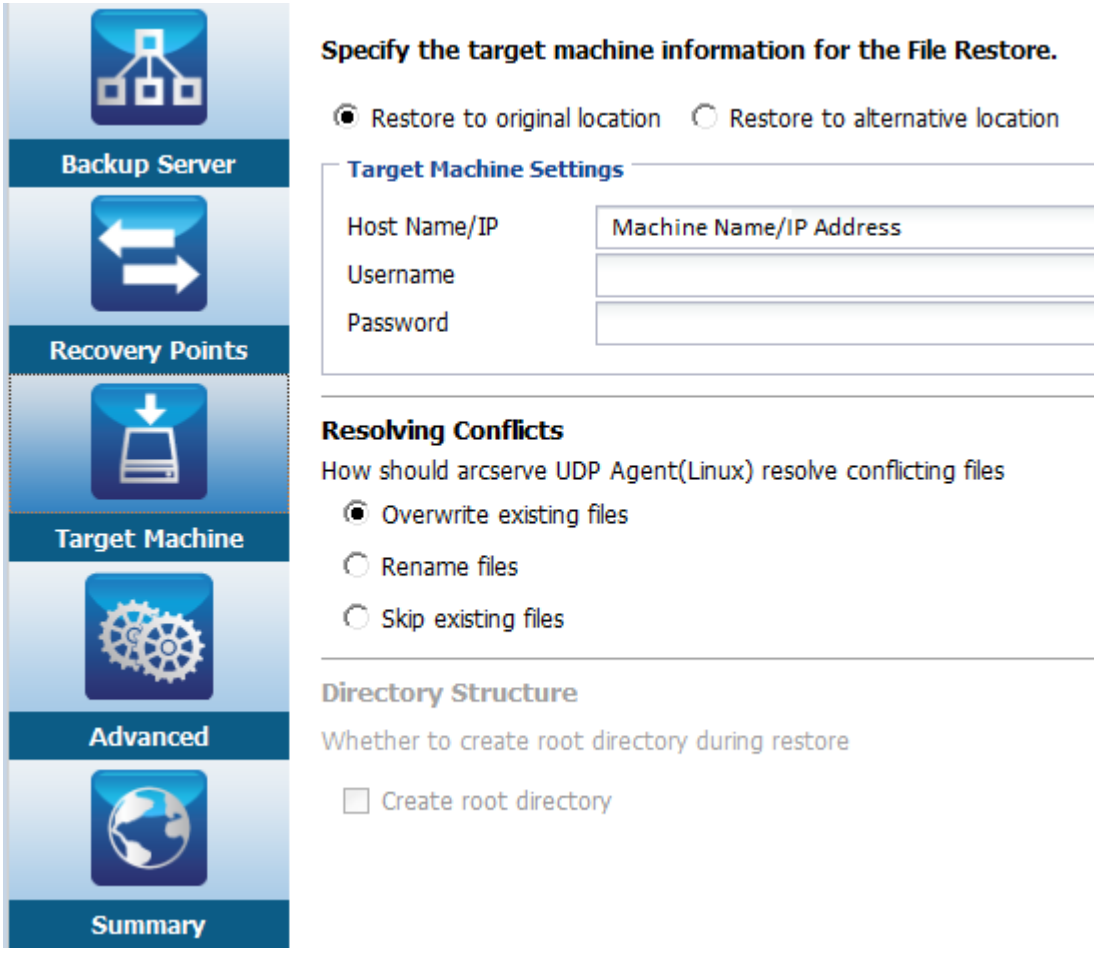
Especificar os detalhes da máquina de destino

Especifique os detalhes do nó de destino, de modo que os dados sejam restaurados para esse nó. É possível restaurar os arquivos ou pastas selecionados no nó de origem ou para um novo nó.

Para fazer a restauração para o nó a partir do qual o backup dos dados foi realizado, siga estas etapas:

1. Selecione **Restaurar no local original** na página **Computador de destino**.

   O campo **Nome do host** em **Configurações do computador de destino** é preenchido com o nome do nó de origem.



2. Digite o nome de usuário e a senha do nó.
3. Selecione uma das seguintes opções para resolver arquivos conflitantes:

   Substituir arquivos existentes

   Especifica que, se o arquivo existe no computador de destino, o arquivo de backup do ponto de recuperação substituirá o arquivo existente.

Renomear arquivos

Especifica que, se o arquivo existir no computador de destino, será criado um novo arquivo com o mesmo nome de arquivo e extensão de arquivo *.d2dduplicate<x>*. <x> especifica o número de vezes que o arquivo é restaurado. Todos os dados serão restaurados para o novo arquivo.

Ignorar arquivos existentes

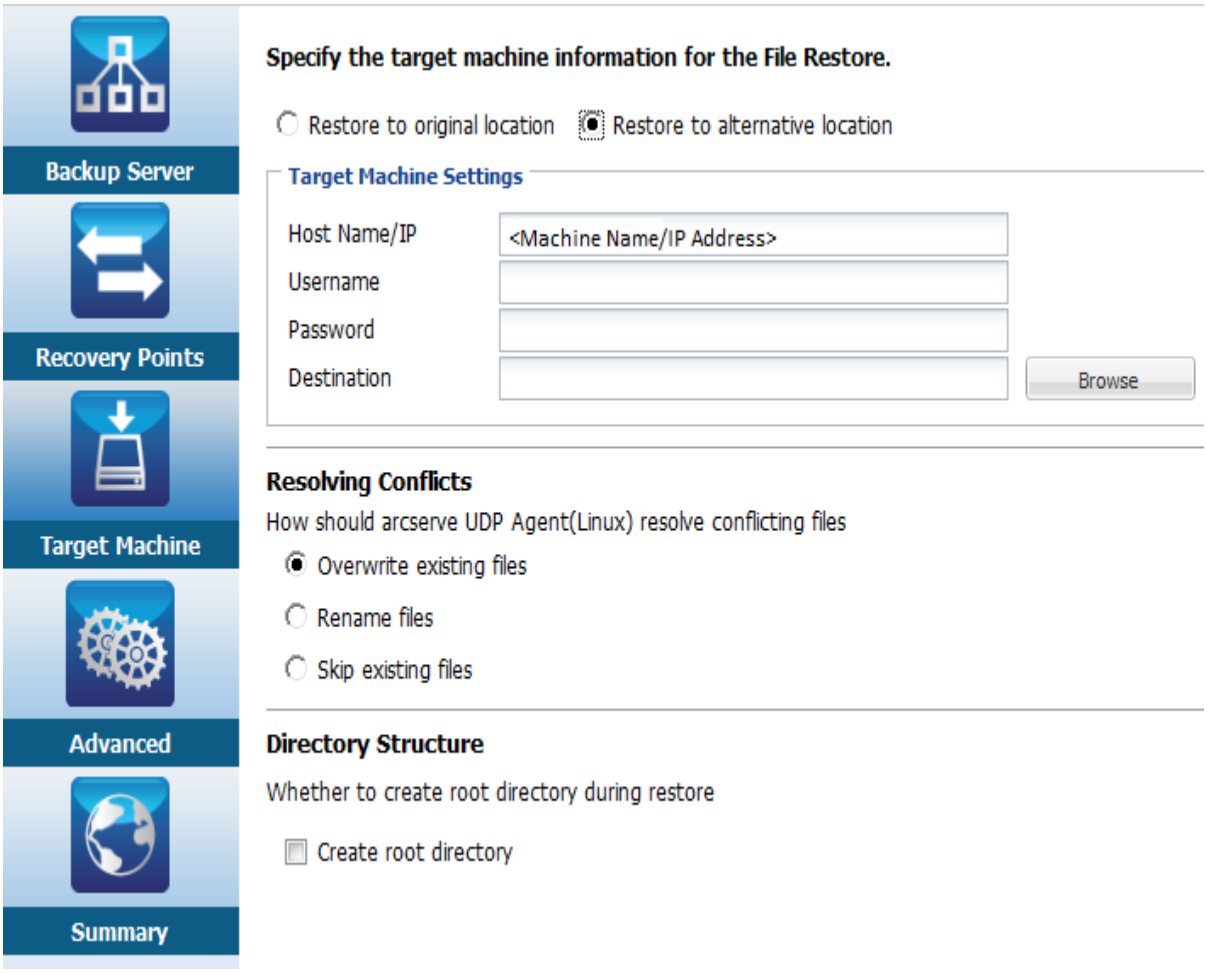
Especifica que, se o mesmo arquivo existe no computador de destino, esses arquivos não serão restaurados a partir do ponto de recuperação.

4. Clique em **Avançar**.

   A página **Avançado** é exibida.

Para restaurar em um novo nó, siga estas etapas:

1. Selecione **Restaurar em um local diferente** na página **Computador de destino**.



2. Digite o nome do host ou o endereço IP do nó de destino.

3. Digite o nome de usuário e a senha do nó.
4. Digite o caminho onde os dados são restaurados ou clique em **Procurar** para selecionar a pasta na qual os dados serão restaurados e, em seguida, clique em **OK**.
5. Selecione uma das seguintes opções para resolver arquivos conflitantes:

   Substituir arquivos existentes

   Especifica que, se o arquivo existe no computador de destino, o arquivo de backup do ponto de recuperação substituirá o arquivo existente.

   Renomear arquivos

   Especifica que, se o arquivo existir no computador de destino, será criado um novo arquivo com o mesmo nome de arquivo e extensão de arquivo *.d2dduplicate<x>*. <x> especifica o número de vezes que o arquivo é restaurado. Todos os dados serão restaurados para o novo arquivo.

   Ignorar arquivos existentes

   Especifica que, se o mesmo arquivo existe no computador de destino, esses arquivos não serão restaurados a partir do ponto de recuperação.
6. (Opcional) Selecione **Criar diretório raiz**.
7. Clique em **Avançar**.

   A página **Avançado** é exibida.

Os detalhes do computador de destino são especificados.

Especificar as configurações avançadas

Especifique as configurações avançadas para executar uma recuperação programada de seus dados. A recuperação programada assegura que os dados sejam recuperados no horário especificado, mesmo em sua ausência.

Siga estas etapas:

1. Defina a hora e data de início, selecionando uma das seguintes opções:

   Executar agora

   Inicia a tarefa de restauração em nível de arquivo assim que você enviar a tarefa.

   Definir data e hora de início

   Inicia a tarefa de restauração em nível de arquivo na data e hora especificadas, após enviar a tarefa.

2. (Opcional) Selecione **Estimativa de tamanho do arquivo**.
3. (Opcional) Selecione um script a partir da opção **Configurações de scripts anteriores e posteriores**.

   Esses scripts executam os comandos de script para as ações a serem realizadas antes do início da tarefa e/ou após a conclusão da tarefa.

   Observação: os campos **Configurações de scripts anteriores e posteriores** serão preenchidos apenas se já tiver criado um arquivo de script e o tiver colocado no seguinte local:

   /opt/Arcserve/d2dserver/usr/prepost

   Observação: para obter mais informações sobre como criar scripts anteriores e posteriores, consulte o tópico *Gerenciar scripts anteriores e posteriores para automação*.

4. Clique em **Avançar**.

   A página **Resumo** é exibida.

   As configurações avançadas são especificadas.

(Opcional) Gerenciar scripts anteriores e posteriores para automação

Os scripts anteriores e posteriores permitem executar sua própria lógica de negócios em estágios específicos de uma tarefa em execução. É possível especificar quando executar os scripts em **Configurações de scripts anteriores e posteriores** do **Assistente de backup** e do **Assistente de restauração** na interface do usuário. Dependendo da sua programação, é possível executar os scripts no servidor de backup.

O gerenciamento dos scripts anteriores e posteriores é um processo em duas etapas, que consiste em criar os scripts anteriores e posteriores e em colocar o script na pasta prepost.

Criar scripts anteriores e posteriores

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Crie um arquivo de script usando as variáveis de ambiente em sua linguagem de scripts de preferência.

   Variáveis de ambiente de script anterior e posterior

   Para criar seu script, use as seguintes variáveis de ambiente:

   D2D_JOBNAME

   Identifica o nome da tarefa.

   D2D_JOBID

   Identifica a ID da tarefa. A ID da tarefa é um número fornecido para a tarefa durante a execução da tarefa. Se você executar novamente a mesma tarefa, receberá um novo número de tarefa.

   D2D_TARGETNODE

   Identifica o nó cujo backup está sendo feito ou restaurado.

   D2D_JOBTYPE

   Identifica o tipo da tarefa em execução. Os valores a seguir identificam a variável D2D_JOBTYPE:

   backup.full

   Identifica a tarefa como um backup completo.

   backup.incremental

Identifica a tarefa como um backup incremental.

backup.verify

Identifica a tarefa como um backup de verificação.

restore.bmr

Identifica a tarefa como uma BMR (Bare-Metal Recovery – Recuperação Bare Metal). Esta é uma tarefa de restauração.

restore.file

Identifica a tarefa como uma restauração em nível de arquivo. Esta é uma tarefa de restauração.

D2D_SESSIONLOCATION

Identifica o local onde os pontos de recuperação estão armazenados.

D2D_PREPOST_OUTPUT

Identifica um arquivo temporário. O conteúdo da primeira linha do arquivo temporário é exibido no log de atividades.

D2D_JOBSTAGE

Identifica o estágio da tarefa. Os valores a seguir identificam a variável D2D_ JOBSTAGE:

pre-job-server

Identifica o script que é executado no servidor de backup antes do início da tarefa.

post-job-server

Identifica o script que é executado no servidor de backup após a conclusão da tarefa.

pre-job-target

Identifica o script que é executado no computador de destino antes do início da tarefa.

post-job-target

Identifica o script que é executado no computador de destino após a conclusão da tarefa.

pre-snapshot

Identifica o script que é executado no computador de destino antes de capturar o instantâneo.

post-snapshot

Identifica o script que é executado no computador de destino depois de capturar o instantâneo.

D2D_TARGETVOLUME

Identifica o volume cujo backup foi feito durante uma tarefa de backup. Essa variável é aplicável a scripts de instantâneo anteriores e posteriores para uma tarefa de backup.

D2D_JOBRESULT

Identifica o resultado de um script de tarefa posterior. Os valores a seguir identificam a variável D2D_JOBRESULT:

success

Identifica o resultado realizado com êxito.

fail

Identifica o resultado realizado sem êxito.

D2DSVR_HOME

Identifica a pasta onde o servidor de backup está instalado. Essa variável é aplicável a scripts que são executados no servidor de backup.

O script é criado.

Observação: para todos os scripts, um valor de retorno zero indica êxito e um valor de retorno diferente de zero indica falha.

Colocar o script na pasta Prepost e verificar

Todos os scripts anteriores e posteriores de um servidor de backup são gerenciados na pasta prepost no seguinte local:

/opt/Arcserve/d2dserver/usr/prepost

Siga estas etapas:

1. Coloque o arquivo no seguinte local do servidor de backup:

   /opt/Arcserve/d2dserver/usr/prepost

2. Forneça a permissão de execução para o arquivo de script.
3. Efetue logon na interface da web do Agente do Arcserve Unified Data Protection para Linux.
4. Abra o **Assistente de backup** ou o **Assistente de restauração** e navegue até à guia **Avançado**.
5. Selecione o arquivo de script na lista suspensa **Configurações de scripts anteriores/posteriores** e, em seguida, envie a tarefa.

6. Clique em **Log de atividades** e verifique se o script é executado para a tarefa de backup especificada.

   O script é executado.

   Os scripts anteriores e posteriores são criados com êxito e colocados na pasta pre-post.

Criar e executar a tarefa de restauração

Crie e execute a tarefa de restauração, para poder iniciar a recuperação de nível de arquivo. Verifique as informações do ponto de recuperação antes de restaurar os arquivos. Se necessário, será possível voltar e alterar as configurações de restauração no assistente.

Siga estas etapas:

1. Verifique os detalhes da restauração na página **Resumo** do **Assistente de restauração**.
2. (Opcional) Clique em **Voltar** para modificar as informações que você digitou em qualquer página do **Assistente de restauração**.
3. Digite um nome da tarefa e clique em **Enviar**.

   O campo **Nome da tarefa** tem um nome padrão inicialmente. É possível digitar um novo nome de tarefa de sua escolha, mas não é possível deixar esse campo em branco.

   O **Assistente de restauração** é fechado. É possível ver o status da tarefa na guia **Status da tarefa**.

   A tarefa de restauração é criada e executada com êxito.

Verificar se os arquivos foram restaurados

Após a conclusão da tarefa de restauração, certifique-se de que todos os arquivos estejam restaurados no nó de destino. Verifique as guias **Histórico da tarefa** e **Log de atividades** no painel **Status** para monitorar o andamento do processo de restauração.

Siga estas etapas:

1. Navegue para o computador de destino em que você restaurou os dados.
2. Verifique se os dados necessários do ponto de recuperação foram restaurados.

   Os arquivos são verificados com êxito.

   A recuperação em nível de arquivo é executada com êxito.

Como executar uma migração da IVM (de um ponto de recuperação do Linux) da nuvem para o local

Se tiver um de um ponto de recuperação do Linux no Amazon S3, será possível executar uma tarefa da IVM no AWS e, em seguida, migrar a IVM do AWS para o local.

Conclua as tarefas seguir para executar uma migração de IVM:

- Verificar os pré-requisitos para uma migração da IVM
- Realizar a migração de IVM da nuvem para o local

Verificar os pré-requisitos e as considerações da migração da IVM

Pré-requisitos:

- Você tem um ponto de recuperação válido e a senha de criptografia, se houver, para restauração.
- Você tem conta Amazon EC2 e Amazon S3.
- O servidor Samba está instalado no servidor de backup Linux.

Considerações:

Esse recurso é suportado apenas no servidor de backup Linux que é instalado no RHEL/CentOS/Oracle Linux 7.x ou SLES 12.x.

Realizar a migração de IVM da nuvem para o local

É possível migrar a IVM da nuvem para o local usando os três procedimentos detalhados. Clique nos links de cada procedimento e execute a migração completa.

- Para criar uma máquina virtual instantânea no Amazon EC2, execute a máquina virtual instantânea a partir do ponto de recuperação de VM do Linux no Amazon EC2.
- Instale o servidor de backup do Linux dentro desta máquina virtual instantânea que acabou de criar. Executar o backup dentro da IVM e fazer backup no Amazon S3.
- Fazer backup do computador linux para o Amazon S3.
- Execute a tarefa de BMR do ponto de recuperação no Amazon S3 cujo backup foi feito.

Como executar uma BMR (Bare Metal Recovery - Recuperação Bare Metal) para computadores Linux

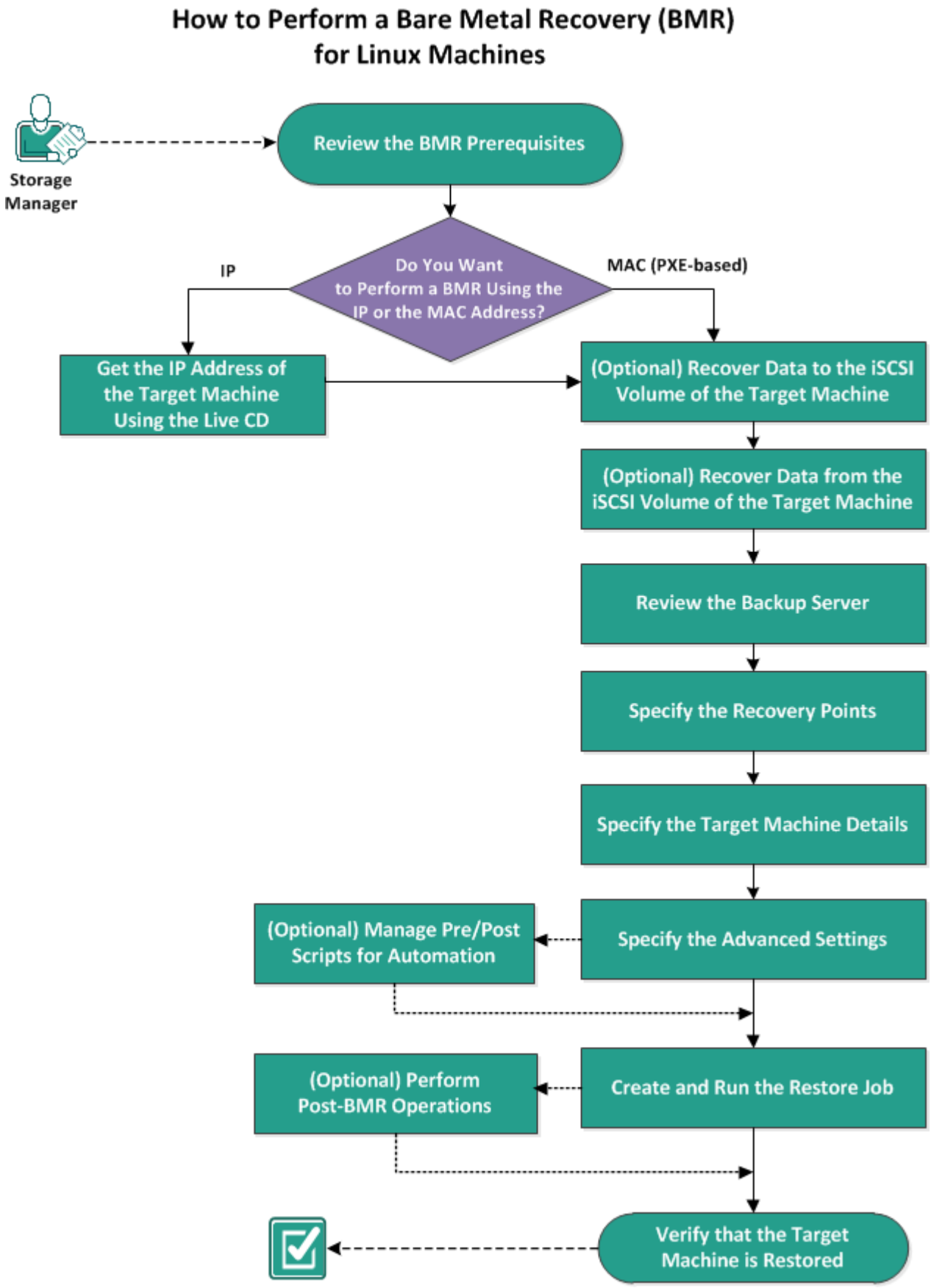
Uma BMR restaura o sistema operacional e os aplicativos de software e recupera todos os dados incluídos no backup. A BMR é o processo de restauração de um sistema de computador do estado *bare metal*. Bare metal é um computador sem sistema operacional, drivers e aplicativos de software. Depois que a restauração for concluída, o computador de destino será reinicializado automaticamente no mesmo ambiente operacional que o nó de origem do backup e todos os dados serão restaurados.

Uma BMR completa é possível porque quando você faz backup de dados, ele também captura informações relacionadas ao sistema operacional, aplicativos instalados, drivers e assim por diante.

É possível executar uma BMR usando o endereço IP ou o endereço MAC (Media Access Control – Controle de Acesso à Mídia) do computador de destino. Se você inicializar o computador de destino usando o Live CD do Agente do Arcserve Unified Data Protection para Linux, poderá obter o endereço IP do computador de destino.

Observação: não é possível inicializar o computador. Apenas uma NIC está configurada.

O diagrama a seguir exibe o processo para executar uma BMR:



Conclua as tarefas a seguir para executar uma BMR:

- Verificar os pré-requisitos da BMR
- Obter o endereço IP do computador de destino usando o Live CD
- (Opcional) Recuperar dados para o volume iSCSI do computador de destino
- (Opcional) Recuperar dados do volume iSCSI para o computador de destino
- Analisar o servidor de backup
- Especificar os pontos de recuperação
- Especificar os detalhes do computador de destino
- Especificar as configurações avançadas
- (Opcional) Gerenciar scripts anteriores e posteriores para automação
- Criar e executar a tarefa de restauração
- (Opcional) Executar as operações pós-BMR
- Verificar se o computador de destino foi restaurado

Verificar os pré-requisitos da BMR

Considere as seguintes opções antes de executar uma BMR:

- Você tem um ponto de recuperação válido e a senha de criptografia, se houver, para restauração.
- Você tem um computador de destino válido para a BMR.
- Você criou o Live CD do Agente do Arcserve Unified Data Protection para Linux.
- Se você deseja executar uma BMR usando o endereço IP, deve obter o endereço IP do computador de destino usando o Live CD.
- Se você deseja executar uma BMR com base em PXE usando o endereço MAC, deve ter o endereço MAC do computador de destino.
- O ponto de recuperação deve ser proveniente do backup com base em agente do Linux.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Obter o endereço IP do computador de destino usando o Live CD

Antes de executar uma BMR usando o endereço IP, é necessário obter o endereço IP do computador de destino. O computador bare metal não tem um endereço IP inicial. Portanto, você precisa inicializar o computador bare-metal usando o Live CD padrão, que é o Live CD do Agente do Arcserve Unified Data Protection para Linux ou o Live CD com base no CentOS para obter o endereço IP. Após obter o endereço IP do computador de destino, é possível configurar o IP estático do computador de destino.

Siga estas etapas:

1. Insira o Live CD ou monte o arquivo .iso do Live CD na unidade de CD-ROM do nó de destino.
2. Inicialize o computador de destino a partir do CD-ROM.

   O computador de destino é inicializado no ambiente do Live CD do Agente do Arcserve Unified Data Protection para Linux. O endereço IP do computador de destino é exibido na tela.
3. Para configurar o IP estático do computador de destino usando o Live CD padrão, siga estas etapas:
   a. Na tela do computador de destino, pressione Enter para inserir o ambiente de shell.
   b. Execute o comando a seguir para configurar o IP estático:

      ifconfig <NIC name> <static IP address> netmask <netmask>

      route add default gw <gateway IP address> <NIC name>

   Observação: o nome da NIC (Network Interface Card –Placa de Interface de Rede) depende do hardware. Por exemplo, os nomes típicos da NIC são eth0 ou em0.
4. Para configurar o IP estático do computador de destino usando o Live CD com base no CentOS, siga estas etapas:
   a. Abra uma janela do terminal no computador de destino clicando em Aplicativos, Ferramentas do sistema, Terminal.
   b. Execute os seguintes comandos:

      sudo ifconfig <NIC name> <static IP address> netmask <netmask>

      sudo route add default gw <gateway IP address> <NIC name>

   O IP estático é configurado.

   O endereço IP do computador de destino é obtido.

Importante: Mantenha um registro desse endereço IP, pois ele será usado no **Assistente de restauração** quando for necessário especificar os detalhes do computador de destino.

(Opcional) Recuperar dados para o volume iSCSI do computador de destino

É possível integrar o volume iSCSI no computador de destino e tornar este volume parte do computador de destino. Em seguida, é possível restaurar os dados para o volume iSCSI do computador de destino. Assim, será possível gerenciar dados e transferi-los por uma rede.

Importante: Ao integrar o volume iSCSI ao computador de destino, você perderá todos os dados existentes do volume iSCSI.

Siga estas etapas:

1. Insira o Live CD do Agente do Arcserve Unified Data Protection para Linux ou monte o arquivo .iso do Live CD do Agente do Arcserve Unified Data Protection para Linux na unidade de CD-ROM do computador de destino.
2. Inicialize o computador de destino a partir do CD-ROM.

   O computador de destino é inicializado no ambiente do Live CD do Agente do Arcserve Unified Data Protection para Linux. O endereço IP do computador de destino é exibido na tela.
3. Digite o ambiente do shell do computador de destino.
4. Execute o seguinte comando para iniciar o daemon do iniciador iSCSI:

   /etc/init.d/iscsid start
5. Execute um script de detecção para detectar o host de destino iSCSI.

   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>

   O valor da porta padrão do host de destino iSCSI é 3260.
6. Anote o IQN (iSCSI Qualified Name – Nome Qualificado iSCSI) do host de destino iSCSI encontrado pelo script de detecção antes de efetuar logon manualmente no destino detectado.
7. Liste o dispositivo de bloqueio disponível do nó de destino.

   #fdisk -l
8. Efetue logon no destino detectado.

   iscsiadm -m node -T <iSCSI Target IQN name> -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number> -l

   É possível ver um dispositivo de bloqueio no diretório /dev do nó de destino.
9. Execute o comando a seguir para obter o novo nome do dispositivo:

#fdisk -l

É possível ver um dispositivo adicional nomeado /dev/sd<x> no nó de destino.

O volume iSCSI é integrado ao volume de destino.

(Opcional) Recuperar dados do volume iSCSI para o computador de destino

Se você tiver armazenado os dados em um volume de destino iSCSI, é possível conectar o volume iSCSI e recuperar os dados. O volume iSCSI permite gerenciar dados e transferi-los por uma rede.

Siga estas etapas:

1. Insira o Live CD do Agente do Arcserve Unified Data Protection para Linux ou monte o arquivo .iso do Live CD do Agente do Arcserve Unified Data Protection para Linux na unidade de CD-ROM do computador de destino.
2. Inicialize o computador de destino a partir do CD-ROM.

   O computador de destino é inicializado no ambiente do Live CD do Agente do Arcserve Unified Data Protection para Linux. O endereço IP do computador de destino é exibido na tela.
3. Digite o ambiente do shell do computador de destino.
4. Execute o seguinte comando para iniciar o daemon do iniciador iSCSI:

   /etc/init.d/iscsid start
5. Execute um script de detecção para detectar o host de destino iSCSI.

   iscsiadm -m discovery -t sendtargets -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number>

   O valor da porta padrão do host de destino iSCSI é 3260.
6. Anote o IQN (iSCSI Qualified Name – Nome Qualificado iSCSI) do host de destino iSCSI encontrado pelo script de detecção antes de efetuar logon manualmente no destino detectado.
7. Liste o dispositivo de bloqueio disponível do nó de destino.

   #fdisk -l
8. Efetue logon no destino detectado.

   iscsiadm -m node -T <iSCSI Target IQN name> -p <ISCSI-SERVER-IP-ADDRESS>:<Port_Number> -l

   É possível ver um dispositivo de bloqueio no diretório /dev do nó de destino.
9. Execute o comando a seguir para obter o novo nome do dispositivo:

   #fdisk -l

   É possível ver um dispositivo adicional nomeado /dev/sd<x> no nó de destino.

Por exemplo, considere que o nome do dispositivo é /dev/sdc. Esse nome de dispositivo é usado para criar uma partição e um sistema de arquivos nas etapas a seguir.

10. Monte o volume iSCSI usando os seguintes comandos:

    # mkdir /iscsi

    # mount /dev/sdc1 /iscsi

    Observação: ao especificar o local da sessão no Assistente de restauração, é necessário selecionar Local e digitar o caminho /iscsi.

    Exemplo: <caminho>/iscsi

    O computador de destino agora pode se conectar ao volume iSCSI e pode recuperar os dados do volume iSCSI.

Analisar o servidor de backup

Ao abrir o **Assistente de restauração**, verifique o servidor de backup no qual deseja executar a operação de restauração.

Siga estas etapas:

1. Acesse o assistente de restauração com um dos seguintes procedimentos:

   A partir do Arcserve UDP :

   a. Efetue logon no Arcserve UDP.

   b. Clique na guia **Recursos**.

   c. Selecione **Todos os nós** no painel esquerdo.

      Todos os nós do adicionados são exibidos no painel central.

   d. No painel central, selecione o nó do e clique em **Ações**.

   e. Clique em **Restaurar** no menu suspenso **Ações**.

      A interface da web do Agente do Arcserve Unified Data Protection para Linux é exibida. A caixa de diálogo Selecionar tipo de restauração é exibida na interface de usuário do agente.

   f. Selecione o tipo de restauração e clique em **OK**.

      Observação: você será automaticamente conectado ao nó do agente e o **Assistente de restauração** será exibido do nó do agente.

   A partir do Agente do Arcserve Unified Data Protection para Linux :

   a. Abra a interface da web do Agente do Arcserve Unified Data Protection para Linux.

      Observação: durante a instalação do Agente do Arcserve Unified Data Protection para Linux, você recebeu o URL para acessar e gerenciar o servidor. Efetue logon no Agente do Arcserve Unified Data Protection para Linux.

   b. Clique em **Restaurar** no menu **Assistente**, selecione **Recuperação bare metal (BMR)**.

      A página **Servidor de backup** do **Assistente de restauração – BMR** é exibida.

2. Verifique o servidor na lista suspensa **Servidor de backup** na página **Servidor de backup**.

   Não é possível selecionar nenhuma opção na lista suspensa **Servidor de backup**.

3. Clique em **Avançar**.

   A página **Pontos de recuperação** do **Assistente de restauração – BMR** é exibida.

O servidor de backup é especificado.

Especificar os pontos de recuperação

Cada vez que você executar um backup com êxito, um ponto de recuperação é criado. Especifique as informações do ponto de recuperação no **Assistente de restauração** de forma que seja possível recuperar exatamente os dados desejados. É possível restaurar arquivos específicos ou todos os arquivos de acordo com as suas necessidades.

Importante: para executar uma BMR a partir de um ponto de recuperação, o volume raiz e o volume de inicialização devem estar presentes no ponto de recuperação.

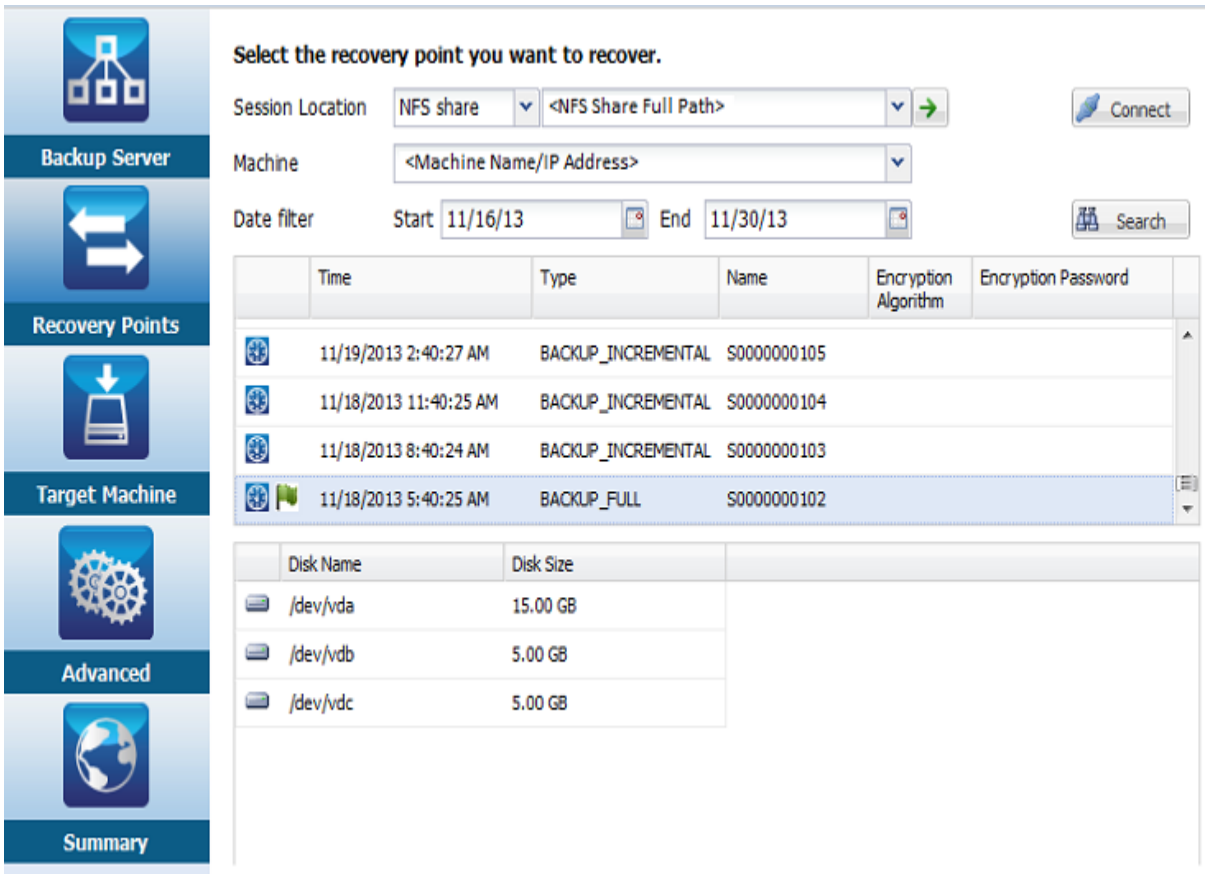
Siga estas etapas:

1. Execute uma das seguintes etapas, dependendo do armazenamento de backup.
   - Execute as seguintes etapas para acessar os pontos de recuperação, caso os pontos de recuperação estejam armazenados em um dispositivo móvel:
     a. Inicie o computador de destino usando o Live CD.
     b. Efetue logon na interface da web do Agente do Arcserve Unified Data Protection para Linux pelo Live CD.
     c. Abra o **Assistente de BMR**.
     d. Vá até à página **Pontos de recuperação**.
     e. Selecione **Local** como **Local da sessão** na página **Pontos de recuperação** do **Assistente de BMR**.
   - Execute as seguintes etapas se o local da sessão for compartilhamento de NFS ou compartilhamento CIFS:
     a. Selecione uma sessão na lista suspensa **Local da sessão** e digite o caminho completo do compartilhamento.

        Por exemplo, considere o local da sessão como o compartilhamento de NFS, xxx.xxx.xxx.xxx como o endereço IP do compartilhamento de NFS e o nome da pasta como *Dados.* Você deve inserir xxx.xxx.xxx.xxx:/Data como o local de compartilhamento de NFS.

        Observação: se os dados de backup forem armazenados no local de origem, será necessário primeiro converter o nó de origem para um ser-

vidor do NFS e, em seguida, compartilhar o local da sessão.



2. Clique em **Conectar**.

   Todos os nós que foram copiados para backup nesse local são listados na lista suspensa **Computador**.

3. Selecione o nó que deseja restaurar na lista suspensa **Computador**.

   Todos os pontos de recuperação do nó selecionado são listados.

4. Aplique o filtro de datas para exibir os pontos de recuperação que são gerados entre a data especificada e clique em **Pesquisar**.

   Padrão: últimas duas semanas.

   Todos os pontos de recuperação disponíveis entre as datas especificadas serão exibidos.

5. Selecione o ponto de recuperação que deseja restaurar e clique em **Avançar**.

   A página **Computador de destino** é exibida.

   O ponto de recuperação é especificado.

Especificar os detalhes do computador de destino

Especifique os detalhes do computador de destino, de modo que os dados sejam restaurados para esse computador. Um computador de destino é um computador bare metal no qual você irá executar uma BMR. Se fizer a restauração usando o endereço IP, será necessário o endereço IP do computador de destino que você já registrou no início deste processo. Se fizer a restauração usando o endereço MAC, será necessário o endereço MAC do computador de destino.

Siga estas etapas:

1. Forneça o endereço MAC ou o endereço IP do computador de destino no campo **Endereço IP/MAC**.
2. Digite um nome no campo **Nome do host**.

   O computador de destino usará esse nome como o nome do host após a conclusão do processo de restauração.
3. Selecione uma das seguintes opções como a rede:

   DHCP

   Configura automaticamente o endereço IP. Esta é a opção padrão. Use essa opção se tiver um servidor DHCP (Dynamic Host Configuration Protocol – Protocolo de Configuração Dinâmica de Host) para restaurar com a rede DHCP.

   IP estático

   Configura manualmente o endereço IP. Se você selecionar essa opção, digite o **Endereço IP**, a **Máscara de sub-rede** e o **Gateway padrão** da máquina de destino.

   Importante: Certifique-se de que o IP estático não seja usado por nenhum outro computador da rede durante o processo de restauração.
4. (Opcional) Selecione a opção **Ativar BMR instantânea**, de modo que possa usar a máquina de destino instantaneamente.

   Quando essa opção for ativada, o Agente do Arcserve Unified Data Protection para Linux primeiro recuperará todos os dados necessários para iniciar a máquina. Os dados restantes serão recuperados depois que a máquina de destino for iniciada. A conexão de rede deve estar constantemente disponível durante a BMR instantânea.

   Exemplo: Se você tiver 100 GB de dados, desejar executar uma BMR e *não* selecionar essa opção, primeiro, todos os 100 GB de dados serão recuperados e, em seguida, será possível usar a máquina de destino. No entanto, apenas aproximadamente 1 GB de dados são necessários para iniciar a máquina. Ao ativar essa opção, primeiro, os 1 GB de dados necessários são recuperados, de modo que seja

possível iniciar e usar a máquina. Depois que a máquina for iniciada, os 99 GB de dados restantes serão recuperados automaticamente.

Observação: os dados necessários para iniciar a máquina dependem da configuração do sistema operacional. Também é possível pausar ou retomar a recuperação automática de dados se a opção **Não recuperar dados automaticamente depois que o computador for iniciado** não estiver selecionada.

5. (Opcional) Selecione a opção **Não recuperar dados automaticamente quando o computador for iniciado** para interromper a recuperação automática de dados quando a máquina de destino for iniciada.

   Quando você seleciona a opção **Ativar BMR instantânea**, o comportamento padrão é primeiro recuperar os dados necessários e iniciar a máquina. Depois que a máquina for iniciada, os dados restantes são recuperados automaticamente. Se você atualizar os dados de origem durante a recuperação, ao selecionar essa opção, os dados serão recuperados até o ponto antes da atualização.

6. Clique em **Avançar**.

   A página **Avançado** é exibida.

   Os detalhes do computador de destino são especificados.

Especificar as configurações avançadas

Especifique as configurações avançadas para executar uma BMR programada dos dados. A BMR programada garante que os dados sejam recuperados no horário especificado, até mesmo, em sua ausência.

Siga estas etapas:

1. Defina a hora e data de início, selecionando uma das seguintes opções:

   Executar agora

   Inicia a tarefa de restauração assim que você enviar a tarefa.

   Definir horário especial

   Inicia a tarefa de restauração no horário especificado, após enviar a tarefa.

2. (Opcional) Selecione um script a partir da opção **Configurações de scripts anteriores e posteriores** para o servidor de backup e o computador de destino.

   Esses scripts executam os comandos de script para as ações a serem realizadas antes do início da tarefa e/ou após a conclusão da tarefa.

   Observação: os campos **Configurações de scripts anteriores e posteriores** serão preenchidos apenas se já tiver criado um arquivo de script e o tiver colocado no seguinte local:

   /opt/Arcserve/d2dserver/usr/prepost

   Observação: para obter mais informações sobre como criar scripts anteriores e posteriores, consulte o tópico *Gerenciar scripts anteriores e posteriores para automação*.

3. (Opcional) Clique em **Mostrar mais configurações** para exibir mais configurações para a BMR.

4. (Opcional) Redefina a senha do nome de usuário especificado para o computador de destino recuperado.

5. (Opcional) Insira o caminho completo do local de armazenamento de backup dos pontos de recuperação no **Acesso local do ponto de recuperação**.

6. (Opcional) Insira o nome completo do disco no campo **Discos** para excluir esses discos no computador de destino da participação no processo de recuperação.

7. (Opcional) Selecione **Ativar o Wake-on-LAN** se estiver executando a BMR de PXE (Preboot Execution Environment – Ambiente de Execução de Pré-inicialização).

   Observação: a opção **Ativar o Wake-on-LAN** aplica-se somente às máquinas físicas. Verifique se você ativou as configurações do Wake-on-LAN nas configurações do BIOS da máquina física.

8. (Opcional) Selecione a opção **Reinicialização** para reiniciar automaticamente o nó de destino, após a conclusão da BMR.
9. Clique em **Avançar**.

   A página **Resumo** é exibida.

   As configurações avançadas são especificadas.

(Opcional) Gerenciar scripts anteriores e posteriores para automação

Os scripts anteriores e posteriores permitem executar sua própria lógica de negócios em estágios específicos de uma tarefa em execução. É possível especificar quando executar os scripts em **Configurações de scripts anteriores e posteriores** do **Assistente de backup** e do **Assistente de restauração** na interface do usuário. Dependendo da sua programação, é possível executar os scripts no servidor de backup.

O gerenciamento dos scripts anteriores e posteriores é um processo em duas etapas, que consiste em criar os scripts anteriores e posteriores e em colocar o script na pasta prepost.

Criar scripts anteriores e posteriores

Siga estas etapas:

1. Efetue logon no servidor de backup como usuário raiz.
2. Crie um arquivo de script usando as variáveis de ambiente em sua linguagem de scripts de preferência.

   Variáveis de ambiente de script anterior e posterior

   Para criar seu script, use as seguintes variáveis de ambiente:

   D2D_JOBNAME

   Identifica o nome da tarefa.

   D2D_JOBID

   Identifica a ID da tarefa. A ID da tarefa é um número fornecido para a tarefa durante a execução da tarefa. Se você executar novamente a mesma tarefa, receberá um novo número de tarefa.

   D2D_TARGETNODE

   Identifica o nó cujo backup está sendo feito ou restaurado.

   D2D_JOBTYPE

   Identifica o tipo da tarefa em execução. Os valores a seguir identificam a variável D2D_JOBTYPE:

   backup.full

   Identifica a tarefa como um backup completo.

   backup.incremental

Identifica a tarefa como um backup incremental.

backup.verify

Identifica a tarefa como um backup de verificação.

restore.bmr

Identifica a tarefa como uma BMR (Bare-Metal Recovery – Recuperação Bare Metal). Esta é uma tarefa de restauração.

restore.file

Identifica a tarefa como uma restauração em nível de arquivo. Esta é uma tarefa de restauração.

D2D_SESSIONLOCATION

Identifica o local onde os pontos de recuperação estão armazenados.

D2D_PREPOST_OUTPUT

Identifica um arquivo temporário. O conteúdo da primeira linha do arquivo temporário é exibido no log de atividades.

D2D_JOBSTAGE

Identifica o estágio da tarefa. Os valores a seguir identificam a variável D2D_ JOBSTAGE:

pre-job-server

Identifica o script que é executado no servidor de backup antes do início da tarefa.

post-job-server

Identifica o script que é executado no servidor de backup após a conclusão da tarefa.

pre-job-target

Identifica o script que é executado no computador de destino antes do início da tarefa.

post-job-target

Identifica o script que é executado no computador de destino após a conclusão da tarefa.

pre-snapshot

Identifica o script que é executado no computador de destino antes de capturar o instantâneo.

post-snapshot

Identifica o script que é executado no computador de destino depois de capturar o instantâneo.

D2D_TARGETVOLUME

Identifica o volume cujo backup foi feito durante uma tarefa de backup. Essa variável é aplicável a scripts de instantâneo anteriores e posteriores para uma tarefa de backup.

D2D_JOBRESULT

Identifica o resultado de um script de tarefa posterior. Os valores a seguir identificam a variável D2D_JOBRESULT:

success

Identifica o resultado realizado com êxito.

fail

Identifica o resultado realizado sem êxito.

D2DSVR_HOME

Identifica a pasta onde o servidor de backup está instalado. Essa variável é aplicável a scripts que são executados no servidor de backup.

O script é criado.

Observação: para todos os scripts, um valor de retorno zero indica êxito e um valor de retorno diferente de zero indica falha.

Colocar o script na pasta Prepost e verificar

Todos os scripts anteriores e posteriores de um servidor de backup são gerenciados na pasta prepost no seguinte local:

/opt/Arcserve/d2dserver/usr/prepost

Siga estas etapas:

1. Coloque o arquivo no seguinte local do servidor de backup:

   /opt/Arcserve/d2dserver/usr/prepost
2. Forneça a permissão de execução para o arquivo de script.
3. Efetue logon na interface da web do Agente do Arcserve Unified Data Protection para Linux.
4. Abra o **Assistente de backup** ou o **Assistente de restauração** e navegue até à guia **Avançado**.
5. Selecione o arquivo de script na lista suspensa **Configurações de scripts anteriores/posteriores** e, em seguida, envie a tarefa.

6. Clique em **Log de atividades** e verifique se o script é executado para a tarefa de backup especificada.

   O script é executado.

   Os scripts anteriores e posteriores são criados com êxito e colocados na pasta pre-post.

Criar e executar a tarefa de restauração

Crie e execute a tarefa de restauração, para poder iniciar o processo de BMR. Verifique as informações do ponto de recuperação antes de executar uma BMR. Se necessário, será possível voltar e alterar as configurações de restauração.

Siga estas etapas:

1. Verifique os detalhes da restauração na página **Resumo** do **Assistente de restauração**.
2. (Opcional) Clique em **Voltar** para modificar as configurações de restauração em qualquer uma das páginas do **Assistente de restauração.**
3. Digite um nome da tarefa e clique em **Enviar**.

   O campo **Nome da tarefa** tem um nome padrão inicialmente. É possível digitar um novo nome de tarefa de sua escolha, mas não é possível deixar esse campo em branco.

   O **Assistente de restauração** é fechado. É possível ver a tarefa na guia **Status da tarefa**. Se você usar o endereço IP para a BMR, o computador de destino será reinicializado automaticamente para o mesmo sistema operacional que a origem do backup, após o processo da BMR.

   Se você usar o endereço MAC para a BMR, o status na guia **Status da tarefa** será alterado para *Aguardando a inicialização do nó de destino*.
4. (Opcional) Para a BMR usando o endereço MAC, inicie o computador de destino quando for exibida a mensagem *Aguardando a inicialização do nó de destino* na guia **Status da tarefa**.

   Observação: se o computador de destino já tiver sido iniciado antes de você enviar a tarefa de restauração, será necessário reiniciá-lo. Certifique-se de que o BIOS esteja configurado para inicializar a partir da rede.

   O status na coluna **Status da tarefa** é alterado para **Restaurando o volume**. Isso indica que a restauração está em andamento. Após a conclusão da tarefa de restauração, o computador de destino será reinicializado automaticamente com o mesmo sistema operacional que a origem do backup.

   A tarefa de restauração foi criada e executada com êxito.

(Opcional) Executar as operações pós-BMR

Os tópicos a seguir são configurações opcionais que você pode ter para executar depois de uma BMR:

Configurar o X Windows

Quando você executa uma BMR em um hardware diferente, o X Windows do SO restaurado não funciona corretamente e o nó de destino exibe uma caixa de diálogo de erro. A caixa de diálogo de erro aparece porque a configuração de exibição foi alterada. Para solucionar este problema, siga as instruções da caixa de diálogo de erro para configurar a placa gráfica. Depois disso, você poderá ver o X Windows e a IU da área de trabalho.

Configurar o FQDN (Fully Qualified Domain Name – Nome de Domínio Totalmente Qualificado) do sistema

Quando precisar de um FQDN, terá que configurá-lo. O processo de BMR não configura automaticamente o FQDN.

Contagem máxima de caracteres do FQDN: 63

Siga estas etapas para configurar o FQDN:

1. Edite o arquivo */etc/hosts* e forneça o endereço IP, o nome do FQDN e o nome do servidor.

   #vi /etc/hosts

   ip_of_system servername.domainname.com servername

2. Reinicie o serviço de rede.

   #/etc/init.d/network restart

3. Verifique o nome do host e o nome do FQDN.

   #hostname

   servername

   #hostname -f

   servername.domainname.com

   O FQDN está configurado.

Estender o volume de dados após uma BMR em discos diferentes

Quando executar uma BMR em um disco maior do que o disco no nó original, algum espaço é deixado sem uso no disco. A operação de BMR não processa automaticamente o espaço em disco não utilizado. É possível formatar o espaço em disco para uma partição separada ou redimensionar a partição

existente com o espaço em disco não utilizado. O volume que você deseja redimensionar não deve estar em uso, por isso, você deve evitar o redimensionamento de um volume do sistema. Nesta seção, o foco será sobre como estender um volume de dados com o espaço em disco não utilizado.

Observação: para evitar a perda de dados, redimensione os volumes imediatamente após o processo de BMR. Também é possível fazer backup do nó antes de iniciar a tarefa de redimensionamento de volume.

Quando o computador de destino reinicia com êxito após a BMR, é possível estender o volume de dados.

Volume de partição bruta

Por exemplo, um disco de 2 GB na sessão é restaurado para um disco de 16 GB nomeado */dev/sdb* com apenas uma partição. A partição bruta */dev/sdb1* é diretamente montada no diretório */data*.

Este exemplo é usado para explicar o procedimento de extensão do volume da partição bruta.

Siga estas etapas:

1. Verifique o status do volume do /dev/sdb1.

   # df –h /dev/sdb1

   /dev/sdb1 2.0G 40M 1.9G 3% /data

2. Desmonte o volume do /dev/sdb1.

   # umount /data

3. Redimensione o /dev/sdb1 para ocupar todo o espaço em disco usando o comando fdisk.

   Para executar esta operação, primeiro exclua suas partições existentes e recrie-as com o mesmo número do setor de inicialização. O mesmo número do setor de inicialização é responsável por evitar a perda de dados.

   # 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

A partição se altera para o mesmo número do setor de inicialização como a partição original e o número do setor de término é 33554431.

4. Redimensione o volume usando o comando resize2fs. Se necessário, execute primeiro o comando e2fsck.

   # e2fsck -f /dev/sdb1

   # resize2fs /dev/sdb1

5. Monte o volume para o ponto de montagem e verifique novamente o status do volume.

   # mount /dev/sdb1 /data

   # df –h /dev/sdb1

   /dev/sdb1 16G 43M 16G 1% /data

   O volume é estendido para 16 GB e está pronto para ser usado.

Volume LVM:

Por exemplo, um disco de 8 GB na sessão é restaurado para um disco de 16 GB nomeado */dev/sdc* com apenas uma partição. A partição bruta */dev/sdc1* é usada como o único volume físico do */dev/mapper/VGTest-LVTest* do volume lógico LVM cujo ponto de montagem é */lvm*.

Esse exemplo é usado para explicar o procedimento de extensão do volume LVM.

Siga estas etapas:

1. Verifique o status do volume /dev/mapper/VGTest-LVTest.

   # lvdisplay –m /dev/mapper/VGTest-LVTest

   --- Logical volume ---

   Nome LV /dev/VGTest/LVTest

   Nome VG VGTest

   UUID LV udoBIx-XKBS-1Wky-3FVQ-mxMf-FayO-tpfPl8

   Acesso de gravação LV leitura/gravação

   Status LV disponível

   número abertura 1

   Tamanho LV 7.88 GB

   LE atual 2018

   Segmentos 1

   Herdar alocação

   Ler setores à frente 0

   Dispositivo de bloco 253:2

   ---Segmentos---

   Extensão lógica de 0 a 2017:

   Type linear

   Volume físico /dev/sdc1

   Extensão física 0 a 2017

   O volume físico é */dev/sdc1*, o grupo do volume é *VGTest* e o volume lógico é */dev/VGTest/LVTest or /dev/mapper/VGTest-LVTest*.

2. Desmonte o volume /dev/mapper/VGTest-LVTest volume.

   # umount /lvm

3. Desative o grupo do volume no qual o volume físico /dev/sdc1 está localizado.

   # vgchange -a n VGTest

4. Crie uma partição para ocupar o espaço em disco não utilizado usando o 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

   A partição /dev/sdc2 é criada.

5. Crie um novo volume físico.

   # pvcreate /dev/sdc2

6. Estenda o tamanho do grupo do volume.

   # vgextend VGTest /dev/sdc2

7. Ative o grupo do volume que você já havia desativado.

   # vgchange -a y VGTest

8. Estenda o tamanho do volume lógico usando o comando lvextend.

   # lvextend -L +8G /dev/VGTest/LVTest

9. Redimensione o volume usando o comando resize2fs. Se necessário, execute primeiro o comando e2fsck.

   # e2fsck -f /dev/mapper/VGTest-LVTest

   # resize2fs /dev/mapper/VGTest-LVTest

10. Monte o volume para o ponto de montagem e verifique novamente o status do volume.

    # mount /dev/mapper/VGTest-LVTest /lvm

    # lvdisplay -m /dev/mapper/VGTest-LVTest

    ---Volume lógico---

    Nome LV /dev/VGTest/LVTest

    Nome VG VGTest

    LV UUID GTP0a1-kUL7-WUL8-bpbM-9eTR-SVzl-WgA11h

    Acesso de gravação LV leitura/gravação

    Status LV disponível

    número abertura 0

    Tamanho LV 15.88 GB

    LE atual 4066

    Segmentos 2

    Herdar alocação

    Ler setores à frente 0

    Dispositivo de bloco 253:2

    --- Segments ---

    Extensão lógica de 0 a 2046:

    Type linear

Volume físico /dev/sdc1

Extensão física 0 a 2046

Extensão lógica de 2047 a 4065:

Type linear

Volume físico /dev/sdc2

Extensão física 0 a 2018

O volume LVM é estendido para 16 GB e está pronto para ser usado.

Verificar se o nó de destino foi restaurado

Após a conclusão da tarefa de restauração, verifique se o nó de destino foi restaurado com os dados relevantes.

Siga estas etapas:

1. Navegue para o computador de destino que você restaurou.
2. Verifique se o computador de destino possui todas as informações incluídas no backup.

   O computador de destino é verificado com êxito.

   A BMR é executada com êxito para computadores Linux.

Como executar uma BMR de migração em computadores Linux

Uma BMR de migração é um processo de duas etapas onde os dados primeiro são restaurados em um computador temporário e, em seguida, no computador real. Uma BMR com a opção de BMR instantânea ativada permite recuperar dados em um computador temporário. É possível usar o computador temporário até que o computador real esteja pronto. Quando você tiver o computador real, uma BMR de migração permite migrar dados do computador temporário para o computador real. Durante a realização de uma BMR de migração, todos os dados que você criar no computador temporário são migrados para o computador real.

Observação: é possível executar a BMR de migração com apenas um backup com base em agente. Um backup sem agente não oferece suporte à BMR de migração.

É possível executar uma BMR usando o endereço IP ou o endereço MAC (Media Access Control – Controle de Acesso à Mídia) do computador de destino. Se você inicializar o computador de destino usando o Live CD do Agente do Arcserve Unified Data Protection para Linux, poderá obter o endereço IP do computador de destino.

Observação: não é possível inicializar o computador. Apenas uma NIC está configurada.

Conclua as tarefas a seguir para executar uma BMR de migração:

- Verifique os pré-requisitos para a BMR de migração
- Executar uma BMR na máquina temporária
- Realizar uma BMR de migração
- Verificar se o computador de destino foi restaurado

Verifique os pré-requisitos para a BMR de migração

Considere as seguintes opções antes de executar uma BMR de migração:

- Você tem um ponto de recuperação válido e a senha de criptografia, se houver, para restauração.
- Você tem um computador de destino válido para a BMR.
- Você criou o Live CD do Agente do Arcserve Unified Data Protection para Linux.
- Se você deseja executar uma BMR usando o endereço IP, deve obter o endereço IP do computador de destino usando o Live CD.
- Se você deseja executar uma BMR com base em PXE usando o endereço MAC, deve ter o endereço MAC do computador de destino.
- O ponto de recuperação deve ser proveniente do backup com base em agente do Linux.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Executar uma BMR para o computador temporário

Antes de realizar uma BMR de migração, você precisa restaurar dados da origem para um computador temporário. Para restaurar os dados temporariamente, é possível executar uma BMR (Bare Metal Recovery – Recuperação Bare-Metal) para o computador temporário. Depois que o computador temporário estiver pronto para uso, é possível continuar trabalhando no computador temporário.

Quando o computador real estiver pronto, você poderá realizar uma BMR de migração do computador temporário para o computador real.

Observação: para obter mais informações sobre como realizar a BMR, consulte o Como executar uma recuperação bare metal (BMR) para máquinas Linux.

Siga estas etapas:

1. Acesse o assistente de restauração com um dos seguintes procedimentos:

   A partir do Arcserve UDP :

   a. Efetue logon no Arcserve UDP.

   b. Clique na guia **Recursos**.

   c. Selecione **Todos os nós** no painel esquerdo.

      Todos os nós do adicionados são exibidos no painel central.

   d. No painel central, selecione o nó do e clique em **Ações**.

   e. Clique em **Restaurar** no menu suspenso **Ações**.

      A interface da web do Agente do Arcserve Unified Data Protection para Linux é exibida. A caixa de diálogo Selecionar tipo de restauração é exibida na interface de usuário do agente.

   f. Selecione o tipo de restauração e clique em **OK**.

      Observação: você será automaticamente conectado ao nó do agente e o **Assistente de restauração** será exibido do nó do agente.

   A partir do Agente do Arcserve Unified Data Protection para Linux :

   a. Abra a interface da web do Agente do Arcserve Unified Data Protection para Linux.

      Observação: durante a instalação do Agente do Arcserve Unified Data Protection para Linux, você recebeu o URL para acessar e gerenciar o servidor.

   b. Efetue logon no Agente do Arcserve Unified Data Protection para Linux.

2. Clique em **Restaurar** no menu **Assistente**, selecione **Recuperação bare metal (BMR)**.

A página **Servidor de backup** do **Assistente de restauração – BMR** é exibida.

3. Forneça todos os detalhes no **Assistente de restauração – BMR** e salve o assistente.
4. Certifique-se de marcar a caixa de seleção **Ativar a BMR instantânea** na página **Computador de destino** do assistente.
5. Certifique-se de marcar a caixa de seleção **Não recuperar os dados automaticamente depois que o computador for iniciado** na página **Computador de destino** do assistente.
6. Execute a tarefa de BMR.

   O computador temporário foi recuperado usando a BMR, com a opção de BMR instantânea ativada. É possível usar o computador temporário até que o computador real esteja pronto.

Realizar uma BMR de migração

Quando o computador real estiver pronto, execute uma BMR de migração. A BMR de migração restaura os dados originais da sessão de backup e os novos dados do computador temporário para o computador real.

Siga estas etapas:

1. Clique em **Restaurar** no menu **Assistente** e selecione **BMR de migração**.

   A página **Servidor de backup** do **Assistente de restauração – BMR de migração** é exibida.

2. Forneça todos os detalhes do **Assistente de restauração – BMR de Migração**.

   Observação: para obter mais informações sobre como realizar a BMR, consulte o Como executar uma recuperação bare metal (BMR) para máquinas Linux.

3. Certifique-se de que as seguintes informações são fornecidas na página **Servidor de Backup** do assistente.

   a. Selecione a tarefa de recuperação de VM instantânea ou a tarefa de BMR instantânea.

      Servidor local

      Especifica que o servidor de backup é gerenciado no local. A tarefa de BMR do computador temporário é executada no servidor local.

      Servidor remoto

      Especifica que o servidor de backup é gerenciado remotamente. A tarefa de BMR do computador temporário é executada no servidor remoto. É necessário fornecer os detalhes do servidor remoto para se estabelecer conexão com o servidor remoto.

   b. Selecione a tarefa de restauração na lista suspensa Nome da tarefa.

      A lista exibe a tarefa de recuperação de VM instantânea ou a tarefa de BMR instantânea, que está na fase da tarefa Pronto para uso ou na fase da tarefa Desligar, quando ela estiver pronta para uso.

4. Salve a tarefa de BMR.

   Na página inicial, a **Fase da tarefa** na guia **Status da tarefa** muda para **Clique aqui para migrar dados**.

5. (Opcional) Inicialize o computador temporário usando um Live CD quando o tipo de tarefa selecionada for BMR instantânea.

6. Na guia **Status da tarefa**, use a opção **Clique aqui para migrar os dados**.

   A migração de dados é iniciada.

Você realizou uma BMR de migração com êxito.

Verificar se o nó de destino foi restaurado

Após a conclusão da tarefa de restauração, verifique se o nó de destino foi restaurado com os dados relevantes.

Siga estas etapas:

1. Navegue para o computador de destino que você restaurou.
2. Verifique se o computador de destino possui todas as informações do computador temporário, incluindo os novos dados criados no computador temporário.

   O computador de destino é verificado com êxito.

   A BMR de migração é executada com êxito para computadores Linux com base em agente.

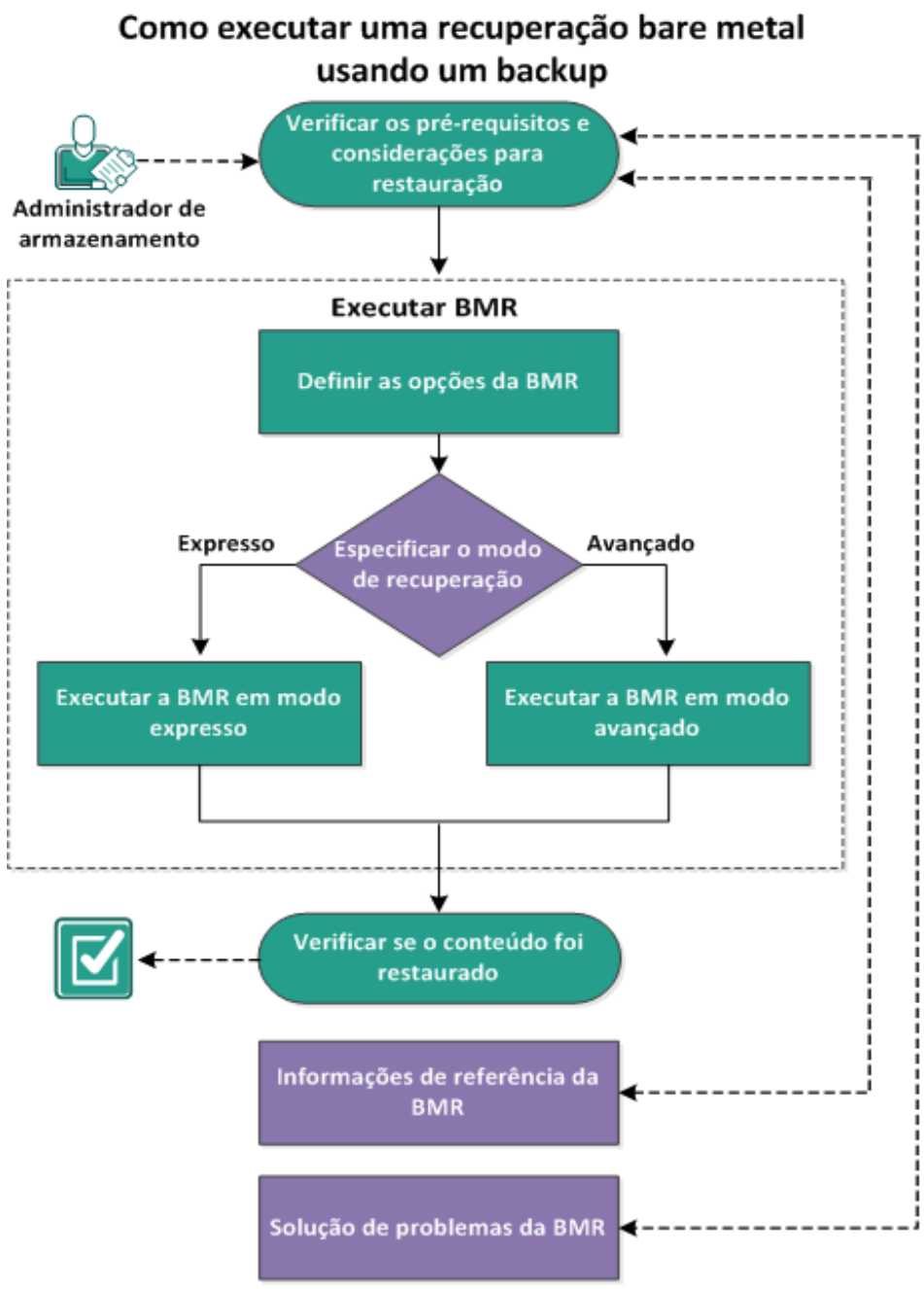
Como executar uma BMR usando um backup

A BMR (Bare Metal Recovery - Recuperação Bare Metal) é o processo de restauração de um sistema de computador a partir do estado bare metal, incluindo a reinstalação do sistema operacional e dos aplicativos de software e, em seguida, a restauração dos dados e das configurações. O processo de BMR permite a restauração completa de um computador com o mínimo de esforço, até mesmo para um hardware diferente. A BMR é possível porque durante o processo de backup em nível de bloco, o agente do Arcserve UDP (Windows) não captura apenas os dados, mas também todas as informações relacionadas aos seguintes aplicativos:

- Sistema operacional
- Aplicativos instalados
- Configurações
- Drivers necessários

Para todas as informações relevantes, necessárias à execução de uma recompilação completa do sistema a partir do estado bare metal, é feito backup em uma série de blocos, os quais são armazenados no local do backup.

O diagrama seguinte ilustra o processo para a realização de uma BMR usando um backup:



Conclua as tarefas a seguir para executar uma BMR usando um backup:

1. Rever os pré-requisitos e considerações da BMR
2. Definir as opções da BMR
   - Executar a BMR em modo expresso
   - Executar a BMR em modo avançado
3. Verificar se a BMR foi bem-sucedida
4. Informações de referência da BMR
5. Solução de problemas da BMR

Rever os pré-requisitos e considerações da BMR

Antes de executar uma BMR, verifique se os seguintes pré-requisitos foram atendidos:

- Você deve possuir uma das seguintes imagens:
  - Uma imagem ISO criada da BMR gravada em um CD/DVD
  - Uma imagem ISO criada da BMR gravada em um dispositivo USB portátil

  Observação: com o agente do Arcserve UDP (Windows), é possível utilizar um Utilitário do kit de Inicialização para combinar uma imagem do WinPE e uma imagem do agente do Arcserve UDP (Windows) para criar uma imagem ISO da BMR. Em seguida, essa imagem ISO é gravada em uma mídia inicializável. Dessa maneira, você pode usar qualquer uma dessas mídias inicializáveis (CD/DVD ou dispositivo USB) para inicializar o novo sistema do computador e permitir que o processo de recuperação bare metal seja iniciado. Para garantir que a imagem salva seja sempre a versão mais atualizada, crie uma nova imagem ISO sempre que você atualizar o agente do Arcserve UDP (Windows).
- Ao menos um backup completo disponível.
- Uma RAM de, pelo menos, 2 GB instalada na máquina virtual e no servidor de origem que você está recuperando.
- Para recuperar máquinas virtuais VMware para máquinas virtuais VMware configuradas para se comportarem como servidores físicos, verifique se o VMware Tools está instalado na máquina virtual de destino.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Revise as seguintes considerações de restauração:

- Independentemente do método usado para criar a imagem do kit de inicialização, o processo de BMR é basicamente o mesmo.

  Observação: não é possível criar espaços de armazenamento por meio do processo de BMR. Se o computador de origem tinha espaço de armazenamento, não será possível criar espaços de armazenamento no computador de destino durante a BMR. Você pode restaurar os volumes em discos/volumes regulares ou criar manualmente espaços de armazenamento antes de executar a BMR e, em seguida, restaurar os dados nesses espaços de armazenamento criados.
- Discos dinâmicos serão restaurados somente no nível do disco. Se o backup dos dados for feito no volume local de um disco dinâmico, você não poderá restaurar este disco durante a BMR. Nesse cenário, para fazer uma restauração

durante uma BMR, é preciso executar uma das tarefas abaixo e, em seguida, realizar a BMR a partir do ponto de recuperação copiado:

- Faça backup em um volume em outra unidade.
- Faça backup em um compartilhamento remoto.
- Copie um ponto de recuperação em outro local.

Observação: se você executar uma BMR com vários discos dinâmicos, ela pode falhar devido a alguns erros inesperados (como falha na inicialização, volumes dinâmicos não reconhecidos e assim por diante). Se isso ocorrer, será necessário restaurar somente o disco do sistema usando a BMR e, em seguida, após a reinicialização do computador, será possível restaurar os outros volumes dinâmicos em um ambiente normal.

- (Opcional) Rever as informações de referência da BMR. Para obter mais informações, consulte os tópicos a seguir:
  - Como a recuperação bare metal funciona
  - Sistemas operacionais que oferecem suporte à conversão de UEFI/BIOS
  - Gerenciando o menu de operações de BMR

Revise as seguintes considerações:

- Se você atualizar para uma versão ou atualização mais recente do Arcserve UDP, deverá recriar o ISO da BMR usando o nível do Windows AIK ou ADK apropriado para incluir suporte para os recursos e as correções de erro mais recentes. No entanto, depois que BMR ISO é criado, o arquivo ISO pode ser usado para o mesmo nível de sistema operacional. Os seguintes níveis de sistema operacional podem usar o mesmo ISO:
  - ISO criado usando o WAIK do Windows 7 – funciona com o Windows 2003, Vista, 2008, 2008 R2
  - ISO criado usando o ADK do Windows 8/8.1 – funciona com o Windows 8, 8.1, Server 2012, Server 2012 R2
  - ISO criado usando o ADK do Windows 10 – funciona com o Windows 10, Windows Server 2016 e Windows Serve 2019

Definir as opções da BMR

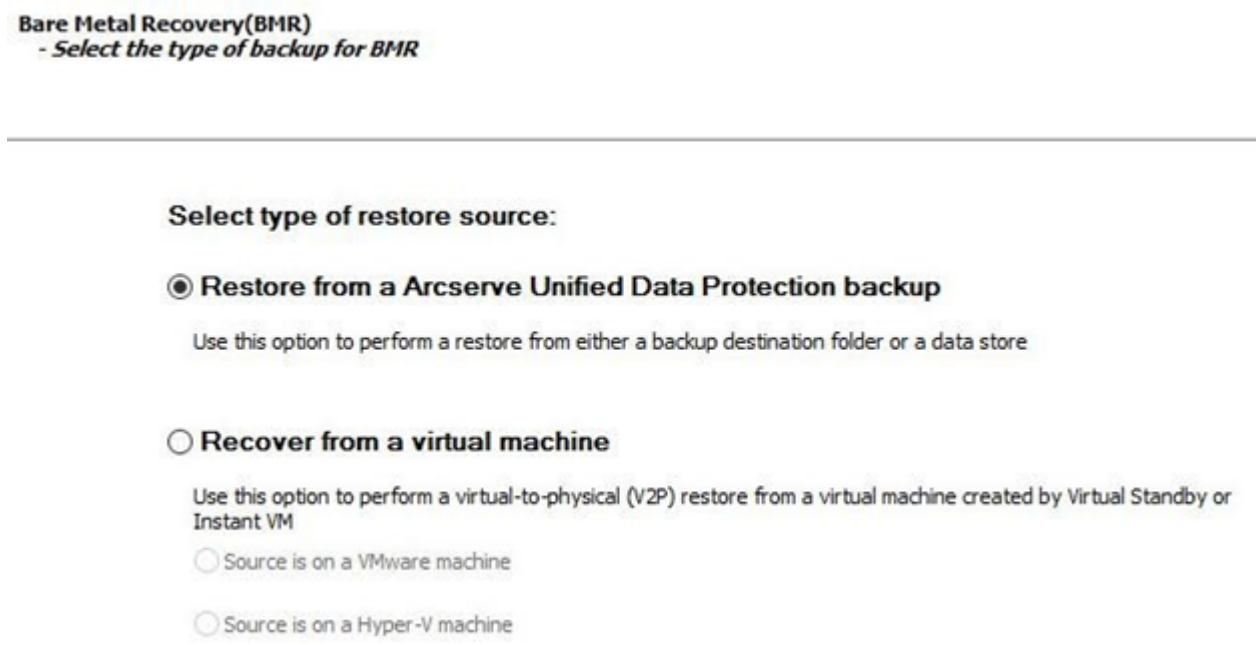
Antes de iniciar o processo da BMR, especifique algumas opções preliminares da BMR.

Siga estas etapas:

1. Insira a mídia da imagem do kit de inicialização salva e inicialize o computador.
   - Se estiver usando uma imagem ISO da BMR gravada em um CD/DVD, insira o CD/DVD.
   - Se estiver usando uma imagem ISO da BMR gravada em um dispositivo USB, insira o dispositivo USB.

   A tela do **Utilitário de instalação do BIOS** é exibida.
2. Na tela do **Utilitário de instalação do BIOS**, selecione a opção da unidade de CD-ROM ou a opção de USB para iniciar o processo de inicialização. Selecione uma arquitetura (x86/x64) e pressione **Enter** para continuar.
3. A tela de seleção de idioma do Agente do Arcserve UDP (Windows) é exibida. Selecione um idioma e clique em **Avançar** para continuar.

O processo de recuperação bare metal é iniciado, e a tela do assistente da BMR inicial é exibida.



A tela do assistente da BMR permite que você selecione o tipo de BMR que deseja executar:

- **Restaurar a partir de um backup do Arcserve Unified Data Protection**

  Use essa opção para executar uma restauração a partir de uma pasta de destino do backup ou de um repositório de dados.

  Essa opção permite recuperar dados cujo backup foi feito usando o Agente do Arcserve UDP (Windows). Essa opção é usada junto com sessões de backup realizadas com o Agente do Arcserve UDP (Windows) ou com o aplicativo de backup de VM com base em host do Arcserve UDP.

  Se selecionar essa opção, continue este procedimento a partir daqui.

- **Recuperar a partir de uma máquina virtual**

  Use essa opção para executar uma restauração V2P (Virtual-to-Physical – Virtual para Física) de uma VM no modo de espera virtual. V2P (Virtual-to-Physical) é um termo que se refere à migração de um SO (Sistema Operacional), aplicativos e dados de uma de máquina virtual ou partição de disco para o disco rígido principal de um computador. O destino pode ser um único computador ou vários computadores.

- **A origem está em uma máquina VMware**

  Permite recuperar dados de uma máquina cuja conversão virtual é executada em uma máquina virtual do VMware. Essa opção é usada junto com o aplicativo do Arcserve Central Virtual Standby.

  Observação: para essa opção, só é possível recuperar dados se a conversão virtual para um arquivo VMDK (para VMware) foi executada usando o Arcserve Central Virtual Standby.

  Se selecionar essa opção, consulte o tópico Recuperar usando uma VM no modo de espera virtual do VMware para continuar com este procedimento.

  Para obter mais informações, consulte Recuperar usando uma VM no modo de espera virtual do VMware na ajuda online do Agente para Windows.

- **A origem está em uma máquina Hyper-V**

  Permite recuperar dados de uma máquina virtual cuja conversão é executada em uma máquina virtual do Hyper-V. Essa opção é usada junto com o aplicativo do Arcserve Central Virtual Standby.

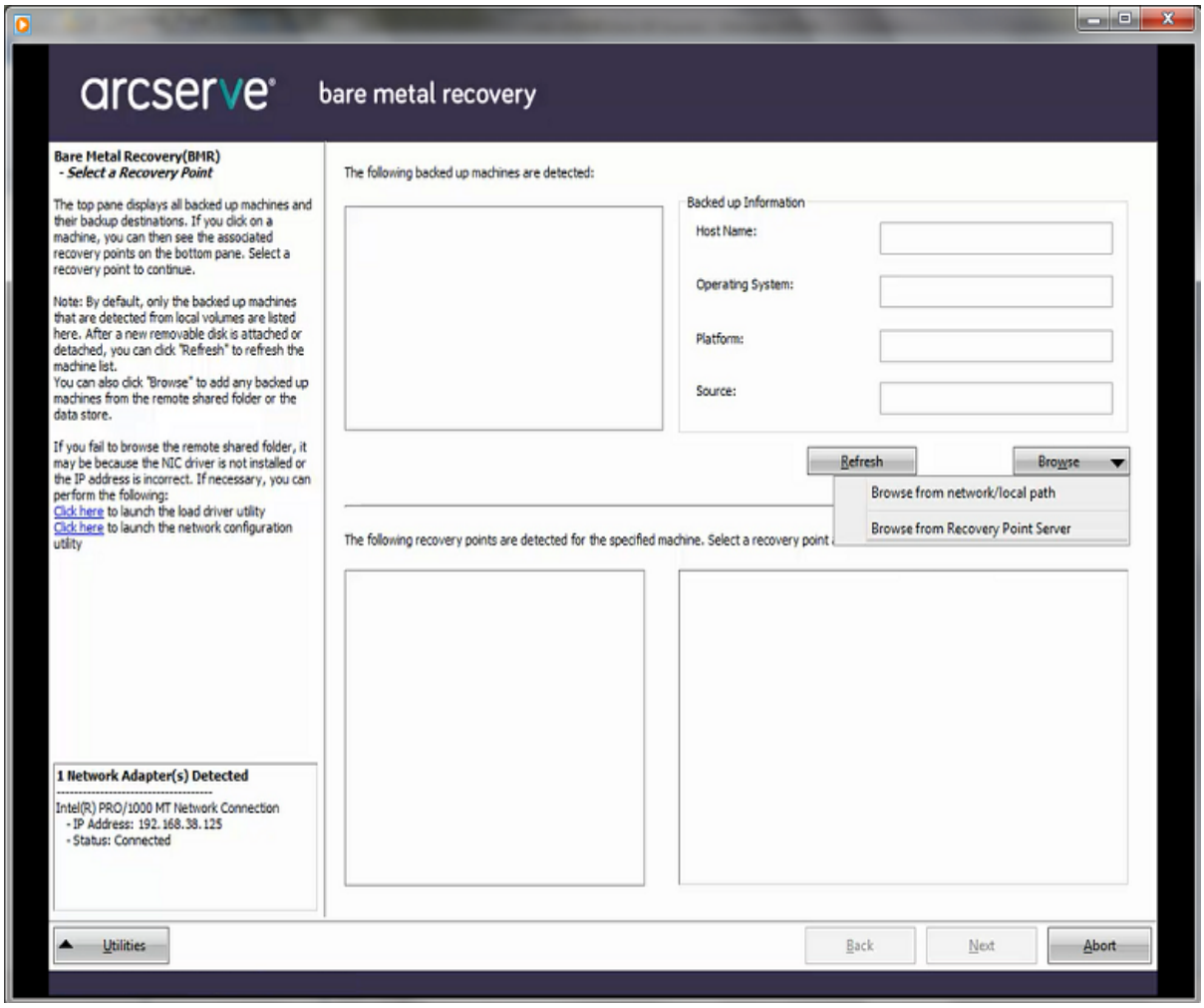
  Observação: para essa opção, só é possível recuperar dados se a conversão virtual para um arquivo VHD (para Hyper-V) foi executada usando o Arcserve Central Virtual Standby.

  Se selecionar essa opção, consulte o tópico Recuperar usando uma VM no modo de espera virtual do Hyper-V para continuar com este procedimento.

  Para obter mais informações, consulte Recuperar usando uma VM no modo de espera virtual do Hyper-V na ajuda online do Agente para Windows.

4. Selecione **Restaurar de um backup do Arcserve Unified Data Protection** e clique em **Avançar**.

   A tela do assistente **Selecionar um ponto de recuperação** é exibida.



5. Na tela do assistente **Selecionar ponto de recuperação**, clique em **Procurar** e selecione **Procurar na rede/caminho local** ou selecione **Procurar no Servidor de ponto de recuperação**.

    a. Se escolher **Procurar** na rede/caminho local, selecione o computador (ou volume) que contenha os pontos de recuperação para sua imagem do backup.

    O Agente do Arcserve UDP (Windows) permite a recuperação a partir de uma unidade local ou de um compartilhamento de rede.

    - Se você estiver recuperando a partir de um backup local, o assistente de BMR detectará e exibirá automaticamente todos os volumes contendo pontos de recuperação.
    - Caso esteja fazendo uma recuperação a partir de um compartilhamento remoto, procure o local remoto em que os pontos de recuperação estão armazenados. Se houver vários computadores contendo pontos de recuperação, todos eles serão exibidos.

Você também pode precisar acessar informações (nome de usuário e senha) para o computador remoto.

Observação: a rede deve estar em funcionamento para procurar pontos de recuperação. Se necessário, você pode verificar e atualizar as informações de configuração de rede ou carregar qualquer driver ausente do menu Utilitários.

- Se o módulo de BMR não puder detectar nenhum volume de destino local, a caixa de diálogo **Selecionar uma pasta** será exibida automaticamente. Forneça o compartilhamento remoto em que os backups residem.
- Se estiver restaurando a partir de um destino iSCSI, o módulo de BMR poderá não detectar esse destino e será necessário fazer o seguinte:

  1. Clique em **Utilitários** e selecione **Executar** no menu pop-up, digite **cmd** e, em seguida, clique em **OK**.

  2. Na janela de prompt de comando, use os comandos iSCSI do Windows a seguir para configurar as conexões iSCSI:

  > net start msiscsi

  > iSCSICLI QAddTargetPortal <TargetPortalAddress>

  > iSCSICLI QLoginTarget <TargetName > [CHAP username] [CHAP password]

  Observação: CHAP=Challenge-Handshake Authentication Protocol

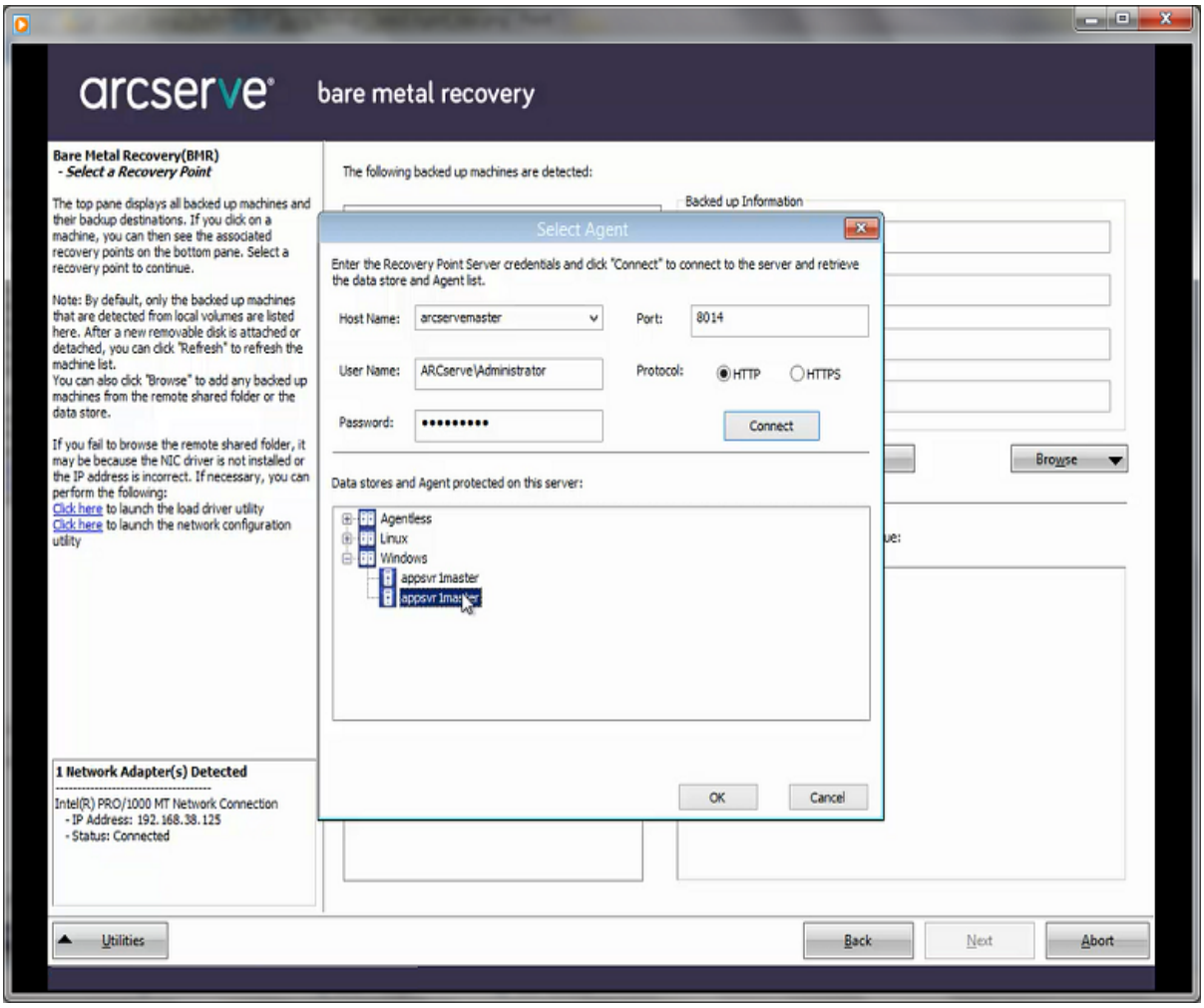
  Para obter mais informações sobre as opções de linha de comando do iSCSI do Windows, consulte este link.

  Observação: etapas extras podem ser necessárias, dependendo do software de destino iSCS que está sendo usado. Para obter mais informações, consulte o manual do software de destino iSCSI.

  3. Na tela de BMR, os discos/volumes conectados ao disco iSCSI devem ser exibidos. O disco iSCSI pode agora ser usado como volume de origem ou o volume de destino de backup.

  Observação: a BMR não oferece suporte a situação na qual o sistema operacional foi instalado em um disco iSCSI. Somente discos de dados são suportados.

b. Se selecionar **Procurar o Servidor de ponto de recuperação**, a caixa de diálogo **Selecionar agente** é exibida. Forneça o **nome do host do servidor de ponto de recuperação**, **nome de usuário**, **senha**, **porta** e **protocolo**. Clique em **Conectar**.



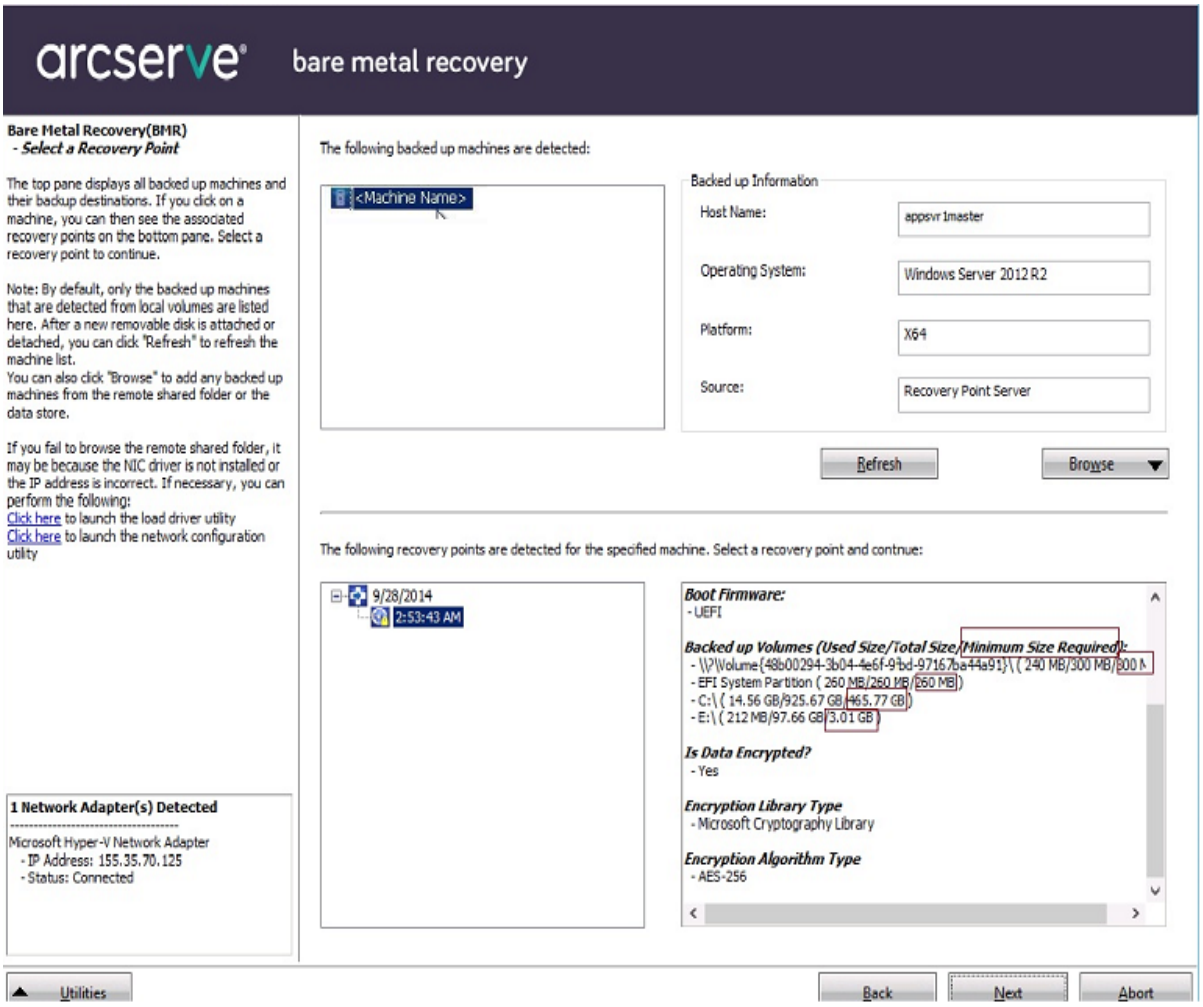
6. Selecione a pasta ou o nome do agente em Repositório de dados onde estão armazenados os pontos de recuperação para o backup e clique em **OK**.

   A tela do assistente de BMR agora exibe as seguintes informações:

   - Nome da máquina (no painel superior à esquerda).
   - Informações relacionadas ao backup (no painel superior à direita).
   - Todos os pontos de recuperação correspondentes (no painel inferior à esquerda).

     Observação: para sistemas operacionais com suporte, é possível realizar uma BMR a partir de um backup executado em um computador UEFI para um computador compatível com o BIOS e a partir de um computador BIOS para um computador compatível com a UEFI. Consulte Sistemas operacionais que oferecem suporte à conversão de UEFI/BIOS para obter uma lista completa de sistemas de conversão de firmware com suporte.

- Em sistemas operacionais que não oferecem suporte à conversão de firmware, para executar uma BMR para um sistema UEFI, você deve inicializar o computador no modo UEFI. A BMR não oferece suporte a restauração de um computador com firmware diferente. Para verificar se o firmware de inicialização é UEFI e não BIOS, clique em **Utilitários**, **Sobre**.
- Em sistemas operacionais que oferecem suporte à conversão de firmware, após selecionar um ponto de recuperação, e se for detectado que o computador de origem não é o mesmo firmware que seu sistema, você será indagado se deseja converter a UEFI em um sistema compatível com o BIOS ou o BIOS em um sistema compatível com a UEFI.

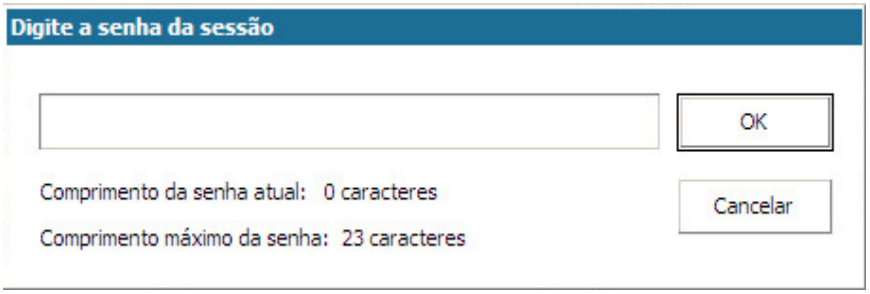


Observação: o Arcserve UDP Versão 5.0 Atualização 2 oferece suporte à BMR em um disco menor apenas quando as sessões são submetidas a backup a partir do Arcserve UDP Versão 5.0 Atualização 2. Consulte o campo **Tamanho mínimo necessário** para o tamanho do disco de destino. A BMR para um disco menor só é suportada no **Modo avançado**.

7. Selecione o ponto de recuperação a ser restaurado.

As informações relacionadas ao ponto de recuperação selecionado são exibidas (no painel inferior à direita). Essa exibição inclui informações como o tipo de backup executado (e salvo), o destino do backup e os volumes incluídos no backup.

Se o ponto de recuperação contiver sessões criptografadas (o ícone de relógio do ponto de recuperação terá um cadeado), uma tela de senha obrigatória será exibida. Digite a senha da sessão e clique em **OK**.



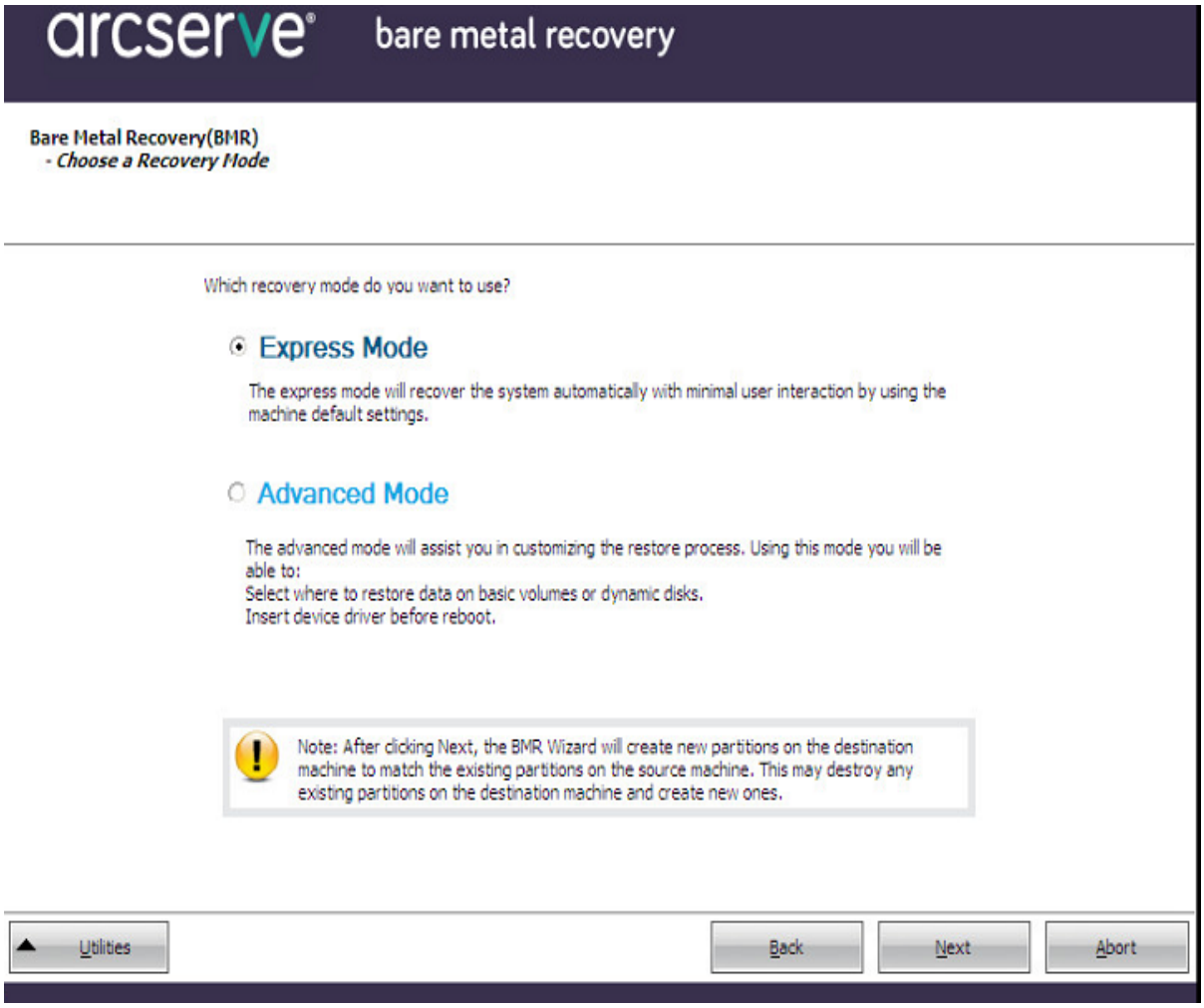
Observações:

se você estiver fazendo a restauração a partir de um servidor de ponto de recuperação do Arcserve UDP, será solicitada uma senha de sessão.

Se seu computador for um controlador de domínio, o Agente do Arcserve UDP (Windows) oferece suporte a uma restauração não autoritativa do arquivo de banco de dados do AD (Active Directory) durante a BMR. (Não há suporte para restauração de agrupamentos do MSCS).

8. Verifique o ponto de recuperação que deseja restaurar e clique em **Avançar**.

   Uma tela do assistente de BMR é exibida com as opções disponíveis do modo de recuperação.



As opções disponíveis são **Modo avançado** e **Modo expresso**.

- Selecione Modo expresso se desejar o mínimo de interação durante o processo de recuperação.
- Selecione Modo avançado se desejar personalizar o processo de recuperação.

  Padrão: Modo expresso.

Executar a BMR em modo expresso

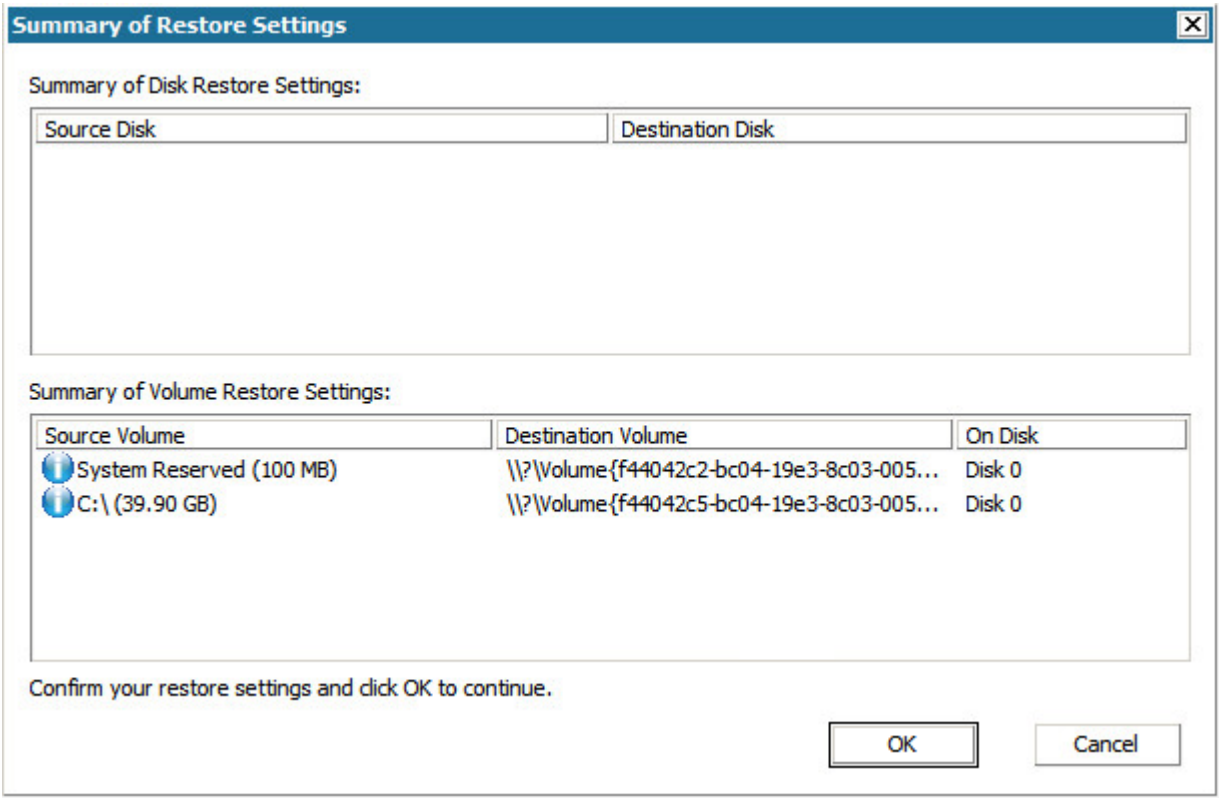
O Modo expresso requer pouca interação durante o processo de recuperação.

Siga estas etapas:

1. Na caixa de diálogo **Selecionar um modo de recuperação**, selecione o **Modo expresso** e clique em **Avançar**.

   A tela **Resumo das configurações de restauração do disco** é exibida, mostrando um resumo dos volumes a serem restaurados.

   Observação: na parte inferior da janela de resumo da restauração, as letras de unidade listadas na coluna **Volume de destino** são geradas automaticamente do WinPE (Windows Preinstallation Environment – Ambiente de Pré-Instalação do Windows). Elas podem ser diferentes das letras das unidades listadas na coluna **Volume de origem**. No entanto, os dados serão restaurados no volume apropriado, mesmo quando as letras forem diferentes.



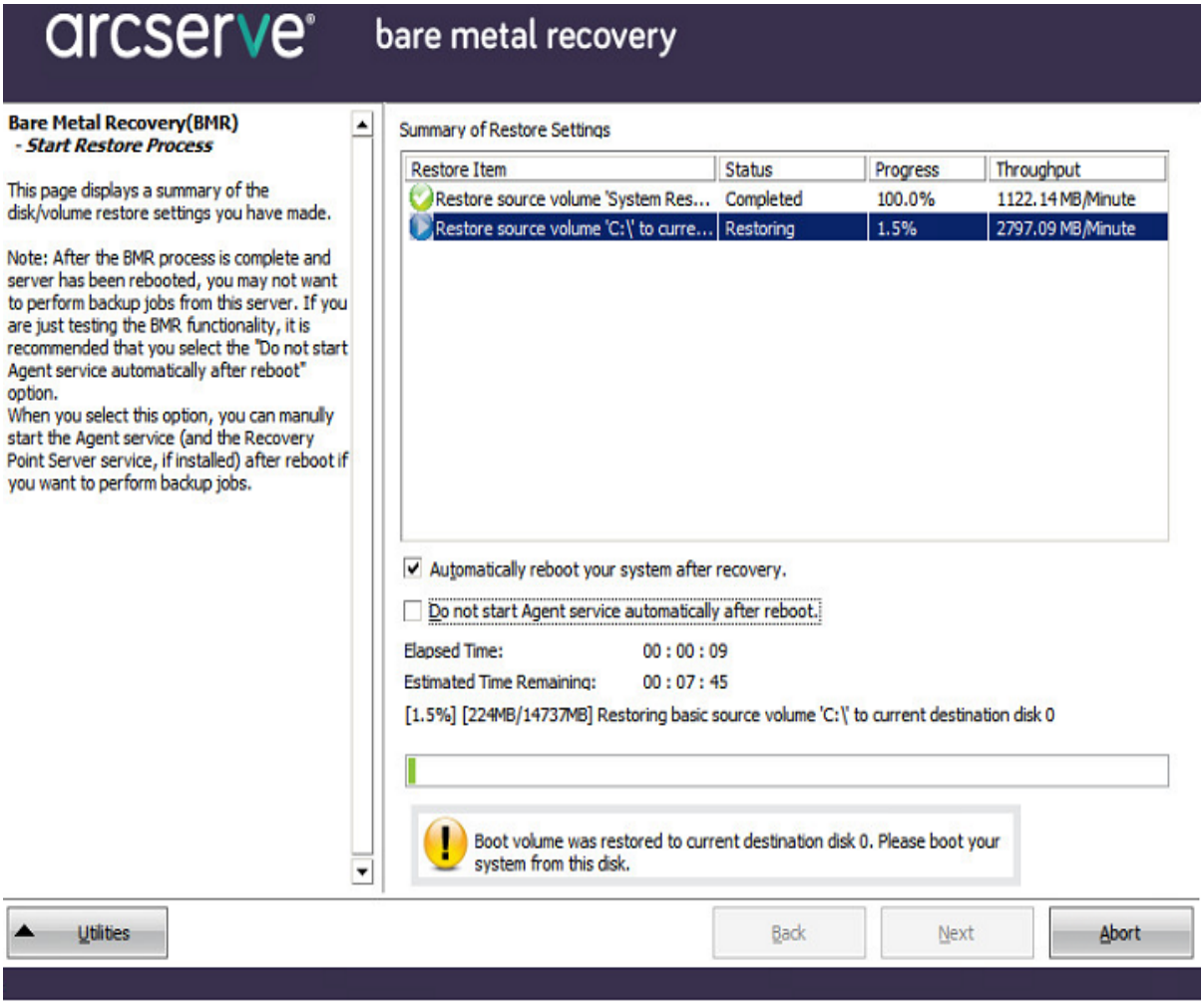
2. Após verificar se as informações de resumo estão corretas, clique em **OK**.

   O processo de restauração é iniciado. A tela do assistente de BMR exibe o status da restauração para cada volume.

   - Dependendo do tamanho do volume sendo restaurado, essa operação pode levar algum tempo.

- Durante este processo, você estará restaurando bloco por bloco tudo o que tiver sido armazenado em backup para esse ponto de recuperação e criando uma réplica do computador de origem no computador de destino.
- Por padrão, a opção que permite reiniciar o sistema automaticamente depois da recuperação é selecionada. Se necessário, você pode desmarcar esta opção e reinicializar manualmente mais tarde.

  Importante: Se estiver executando uma restauração autoritativa de um Active Directory após BMR, é necessário desmarcar a opção **Reiniciar o sistema automaticamente depois da recuperação** e, para obter mais informações, consulte Como realizar uma restauração autoritativa de um Active Directory após BMR.
- Se necessário, é possível selecionar Do not start Agent service automatically after reboot.
- Se necessário, é possível cancelar ou anular a operação a qualquer momento.



3. No menu **Utilitários**, é possível acessar o **Log de atividades** da BMR e usar a opção **Salvar** para salvar o Log de atividades.

   Por padrão, o log de atividades será salvo no seguinte local:

   X:\windows\system32\dr\log

   Observação: para evitar um erro gerado pelo Windows, não salve o Log de atividades na área de trabalho ou crie uma pasta na área de trabalho usando a opção **Salvar como**, na janela Log de atividades da BMR.

4. Caso esteja restaurando em diferentes tipos de hardware (o adaptador SCSI/FC usado para conectar unidades de disco rígido pode ter sido alterado) e nenhum driver compatível tenha sido detectado no sistema original, uma página de injeção de drivers será exibida para permitir o fornecimento de drivers a esses dispositivos.

   Procure e selecione os drivers a serem injetados no sistema recuperado de forma que, mesmo se estiver fazendo a recuperação em um computador com tipos diferentes de hardware, ainda seja possível trazer o computador de volta após a BMR.

   Quando o processo de BMR for concluído, uma notificação de confirmação é exibida.

Executar a BMR em modo avançado

A opção **Modo Avançado** permite personalizar o processo de recuperação.

Siga estas etapas:

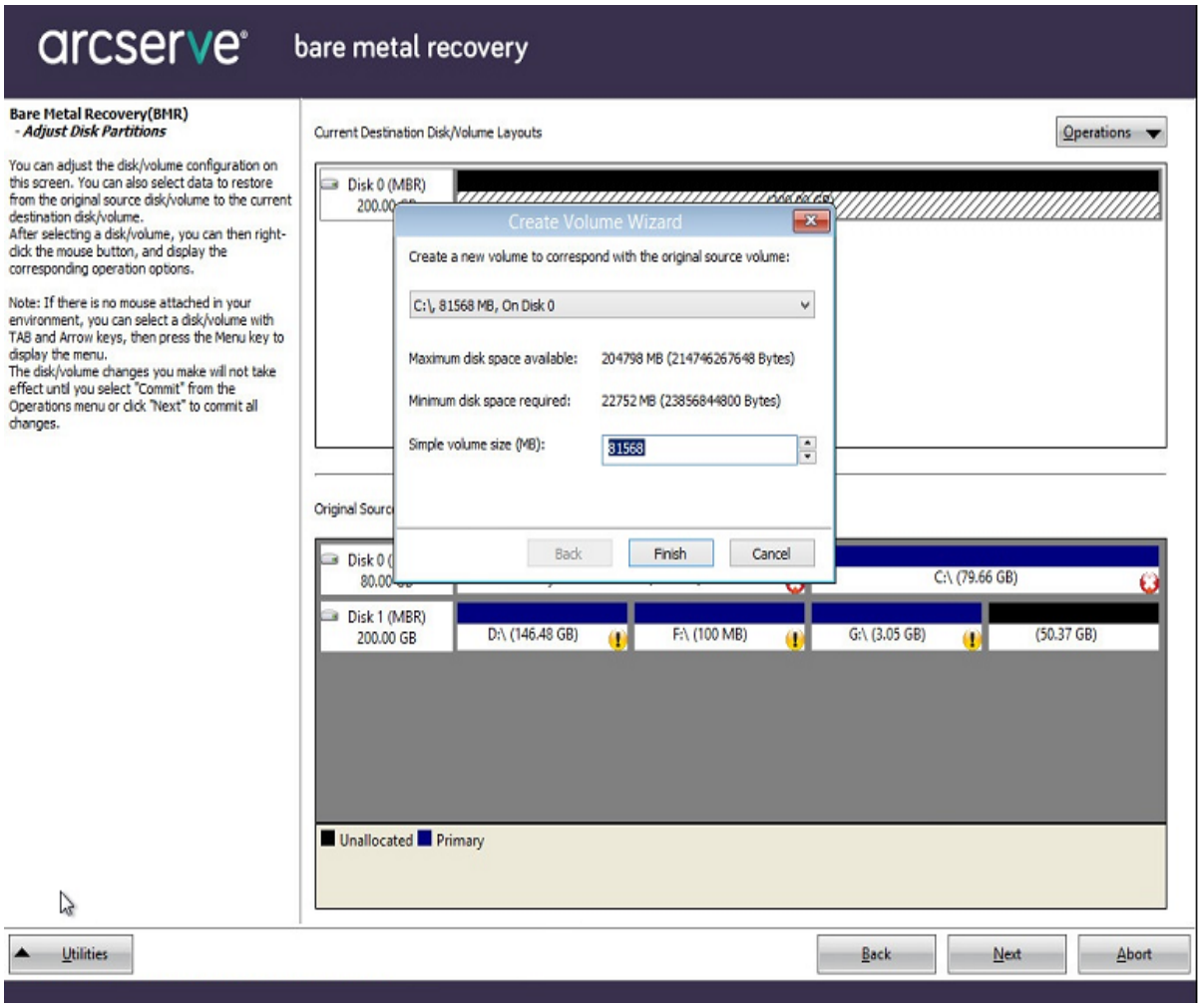
1. Na caixa de diálogo **Selecionar um modo de recuperação**, selecione **Modo avançado** e clique em **Avançar**.

   O utilitário BMR inicia localizando o computador a ser recuperado e exibe as informações da partição de disco correspondente.

   O painel superior mostra a configuração de disco que você possui no computador atual (destino) e o painel inferior mostra as informações da partição de disco que havia no computador original (origem).

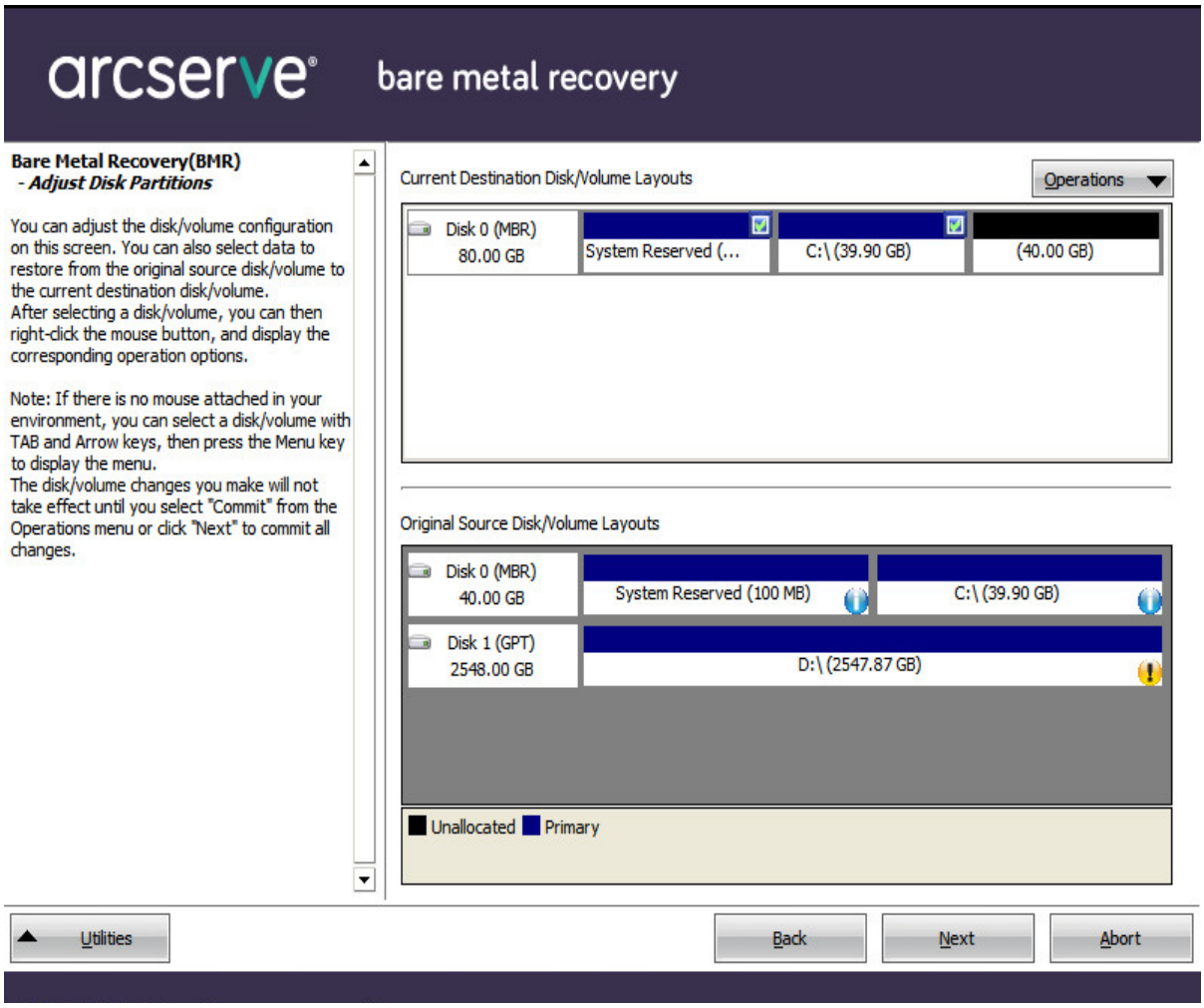
   Importante: um ícone vermelho em forma de X exibido para um volume de origem no painel inferior indica que o volume contém informações do sistema e não foi atribuído (mapeado) ao volume de destino. O volume contendo informações do sistema do disco de origem deve ser atribuído ao disco de destino e restaurado durante a BMR, caso contrário, haverá falha na reinicialização.

   Você pode criar volumes em um disco menor com base no **Mínimo de espaço em disco exigido** que é sugerido. No exemplo, o tamanho do volume original é de 81568 MB. Ao criar o volume no disco de destino, o tamanho mínimo sugerido é de 22752 MB. Nesse caso, é possível criar o volume original com um tamanho de 22752 MB.



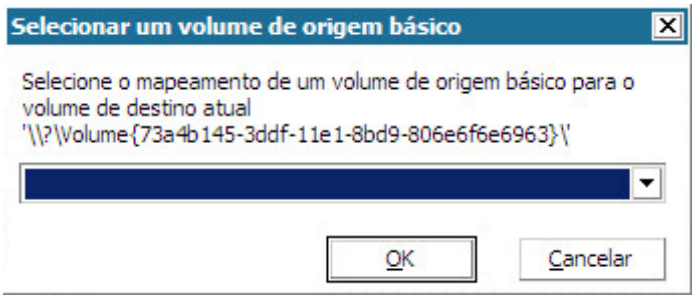
Observação: se executar a BMR e restaurar o volume do sistema em um disco que não está configurado como disco de inicialização, haverá falha ao iniciar o computador após o término da BMR. Verifique se está restaurando o volume do sistema em um disco de inicialização configurado corretamente.

Observação: ao restaurar em outro disco/volume, a capacidade do novo disco/volume pode ter o mesmo tamanho, ser maior do que o disco/volume original ou ser menor que o disco/volume original. Além disso, o redimensionamento do volume não se aplica a discos dinâmicos.



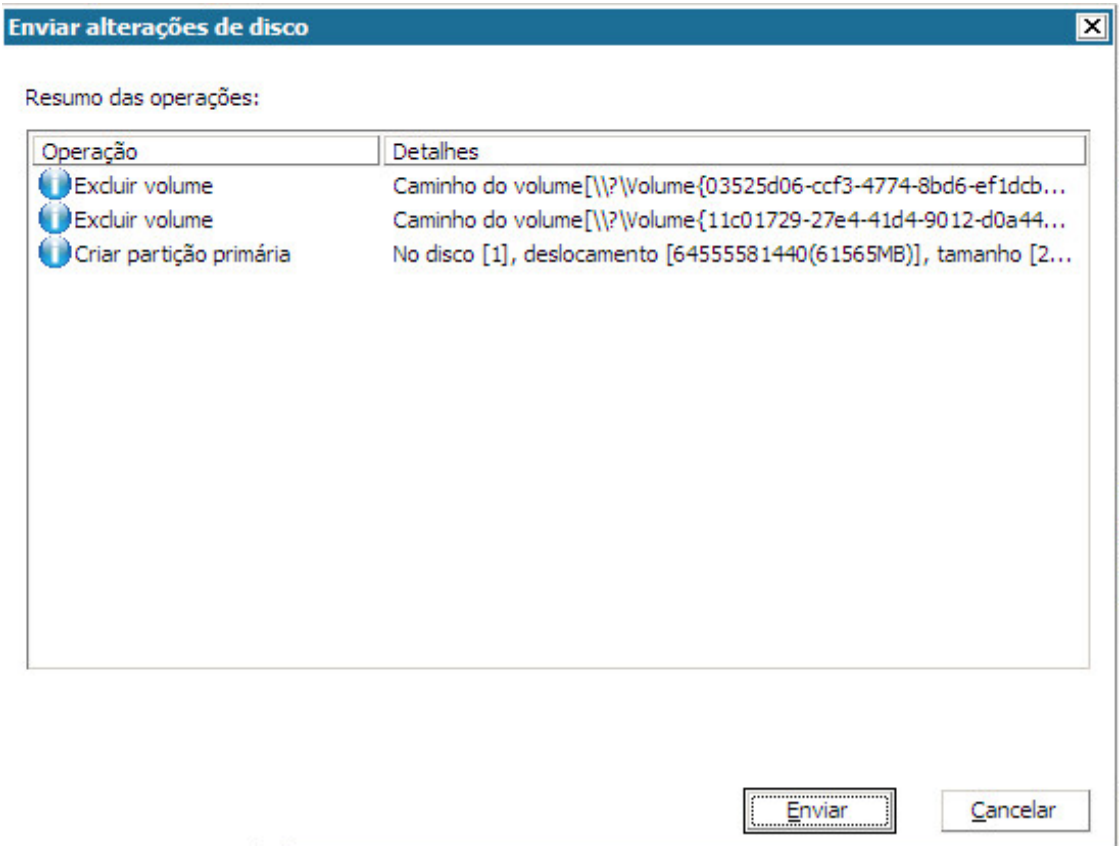
2. Se as informações do disco atual que você estiver vendo não parecerem corretas, acesse o menu **Utilitários** e verifique se há drivers ausentes.
3. Se necessário, no painel de disco/volume de destino, é possível clicar no menu suspenso **Operações** para exibir as opções disponíveis. Para obter mais informações sobre essas opções, consulte Gerenciando o menu operações de BMR.
4. Clique em cada volume de destino e, no menu pop-up, selecione a opção **Mapear volume de** para atribuir um volume de origem a esse volume de destino.

   A caixa de diálogo **Selecionar um volume de origem básico** é exibida.



5. Na caixa de diálogo **Selecionar um volume de origem básico**, clique no menu suspenso e selecione o volume de origem disponível para atribuí-lo ao volume de destino selecionado. Clique em **OK**.
   - No volume de destino, um ícone de marca de seleção é exibido, indicando que o volume de destino foi mapeado.
   - No volume de origem, o ícone em forma de X vermelho muda para verde, indicando que o volume de origem foi atribuído a um volume de destino.
6. Quando tiver certeza de que todos os volumes que desejar restaurar e todos os volumes que contêm informações do sistema foram atribuídos a um volume de destino, clique em **Avançar**.

   A tela **Enviar alterações de disco** é exibida, mostrando um resumo das operações selecionadas. Para cada novo volume criado, são exibidas as informações correspondentes.



7. Ao confirmar se as informações de resumo estão corretas, clique em **Enviar**. (Se as informações não estiverem corretas, clique em **Cancelar**).

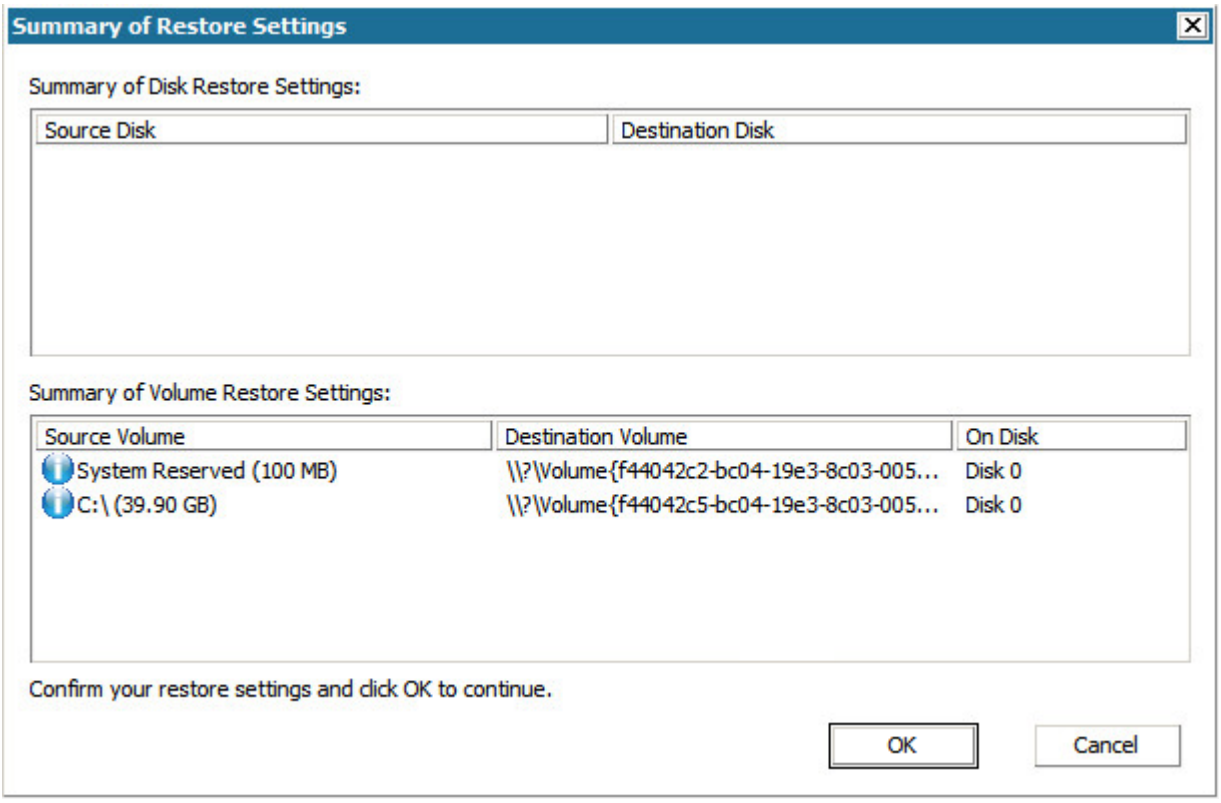
   Observação: as operações no disco rígido não entrarão em vigor até que sejam enviadas.

No computador de destino, os novos volumes são criados e mapeados para o computador de origem correspondente.

8. Quando as alterações forem concluídas, clique em **OK**.

   A tela Resumo das configurações de restauração do disco é exibida, mostrando um resumo dos volumes a serem restaurados.

   Observação: na parte inferior da janela de resumo da restauração, as letras de unidade listadas na coluna Volume de destino são geradas automaticamente no WinPE (Windows Preinstallation Environment - Ambiente de Pré-Instalação do Windows). Elas podem ser diferentes das listadas na coluna Volume de origem. No entanto, os dados serão restaurados no volume apropriado, mesmo quando as letras forem diferentes.



9. Após verificar se as informações de resumo estão corretas, clique em **OK**.

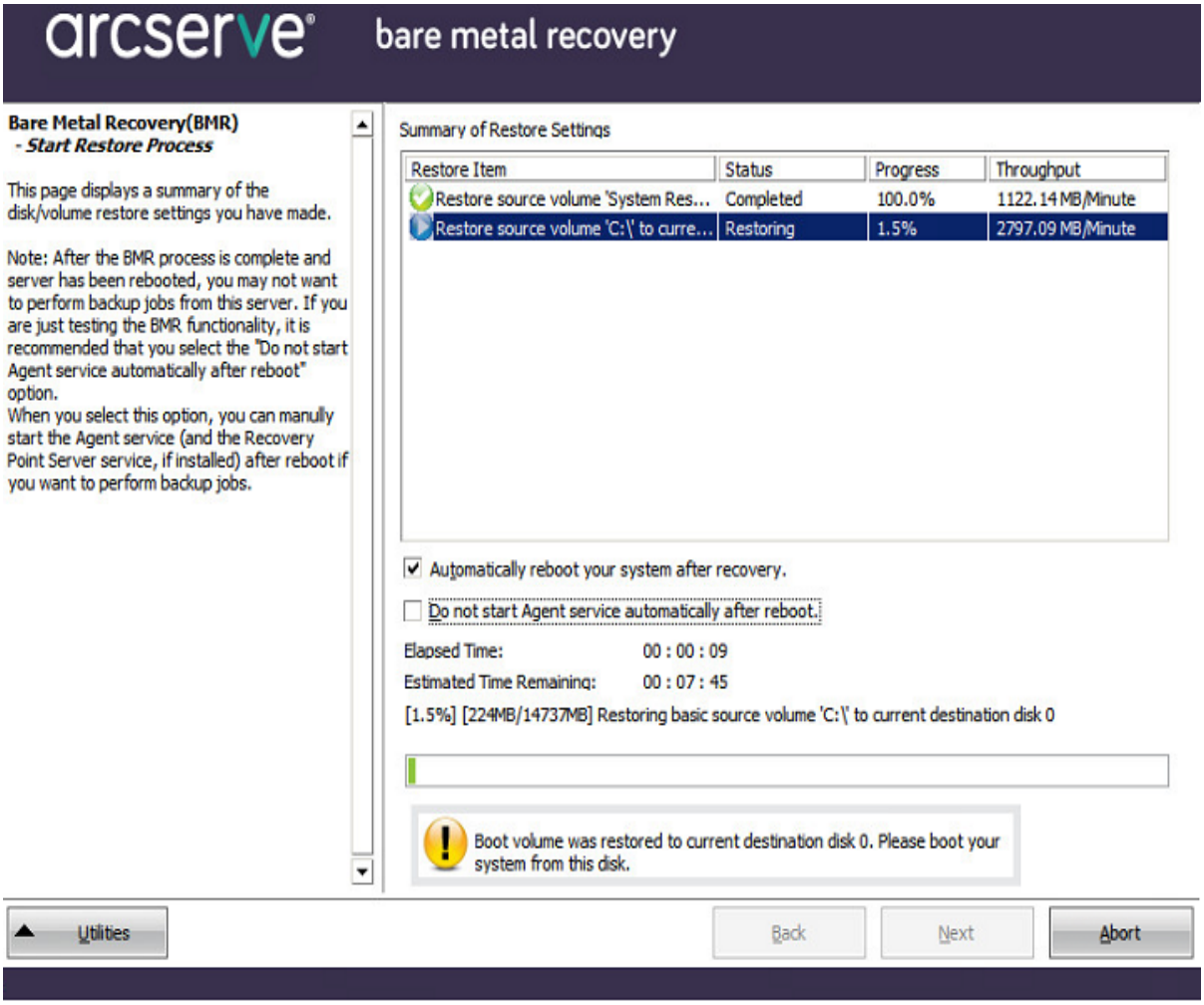
   O processo de restauração é iniciado. A tela do assistente de BMR exibe o status da restauração para cada volume.

   - Dependendo do tamanho do volume sendo restaurado, essa operação pode levar algum tempo.
   - Durante este processo, você estará restaurando bloco por bloco tudo o que tiver sido armazenado em backup para esse ponto de recuperação e criando uma réplica do computador de origem no computador de destino.

- Por padrão, a opção que permite reiniciar o sistema automaticamente depois da recuperação é selecionada. Se necessário, você pode desmarcar esta opção e reinicializar manualmente mais tarde.

  Importante: Se estiver executando uma restauração autoritativa de um Active Directory após BMR, é necessário desmarcar a opção **Reiniciar o sistema automaticamente depois da recuperação** e, para obter mais informações, consulte Como realizar uma restauração autoritativa de um Active Directory após BMR.

- Se necessário, é possível selecionar Do not start Agent service automatically after reboot.
- Se necessário, é possível cancelar ou anular a operação a qualquer momento.



10. No menu **Utilitários**, é possível acessar o **Log de atividades** da BMR e usar a opção **Salvar** para salvar o Log de atividades.

    Por padrão, o log de atividades será salvo no seguinte local:

X:\windows\system32\dr\log.

Observação: para evitar um erro gerado pelo Windows, não salve o Log de atividades na área de trabalho ou crie uma pasta na área de trabalho usando a opção **Salvar como**, na janela **Log de atividades** da BMR.

11. Caso esteja restaurando em diferentes tipos de hardware (o adaptador SCSI/FC usado para conectar unidades de disco rígido pode ter sido alterado) e nenhum driver compatível tenha sido detectado no sistema original, uma página de injeção de drivers será exibida para permitir o fornecimento de drivers a esses dispositivos.

    Procure e selecione os drivers a serem injetados no sistema recuperado de forma que, mesmo se estiver fazendo a recuperação em um computador com tipos diferentes de hardware, ainda seja possível trazer o computador de volta após a BMR.

12. Quando o processo de BMR for concluído, uma notificação de confirmação é exibida.

Verificar se a BMR foi bem-sucedida

Para verificar se a BMR foi concluída com êxito, execute as seguintes tarefas:

- Reinicie o sistema operacional.
- Verifique se todos os sistemas e aplicativos funcionam corretamente.
- Verifique se todas as configurações de rede foram configuradas corretamente.
- Verifique se a BIOS está configurada para inicializar a partir do disco no qual o volume de inicialização foi restaurado.
- Quando a BMR for concluída lembre-se das seguintes condições:
  - O primeiro backup realizado depois da BRM é um backup de verificação.
  - Após a reinicialização do computador, talvez seja necessário configurar os adaptadores de rede manualmente caso você tenha restaurado em um hardware diferente.

    Observação: Quando o computador for reinicializado, uma tela de recuperação de erro do Windows pode ser exibida indicando que o Windows não foi desligado corretamente. Se isso ocorrer, você poderá ignorar esse aviso com segurança e continuar para iniciar o Windows normalmente.
  - Para discos dinâmicos, se o status do disco for offline, é possível alterá-lo manualmente para online na interface de gerenciamento de disco (acessado executando o utilitário de controle Diskmgmt.msc).
  - Para discos dinâmicos, se os volumes dinâmicos estiverem em um status de falha de redundância, é possível sincronizar novamente os volumes na interface de gerenciamento de disco (acessado usando o utilitário de controle Diskmgmt.msc).

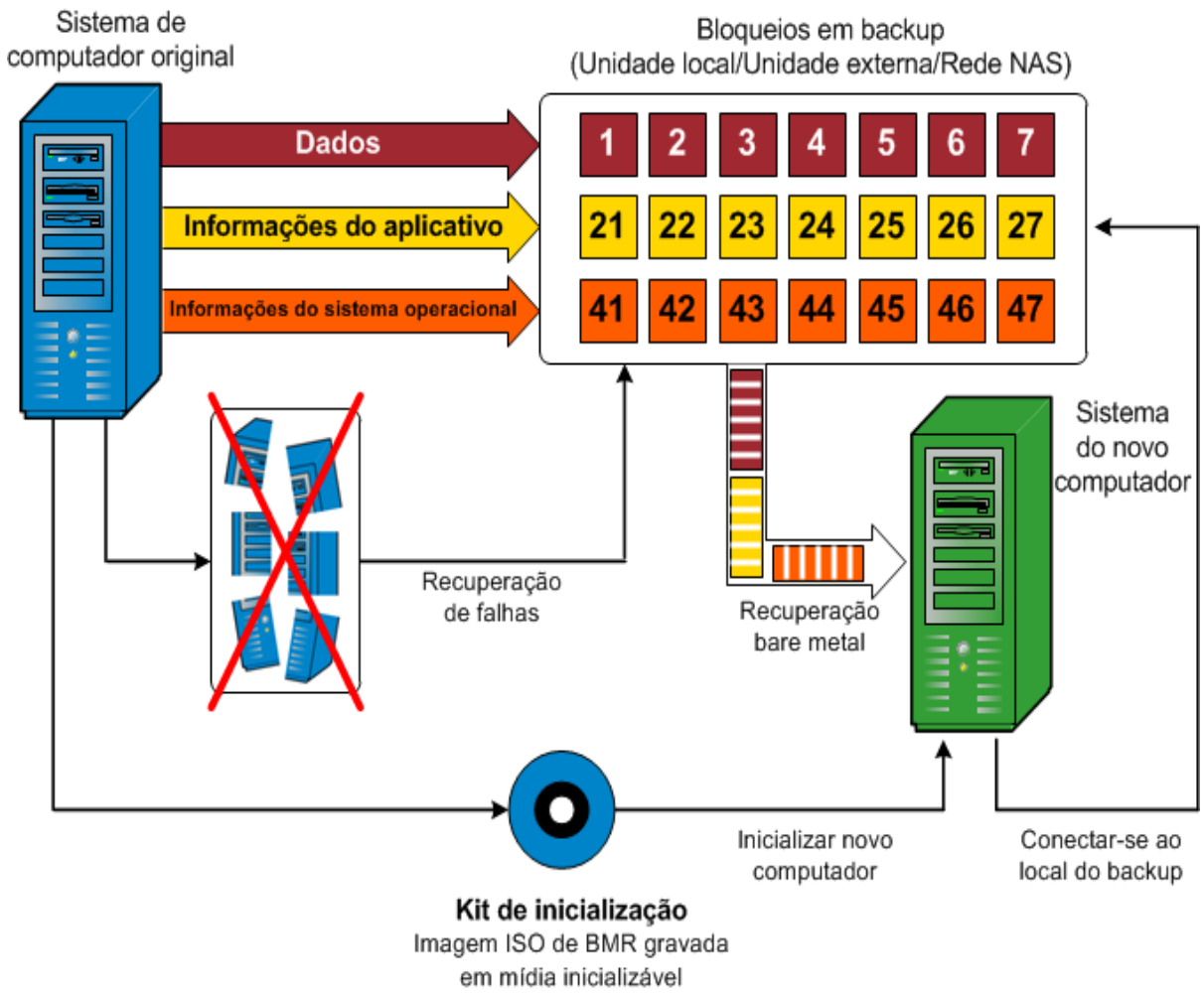
Informações de referência da BMR

- Como a recuperação bare metal funciona
- Sistemas operacionais que oferecem suporte à conversão de UEFI/BIOS
- Gerenciando o menu de operações de BMR

Como a recuperação bare metal funciona

A Recuperação bare metal é o processo de restauração de um sistema de computador a partir do estado “bare metal”, por meio da reinstalação do sistema operacional e dos aplicativos de software e, em seguida, da restauração dos dados e das configurações. Os motivos mais comuns para a execução de uma recuperação bare metal são a falha ou enchimento completo do disco rígido e você deseja atualizar (migrar) para uma unidade maior ou migrar para um hardware mais recente. A recuperação bare metal é possível porque, durante o processo de backup em nível de bloco, o agente do Arcserve UDP (Windows) não só captura os dados, mas também todas as informações relacionadas ao sistema operacional, aplicativos instalados, configurações, drivers necessários, e assim por diante. Para todas as informações relevantes, necessárias à execução de uma recompilação completa do sistema a partir do estado bare metal, é feito backup em uma série de blocos, os quais são armazenados no local do backup.

Observação: os discos dinâmicos serão restaurados somente no nível do disco. Se o backup dos dados for feito no volume de um disco dinâmico, não será possível restaurar este disco (incluindo todos os volumes) durante a BMR.



Ao executar uma recuperação bare metal, o disco de inicialização do agente do Arcserve UDP (Windows) é usado para inicializar o novo sistema do computador e permitir que o processo de recuperação bare metal seja iniciado. Ao iniciar a recuperação bare metal, o agente do Arcserve UDP (Windows) solicitará que você selecione ou forneça um local válido para recuperar esses blocos armazenados em backup, como também o ponto de recuperação para restauração. Caso seja necessário, também pode ser solicitado que você forneça drivers válidos para o novo sistema do computador. Quando essas informações de configuração e conexão forem fornecidas, o agente do Arcserve UDP (Windows) começa a receber a imagem de backup especificada do local do backup e restaura todos os blocos armazenados em backup no novo sistema (blocos vazios não são restaurados). Após a recuperação bare metal, a imagem é totalmente restaurada em um novo sistema de computador, o computador voltará ao estado que era quando o último backup foi realizado e os backups do agente do Arcserve UDP (Windows) poderão continuar conforme programado. (Após a conclusão da BMR, o primeiro backup será um Backup de verificação).

Sistemas operacionais que oferecem suporte à conversão de UEFI/BIOS

Se for detectado que o sistema operacional do computador de origem não é o mesmo firmware de seu sistema, você será questionado se deseja converter a UEFI em um sistema compatível com o BIOS ou o BIOS em um sistema compatível com a UEFI. A tabela a seguir lista cada sistema operacional e o tipo de conversão com suporte:

Sistema operacional (SO)	CPU	uEFI para BIOS	BIOS para uEFI
Windows Vista (nenhum SP)	x86	Não	Não
Windows Vista (nenhum SP)	x64	Não	Não
Windows Vista SP1	x86	Não	Não
Windows Vista SP1	x64	Sim	Sim
Windows Server 2008	x86	Não	Não
Windows Server 2008	x64	Sim	Sim
Windows Server 2008 R2	x64	Sim	Sim
Windows 7	x86	Não	Não
Windows 7	x64	Sim	Sim
Windows 8	x86	Não	Não
Windows 8	x64	Sim	Sim
Windows Server 2012	x64	Sim	Sim
Windows 8.1	x86	Não	Não
Windows 8.1	x64	Sim	Sim
Windows 10	x86	Não	Não
Windows 10	x64	Sim	Sim
Windows Server 2012 R2	x64	Sim	Sim
Windows Server 2016	x64	Sim	Sim
Windows Server 2019	x64	Sim	Sim

Gerenciando o menu de operações de BMR

O menu de operações de BMR consiste nos três seguintes tipos de operações:

- Operações específicas de disco
- Operações específicas de volume/partição
- Operação específica da BMR

Operações específicas de disco:

Para executar as operações de disco específicas, selecione o cabeçalho do disco e clique em **Operações**.

Limpar o disco

Essa operação é usada para limpar todas as partições de um disco e é:

- Um método alternativo para excluir todos os volumes de um disco. Com a operação **Limpar o disco**, não é necessário excluir os volumes um a um.
- Usada para excluir as partições que não sejam Windows. Devido a uma limitação do VDS, as partições que não são Windows não podem ser excluídas da IU, mas você pode usar esta operação para limpar todas elas.

  Observação: durante a BMR, quando o disco de destino possui partições não Windows ou partições OEM, não é possível selecionar essa partição e excluí-la da UI da BMR. Geralmente isso pode ocorrer se você nunca instalou o Linux/Unix no disco de destino. Para solucionar o problema, execute uma das seguintes tarefas:
- Selecione o cabeçalho do disco na IU da BMR, clique em **Operações** e use a operação **Limpar o disco** para apagar todas as partições no disco.
- Abra um prompt de comando e digite **Diskpart** para abrir o console do comando Diskpart. Em seguida, digite "select disk x", em que 'x' é o número de disco e "clean" para apagar todas as partições no disco.

Converter em MBR

Essa operação é usada para converter um disco em MBR (Master Boot Record – Registro mestre de inicialização). Ela está disponível apenas quando o disco selecionado é um disco GPT (GUID Partition Table – Tabela de partição GUID) e não há volumes nesse disco.

Converter em GPT

Essa operação é usada para converter um disco em GPT. Ela está disponível apenas quando o disco selecionado é um disco MBR e não há volumes nesse disco.

Converter em básico

Essa operação é usada para converter um disco em disco básico. Ela está disponível apenas quando o disco selecionado é um disco dinâmico e não há volumes nesse disco.

Converter em dinâmico

Essa operação é usada para converter um disco em disco dinâmico. Ela está disponível apenas quando o disco selecionado é um disco básico.

Disco online

Essa operação é usada para colocar um disco online. Ela está disponível apenas quando o disco selecionado está no status offline.

Propriedades do disco

Essa operação é usada para exibir detalhes sobre as propriedades do disco. Está sempre disponível e quando você seleciona essa operação, uma caixa de diálogo **Propriedades do disco** é exibida.

Operações específicas de volume/partição:

Para executar operações de volume/partição, selecione a área de corpo do disco e clique em **Operações**. Nesse menu, é possível criar novas partições que correspondam às partições do disco no volume de origem.

Criar partição primária

Essa operação é usada para criar uma partição em um disco básico. Ela está disponível somente quando a área selecionada é um espaço em disco não alocado.

Criar partição lógica

Essa operação é usada para criar uma partição lógica em um disco MBR básico. Está disponível somente quando a área selecionada é uma partição estendida.

Criar partição estendida

Essa operação é usada para criar uma partição estendida em um disco MBR básico. Está disponível apenas quando o disco é um disco MBR e a área selecionada é um espaço em disco não alocado.

Criar partição reservada do sistema

Essa operação é usada para criar a partição reservada do sistema em um sistema de firmware do BIOS e compilar um relacionamento de mapeamento com a partição de sistema EFI de origem. Está disponível apenas quando você restaura um sistema UEFI para um sistema BIOS.

Observação: se você tiver feito a conversão de UEFI para um sistema compatível com o BIOS anteriormente, use a operação Criar partição reservada do sistema para redimensionamento do disco de destino.

Criar partição de sistema EFI

Essa operação é usada para criar a partição de sistema EFI em um disco GPT básico. Está disponível apenas quando o firmware do computador de destino é UEFI e o disco selecionado é um disco GPT básico.

Observação: se tiver feito a conversão de BIOS para um sistema compatível com UEFI anteriormente, use a operação Criar partição de sistema EFI para o redimensionamento do disco de destino.

Observação: os sistemas que oferecem suporte à UEFI também exigem que a partição de inicialização resida em um disco GPT (GUID Partition Table - Tabela de Partição do GUID). Se estiver usando um disco MBR (Master Boot Record), você deverá converter esse disco em um disco GPT e, em seguida, usar a operação Criar partição de sistema EFI para redimensionamento do disco.

Redimensionar volume

Essa operação é usada para redimensionar um volume. Ela é um método alternativo do Windows "Ampliar volume/Reduzir volume". Está disponível somente quando a área selecionada é uma partição de disco válida.

Excluir volume

Essa operação é usada para excluir um volume. Está disponível somente quando a área selecionada é um volume válido.

Excluir partição estendida

Essa operação é usada para excluir a partição estendida. Está disponível somente quando a área selecionada é a partição estendida.

Propriedades do volume

Essa operação é usada para exibir propriedades de volume detalhadas. Quando você seleciona essa operação, uma caixa de diálogo **Propriedades do volume** é exibida.

Operações específicas de BMR:

Essas operações são específicas para a BMR. Para executar operações de BMR, selecione o cabeçalho do disco ou a área de corpo do disco e clique em **Operações**.

Mapear disco de

Essa operação é usada para compilar um mapeamento de relacionamento entre os discos dinâmicos de origem e de destino. Está disponível apenas quando o disco selecionado é um disco dinâmico.

Observação: ao fazer o mapeamento para outro disco, a capacidade de cada volume de destino mapeado deve ser do mesmo tamanho ou maior do que o volume de origem correspondente.

Mapear volume a partir de

Essa operação é usada para compilar um relacionamento de mapeamento entre o volume básico de origem e de destino. Ela está disponível apenas quando o volume selecionado é um volume básico.

Observação: ao fazer o mapeamento para outro disco, a capacidade de cada volume de destino mapeado deve ser do mesmo tamanho ou maior do que o volume de origem correspondente.

Confirmar

Essa operação está sempre disponível. Todas as operações são armazenadas em cache na memória e não modificam os discos de destino até que você selecione a operação de **Confirmação**.

Redefinir

Essa operação está sempre disponível. A operação **Redefinir** é usada para abandonar suas operações e restaurar o layout do disco para o status padrão. Essa operação limpará todas as operações em cache. Redefinir significa recarregar as informações de layout do disco de origem e de destino a partir do arquivo de configuração e do sistema operacional atual, e descartar quaisquer informações de layout de disco alteradas pelo usuário.

Solução de problemas da BMR

Quando um problema é detectado, o agente do Arcserve UDP (Windows) gera uma mensagem para ajudá-lo a identificar e solucionar o problema. Essas mensagens estão contidas no **Log de atividades** do Agente do Arcserve UDP (Windows), que é acessado pela opção **Exibir logs** na IU da página inicial. Além disso, ao tentar uma ação incorreta, o Agente do Arcserve UDP (Windows) em geral exibe uma mensagem pop-up para ajudá-lo a identificar e resolver o problema rapidamente.

- Baixo desempenho da taxa de transferência durante a BMR
- Volumes dinâmicos não são reconhecidos pelo sistema operacional após a BMR
- Não é possível reinicializar a VM Hyper-V após a BMR
- Não é possível reinicializar a VM VMware após a BMR
- Não é possível inicializar o servidor após executar uma BMR
- Falha ao enviar a tarefa BMR para o Servidor do ponto de recuperação

Baixo desempenho da taxa de transferência durante a BMR

Esse problema pode ser causado por controladores SATA com "AHCI" ativado.

Durante a BMR, o agente do Arcserve UDP (Windows) instalará drivers para dispositivos desconhecidos importantes. Se o dispositivo já tiver um driver instalado, o agente do Arcserve UDP (Windows) não atualizará o driver novamente. Para alguns dispositivos, o Windows 7PE pode conter os drivers, mas tais drivers podem não ser os melhores, e fazer com que a BMR seja executada de maneira muito lenta.

Para solucionar o problema, execute uma das seguintes tarefas:

- Verifique se a pasta do pool de drivers contém os drivers de disco mais novos. Caso contenha, e você esteja restaurando para a máquina original, instale o novo driver a partir da pasta do pool de drivers. Caso esteja restaurando para uma máquina alternativa, faça download dos drivers de disco mais recentes a partir da internet e carregue-os antes de iniciar a recuperação dos dados. Para carregar o driver, pode-se usar o utilitário "drvload.exe" que está incluído no Windows PE.
- Altere o modo de operação do dispositivo de AHCI (Advanced Host Controller Interface) para o modo de compatibilidade. (O modo de compatibilidade fornece uma melhor taxa de transferência).

Se o problema persistir, use o Bate-papo ao vivo para entrar em contato com o suporte da Arcserve. O Bate papo ao vivo permite viabilizar uma comunicação inteligente entre você e a equipe do suporte técnico, de modo que suas dúvidas e preocupações sejam atendidas imediatamente, sem interromper o acesso ao produto.

Volumes dinâmicos não são reconhecidos pelo sistema operacional após a BMR

Para manter os discos dinâmicos em um estado consistente, o sistema operacional Windows sincroniza automaticamente o metadados do LDM (Logical Disk Manager - Gerenciador de discos lógicos) em cada disco dinâmico. Assim, quando a BMR restaura um disco dinâmico e coloca-o online, o metadados do LDM neste disco será atualizado automaticamente pelo sistema operacional. Isso pode resultar em um volume dinâmico não reconhecido pelo sistema operacional e ausente após a reinicialização.

Para corrigir este problema, ao executar a BMR com vários discos dinâmicos, você não deve executar operações de disco antes da BMR, como limpeza, exclusão de volume, etc.

Se o problema persistir, use o Bate-papo ao vivo para entrar em contato com o suporte da Arcserve. O Bate papo ao vivo permite viabilizar uma comunicação inteligente entre você e a equipe do suporte técnico, de modo que suas dúvidas e preocupações sejam atendidas imediatamente, sem interromper o acesso ao produto.

Não é possível reinicializar a VM Hyper-V após a BMR

Se você executou a BMR em um computador Hyper-V que consiste em mais de um disco conectado a um controlador IDE (Integrated Drive Electronics), e o servidor não está reinicializando, execute o seguinte procedimento para solucionar o problema:

1. Verifique se o disco que contém o volume do sistema é o disco mestre.

   O BIOS do Hyper-V procura o volume do sistema no disco mestre (disco 1) que está conectado ao canal mestre. Se o volume do sistema não estiver localizado no disco mestre, a VM não será reinicializada.

   Observação: verifique se o disco que contém o volume do sistema está conectado a um controlador IDE. O Hyper-V não consegue inicializar a partir de um disco SCSI.

2. Se necessário, modifique as configurações do Hyper-V para conectar o disco que contém o volume do sistema ao canal mestre de IDE e reinicialize o computador virtual novamente.

   Se o problema persistir, use o Bate-papo ao vivo para entrar em contato com o suporte da Arcserve. O Bate papo ao vivo permite viabilizar uma comunicação inteligente entre você e a equipe do suporte técnico, de modo que suas dúvidas e preocupações sejam atendidas imediatamente, sem interromper o acesso ao produto.

Não é possível reinicializar a VM VMware após a BMR

Caso tenha executado a BMR em um computador VMware que consiste em mais de um disco conectado a um controlador IDE (Integrated Drive Electronics) ou a um adaptador SCSI, e o servidor não está reinicializando, execute o seguinte procedimento para solucionar o problema:

1. Verifique se o disco que contém o volume do sistema é o disco mestre.

   O BIOS do VMware procura o volume do sistema no disco mestre (disco 0) que está conectado ao canal mestre. Se o volume do sistema não estiver localizado no disco mestre, a VM não será reinicializada.

2. Se necessário, modifique as configurações do VMware para conectar o disco que contém o volume do sistema ao canal mestre de IDE e reinicialize o computador virtual novamente.

3. Se o disco for SCSI, certifique-se de que o disco contendo o volume de inicialização seja o primeiro a estabelecer conexão com o adaptador SCSI. Caso contrário, atribua o disco de inicialização do BIOS da VMware.

4. Verifique se o disco que contém o volume de inicialização está entre os oito discos anteriores, pois o BIOS da VMware detecta apenas oito discos durante a inicialização. Se houver mais de sete discos à frente do disco que contém os volumes do sistema conectados ao adaptador SCSI, a VM não poderá executar a inicialização.

   Se o problema persistir, use o Bate-papo ao vivo para entrar em contato com o suporte da Arcserve. O Bate papo ao vivo permite viabilizar uma comunicação inteligente entre você e a equipe do suporte técnico, de modo que suas dúvidas e preocupações sejam atendidas imediatamente, sem interromper o acesso ao produto.

Não é possível inicializar o servidor após executar uma BMR

Sintoma

Quando o computador de origem for um servidor Active Directory executando uma BMR para uma máquina física com um hardware diferente ou para uma máquina virtual em um servidor Hyper-V, o servidor não será inicializado e uma tela azul será exibida com a seguinte mensagem:

INTERROMPER: não foi possível iniciar os serviços de diretório c00002e2 devido ao seguinte erro: um dispositivo conectado ao sistema não está funcionando. Status do erro: 0xc0000001.

Solução

Reinicialize o sistema para o ambiente do Windows PE da BMR, renomeie todos os arquivos *.log na pasta C:\Windows\NTDS e reinicie o sistema. Por exemplo, renomeie o arquivo edb.log como edb.log.old e reinicie o sistema.

Se o problema persistir, use o Bate-papo ao vivo para entrar em contato com o suporte da Arcserve. O Bate papo ao vivo permite viabilizar uma comunicação inteligente entre você e a equipe do suporte técnico, de modo que suas dúvidas e preocupações sejam atendidas imediatamente, sem interromper o acesso ao produto.

Falha ao enviar a tarefa BMR para o Servidor do ponto de recuperação

Apenas uma tarefa de BMR é suportada quando a restauração do mesmo servidor de RPS para o mesmo nó (Backup do agente ou Backup com base em host). Isso é controlado pelo monitor de tarefas no servidor de RPS.

Se a máquina em que a tarefa BMR está em execução estiver desligada ou for reiniciada de forma inesperada, o monitor de tarefas no servidor de RPS aguardará 10 minutos e, em seguida, o tempo limite. Durante esse tempo, não será possível iniciar outra BMR para o mesmo nó do mesmo servidor de RPS.

Se anular a BMR na IU da BMR, esse problema não existirá.

Se o problema persistir, use o Bate-papo ao vivo para entrar em contato com o suporte da Arcserve. O Bate papo ao vivo permite viabilizar uma comunicação inteligente entre você e a equipe do suporte técnico, de modo que suas dúvidas e preocupações sejam atendidas imediatamente, sem interromper o acesso ao produto.

O computador de destino da BMR inicializa nas opções de recuperação do sistema após a execução de uma BMR

Sintoma

Se você executar uma BMR em uma máquina virtual em um servidor ESX, às vezes o computador de destino da BMR inicializa na tela Opções de recuperação do sistema.

Solução

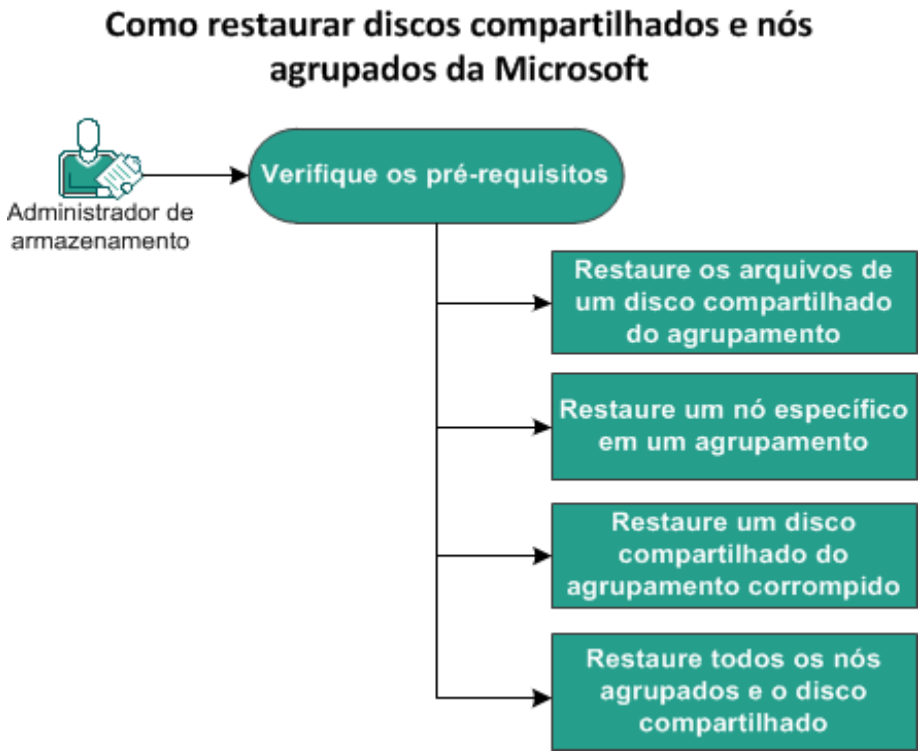
Para resolver esse problema, Desative gravadores VSS específicos com o VMware Tools na máquina da VM instantânea e, em seguida, execute uma BMR novamente.

Como restaurar nós agrupados e discos compartilhados da Microsoft

Se tiver um ambiente agrupado e os nós agrupados e o disco compartilhado não estiverem funcionando adequadamente, é possível recuperar facilmente os nós e os discos. É possível restaurar os seguintes itens:

- Arquivos individuais e pastas em discos compartilhados
- Nós específicos de um agrupamento
- Todo o disco compartilhado
- Configuração de agrupamento inteiro (todos os nós agrupados e o disco compartilhado)

O diagrama a seguir ilustra o processo para restaurar os nós agrupados e os discos compartilhados:



Siga estas etapas para restaurar os nós agrupados e os discos compartilhados da Microsoft:

- Verificar os pré-requisitos
- Restaurar os arquivos do disco compartilhado de um agrupamento
- Restaurar um nó específico em um agrupamento

- Restaurar um disco compartilhado de um agrupamento corrompido
- Restaurar os nós agrupados e disco compartilhado inteiros

Verificar os pré-requisitos

Verifique se concluiu os seguintes pré-requisitos:

- Você tem um ponto de recuperação válido para restauração.
- Você possui uma imagem ISO válida para uma BMR.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Restaurar os arquivos do disco compartilhado de um agrupamento

O disco compartilhado pertence a um dos nós do agrupamento. Ao recuperar quaisquer arquivos do disco compartilhado (não o disco de quorum do agrupamento), você deve encontrar o nó pai do disco compartilhado. Depois de identificar o nó pai, é possível recuperar arquivos para o nó pai a partir do disco compartilhado.

Observação: após a ocorrência de uma tolerância a falhas, procure o ponto de recuperação de um agente diferente para descobrir o ponto de recuperação desejado.

Siga estas etapas:

1. Efetue logon no agente que possui o disco compartilhado.
2. Abra o Assistente de restauração e selecione Localizar arquivos/pastas para restauração.

   Observação: para obter mais informações sobre como restaurar os arquivos e as pastas, consulte o tópico Como restaurar arquivos/pastas.
3. Selecione todos os arquivos do Assistente de restauração que deseja restaurar para o local original.
4. Preencha as configurações do Assistente de restauração e envie a tarefa.

   Os arquivos são recuperados.
5. Efetue logon no nó pai do disco compartilhado e verifique se os arquivos foram recuperados.

   Os arquivos do disco compartilhado foram recuperados.

Restaurar um nó específico em um agrupamento

Se um determinado nó em um agrupamento estiver desativado, é possível executar uma BMR apenas para esse nó. Normalmente, neste cenário, o disco compartilhado está em bom estado e não precisa de uma recuperação.

Siga estas etapas:

1. Prepare a imagem BMR (CD/DVD ou dispositivo USB).
2. Remova todas as conexões entre o nó que você deseja recuperar e os discos compartilhados.

   Exemplo: desconecte a conexão de fibre channel.
3. Execute uma BMR para o nó do agrupamento.

   Observação: para obter mais informações sobre como executar uma recuperação "bare metal", consulte o tópico Como executar uma BMR usando um backup.

   O nó específico em um agrupamento foi recuperado.
4. Verifique o status do nó recuperado no console de gerenciamento do agrupamento e garanta que ele funcione como parte do agrupamento.

   O nó específico em um agrupamento foi recuperado.

Restaurar um disco compartilhado de um agrupamento corrompido

O disco compartilhado pertence a um dos nós do agrupamento. Se o disco compartilhado estiver corrompido ou danificado, é possível restaurar os arquivos e pastas específicos do disco compartilhado, sem recuperar os nós do agrupamento. Normalmente, neste cenário, o disco de quorum e todos os nós do agrupamento estão em bom estado.

Siga estas etapas:

1. Substitua o disco danificado manualmente e reconfigure o disco compartilhado do agrupamento.
2. Identifique o agente que possui o disco compartilhado e efetue logon nesse agente.
3. Abra o Assistente de restauração e selecione Localizar arquivos/pastas para restauração.

   Observação: para obter mais informações sobre como restaurar os arquivos e as pastas, consulte o tópico Como restaurar arquivos/pastas.
4. Selecione todos os arquivos do Assistente de restauração que deseja restaurar para o local original.
5. Preencha as configurações do Assistente de restauração e envie a tarefa.

   O disco compartilhado foi recuperado.
6. Verifique o status do disco compartilhado no console de gerenciamento do agrupamento e garanta que ele funcione como parte do agrupamento.

   O disco compartilhado foi recuperado.

Restaurar os nós agrupados e disco compartilhado inteiros

Se toda a instalação agrupada estiver corrompida ou não estiver funcionando, é possível recuperar o agrupamento inteiro. A recuperação do agrupamento inteiro é um processo em duas partes. Primeiro, recupere os nós agrupados individuais usando a BMR. Em seguida, recupere os arquivos e as pastas do disco compartilhado.

Observação: para os discos de quorum, recrie o disco usando o console de gerenciamento de agrupamentos, em vez de recuperá-lo usando o Assistente de restauração no Agente do Arcserve UDP (Windows).

Siga estas etapas:

1. Prepare a imagem BMR (CD/DVD ou dispositivo USB).
2. Remova todas as conexões entre o nó que você deseja recuperar e os discos compartilhados.

   Exemplo: desconecte a conexão de fibre channel.
3. Execute uma BMR para o nó do agrupamento.

   Observação: para obter mais informações sobre como executar uma recuperação "bare metal", consulte o tópico Como executar uma BMR usando um backup.

   O nó específico em um agrupamento foi recuperado.
4. Verifique o status do nó recuperado no console de gerenciamento do agrupamento e garanta que ele funcione como parte do agrupamento.

   O nó específico em um agrupamento foi recuperado.
5. Repita as etapas para recuperar todos os nós agrupados.

   Todos os nós agrupados foram recuperados. Agora, recupere o disco compartilhado.
6. Substitua o disco danificado manualmente e reconfigure o disco compartilhado do agrupamento.
7. Identifique o agente que possui o disco compartilhado e efetue logon nesse agente.
8. Abra o Assistente de restauração e selecione Localizar arquivos/pastas para restauração.

   Observação: para obter mais informações sobre como restaurar os arquivos e as pastas, consulte o tópico Como restaurar arquivos/pastas.

9. Selecione todos os arquivos do Assistente de restauração que deseja restaurar para o local original.
10. Preencha as configurações do Assistente de restauração e envie a tarefa.

    O disco compartilhado foi recuperado.
11. Verifique os arquivos do disco compartilhado e certifique-se de que os arquivos foram recuperados.

    O agrupamento inteiro foi recuperado.

Como restaurar um Active Directory

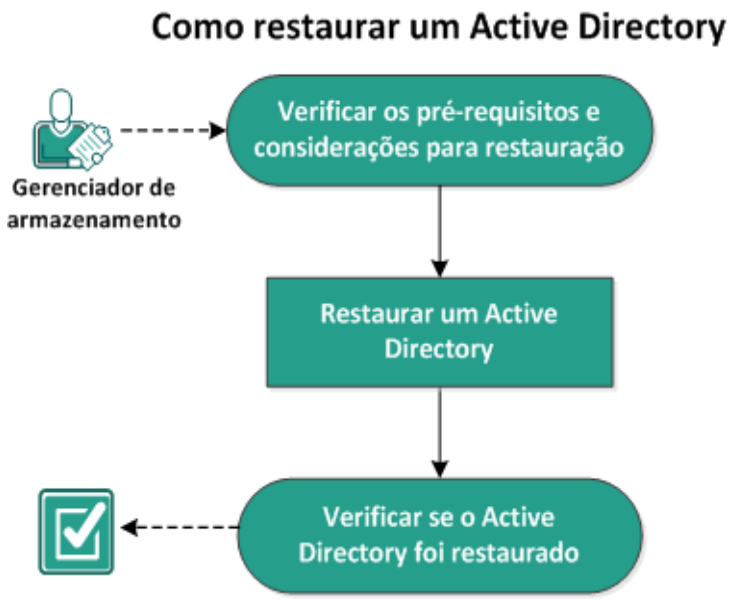
Você precisa restaurar uma sessão cujo backup foi feito do Active Directory se tiver um dos seguintes cenários:

- Você deseja recuperar um atributo do objeto do Active Directory a partir uma sessão de backup do Active Directory disponível (e não apenas da última sessão de backup).
- Você deseja recuperar o objeto do Active Directory a partir uma sessão de backup do Active Directory disponível (não apenas da última sessão de backup).
- Você deseja recuperar vários atributos ou objetos do Active Directory a partir de qualquer sessão com backup do Active Directory disponível (e não apenas da última sessão com backup).

Importante: para realizar uma recuperação granular de um Active Directory, é preciso um backup com base em agente.

Lista dos objetos do Active Directory recuperados pela restauração em nível de objeto		
Unidade organizacional	Instalação	Classe Achados e perdidos
Usuário	Recipiente de site	Classe Domínio integrado
Grupo	Link de site	Classe Zona DNS
Computador	Ponte de link de site	Classe Domínio
Contato	Configurações de site	Classe Domínio NDS
Conexão	Recipiente de sub-rede	Classe DMD
Pasta compartilhada	Domínio confiável	Classe Unidade organizacional
Impressora	Classe Configuração	Classe Containerecifiers

O cenário descreve como restaurar um Active Directory.



Execute as tarefas a seguir para restaurar um Active Directory:

1. Revisar os pré-requisitos e as considerações para restauração
2. Restaurar um Active Directory
3. Verificar se o Active Directory foi restaurado

Verificar os pré-requisitos e as considerações para restauração

Verifique se os pré-requisitos a seguir existem antes de executar uma restauração:

- Você já fez backup dos volumes que incluem a pasta do banco de dados do Active Directory e da pasta de arquivos de log.
- Você instalou o Agente do Arcserve UDP (Windows) no controlador de domínio.
- Você executou um backup com base em agente.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Revise as seguintes considerações de restauração:

- Para um ponto de recuperação sem um catálogo do sistema de arquivos criado, para garantir que você possa navegar e selecionar arquivos/pastas para restaurar, deve ser concedido acesso à conta/ao grupo para todas as pastas/arquivos em todos os volumes com acesso de leitura/lista antes de realizar o backup.
- É possível executar uma restauração do Active Directory somente no Agente do Arcserve UDP (Windows).

Restaurar um Active Directory

Depois de instalar o Active Directory em volumes diferentes e ter executado um backup de ambos os volumes, talvez você deseje restaurar os volumes com o Active Directory. Este cenário descreve como é possível restaurar volumes do Active Directory do qual foi feito backup.

Observação: verifique se concluiu os pré-requisitos e fez o backup dos volumes do Active Directory.

Siga estas etapas:

1. Acesse a caixa de diálogo de seleção de método de restauração de uma das seguintes maneiras:

   No Arcserve UDP:

   a. Efetue logon no Arcserve UDP.

   b. Clique na guia **Recursos**.

   c. Selecione **Todos os nós** no painel esquerdo.

      Todos os nós do adicionados são exibidos no painel central.

   d. No painel central, selecione o nó do e clique em **Ações**.

   e. Clique em **Restaurar** no menu suspenso **Ações**.

      A caixa de diálogo de seleção do método de restauração é exibida.

      Observação: você é automaticamente conectado ao nó do agente e a caixa de diálogo de seleção do método de restauração é exibida no nó do agente.

   No agente do Arcserve UDP (Windows):

   a. Efetue logon no Agente do Arcserve UDP (Windows).

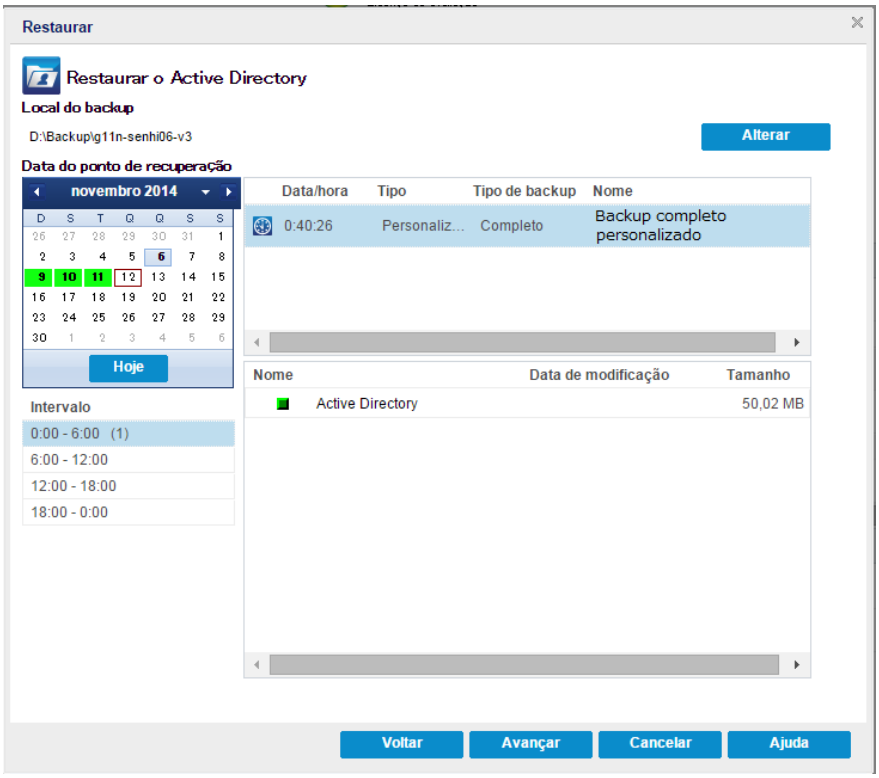
   b. Na página inicial, selecione **Restaurar**.

   A caixa de diálogo de seleção do método de restauração é exibida.

2. Na tela Restaurar, clique em Restaurar o Active Directory.

   A caixa de diálogo Restaurar o Active Directory é exibida.

3. Na tela Restaurar o Active Directory, execute as seguintes etapas:



a. No calendário, selecione a data para o backup do Active Directory que deseja restaurar.

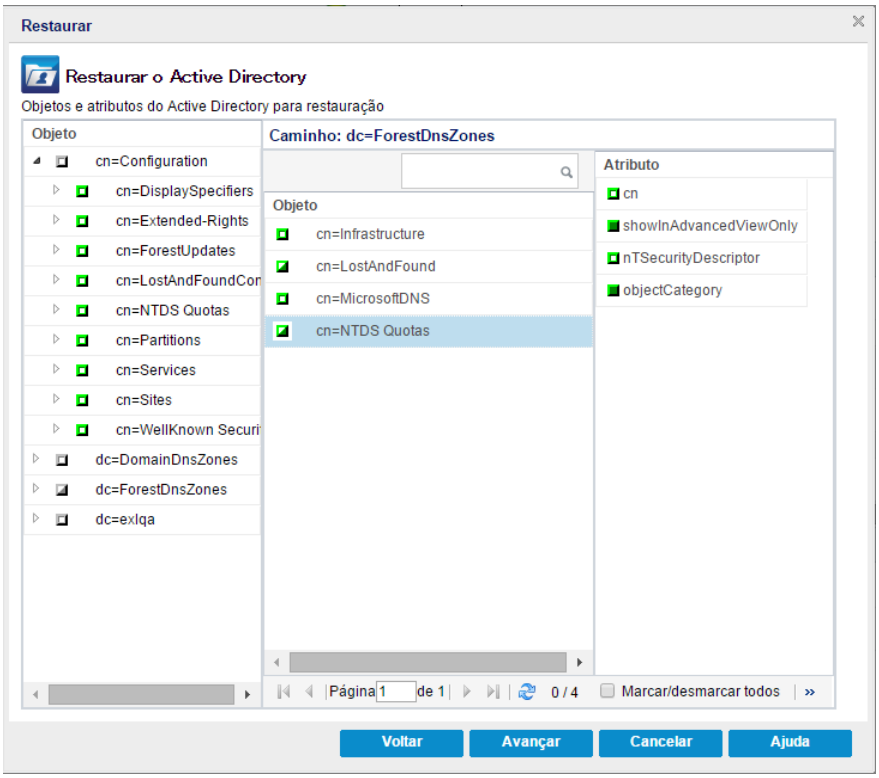
b. No intervalo de tempo, selecione o tempo de backup.

c. A partir da tela de restauração do Active Directory, selecione um ponto de recuperação que tenha identificação de Tempo, Tipo, Tipo de backup e Nome.

d. Na seção Name, selecione uma sessão de backup para restauração do Active Directory.

4. Clique em Avançar.

5. Selecione as seguintes opções para definir ainda mais os objetos, caminho e atributos para restauração:



a. Na coluna Objeto, selecione o nome de um objeto. Os caminhos relacionados ao objeto selecionado são exibidos.

b. Na coluna Caminho, selecione um caminho. Os atributos relacionados ao caminho selecionado são exibidos.

   Observação: é possível usar o ícone de pesquisa para procurar o caminho.

c. Na coluna Atributo, selecione um ou mais atributos.

6. Clique em Avançar.

   A caixa de diálogo Opções de restauração é exibida.

7. Na guia Opções de restauração, selecione os seguintes objetos de acordo com suas necessidades:

   a. Se o objeto selecionado foi renomeado depois do backup, clique na opção "Restaurar nome original dos objetos renomeados" para restaurar o objeto renomeado.

      Observação: se não selecionar essa opção, o objeto não será restaurado.

   b. Se o objeto selecionado foi movido para outro contêiner após o backup, clique na opção Restaurar no local original dos objetos movidos para restaurar o objeto movido.

      Observação: se não selecionar essa opção, o objeto não será restaurado.

c. Se o objeto selecionado foi excluído permanentemente após o backup, clique na opção "Restaurar com a nova ID de objeto dos objetos excluídos" para restaurar o objeto excluído permanentemente.

   Observação: essa opção ajuda a manter o objeto restaurado com a nova ID do objeto.

8. Clique em Avançar.

   A tela Resumo da restauração é exibida.

9. Verifique os detalhes e execute uma das ações a seguir:

   - Clique em Voltar, se quiser modificar os detalhes.
   - Clique em Concluir para executar a restauração.

   Uma mensagem de status é exibida, informando quando a tarefa de restauração é concluída. Se a operação não tiver êxito, consulte os logs e tente novamente.

Verificar se o Active Directory foi restaurado

Após a conclusão do processo de restauração, é possível usar o utilitário de usuários e computadores do Active Directory para verificar se o Active Directory (objeto e/ou atributo) foi restaurado para o destino especificado.

Observação: o utilitário do Active Directory é instalado automaticamente com o Active Directory.

Como restaurar dados do Active Directory usando o utilitário de restauração no nível de objeto do Active Directory do Arcserve UDP

Depois de instalar o Active Directory em diferentes volumes e fazer backup de ambos os volumes usando uma tarefa de backup sem agente com base em host, convém realizar uma restauração granular dos objetos e dos atributos do Active Directory. Este cenário descreve como você pode restaurar os objetos e os atributos do Active Directory partir dos volumes que eles contêm.

Antes de fazer qualquer restauração, verifique se os seguintes pré-requisitos foram atendidos:

- O utilitário de restauração no nível de objeto do Active Directory precisa estar disponível em:

  <Caminho de instalação do Arcserve UDP>\Engine\BIN\

  Observação: a ferramenta é instalada com o agente do Arcserve UDP.
- A tarefa de restauração precisa estar configurada para ser executada no computador de proxy de backup com base em host.

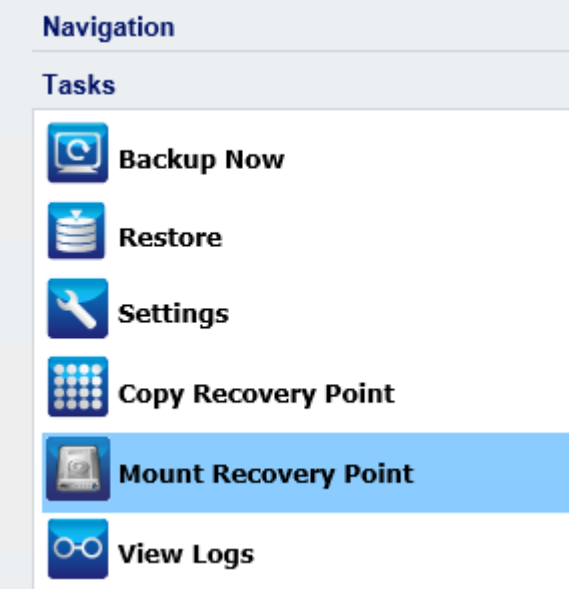
  Observação: caso queira executar a tarefa de restauração em outro computador, procure o ponto de recuperação no destino do backup.
- O caminho para o banco de dados do Active Directory (NTDS.dit) precisa estar identificado para a tarefa de restauração ser executada.

  Observação: por padrão, o arquivo NTDS.dit está no caminho C:\Windows\NTDS\NTDS.dit.

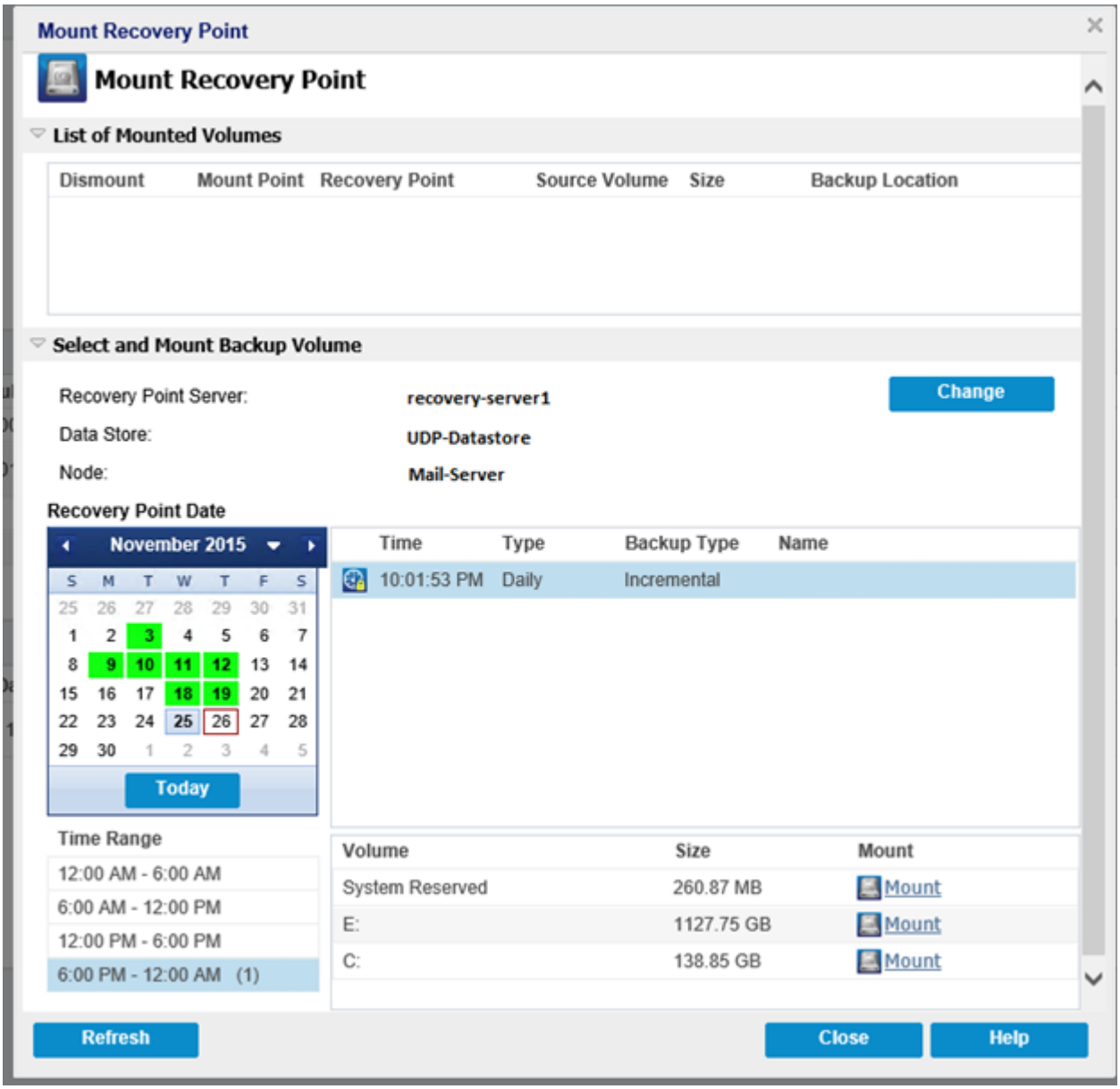
Siga estas etapas:

1. No console do agente do Arcserve UDP, no computador de proxy de backup com base em host, selecione a tarefa Montar ponto de recuperação. A caixa

de diálogo Montar ponto de recuperação é exibida.

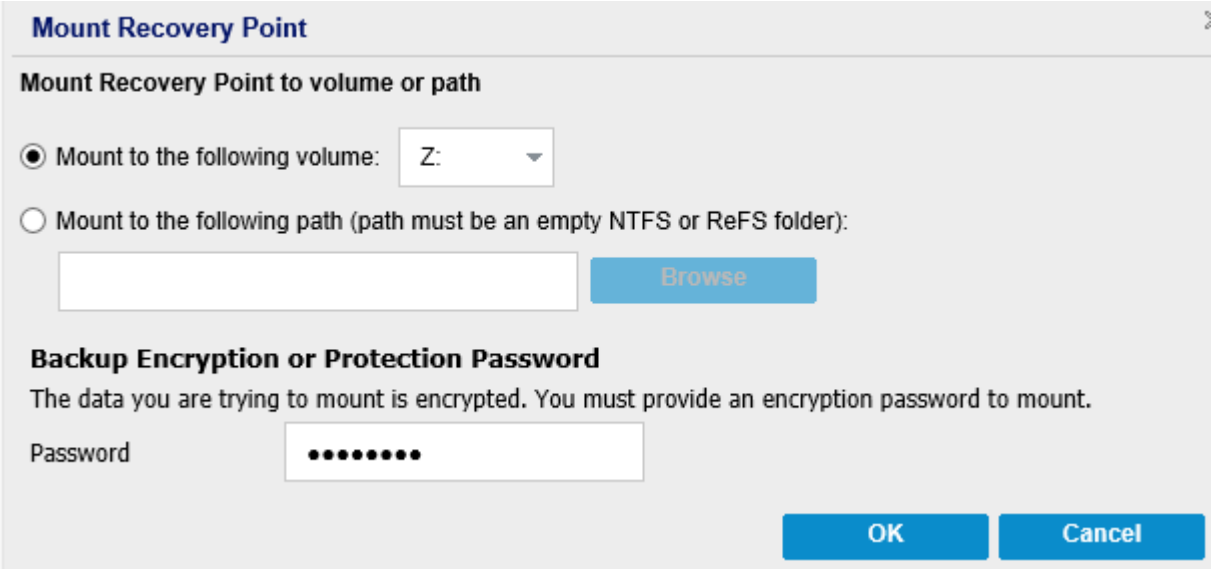


2. Selecione a data do ponto de recuperação.
3. Para obter o volume que contém o banco de dados do Active Directory, clique em **Montar**.



Observação: se o servidor que está executando a tarefa de restauração não for o proxy HBBU, clique em **Alterar** para fazer as seleções corretas de servidor de ponto de recuperação, repositório de dados e servidor do Active Directory.

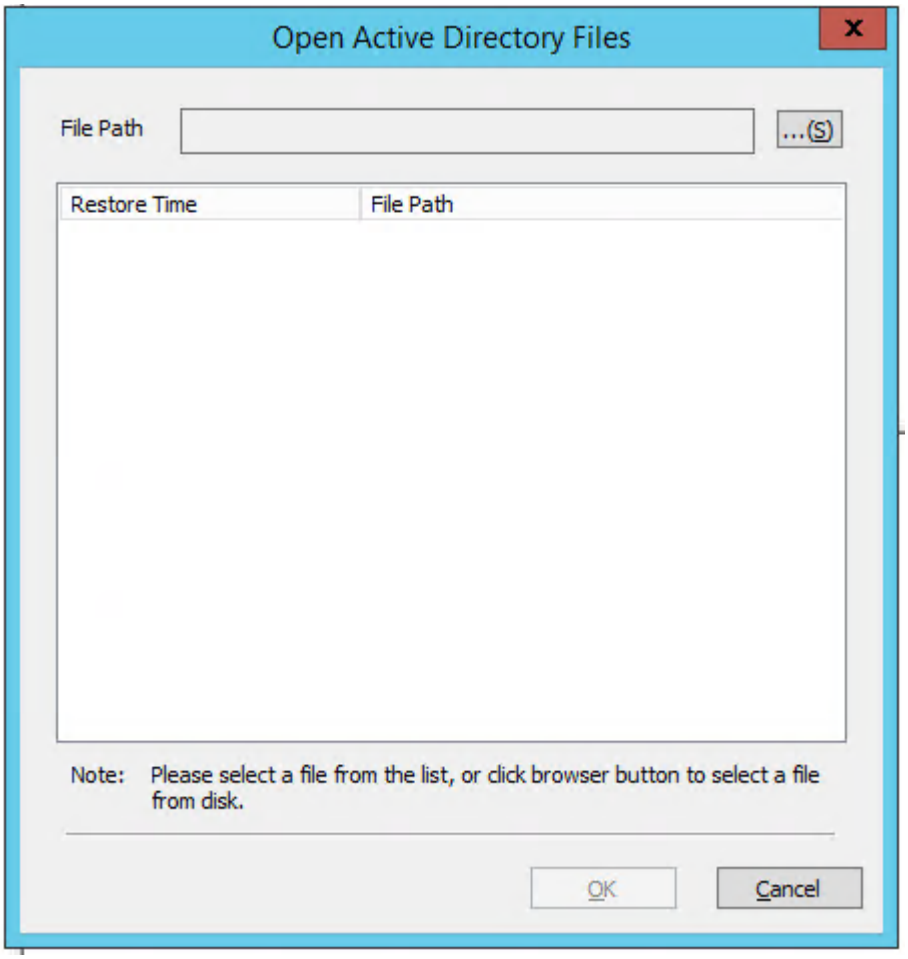
4. Selecione a letra da unidade onde o volume deve ser montado e clique em **OK**.



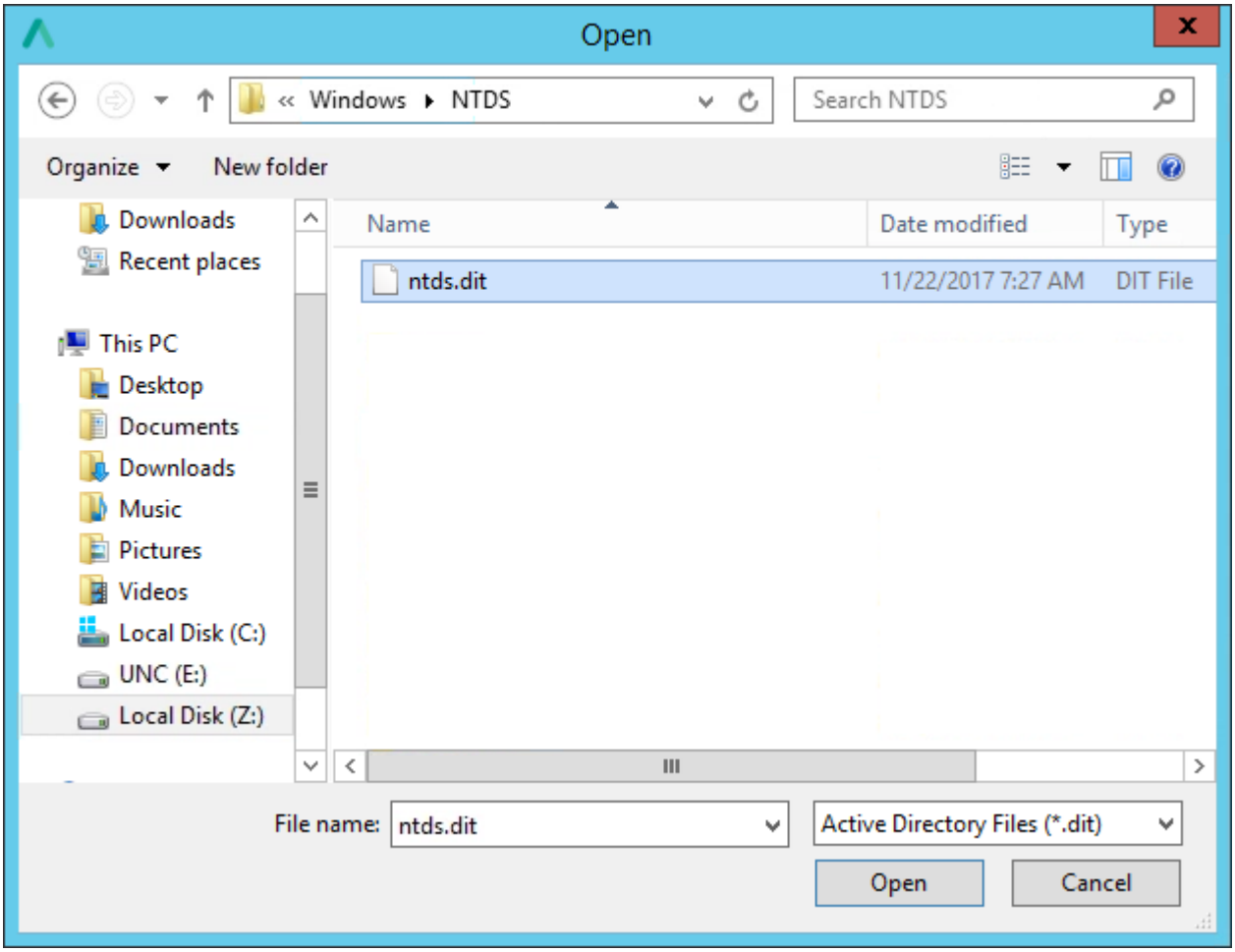
5. Inicie o utilitário de restauração no nível de objeto do Active Directory em:

   <caminho de instalação do Arcserve UDP>\Engine\BIN\AD_restore.exe

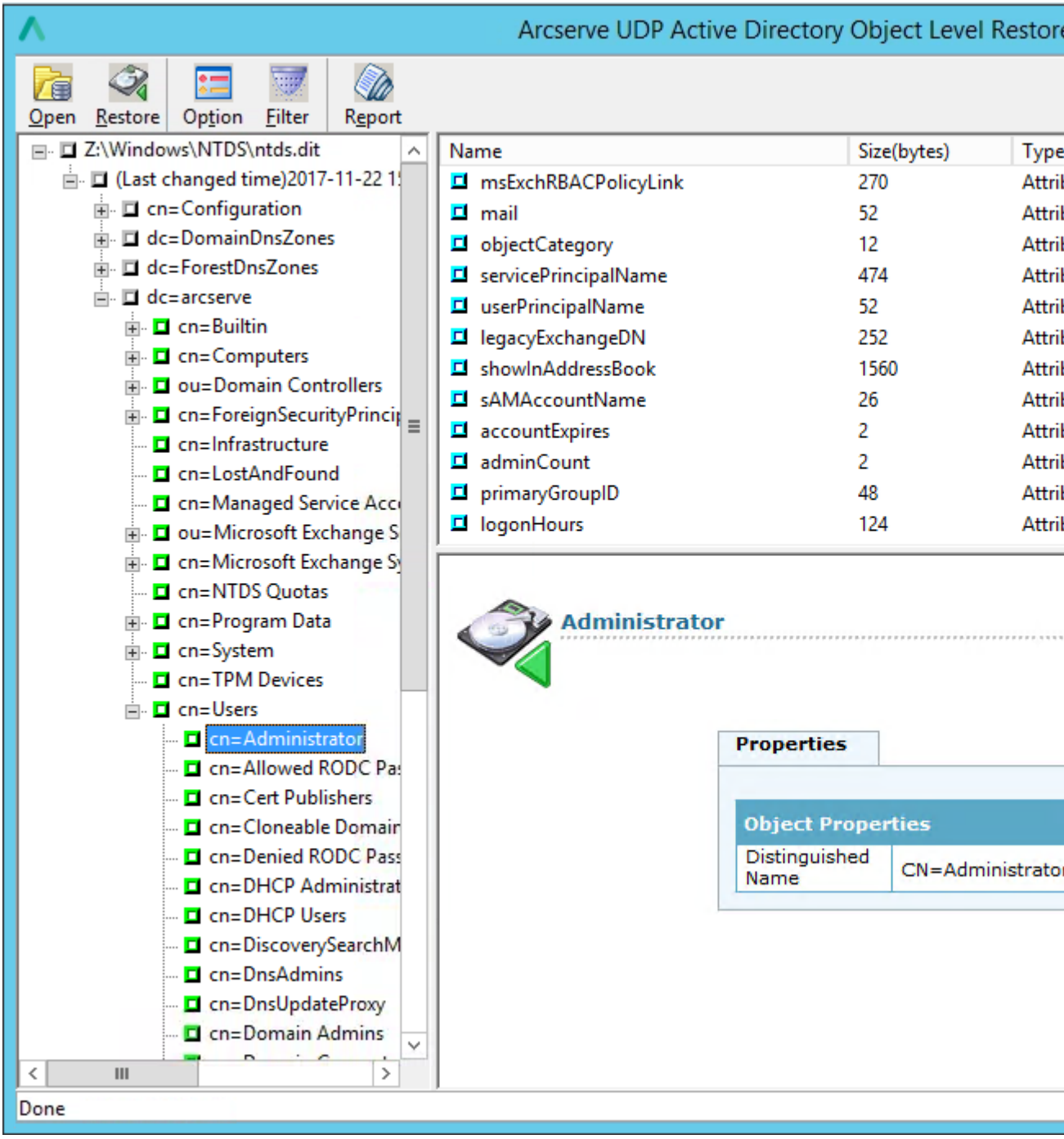
6. Clique em **Abrir** para abrir a janela de seleção.



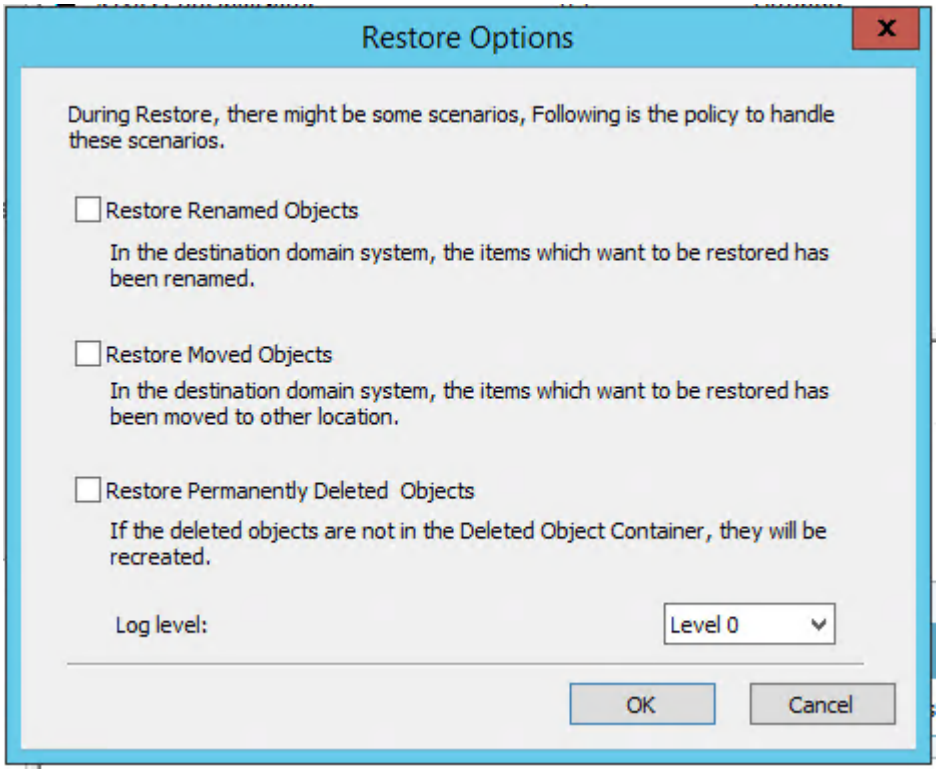
7. Clique no ícone ...(S) e procure o banco de dados do Active Directory (NTDS.-dit) no ponto de recuperação montado. Em seguida, clique em **Abrir** e **OK**.



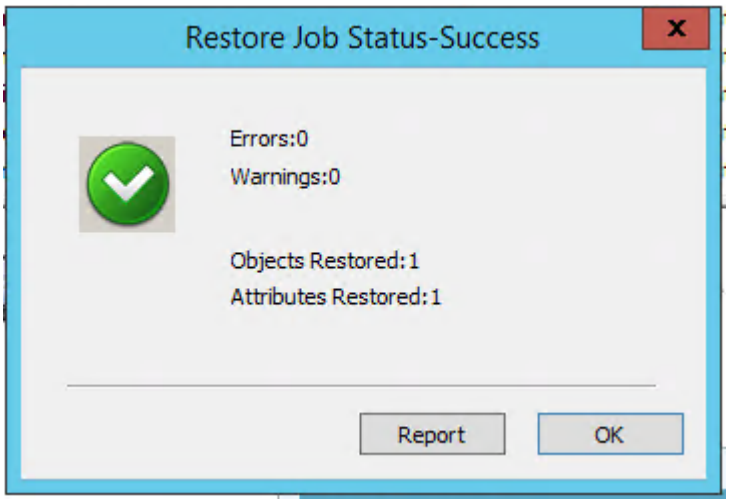
8. Procure e selecione os objetos ou atributos do Active Directory que você deseja restaurar.



9. Clique em **Opções** para fazer os ajustes necessários no comportamento padrão.



10. Quando quiser, clique em **OK** para executar a tarefa de restauração.
11. Quando a tarefa de restauração for concluída, será exibida uma janela com o resultado. Clique em **Relatório** para ver detalhes da tarefa ou em **OK** para fechar a janela.



Observações:

- Por padrão, o utilitário estabelece conexão com o Windows por meio do usuário atualmente conectado.

- Em caso de erro, é recomendado efetuar logon no computador usando uma conta com direitos de administrador de domínio para realizar a restauração.

12. Quando a tarefa de restauração é concluída, desmonte o volume que foi usado para a recuperação.
13. Para desmontar o volume, no console do agente do Arcserve UDP no computador de backup com base em host, clique em **Montar ponto de recuperação**, depois, em **Desmontar**.

Como restaurar os dados do Microsoft Office 365

Esta seção contém os seguintes tópicos:

Como restaurar dados da caixa de correio do Exchange Online

É possível restaurar dados da caixa de correio do Exchange Online (emails, calendários, contatos, notas, tarefas e assim por diante) na nuvem da Microsoft usando-se qualquer computador. Você pode restaurar dados do ponto de recuperação para o local original ou um local alternativo.

Execute as tarefas a seguir para restaurar os dados do Exchange Online:

1. Selecionar os itens de caixa de correio do Exchange Online a serem restaurados
2. Definir as opções de restauração
3. Restaurar os itens recuperáveis
4. Restaure o conteúdo do ponto de recuperação
5. Verificar se o conteúdo foi restaurado

Selecione os itens de email do Exchange Online a serem restaurados

É possível restaurar dados de email do Exchange Online a partir de um ponto de recuperação. Ao selecionar uma data de recuperação e, em seguida, especificar a hora, todos os pontos de recuperação associados a esse período são exibidos. Você pode procurar e selecionar o conteúdo do backup (incluindo aplicativos) a ser restaurado.

Siga estas etapas:

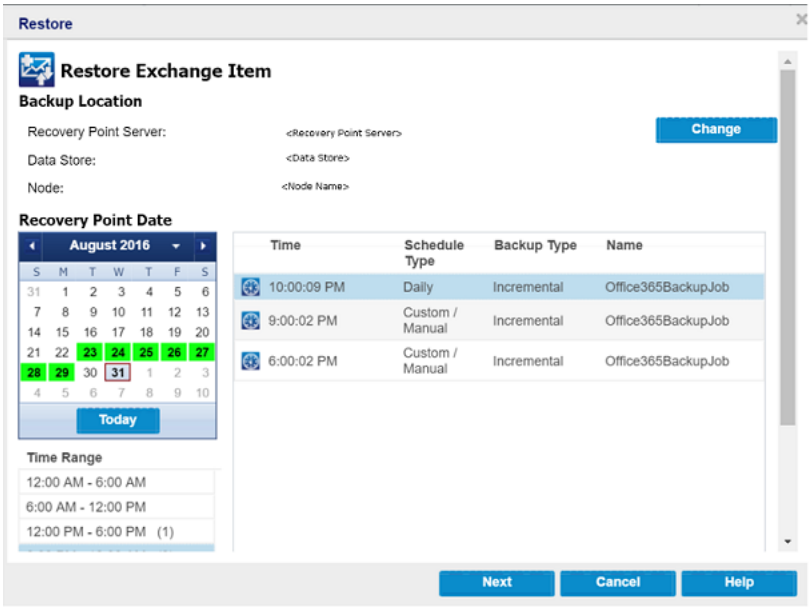
1. Efetue logon no Arcserve UDP.
2. Clique na guia **Recursos**.
3. Selecione **Todos os nós** no painel esquerdo.

   Todos os nós do adicionados são exibidos no painel central.
4. No painel central, selecione o nó do Exchange Online e clique em **Ações**.
5. Clique em **Restaurar** no menu suspenso Ações.

   A caixa de diálogo Restaurar item do Exchange é exibida.

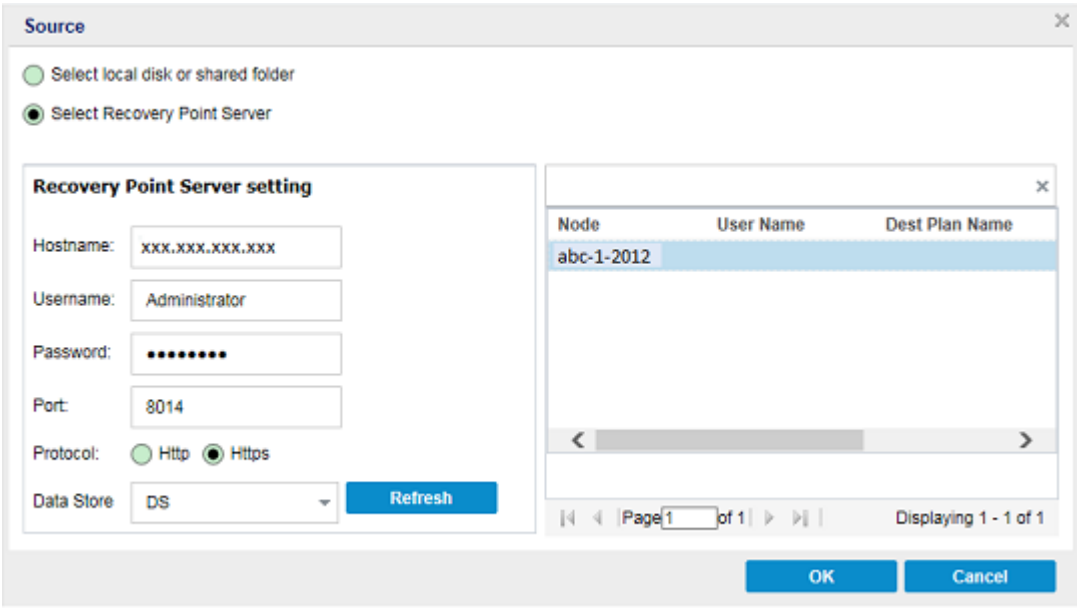
   Observação: você é automaticamente conectado ao nó do agente, e a caixa de diálogo Restaurar item do Exchange é aberta.

   É possível ver os detalhes do Servidor de ponto de recuperação no Local do backup.



6. (Opcional) Clique em **Alterar** se você quiser modificar o local do backup.

   A caixa de diálogo Origem é exibida. É possível selecionar o local do backup na caixa de diálogo.



   Observação: quando você adiciona uma tarefa de cópia em fita ao plano e deseja restaurar o ponto de recuperação de backup da cópia em fita, selecione o ponto de recuperação no backup da cópia em fita. Para obter mais informações, consulte Procurar ponto de recuperação de cópia em fita para restauração.

7. Para especificar a origem, selecione uma das opções a seguir e clique em **OK**:

   Selecionar o disco local ou uma pasta compartilhada

   Observação: no Arcserve UDP, não recomendamos que você marque a opção **Selecione o disco local ou uma pasta compartilhada**.

   Selecionar servidor de ponto de recuperação

   a. Especifique os detalhes da configuração do servidor de ponto de recuperação e clique em **Atualizar**.

      Todos os agentes estão listados na coluna Agente de proteção de dados na caixa de diálogo Origem.

   b. Selecione o agente na lista exibida e clique em **OK**.

      Os pontos de recuperação são listados na caixa de diálogo Restaurar item do Exchange.

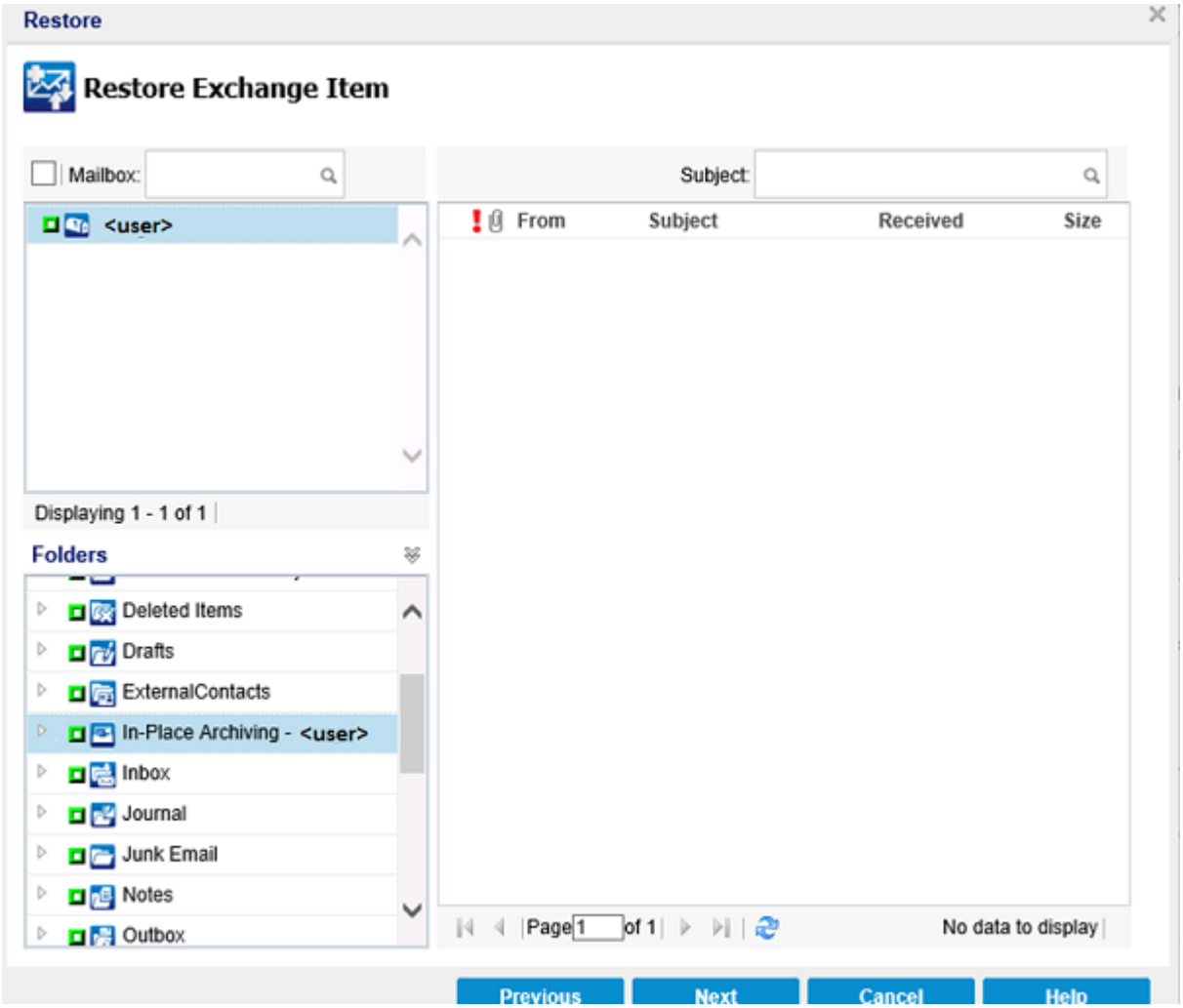
Observação: na Pasta do ponto de recuperação, você pode ver várias subpastas de mesmo nome junto com os nós do Exchange Online. Isso acontece porque a GUID do nó muda e uma nova pasta de ponto de recuperação é criada quando você exclui um nó e o adiciona novamente no plano de teste.

8. Selecione a data do calendário para a imagem de backup a ser restaurada e clique em **Avançar**.

   Todas as datas que contém pontos de recuperação para a origem do backup especificado são realçadas em verde.

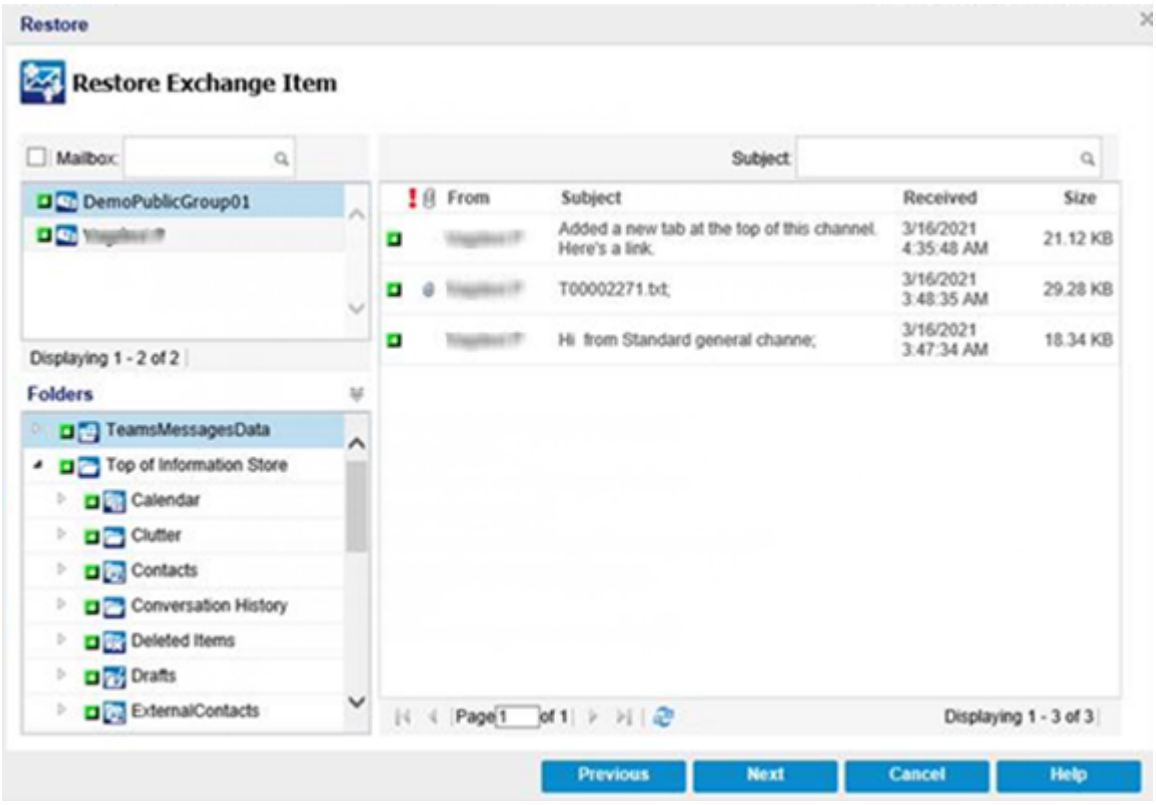
   Os pontos de recuperação correspondentes a essa data são exibidos, juntamente com a hora do backup, o tipo de backup que foi executado (completo, incremental ou de verificação) e o nome do backup.

9. No painel Caixa de correio, clique na caixa de correio que deseja restaurar.



Todos os itens de email relacionados à caixa de correio são exibidos sob o painel Pastas.

Observação: para o backup de grupos do Office 365 Exchange Online, a estrutura de pastas da caixa de correio do grupo é diferente da caixa de correio do usuário. As pastas da caixa de correio do grupo são mostradas na parte superior da pasta Armazenamento de informações. Por exemplo, quando o usuário faz backup de caixas de correio/listas de distribuição do grupo do AD, todas as pastas com backup efetuado são mostradas na parte superior da pasta Armazenamento de informações.



10. Selecione os itens ou pastas de email relacionados (incluindo a caixa de correio inteira, os emails, os calendários, os contatos, as notas, as tarefas e assim por diante) que você deseja restaurar a partir de Pastas e clique em **Avançar**.

    Observações:

    - É possível selecionar parte ou todo o conteúdo do objeto do Exchange a ser restaurado. Para selecionar o conteúdo parcial, expanda o objeto e clique na caixa de seleção do conteúdo.
    - Você pode selecionar vários objetos do Exchange a serem restaurados.

    A caixa de diálogo Opções de restauração é exibida.

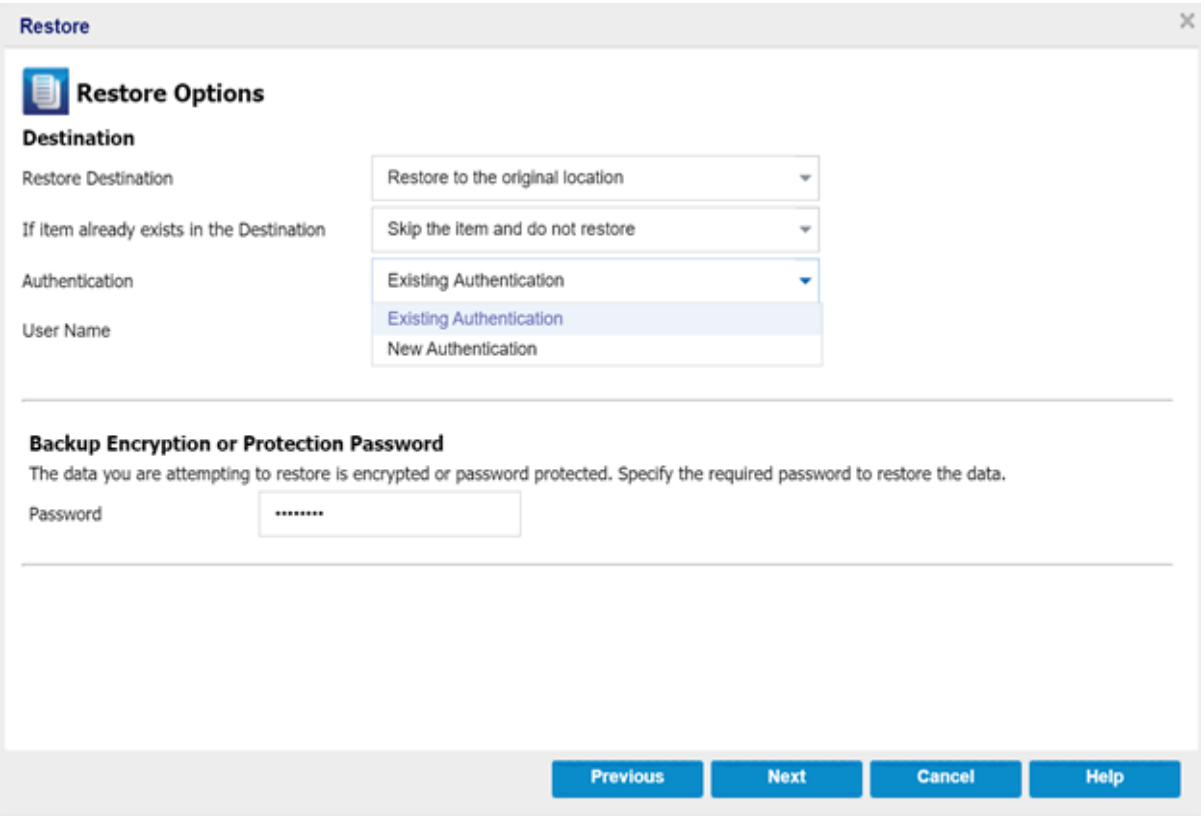
    Os itens de email do Exchange Online a serem restaurados são selecionados. Agora, você pode definir as opções de restauração.

Definir as opções de restauração

Depois de especificar as informações do Exchange Online a serem restauradas, defina as opções de restauração do conteúdo selecionado.

Siga estas etapas:

1. Na caixa de diálogo **Opções de restauração**, selecione o destino da restauração.



As opções de destino disponíveis são:

Restaurar no local original

Restaura os dados de email para o mesmo local do qual você fez um backup.

Observações:

- Se você restaurar um item de email no local original usando a opção Substituir duas vezes, após a restauração pela segunda vez, o item de email da primeira restauração não será substituído. Como resultado, dois itens de email semelhantes serão exibidos no local original.

- Se você restaurar um item de email no local original usando a opção Ignorar, e na pasta original um item semelhante ao item restaurado já existir, a tarefa de backup exibirá o resultado incompleto.

Restaure em um local alternativo.

Restaura os dados de email em outra caixa de correio ou outra pasta na caixa de correio original. Ao selecionar essa opção, procure e selecione o destino.

2. Especifique uma das opções a seguir no menu suspenso **Se o item já existir no destino**:

Ignorar o item e não restaurar

Ignora os itens e não restaura.

Padrão: ignorar o item e não restaurar.

Substituir o item no destino

Substitui o item no destino.

Observação: a lista suspensa **Se o item já existir no destino** ficará disponível se você selecionar a opção **Restaurar no local original** na lista suspensa **Restaurar o destino**.

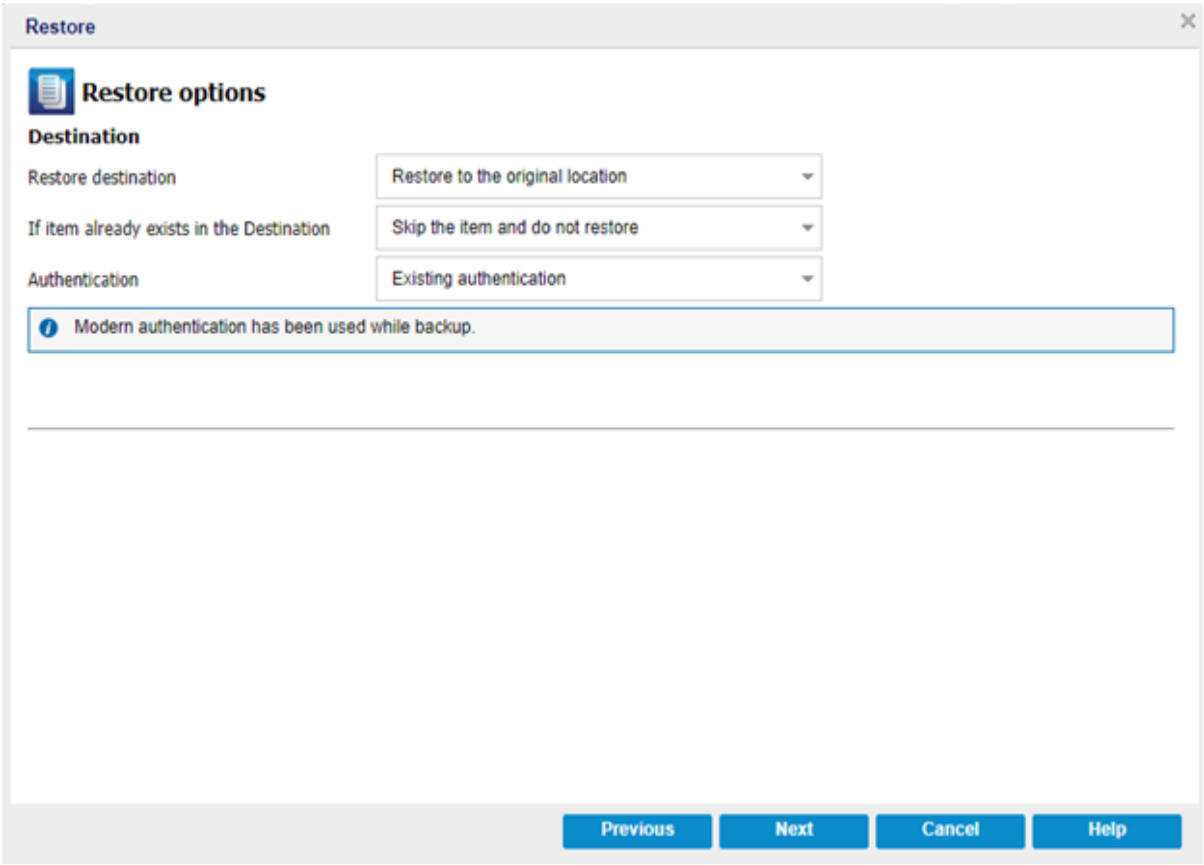
Autenticação

Valida e identifica a conta de usuário. Selecione uma das seguintes opções:

- **Autenticação existente**

  Quando você seleciona Autenticação existente, o tipo de autenticação que foi selecionado durante a criação do nó é usado.

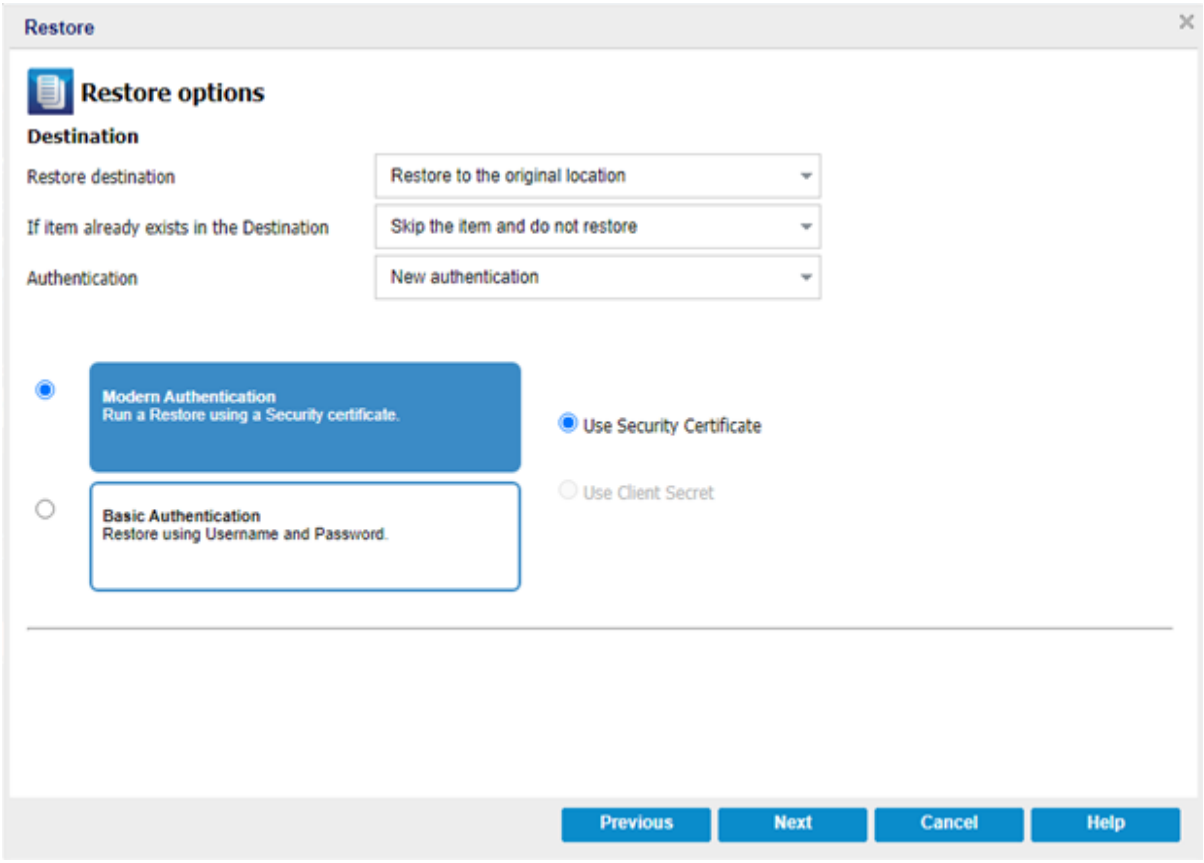
  - Se a autenticação do nó for básica, parâmetros como Nome de usuário, Senha e Criptografia de backup ou proteção por senha [se criptografada], serão carregados automaticamente para prosseguir com a restauração.
  - Se a autenticação do nó for moderna, parâmetros como Nome de usuário e Criptografia de backup ou proteção por senha [se criptografada], serão carregados automaticamente para prosseguir com a restauração.



- **Nova autenticação**

  Durante a restauração, é possível selecionar uma das seguintes opções para alterar o tipo de autenticação:

  - Autenticação moderna
  - Autenticação básica



3. Para aplicar a autenticação, siga um destes procedimentos:

   Autenticação moderna

   Para a autenticação moderna, é possível executar uma restauração usando o certificado de segurança.

   Usar certificado de segurança

   Observação: por padrão, o plano de backup seleciona **Usar certificado de segurança** para a autenticação moderna.

   Siga estas etapas:

   a. Para autenticar usando um certificado autoassinado, consulte Fazendo download do certificado do UDP e carregando-o no Azure.

   b. Digite a ID do aplicativo e o nome do usuário.

   c. Para aplicar as funções e permissões necessárias, marque a caixa de seleção **Permitir que o Arcserve UDP defina as funções e permissões necessárias do Azure para este aplicativo** e clique em **Avançar**.

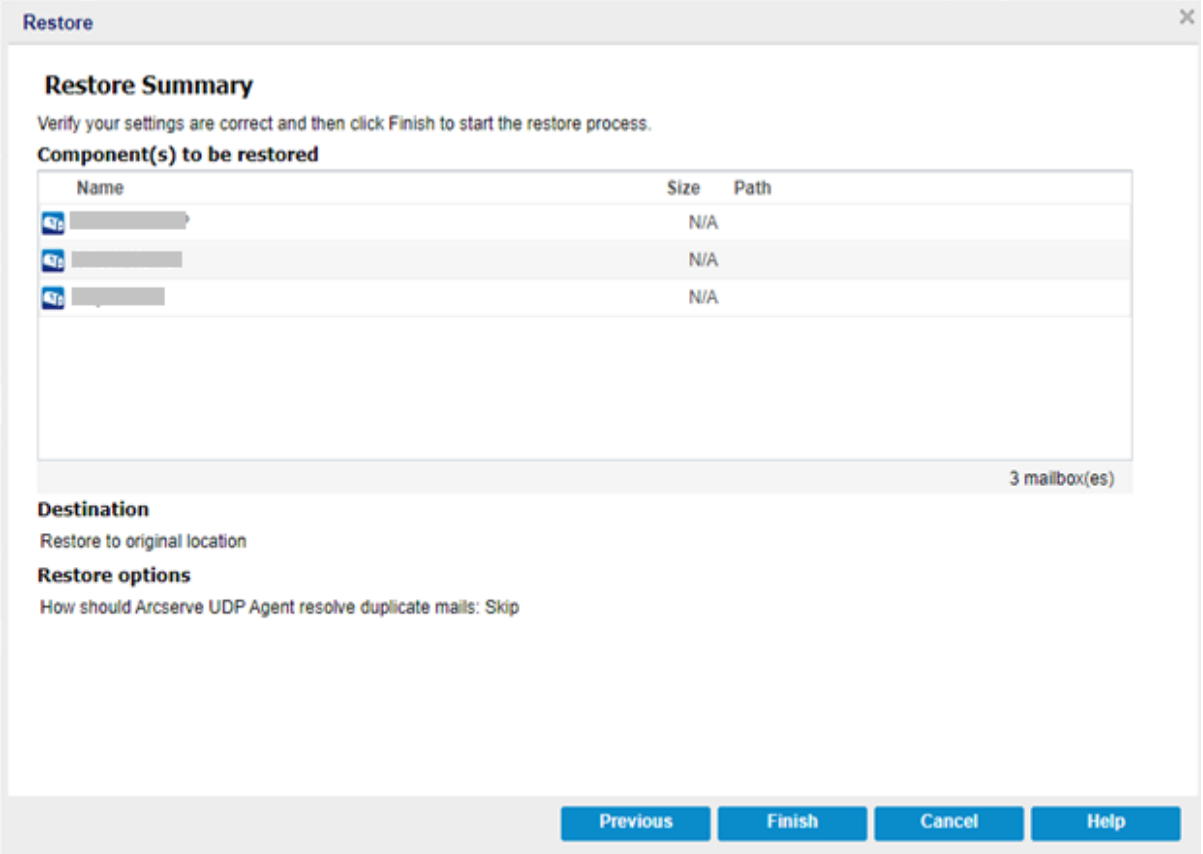
Autenticação básica

Para Autenticação básica, para continuar com a restauração, digite o nome do usuário e a senha.

Observação: essa opção falhará se a autenticação moderna estiver ativada no locatário ou na conta.

4. Clique em **Avançar**.

   A caixa de diálogo **Resumo da restauração** é exibida.



5. Na janela Resumo da restauração, verifique as configurações e clique em **Concluir**.

As opções de restauração são definidas para restaurar as informações do Exchange Online.

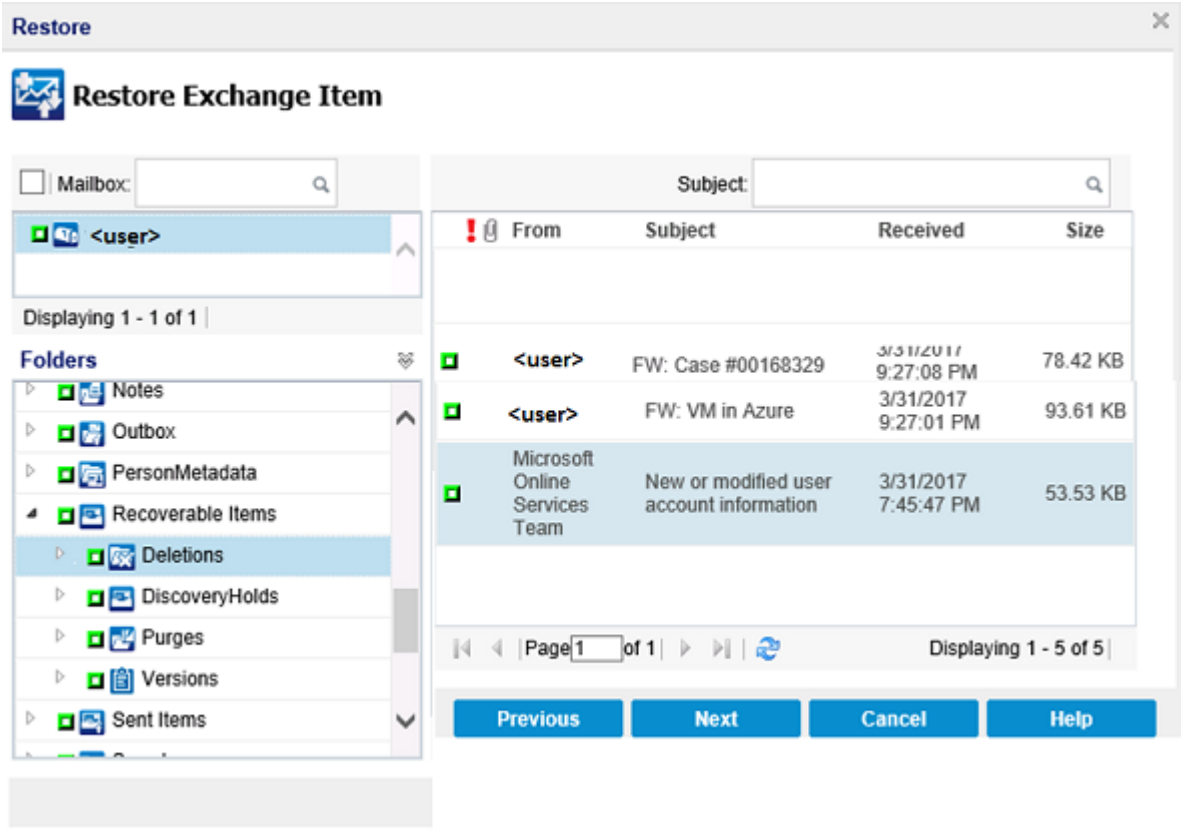
Restaurar os itens recuperáveis

Você pode restaurar os itens recuperáveis da caixa de correio que ativa o recurso Retenção local ou Retenção de litígio, pela IU do nó do Exchange Online, para procurar a sessão de backup. Para ativar esse recurso, consulte Especificar a origem.

Depois de ativar o recurso, usando o Assistente de restauração, é possível restaurar os itens recuperáveis.

Siga estas etapas:

1. Na caixa de diálogo **Restaurar item do Exchange**, selecione as pastas desejadas em **Itens recuperáveis** e clique em **Avançar**.



A tela Opção de restauração é exibida.

2. Na tela Opção de restauração, siga os passos abaixo e clique em **Avançar**:
   - Selecione o destino da restauração.
   - Caso o item já exista no destino, ignore-o ou substitua-o.

   Você pode executar uma restauração Original ou Alternativa.

   Restauração original

Os itens em Itens recuperáveis são restaurados na pasta *UDP_RecoverableItems_yyyyMMdd_HHmmssfff*, que é criada na caixa de correio de destino. As opções Ignorar e Substituir apresentadas para restauração não se aplicam a esses itens.

Restauração alternativa

Como ocorre com a caixa de correio do usuário, os itens selecionados são restaurados no caminho de destino em uma pasta exclusiva com carimbo de data/hora, como *titled /restore_yyyyMMdd-mmssff*.

- Forneça a ID de usuário e senha do destino onde você deseja restaurar os itens.

Os itens recuperáveis selecionados são restaurados.

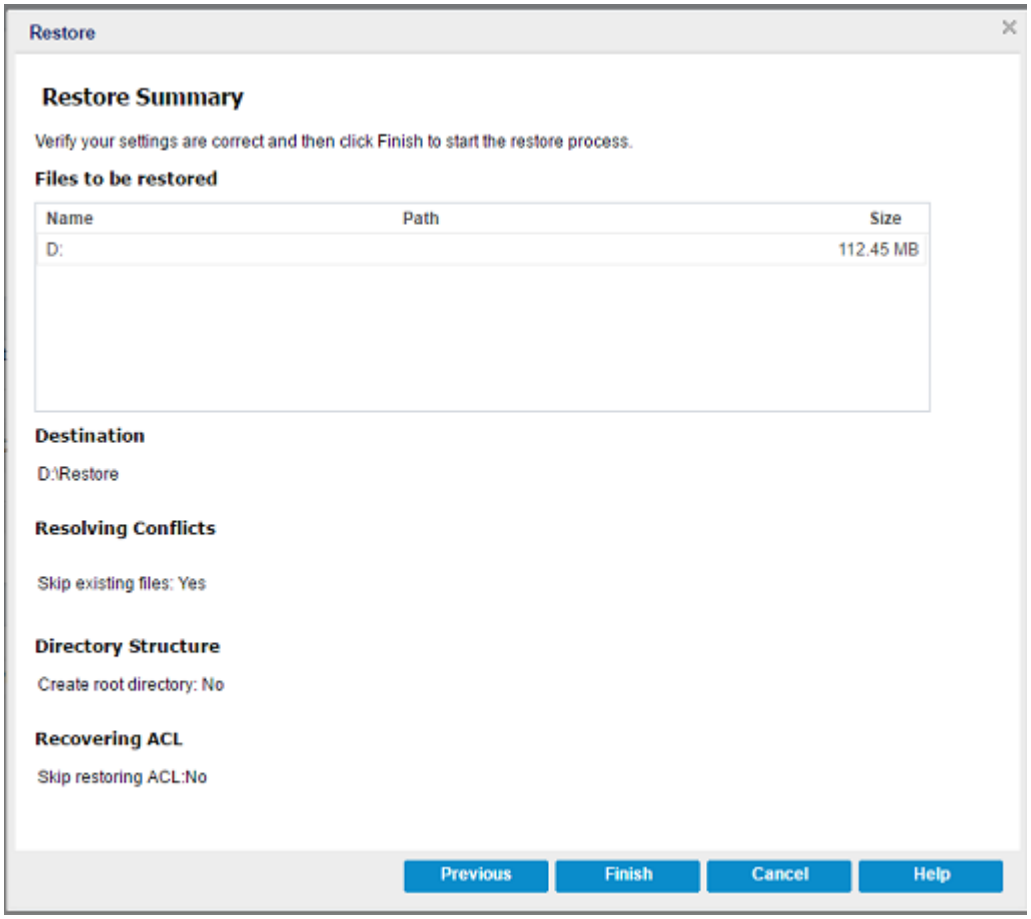
O ponto de recuperação do conteúdo é guardado.

Restaurar o conteúdo do ponto de recuperação

Após definir as opções de restauração, verifique se suas configurações estão corretas e confirme o processo de restauração. O **Resumo da restauração** o auxilia a revisar todas as opções de restauração definidas e modificá-las se necessário.

Siga estas etapas:

1. Na caixa de diálogo **Resumo da restauração**, examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.



   - Se as informações do resumo não estiverem corretas, clique em **Anterior** e volte à caixa de diálogo em questão para alterar a configuração incorreta.
   - Se as informações de resumo estiverem corretas, clique em **Concluir** para iniciar a tarefa de restauração.

O ponto de recuperação do conteúdo é guardado.

Verificar se o conteúdo foi restaurado

Após a conclusão do processo de restauração, verifique se o conteúdo foi restaurado no destino especificado.

Siga estas etapas:

1. Efetue logon na caixa de correio de destino.
2. Verifique o item de caixa de correio que você restaurou.
3. Verifique o conteúdo restaurado.

   A restauração do conteúdo é verificada com êxito.

Como restaurar dados da coleção de sites do SharePoint Online

É possível restaurar a lista/biblioteca ou item da lista do SharePoint Online no site ou no site principal do SharePoint. Você pode restaurar os dados ao site original usando o novo nome, restaurar os dados ao local original e exportar para o disco a partir dos pontos de recuperação.

Execute as seguintes tarefas para restaurar item de lista do SharePoint Online:

1. Selecionar itens de lista do site do SharePoint Online para restauração
2. Definir as opções de restauração
3. Verificar se o conteúdo foi restaurado

Selecionar itens de lista do site do SharePoint Online para restauração

É possível restaurar dados de itens de lista do SharePoint Online a partir de um ponto de recuperação. Ao selecionar uma data de recuperação e, em seguida, especificar a hora, todos os pontos de recuperação associados a esse período são exibidos. Você pode procurar e selecionar o conteúdo do backup (incluindo aplicativos) a ser restaurado.

Siga estas etapas:

1. Efetue logon no Arcserve UDP.
2. Clique na guia **Recursos**.
3. Selecione **Todos os nós** no painel esquerdo.

   Todos os nós do adicionados são exibidos no painel central.

   Ou

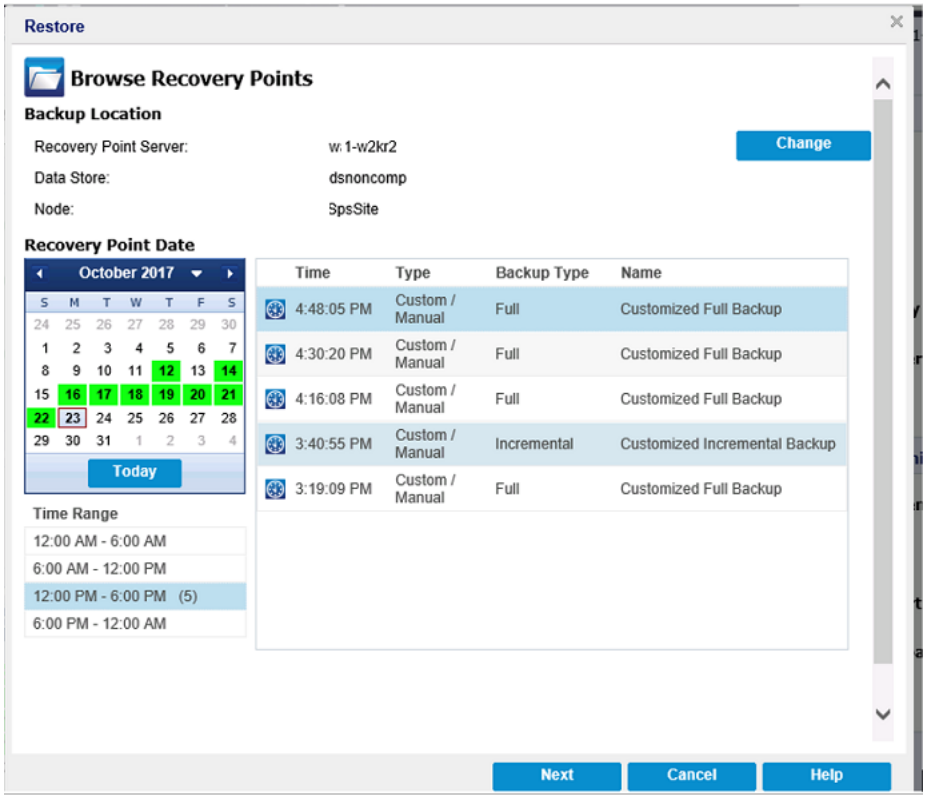
   Selecione o grupo **Nós do SharePoint Online**.

   Todos os nós do SharePoint adicionados são exibidos no painel central.
4. No painel central, selecione o nó do SharePoint Online e clique em **Ações**.
5. Clique em **Restaurar** no menu suspenso **Ações**.

   A caixa de diálogo **Restaurar item do SharePoint** é exibida.

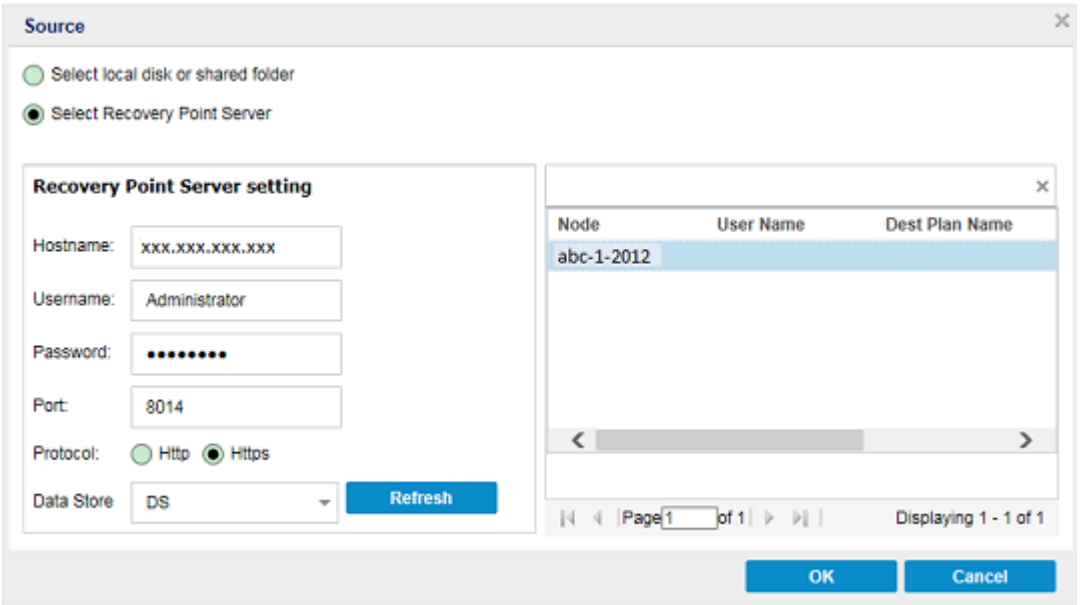
   Observação: você é automaticamente conectado ao nó do agente, e a caixa de diálogo **Restaurar item do SharePoint** é aberta.

   O **Local do backup** exibe os detalhes do **Servidor de ponto de recuperação**.



6. (Opcional) Clique em **Alterar** para modificar o local do backup.

   A caixa de diálogo **Origem** é exibida. É possível selecionar o local do backup na caixa de diálogo.



Observação: quando você adiciona uma tarefa de cópia em fita ao plano e deseja restaurar o ponto de recuperação de backup da cópia em fita, selecione o ponto de

recuperação no backup da cópia em fita. Para obter mais informações, consulte Procurar ponto de recuperação de cópia em fita para restauração.

7. Para especificar a origem, selecione uma das opções a seguir e clique em **OK**:

   Selecionar o disco local ou uma pasta compartilhada

   Observação: no Arcserve UDP, não recomendamos que você marque a opção **Selecione o disco local ou uma pasta compartilhada**.

   Selecionar servidor de ponto de recuperação

   a. Especifique os detalhes da configuração do Servidor de ponto de recuperação e clique em **Atualizar**.

      Todos os agentes estão listados na coluna Agente de proteção de dados na caixa de diálogo **Origem**.

   b. Selecione o agente na lista/biblioteca exibida e clique em **OK**.

      Os pontos de recuperação são listados na caixa de diálogo **Restaurar item do SharePoint**.

8. Selecione a data do calendário para a imagem de backup a ser restaurada e clique em **Next**.

   Todas as datas que contém pontos de recuperação para a origem do backup especificado são realçadas em verde.

   Os pontos de recuperação correspondentes a essa data são exibidos, juntamente com a hora do backup, o tipo de backup que foi executado (completo ou incremental) e o nome do backup.

9. Na caixa de diálogo **Restaurar itens do SharePoint Online**, expanda a coleção de sites.

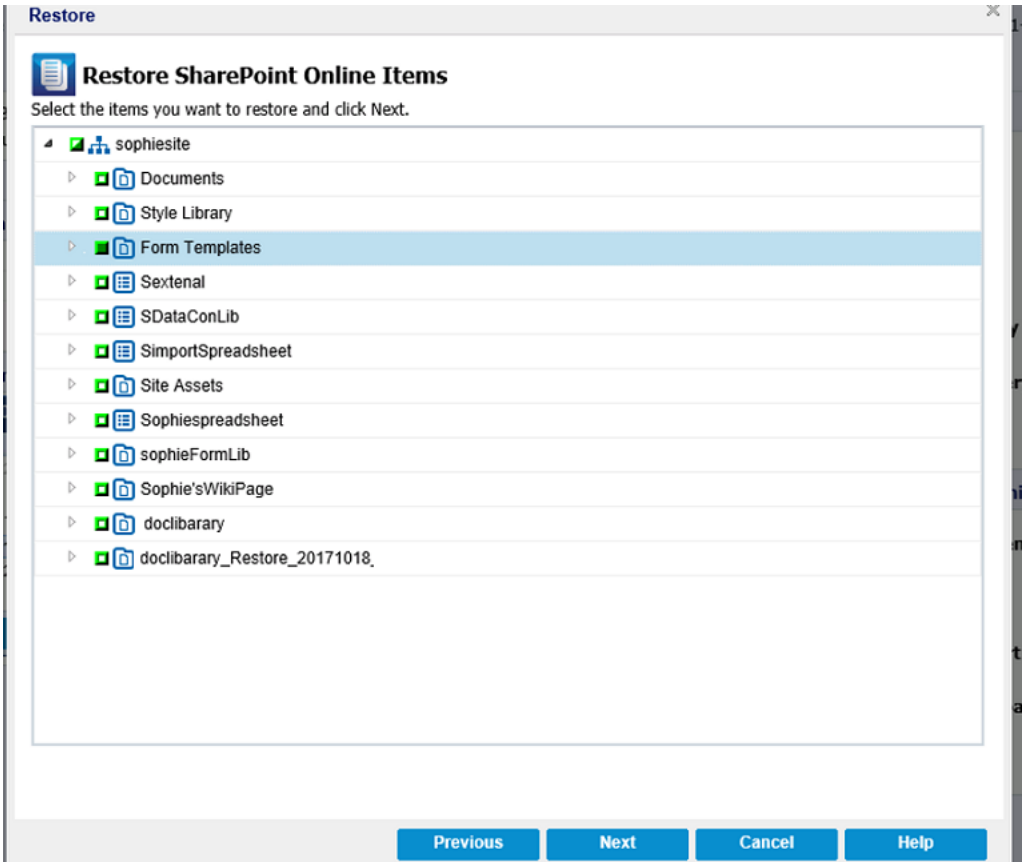
   Todas as listas/bibliotecas e os itens de lista são exibidos.

10. Selecione a lista/biblioteca ou o item disponível na coleção de sites que você deseja restaurar da coleção de sites do SharePoint e clique em **Avançar**.

    Observações:

    - É possível selecionar parte ou todo o conteúdo do objeto do SharePoint a ser restaurado. Para selecionar o conteúdo parcial, expanda o objeto e clique na caixa de seleção do conteúdo.
    - É possível selecionar várias listas/bibliotecas ou itens de lista do SharePoint para restaurar.

    A caixa de diálogo **Opções de restauração** é exibida.



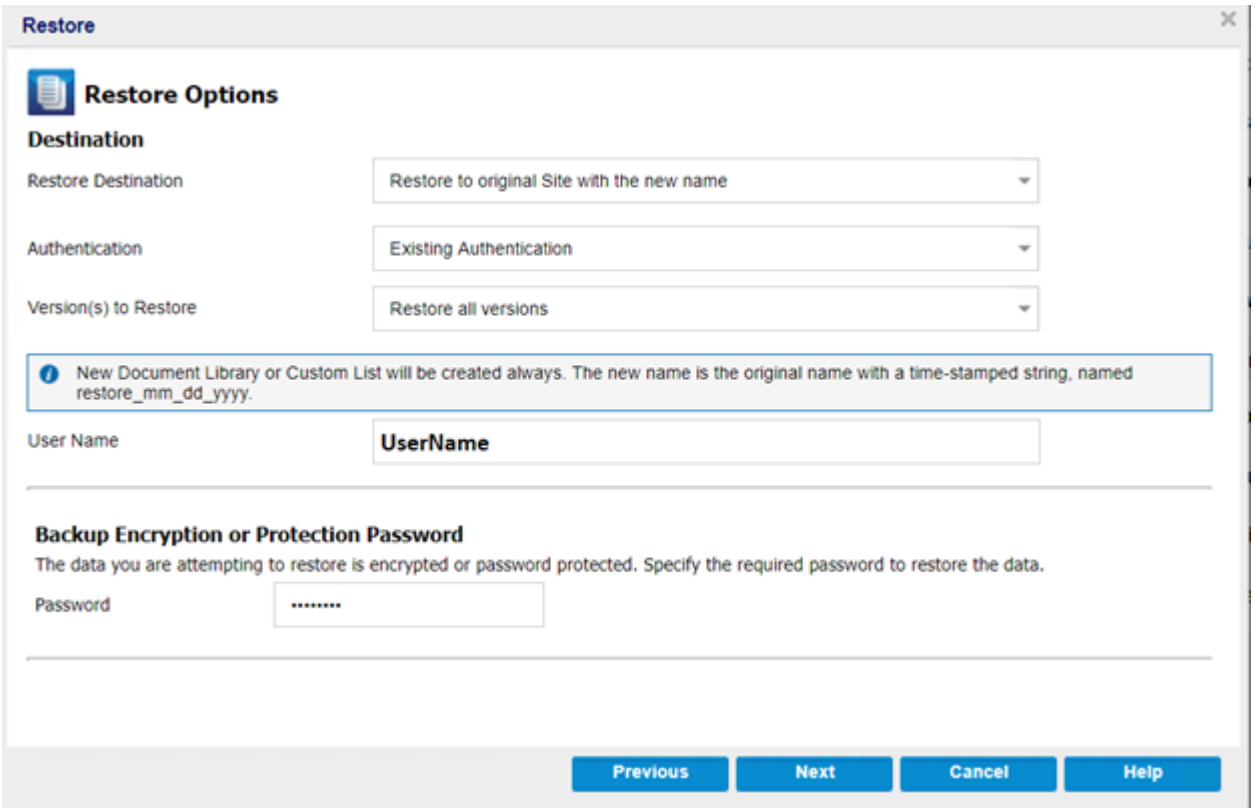
As listas/bibliotecas ou os itens de lista do SharePoint Online a serem restaurados são selecionados. Agora, você pode definir as opções de restauração.

Definir as opções de restauração

Depois de especificar as informações do SharePoint Online a serem restauradas, defina as opções de restauração do conteúdo selecionado.

Siga estas etapas:

1. Na caixa de diálogo **Opções de restauração**, selecione o destino da restauração.



As opções de destino disponíveis são:

Restaurar no site original com o novo nome

Restaura os dados da lista/biblioteca e dos itens de lista no mesmo site de onde você pegou um backup com um novo nome de lista.

Restaurar para o local original

Restaura os dados da lista/biblioteca e dos itens de lista no mesmo local de onde você pegou um backup.

2. Especifique uma das opções a seguir no menu suspenso **Se o item já existir no destino**:

Acrescentar como versão nova se o controle de versão estiver ativado

Essa opção funciona quando sua configuração de versão está ativada na configuração da biblioteca no site do SharePoint. Depois que você selecionar essa

opção, a nova versão será acrescentada às versões atuais dos itens de lista se os itens de lista forem existentes.

Ignorar o item e não restaurar

Ignora os itens e não restaura.

Substituir o item no destino

Substitui o item no destino.

Exportar para o disco

Restaura as listas/bibliotecas ou os itens de lista da coleção de sites em uma pasta ou em uma pasta compartilhada no disco.

Observação: na restauração de listas quando a opção de restauração Exportar para o disco é selecionada, exporte somente o(s) anexo(s) da lista para o disco.

Autenticação

Valida e identifica a conta de usuário. Selecione uma das seguintes opções:

- **Autenticação existente**

  Quando você seleciona Autenticação existente, o tipo de autenticação que foi selecionado durante a criação do nó é usado.

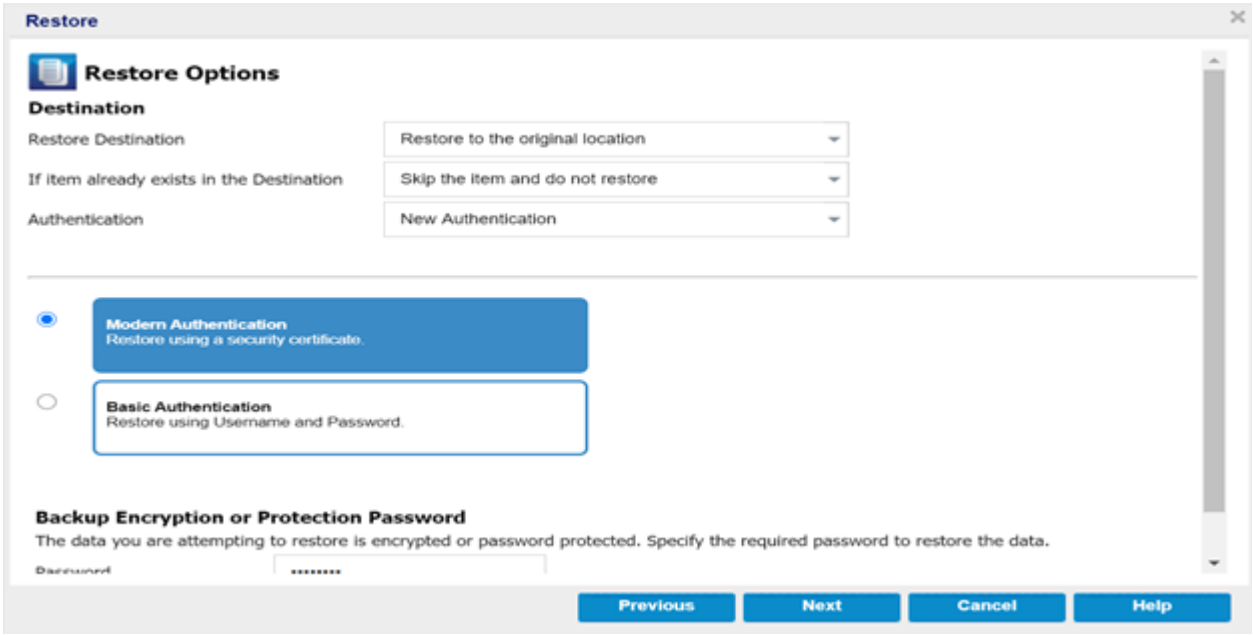
  - Se a autenticação do nó for básica, parâmetros como Nome de usuário, Senha e Criptografia de backup ou proteção por senha [se criptografada], serão carregados automaticamente para prosseguir com a restauração.
  - Se a autenticação do nó for moderna, parâmetros como Nome de usuário e Criptografia de backup ou proteção por senha [se criptografada], serão carregados automaticamente para prosseguir com a restauração.

- **Nova autenticação**

  Durante a restauração, é possível selecionar uma das seguintes opções para alterar o tipo de autenticação:

  - Autenticação moderna

- Autenticação básica



3. Para aplicar a autenticação, siga um destes procedimentos:

Autenticação moderna

Para a autenticação moderna, é possível executar uma restauração usando o certificado de segurança.

Usar certificado de segurança

Observação: por padrão, o plano de backup seleciona **Usar certificado de segurança** para a autenticação moderna.

Siga estas etapas:

a. Para autenticar usando um certificado autoassinado, consulte Fazendo download do certificado do UDP e carregando-o no Azure.

b. Digite a ID do aplicativo e o nome do usuário.

c. Para aplicar as funções e permissões necessárias, marque a caixa de seleção **Permitir que o Arcserve UDP defina as funções e permissões necessárias do Azure para este aplicativo** e clique em **Avançar**.

Autenticação básica

Na autenticação básica, para continuar com a restauração, digite o nome de usuário e a senha.

Observação: essa opção falhará se a autenticação moderna estiver ativada no locatário ou na conta.

4. Especifique as versões do item de lista que você quer restaurar quando sua configuração de versão estiver ativada na configuração da biblioteca no site do SharePoint.

   Restaurar todas as versões

   Restaura todas as versões do backup.

   Restaurar somente a versão mais recente

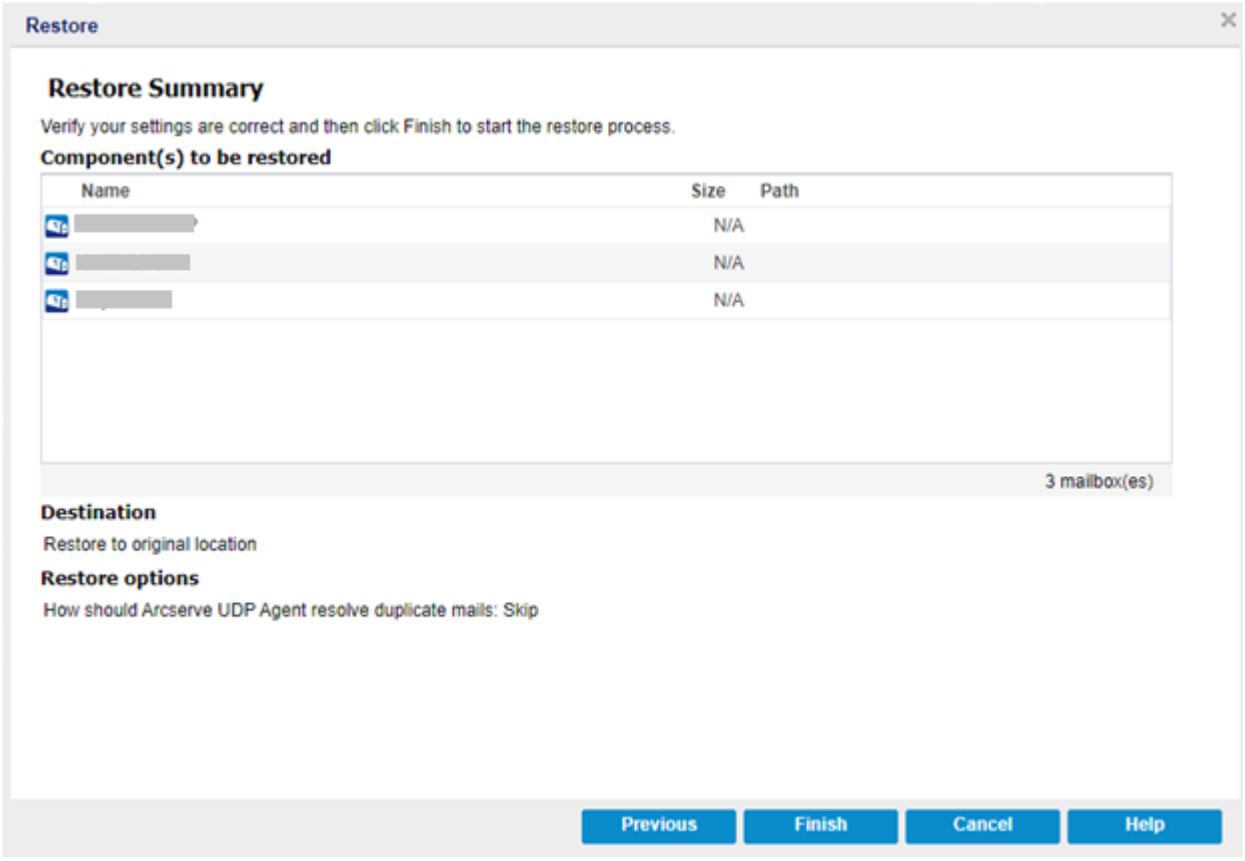
   Restaura somente a versão mais recente no backup.

   Restaurar somente a versão principal mais recente

   Restaura somente a versão principal mais recente no backup.

5. Especifique a senha da sessão, se houver.
6. Clique em **Avançar**.

   A caixa de diálogo **Resumo da restauração** é exibida.



   É possível verificar as informações da restauração na caixa de diálogo Resumo da restauração.

7. Clique em **Concluir** para enviar a tarefa de restauração.

   As opções de restauração são definidas para restaurar as informações do SharePoint Online.

Verificar se o conteúdo foi restaurado

Após a conclusão do processo de restauração, verifique se o conteúdo foi restaurado no destino especificado.

Siga estas etapas:

1. Efetue logon na coleção de sites do SharePoint.
2. Verifique a lista/biblioteca e os itens de lista.
3. Verifique o conteúdo restaurado.

   A restauração do conteúdo é verificada com êxito.

Como restaurar dados do OneDrive

É possível restaurar dados do OneDrive (arquivos, pastas e outros) usando qualquer computador. Você pode restaurar usando a opção de restauração ou, também, usando a opção de montagem de volume na interface do usuário do agente.

Execute as seguintes tarefas para restaurar dados do OneDrive usando a opção de restauração:

1. Selecionar itens do OneDrive a serem restaurados
2. Definir as opções de restauração
3. Exibir o resumo da restauração

Ou

Restaurar dados do OneDrive usando a opção de montagem de volume.

Selecionar itens do OneDrive a serem restaurados

É possível restaurar dados do OneDrive a partir de um ponto de recuperação. Ao selecionar uma data de recuperação e, em seguida, especificar a hora, todos os pontos de recuperação associados a esse período são exibidos. Você pode procurar e selecionar o conteúdo do backup (incluindo aplicativos) a ser restaurado.

Siga estas etapas:

1. Efetue logon no Arcserve UDP.
2. Clique na guia **Recursos**.
3. Selecione **Todos os nós** no painel esquerdo.

   Todos os nós do adicionados são exibidos no painel central.
4. No painel central, selecione o nó do OneDrive e clique em **Ações**.
5. Clique em **Restaurar** no menu suspenso **Ações**.

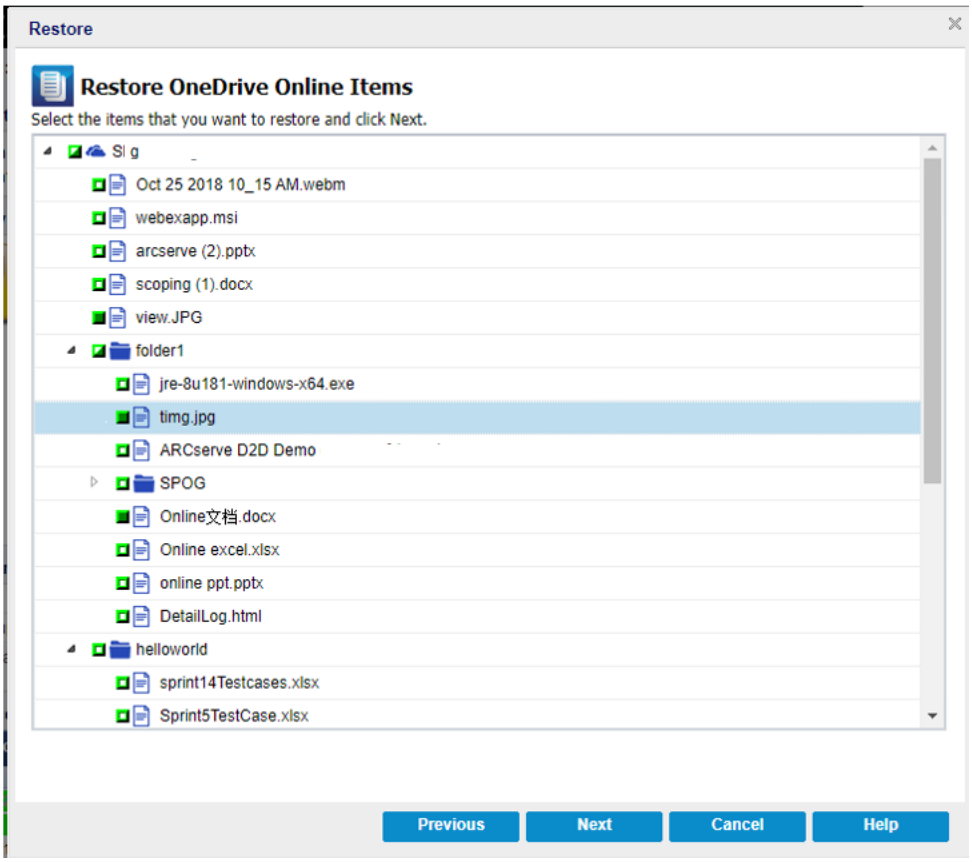
   Observação: você é automaticamente conectado ao nó do agente, e a caixa de diálogo **Nó** é aberta.

   É possível exibir os detalhes de **Procurar pontos de recuperação** no Local do backup. O nome do *Servidor de ponto de recuperação* selecionado é exibido. Se desejar, clique em **Alterar** e modifique a **configuração de Servidor de ponto de recuperação** na janela pop-up **Origem**.

   Observação: quando você adiciona uma tarefa de cópia em fita ao plano e deseja restaurar o ponto de recuperação de backup da cópia em fita, selecione o ponto de recuperação no backup da cópia em fita. Para obter mais informações, consulte Procurar ponto de recuperação de cópia em fita para restauração.
6. Selecione a data do calendário para a imagem de backup a ser restaurada e clique em **Next**.

   Todas as datas que contém pontos de recuperação para a origem do backup especificado são realçadas em verde.

   Os pontos de recuperação correspondentes a essa data são exibidos, juntamente com a hora do backup, o tipo de backup que foi executado (completo ou incremental) e o nome do backup.
7. No painel **Restaurar itens do OneDrive Online**, marque as caixas de seleção de itens ou pastas relacionadas que deseja restaurar a partir de Pastas e clique em **Avançar**.



Observações:

- É possível selecionar parte ou todo o conteúdo do objeto do OneDrive para restauração. Para selecionar o conteúdo parcial, expanda o objeto e clique na caixa de seleção do conteúdo.
- Você pode selecionar vários objetos do OneDrive para restauração.

A caixa de diálogo **Opções de restauração** é exibida.

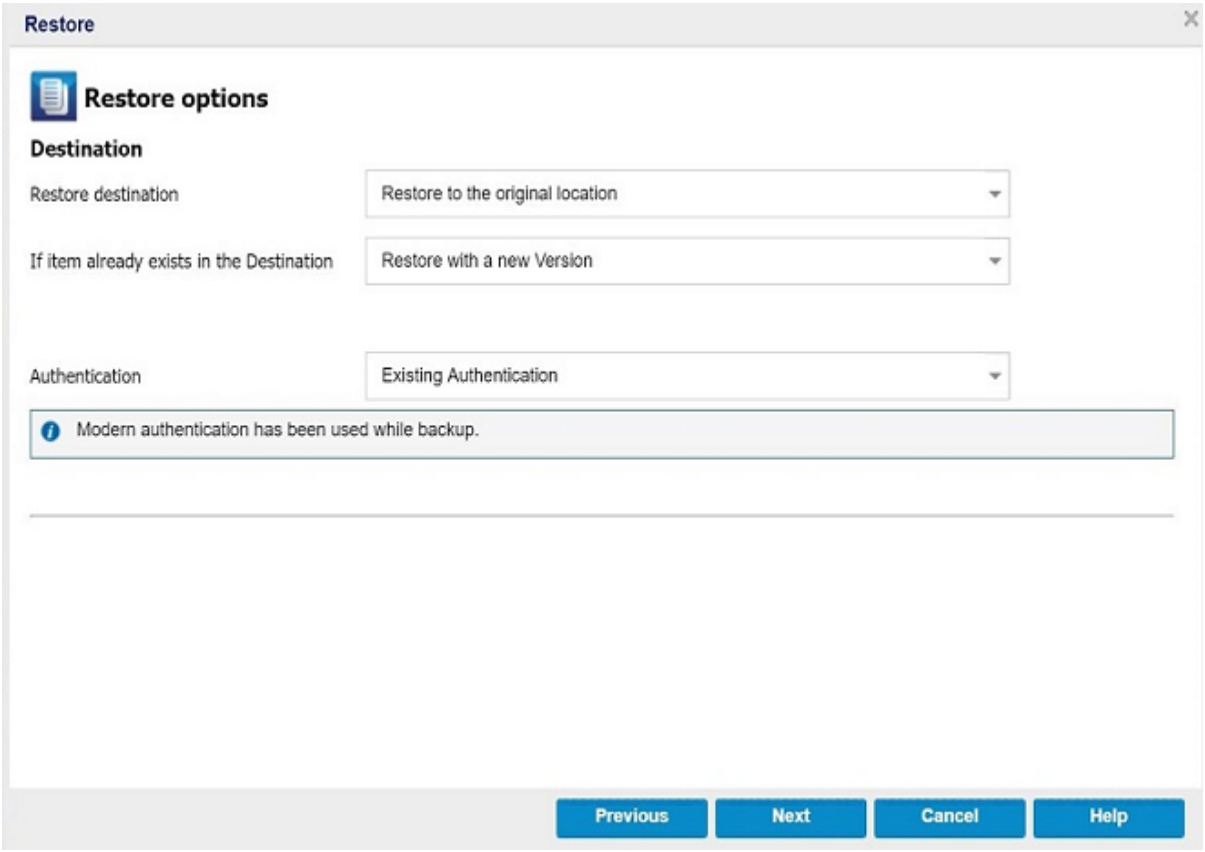
Os itens do nó do OneDrive a serem restaurados são selecionados. Agora, você pode definir as opções de restauração.

Definir as opções de restauração

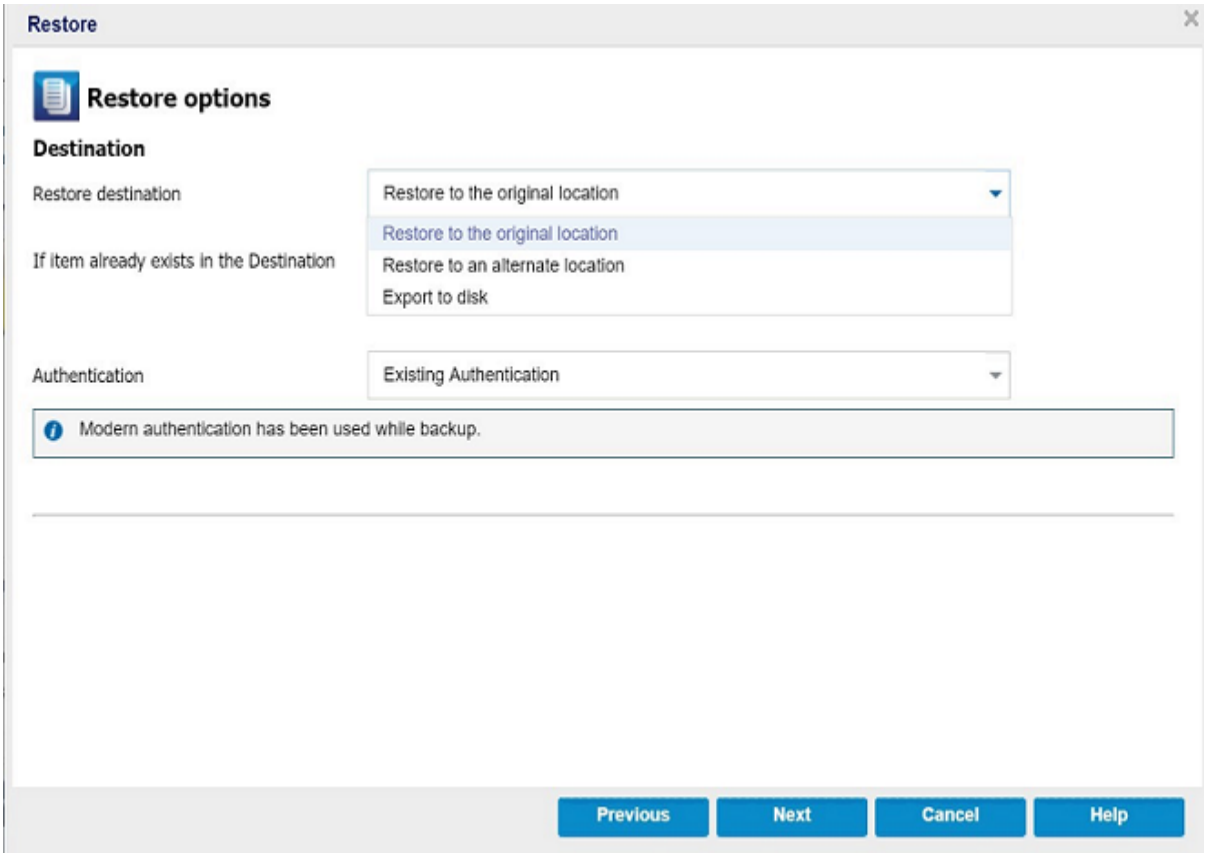
Depois de especificar as informações do OneDrive a serem restauradas, defina as opções de restauração para o conteúdo selecionado.

Siga estas etapas:

1. Na caixa de diálogo **Opções de restauração**, selecione o destino da restauração.



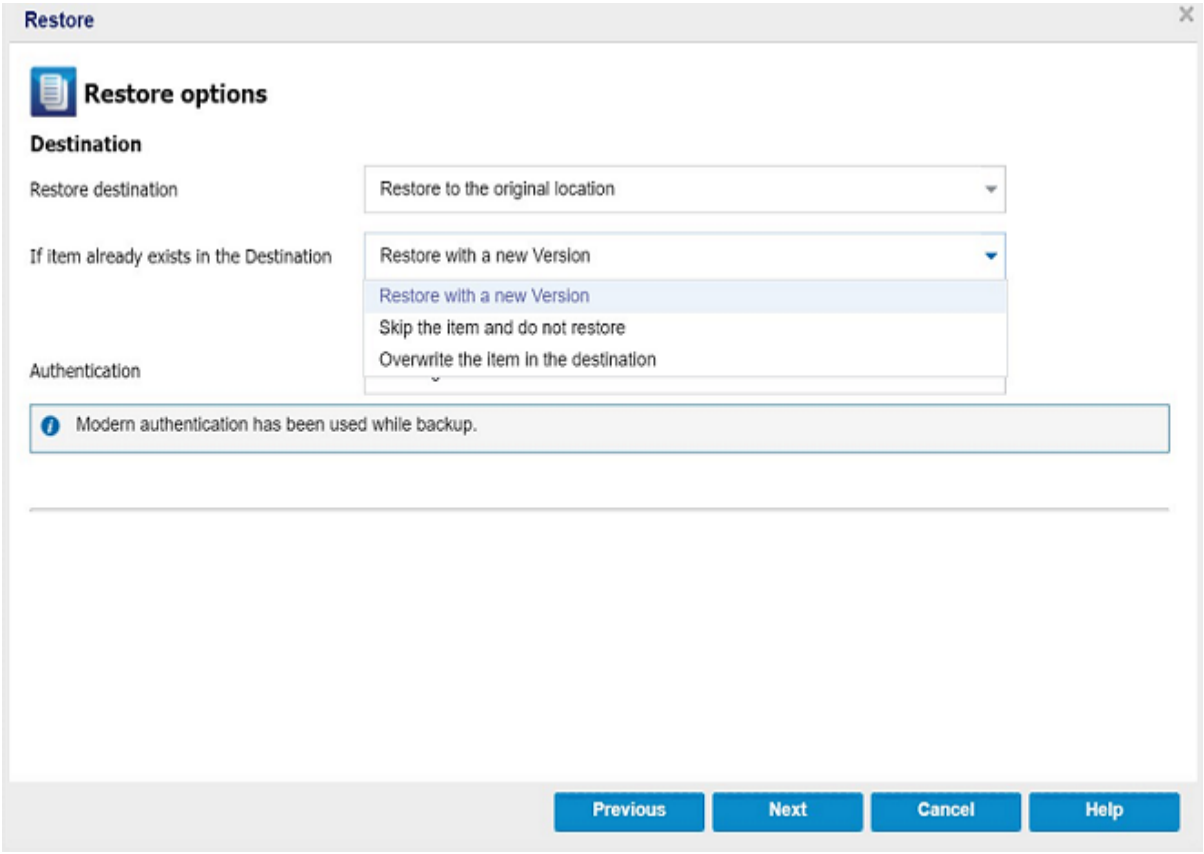
As opções de destino disponíveis são:



Restaurar para o local original

Restaura os arquivos ou pastas para o mesmo local do qual você fez um backup.

Se você selecionar a opção **Restaurar no local original**, na lista suspensa **Se o item já existir no destino**, selecione uma das seguintes opções:



Restaurar com uma nova versão

Anexa uma nova versão aos arquivos existentes.

Esta opção é selecionada por padrão.

Ignorar o item e não restaurar

Ignora os itens e não restaura.

Substituir o item no destino

Substitui o item no destino.

Restaure em um local alternativo.

Restaura os arquivos, pastas ou contas para uma conta no local alternativo. Ao selecionar essa opção, procure e selecione o destino.

Hierarquia da origem

Mantém a árvore hierárquica conforme especificado na origem ao criar planos de backup.

Observação: essa opção é exibida apenas quando a opção Restaurar para um local alternativo é selecionada.

Exportar para o disco

Restaura na pasta ou na pasta compartilhada no disco.

2. Para validar e identificar a conta do usuário, na lista suspensa **Autenticação**, selecione uma das seguintes opções:

   Autenticação existente

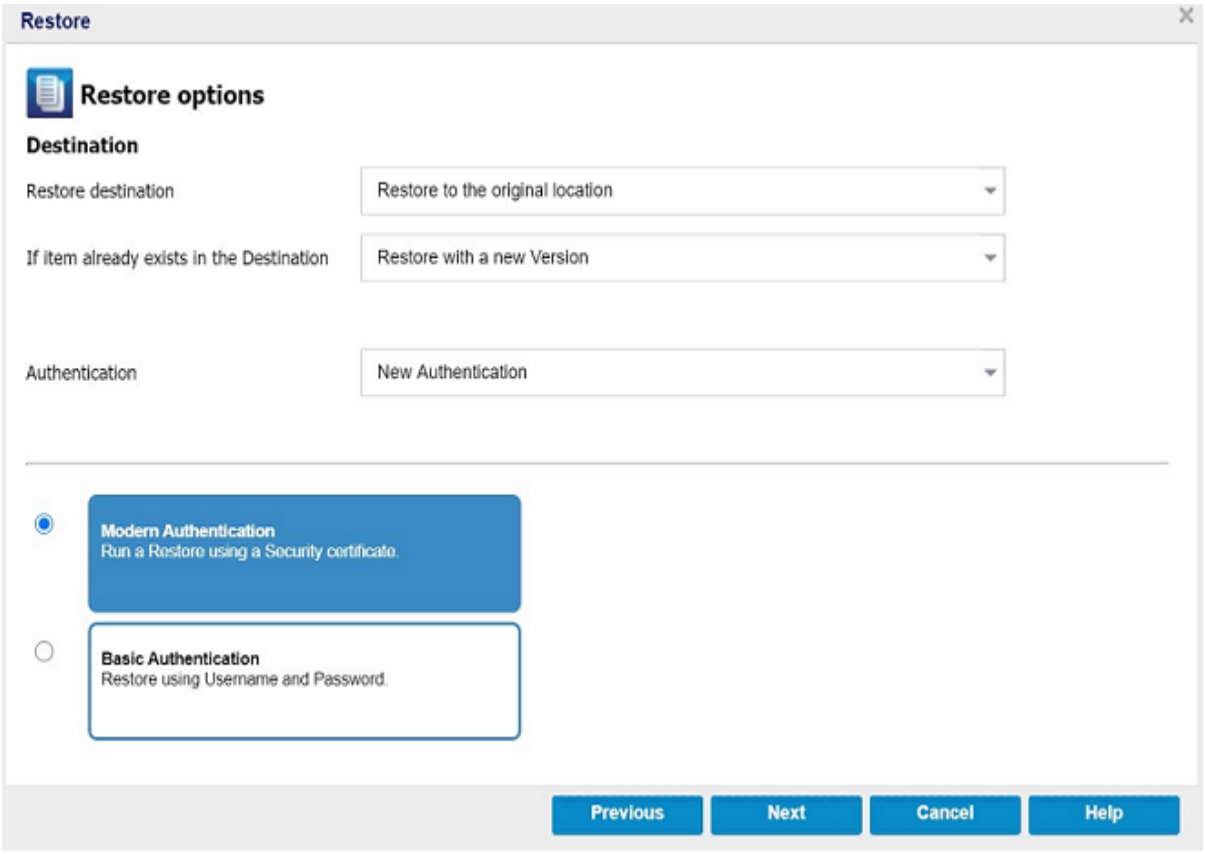
   Quando você seleciona Autenticação existente, o tipo de autenticação que foi selecionado durante a criação do nó é usado.

   - Se a autenticação do nó for básica, parâmetros como Nome de usuário, Senha e Criptografia de backup ou proteção por senha [se criptografada], serão carregados automaticamente para prosseguir com a restauração.
   - Se a autenticação do nó for moderna, parâmetros como Nome de usuário e Criptografia de backup ou proteção por senha [se criptografada], serão carregados automaticamente para prosseguir com a restauração.

   Nova autenticação

   Durante a restauração, é possível selecionar uma das seguintes opções para alterar o tipo de autenticação:

   - Autenticação moderna
   - Autenticação básica



3. Para aplicar a nova autenticação, siga um destes procedimentos:

Autenticação moderna

Para a autenticação moderna, é possível executar uma restauração usando o certificado de segurança.

Siga estas etapas:

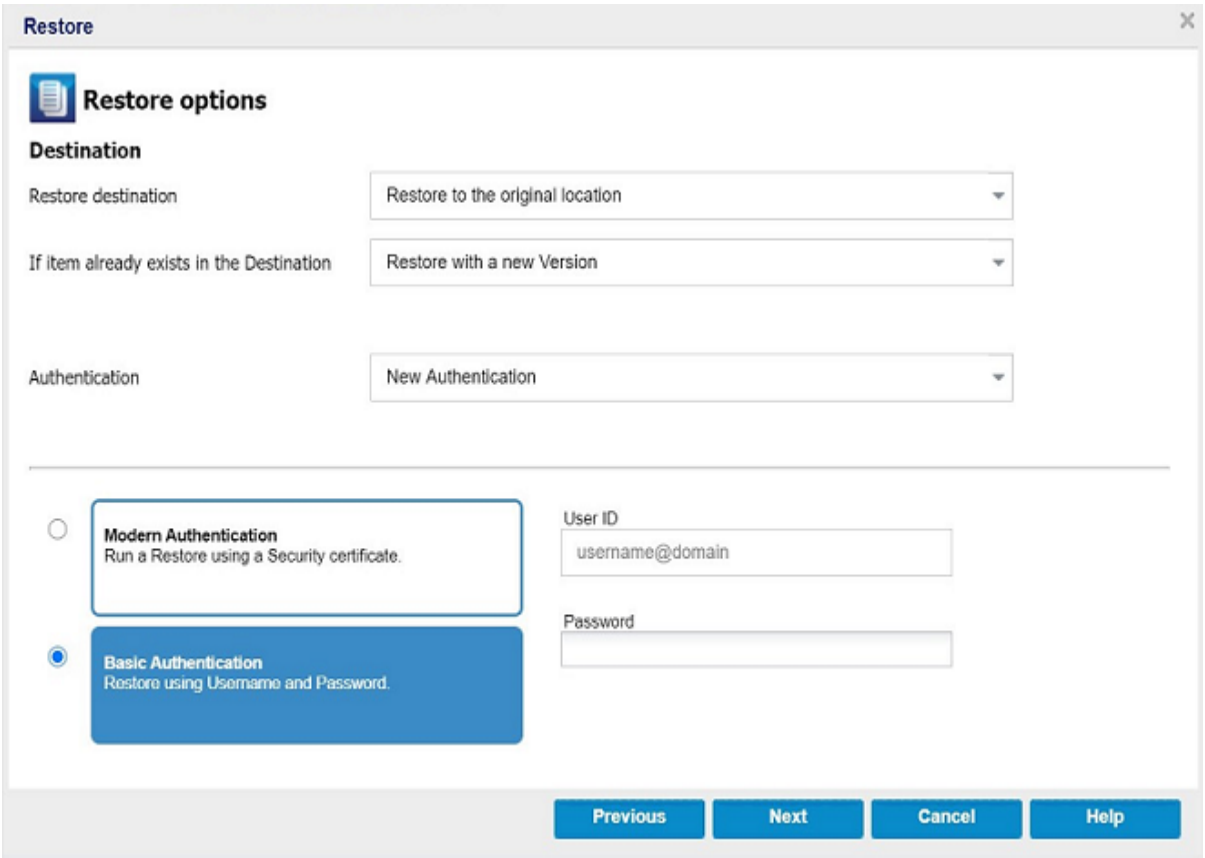
a. Para autenticar usando o certificado autoassinado, consulte Fazendo download do certificado do UDP e carregando-o no Azure.

b. Digite a ID do aplicativo e o nome do usuário.

c. Para aplicar as funções e permissões necessárias, marque a caixa de seleção **Permitir que o Arcserve UDP defina as funções e permissões necessárias do Azure para este aplicativo** e clique em **Avançar**.

Autenticação básica

Na autenticação básica, para continuar com a restauração, digite a ID do usuário e a senha.



4. Clique em **Avançar**.

   A caixa de diálogo **Resumo da restauração** é exibida.

5. Na caixa de diálogo Resumo da restauração, verifique as configurações e clique em **Concluir**.

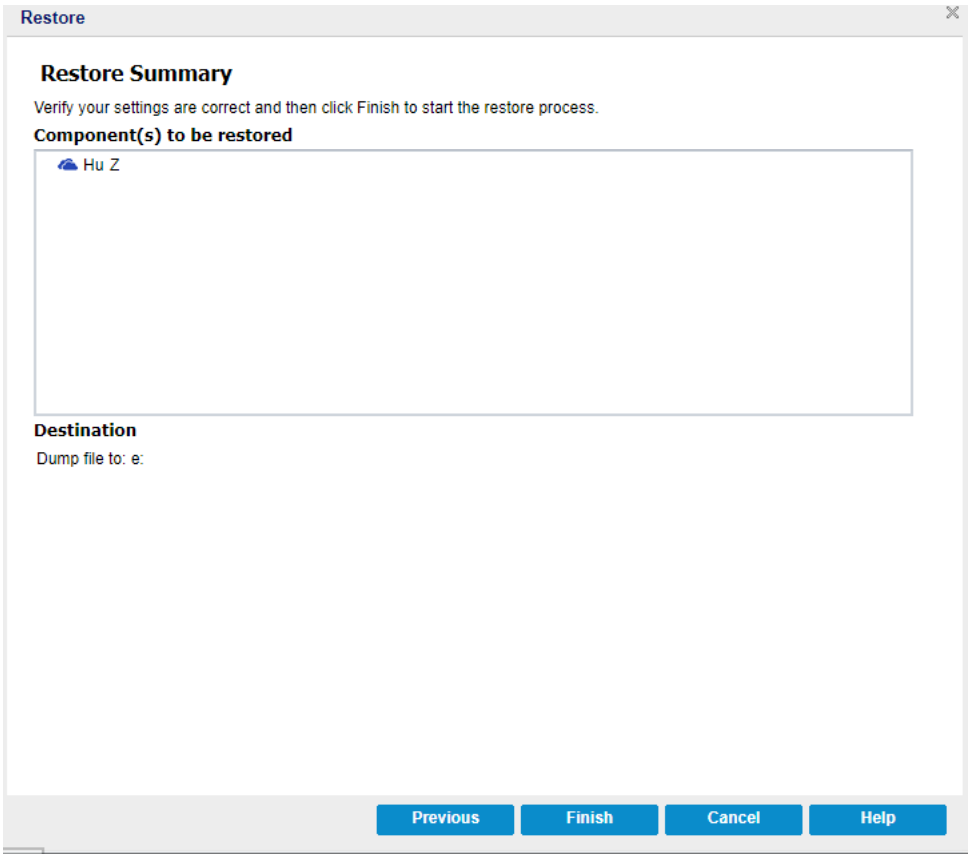
As opções de restauração são definidas para restaurar as informações do OneDrive. Agora, é possível exibir o resumo da restauração.

Exibir o resumo da restauração

Após definir as opções de restauração, verifique se suas configurações estão corretas e confirme o processo de restauração. **Resumo da restauração** ajuda a revisar todas as a opções de restauração e o caminho de destino definidos por você. Se for necessário fazer modificações, clique em **Voltar**.

Siga estas etapas:

1. Na caixa de diálogo **Resumo da restauração**, examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.



   - Se as informações do resumo não estiverem corretas, clique em **Voltar** e retorne à caixa de diálogo aplicável para alterar as configurações.
   - Se as informações de resumo estiverem corretas, clique em **Concluir** para iniciar a tarefa de restauração.

O ponto de recuperação do conteúdo é restaurado.

Restaurar dados do OneDrive usando a opção de montagem de volume

A proteção do OneDrive usa o formato de sessão de backup universal. É possível montar a sessão de backup como uma letra de unidade e, em seguida, copiar o arquivo/a pasta do volume montado.

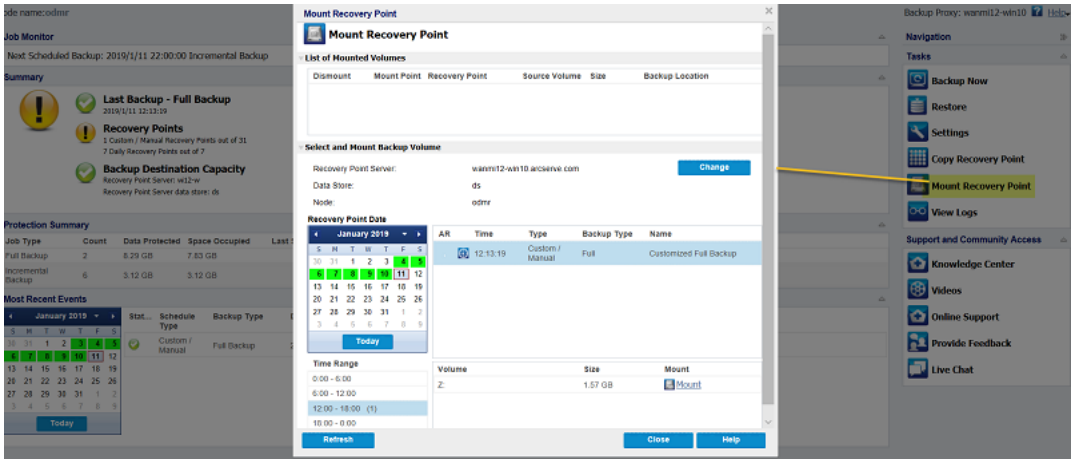
Siga estas etapas:

1. Efetue logon no Arcserve UDP.
2. Clique na guia **Recursos**.
3. Selecione **Todos os nós** no painel esquerdo.

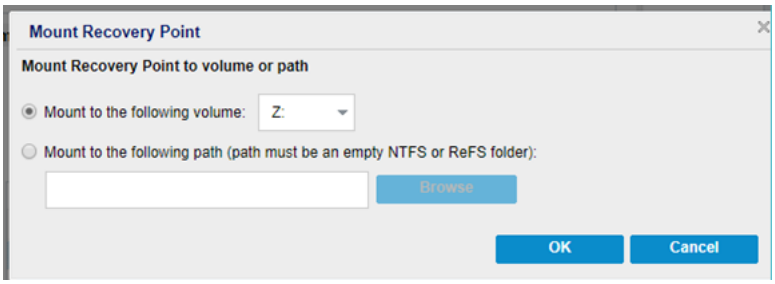
   Todos os nós do adicionados são exibidos no painel central.
4. No painel central, selecione o nó do OneDrive e clique em **Ações**.
5. Clique em **Efetuar logon no agente** no menu suspenso **Ações**.

   Observação: será efetuado logon automaticamente no nó do agente. Você pode exibir detalhes completos sobre o nó e, também, exibir a lista de tarefas que podem ser executadas no painel direito.
6. No painel à direita, sob **Tarefas**, clique em **Montar ponto de recuperação**.

   A caixa de diálogo **Montar ponto de recuperação** é exibida. É possível selecionar a sessão de backup nessa caixa de diálogo.



7. Selecione o destino e monte a sessão como uma letra de unidade ou monte-a em uma pasta NTFS vazia.



É possível navegar pelo volume. Em Volume, o Arcserve UDP salvou todos os metadados do OneDrive. Cada conta terá uma pasta relacionada no volume raiz. A pasta é nomeada de acordo com o nome da conta.

É possível abrir a pasta criada por esse nome de conta e verificar se foi feito backup dos dados do OneDrive.

Procurar ponto de recuperação de cópia em fita para restauração

Esta seção fornece informações sobre como selecionar um ponto de recuperação de backups de cópia em fita.

Siga estas etapas:

1. Faça download dos pontos de recuperação usando o Gerenciador do Arcserve Backup e copie-os em um disco local.
2. Na caixa de diálogo Restaurar, clique no botão **Alterar**.
3. Selecione a opção **Selecionar disco local ou pasta compartilhada**.
4. Clique em **Procurar** para navegar até o local da pasta onde os pontos de recuperação foram copiados na etapa 1.
5. Na lista de pontos de recuperação, selecione um ponto de recuperação e clique em **OK**.

   O ponto de recuperação selecionado é exibido na caixa de diálogo Restaurar.

Como executar uma restauração pontual

A restauração pontual oferece suporte à restauração do banco de dados SQL em qualquer período de tempo específico entre os pontos de recuperação N e N+1. A Restauração pontual ajuda os administradores a restaurar as transações ocorridas no banco de dados SQL entre dois pontos de recuperação. Por exemplo, considere que você tenha um ponto de recuperação em 03/16/2019 12:14:04:177 e o ponto de recuperação subsequente em 03/29/2019 22:03:14:177. Com a Restauração pontual, é possível restaurar as transações ocorridas entre os dois pontos de

recuperação. Isso ajuda os administradores a restaurar apenas as transações necessárias a partir de uma grande quantidade de dados de backup.

O que fazer a seguir?

1. Verificar pré-requisitos
2. Analisar as considerações
3. Executar uma restauração pontual

Pré-requisitos

Verifique os seguintes pré-requisitos antes de executar a Restauração pontual:

- O servidor do banco de dados MS SQL deve estar instalado no computador do agente do Windows.
- É necessário ter, pelo menos, dois pontos de recuperação para executar a Restauração pontual.
- Você deve ativar manualmente a Restauração pontual sempre que executar a restauração.

Considerações

Revise as seguintes considerações antes de executar a Restauração pontual:

- É possível executar a Restauração pontual apenas por meio do utilitário de linha de comando PIT.EXE.
- É necessário ter dois pontos de recuperação trabalhando em conjunto para executar a Restauração pontual.
- A Restauração pontual oferece suporte apenas a backups com base em agente. Os backups com base em host não têm suporte.
- A Restauração pontual oferece suporte apenas à restauração no local original. Não há suporte para a restauração em local alternativo e o despejo em disco.
- O backup do log de transações do banco de dados SQL é salvo no mesmo diretório do arquivo de log do SQL antes de gerar o instantâneo.
- O primeiro ponto de recuperação fornece a restauração em nível de banco de dados SQL. Após a Restauração pontual, o banco de dados SQL é definido como em estado de recuperação. É possível fazer backup do ponto de recuperação no modo desativado da Restauração pontual.

- Para executar a Restauração pontual, você deve selecionar o ponto no tempo entre os pontos de recuperação N e N+1. Qualquer ponto no tempo anterior ao ponto de recuperação N e posterior a N+1 não será permitido. Se você definir um ponto no tempo que não esteja entre os pontos de recuperação N e N+1, a tarefa de restauração falhará e causará a corrupção do banco de dados.
- A opção Truncar log é desativada por padrão nos planos de backup e restauração pontuais. Se estiver ativada, depois do backup, os logs da transação são truncados e o próximo backup pontual perde algumas transações.

Executar uma restauração pontual

1. Execute o arquivo **PIT.EXE**.

   O utilitário de linha de comando Point-In-Time é aberto e exibe o prompt de comando PIT$.

   Para obter mais informações, consulte Entendendo o utilitário de linha de comando Point-In-Time.

2. No prompt de comando, execute **set pitbackup=1**.

   O backup pontual é ativado.

3. No **console** do **Arcserve UDP**, execute um backup do banco de dados SQL.

   O ponto de recuperação N é criado.

4. Verifique se os arquivos a seguir são gerados na pasta **Catálogo**:

   - Se o nome da instância do SQL Server for MSSQLSERVER (nome de instância padrão):
     - ***_<DatabaseName>.idx.pit***

       Contém o tamanho fixo do resumo do ponto no tempo.

     - ***_<DatabaseName>.cat.pit***

       Contém o tamanho variável dos detalhes do ponto no tempo.

     - ***_<DatabaseName>.map.pit***

       Contém o mapeamento entre a sequência de caracteres interna e a identidade da sequência de caracteres interna.

   - Se o nome da instância do SQL Server for diferente de MSSQLSERVER (nome de instância diferente do padrão):
     - ***<SQLInstanceName>_<DatabaseName>.idx.pit***

       Contém o tamanho fixo do resumo do ponto no tempo.

- ***<SQLInstanceName>_<DatabaseName>.cat.pit***

  Contém o tamanho variável dos detalhes do ponto no tempo.

- ***<SQLInstanceName>_<DatabaseName>.map.pit***

  Contém o mapeamento entre a sequência de caracteres interna e a identidade da sequência de caracteres interna.

5. No **console do Arcserve UDP**, execute outro backup do banco de dados SQL.

   O ponto de recuperação N+1 é criado.

6. No prompt de comando, execute ***set pitrestore=1***.

   A Restauração pontual é ativada.

7. No prompt de comando, execute as consultas SQL para exibir as informações do ponto no tempo da sessão de backup de N+1:

   - *Query <SQLInstanceName>\<DatabaseName> <BackupDestination>\Catalog\<nome da pasta da sessão de backup de N+1>*

     Exibe o resumo de todos os pontos no tempo no backup

8. No prompt de comando, execute ***set pittime="<MM/DD/AAAA HH:MM:SS:ss>"***

9. No **console** do **Arcserve UDP**, execute a restauração em nível de banco de dados para o local original usando o ponto de recuperação N.

   A Restauração pontual é concluída com êxito. Verifique se os dados esperados foram restaurados no banco de dados.

Entendendo o utilitário de linha de comando Point-In-Time

O utilitário de linha de comando Point-In-Time está disponível no caminho *<Caminho de instalação do Arcserve UDP>\BIN* com o nome de arquivo *PIT.exe*.

O prompt de comando do utilitário de linha de comando é exibido como **PIT$**.

A seguir estão as opções disponíveis que podem ser executadas no utilitário de linha de comando:

Ajuda

Exibe todas as opções disponíveis no PIT.exe.

COMMAND /?

Exibe o uso do comando.

CONFIG

Usa a configuração no Registro.

OPTION

Especifica a opção global. VALUE é sempre um número hexadecimal.

SEQ

Especifica o número de sequência no backup de DB/TLog.

TIMEOUT

Especifica o tempo limite da conexão, em segundos.

DEVICE

Especifica que o tipo de dispositivo de backup será sempre um disco.

DATABASE

Especifica o nome do banco de dados. Digite o valor no formato *[server]\[instance]\<banco de dados>*.

LOGBACKUP

Especifica o caminho do backup de TLog.

LOGRESTORE

Especifica o caminho da restauração de TLog.

DBBACKUP

Especifica o caminho do backup de TLog.

DBRESTORE

Especifica o caminho da restauração de TLog.

CATALOG

Especifica o caminho do catálogo.

STOPAT

Especifica o ponto no tempo a ser restaurado.

NORECOVERY

Especifica a desativação (1) ou a ativação (0) da recuperação automática após a restauração do banco de dados do UDP.

PITBACKUP

Especifica a ativação (1) ou a desativação (0) do backup pontual para o UDP.

Exemplo: set pitbackup=1

PITRESTORE

Especifica a ativação (1) ou a desativação (0) da restauração pontual para o UDP.

Exemplo: *set pitrestore=1*

PITTEMP

Pasta temporária para a restauração pontual

PITTIME

Especifica um ponto no tempo para restauração pontual.

Exemplo: set pittime="<MM/DD/AAAA HH:MM:SS:ss>

PITNOSTAGE

Especifica o uso de logs no volume montado, em vez de restauração na pasta temporária.

BACKUPOPT

Especifica a opção de backup para controlar o VSS.

RESTOREOPT

Especifica a opção de restauração para controlar o VSS.

A seguir estão as consultas SQL que podem ser executadas no utilitário de linha de comando:

- *Query <SQLInstanceName>\<DatabaseName> <BackupDestination>\Catalog\<nome da pasta da sessão de backup de N+1>*

  Exibe o resumo de todos os pontos no tempo no backup.

- *Query /d <SQLInstanceName>\<DatabaseName> <BackupDestination>\Catalog\<nome da pasta da sessão de backup de N+1>*

  Exibe todos os detalhes do ponto no tempo no backup.

- *Query /i N <SQLInstanceName>\<DatabaseName> <BackupDestination>\Catalog\<nome da pasta da sessão de backup de N+1>*

  Exibe o resumo do ponto no tempo de N no backup.

- *Query /d /i N <SQLInstanceName>\<DatabaseName> <BackupDestination>\Catalog\<nome da pasta da sessão de backup de N+1>*

  Exibe os detalhes do ponto no tempo de N no backup.

Como restaurar volumes compartilhados do agrupamento

Cada vez que o Arcserve UDP executa um backup com êxito, também é criada uma imagem de instantâneo pontual de seu backup (ponto de recuperação). Essa coleta de pontos de recuperação permite localizar e especificar exatamente qual imagem

de backup deve ser restaurada. Posteriormente, se você suspeitar que as informações de backup estão ausentes, corrompidas ou não são confiáveis, é possível localizar e restaurar a partir de uma versão anterior válida.

O que fazer a seguir?

1. Verificar os pré-requisitos e as considerações
2. Especificar as informações do CSV a serem restauradas
   a. Especificar o CSV e o conteúdo a serem restaurados
   b. Definir as opções de restauração
3. Restaurar o conteúdo do CSV

Verificar os pré-requisitos e as considerações

Verifique se os pré-requisitos a seguir existem antes de executar uma restauração:

- Você tem pelo menos um ponto de recuperação para restauração.
- Você tem um destino válido e acessível de ponto de recuperação para do qual restaurar o ponto de recuperação de conteúdo.
- Você tem um local de destino válido e acessível para o qual restaurar o ponto de recuperação de conteúdo.
- Consulte a Matriz de compatibilidade, que fornece os navegadores, bancos de dados e sistemas operacionais com suporte.

Revise as seguintes considerações de restauração:

- Se a restauração para um destino remoto e se todas as letras de unidade (A - Z) estiverem ocupadas, a restauração de dados para um caminho remoto não serão bem-sucedidas. O agente do Arcserve UDP (Windows) precisa usar uma letra de unidade para montar o caminho do destino remoto.
- (Opcional) Compreenda como funciona o processo de restauração. Para obter mais informações, consulte Como a restauração em nível de arquivo funciona.
- (Opcional) Examine os arquivos ignorados durante a restauração. Para obter mais informações, consulte o tópico Arquivos ignorados durante a restauração.
- Ao tentar restaurar uma sessão de backup otimizada em um volume que não esteja vazio (restauração não otimizada), a tarefa de restauração pode levar mais tempo do que o exibido no tempo estimado do monitor de tarefas. A quantidade de dados que é processada e o tempo decorrido pode aumentar com base nos dados que são otimizados no volume.

Exemplo:

O tamanho do volume de backup é de 100 GB e, após a otimização, o tamanho do volume é reduzido para 50 GB.

Ao executar uma restauração não otimizada desse volume, o monitor de tarefas de restauração exibe 100% após restaurar 50 GB, mas levará mais tempo para restaurar todos os 100 GB.

- A mensagem do log de atividades a seguir será exibida durante a restauração de arquivos do sistema:

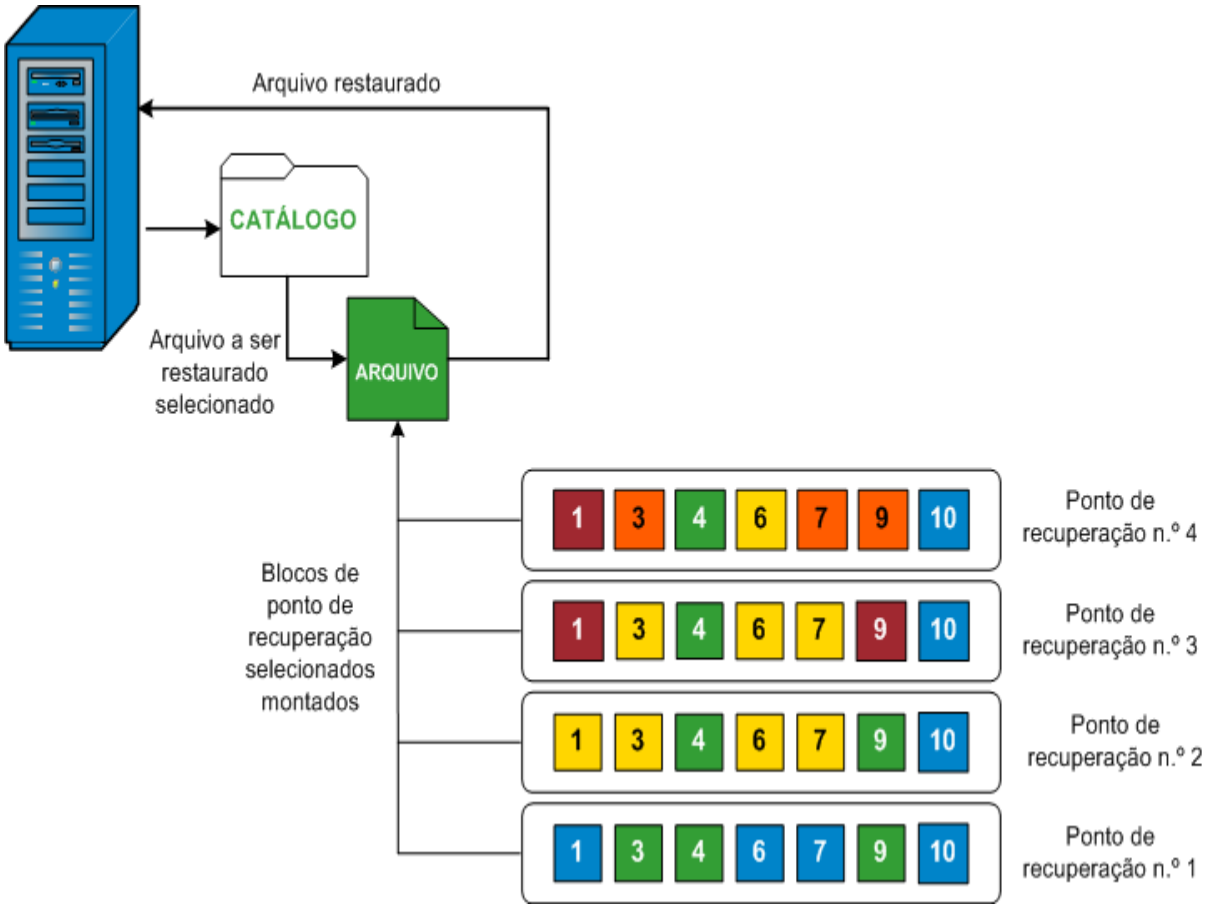
  "Os arquivos do sistema foram ignorados. Se necessário, é possível usar a opção Recuperação bare metal (BMR) para restaurá-los."

Como a restauração em nível de arquivo funciona

Durante um backup em nível de bloco, cada arquivo de backup é composto de um conjunto de blocos que definem aquele arquivo específico. Um arquivo de catálogo é criado contendo uma lista dos arquivos de backup, juntamente com os blocos individuais que foram usados para cada arquivo e os pontos de recuperação disponíveis para esses arquivos. Se precisar restaurar um arquivo específico, é possível pesquisar o backup e selecionar o arquivo que deseja restaurar e o ponto de recuperação de onde deseja restaurar. Em seguida, o Arcserve UDP coleta a versão dos blocos que foram usados para o ponto de recuperação do arquivo especificado, monta novamente o arquivo e o restaura.

Observação: também é possível executar uma restauração sem um arquivo de catálogo de um ponto de recuperação do backup sem catálogo.

O diagrama de fluxo a seguir mostra o processo de como o Arcserve UDP restaura um arquivo específico:



Arquivos ignorados durante a restauração

Durante a execução de uma restauração pelo agente do Arcserve UDP (Windows), alguns arquivos podem ser ignorados propositalmente.

Os arquivos e as pastas na tabela a seguir são ignorados durante uma restauração se as duas condições a seguir existirem:

- Os arquivos são ignorados quando tais arquivos existirem antes da restauração e a opção de conflito for "Ignorar arquivos existentes".
- As pastas e os arquivos listados na tabela a seguir são ignorados porque são um componente importante para o Windows ou o agente do Arcserve UDP (Windows).

Sistema operacional	Pasta ou local	Nome do arquivo ou pasta	Observações

Todos	Pasta raiz de cada volume	CAVolTrc.dat	Usado pelo driver de rastreamento do Arcserve UDP.
		cavoltrcsnapshot.dat	
		Informações de volume do sistema*	Usado para salvar arquivos/pastas por um sistema Windows, por exemplo, arquivos de cópia de sombra de volume.
		RECYCLER*	Usado apenas em partições NTFS. Contém uma lixeira para cada usuário que efetua logon no computador, classificadas por seu SID (Security Identifier – Identificador de Segurança).
		$Recycle.Bin*	Ao excluir um arquivo no Windows NT Explorer ou Meu computador, o arquivo é armazenado na Lixeira até que você a esvazie ou restaure o arquivo.
	Qualquer pasta contém arquivos de imagem	Thumbs.db	Armazena imagens em miniatura para o modo de exibição de miniatura do Windows Explorer.
	Pasta raiz do volume	PageFile.Sys	Arquivo de troca de memória virtual do Windows.
		Hiberfil.sys	Arquivo Hibernate usado para salvar os dados do sistema quando o computador entra no modo de hibernação.

As pastas e os arquivos a seguir são ignorados apenas quando você restaura no local original ou alternativo:

Sistema operacional	Pasta ou local	Nome do arquivo ou pasta	Observação
Todos	Pasta especificada no registro de valor em: HKLM\Software\Microsoft\Windows NT\CurrentVersion\WinLogon\SfcDllCache	Todos os arquivos/pastas (de maneira recursiva)	A pasta contém um arquivo DLL em cache que é usado para o SFC (System File Checker – Verificador de Arquivos do Sistema) e o con-

			teúdo do diretório de cache da DLL do sistema é recriado usando SFC.
	%SystemRoot%\SYSTEM32\dllCache		
	Pasta raiz do quorum_device	MSCS*	Usado para o Microsoft Cluster Server.
	%SystemRoot%\SYSTEM32\	perf?00?.dat	Dados de desempenho usados pelo contador de desempenho do Windows.
		perf?00?.bak	Usado para Proteção de arquivos do Windows (WFP) registra as assinaturas digitais das instalações do sistema operacional (como EXE, DLL, SYS, OCX e assim por diante) para protegê-las contra exclusão ou de substituição por versões mais antigas.
		CATROOT*	
	%SystemRoot%\inetsrv\	metabase.bin	O arquivo binário de metabase de versões do IIS anteriores ao 6.0.

	Arquivo ou pasta especificada no valor diferente de "Armazenamento comum do SIS" em HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup	Todos os arquivos/pastas (de maneira recursiva)	Arquivos e pastas não devem ser copiados para backup e restaurados. Para obter mais informações, consulte o link.
XP W2003	Volume do sistema	NTLDR	O principal carregador de inicialização.
		BOOT.INI	Contém a configuração de inicialização (se a configuração estiver ausente, como padrão, o NTLDR usará \Windows na primeira partição do primeiro disco rígido).
		NTDETECT.COM	Obrigatório para inicializar um sistema operacional com base em NT. Detecta informações de hardware básicas

			necessárias para uma inicialização bem-sucedida.
Vista e posterior	Pasta raiz do volume do sistema	boot*	Pasta de inicialização para Windows.
		bootmgr	Arquivo do gerenciador de inicialização do Windows.
		EFI\Microsoft\Boot*	Usado para inicialização de EFI.
	%SystemRoot%\SYSTEM32\	LogFiles\WMI\RTBackup*	Armazena os arquivos de rastreamento de ETW (extension .etl) para as sessões de rastreamento de eventos em tempo real.
		config\RegBack*	Backup da tabela do registro atual.
Win8 e posterior	Volume do sistema	swapfile.sys	Arquivo do controlador de sistema, normalmente cerca de 256 MB. Ele é usado pelos apli-

			cativos do Metro style que não podem se encaixar nas carac-terísticas de paginação tradicional (como padrões de uso, cres-cimento, reserva de espaço) do pagefile.sys.
		BOOTNXT	Usado para inicializar a partir do sis-tema ope-racional, que não seja o Windows 8. Criado ao ativar as opções de inicialização e atualizado pelo Win-dows.

O Log de atividades fornece as seguintes informações:

- Informações de data e hora: arquivos de sistema jobxxxx ignorados. Você pode usar a BMR (Recuperação Bare Metal) para restaurá-los.
- Informações de data e hora: arquivos ou diretórios de sistema jobxxxx igno-rados. Arquivos ou diretórios ignorados estão disponíveis em: C:\Arquivos de programas\Arcserve\Unified Data Protection\Engine\Logs\Restore-<YYYYMMDD>-<hhmmss>-<Process ID>-<Job ID>.log.

Especificar as informações do CSV a serem restauradas

O Arcserve UDP fornece uma opção para restaurar os dados a partir de um ponto de recuperação. O objetivo de executar uma tarefa de restauração com êxito é identificar rapidamente os dados necessários e recuperá-los do local de backup adequado. Cada tarefa de restauração requer uma origem e um destino.

O que fazer a seguir?

1. Especificar o CSV e o conteúdo a serem restaurados
2. Definir as opções de restauração

Especificar o CSV e o conteúdo a serem restaurados

Use a opção **Procurar pontos de recuperação** para restaurar a partir de um ponto de recuperação. Ao selecionar uma data de recuperação e, em seguida, especificar a hora, todos os pontos de recuperação associados a esse período são exibidos. Você pode procurar e selecionar o conteúdo do backup (incluindo aplicativos) a ser restaurado.

Siga estas etapas:

1. Acesse a caixa de diálogo de seleção de método de restauração de uma das seguintes maneiras:

   A partir do console do Arcserve UDP:

   a. Efetue logon no **Arcserve UDP**.

   b. Clique na guia **Recursos**.

   c. Selecione **Todos os nós** no painel esquerdo.

      Todos os nós do adicionados são exibidos no painel central.

   d. No painel central, selecione o nó do e clique em **Ações**.

   e. Clique em **Restaurar** no menu suspenso **Ações**.

      A caixa de diálogo de seleção do método de restauração é exibida.

      Observação: você é automaticamente conectado ao nó do agente e a caixa de diálogo de seleção do método de restauração é exibida no nó do agente.

   No agente do Arcserve UDP (Windows):

   a. Efetue logon no agente do Arcserve UDP (Windows).

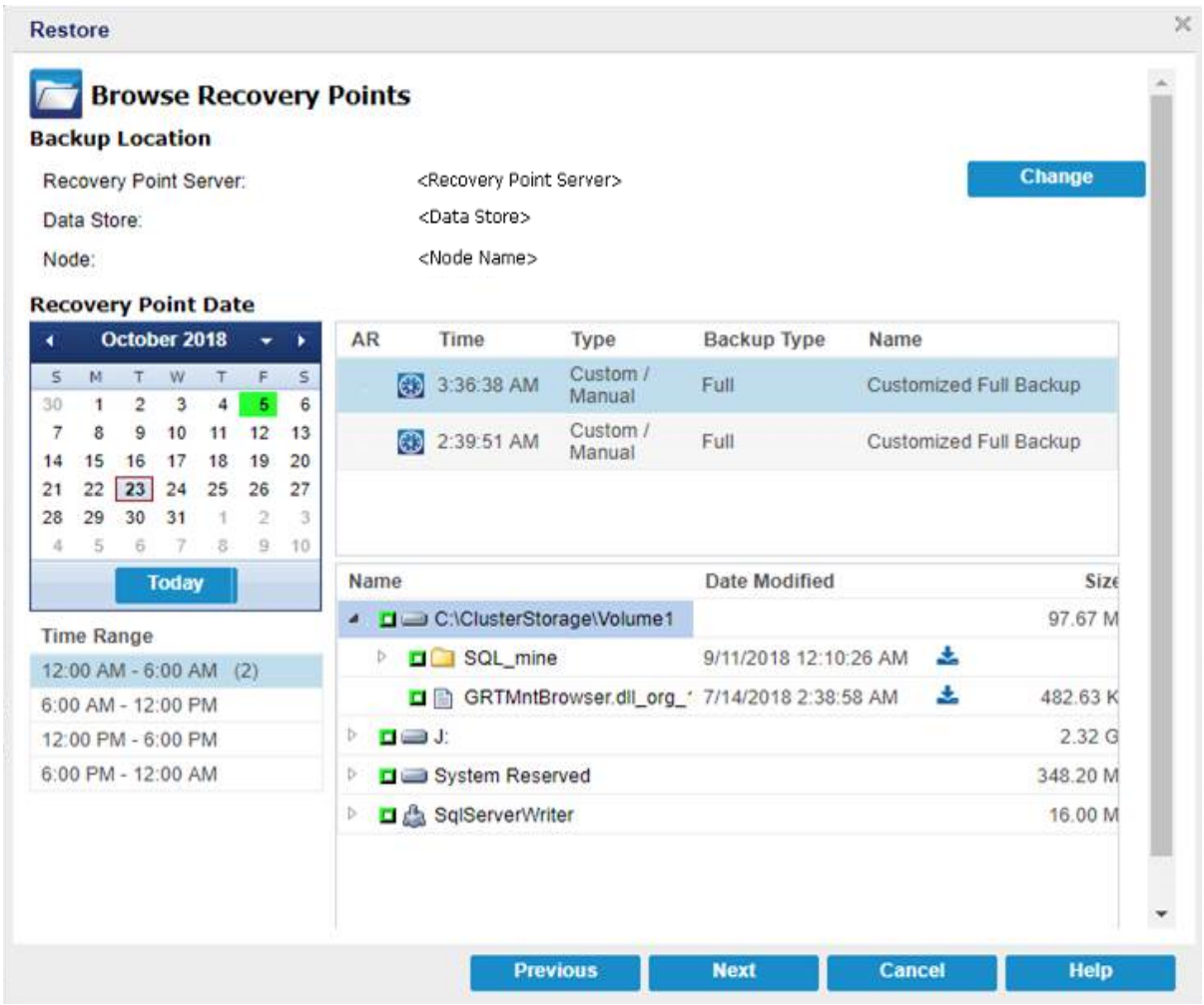
   b. Na página inicial, selecione **Restaurar**.

   A caixa de diálogo de seleção do método de restauração é exibida.

2. Clique na opção **Procurar pontos de recuperação**.

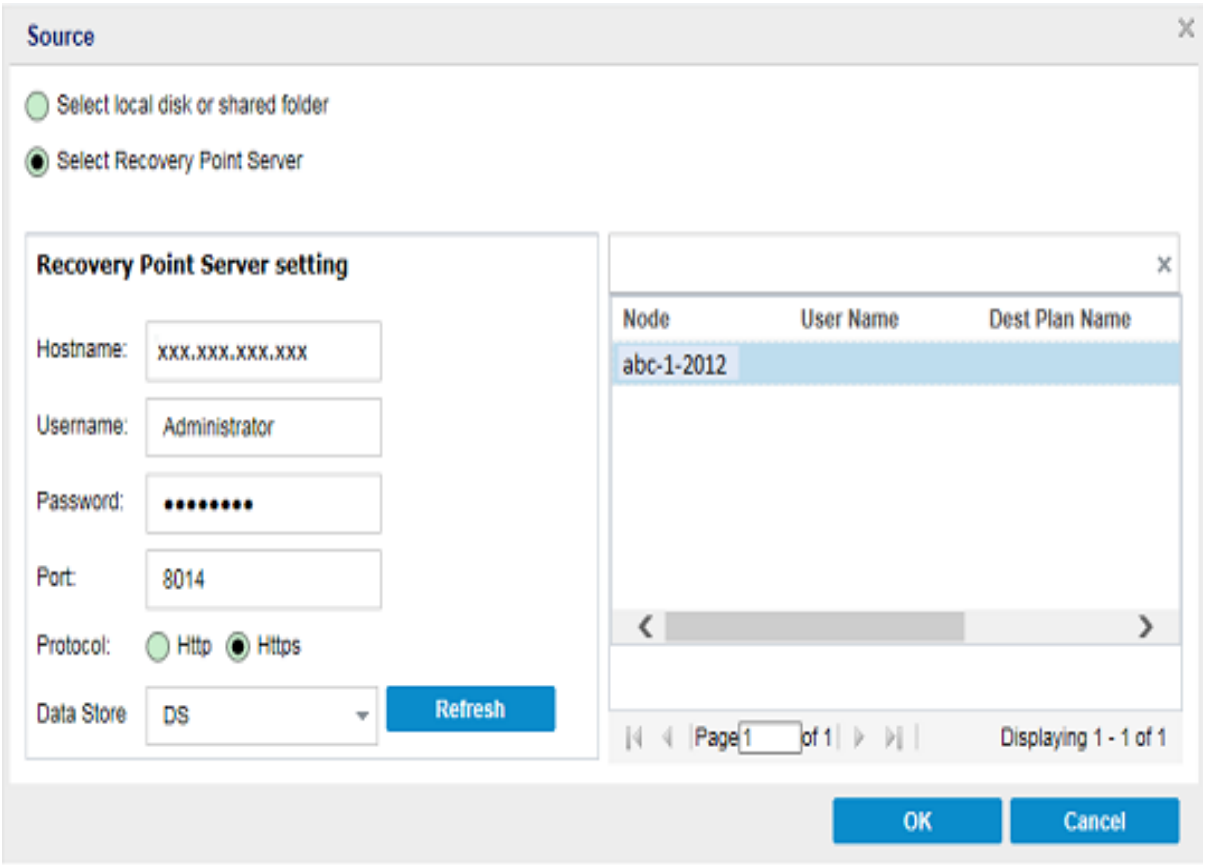
   A caixa de diálogo **Procurar pontos de recuperação** é exibida. É possível ver os detalhes do **Servidor de ponto de recuperação** no **Local do backup**.

   AR indica o resultado da execução, se a Recuperação garantida tiver sido executada para a sessão.



3. Clique em **Alterar** para atualizar o local do backup.

   A caixa de diálogo **Origem** é exibida e será possível selecionar o local do backup.



4. Selecione uma das seguintes origens:

   Selecionar o disco local ou uma pasta compartilhada

   a. Especifique ou procure o local onde as suas imagens de backup estão armazenadas e selecione o backup de origem adequado.

      É possível clicar no botão com a seta verde para verificar a conexão com o local especificado. Se necessário, forneça as credenciais de **Nome de usuário** e **Senha** para acessar esse local de origem.

      A caixa de diálogo **Selecionar o local do backup** é exibida.

   b. Selecione a pasta onde estão armazenados os pontos de recuperação e clique em **OK**.

      A caixa de diálogo **Selecione o local do backup** será fechada, e você poderá ver o local do backup na caixa de diálogo **Origem**.

   c. Clique em **OK**.

      Os pontos de recuperação são listados na caixa de diálogo **Procurar pontos de recuperação**.

      Selecionar servidor de ponto de recuperação

d. Especifique os detalhes da configuração do servidor de ponto de recuperação e clique em **Atualizar**.

   Todos os agentes estão listados na coluna Agente de proteção de dados na caixa de diálogo Origem.

e. Selecione o agente na lista exibida e clique em **OK**.

   Os pontos de recuperação são listados na caixa de diálogo **Procurar pontos de recuperação**.

5. Selecione a data no calendário para a imagem de backup para restaurar.

   Todas as datas que contém pontos de recuperação para a origem do backup especificado são realçadas em verde.

   Os pontos de recuperação correspondentes a essa data são exibidos, juntamente com a hora do backup, o tipo de backup que foi executado (completo, incremental ou de verificação) e o nome do backup.

6. Selecione um ponto de recuperação para restaurar.

   O conteúdo do backup (incluindo aplicativos) para o ponto de recuperação selecionado é exibida.

   Observação: um ícone de relógio com um símbolo de cadeado indica que o ponto de recuperação contém informações criptografadas e que pode ser necessária uma senha para restaurar.

7. Selecione o volume CSV a ser restaurado.

   - Para uma restauração de nível do volume, pode-se especificar a restauração do volume inteiro ou de arquivos/pastas selecionados no volume.
   - Para uma restauração de nível do aplicativo, pode-se especificar a restauração do aplicativo inteiro ou de itens selecionados no aplicativo, como componentes, bancos de dados, instâncias e assim por diante.

8. Clique em **Avançar**.

   A caixa de diálogo **Opções de restauração** é exibida.

   O ponto de recuperação e o conteúdo para restauração é especificado.

Definir as opções de restauração

Depois de especificar um ponto de recuperação e conteúdo para restauração, defina as opções de cópia do ponto de recuperação selecionado.

Siga estas etapas:

1. Na caixa de diálogo **Opções de restauração**, selecione o destino da restauração.

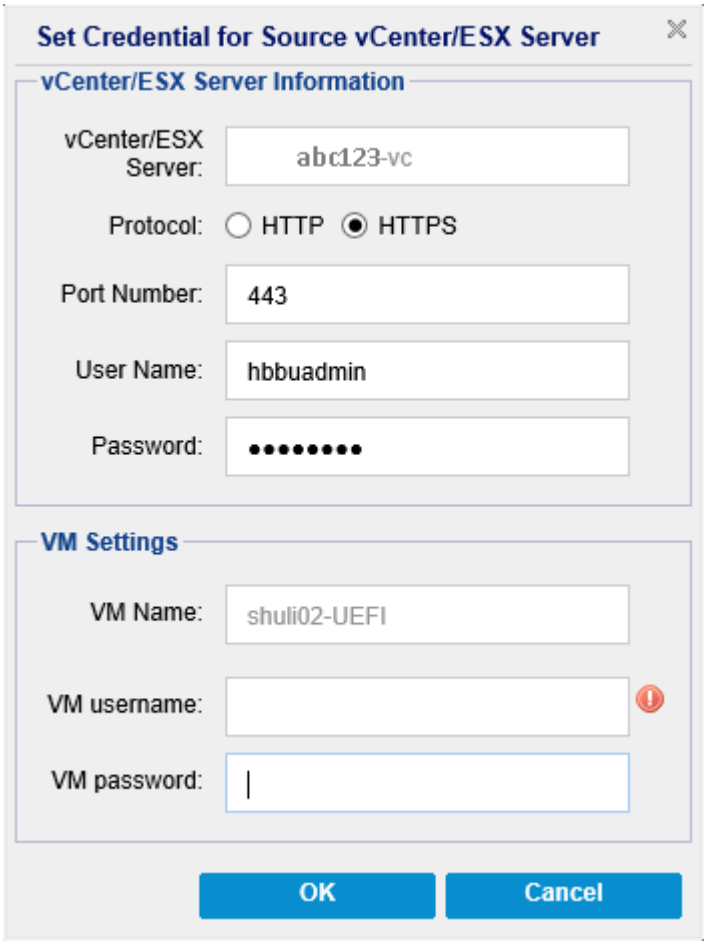
As opções de destino disponíveis são:

Restaurar no local original

Restaura no local original a partir do qual a imagem de backup foi capturada.

Observação: se você tiver feito backup do ponto de recuperação usando o backup sem agente com base em host, a opção Restaurar no local original restaurará o arquivo na máquina virtual. Nesse caso, uma caixa de diálogo abre. Você pode digitar as credenciais do hipervisor e do sistema operacional da máquina virtual.

Para a VM do VMware:



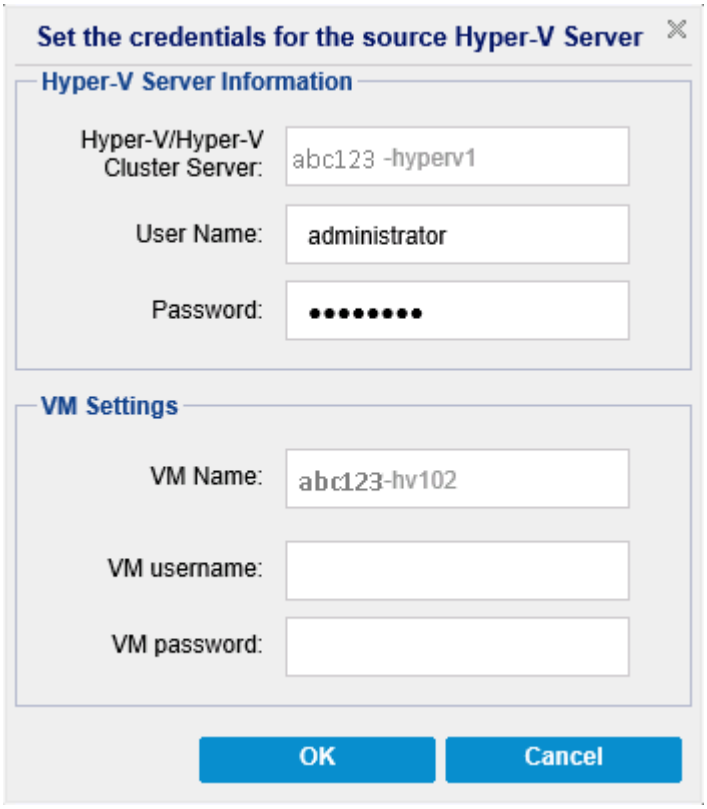
Observação: para criar ou gravar arquivos na VM, considere os seguintes requisitos de configuração e a permissão de conta da máquina virtual:

- o VMware Tools está instalado e em execução.
- o Firewall deve permitir que o compartilhamento de arquivo e de impressora.
- A conta é o administrador local internos, o administrador de domínio interno ou conta de domínio que é integrante do grupo de administradores locais. Se forem usadas outras contas:
  - Desative o acesso remoto ao UAC. Para desativar o acesso remoto de UAC, consulte Importar máquina virtual usando a conta administrativa adicional.
  - Desative o UAC na Diretiva de Segurança Local, desativando a configuração Executar todos os administradores no modo de aprovação de administrador em secpol.msc -> Diretivas

Locais -> Opções de Segurança. (Secpol.msc é editor da diretiva de segurança da Microsoft).

Importante: não tente desativar o UAC na caixa de diálogo Configurações de controle de conta do usuário, que é aberta no painel de controle.

Para a VM do Hyper-V:



Observação: para criar ou gravar arquivos na VM, considere os seguintes requisitos de configuração e a permissão de conta da máquina virtual:

- os serviços de integração do Hyper-V estão instalados e em execução.
- o Firewall deve permitir que o compartilhamento de arquivo e de impressora.
- A conta é o administrador local internos, o administrador de domínio interno ou conta de domínio que é integrante do grupo de administradores locais. Se forem usadas outras contas:

Desative o acesso remoto ao UAC. Para desativar o acesso remoto de UAC, consulte Importar máquina virtual usando a conta administrativa adicional.

- Se o sistema operacional convidado da máquina virtual for a versão de cliente do Windows (por exemplo, o Windows 10), será necessário configurar manualmente o firewall para permitir a WMI (Windows Management Instrumentation - Instrumentação de Gerenciamento do Windows).

Restaurar para

Restaura no local especificado. É possível clicar no botão com a seta verde para verificar a conexão com o local especificado. Se necessário, forneça as credenciais de nome de usuário e senha para acessar esse local.

2. Especifique a opção **Resolvendo conflitos** que o Arcserve UDP executará se forem encontrados conflitos durante o processo de restauração.

   As opções disponíveis são:

   Substituir arquivos existentes

   Sobrescreve (substitui) qualquer arquivo existente que está localizado no destino da restauração. Todos os objetos serão restaurados dos arquivos de backup, independentemente da presença atual deles no computador.

   Substituir os arquivos ativos

   Substitui todos os arquivos ativos ao reinicializar. Se, durante a tentativa de restauração, o agente do Arcserve UDP (Windows) detectar que o arquivo existente está em uso ou sendo acessado, para evitar erros, ele não substituirá o arquivo imediatamente, só depois que o computador for reinicializado. (A restauração ocorrerá imediatamente, mas a substituição de arquivos ativos é feita durante a próxima reinicialização).

   Essa opção só estará disponível se você selecionar a opção **Substituir os arquivos existentes**.

   Observação: se essa opção não estiver selecionada, qualquer arquivo ativo será ignorado na restauração.

   Renomear arquivos

   Cria um novo arquivo se o nome de arquivo já existir. A seleção desta opção copia o arquivo de origem no destino com o mesmo nome de arquivo, mas com uma extensão diferente. Os dados serão restaurados no novo arquivo.

   Ignorar arquivos existentes

Ignora e não substitui (sobrescreve) os arquivos localizados no destino da restauração. Apenas os objetos inexistentes em seu computador no momento serão restaurados dos arquivos de backup.

Padrão: Ignorar arquivos existentes.

3. Especifique a **Estrutura de diretórios** para criar um diretório raiz durante a restauração.

Criar diretório raiz

Especifica que, se uma estrutura de diretório raiz existir na imagem de backup capturada, o Arcserve UDP recriará a mesma estrutura no caminho de destino de restauração.

Se essa opção não for selecionada, o arquivo ou pasta será restaurado diretamente para a pasta de destino.

Por exemplo, se durante o backup você capturou os arquivos "C:\Pasta1\Subpasta2\A.txt" e "C:\Pasta1\Subpasta2\B.txt" e durante a restauração foi especificado como destino o local "D:\Restore".

- Se você optar por restaurar os arquivos "A.txt" e "B.txt" individualmente, o destino dos arquivos restaurados será "D:\Restore\A.txt" e "D:\Restore\B.txt" (o diretório raiz acima do nível de arquivo especificado não será recriado).
- Se você optar por restaurar a partir do nível da "Subpasta2", o destino dos arquivos restaurados será "D:\Restore\Subpasta2\A.txt" e "D:\Restore\Subpasta2\B.txt" (o diretório acima do nível de pasta especificado não será recriado).

Com esta opção selecionada, todo o caminho de diretório raiz para os arquivos / pastas (incluindo o nome de volume) é recriado até a pasta de destino. Se os arquivos/pastas a serem restaurados tiverem o mesmo nome de volume, o caminho do diretório raiz de destino não incluirá esse nome de volume. No entanto, se os arquivos/pastas a serem restaurados forem de nomes de volume diferentes, o caminho do diretório raiz do destino incluirá o nome do volume.

Por exemplo, se durante o backup você capturou os arquivos "C:\Pasta1\Subpasta2\A.txt", "C:\Pasta1\Subpasta2\B.txt" e também "E:\Pasta3\Subpasta4\C.txt" e durante a restauração foi especificado como destino de restauração o local "D:\Restore".

- Se você optar por restaurar apenas o arquivo "A.txt", o destino do arquivo restaurado será "D:\Restore\Pasta1\Subpasta2\A.txt" (o diretório raiz inteiro, sem o nome do volume, será recriado).

- Se você optar por restaurar tanto o arquivo "A.txt" como o "C.txt", o destino dos arquivos restaurados será "D:\Restore\C\Pasta1\Subpasta2\A.txt" e "D:\Restore\E\Pasta3\Subpasta4\C.txt" (o diretório raiz inteiro, com o nome do volume, será recriado).

4. Em **Recuperar ACL**, selecione a opção **Ignorar recuperar ACL de arquivos / pastas** para ignorar a permissão original para os arquivos/pastas restaurados. Selecionar a opção permite, em vez disso, herdar as permissões da pasta de destino. Se a opção não for selecionada, as permissões originais são mantidas.
5. Se necessário, digite a **Senha de criptografia de backup** se os dados que está tentando restaurar estiverem criptografados.

   A senha não será necessária se você estiver tentando fazer a restauração a partir do mesmo computador do agente do Arcserve UDP (Windows) em que o backup criptografado foi executado. No entanto, se você estiver tentando fazer a restauração a partir de um computador diferente do agente do Arcserve UDP (Windows), a senha será necessária.

   Observação: um ícone de relógio com um símbolo de cadeado indica que o ponto de recuperação contém informações criptografadas e que pode ser necessária uma senha para restaurar.
6. Clique em **Avançar**.

   A caixa de diálogo **Resumo da restauração** é exibida.

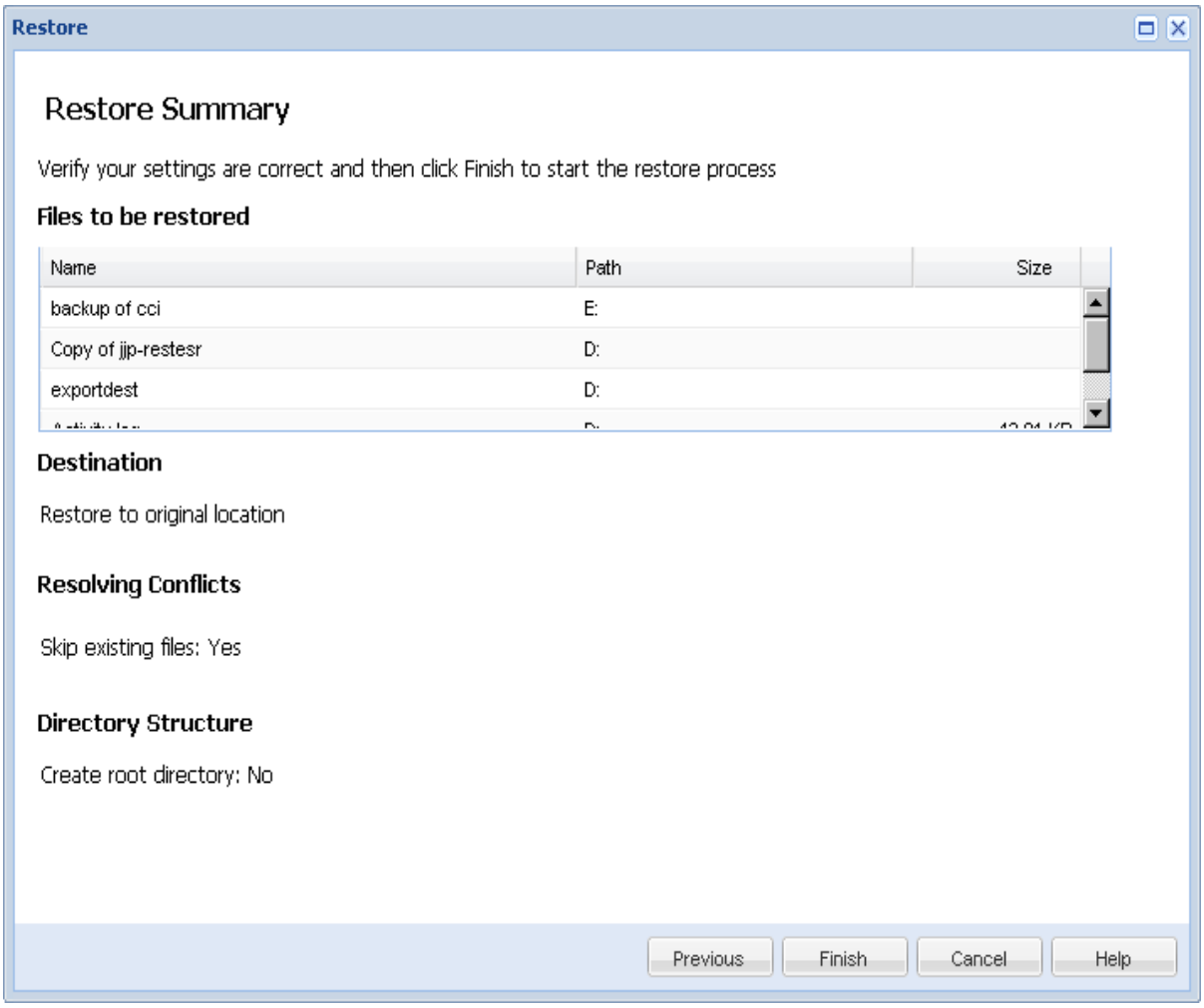
   As opções de restauração são definidas para restaurar a partir de um ponto de recuperação.

Restaurar o conteúdo do CSV

Após definir as opções de restauração, verifique se suas configurações estão corretas e confirme o processo de restauração. O **Resumo da restauração** o auxilia a revisar todas as opções de restauração definidas e modificá-las se necessário.

Siga estas etapas:

1. Na caixa de diálogo **Resumo da restauração**, examine as informações exibidas para verificar se todas as opções e configurações de restauração estão corretas.



- Se as informações do resumo não estiverem corretas, clique em **Anterior** e volte à caixa de diálogo em questão para alterar a configuração incorreta.
- Se as informações de resumo estiverem corretas, clique em **Concluir** para iniciar o processo de restauração.

O ponto de recuperação do conteúdo é restaurado.

Capítulo 2: Gerenciando o backup e a restauração em fita

O Arcserve UDP permite fazer backup de dados em uma fita e a restauração dos dados que foram obtidos em backup da fita para um nó.

Esta seção contém os seguintes tópicos:

Como fazer backup de um repositório de dados de redução de redundância em uma fita

Para fazer backup de um repositório de dados de redução de redundância em fita, use os seguintes métodos:

- Faça backup dos nós do UDP em fita. Para obter mais informações, consulte a seção Método 1: Fazer backup da sessão de backup do UDP mais recente em fita no Guia de Administração do Arcserve Backup.
- Faça backup dos dados do Arcserve UDP a partir de repositórios de dados. Para obter mais informações, consulte a seção Método 2: Fazer backup dos dados do Arcserve UDP a partir de repositórios de dados no Guia de Administração do Arcserve Backup.

Como restaurar um repositório de dados de redução de redundância de uma fita

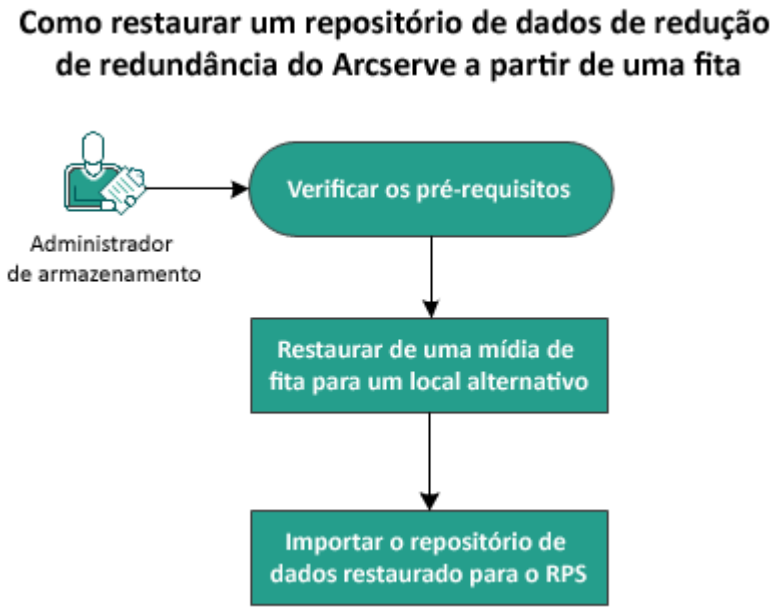
Se já tiver feito backup de um repositório de dados de redução de redundância de um RPS (Recovery Point Server - Servidor de Ponto de Recuperação) para um dispositivo de fita, você poderá restaurar o repositório de dados. Para este procedimento, o Arcserve Backup e o Arcserve UDP são usados em conjunto para restaurar um repositório de dados de redução de redundância de uma fita. O Arcserve Backup é usado para restaurá-lo da fita para um destino especificado, e o Arcserve UDP é usado para importá-lo para um RPS.

Os dois processos a seguir são envolvidos no procedimento de restauração:

1. O primeiro processo usa o Arcserve Backup para restaurar as sessões da mídia de fita para um volume. É recomendável restaurar os componentes em outro local.
2. O segundo processo usa o Arcserve UDP para importar o repositório de dados restaurado para o RPS.

Observação: será necessário fornecer o caminho da **pasta de destino do backup** do repositório de dados de redução de redundância ao procurar pelo local durante a importação.

O diagrama a seguir ilustra como restaurar um repositório de dados de redução de redundância do Arcserve de uma fita:



O que fazer a seguir?

1. Verificar os pré-requisitos
2. Restaurar de uma mídia de fita para um local alternativo
3. Importar o repositório de dados restaurado para o RPS

Verificar os pré-requisitos

Verifique os pré-requisitos a seguir antes de começar a restaurar:

- Você deve ter feito backup de um repositório de dados de RPS na fita.
- Você precisará digitar a senha da sessão, se necessário.
- Você precisará fornecer o nome do usuário e a senha para o destino da restauração.

Restaurar de uma mídia de fita para um local alternativo

Para restaurar a sessão da mídia de fita em outro local, você precisará usar o Gerenciador de Backup do Arcserve.

Depois de restaurar com êxito, é possível importar o repositório de dados restaurado no RPS usando o Arcserve UDP.

Siga estas etapas:

1. No Arcserve Backup, efetue logon no Gerenciador do Arcserve Backup.
2. No painel de navegação **Início rápido**, clique em **Restaurar** e, no painel central, selecione a guia **Origem**.
3. No menu suspenso, selecione **Restaurar por sessão** e selecione a sessão que deseja restaurar.
4. Clique na guia **Destino**.
5. Limpe (desmarque) a caixa de seleção **Restaurar arquivos em seus locais originais**.
6. Expanda **Sistemas Windows** e procure o local onde você deseja restaurar.
7. Clique na guia **Programação** e selecione **Uma vez** para a opção **Método de repetição**.
8. Clique em **Enviar**.

   A caixa de diálogo **Restaurar mídia** é aberta.
9. Selecione a mídia de restauração e clique em **OK**.

   A caixa de diálogo **Nome de usuário e senha da sessão** é aberta.
10. Forneça o nome de usuário e a senha para o local de restauração e a senha da sessão para os pontos de recuperação, se necessário.
11. Clique em **OK**.

    A caixa de diálogo **Enviar tarefa** é exibida.
12. Preencha as informações necessárias na caixa de diálogo **Enviar tarefa** e clique em **OK**.

    A tarefa de restauração será enviada.

    Depois que a tarefa de restauração for concluída, os arquivos do repositório de dados do Arcserve UDP serão exibidos no local especificado.

Importar o repositório de dados restaurado para o RPS

Para importar o repositório de dados restaurados para o RPS, será necessário usar o Console do Arcserve UDP. O recurso **Importar repositório de dados** permite adicionar um repositório de dados para o servidor de ponto de recuperação. É possível importar quaisquer repositórios de dados existentes para um servidor de ponto de recuperação.

Siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Destinos** e clique em **Servidores de ponto de recuperação**.

   A página **Destinos: servidores de ponto de recuperação** é exibida.
3. Execute uma das seguintes ações:
   - Clique em um servidor de ponto de recuperação.
   - Selecione o servidor de ponto de recuperação e, no menu central, clique no menu suspenso **Ações**.
4. Clique **Importar repositório de dados**.

   A página **Importar um repositório de dados** é exibida.
5. Selecione as opções a seguir e clique em **Avançar**:
   a. Clique em **Procurar** e selecione a **Pasta de destino do backup** da qual você deseja importar o repositório de dados.
   b. Se necessário, digite a **Senha de criptografia**.

      Observação: se o repositório de dados não estiver criptografado, você poderá deixar este campo vazio.

   Após a autenticação da **pasta de Destino do backup**, a página **Importar um repositório de dados** exibe os detalhes do repositório de dados.

   Observação: a importação do repositório de dados restaurado não será possível se o repositório de dados original estiver presente no mesmo RPS. É necessário excluir o repositório de dados original antes de importar o restaurado. Como alternativa, importe o repositório de dados para outro RPS.
6. Se necessário, modifique os detalhes do repositório de dados e clique em **Salvar**.

   Quando o repositório de dados restaurado for importado, o Arcserve UDP continuará a ler os destinos de índice, hash e dos dados das definições da configuração

do repositório de dados e mostrará os caminhos reais em que o repositório de dados residia originalmente. Depois da conclusão da importação, esses destinos de caminhos precisam ser alterados para os novos caminhos restaurados.

Observação: não é possível ativar ou desativar a opção de criptografia para um repositório de dados existente.

O repositório de dados é adicionado ao servidor de ponto de recuperação e exibido na caixa de diálogo **Destinos: servidores de ponto de recuperação**.

Depois da conclusão de uma importação com êxito, uma marca de seleção verde é exibida ao lado do nome do repositório de dados correspondente.

Você restaurou com êxito um repositório de dados de redução de redundância de uma fita.

Capítulo 3: Usando a interface do PowerShell

Esta seção contém os seguintes tópicos:

Como usar a interface do PowerShell

O Arcserve UDP fornece recursos do PowerShell que permitem que você envie uma tarefa de backup, execute uma restauração e recupere uma VM a partir da linha de comando. A interface do PowerShell é chamada de UDPPowerCLI.ps1.

Verificar o pré-requisito

Verifique os pré-requisitos a seguir antes de usar a interface do PowerShell:

- É necessário ter o Windows 2008 R2 Server ou versões posteriores.
- É necessário ter o PowerShell 3 ou versão superior instalado no servidor.

Usando a interface do PowerShell para Arcserve UDP

O utilitário PowerShell é fornecido com o arquivo de instalação do Arcserve UDP.

Quando você instala o Arcserve UDP, o arquivo normalmente é instalado no seguinte local:

C:\Arquivos de programas\Arcserve\Unified Data Protection

Nesses casos, no Console, a UDPPowerCLI.ps1 é instalada no seguinte local:

C:\Arquivos de programas\Arcserve\Unified Data Protection\Management\PowerCLI

No RPS ou no Agente, o UDPPowerCLI.ps1 é instalado no seguinte local:

C:\Arquivos de programas\Arcserve\Unified Data Protection\Engine\PowerCLI

Consulte as opções a seguir para obter ajuda ao usar a interface do PowerShell:

- Atualize a diretiva de execução do PowerShell para permitir que os scripts sejam executados. Por exemplo, atualize a diretiva de execução para **Set-ExecutionPolicy Unrestricted**.

  Observação: para obter mais informações sobre como alterar a diretiva de execução, consulte o site da Microsoft.

- Execute o seguinte comando do PowerShell para obter mensagens de ajuda e exemplos detalhados dos scripts:

  ```
  No Console:
  ```

  Get-Help 'C:\Program Files\Arcserve\Unified Data Protection\Management\PowerCLI\UDPPowerCLI.ps1' -full

  No RPS ou no Agente:

  Get-Help 'C:\Arquivos de programas\Arcserve\Unified Data Protection\Engine\PowerCLI\UDPPowerCLI.ps1' -full

Sintaxe do PowerShell e parâmetros

SYNTAX 1

```
UDPPowerCLI.ps1 -Command <CreatePswFile> -Password
<System.Security.SecureString> -PasswordFile
<string> [<CommonParameters>]
```

SYNTAX 2

```
UDPPowerCLI.ps1 -Command <Backup> [-UDPCon-
soleServerName <String>] [-UDPConsoleProtocol <
{http|https}>] [-UDPConsolePort <int>] [-UDPCon-
soleUserName [<String>]] [-UDPConsolePassword <Sys-
tem.Security.SecureString>] [-UDPConsolePasswordFile
<String>] [-UDPConsoleDomainName <String>] -planName
<String> -nodeName <String> [-backupJobType
<String>] [-jobDescription <String>] [-waitJobFinish
<String String>] [-timeOut <int>] [-jobType <{ agent-
base|agentless|uncpath} String>] [-backupS-
cheduleType <String>] [<CommonParameters>]
```

SYNTAX 3

```
UDPPowerCLI.ps1 -Command <Restore> [-UDPCon-
soleServerName <String>] [-UDPConsoleProtocol
<String>] [-UDPConsolePort <int>] [-UDPCon-
soleUserName <String>] [-UDPConsolePassword <Sys-
tem.Security.SecureString>] [-UDPConsolePasswordFile
<String>] [-UDPConsoleDomainName <String>] [-UDPA-
gentServerName <String>] [-UDPAgentProtocol
<String>] [-UDPAgentPort <int>] [-UDPAgentUserName
<String>] [-UDPAgentPassword <Sys-
tem.Security.SecureString>] [-UDPAgentPasswordFile
<String>] [-UDPAgentDomainName <String>] [-Res-
toreDirectoryPath <String>] [-RestoreFilePath
<String>] [-BackupSessionNumber <int>] [-VmName
<String>] -RestoreDestination <String> [-Res-
toreDestinationUserName <String>] [-Res-
toreDestinationPassword
<System.Security.SecureString>] [-CreateRootFolder
<String>] [-ChangeFileName <String>] [-Repla-
ceActiveFilesFlag <String>] [-OverwriteExistFiles
<String>] [<CommonParameters>]
```

SYNTAX 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>] [-
BackupSessionNumber <int>] -RecoverVmName <String>
[-OverwriteExistingVM <String>] [-PoweronVM
<String>] [<CommonParameters>]
```

DESCRIÇÃO

Um utilitário para estabelecer conexão com o serviço do console do Arcserve UDP e enviar tarefas de backup e restauração.

PARÂMETROS

-Command <String>

Especifica o comando usado. Atualmente as sequência de caracteres a seguir são suportadas:

- CreatePswFile
- Backup
- Restauração
- RecoverVM

Necessário? **verdadeiro**

Posição? **nomeado**

Valor padrão

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-Password <System.Security.SecureString>

Especifica a senha que você deseja usar para criar o arquivo de senhas.

Necessário? **falso**

Posição? **nomeado**

Valor padrão

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-UDPConsoleServerName <String>

Especifica o nome DNS do servidor UDP (o servidor em que você instalou o Console) ao qual você deseja se conectar. Se esse valor não for especificado, o cmdlet usa o valor padrão, o nome DNS da máquina local.

Necessário? **falso**

Posição? **nomeado**

Valor padrão **$env:NOMEDOCOMPUTADOR**

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-UDPConsolePort <int>

Especifique o número de porta que deseja usar para a conexão. Se esse valor não for especificado, o cmdlet usa o valor padrão, 8015.

Necessário? **falso**

Posição? **nomeado**

Valor padrão **8015**

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-UDPConsoleProtocol <String>

Especifica o protocolo no servidor que deseja usar para a conexão. O protocolo pode ser http ou https. Se esse valor não for especificado, o cmdlet usará o valor padrão (http).

Necessário? **falso**

Posição? **nomeado**

Valor padrão **http**

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-UDPConsoleUserName <String>

Especifica o nome do usuário que você deseja usar para conectar ao servidor UDP. Se o nome de usuário não for especificado, o cmdlet usa o nome de usuário atualmente usado para efetuar logon no sistema.

Necessário? **falso**

Posição? **nomeado**

Valor padrão **$env:UserName**

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-UDPConsolePassword <System.Security.SecureString>

Especifica a senha que você deseja usar para conectar ao servidor UDP.

Necessário? **falso**

Posição? **nomeado**

Valor padrão

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-PasswordFile <String>

Especifica a geração do arquivo de senha.

Necessário? **verdadeiro**

Posição? **nomeado**

Valor padrão

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-UDPConsolePasswordFile <String>

Especifica o arquivo de senha do UDP que você deseja usar para se conectar ao servidor do UDP.

Necessário? **falso**

Posição? **nomeado**

Valor padrão

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-UDPAgentServerName <String>

Especifica o nome DNS do servidor do agente UDP para o qual você deseja conectar-se para restauração.

Necessário? **falso**

Posição? **nomeado**

Valor padrão **$env:NOMEDOCOMPUTADOR**

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-UDPAgentProtocol <String>

Especifique o protocolo da internet que deseja usar para conectar ao servidor do agente UDP. Ele pode ser http ou https. Se esse valor não for especificado, o cmdlet usará o valor padrão (http).

Necessário? **falso**

Posição? **nomeado**

Valor padrão **http**

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-UDPAgentPort <int>

Especifica o número da porta que deseja usar para se conectar ao servidor do agente UDP. Se esse valor não for especificado, o cmdlet usa o valor padrão, 8014.

Necessário? **falso**

Posição? **nomeado**

Valor padrão **8014**

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-UDPAgentUserName <String>

Especifica o nome de usuário que você deseja usar para conectar ao servidor do agente UDP. Se o nome de usuário não for especificado, o cmdlet usa o nome de usuário atualmente usado para efetuar logon no sistema.

Necessário? **falso**

Posição? **nomeado**

Valor padrão **$env:UserName**

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-UDPAgentPassword <System.Security.SecureString>

Especifique a senha que deseja usar para se conectar ao servidor do agente UDP.

Necessário? **falso**

Posição? **nomeado**

Valor padrão

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-UDPAgentPasswordFile <String>

Especifica o arquivo de senha do agente UDP que você deseja usar para se conectar ao servidor do agente UDP.

Necessário? **falso**

Posição? **nomeado**

Valor padrão

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-UDPAgentDomainName <String>

Especifica o nome do domínio em que o usuário do agente UDP especificado está localizado.

Necessário? **falso**

Posição? **nomeado**

Valor padrão

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-NodeName <String>

Especifica o nome do nó que deseja fazer backup.

Necessário? **verdadeiro**

Posição? **nomeado**

Valor padrão

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-RestoreFilePath <String>

Especifica o arquivo que você deseja restaurar.

Necessário? **falso**

Posição? **nomeado**

Valor padrão

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-RestoreDirectoryPath <String>

Especifica o diretório que você deseja restaurar.

Necessário? **falso**

Posição? **nomeado**

Valor padrão

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-BackupSessionNumber <int>

Especifica o número de sessão que será usada para a tarefa de restauração.

Necessário? **falso**

Posição? **nomeado**

Valor padrão

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-VmName <String>

Especifica o nome de host de uma máquina virtual para a restauração de arquivo ou diretório a partir de sua sessão de backup.

Necessário? **falso**

Posição? **nomeado**

Valor padrão

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-RestoreDestination <String>

Especifica o caminho do diretório em que os arquivos serão restaurados.

Necessário? **falso**

Posição? **nomeado**

Valor padrão

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-RestoreDestinationUserName <String>

Especifica o nome do usuário do computador de destino para o qual deseja restaurar dados. O nome de usuário pertence ao usuário que pode efetuar logon no computador de destino.

Necessário? **falso**

Posição? **nomeado**

Valor padrão

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-RestoreDestinationPassword <System.Security.SecureString>

Especifica a senha que será usada para efetuar logon no computador de destino.

Necessário? **falso**

Posição? **nomeado**

Valor padrão

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-CreateRootFolder <String>

Especifica que se uma estrutura de diretórios raiz existir na imagem de backup capturada, o Arcserve UDP recriará a mesma estrutura de diretórios raiz no caminho de destino de restauração. Quando essa opção não é selecionada, o arquivo ou pasta é restaurado diretamente para a pasta de destino. É possível usar qualquer uma das seguintes sequências de caracteres:

- Verdadeiro
- Falso

Necessário? **falso**

Posição? **nomeado**

Valor padrão **Falso**

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-ChangeFileName <String>

Cria um novo arquivo se o nome de arquivo já existir. A seleção desta opção copia o arquivo de origem no destino com o mesmo nome de arquivo, mas com uma extensão diferente. Os dados serão restaurados no novo arquivo. É possível usar qualquer uma das seguintes sequências de caracteres:

- Verdadeiro
- Falso

Necessário? **falso**

Posição? **nomeado**

Valor padrão **Falso**

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-ReplaceActiveFilesFlag <String>

Substitui todos os arquivos ativos após reinicializar. Se, durante a tentativa de restauração, o Agente do Arcserve Unified Data Protection para Windows detectar que o arquivo existente está em uso ou sendo acessado, ele não substituirá o arquivo imediatamente, mas evitará que qualquer problema atrase a substituição dos arquivos ativos até a próxima reinicialização do computador. (A restauração ocorrerá imediatamente, mas a substituição de arquivos ativos é feita durante a próxima reinicialização). Essa opção está disponível apenas quando o parâmetro **OverwriteExistingFiles** for True. É possível usar qualquer uma das seguintes sequências de caracteres:

- Verdadeiro
- Falso

Necessário? **falso**

Posição? **nomeado**

Valor padrão **Falso**

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-OverwriteExistingFiles <String>

Sobrescreve (substitui) qualquer arquivo existente que está localizado no destino da restauração. Todos os objetos serão restaurados dos arquivos de backup, independentemente da presença atual deles no computador. É possível usar qualquer uma das seguintes sequências de caracteres:

- Verdadeiro
- Falso

Necessário? **falso**

Posição? **nomeado**

Valor padrão **Falso**

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-UDPConsoleDomainName <String>

Especifica o nome do domínio em que o usuário especificado está localizado. Se esse valor não for especificado, o cmdlet usará o nome do domínio do computador local; ou o nome DNS do computador local se ele não estiver em um domínio.

Necessário? **falso**

Posição? **nomeado**

Valor padrão

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-PlanName <String>

Especifica o nome do plano que define a configuração da tarefa de backup.

Necessário? **verdadeiro**

Posição? **nomeado**

Valor padrão

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-BackupJobType <String>

Especifica o tipo da tarefa de backup. Um dos valores a seguir pode ser usado: Full (indica um backup completo), Incr (indica um backup Incremental) ou Rsyn (indica um backup de ressincronização). As seguintes sequências de caracteres são suportadas:

- Completo
- Incr
- Rsyn

Necessário? **verdadeiro**

Posição? **nomeado**

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-JobDescription <String>

Especifica a descrição da tarefa de backup.

Necessário? **verdadeiro**

Posição? **nomeado**

Valor padrão **PowerCLIJo**

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-RecoverVmName <String>

Especifica o nome de host da máquina virtual que deseja recuperar.

Necessário? **verdadeiro**

Posição? **nomeado**

Valor padrão

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-OverwriteExistingVM <String>

Especifica que, se o valor for verdadeiro, a tarefa de restauração substituirá a máquina virtual existente. O valor padrão é falso. É possível usar qualquer uma das seguintes sequências de caracteres:

- Verdadeiro
- Falso

Necessário? **falso**

Posição? **nomeado**

Valor padrão **Falso**

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-PoweronVM <String>

Especifica que se o valor é verdadeiro, a máquina virtual é ligada após ser recuperada. O valor padrão é falso. É possível usar qualquer uma das seguintes sequências de caracteres:

- Verdadeiro
- Falso

Necessário? **falso**

Posição? **nomeado**

Valor padrão **Falso**

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-waitJobFinish <{true|false} String>

Especifica que se o valor for verdadeiro, o comando aguardará mais instruções até que a tarefa de backup seja concluída. O valor padrão é falso. É possível usar qualquer uma das seguintes sequências de caracteres:

- Verdadeiro
- Falso

Necessário? **falso**

Posição? **nomeado**

Valor padrão **Falso**

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-timeOut <int>

Especifica o tempo máximo de espera (em segundos) para a tarefa de backup ser concluída.

Necessário? **falso**

Posição? **nomeado**

Valor padrão **600**

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-jobType <String>

Especifica o tipo de tarefa de backup para tipos de nós diferentes. O valor padrão é agentbase. Use qualquer uma das seguintes strings:

- agentbase
- agentless
- uncpath

Necessário? **falso**

Posição? **nomeado**

Valor padrão **agentbase**

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

-backupScheduleType <String>

Especifica a tarefa de backup de programação, envia a tarefa de backup de programação especificada imediatamente e é executada somente uma vez. As seguintes sequências de caracteres são suportadas:

- Diário
- Semanal
- Mensal

Necessário? **falso**

Posição? **nomeado**

Valor padrão

Aceitar entrada do pipeline? **falso**

Aceitar caracteres curinga? **falso**

<CommonParameters>

Esse cmdlet oferece suporte para os parâmetros comuns como **Verbose**, **Debug**, **ErrorAction**, **ErrorVariable**, **WarningAction**, **WarningVariable**, **OutBuffer** e **OutVariable**. Para obter mais informações, consulte about_CommonParameters.

ENTRADAS

SAÍDAS

- 0 ou 1

Se a tarefa for enviada com êxito, o comando retorna 0; caso contrário retorna 1.

Exemplos do PowerShell

Create System.Security.SecureString type of password

Observação: se você tiver um script de PowerShell configurado no Arcserve UDP 6.5 que utiliza uma senha de texto simples, modifique-o para usar $SecurePassword ou um arquivo de senhas.

Descrição

O comando é usado para criar a senha com o tipo System.Security.SecureString e também é usado por todos os outros comandos. O tipo System.Security.SecureString é predefinido pelo sistema. Há várias maneiras de gerá-lo. Os dois tipos a seguir são usados com frequência para diferentes finalidades:

- Esse comando solicita a inserção da senha no console do PowerShell. É necessário interação com os usuários finais. Geralmente, depois de executar esse comando, pode-se executar o comando *CreatePswFile* para gravar a senha em um arquivo de senhas. Em seguida, use o arquivo de senhas para executar scripts do PowerShell automaticamente.

  ```
  $SecurePassword = Read-Host -AsSecureString
  ```

- Esse comando requer a senha em texto sem formatação. Ele pode ser usado diretamente para executar scripts do PowerShell automaticamente.

  ```
  $SecurePassword = ConvertTo-SecureString
  "<PlainPassword>" - AsPlainText - Force
  ```

- (Opcional) Depois de executar um dos comandos anteriores para atribuir uma senha, execute o comando CreatePswFile para gravar a senha em um arquivo de senhas. Em seguida, use o arquivo de senhas para executar scripts do PowerShell automaticamente.

  O comando criptografa a senha de segurança e a salva no arquivo de senhas.

  ```
  C:\PS>UDPPowerCLI.ps1 -Command CreatePswFile
  -Password $SecurePassword -PasswordFile
  myUDPPasswordFile
  ```

Exemplo 1

Descrição

O comando criptografa a senha de segurança e a salva no arquivo de senhas.

```
C:\PS>UDPPowerCLI.ps1 -Command CreatePswFile -
Password $SecurePassword -PasswordFile
myUDPPasswordFile
```

Exemplo 2

Descrição

No servidor local, o comando se conecta ao serviço do Console UDP com o protocolo HTTP pela porta 8015 e envia uma tarefa de backup incremental para o plano chamado *myplan*.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPCon-
soleUserName myUsr -UDPConsolePassword $Se-
curePassword -PlanName myPlan -BackupJobType Incr
```

Exemplo 3

Descrição

No servidor local, o comando se conecta ao serviço do Console UDP com o protocolo HTTP pela porta 8015 e, em seguida, envia uma tarefa de backup Incremental para o nó chamado *myNodeName*.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPCon-
soleUserName myUsr -UDPConsolePasswordFile
myUDPPasswordFile -NodeName myNodeName -
BackupJobType Incr
```

Exemplo 4

Descrição

O comando se conecta ao serviço do Console do UDP no servidor chamado *myServer* com protocolo HTTPS pela porta 8018 e, em seguida, envia uma tarefa de backup completo para o plano chamado *myPlan*e defina a descrição da tarefa como *myJob*.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPCon-
soleServerName myServer -UDPConsoleProtocol https -
UDPConsolePort 8018 -UDPConsoleUserName myUsr -
UDPConsolePassword $SecurePassword -UDPCon-
soleDomainName myDomain -PlanName myPlan -
BackupJobType Full -JobDescription myJob
```

Exemplo 5

Descrição

O comando conecta-se ao serviço do agente do UDP no servidor *yourUDPAgentServer* com o protocolo HTTP pela porta 8014 e, em seguida, envia uma tarefa de backup incremental para o *yourUDPAgentServer*.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPA-
gentServerName yourUDPAgentServer -UDPA-
gentPasswordFile myUDPAgentPasswordFile -
BackupJobType Incr
```

Exemplo 6

Descrição

O comando abrevia o nome do parâmetro.

```
C:\PS>UDPPowerCLI.ps1 -Cmd Backup -Svr myServer -Ptc
https -Prt 8018 -Usr myUsr -Psw $SecurePassword -Dmn
myDomain -Pln myPlan -Jbt Full -Jbd myJob
```

Exemplo 7

Descrição

O comando se conecta ao servidor chamado *yourUDPAgentServer* usando o nome de usuário do ambiente, o protocolo HTTP padrão e a porta 8014. Ele verifica se a sessão de backup é número 1 na configuração de backup do *yourUDPAgentServer* e, em seguida, restaura o diretório para o local original, com a opção de restauração selecionada como Substituir os arquivos existentes.

```
C:\PS>UDPPowerCLI.ps1 -Command restore -UDPA-
gentServerName yourUDPAgentServer -UDPA-
gentPasswordFile myUDPAgentPasswordFile -
RestoreDirectoryPath 'c:\Test' -BackupSessionNumber
1
```

Exemplo 8

Descrição

O comando se conecta ao servidor chamado *yourUDPAgentServer* usando o protocolo HTTPS e a porta 8018. Ele verifica se a sessão de backup é número 1 na configuração de backup do *yourUDPAgentServer* e, em seguida, restaura o arquivo 1.txt para um local alternativo, com a opção de restauração selecionada como Substituir arquivo existente e criar diretório raiz.

```
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' -Res-
toreDestinationUserName remoteAccessUser -Res-
toreDestinationPassword remoteAccessPsw -
CreateBaseFolder 'true'
```

Exemplo 9

Descrição

O comando se conecta ao servidor chamado *yourUDPAgentServer* usando o nome de usuário do ambiente, o protocolo HTTP padrão e a porta 8014. Em seguida, ele se conecta ao servidor de UDP usando a porta padrão 8015 e o protocolo HTTP para verificar se o número da sessão de backup é 1. Por fim, ele restaura o diretório para um local alternativo, com a opção de restauração selecionada como Substituir arquivo existente e criar diretório raiz.

```
C:\PS>UDPPowerCLI.ps1 -Command restore -UDPA-
gentServerName yourUDPAgentServer -UDPA-
gentPasswordFile myUDPAgentPasswordFile -
RestoreDirectoryPath 'c:\Test' -BackupSessionNumber
1 -RestoreDestination 'C:\restore' -Res-
toreDestinationUserName remoteAccessUser -Res-
toreDestinationPassword remoteAccessPsw -
UDPConsoleServerName yourUDPServer -vmname sour-
ceVMName -UDPConsolePasswordFile myUDPPasswordFile -
domainname yourUDPDomainName -OverwriteExistFiles
'true' -CreateRootFolder 'true'
```

Exemplo 10

Descrição

O comando se conecta ao servidor chamado *yourUDPAgentServer* usando o nome de usuário do ambiente, o protocolo HTTP padrão e a porta 8014. Em seguida, ele se conecta ao servidor de UDP usando a porta padrão 8015 e o protocolo HTTP para verificar se o número da sessão de backup é 1. Por fim, ele recupera a VM no local original, com a opção de recuperar a VM selecionada como Substituir a vm existente e ligar a vm após a recuperação.

```
C:\PS>UDPPowerCLI.ps1 -Command RecoverVM -UDPA-
gentServerName yourUDPAgentServer -UDPA-
gentPasswordFile myUDPAgentPasswordFile -
BackupSessionNumber 1 -UDPConsoleServerName
yourUDPServer -recovervmname sourceVMName -UDPCon-
solePasswordFile myUDPPasswordFile -UDPCon-
soleDomainName yourUDPDomainName -
OverwriteExistingVM 'true' -PoweronVM 'true'
```

Exemplo 11

Descrição

O comando envia a tarefa de backup semanal no agente do UDP imediatamente, sendo executado apenas uma vez.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPA-
gentServerName myServer -UDPAgentPassword $Se-
curePassword -UDPAgentDomainName myDomainName -
UDPAgentUserName UDPAgentUsername -BackupJobType
Incr -backupScheduleType 'weekly' -jobDescription
'PowerCLIJob'
```

Exemplo 12

Descrição

O comando envia a tarefa de backup e define o tempo limite em segundos para a conclusão da tarefa.

```
C:\PS>UDPPowerCLI.ps1 -Command Backup -UDPCon-
soleServerName myServer -UDPConsolePasswordFile
myUDPPasswordFile -UDPConsoleDomainName myDomainName
-nodeName myNodeName -UDPConsoleUserName myAdmin -
BackupJobType Incr -jobDescription 'PowerCLIJob'
waitJobFinish 'true' -timeout 600 -jobType 'agent-
base'
```

Arquivo de configuração e propriedades do PowerCLI

É possível personalizar o seguinte arquivo de configuração e propriedades do UDP PowerCLI:

Nome do arquivo de configuração: *PowerCLIConfiguration.properties*

Local de instalação do arquivo de configuração:

- *C:\Arquivos de programas\Arcserve\Unified Data Protection\Management\Configuration*
- *C:\Arquivos de programas\Arcserve\Unified Data Protection\Engine\Configuration*

Formato do arquivo de configuração:

Enable24HoursSetting=yes

LogPath=D:\PowerCLILogPath

RotationSizeInMB=2

RetentionPeriodInDays=5

RetainNoOfFiles=6

Propriedades de configuração:

Nome da propriedade	Descrição	Valor padrã-	Valor aceito

		o	
Enable24HoursSetting	▪ Se o valor for definido como Sim, o carimbo de data e hora do arquivo de log será gravado no formato de 24 horas. ▪ Se o valor for definido como Não, o carimbo de data e hora do arquivo de log será gravado no formato de 12 horas.	Sim	Sim ou Não
LogPath	▪ O local da pasta dos arquivos de log do PowerCLI. ▪ Se o local não for fornecido, o arquivo de log será gravado em seu local padrão. ▪ LogPath aceita caminhos relativos e absolutos. ▪ Símbolos, exceto \ / : * ? < > | são aceitáveis para nome de arquivo ou pasta.	-	-
RotationSizeInMB	▪ Se o limite especificado fornecido em RotationSizeInMB for atingido, o arquivo de log do PowerCLI será renomeado (rotacionado) com um carimbo de data e hora.	0	Mínimo = 1 Máximo = 1024
RetentionPeriodInDays	▪ Se os arquivos rotacionados forem mais antigos que o valor fornecido em RetentinPeriodInDays, os arquivos de log antigos serão excluídos.	0	Mínimo = 5 Máximo = 365
RetainNoOfFiles	▪ Se houver mais arquivos de log rotacionados do que o valor fornecido em RetainNoOfFiles, os arquivos extras serão excluídos.	0	Mínimo = 5 Máximo = 1000

Observações:

- Se você fornecer valores para propriedades de configuração diferentes do valor permitido, o PowerCLI exibirá erro e a execução será interrompida.
- Se você fornecer valores padrão para as propriedades de configuração, a execução do PowerCLI continuará e será executada com o comportamento padrão.

Capítulo 4: Protegendo o sistema Oracle usando o RMAN (Recovery Manager - Gerenciador de recuperação)

O RMAN é um utilitário Oracle que executa tarefas de backup, restauração e recuperação em bancos de dados e automatiza a administração de estratégias de backup. Com esse recurso, é possível fazer backup, restaurar e recuperar facilmente os arquivos do banco de dados.

Esta seção contém os seguintes tópicos:

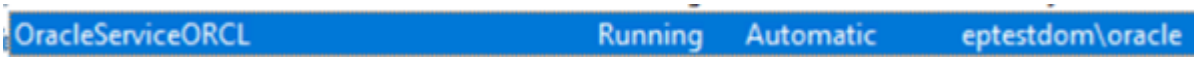
Revisar os pré-requisitos do banco de dados Oracle com RMAN (Windows e Linux)

Pré-requisitos para configurar quando o Oracle está instalado no Windows

Adicionar plano

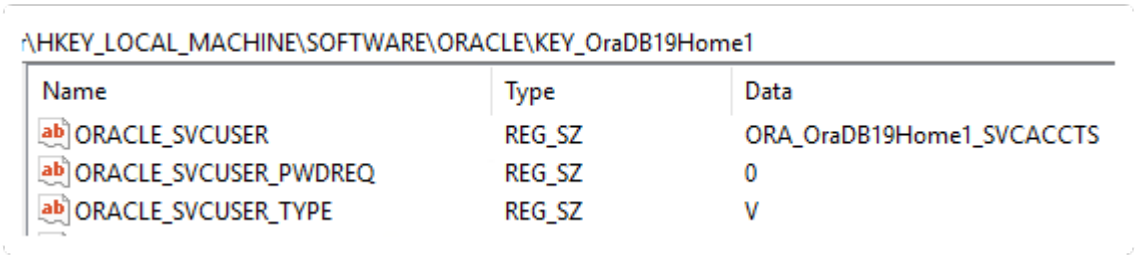
- Os nós do Oracle no Windows, o console do UDP e o RPS devem estar no mesmo domínio.
- O console do UDP e os sistemas RPS devem ser instalados e usados com o administrador de domínio (“<domínio>\administrator”) ou conta equivalente.
- Ao efetuar logon no console do UDP, faça o seguinte:
  1. O usuário "<domínio>\Administrador" é adicionado ao grupo local "ORA_DBA" nos nós do Windows Oracle.
  2. Adicione o nó do Oracle ao console do UDP usando a ID de usuário "<domínio>\DomainUser".

  Observação: é possível usar qualquer usuário do UDP que não seja administrador, mas as permissões apropriadas precisam ser fornecidas.
- Oferece suporte às contas do Oracle usadas durante as instalações do Oracle (aplicável para contas independentes e RAC).
  - Usuário do domínio: anote o usuário do domínio que possui o serviço Oracle (conta de serviço). Por exemplo, eptestdom\oracle.

  - Conta virtual: quando o Oracle é instalado usando uma conta virtual, verifique os parâmetros no registro do servidor Oracle antes de adicionar o banco de dados ao plano do UDP.

    Observação: por padrão, as contas virtuais são ativadas no Windows.

- Certifique-se de configurar adequadamente o Listener, que ajuda a proteger o banco de dados Oracle e se conecta ao sqlplus e ao RMAN desse banco de dados.

Exemplo: “rman target / “ deve levar ao banco de dados correto.

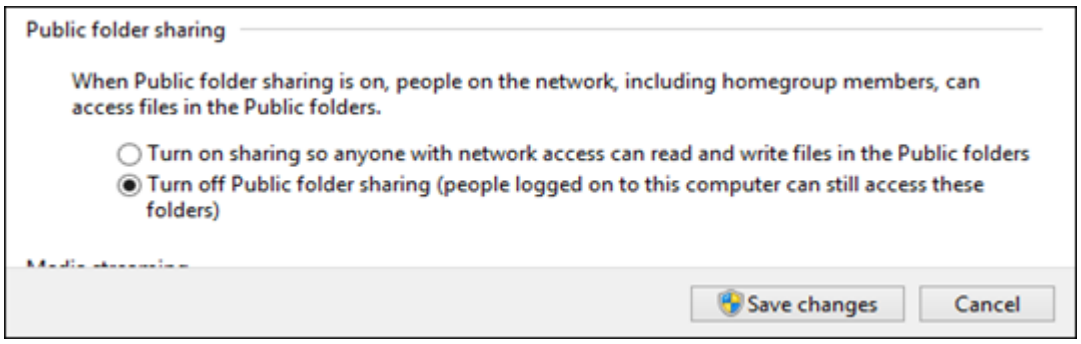
Backup

- Ao fazer backup dos bancos de dados Oracle, certifique-se de que ele esteja no estado ABERTO com o modo ARCHIVELOG ativado. Para obter mais informações, consulte Como ativar o modo ARCHIVELOG.
- Para executar com êxito os backups do Oracle RMAN com o Arcserve UDP, é necessário ativar a autenticação nativa do Windows. Para confirmar se a autenticação do Windows está ativada, certifique-se de que a linha abaixo seja adicionada ao arquivo sqlnet.ora no caminho ORACLE_HOME/-network/admin.

  SQLNET.AUTHENTICATION_SERVICES= (NTS)
- Compartilhamento de pasta pública é desativado para permitir o acesso seguro aos bancos de dados.

  Para desativar o uso da pasta pública para compartilhamento de rede, siga estas etapas:

  1. Vá para a Central de rede e compartilhamento e clique em **Alterar configurações de compartilhamento avançadas**.
  2. No painel esquerdo, procure a configuração de compartilhamento de pasta pública para o local de rede ativo e, em seguida, clique em **Desativar compartilhamento de pasta pública (as pessoas conectadas a este computador ainda podem acessar essas pastas)**.
  3. Clique em **Salvar alterações**.



Restaurar tabelas

As restaurações no nível de espaço para tabela e tabela usam o banco de dados auxiliar, que requer as seguintes permissões:

- **Usuário de domínio para instalação do Oracle:** adicione a conta de serviço do usuário do Oracle ao grupo “Administradores” nos nós do Oracle. Por

exemplo, eptestdom\oracle é adicionado ao grupo de administradores locais.

- **Conta virtual para instalação do Oracle:** abra a chave do Registro: HKLM\SYSTEM\CurrentControlSet\services\eventlog\Application e, em seguida, clique com o botão direito do mouse e adicione permissões ao grupo, como 'ORA_OraDB18Home1_SVCACCTS'.

Restaurar para o nó alternativo

- A mesma versão do Oracle com a mesma configuração está instalada no sistema de destino.
- O banco de dados é instalado com o mesmo SID do computador de origem (original).
- O banco de dados Oracle no nó de destino deve estar no estado desligado.

Configurações de firewall para permitir acesso aos nós do Oracle no 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**	O número da porta pode ser alterado com base na porta configurada.

Pré-requisitos para configurar quando o Oracle está instalado no Linux

Adicionar plano

- O nó do Oracle /etc/hosts deve ter uma entrada para FQDN e “resolv.conf” com a entrada de DNS apropriada.
- Todo banco de dados que precisa ser protegido deve ter uma entrada no arquivo /etc/oratab.

  Observação: no ambiente RAC, certifique-se de que o conteúdo esteja atualizado para ambos os nós.

  A sintaxe no arquivo /etc/oratab é a seguinte:

  <DB_UNIQUE_NAME>:<ORACLE_HOME>:<ACTIVE/INACTIVE>

  Exemplo: ORCL:/u01/app/oracle/ORCL/:Y

Backup

- Ao fazer backup dos bancos de dados Oracle, certifique-se de que ele esteja no estado ABERTO com o modo ARCHIVELOG ativado. Para obter mais informações, consulte Como ativar o modo ARCHIVELOG.
- Instale smbclient usando o seguinte comando:

  #yum install smbclient
- Certifique-se de configurar adequadamente o Listener, que ajuda a proteger o banco de dados Oracle e a se conectar ao sqlplus e ao RMAN para esse banco de dados.

  Exemplo: marque “lsnrctl status” para os bancos de dados disponíveis para um determinado listener.

  O comando “rman target /“ deve estar conectado ao banco de dados correto especificado para o backup.

Tarefas de recuperação garantida

- Certifique-se de que os bancos de dados Oracle para backup estejam no estado MONTAGEM ou ABERTO.

Autenticação com base em chave pública e privada

Observação: a autenticação com base em chave pública e privada foi implantada para a execução de scripts RMAN do Linux. Isso evita senhas de texto sem formatação ao executar scripts remotos no servidor Oracle Linux a partir do RPS (Recovery Point Server - Servidor de Ponto de Recuperação).

1. No nó do RPS, faça o seguinte:
   a. Verifique se o instalador criou o diretório *PrivateKey* no seguinte caminho:

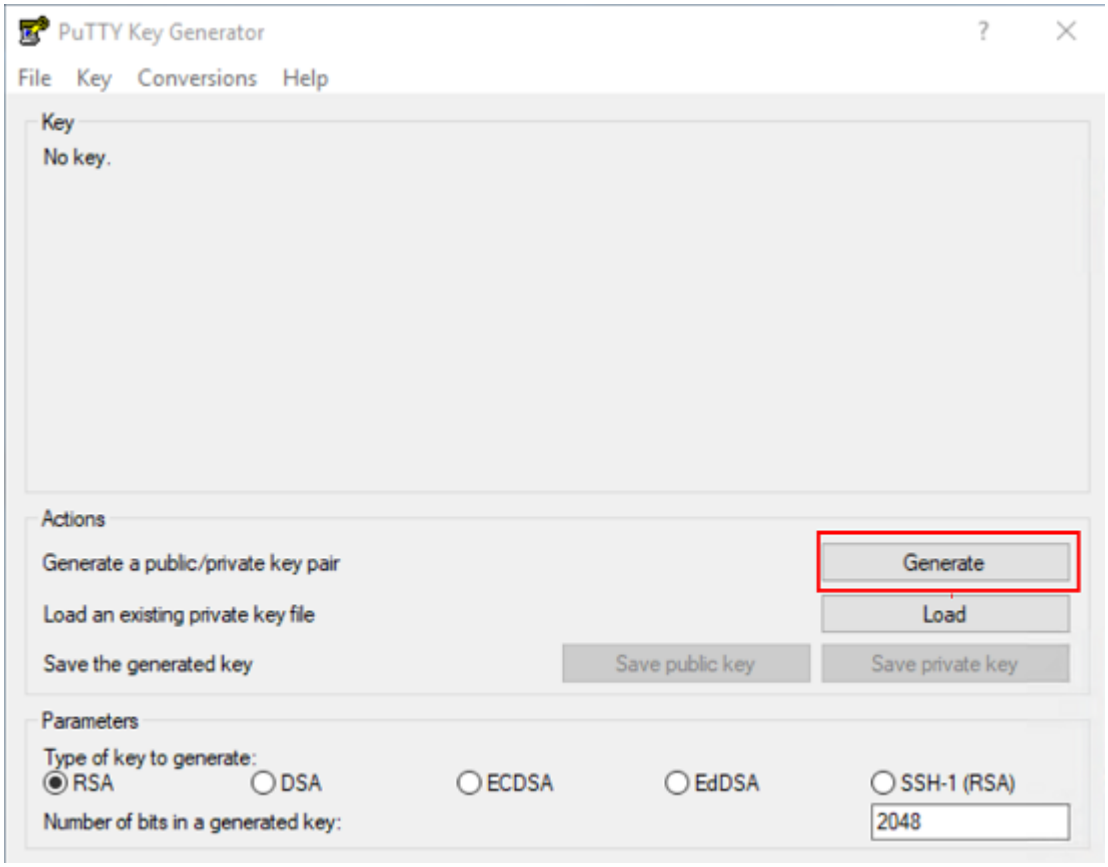
      *Install Path**Arcserve**Unified Data Protection**Engine**BIN**OracleRMAN**PrivateKey*

   b. Instale o PuTTY (versão 0.73 ou superior) e, em seguida, para abrir o PuTTY Key Generator, execute um dos procedimentos a seguir:
      - Em cmd.exe, execute o comando *puttygen*.
      - Vá para **Todos os programas** > **PuTTY** > **PuTTYgen**.

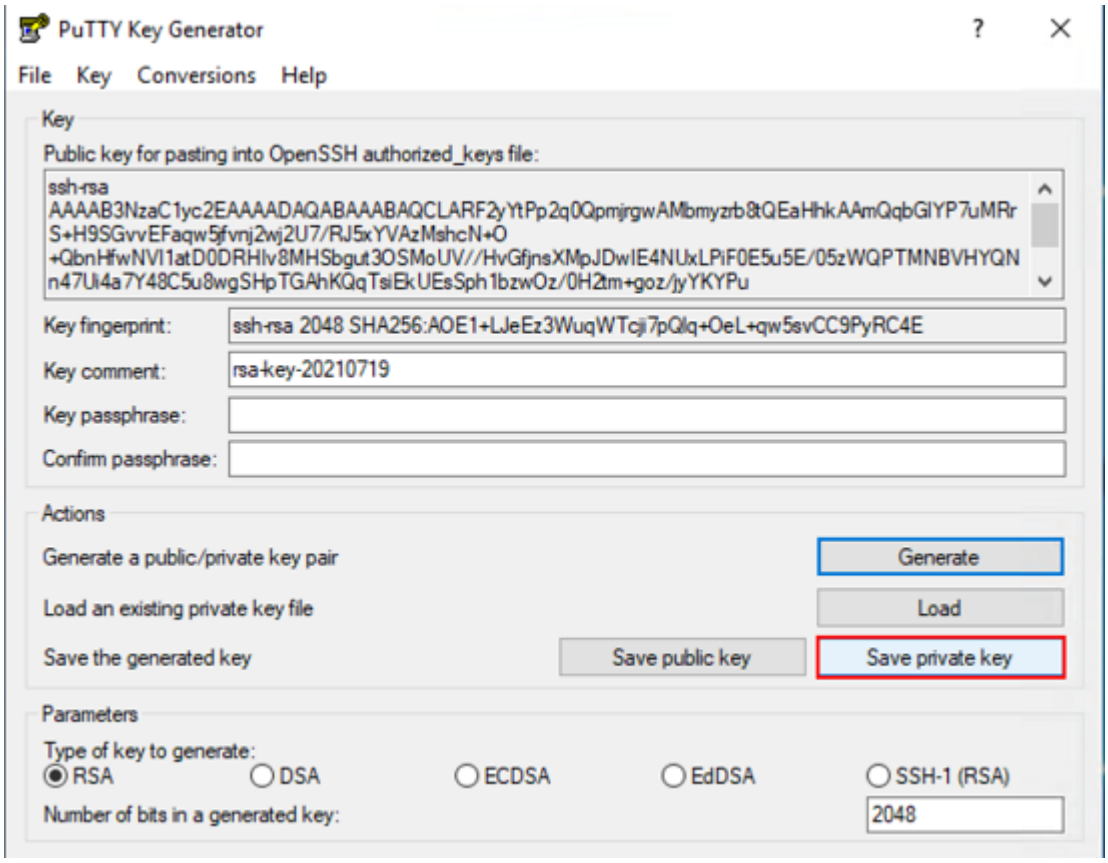
      A caixa de diálogo Gerador de chaves PuTTY é exibida.

   c. Na caixa de diálogo Gerador de chaves PuTTY, clique em **Gerar**.

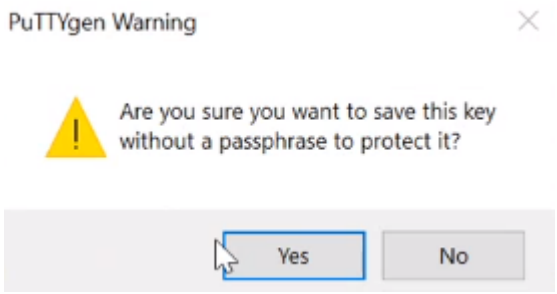
      As chaves públicas e privadas são geradas.



   d. Clique em **Salvar chave privada**.



e. Na caixa de diálogo Aviso de PuTTYgen, clique em **Sim** para salvar a chave privada sem uma frase secreta.



f. Ao salvar a chave privada, navegue até o seguinte caminho, digite o nome do arquivo e clique em **Salvar**:

Install Path\Arcserve\Unified Data Protection\Engine\BIN\OracleRMAN\PrivateKey

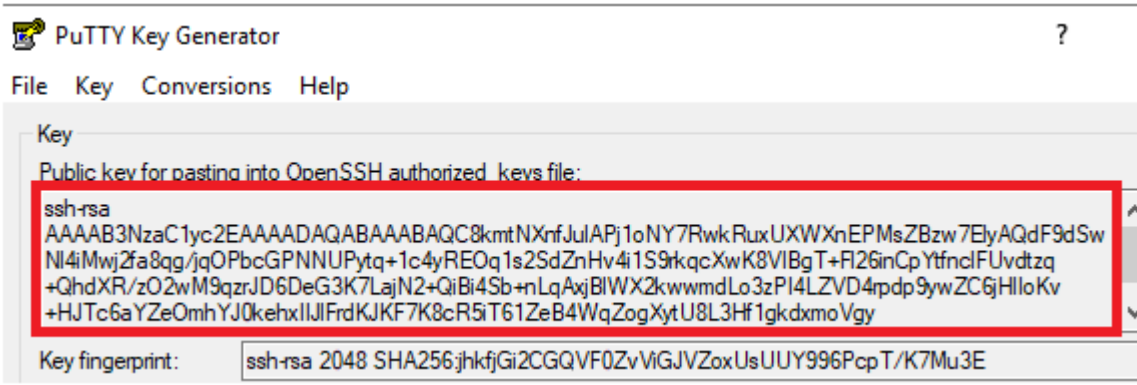
Observações:

- O nome do arquivo deve estar no formato PrivateKeyFile.ppk. Você pode fornecer qualquer nome.
- Salve a chave privada com a extensão .ppk no seguinte caminho:

  Engine\Bin\OracleRMAN\PrivateKey

- Copie a chave pública manualmente a partir da caixa de diálogo Gerador de chaves PuTTY e salve-a em um formato de texto na pasta a seguir para referências futuras, caso ela precise ser adicionada a alguns outros servidores Linux Oracle:

  Engine\Bin\OracleRMAN\PrivateKey



g. Abra o caminho do *diretório Engine\Bin* em cmd.exe.

h. Execute o seguinte comando para criptografar a chave privada usando o utilitário de linha de comando RMANCryptUtil.exe:

   RMANCryptUtil.exe "C:\Arquivos de programas\Arcserve\Unified Data Protection\Engine\BIN\<Nome da chave privada gerada>.ppk"

   O arquivo de chave privada criptografada é gerado com uma extensão de **.enc** no seguinte local:

   Engine\Bin\OracleRMAN\PrivateKey

   Um exemplo de nome de arquivo: PrivateKey.ppk.enc

   A chave privada criptografada (.enc), que é gerada usando RMANCryptutil, é salva na pasta Chave privada.

i. Copie a chave**.enc** para outros nós do RPS e consoles do UDP.

j. No nó do console do UDP, crie a pasta PrivateKey como a seguir, e copie a chave .enc na pasta PrivateKey:

   UDP\Engine\Bin\OracleRMAN\PrivateKey

k. Copie a chave pública da interface do usuário de PuTTYgen e consulte a etapa 2 para adicionar a chave pública ao nó do Oracle Linux, conforme apropriado.

2. No nó do Linux no qual o Oracle está instalado, execute as seguintes operações:

a. Verifique se a pasta *.ssh* está disponível no diretório raiz (~). Se o diretório *.ssh* não estiver disponível, crie o diretório usando o seguinte comando e as permissões padrão:

   mkdir ~.ssh

b. Verifique se o serviço *sshd* está em execução no servidor Linux usando o seguinte comando:

   service sshd status

   Observação: se o *sshd* não estiver instalado, instale o *sshd* com base no tipo do sistema operacional Linux.

c. Abra ou edite o arquivo *authorized_keys* usando o seguinte comando:

   vim authorized_keys

d. Crie ou modifique o arquivo *.ssh/authorized_keys*.

e. Adicione a chave pública gerada no servidor de RPS para o arquivo *.ssh/authorized_keys* usando o Gerador de chaves PuTTY.

f. Defina as permissões mínimas necessárias para o arquivo *.ssh/authorized_keys* usando o seguinte comando:

   chmod 400 .ssh/authorized_keys

Observações:

- Para adicionar uma chave pública em qualquer outro nó do Oracle Linux, desde que o RPS permaneça o mesmo, siga apenas a etapa 2 mencionada acima.
- Ao alterar o nó do RPS, siga as etapas 1 e 2 mencionadas acima.

Como criar um plano de backup para o banco de dados Oracle (Windows e Linux)

Para proteger os nós do Windows ou os nós agrupados, é necessário criar um plano. O plano consiste em uma tarefa de backup. Esta tarefa de backup permite especificar os nós que deseja proteger, o destino do backup e a programação de backup. O destino do backup é um servidor de ponto de recuperação onde você deseja armazenar os dados de backup. O destino também pode ser um destino local ou uma pasta compartilhada remota.

Esta seção contém os seguintes tópicos:

Criar um plano de backup com uma tarefa de backup

Um plano de backup inclui uma tarefa de backup que executa um backup de um nó e armazena os dados em um destino especificado. Cada tarefa consiste em parâmetros que definem a origem, o destino, a programação e outros detalhes de backup. Esta seção fornece informações sobre como criar um plano de backup para o banco de dados Oracle.

Siga estas etapas:

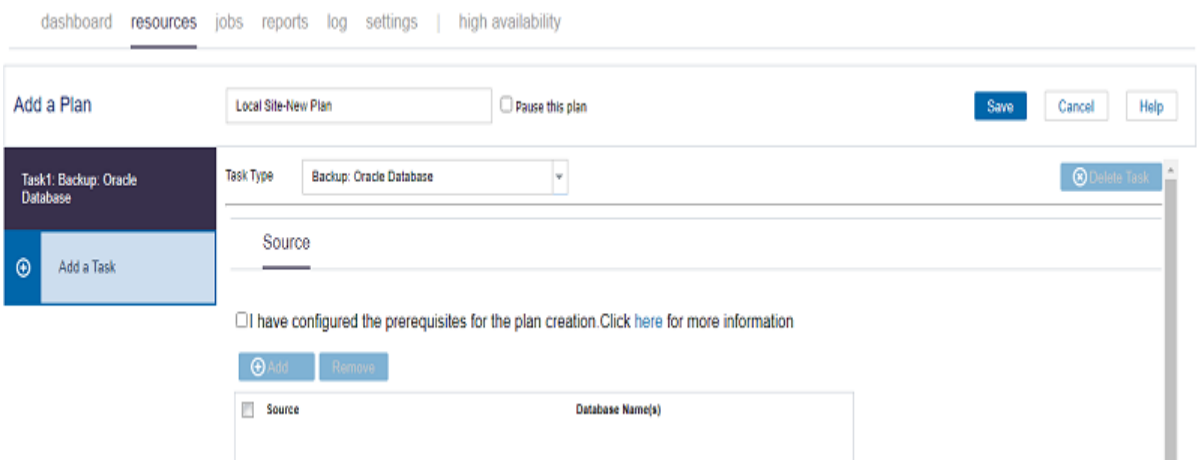
1. Efetue logon no Console do Arcserve UDP.
2. Navegue até **recursos** > **Plano** > **Todos os planos**.

   Se tiver criado os planos anteriores, esses planos serão exibidos no painel central.
3. No painel central, clique em **Adicionar um plano**.

   A opção Adicionar um plano é aberta.
4. Digite o nome do plano.
5. (Opcional) Selecione a caixa de seleção **Pausar este plano**.

   O plano não será executado até que você desmarque a caixa de seleção para retomar o plano.

   Observação: se um plano for pausado, nenhuma tarefa em andamento será pausada, mas todas as tarefas programadas correspondentes associadas a esse plano serão pausadas. No entanto, você pode executar uma tarefa manualmente. Por exemplo, você pode executar manualmente a tarefa de backup e a tarefa de replicação para um nó mesmo que o respectivo plano esteja pausado. Nesse caso, a tarefa seguinte da tarefa sob demanda (manual) não será executada. Por exemplo, há uma tarefa de replicação após uma tarefa de backup sob demanda, a tarefa de replicação não será executada para a tarefa de backup sob demanda. É necessário executar manualmente a tarefa de replicação. Quando você retomar o plano, as tarefas pendentes não são retomadas imediatamente. Depois de retomar o plano, as tarefas pendentes serão executadas no próximo horário programado.
6. Na lista suspensa Tipo de tarefa, selecione **Backup: banco de dados Oracle**.



Agora, especifique os detalhes de Origem, Destino, Programação e Avançado.

Observações:

- Para verificar se os blocos físicos e lógicos estão corrompidos nos arquivos de dados existentes no computador de origem do Oracle, é usado o comando Backup Validate RMAN.
- Para adicionar validação à tarefa de backup, use a seguinte chave do Registro:

  \HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\SourceDBValidation

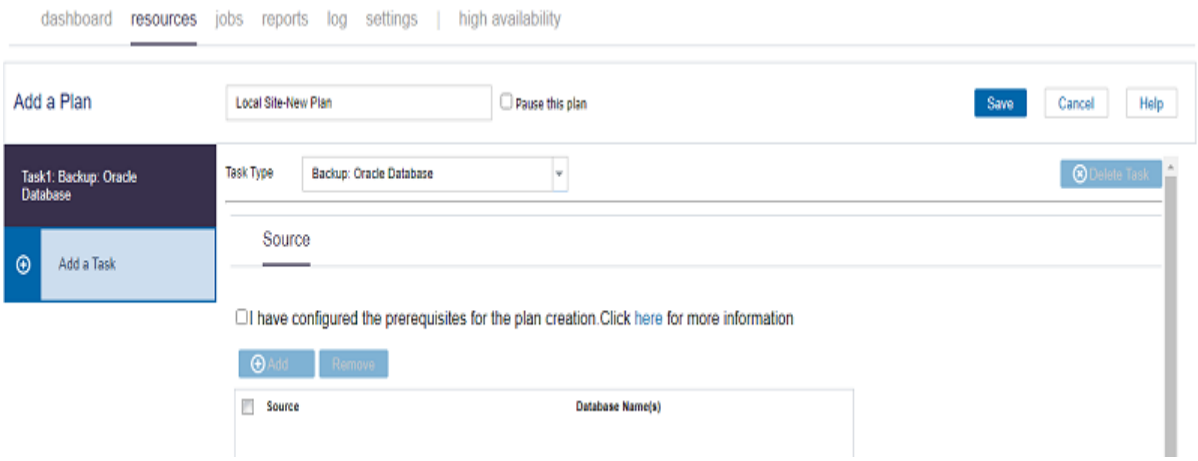
  - Se a chave não for adicionada (padrão) - a validação de backup não está ativada
  - Se a chave for adicionada como 1 - a validação de backup está ativada
  - Se a chave for adicionada com qualquer outro valor - a validação de backup não está ativada
- A validação de backup é uma tarefa demorada. Ativar essa configuração aumenta o tempo de backup, dependendo do tamanho dos arquivos de dados. A validação é executada em todo o arquivo de dados de origem, mesmo para um backup incremental.

Especificar a origem

A página Origem permite especificar os nós de origem que deseja proteger. É possível selecionar mais de um nó em um plano. Caso não tenha adicionado nós para o console, você pode adicionar nós ao criar ou modificar um plano da página de origem. Também é possível salvar um plano sem adicionar nenhum nó de origem. O plano é implantado somente após você adicionar nós de origem.

Siga estas etapas:

1. Na guia Origem, para confirmar as configurações de pré-requisitos, marque a caixa de seleção **Os pré-requisitos para criar este plano foram configurados**. Para obter mais informações, consulte Revisar os pré-requisitos do banco de dados Oracle para RMAN (Windows e Linux).



2. Clique em **+Adicionar**.
3. Selecione uma das seguintes opções:

Selecionar as origens a serem protegidas no Arcserve UDP

A caixa de diálogo Selecionar Nós para proteger é aberta. Selecione os nós na lista exibida. Selecione esta opção se você já tiver adicionado os nós para o console.

Adicionar nó do Windows

A caixa de diálogo Adicionar nó do Oracle no Windows é aberta. Selecione esta opção se você não tiver adicionado os nós e desejar adicionar manualmente os nós para proteger.

Adicionar nó do Linux

A caixa de diálogo Adicionar nó do Oracle no Linux é aberta. Selecione esta opção se você não tiver adicionado os nós e desejar adicionar manualmente os nós para proteger.

4. Se você selecionar a opção **Selecionar origens para proteger no Arcserve UDP**, na caixa de diálogo Selecionar nós para proteger, faça o seguinte:

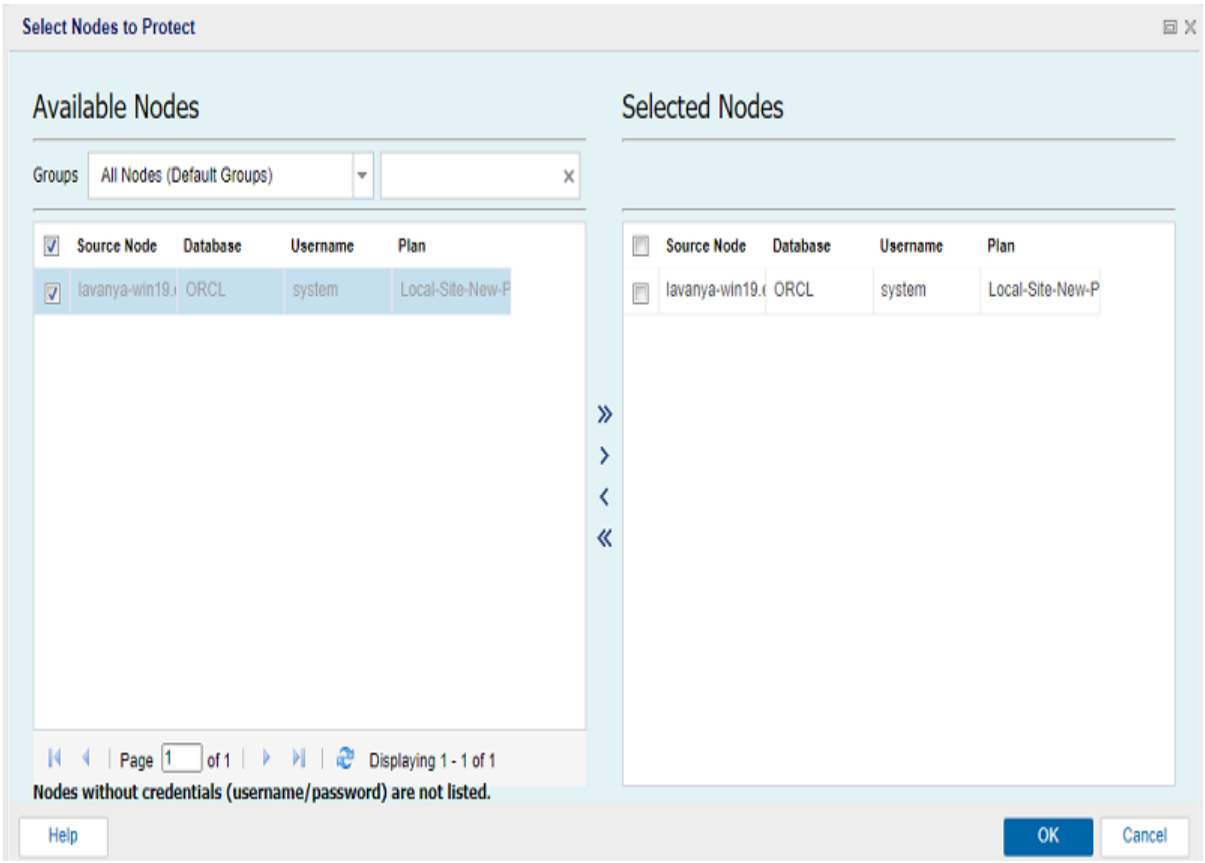
   a. (Opcional) Selecione um filtro na lista suspensa Grupos para filtrar os nós. É possível digitar as palavras-chave para filtrar melhor seus nós.

      Os nós são exibidos na coluna Nós disponíveis.

   b. Selecione os nós na coluna Nós disponíveis e, em seguida, clique na seta simples à direita (>) ou na seta dupla à direita (>>) para mover os nós selecionados ou todos os nós, respectivamente, para a coluna Nós selecionados.

      Os nós são exibidos na coluna Nós selecionados.

   c. Clique em **OK** para fechar a caixa de diálogo.



5. Se você selecionar a opção **Adicionar nó do Windows**, na caixa de diálogo Adicionar nó do Oracle no Windows, faça o seguinte:

   a. Digite o nome ou o endereço IP do nó do Oracle que deseja adicionar.

   b. Digite uma descrição para o nó.

c. Digite as credenciais do administrador.

d. Clique em **Adicionar**.

   Aguarde até que a validação do nome de usuário e da senha seja concluída.

   O nó é adicionado no painel central.

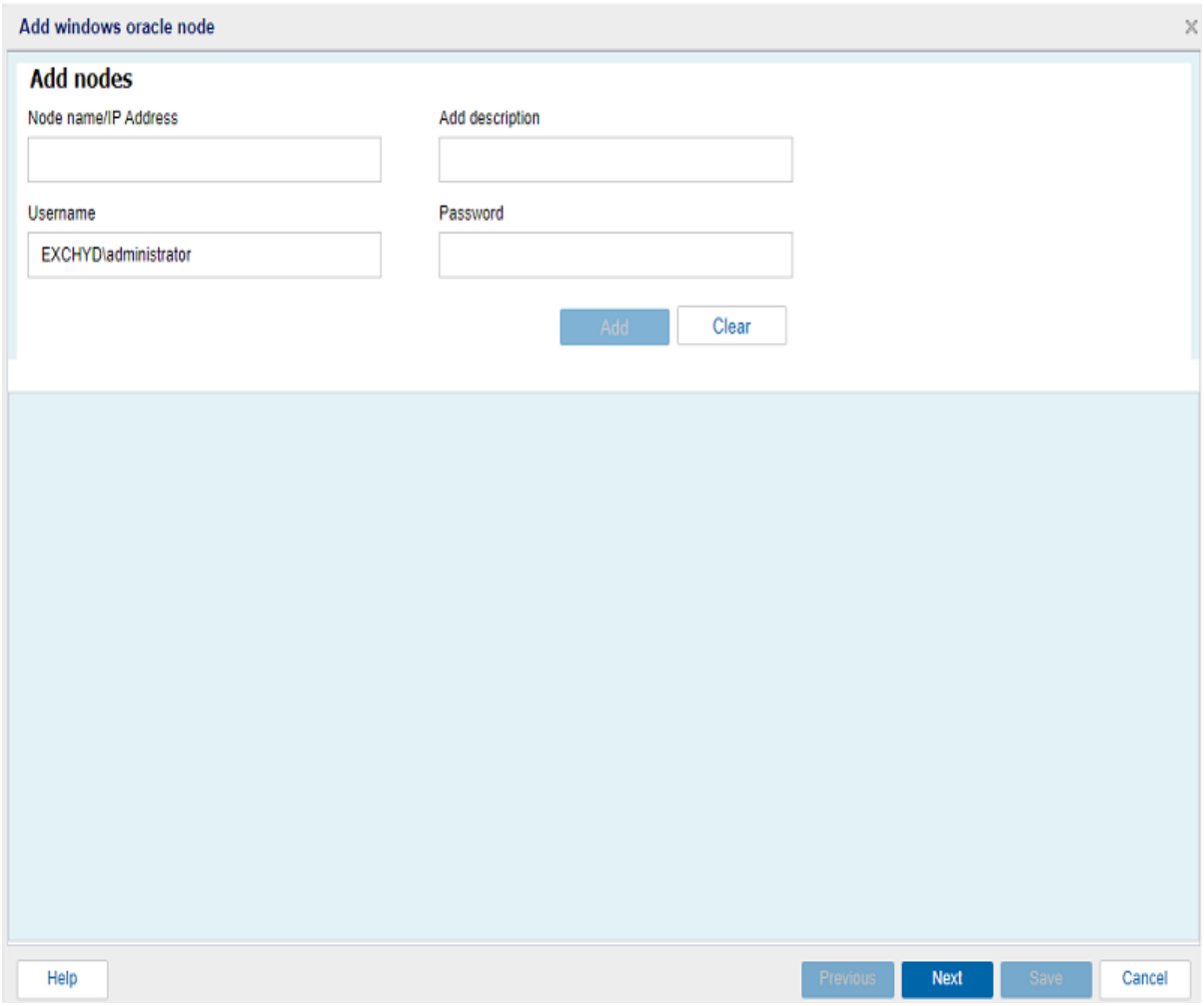
e. Para adicionar vários nós, siga as etapas novamente. Todos os nós adicionados são listados no painel central.

f. Clique no símbolo de expansão ao lado do endereço IP e, em seguida, verifique os detalhes adicionados.

   Observações:

   - Para editar os nós adicionados na lista, selecione o nó que deseja editar e, em seguida, clique em **Editar**.
   - Para remover os nós adicionados da lista, selecione os nós que deseja remover e clique em **Remover**.
   - Para remover todos os nós adicionados, clique em **Remover todos**.

g. Clique em **Avançar**.



6. Se você selecionar a opção **Adicionar nó do Linux**, na caixa de diálogo Adicionar nó do Oracle no Linux, faça o seguinte:
   a. Digite o nome ou o endereço IP do nó do Oracle que deseja adicionar.
   b. Digite uma descrição para o nó.
   c. Digite o nome do usuário do .
   d. Para o proprietário do Oracle, digite o nome de usuário, que é usado para a instalação do Oracle.
   e. Em Porta SSH, especifique o valor da porta. O valor padrão da porta é 22.
   f. Clique em **Adicionar**.

      Aguarde até que a validação do nome de usuário e senha seja concluída.

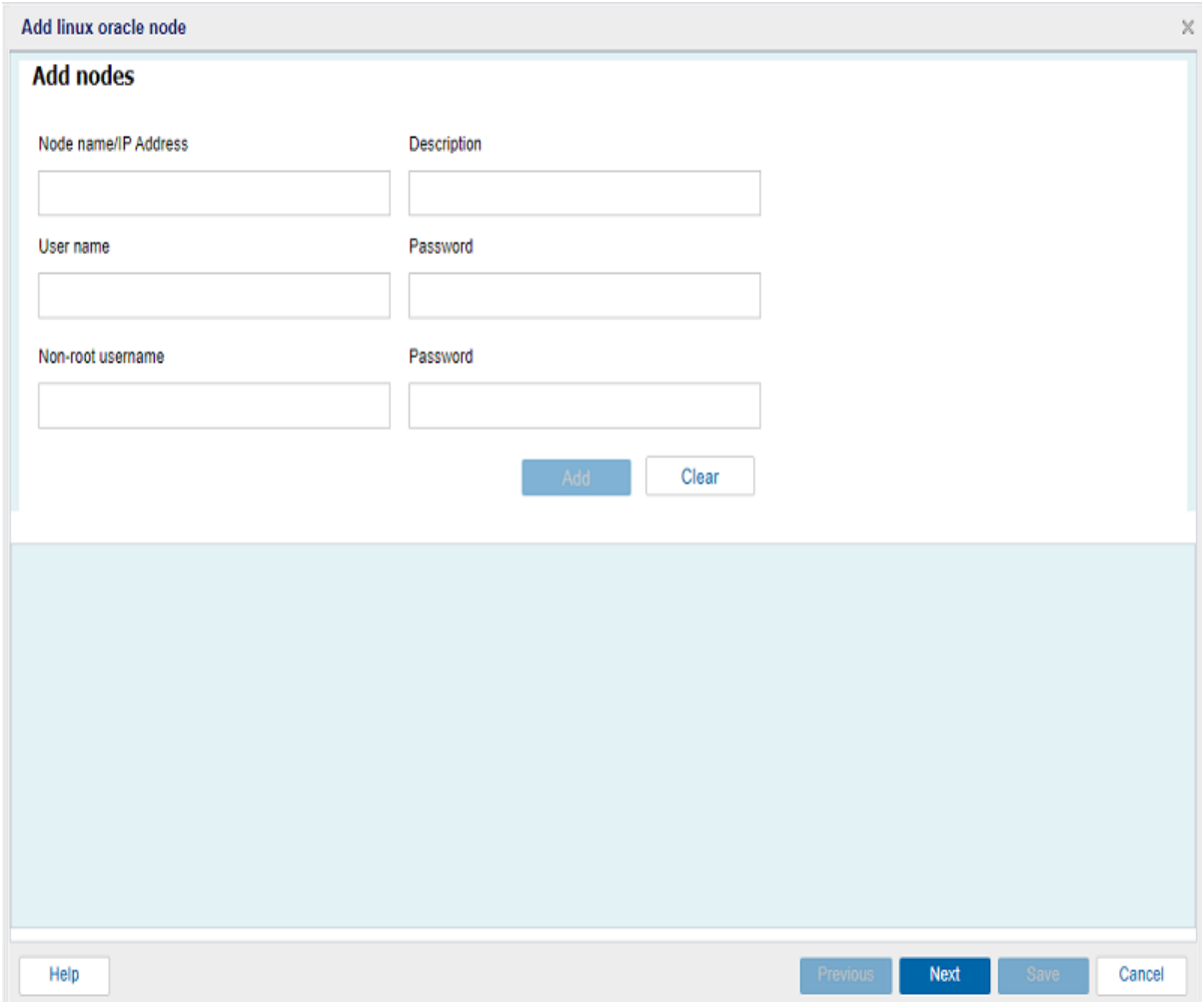
      O nó é adicionado no painel central.
   g. Para adicionar vários nós, siga as etapas novamente. Todos os nós adicionados são listados no painel central.

h. Clique no símbolo de expansão ao lado do endereço IP e, em seguida, verifique os detalhes adicionados.

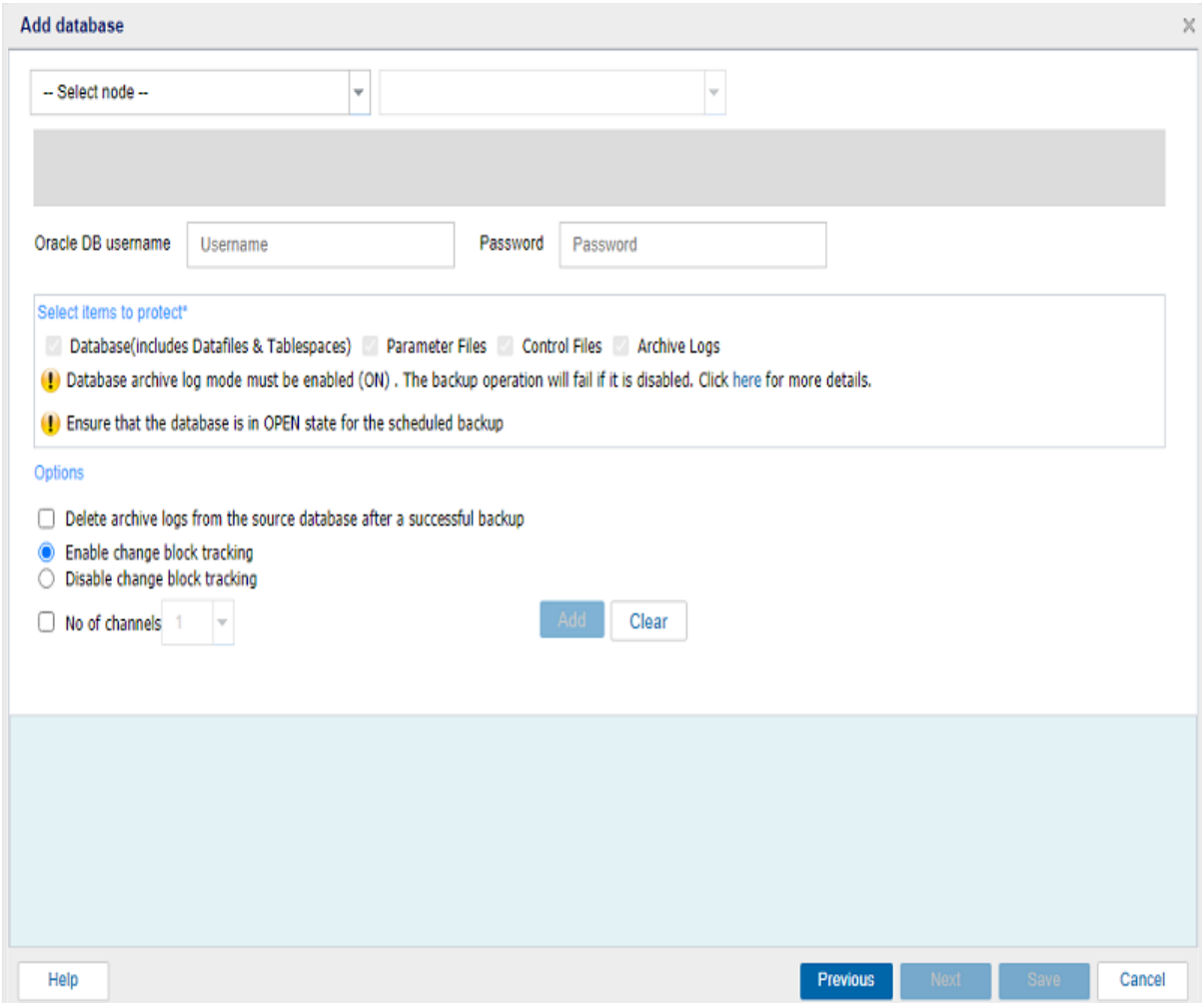
Observações:

- Para editar os nós adicionados na lista, selecione o nó que deseja editar e, em seguida, clique em **Editar**.
- Para remover os nós adicionados da lista, selecione os nós que deseja remover e clique em **Remover**.
- Para remover todos os nós adicionados, clique em **Remover todos**.

i. Clique em **Avançar**.



7. Na caixa de diálogo Adicionar banco de dados, execute o seguinte:



a. Selecione o nó na lista suspensa.

   Aguarde até que a lista de bancos de dados disponíveis no host selecionado seja exibida e a lista suspensa seja ativada.

b. Na lista suspensa, selecione uma das seguintes opções:

   Adicionar novo banco de dados

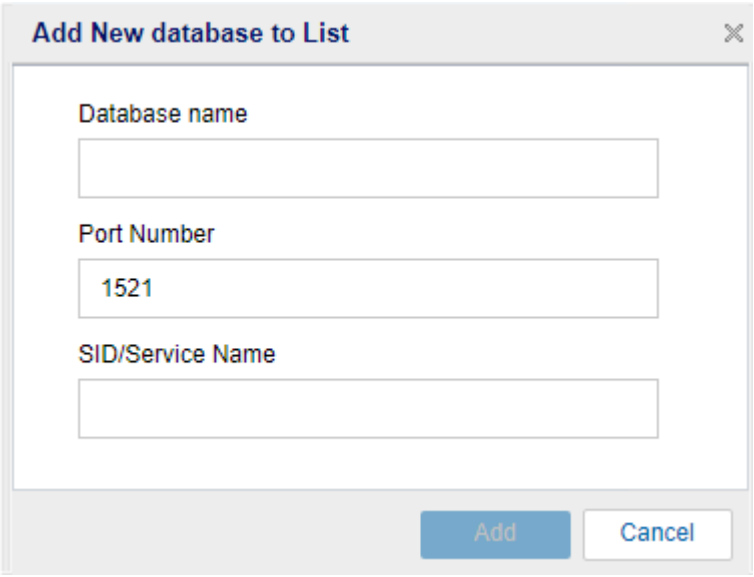
   Para adicionar um novo banco de dados, siga estas etapas:

   1. Selecione a opção **Adicionar novo banco de dados**.
   2. Na caixa de diálogo Adicionar novo banco de dados à lista, faça o seguinte e clique em **Adicionar**:

      - **Nome do banco de dados/SID:** digite o nome do banco de dados ou o nome da SID.
      - **Número da porta**: digite o número da porta. O valor padrão da

porta é 1521.

- **Nome do serviço:** digite o nome do serviço.



O novo banco de dados é adicionado à lista suspensa.

Selecione o banco de dados existente

Selecione o banco de dados na lista suspensa, conforme necessário. Depois que o banco de dados é selecionado, ele é movido para fora da lista e aparece no painel central.

Observações:

- Para evitar várias entradas em cada banco de dados, agrupe os bancos de dados configurados com o mesmo nome de usuário e senha.
- Para adicionar diferentes tipos de arquivos aos bancos de dados com credenciais diferentes, selecione os bancos de dados individuais e, em seguida, adicione-os.
- Para remover o banco de dados do grupo (no painel central), faça o seguinte:

  a. Clique no nome do banco de dados.

     Uma mensagem de confirmação é exibida.

  b. Clique em **Sim** para confirmar.

  O banco de dados é removido com êxito e é adicionado novamente à lista suspensa.

c. Digite as credenciais do usuário do sistema para o banco de dados Oracle.

Observações:

- Todos os itens a serem protegidos, como banco de dados (inclui arquivos de dados e espaços para tabelas), arquivos de controle, arquivos de parâmetros e logs de arquivamento, são ativados por padrão.
- Certifique-se de ativar o banco de dados ARCHIVELOG antes que a operação de backup seja disparada. Para verificar se o modo de log ARCHIVELOG está ativado, consulte Revisar os pré-requisitos do banco de dados Oracle. Se o ARCHIVELOG não estiver ativado, a tarefa de backup falhará.

d. Para Opções, especifique o seguinte:

Excluir os logs de arquivo do banco de dados de origem após um backup bem-sucedido

Permite excluir os logs de arquivo do banco de dados de origem após um backup bem-sucedido.

Nº de canais

Permite selecionar o número de canais ou segmentos que deseja criar para a tarefa de backup.

Observação: o número máximo de canais suportados é 10.

Ativar rastreamento do bloco alterado

Permite ativar o recurso de rastreamento do bloco alterado. Use essa opção para aprimorar o desempenho do RMAN. Ele ajuda o utilitário RMAN ou o binário a localizar os dados diferenciais mais rapidamente e a executar a tarefa de backup.

Desativar o rastreamento do bloco alterado

Permite desativar o recurso de rastreamento do bloco alterado.

Observação: o Oracle oferece suporte ao recurso Desativar controle de bloco de alterações apenas para a Enterprise Edition (EE).

e. Clique em **Adicionar**.

Todos os bancos de dados adicionados são listados.

Observação: depois de clicar no botão Adicionar, todas as credenciais do banco de dados e os parâmetros do firewall são verificados.

f. Para adicionar vários bancos de dados, siga as etapas novamente. Todos os bancos de dados adicionados são listados.

g. Clique no símbolo de expansão ao lado do endereço IP e, em seguida, verifique os detalhes adicionados.

Observações:

- Para editar os bancos de dados adicionados na lista, selecione o banco de dados que deseja editar e, em seguida, clique em **Editar**.
- Para remover os bancos de dados adicionados da lista, selecione os bancos de dados que deseja remover e clique em **Remover**.

8. Clique em **Salvar**.

   Observações:

   - Você pode adicionar vários nós e vários bancos de dados.
   - Para remover a origem, marque a caixa de seleção ao lado da origem adicionada e clique em **Remover**.

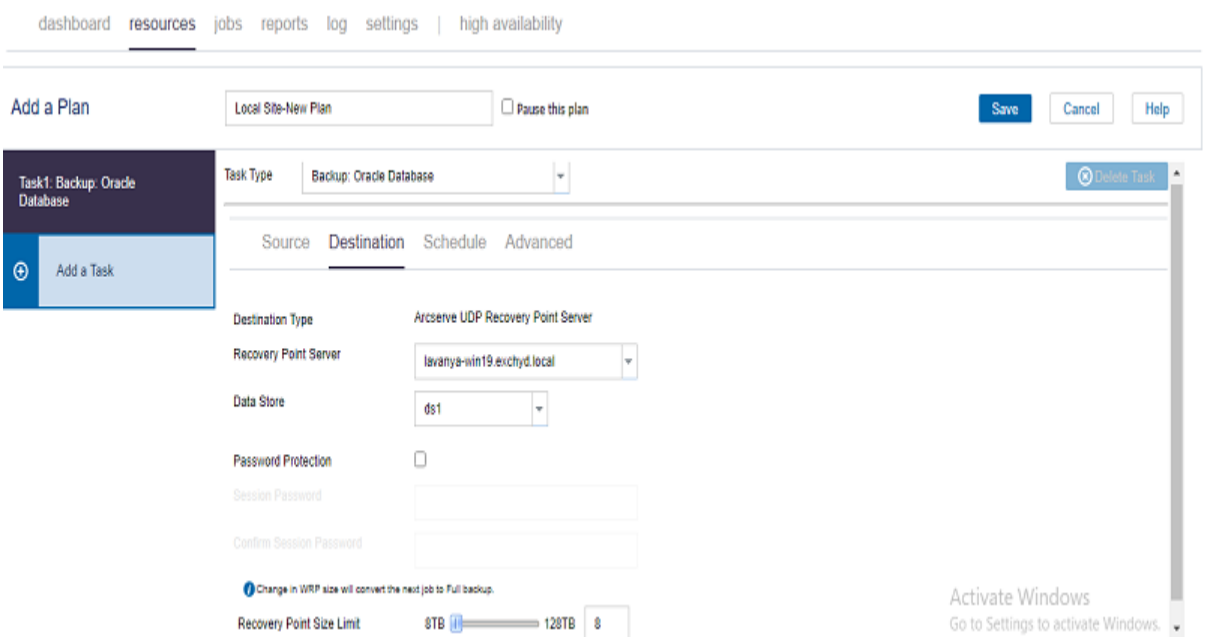
   A origem é especificada.

Especificar o destino

O destino é o local onde você armazena os dados de backup. É necessário, no mínimo, especificar o destino para salvar o plano.

Siga estas etapas:

1. Clique na guia **Destino**.



2. Faça o seguinte:
   - **Servidor de ponto de recuperação:** na lista suspensa, selecione o RPS (Recovery Point Server - Servidor de ponto de recuperação) de destino.
   - **Repositório de dados:** na lista suspensa, selecione o repositório de dados de destino.
   - **Proteção por senha:** marque a caixa de seleção **Proteção por senha**, forneça a senha da sessão e, em seguida, digite a senha da sessão novamente para confirmar.

     Observação: a senha da sessão é opcional quando o destino de backup é um repositório de dados do RPS não criptografado.
   - **Limite de tamanho do ponto de recuperação:** especifica o tamanho do servidor de ponto de recuperação para backup. Defina o tamanho do servidor de ponto de recuperação na escala.

     Intervalo: 8 TB a 128 TB

   O destino é especificado.

Especificar a programação

A página Programar permite definir uma programação para o backup e para que as funções Mesclar e Acelerar sejam repetidas em intervalos específicos. Após definir uma programação, as tarefas são executadas automaticamente de acordo com a programação. É possível adicionar várias programações e fornecer configurações de retenção.

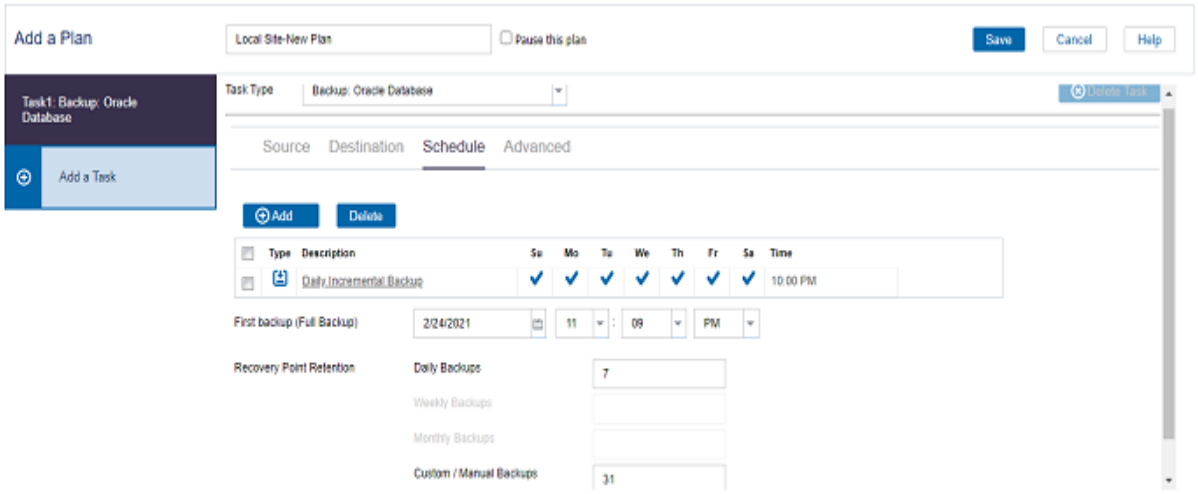
Uma Programação de backup se refere a programação regular que é repetida várias vezes ao dia, com base no número de horas ou de minutos selecionado. Além da programação regular, uma programação de backup também fornece opções para adicionar programações diária, semanal e mensal.

Se o servidor RPS for o destino do backup, o valor padrão será um backup incremental diário de todos os tipos de arquivos sempre às 22h.

É possível editar ou excluir uma programação de tarefas de backup.

Siga estas etapas:

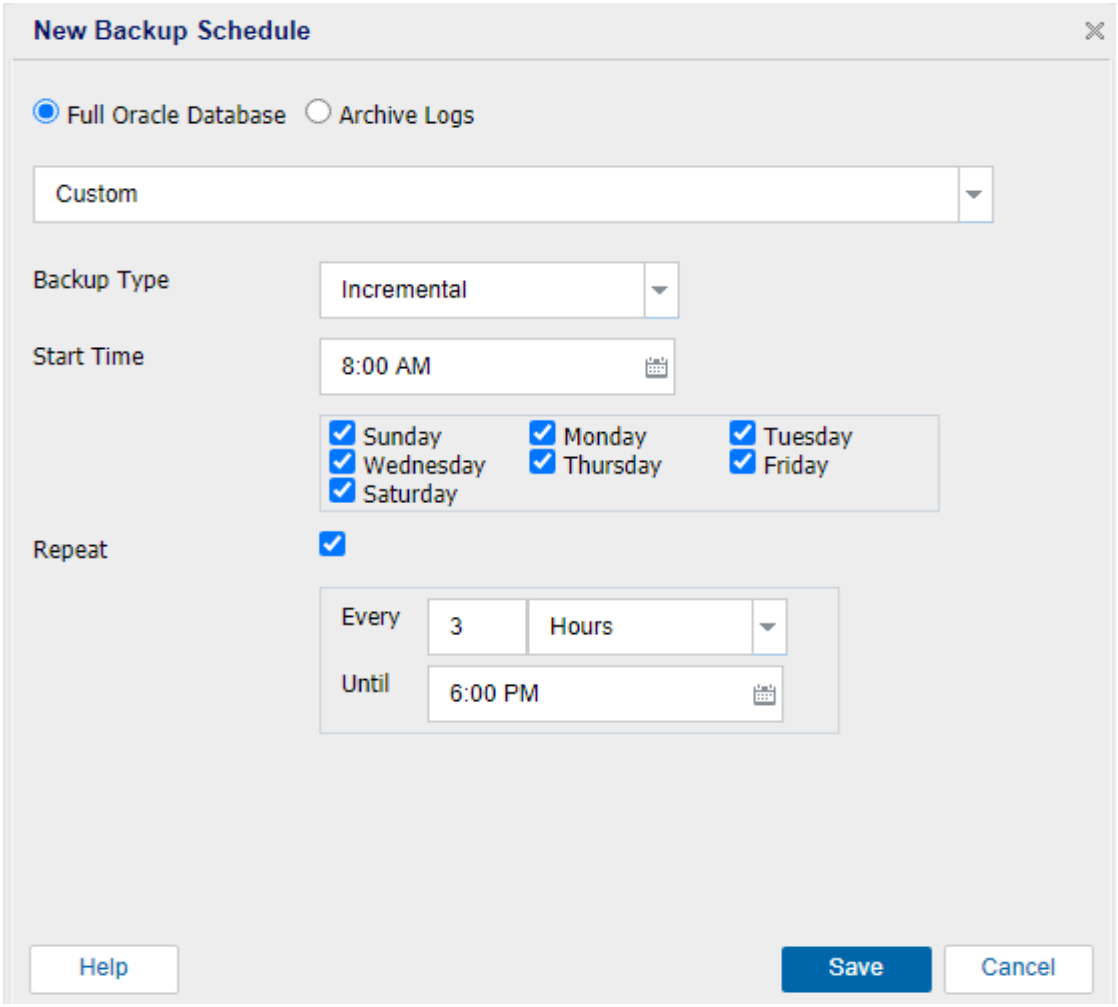
1. Clique na guia **Programar** e, em seguida, adicione programações de backup, mesclagem e de aceleração de leitura de disco.



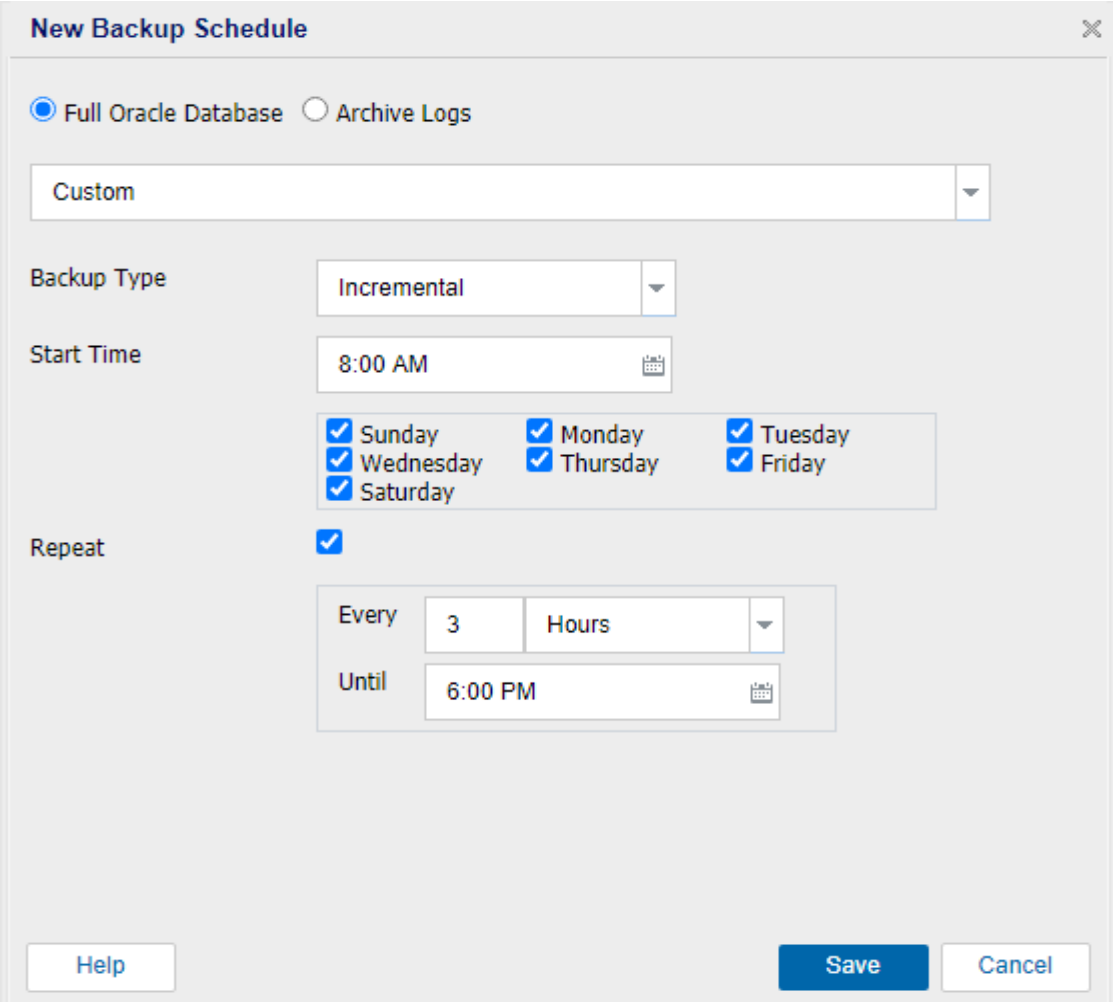
2. Para adicionar uma programação de backup, execute as seguintes etapas:
   a. Clique em **Adicionar** e selecione a opção **Adicionar programação de backup**.

      A caixa de diálogo Nova programação de backup é aberta.

   b. Na caixa de diálogo Nova programação de backup, selecione uma das seguintes opções:



Banco de dados Oracle completo



Faça o seguinte:

a. Na lista suspensa, selecione uma das seguintes opções:

Personalizado

Especifica a programação de backup que se repete várias vezes por dia.

Diário

Especifica a programação de backup que ocorre uma vez por dia. Por padrão, todos os dias da semana estão selecionados para o backup diário. Se não desejar executar a tarefa de backup em um dia específico, desmarque a caixa de seleção correspondente àquele dia da semana.

Semanal

Especifica a programação de backup que ocorre uma vez por semana.

Mensal

Especifica a programação de backup que ocorre uma vez por mês.

Horário

Especifica a programação de backup que ocorre uma vez por hora.

Minuto

Especifica a programação de backup que ocorre em um tempo mínimo de 15 minutos.

b. Na lista suspensa Tipo de backup, selecione o tipo de backup.

Completo

Determina a programação de backup para backups completos (todos os tipos de arquivos). Conforme programado, o Arcserve UDP executa um backup completo de todos os tipos de arquivos do computador de origem. Um backup completo em geral, consome tempo, dependendo do tamanho do backup.

Incremental

Especifica a programação de backups para backups incrementais.

Conforme programado, o Arcserve UDP faz backup incremental de todos os tipos de arquivo desde o último backup bem-sucedido. As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a executar um backup.

Observação: sempre é feito o backup completo do arquivo de controle para qualquer tipo de backup.

c. Especifique a hora de início do backup.

d. (Opcional) Marque a caixa de seleção de **Repetição** e especifique a programação a ser repetida.

Observação: certifique-se de que o tempo para repetir a programação não seja inferior a 15 minutos.

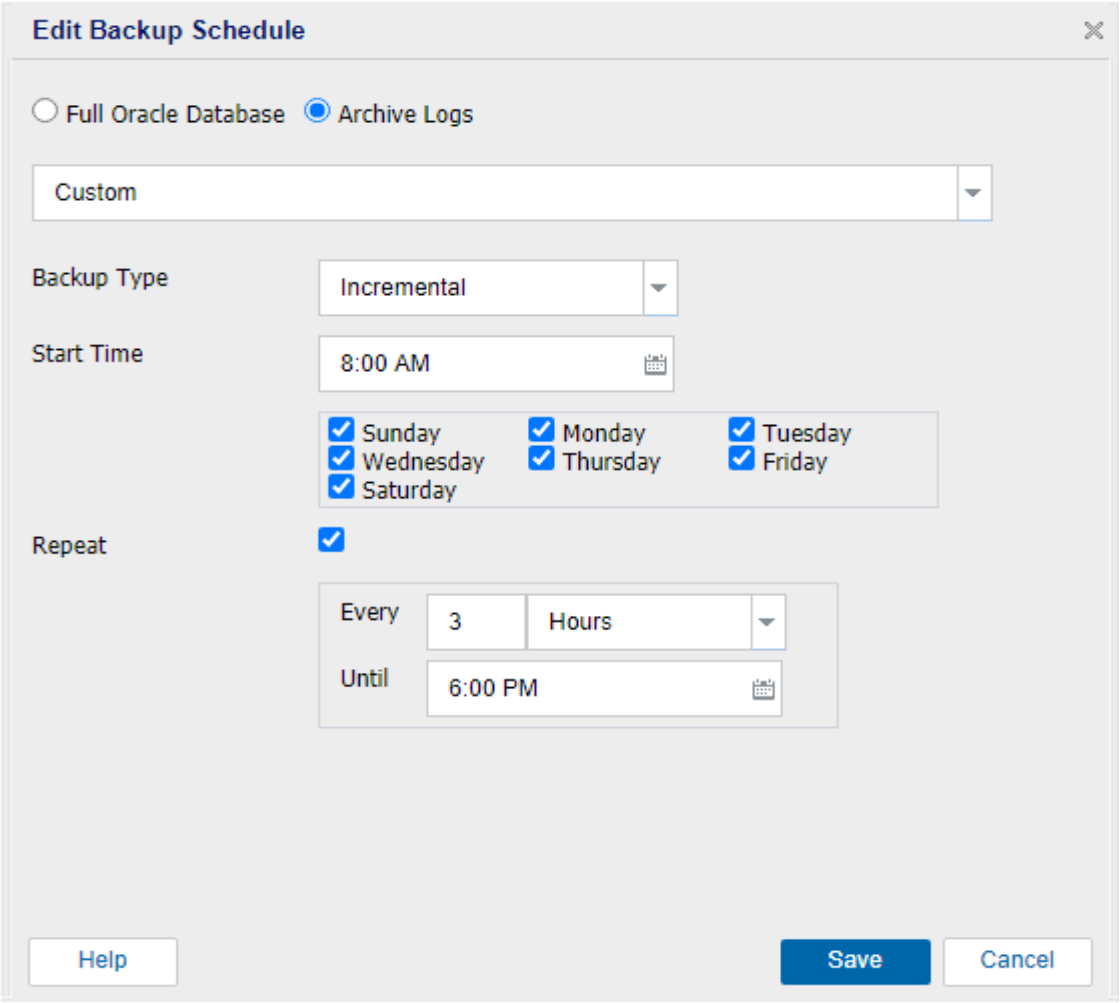
e. Se você selecionou a opção **Por hora** na lista suspensa, faça o seguinte:

1. Selecione o tipo de backup na lista suspensa Tipo de backup.
2. Especifique a hora de início do backup.
3. Especifique a hora de término do backup.
4. Selecione a data/hora de repetição do backup na lista suspensa.

   Observação: se desejar personalizar o tempo de repetição do backup, selecione Personalizado na lista suspensa e insira o tempo em horas.

f. Clique em **Salvar**.

Logs de arquivo



Faça o seguinte:

a. Na lista suspensa, selecione uma das seguintes opções:

Personalizado

Especifica a programação de backup que se repete várias vezes por dia.

Diário

Especifica a programação de backup que ocorre uma vez por dia. Por padrão, todos os dias da semana estão selecionados para o backup diário. Se não desejar executar a tarefa de backup em um dia específico, desmarque a caixa de seleção correspondente àquele dia da semana.

Semanal

Especifica a programação de backup que ocorre uma vez por semana.

Mensal

Especifica a programação de backup que ocorre uma vez por mês.

Horário

Especifica a programação de backup que ocorre uma vez por hora.

Minuto

Especifica a programação de backup que ocorre em um tempo mínimo de 15 minutos.

b. Na lista suspensa Tipo de backup, selecione o tipo de backup.

Completo

Determina a programação de backup para backups completos do log de arquivamento. Conforme programado, o Arcserve UDP executa um backup completo de todos os logs de arquivamento do computador de origem. Um backup completo em geral, consome tempo, dependendo do tamanho do backup.

Incremental

Determina a programação de backup para backups incrementais do log de arquivamento.

Conforme programado, o Arcserve UDP faz backup incremental apenas dos logs de arquivamento que foram alterados desde o último backup realizado com êxito. As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a executar um backup.

c. Especifique a hora de início do backup.

d. (Opcional) Marque a caixa de seleção de **Repetição** e especifique a programação a ser repetida.

Observação: certifique-se de que o tempo para repetir a programação não seja inferior a 15 minutos.

e. Se você selecionou a opção **Por hora** na lista suspensa, faça o seguinte:

1. Selecione o tipo de backup na lista suspensa Tipo de backup.
2. Especifique a hora de início do backup.
3. Especifique a hora de término do backup.
4. Selecione a data/hora de repetição do backup na lista suspensa.

   Observação: se desejar personalizar o tempo de repetição do backup, selecione **Personalizado** na lista suspensa e insira o tempo em horas.

f. Clique em **Salvar**.

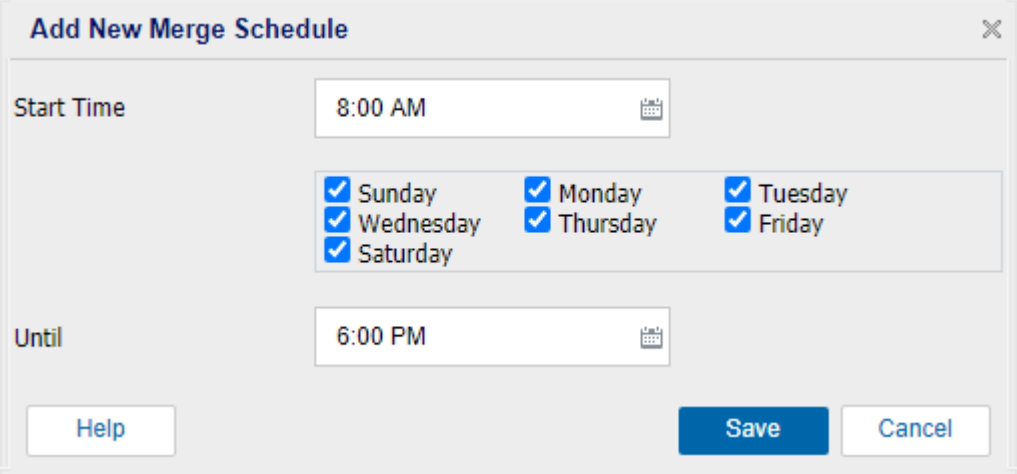
A programação de backup é especificada e aparece na página Programar.

3. Para adicionar uma programação de mesclagem, faça o seguinte:
    a. Clique em **Adicionar** e selecione a opção **Adicionar programação de mesclagem**.

       A caixa de diálogo Adicionar nova programação de mesclagem é aberta.

    b. Na caixa de diálogo Adicionar nova programação de mesclagem, faça o seguinte:

        - **Hora de início:** especifique a hora de início para iniciar a tarefa de mesclagem.
        - **Até:** especifique a hora de término para a tarefa de mesclagem.



    c. Clique em **Salvar**.

   A programação de mesclagem é especificada e aparece na página Programar.

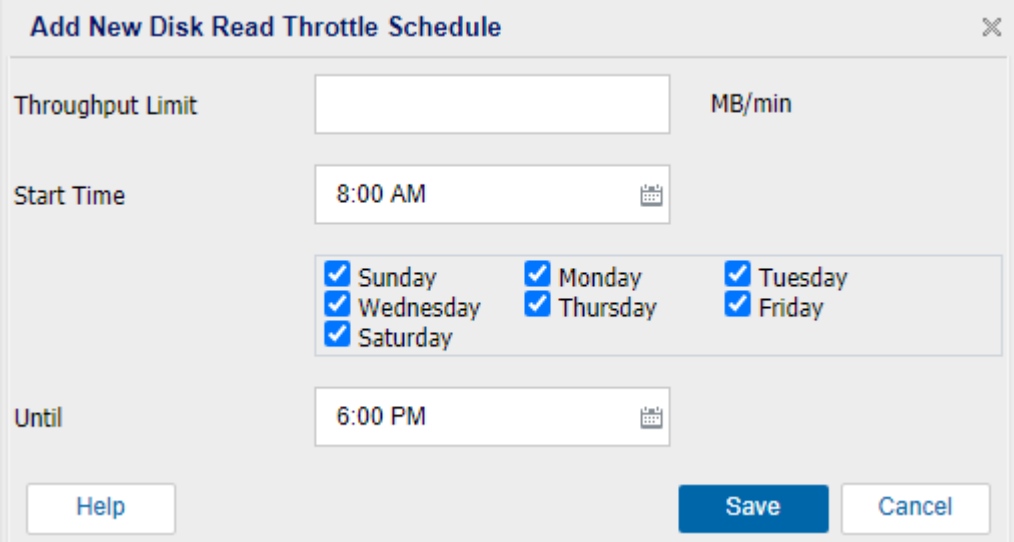
4. Para adicionar uma programação de aceleração de leitura de disco, faça o seguinte:
    a. Clique em **Adicionar** e selecione a opção **Adicionar programação de aceleração de leitura de disco**.

       A caixa de diálogo Adicionar nova programação de acelerador de leitura de disco é aberta.

    b. Na caixa de diálogo Adicionar nova programação de aceleração de leitura de disco, faça o seguinte:

        - **Taxa de transferência:** especifique o limite da taxa de transferência em MB por minuto.
        - **Hora de início:** especifique a hora de início para iniciar a tarefa de taxa de transferência de backup.

- **Até:** especifique a hora de término da tarefa de taxa de transferência de backup.



c. Clique em **Salvar**.

A Programação de acelerador de leitura de disco é especificada e aparece na página Programação.

5. Especifique a hora de início do backup programado.

Observação: a captura de tela acima não é válida para backups RMAN.

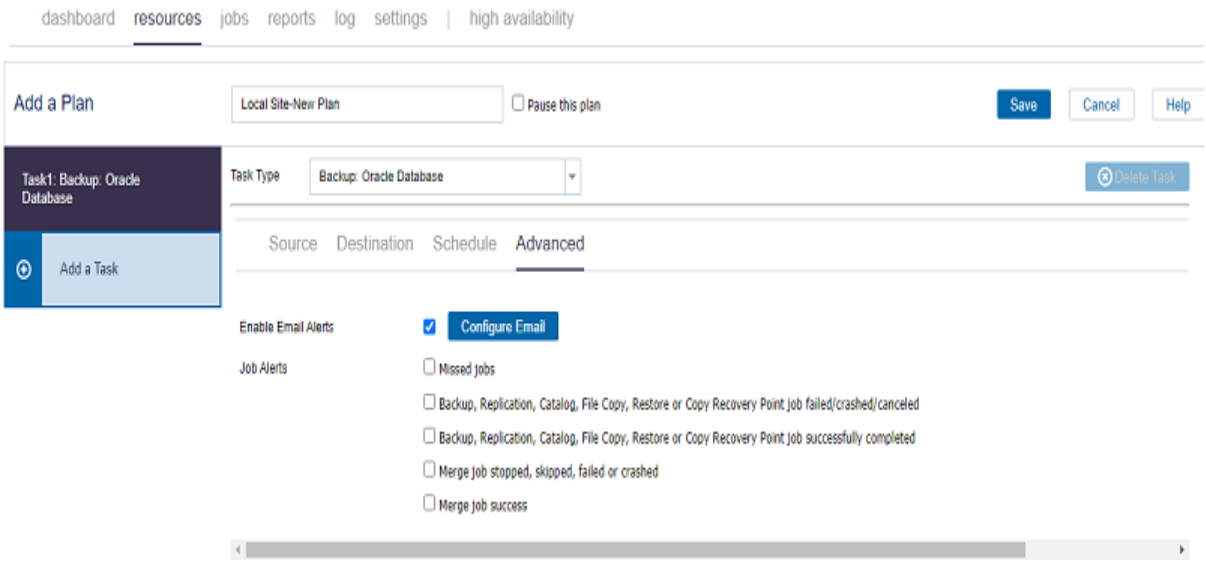
6. Especifique as configurações de retenção de pontos de recuperação para programação diária, semanal e mensal.

   Essas opções serão ativadas se tiver adicionado a programação de backup correspondente. Se você modificar as configurações de retenção desta página, as alterações serão refletidas na caixa de diálogo Programação de backup.

A programação é especificada.

Especificar as configurações avançadas

A guia Avançado permite especificar algumas configurações avançadas para a tarefa de backup.



Siga estas etapas:

1. Especifique os seguintes detalhes:

   Ativar alertas por email

   Permite ativar alertas por email. É possível especificar configurações de email e os tipos de alertas que você deseja receber por email. Ao selecionar esta opção, as seguintes opções serão ativadas para a seleção.

   Configurar email

   Permite configurar as definições de email.

   Para configurar o servidor de email e os detalhes do servidor proxy, clique em **Configurar email**.

   Alertas de tarefa

   Permite especificar os tipos de emails de tarefas que você deseja receber.

2. Clique em **Salvar**.

As configurações avançadas são especificadas.

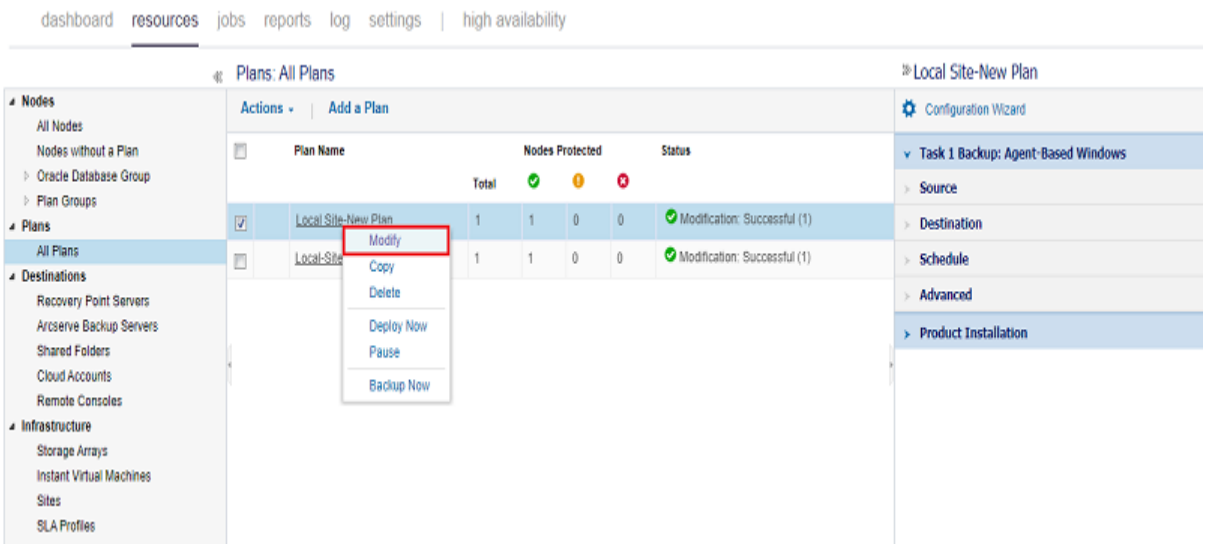
Adicionar ao plano uma tarefa de recuperação garantida

Uma tarefa de recuperação garantida inclui uma tarefa de recuperação garantida para um existente plano de backup/replicação. Cada tarefa consiste em parâmetros que definem a origem, as configurações de teste, a programação e as configurações avançadas. Crie uma tarefa de recuperação garantida com base na tarefa de backup/replicação para verificar a acessibilidade e a recuperação garantida dos dados e fornecer a verificação de integridade de dados.

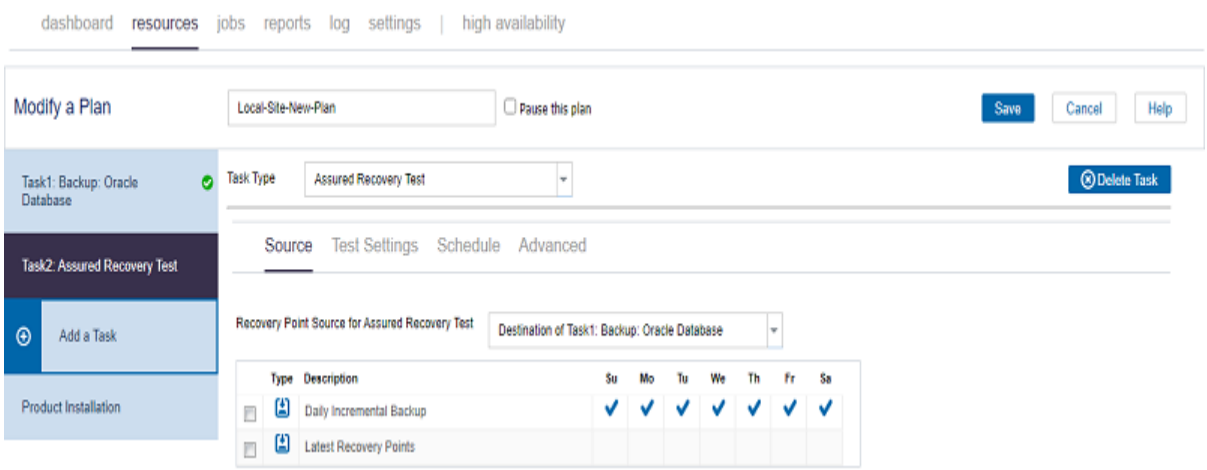
Siga estas etapas:

1. Clique na guia **Recursos** no Console.
2. No painel esquerdo, navegue para **Planos** e clique em **Todos os planos**.

   Se tiver criado os planos anteriores, esses planos serão exibidos no painel central.
3. No painel central, clique com o botão direito do mouse no plano de backup existente e, em seguida, clique em **Modificar**.



4. Na página Modificar um plano, clique em **Adicionar uma tarefa** no painel esquerdo.



5. (Opcional) Selecione a caixa de seleção **Pausar este plano**.

   O plano não será executado até que você desmarque a caixa de seleção para retomar o plano.

   Observação: se você pausar o plano, a tarefa Recuperação garantida não iniciará. Ao retomar o plano novamente, a tarefa Recuperação garantida não é retomada automaticamente. É necessário executar manualmente outra tarefa de backup para iniciar a tarefa Recuperação garantida.

6. Na lista suspensa Tipo de tarefa, selecione a opção **Teste de recuperação garantida**.

7. Agora especifique os detalhes de Origem, Configurações de teste, Programação e Avançado.

8. Clique em **Salvar**

   As alterações são salvas e a tarefa de recuperação garantida é automaticamente implantada.

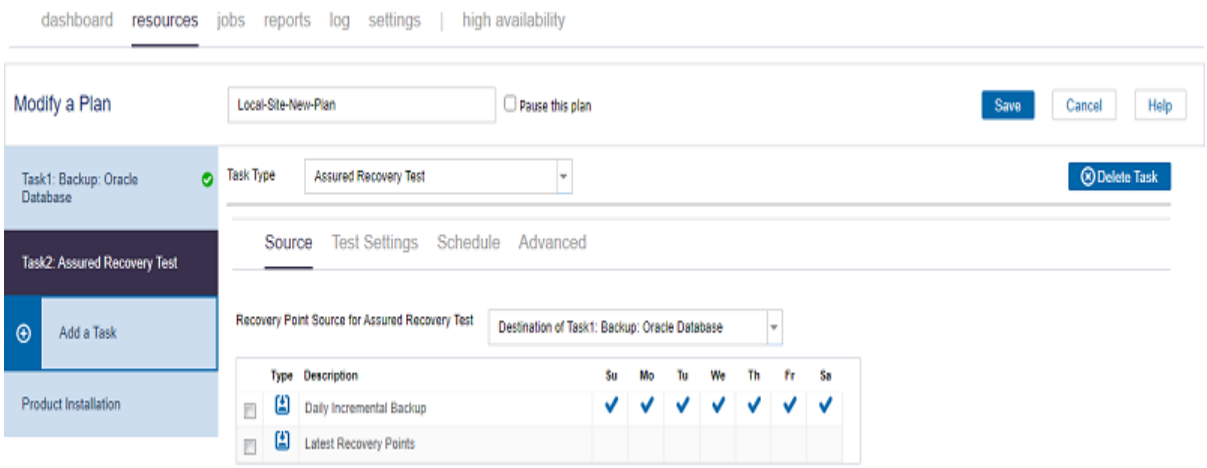
   Observação: para verificar a integridade dos dados de backup do Oracle, como arquivos de controle, arquivos de dados, logs de arquivamento e arquivo SP, a tarefa de recuperação garantida executa o comando Restaurar e validar RMAN no servidor do ponto de recuperação.

Especificar a origem

A guia Origem permite especificar o ponto de recuperação de origem que você deseja proteger.

Siga estas etapas:

1. Na guia Origem, na lista suspensa Origem do ponto de recuperação para o teste de recuperação garantida, selecione a opção desejada.



2. Selecione os tipos de pontos de recuperação para o teste de recuperação garantida. É possível selecionar qualquer uma das duas opções a seguir:

   - Teste de recuperação garantida a partir dos tipos de backup selecionados

     Você pode selecionar Backups diários, Backups semanais ou Backups mensais. As opções de backup diário, semanal ou mensal são ativadas de acordo com a programação do backup de origem. Por exemplo, se o backup de origem tiver somente o backup mensal programado, o teste de recuperação garantida da opção de tipos de backup selecionados terá somente backups mensais ativados.

   - Teste de recuperação garantida a partir dos pontos de recuperação mais recentes

   A origem é especificada

   Próximas etapas:

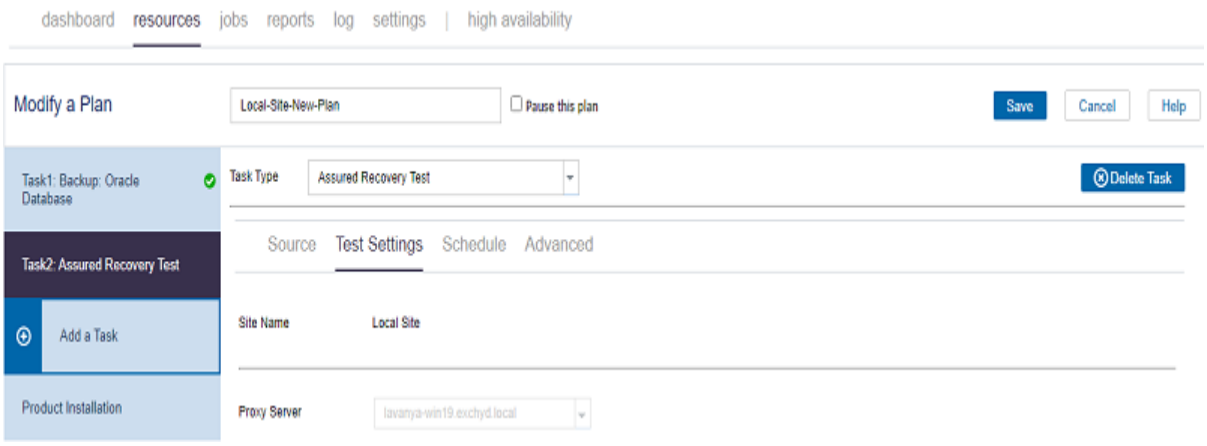
   - Especificar as configurações de teste
   - Especificar a programação de tarefas do teste de recuperação garantida
   - Especificar as configurações avançadas

Especificar as configurações de teste

A guia Configurações de teste permite especificar o servidor proxy.

Siga estas etapas:

1. Clique na guia **Configurações de teste**.



2. Na lista suspensa Servidor proxy, selecione o nó do proxy.

   Observação: para Oracle, o próprio servidor de ponto de recuperação atua como o servidor proxy no teste de recuperação garantida.

   As configurações de teste são especificadas.

Próximas etapas:

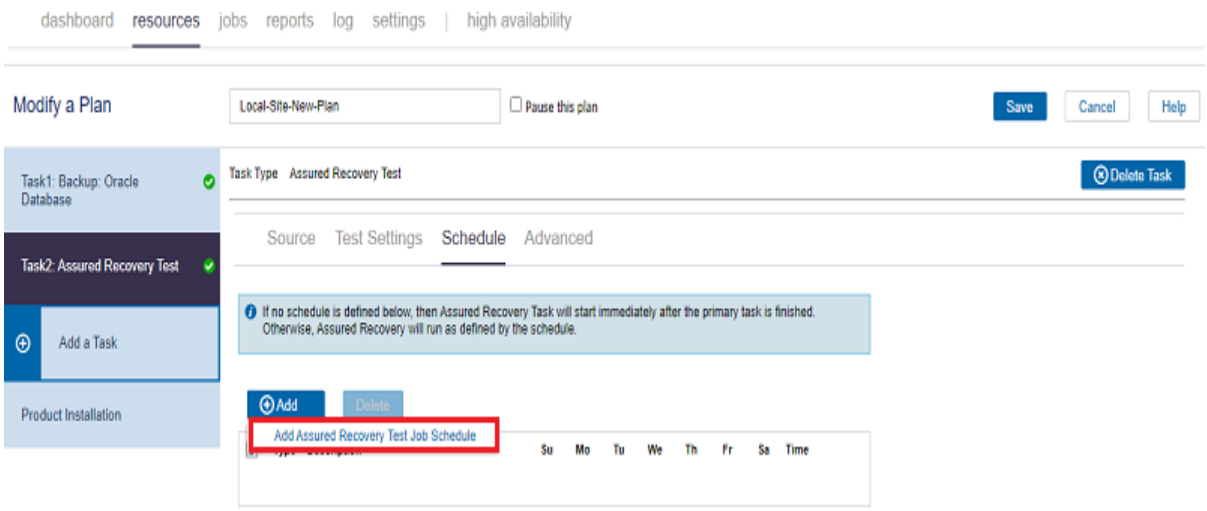
- Especificar a programação de tarefas do teste de recuperação garantida
- Especificar as configurações avançadas

Especificar a programação de tarefas do teste de recuperação garantida

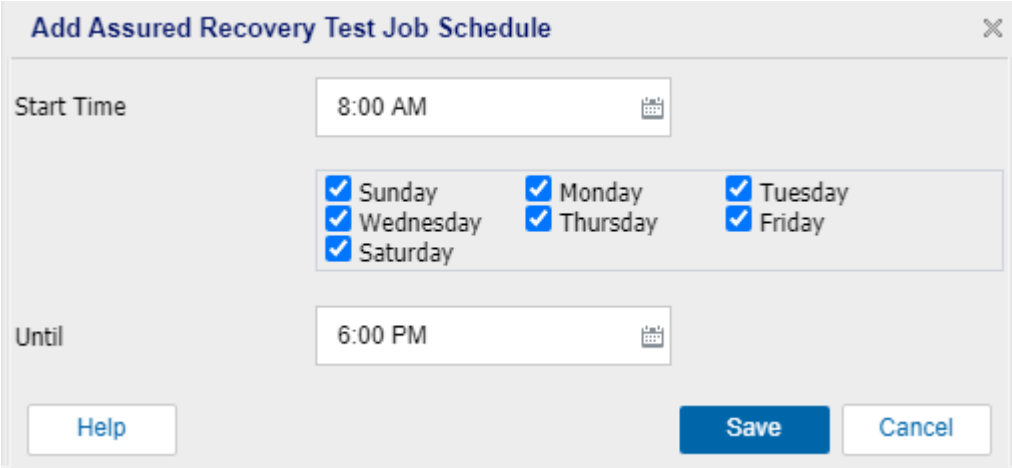
A guia de programação permite especificar a programação de tarefas do teste de recuperação garantida. Se não especificar uma programação, a tarefa será iniciada imediatamente quando você executar a tarefa principal.

Siga estas etapas:

1. Clique na guia **Programar**.



2. Clique em **Adicionar** e, em seguida, selecione **Adicionar programação da tarefa de teste de recuperação garantida**.
3. Na caixa de diálogo Adicionar programação da tarefa de teste de recuperação garantida, faça o seguinte e clique em **Salvar**:
   - **Hora de início:** especifique a hora de início para iniciar a tarefa de teste de recuperação garantida.
   - **Até:** especifique a hora de término da tarefa de teste de recuperação garantida.



A tarefa de teste de recuperação garantida é programada e aparece na página Programar.

Observações:

- Se a origem de recuperação garantida for Pontos de recuperação mais recentes + Ativar programação de recuperação garantida, o valor padrão é 1. Como resultado, por padrão, a mais recente é verificada.

  Para o valor <=0, todos os pontos de recuperação não verificados são testados.

- Se a origem de recuperação garantida for Diário/semanal/mensal + Ativar programação de recuperação garantida, o valor padrão é 9 (7 diárias + 1 semanal + 1 mensal).

  Para o valor <=0, todos os pontos de recuperação não verificados são testados.

- Se não desejar usar o valor padrão, é possível adicionar uma chave de Registro DWORD de 32 bits no seguinte local:

  HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AssuredRecovery\MaxNumberOfRecoveryPoint

Próxima etapa:

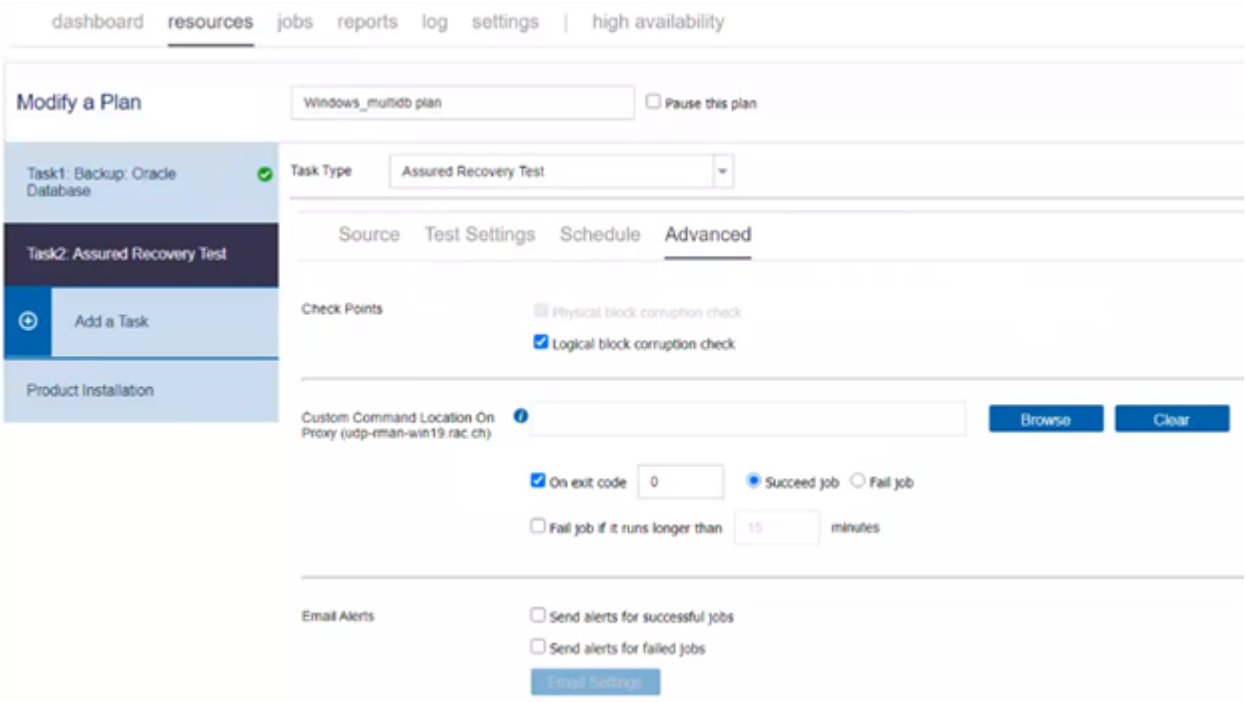
- Especificar as configurações avançadas

Especificar as configurações avançadas

A guia Avançado ajuda aplicar outras configurações necessárias para a conclusão do plano. Isso é opcional se você não precisar adicionar mais configurações.

Siga estas etapas:

1. Clique na guia **Avançado**.



2. Faça o seguinte:

   Pontos de verificação

   Verificação de danos ao bloco físico

   O RMAN detecta apenas blocos fisicamente corrompidos a cada backup que faz e armazena as informações corrompidas no arquivo de controle e no arquivo alert.log. Por padrão, a opção **Verificação de danos ao bloco físico** está ativada.

   Verificação de danos ao bloco lógico

   O RMAN não detecta automaticamente blocos logicamente corrompidos por padrão. Marque a caixa de seleção **Verificação de danos ao bloco lógico** para detectar o corrompimento lógico juntamente com o corrompimento físico. Se um corrompimento lógico for encontrado, o RMAN armazenará as informações no arquivo alert.log.

   Local de comando personalizado no proxy

Observação: essa opção não será exibida se você selecionou backup/-replicação do Linux com base em agente como a origem do ponto de recuperação do teste de recuperação garantida.

Especifica o script personalizado armazenado no servidor proxy. Você pode procurar as informações de volume do servidor proxy. Se o tipo de recuperação garantida da IVM estiver selecionado, o script é copiado na VM e executado quando a VM for inicializada. Se o tipo de recuperação garantida de IVHD estiver selecionado, o script é executado no servidor proxy.

Observação: a tarefa de recuperação garantida pode oferecer suporte apenas ao script bat executável do Windows ou ao binário executável. Entretanto, essa limitação não restringe o uso da tarefa de recuperação garantida. É possível usar um script em lote do Windows criado para iniciar o script powershell, como o nome test.bat com o seguinte conteúdo:

Powershell.exe -NoProfile -ExecutionPolicy ByPass -Command "& '%ScriptPath%\AR-check.ps1'"

Além disso, os argumentos a seguir são transmitidos para o script de acordo com os requisitos.

- set PlanName=%1%

- set NodeName=%2%

- set ProxyServer=%3%

- set RecoveryPointName=%3%

- set MountPointRootPathName=%5% (aplicável apenas para o tipo de teste de disco virtual instantâneo)

Como resultado, o bat é invocado e executado da seguinte maneira:

Para o tipo de teste de máquina virtual instantânea:

"%ScriptPath%\test.bat PlanName NodeName ProxyServer RecoveryPointName

Para o tipo de teste de disco virtual instantâneo:

%ScriptPath%\test.bat PlanName NodeName ProxyServer RecoveryPointName MountPointRootPathName

Código de saída

Especifica o código de saída para a Tarefa bem-sucedida ou a Tarefa com falha.

Tarefa bem-sucedida

Especifica que a tarefa de recuperação garantida está definida como Bem-sucedida quando o script retorna o código de saída.

Tarefa com falha

Especifica que a tarefa de recuperação garantida está definida como Com falha quando o script retorna o código de saída.

A tarefa falha quando executada por mais tempo

Especifica se o script é executado por mais tempo que as vezes especificadas.

Valor padrão: 15 minutos.

Alertas por email

Permite ativar alertas por email. É possível especificar configurações de email e os tipos de alertas que você deseja receber por email.

- Se desejar receber alertas por email sobre o êxito de tarefas de recuperação garantida, marque a caixa de seleção **Enviar alertas para tarefas bem-sucedidas**.
- Se desejar receber alertas por email sobre falhas na tarefa de recuperação garantida, marque a caixa de seleção **Enviar alertas para tarefas com falha**.

  Observação: indisponíveis para tarefas executadas com o servidor de backup Linux.

  Configurações de email

  Permite configurar as definições de email.

  Para configurar o servidor de email e os detalhes do servidor proxy, clique em **Configurações de email**. Para obter mais informações sobre como definir as configurações de email, consulte Configurar email e alerta.

As configurações avançadas são especificadas.

(Opcional) Executar um backup manual

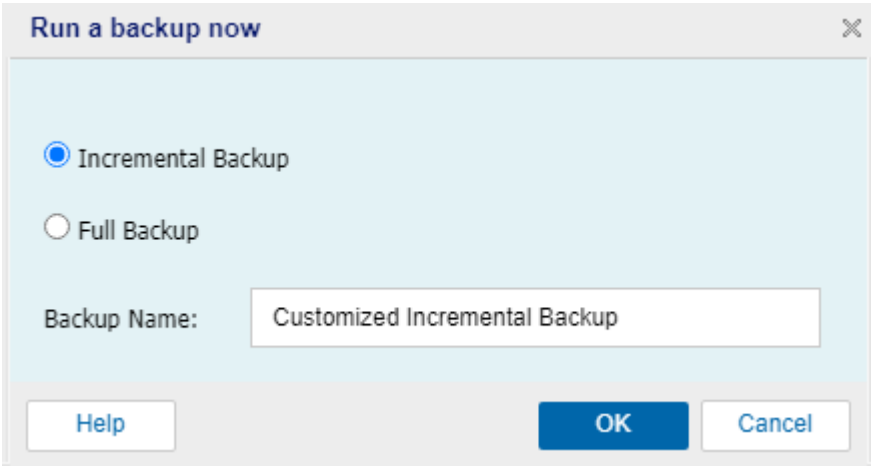
Em geral, os backups são executados automaticamente e controlados pelas configurações da programação. Além do backup programado, um backup manual fornece a opção de fazer backup dos nós de acordo com a necessidade. Por exemplo, se repetir a programação para backups completos e incrementais e desejar fazer grandes alterações em seu computador, você deverá executar um backup manual imediato sem esperar até que ocorra o próximo backup programado.

Siga estas etapas:

1. Efetue logon no Console do Arcserve UDP.
2. Navegue até **recursos** > **Plano** > **Todos os planos**.

   A lista de todos os planos é exibida no painel central.
3. Clique com o botão direito do mouse no plano e selecione **Fazer backup agora**.

   A caixa de diálogo Fazer backup agora é exibida.
4. Na caixa de diálogo Executar um backup agora, selecione o tipo de backup que deseja executar e, em seguida, especifique o nome do backup, se necessário.



As opções disponíveis são:

Backup incremental

Inicia um backup incremental do computador inteiro. Um backup incremental realiza backup somente dos blocos que foram alterados desde o backup anterior.

Observação: se estiver executando um backup pela primeira vez, o backup completo será iniciado automaticamente, mesmo que você tenha selecionado a opção Backup incremental.

As vantagens dos backups incrementais são a rapidez e o tamanho reduzido da imagem de backup gerada. Esta é a forma ideal para a execução de backups.

Backup completo

Inicia um backup completo do computador inteiro ou dos volumes selecionados.

Observações:

- Você também pode executar o backup manualmente na página Nós.
- Se nenhum nome de backup for especificado, por padrão, ele será automaticamente nomeado como Backup completo ou incremental personalizado.

5. Clique em **OK**.

   A caixa de diálogo Informações do andamento é exibida.

6. Aguarde até que a tarefa de backup seja concluída e clique em **OK**.

7. Para monitorar as tarefas de backup, navegue até **tarefas** > **Tarefas em andamento**.

   Aguarde até a conclusão da tarefa de backup.

   Observação: apenas uma tarefa pode ser executada em uma hora. Se você tentar iniciar manualmente uma tarefa de backup quando outra tarefa estiver em execução no mesmo momento, uma mensagem de alerta será exibida informando sobre a existência de outra tarefa em execução e solicitando uma nova tentativa mais tarde.

   O backup manual é realizado com êxito.

Como restaurar um banco de dados Oracle usando o RMAN

É possível restaurar todo o banco de dados Oracle ou executar a recuperação granular de espaços para tabelas e tabelas. Você também pode restaurar o banco de dados do ponto de recuperação no local de base do Oracle ou em um local ou nó alternativo.

Para restaurar o banco de dados Oracle, siga estas etapas:

1. Selecionar os itens do banco de dados Oracle para restauração
2. Definir as opções de restauração

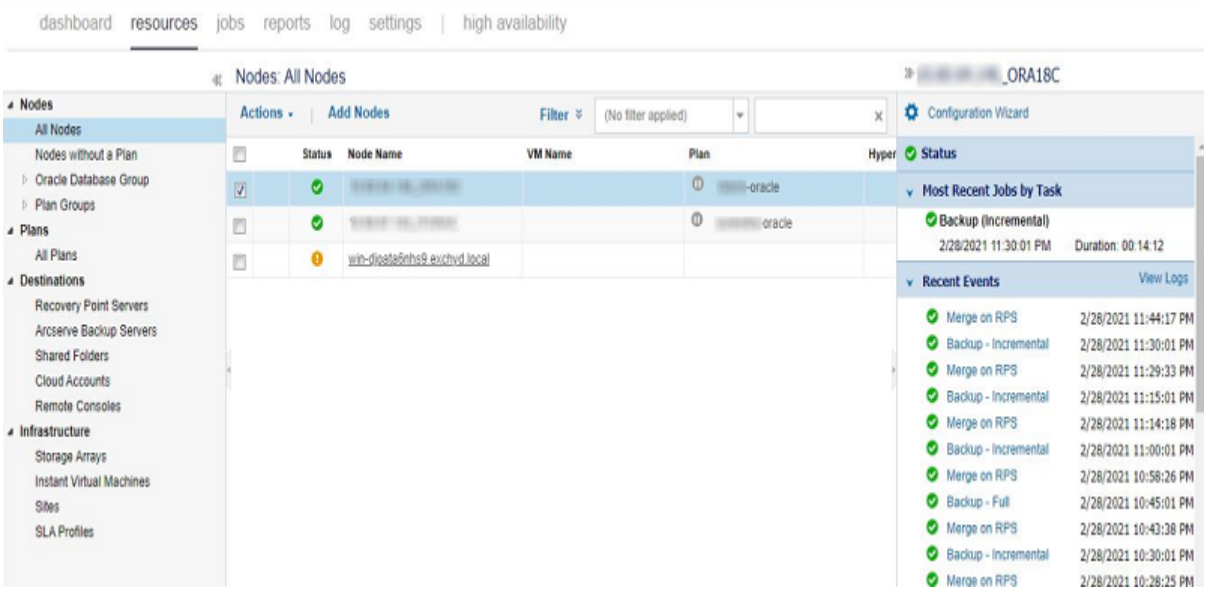
Selecionar os itens do banco de dados Oracle para restauração

Esta seção fornece informações sobre como procurar e selecionar itens do banco de dados Oracle para restauração.

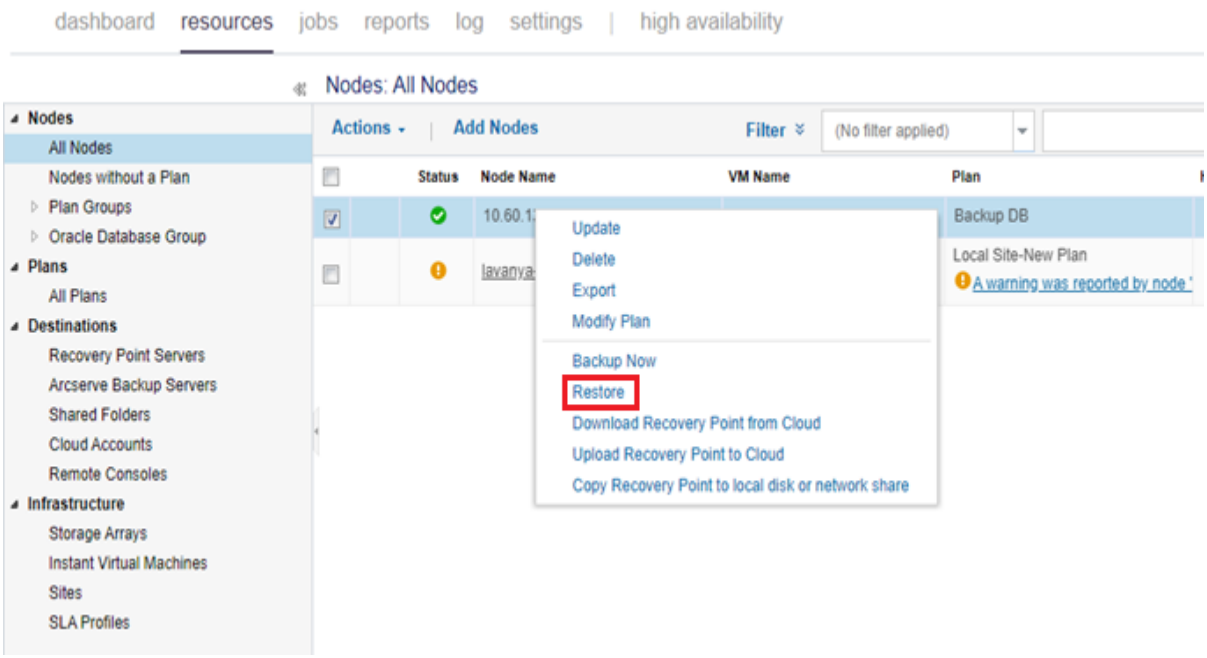
Siga estas etapas:

1. Efetue logon na conta do console do UDP.
2. Na página Console do UDP, clique na guia **recursos**.
3. No painel esquerdo, navegue para **Nós** > **Todos os nós**.

   A lista de nós existentes é exibida no painel central.



4. Clique com o botão direito do mouse no nó do Oracle e, em seguida, selecione a opção **Restaurar**.

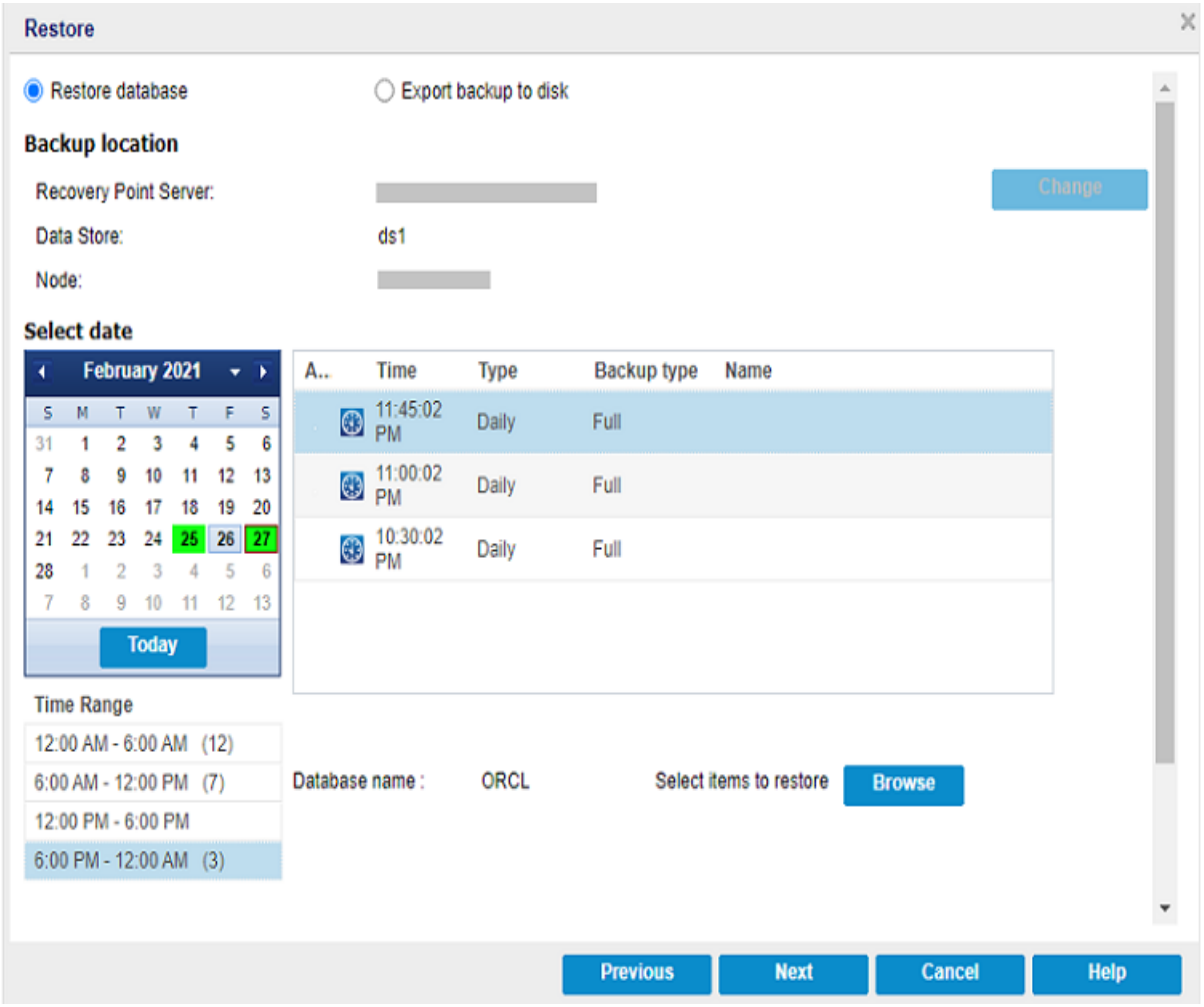


Você é conectado automaticamente ao nó do agente e o assistente de restauração é exibido.

5. No assistente de restauração, selecione uma das seguintes opções:

   Restaurar banco de dados

   A restauração do banco de dados inclui etapas para a restauração completa e granular do banco de dados.



Para selecionar os itens do banco de dados Oracle, siga estas etapas:

a. (Opcional) Para modificar os detalhes do local do backup, clique em **Alterar**.

   Observação: essa opção é válida somente quando a opção Exportar backup para disco está selecionada.

b. Na seção Selecionar data, selecione uma data.

   Com base na seleção, a lista de pontos de recuperação de backup é exibida com a hora do backup, o tipo de backup que foi executado (completo ou incremental) e o nome do backup.

c. Na lista de pontos de recuperação de backup, selecione um ponto de recuperação de backup que deseja restaurar.

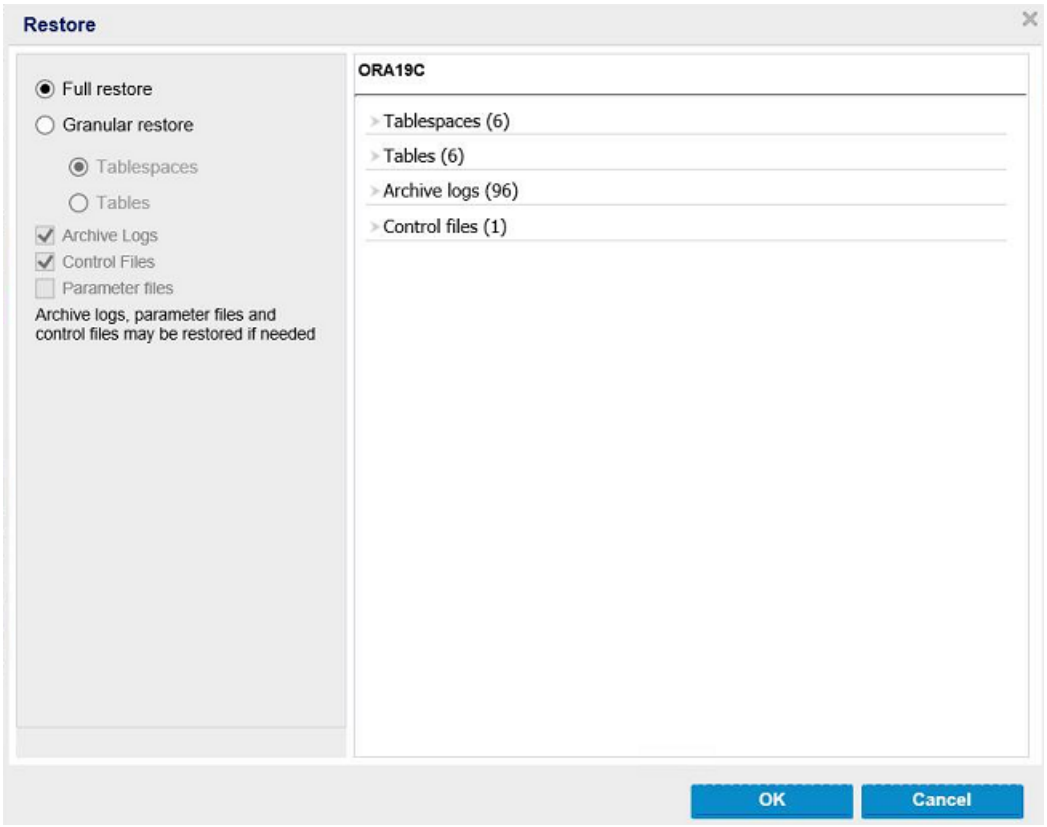
   Observação: por padrão, o ponto de recuperação do backup mais recente é selecionado.

d. Para selecionar os itens do banco de dados, siga estas etapas:

- Clique no botão **Procurar**.

  A caixa de diálogo Restaurar é exibida.

- Na caixa de diálogo Restaurar, execute o seguinte:



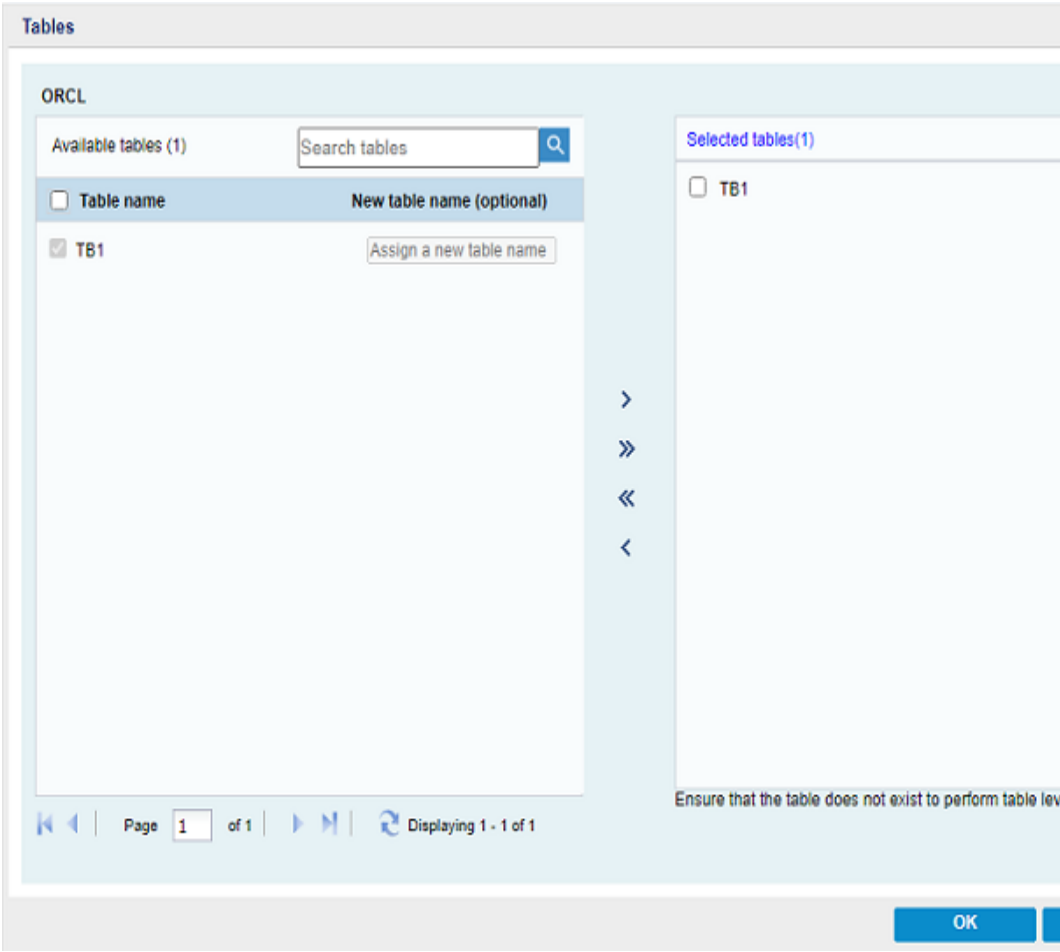
  - No painel esquerdo, faça o seguinte:
    - Para executar a restauração completa de itens inteiros do banco de dados, selecione **Restauração completa**.
    - Para executar a restauração de espaços para tabelas e tabelas, selecione **Restauração granular**.

    Observação: os itens do banco de dados Oracle, como logs de arquivo, arquivos de controle e arquivos de parâmetros, são selecionados por padrão quando a caixa de diálogo Restaurar é exibida. Além disso, esses itens são restaurados, se necessário.
  - No painel direito, clique em cada arquivo a ser expandido e, em seguida, exiba os detalhes.

- (Opcional) Para selecionar as tabelas específicas, no painel direito, clique na opção **Tabelas**.

  Uma caixa de diálogo de seleção de tabela é exibida.

  Na caixa de diálogo de seleção de tabela, faça o seguinte e clique em **OK**:



  - No painel esquerdo, faça o seguinte:
    - Para pesquisar as tabelas disponíveis, na caixa de pesquisa, selecione o nome da tabela e clique no ícone de pesquisa.
    - Selecione as tabelas que você deseja restaurar.
    - (Opcional) Digite o novo nome de uma tabela que deseja restaurar.

Após a seleção das tabelas, clique na seta para a direita (>) para movê-las para a lista de tabelas selecionadas().

- No painel direito, desmarque as tabelas que não deseja restaurar e, em seguida, clique na seta para a esquerda (<) para movê-las para a lista de tabelas disponíveis().

- Clique em **OK**.

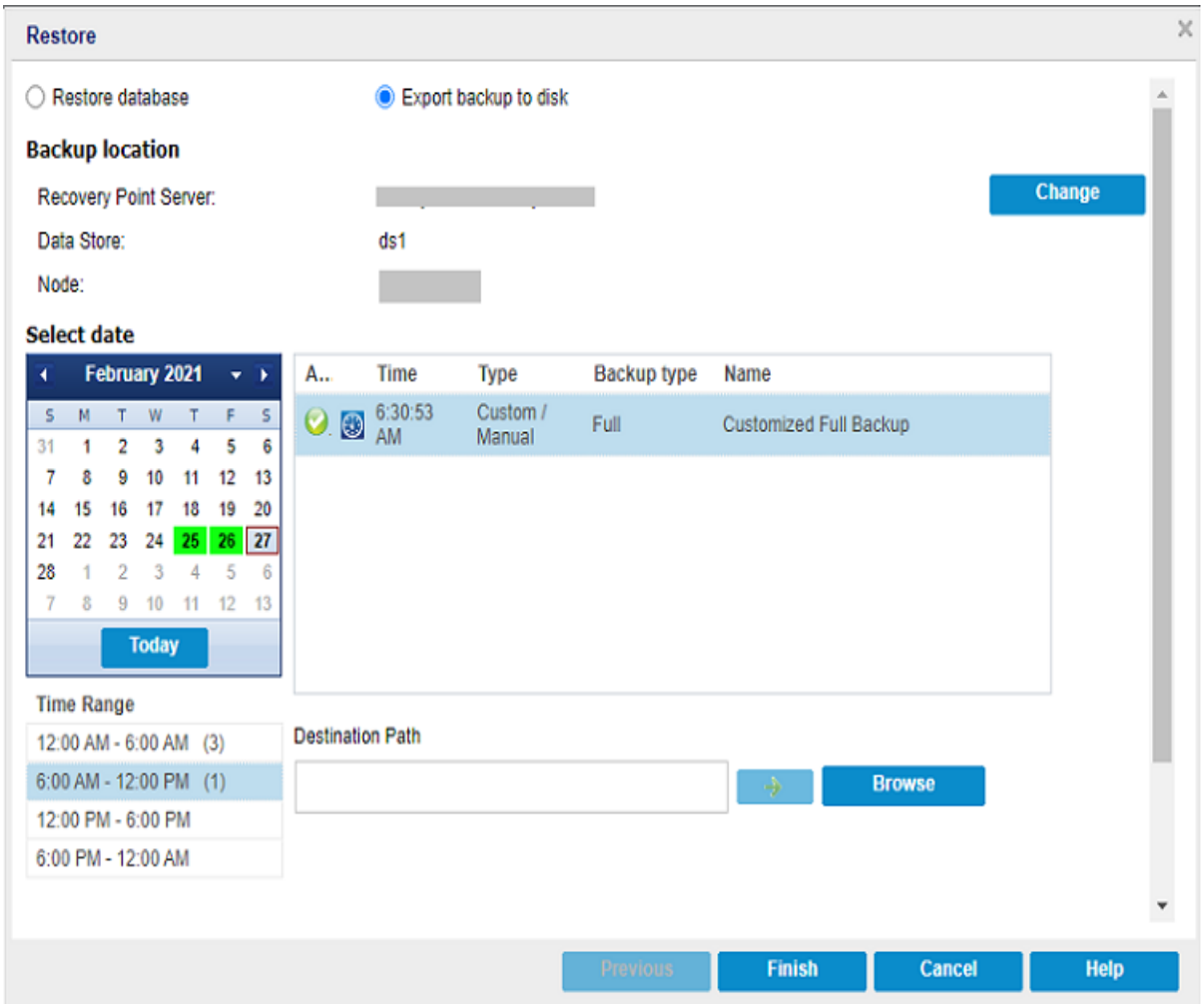
e. Clique em **Avançar**.

A caixa de diálogo Opções de restauração do é exibida.

Os itens do banco de dados Oracle a serem restaurados são selecionados. Agora, você pode definir as opções de restauração.

Exportar backup para disco

Restaura os itens do banco de dados Oracle na pasta ou na pasta compartilhada no disco.



Para exportar o backup para o disco, siga estas etapas:

a. (Opcional) Para modificar os detalhes do local do backup, clique em **Alterar**.

b. Na seção Selecionar data, selecione uma data.

   Com base na seleção, a lista de pontos de recuperação de backup é exibida com a hora do backup, o tipo de backup que foi executado (completo ou incremental) e o nome do backup.

c. Na lista de pontos de recuperação de backup, selecione um ponto de recuperação de backup que deseja restaurar.

   Observação: por padrão, o ponto de recuperação do backup mais recente é selecionado.

d. No campo Caminho de destino, forneça o caminho completo do compartilhamento de rede remota.

e. Para validar a conexão, clique no ícone de seta verde ao lado do campo Caminho de destino, digite o nome do usuário e a senha, conforme necessário, e clique em **OK**.

f. Em caso de conexão bem-sucedida com o compartilhamento de rede remota, clique no botão **Procurar**.

   A caixa de diálogo Selecionar o local do backup é exibida.

g. Na caixa de diálogo Selecionar o local do backup, selecione uma pasta para restauração e clique em **OK**.

h. Clique em **Concluir**.

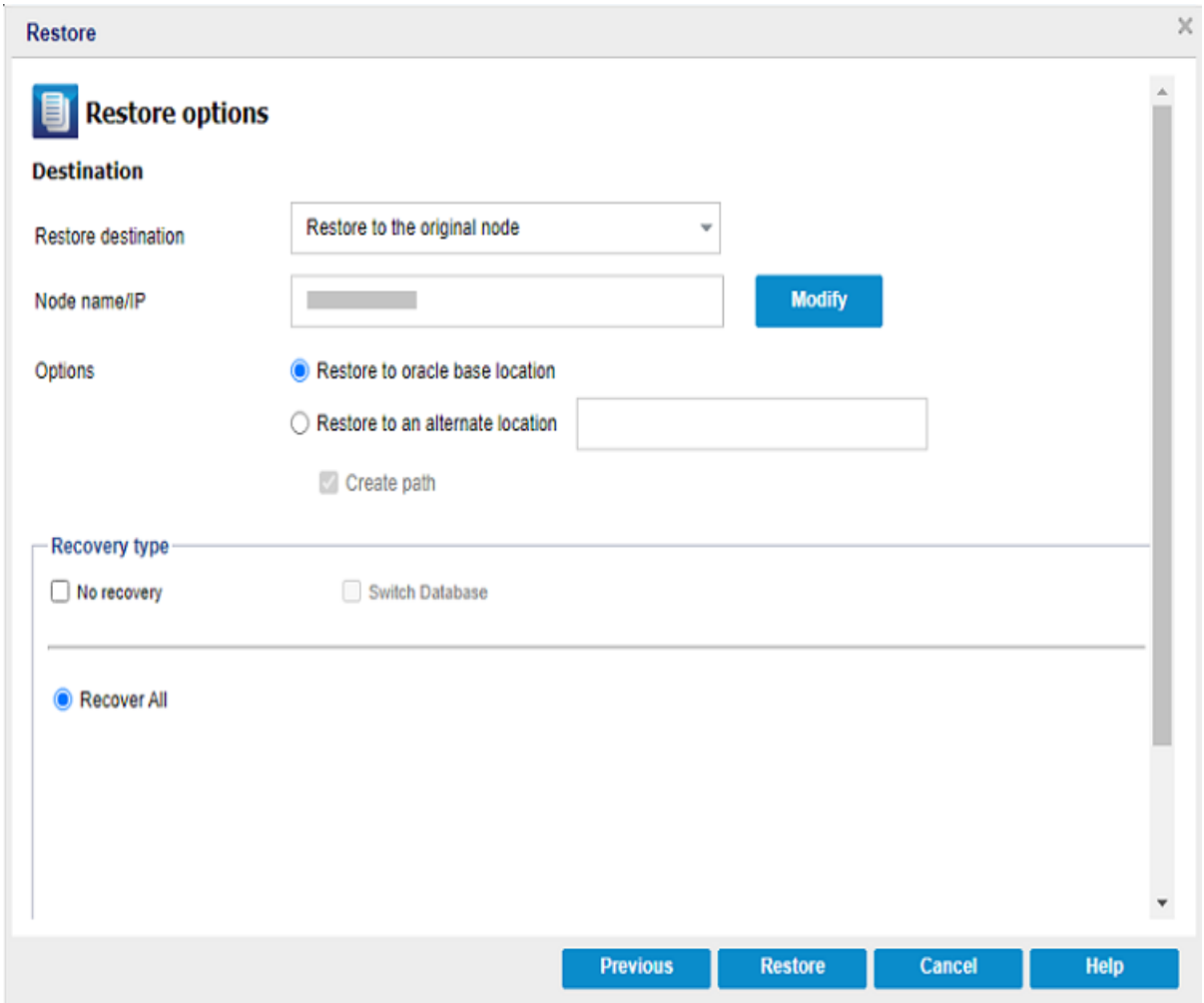
   Os itens do banco de dados Oracle são exportados para o disco.

Definir as opções de restauração

Esta seção fornece informações sobre como definir opções de restauração para os itens selecionados do banco de dados Oracle.

Siga estas etapas:

1. Na caixa de diálogo Opções de restauração, selecione o destino da restauração.



Observações:

- Durante a restauração, para qualquer ponto de recuperação de backup completo, apenas a opção Recuperar tudo está disponível.
- Os pontos de recuperação associados aos backups incrementais incluem todas as opções, como Recuperar tudo, Horário definido, Até o SCN e Até o número de sequências do log para restauração.

As opções de destino disponíveis são:

Restaurar para o nó original

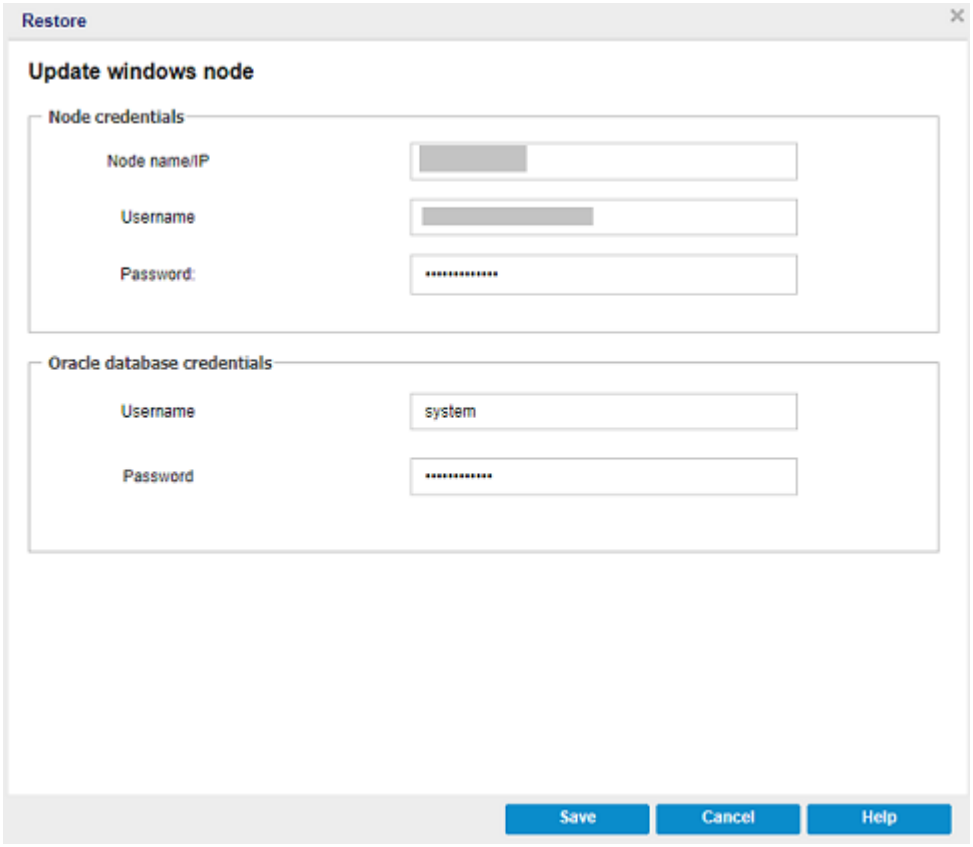
Para restaurar para o nó original, faça o seguinte:

- Os detalhes de nome/IP do nó existente são exibidos automaticamente. Caso seja necessário alterar os detalhes de nome/IP do nó, clique em **Modificar**.

  Com base no tipo de nó, a caixa de diálogo Atualizar nó do Windows ou Atualizar nó do Linux é exibida.

Atualizar nó do Windows

Na caixa de diálogo Atualizar nó do Windows, insira o nome/IP do nó, o nome de usuário e a senha, conforme necessário, e clique em **Salvar**.

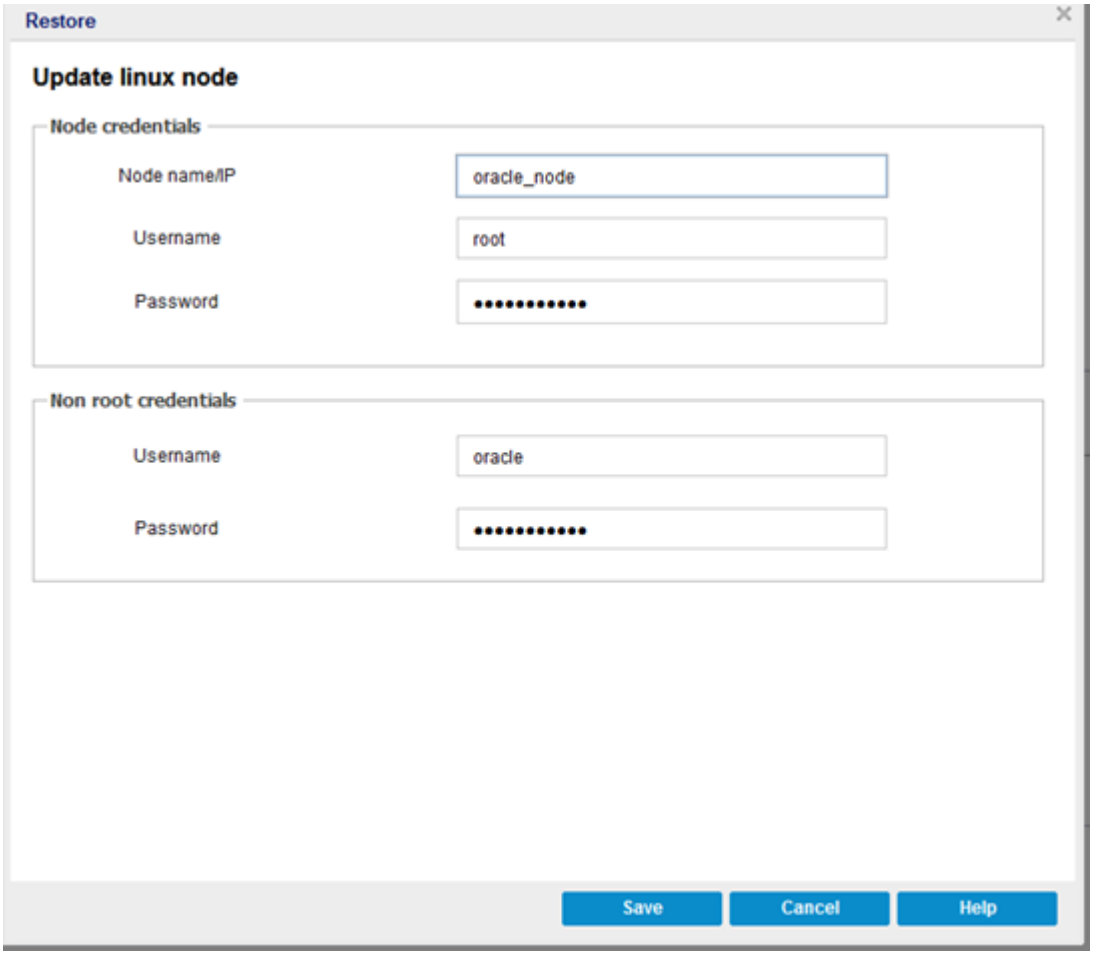


Atualizar nó do Linux

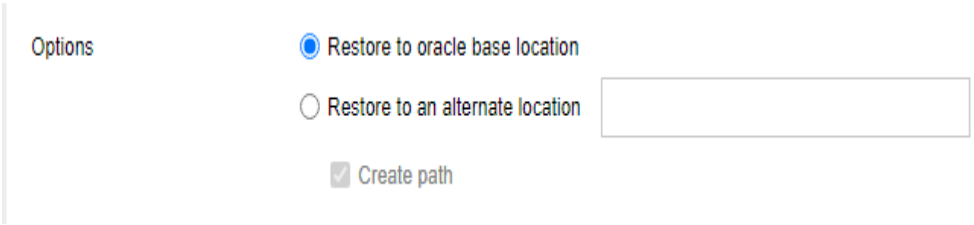
Na caixa de diálogo Atualizar nó do Linux, atualize os seguintes detalhes e clique em **Salvar**:

- Para as credenciais do nó, digite o nome/IP do nó, o nome do usuário e a senha, conforme necessário.

- Para as credenciais não raiz, digite o nome do usuário e a senha, conforme necessário.



- Para as opções, selecione uma das seguintes:



As opções disponíveis são:

Restaurar no local de base do Oracle

Restaura os itens selecionados do banco de dados no local de base do Oracle, de onde foi feito o backup.

Restaurar em um local alternativo

Restaura em um local alternativo. Ao selecionar essa opção, é necessário adicionar um caminho do local alternativo.

Observação: a caixa de seleção **Criar caminho** é marcada automaticamente quando você seleciona a opção **Restaurar em um local alternativo**.

Restaurar para o nó alternativo

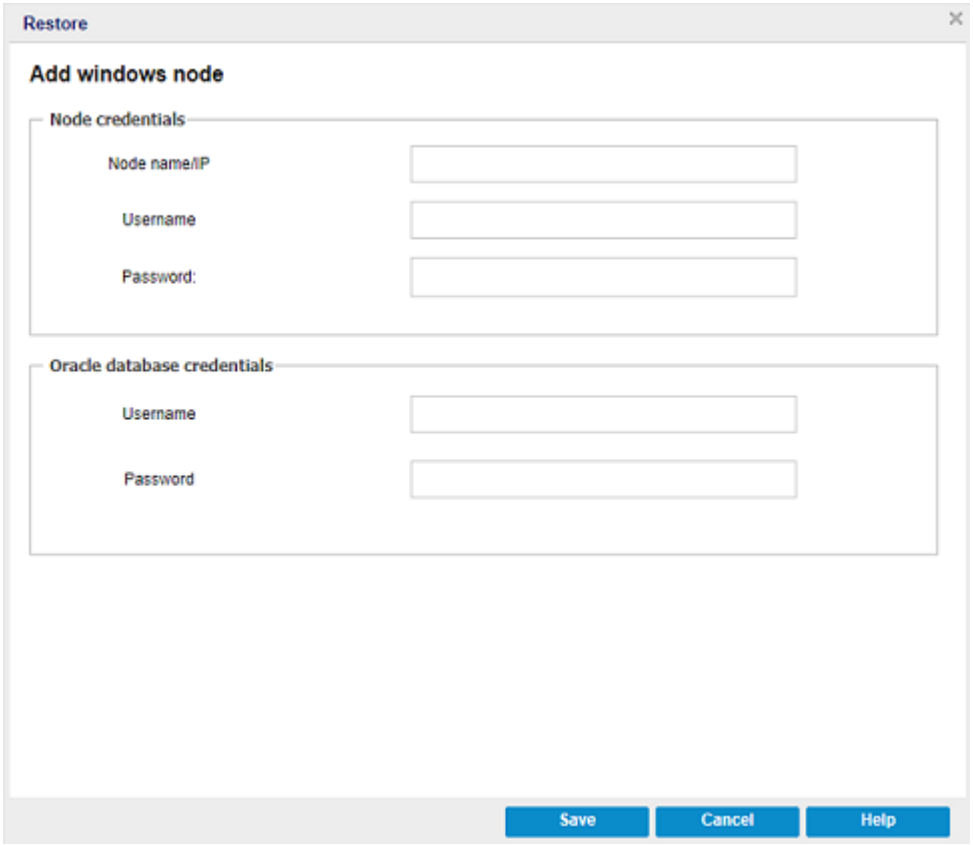
Para restaurar para o nó alternativo, faça o seguinte:

- Para adicionar um novo nó/IP, clique no botão **Adicionar**.

  Com base no tipo de nó, a caixa de diálogo Adicionar nó do Windows ou Adicionar nó do Linux é exibida.

  Adicionar nó do Windows

  Na caixa de diálogo Adicionar nó do Windows, digite o nome/IP do nó, o nome de usuário e a senha, conforme necessário, e clique em **Salvar**.

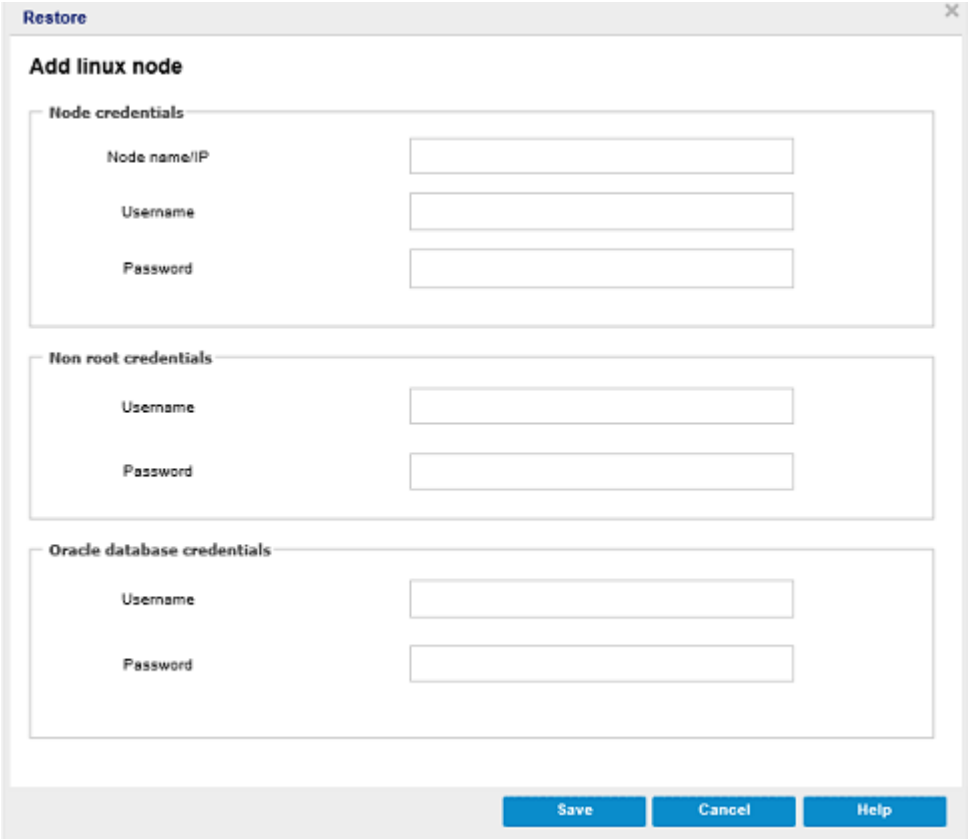


  Adicionar nó do Linux

  Na caixa de diálogo Adicionar nó do Linux, adicione os seguintes

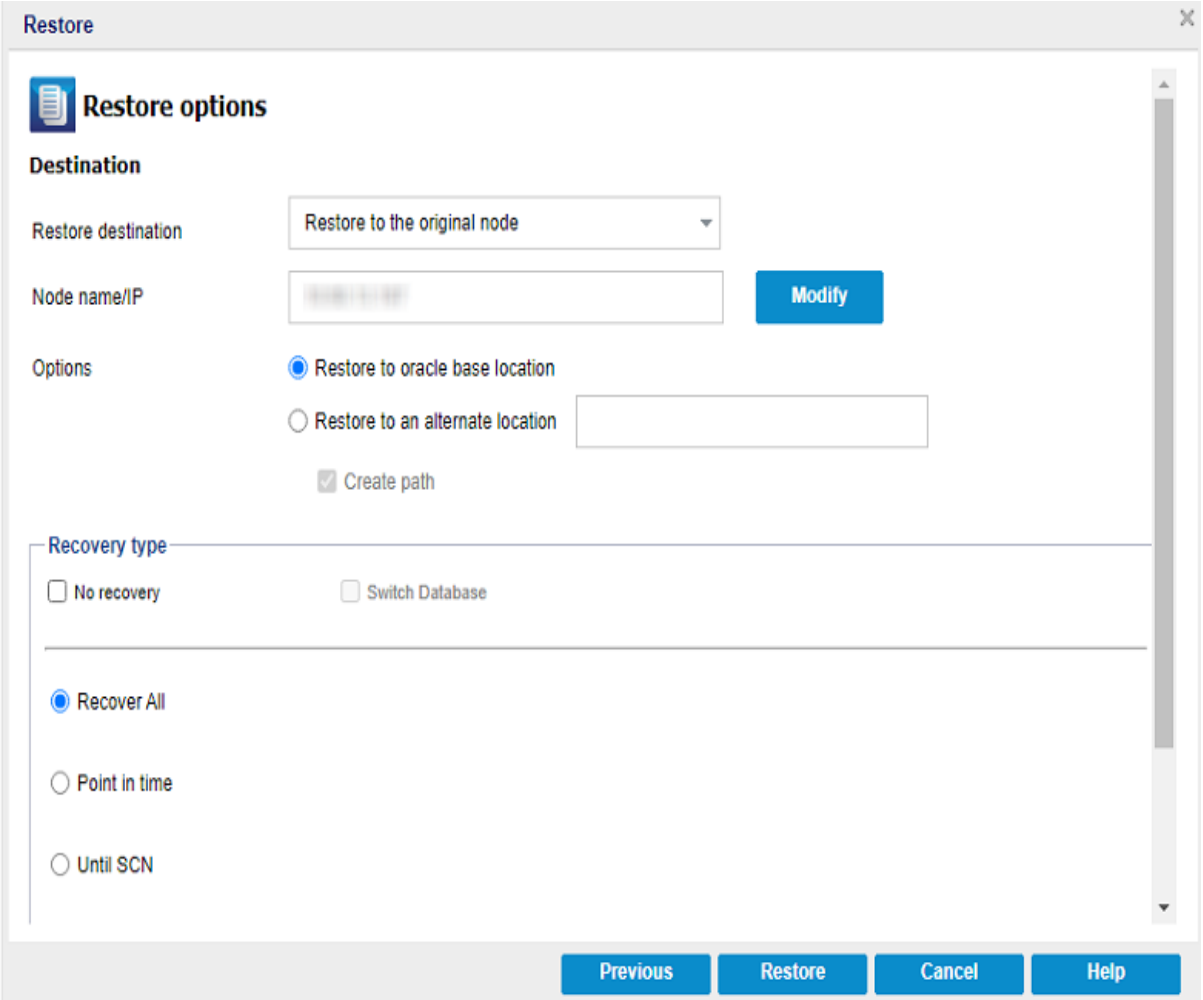
detalhes e clique em **Salvar**:

- Para as credenciais do nó, digite o novo nome/IP do nó, nome do usuário e senha, conforme necessário.
- Para as credenciais não raiz, digite o novo nome de usuário e senha, conforme necessário.



- Para Opções, a opção **Restaurar para um local alternativo** é selecionada por padrão. Digite um caminho do local alternativo.

2. Na seção Tipo de recuperação, faça o seguinte:



- Se não quiser executar a recuperação, marque a caixa de seleção **Sem recuperação**. Com base na seleção, a seguinte opção é ativada:

  Alternar banco de dados

  Se desejar alternar os itens do banco de dados para o novo local, marque a caixa de seleção **Alternar banco de dados**.

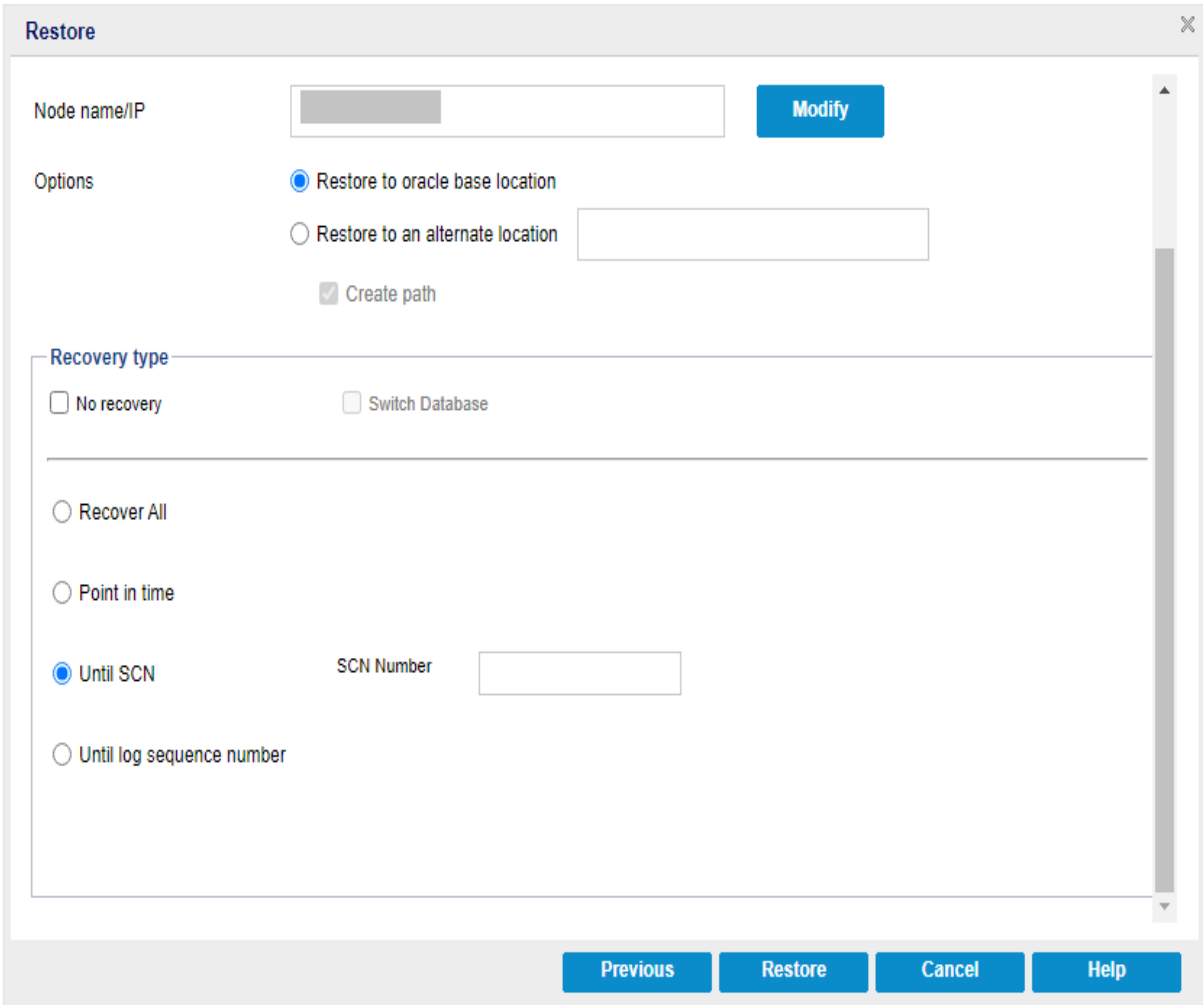
  Observação: a opção Alternar banco de dados só é suportada quando a restauração para um local ou nó alternativo é executada.

- Se você deseja executar a restauração pontual, selecione **Horário definido** e forneça o seguinte:

  - Selecione uma data para executar a restauração pontual.
  - Selecione a hora de início, conforme necessário.

  Observação: a data e a hora de início da restauração pontual devem ser menores que o ponto de recuperação de backup selecionado e maiores que o ponto de recuperação anterior.

- Se desejar recuperar todos os itens do banco de dados até o carimbo de data e hora do SCN (System Change Number - Número de alteração do sistema), selecione **Até o SCN** e, em seguida, digite o valor do número do SCN, conforme necessário.



- Se desejar recuperar todos os itens do banco de dados até o número de sequência do log fornecido, selecione **Até o número de sequência do log** e, em seguida, digite os valores para a sequência do log e o número do segmento, conforme necessário.

3. Clique em **Restaurar**.

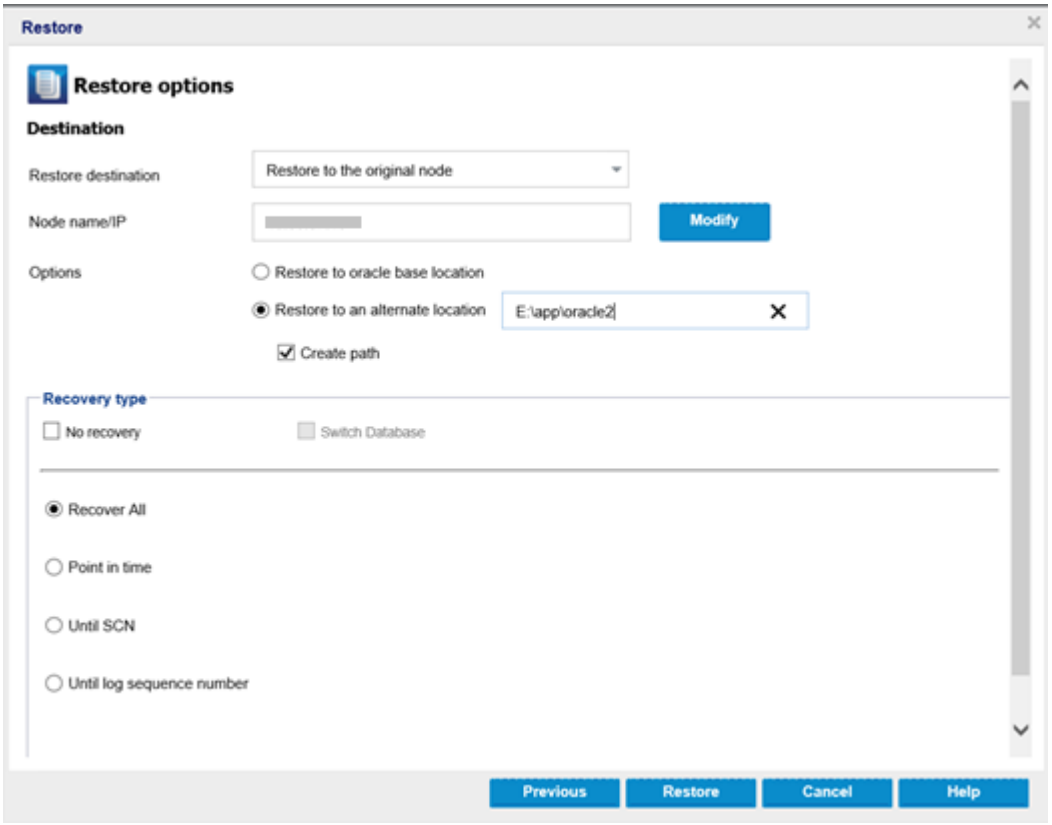
Os itens do banco de dados Oracle são restaurados.

Como restaurar o banco de dados em um local alternativo no Windows

Esta seção fornece informações sobre como restaurar o banco de dados em um local alternativo no Windows.

Siga estas etapas:

1. No console do UDP, selecione o ponto de recuperação a partir do qual você precisa executar a restauração. Para obter mais informações, consulte Definir as opções de restauração.
2. Na caixa de diálogo Opções de restauração, na lista suspensa Destino da restauração, selecione **Restaurar para o nó original**.



3. Para Nome/IP do nó, digite o nome ou o endereço IP do nó.
4. Para Opções, selecione a opção **Restaurar em um local alternativo** e, em seguida, adicione um caminho do local alternativo.

   Observações:

   - Verifique se o caminho adicionado não possui caracteres especiais ou espaços.

- A caixa de seleção **Criar caminho** é marcada automaticamente quando você seleciona a opção **Restaurar em um local alternativo**.
- Se o banco de dados ainda não estiver encerrado, será exibida uma notificação solicitando o encerramento do banco de dados. Para confirmar, clique em **OK**.

5. Confirme se a tarefa de restauração foi bem-sucedida no console do UDP.
6. Conecte-se ao **sqlplus** e confirme se o banco de dados está ativo e em execução.

   O banco de dados restaurado está operacional com o local alternativo especificado. No entanto, após a reinicialização do banco de dados, o banco de dados pode voltar à cópia anterior ou pode não retornar corretamente devido a um problema conhecido. Para evitar mais problemas após a restauração em um local alternativo, é recomendável seguir as etapas abaixo. Essas etapas ajudam a criar ou colocar a cópia correta de spfile/pfile.

   a. Vá para **%ORACLE_HOME%\database e renomeie spfile<SID>.ora**.

   b. Conecte-se a **sqlplus**.

   c. Vá para o prompt do SQL e execute o seguinte comando:

      sqlplus > create pfile from spfile.

   d. Vá para **%ORACLE_HOME%\database**, abra **init<SID>.ora** em qualquer editor e faça o seguinte:

      1. Atualize o valor de “db_create_file_dest” com o caminho especificado para o local de restauração alternativo.
      2. Remova a barra “\” adicional do final do caminho no parâmetro *diagnostic_dest*.

         Altere o seguinte:

         De *diagnostic_dest='E:\app\oracle2\ORA19C280220211833\'*

         Para *diagnostic_dest='E:\app\oracle2\ORA19C280220211833'*
      3. Salve o arquivo.

   e. Vá para o prompt do SQL e execute os seguintes comandos:

      Sqlplus > shutdown immediate

      sqlplus > startup

      sqlplus > create spfile from pfile

      Observação: se o banco de dados não for iniciado a partir de *spfile*, as restaurações dos backups correspondentes serão limitadas apenas ao

nó original. Para evitar isso, reinicie o banco de dados novamente após a criação de *spfile*. Para reiniciar, execute os seguintes comandos:

Sqlplus > shutdown immediate

sqlplus > startup

Como restaurar o banco de dados em um nó alternativo no Windows

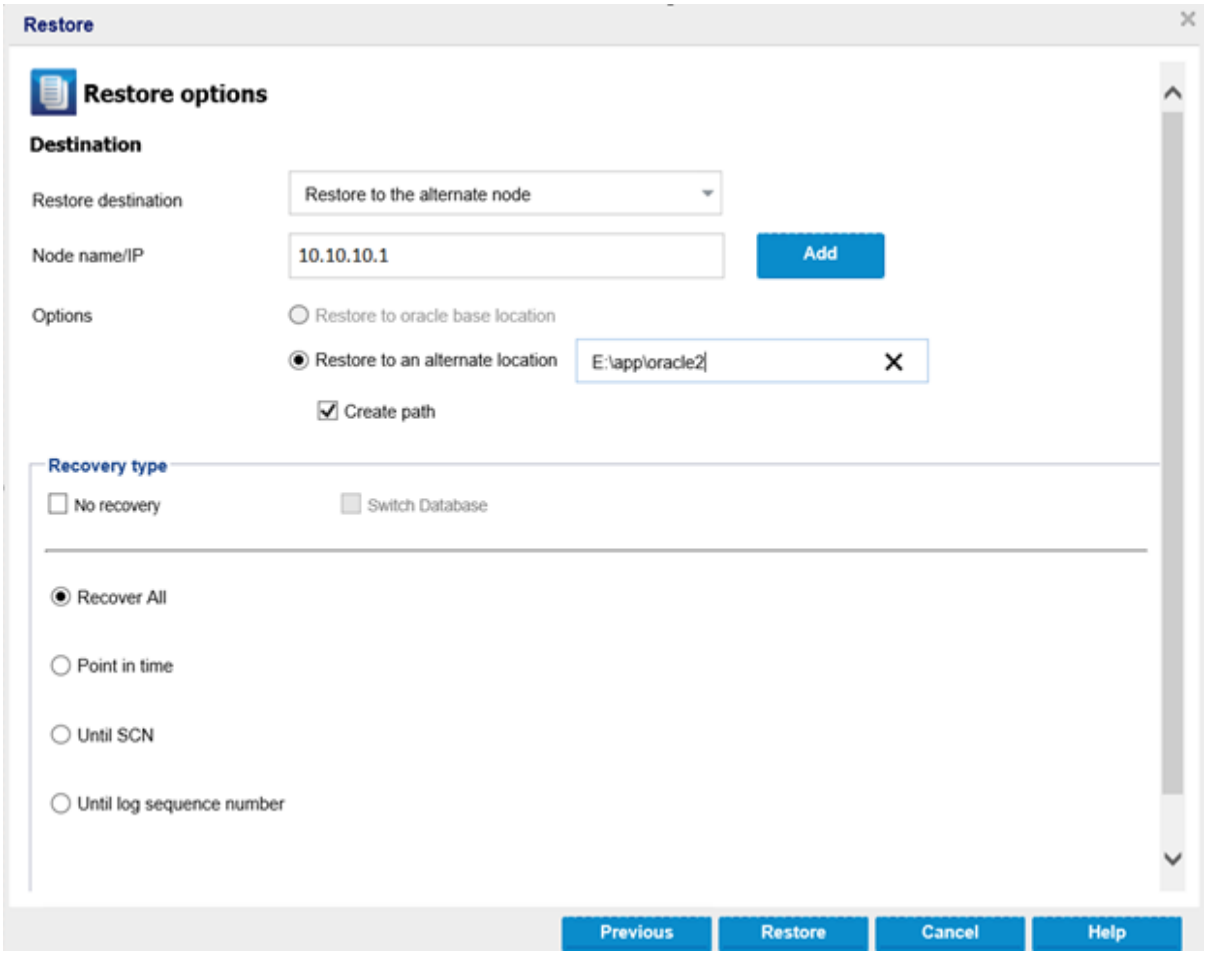
Esta seção fornece informações sobre como restaurar o banco de dados em um nó alternativo no Windows.

Observações:

- Quando o **Rastreador do bloco alterado** está desativado e a restauração de nós alternativos é executada, a restauração pode falhar. Portanto, selecione a opção de restauração somente quando tiver os logs necessários disponíveis e puder recuperar o banco de dados manualmente após a restauração. Como solução alternativa, ative o **Rastreador do bloco alterado** antes de executar a restauração de nó alternativo no nó de origem.
- Certifique-se de instalar a mesma versão do software Oracle e criar o banco de dados com o mesmo SID no nó alternativo onde você planejou executar a restauração como o nó original (nó de origem). Por exemplo, quando o SID do nó de origem for orcl, crie orcl no nó alternativo antes de iniciar a restauração. Isso é necessário quando o software Oracle é instalado com a conta de domínio. Isso não é necessário ao usar a conta virtual.

Siga estas etapas:

1. No console do UDP, selecione o ponto de recuperação a partir do qual você precisa executar a restauração. Para obter mais informações, consulte Definir as opções de restauração.
2. Na caixa de diálogo Opções de restauração, na lista suspensa Destino da restauração, selecione **Restaurar para o nó alternativo**.



3. Para Nome/IP do nó, digite o nome ou o endereço IP do nó.
4. Para Opções, selecione a opção **Restaurar em um local alternativo** e, em seguida, adicione um caminho do local alternativo.

   Observações:

   - Verifique se o caminho adicionado não possui caracteres especiais ou espaços.
   - A caixa de seleção **Criar caminho** é marcada automaticamente quando você seleciona a opção **Restaurar em um local alternativo**.
   - Se o banco de dados ainda não estiver encerrado, será exibida uma notificação solicitando o encerramento do banco de dados. Para confirmar, clique em **OK**.
5. Confirme se a tarefa de restauração foi bem-sucedida no console do UDP.
6. Conecte-se ao **sqlplus** no nó alternativo e confirme se o banco de dados está ativo e em execução.

O banco de dados restaurado está operacional com o local alternativo especificado. No entanto, após a reinicialização do banco de dados, o banco de dados pode voltar à cópia anterior ou pode não retornar corretamente devido a um problema conhecido. Para evitar mais problemas após a restauração em um local alternativo, é recomendável seguir as etapas abaixo. Essas etapas ajudam a criar ou colocar a cópia correta de spfile/pfile.

a. Vá para **%ORACLE_HOME%\database e renomeie spfile<SID>.ora**.

b. Conecte-se a **sqlplus**.

c. Vá para o prompt do SQL e execute o seguinte comando:

   sqlplus > create pfile from spfile.

d. Vá para **%ORACLE_HOME%\database**, abra **init<SID>.ora** em qualquer editor e faça o seguinte:

   1. Atualize o valor de “db_create_file_dest” com o caminho especificado para o local de restauração alternativo.

      Exemplo: **.db_create_file_dest-='E:\app\oracle2\ORA19C280220211833'*

   2. Remova a barra “\” adicional do final do caminho no parâmetro *diagnostic_dest*.

      Altere o seguinte:

      De *diagnostic_dest='E:\app\oracle2\ORA19C280220211833\'*

      Para *diagnostic_dest='E:\app\oracle2\ORA19C280220211833'*

   3. Salve o arquivo.

e. Vá para o prompt do SQL e execute os seguintes comandos:

   Sqlplus > shutdown immediate

   sqlplus > startup

   sqlplus > create spfile from pfile

   Observação: se o banco de dados não for iniciado a partir de *spfile*, as restaurações dos backups correspondentes serão limitadas apenas ao nó original. Para evitar isso, reinicie o banco de dados novamente após a criação de *spfile*. Para reiniciar, execute os seguintes comandos:

   Sqlplus > shutdown immediate

   sqlplus > startup

Limitações

As limitações a seguir estão presentes na release atual:

- Se o servidor RPS for alterado, o backup subsequente será um backup completo.
- A restauração para um nó alternativo não será suportada se a origem e o destino estiverem em duas versões diferentes do Oracle.
- Após a atualização para 8.1, quando a tarefa Restaurar em um local alternativo ou nó alternativo é executada, os pontos de recuperação do log de arquivamento que foram criados antes da atualização para 8.0 se tornam inválidos. Os pontos de recuperação se tornam inválidos porque não contêm detalhes de mapeamento de DataFile no banco de dados do Flash, conforme necessário.
- Para restaurações do log de arquivamento em um local ou nó alternativo na versão 8.1, o backup incremental (todos os tipos de dados) deve ser executado primeiro e, em seguida, as programações do log de arquivamento subsequentes podem ser usadas para restaurações.
- Quando o listener do Oracle é configurado no local não padrão, o banco de dados Oracle não aparece na lista de nós automaticamente e deve ser adicionado manualmente durante a criação do plano.
- A opção Pausar/continuar não está disponível no menu Nó para nós do Oracle.
- O Oracle não oferece suporte ao espaço para tabelas se o nome do espaço para tabelas contiver o sinal de dólar ($) no Oracle 19c.
- A restauração granular não oferece suporte quando o banco de dados Oracle é instalado usando a conta virtual.
- O UDP 8.1 não oferece suporte ao backup de bancos de dados de versões diferentes do Oracle instaladas no mesmo servidor.
- Recuperação de tabela de acordo com as limitações do Oracle:
  - As tabelas criadas a partir dos espaços para tabelas SYSTEM e SYSAUX não podem ser recuperadas.
  - As tabelas criadas a partir do sistema ou do usuário do sistema não podem ser recuperadas.
- O RPS atua como um agente de backup, restauração e recuperação garantida.

- Para Standard Edition, somente a restauração completa do banco de dados com recuperação total e PIT (Point-in-time - Pontual) é suportada nos pontos de recuperação mais recentes e intermediários.
- Para Standard Edition, a restauração do espaço para tabelas com recuperação total é suportada no ponto de recuperação mais recente e a cláusula UNTIL não é suportada no script do RMAN.
- Para a Standard Edition, o Oracle não oferece suporte a restaurações em nível de tabela.
- Após uma restauração do banco de dados completo, o próximo backup incremental será automaticamente convertido em um backup completo.
- Se o tamanho do WRP for alterado, o próximo backup será um backup completo.
- O número máximo de canais suportados é 10.

Capítulo 5: Proteger o ambiente do Microsoft SharePoint

Esta seção contém os seguintes tópicos:

Considerações sobre a instalação em um ambiente do Microsoft SharePoint

Este tópico fornece as informações necessárias para instalar e configurar o agente do Arcserve UDP para o ambiente do Microsoft SharePoint. As informações deste tópico pressupõem que você esteja familiarizado com as características e os requisitos do servidor farm do Microsoft SharePoint.

Considerações quanto ao ambiente

Os ambientes do SharePoint podem ser complexos e distribuídos por uma série de computadores. A configuração do server farm deve ser aceita pela Microsoft. Como um exemplo, um ambiente distribuído do SharePoint pode conter os seguintes componentes:

- Um ou mais servidores Web-Front-End.
- Um ou mais servidores de banco de dados usado pelo farm do SharePoint Server.
- Na maioria dos casos, o SharePoint é instalado em um ambiente de domínio. Haverá uma ou mais servidores DNS e controladores de domínio.

Considerações sobre a instalação

Ao instalar o agente, considere o seguinte:

- O SharePoint é um ambiente distribuído. É recomendável instalar o agente do UDP em cada servidor Farm do SharePoint, incluindo servidores Web-Front-End e servidores de banco de dados.
- Também é recomendável proteger todo o ambiente de domínio, incluindo o controlador de domínio, servidor DNS. Aqueles são necessários para restauração de Farm, configuração do Farm e do aplicativo web.

Como fazer backup de servidores do Microsoft SharePoint

É possível fazer backup dos servidores do Microsoft SharePoint usando o Arcserve UDP. Para garantir que a restauração funciona como esperado, é recomendável proteger a máquina inteira e os volumes não selecionados em todos os servidores do SharePoint.

Para servidores de controlador de domínio e o DNS, desde que o serviço de domínio e o serviço DNS funcionem corretamente, após serem inicializados pela VM de instância, é possível fazer backup dos volumes selecionados.

- Verificar as considerações
- Executar um backup do servidor SharePoint

Verificar as considerações

É recomendável para adicionar todos os servidores, incluindo servidores Web-Front-End, servidores de banco de dados, controladores de domínio e servidores DNS em um plano com a mesma programação de backup. Como resultado, todos os servidores são obtidos em backup quase ao mesmo tempo. Isso é muito importante para um ambiente distribuído. Durante a restauração, é possível fazer o mesmo de pontos de recuperação cujo backup será feito ao mesmo tempo para todos os servidores.

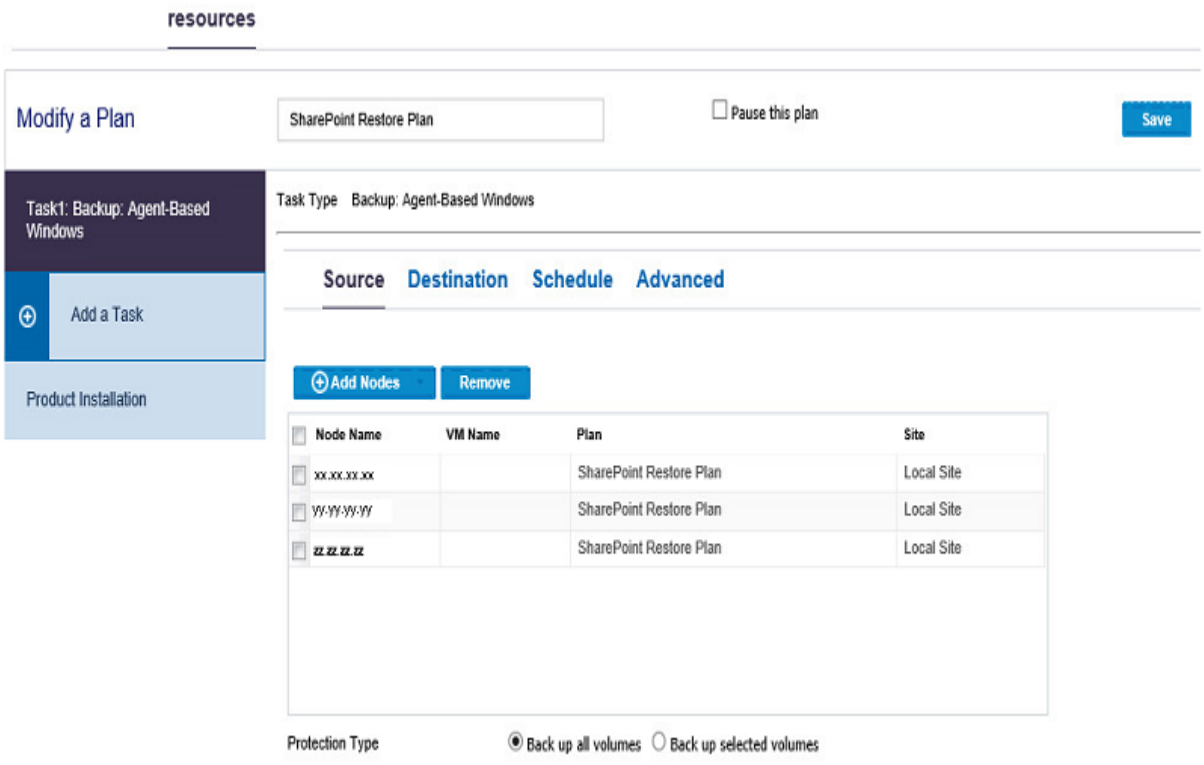
Observação: Se a topologia de Farm do SharePoint for alterada, novos servidores serão adicionados para executar uma melhoria de balanceamento de carga do SharePoint. É necessário adicionar os novos servidores imediatamente ao mesmo plano.

Executar um backup do servidor SharePoint

Use o Console do Arcserve UDP para executar o backup de nível de banco de dados no ambiente do SharePoint.

Siga estas etapas:

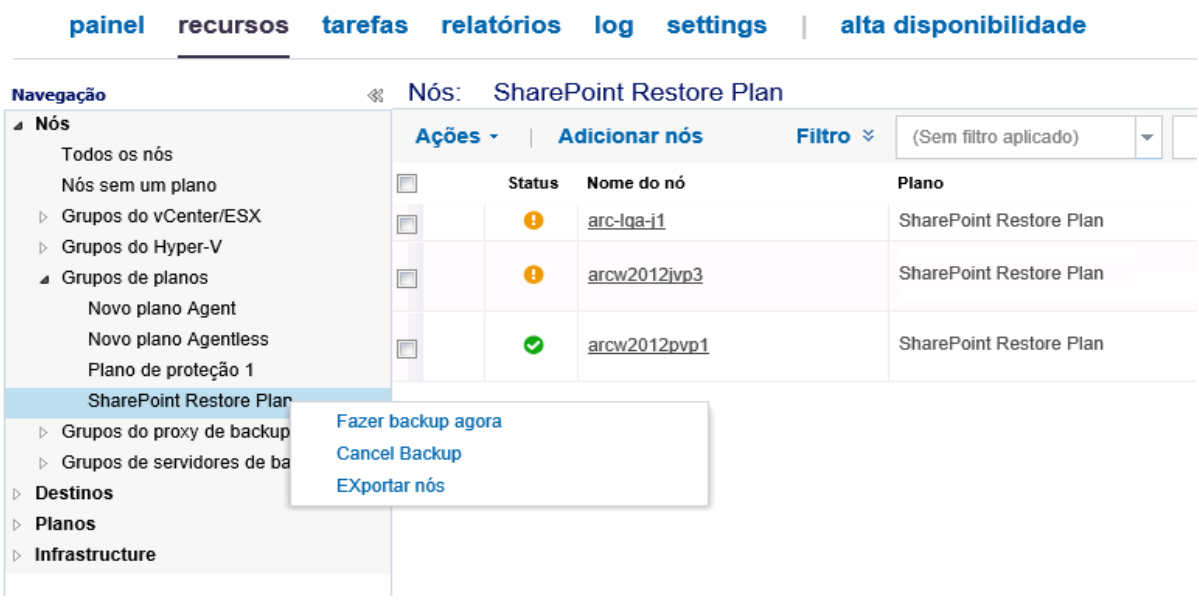
1. Efetue logon no Console.
2. Clique em **recursos** e navegue até **nós** no painel esquerdo de **navegação**.
3. Clique em **Todos os nós**.
4. Adicione todos os nós no ambiente do farm do SharePoint.
5. (opcional) Crie um repositório de dados.
6. Expanda **planos** no painel de **navegação** e clique em **Todos os planos**.
7. Clique em **Adicionar** para criar um plano.
8. Na guia **Origem**, adicione todos os nós que estão no ambiente de Farm do SharePoint.



9. Especifique outras configurações e salve o plano.

O plano é criado para o ambiente do farm do SharePoint. As configurações do plano são implantadas em todos os nós. A tarefa de backup é iniciada no horário programado.

É possível iniciar manualmente a tarefa de backup clicando em Fazer backup agora. A tarefa de backup em todos os nós de Farm do SharePoint é iniciada. Os dados são salvos no mesmo repositório de dados.



Como restaurar um ambiente do SharePoint

A restauração de granularidade a seguir é suportada:

- Farm
- Farm apenas com a configuração
- Serviços do SharePoint
- Aplicativos web
- Bancos de dados de conteúdo
- Coleções de sites
- Sites
- Listas
- Itens de lista (incluindo documentos)

Granularidades diferentes são restauradas com diferentes soluções:

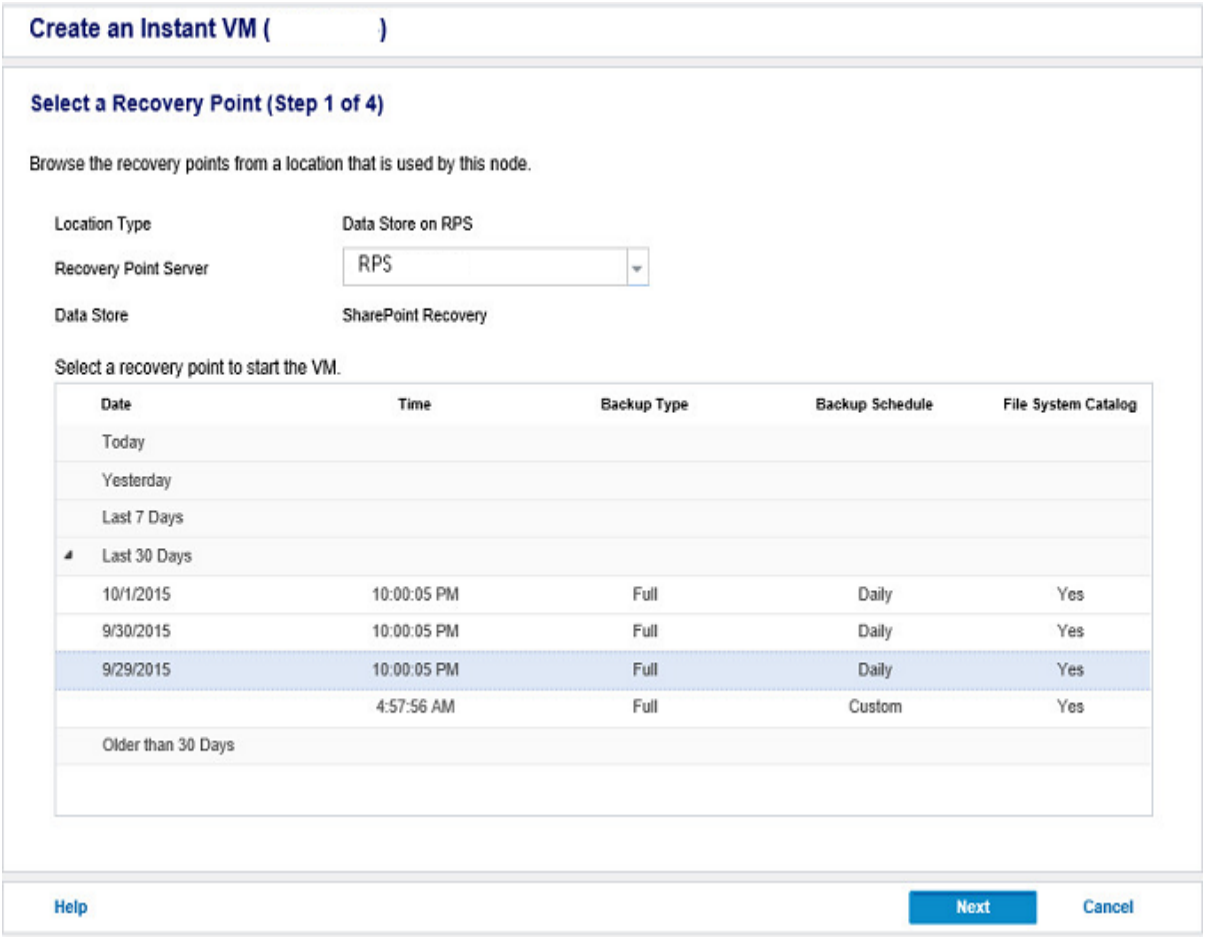
- Restaurar usando a VM instantânea: oferece suporte ao farm, farm somente com configuração, serviços do SharePoint e aplicativos web.
- Restaurar usando a interface de usuário do Agente do Arcserve UDP: oferece suporte a bancos de dados de conteúdo.
- Restaurar usando a montagem do banco de dados a partir do ponto de recuperação: oferece suporte a coleções de sites, sites, listas e itens de lista.

Restaurar usando uma VM instantânea

Siga estas etapas:

1. Efetue logon no Console.
2. Clique em **recursos**, **Nós**.
3. Clique com o botão direito do mouse no nó, que está no plano para o ambiente do SharePoint.
4. Clique em **Criar uma VM instantânea**para criar máquinas virtuais instantâneas para máquina de ambiente do SharePoint.

   O assistente do **Criar uma VM instantânea** abre.
5. Pesquise os pontos de recuperação de um local e selecione um ponto de recuperação para iniciar a VM instantânea.

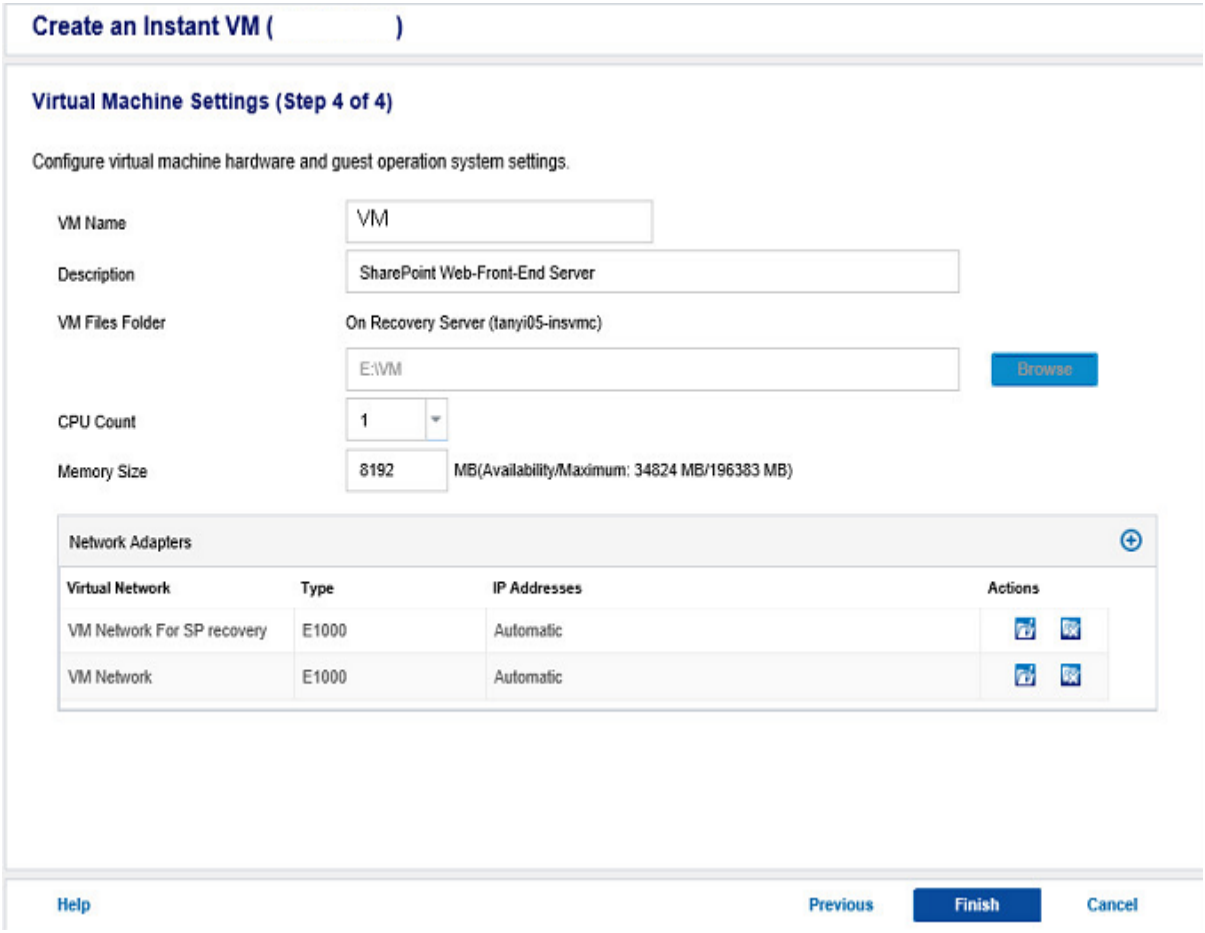


6. Clique em **Avançar**.
7. Especifique um local no VMware vSphere ou no Microsoft Hyper-V para hospedar a VM instantânea. Por exemplo: o tipo de hipervisor é o VMware vSphere.

8. Clique em **Avançar**.
9. Especifique uma máquina para executar a VM instantânea.

   Exemplo, use o RPS atual.
10. Clique em **Avançar**.
11. Defina as configurações de hardware e do sistema da VM instantânea.
12. Crie uma nova rede virtual como um ambiente de rede isolado para a recuperação do SharePoint. Para obter mais informações sobre como criar uma rede isolada, consulte Criar uma rede isolada para a recuperação do SharePoint.
13. Clique no sinal de mais (adição) para adicionar o adaptador de rede.
14. Selecione a rede virtual correta, que é um ambiente de rede isolada para a recuperação do SharePoint, e use a configuração padrão das configurações de TCP/IP "Source:XXX.XXX.XXX.XXX".

    Importante: Ao criar uma VM instantânea para um computador que é de servidores web front-end para o ambiente do SharePoint, adicione mais um adaptador de rede para transferir o arquivo de dados de backup. O endereço IP do novo adaptador deve estar na mesma rede virtual com os servidores web de front-end originais para o SharePoint, e no mesmo segmento de IP. Em seguida, o ambiente original do SharePoint pode usar o adaptador de rede para acessar qualquer pasta compartilhada com a VM instantânea.



15. Clique em **Concluir**.

    A caixa de diálogo Inicializar VM é exibida.

16. Clique em **Inicializar depois**.

    Cria-se uma nova VM instantânea que aparece em **Infraestruturas**, **Máquinas virtuais instantâneas** no console.

17. Crie a VM instantânea para todos os nós no ambiente do farm do SharePoint.

18. Após a criação das VMs instantâneas de todos os nós, inicie-as uma a uma.

    - Inicie o controlador de domínio primeiro e, em seguida, o servidor DNS.
    - Após isso, inicie o servidor de banco de dados e, por último, os servidores de front-end da web.

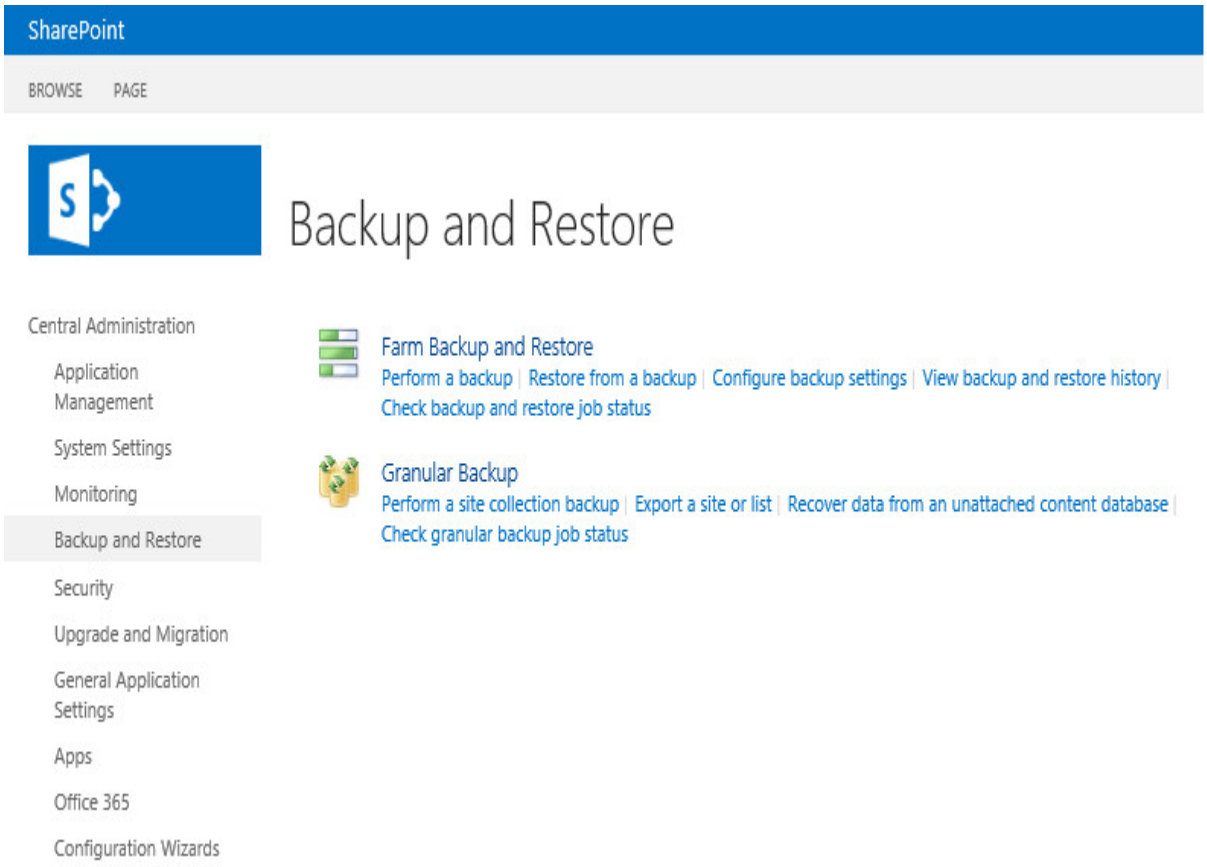
19. Clique com o botão direito do mouse na VM instantânea que você deseja iniciar e selecione **Ligar** para iniciar a VM instantânea.

20. Aguarde essas VMs instantâneas para que os computadores do ambiente do SharePoint liguem.

    O ambiente temporário do SharePoint foi configurado.

21. Efetue logon na VM instantânea em que o computador é de servidores web front-end para o ambiente do SharePoint. Abra a Administração central, clique no cabeçalho Backup e Restauração e selecione o link Execução de um backup.

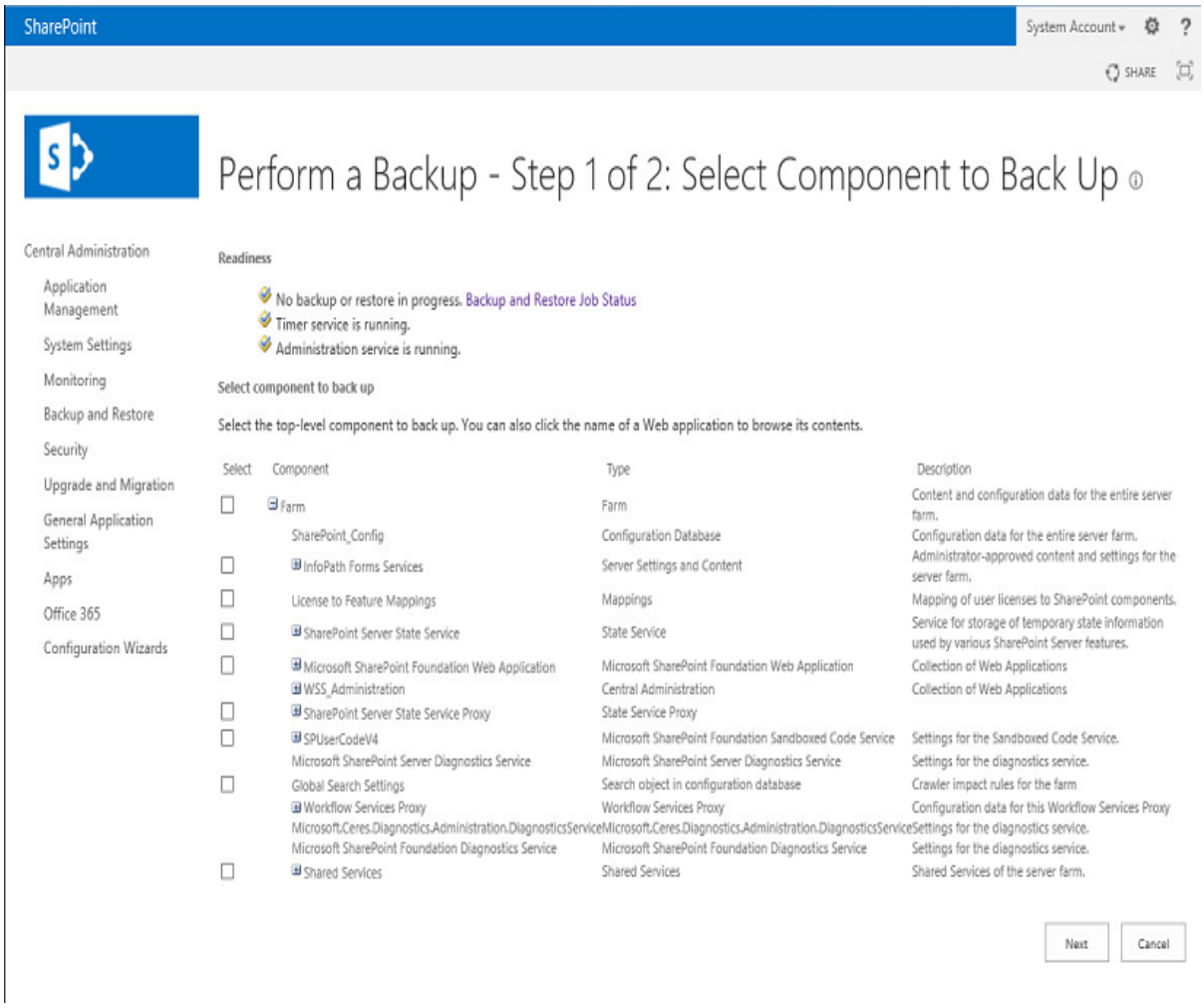
    Observação: se você receber o erro de HTTP 404 depois de abrir o aplicativo web como Sharepoint - 80, desative o protocolo IPv6 e desmarque a caixa de seleção de **Internet Protocol versão 6 (TCP/IP)** na janela Propriedades da rede de área local.



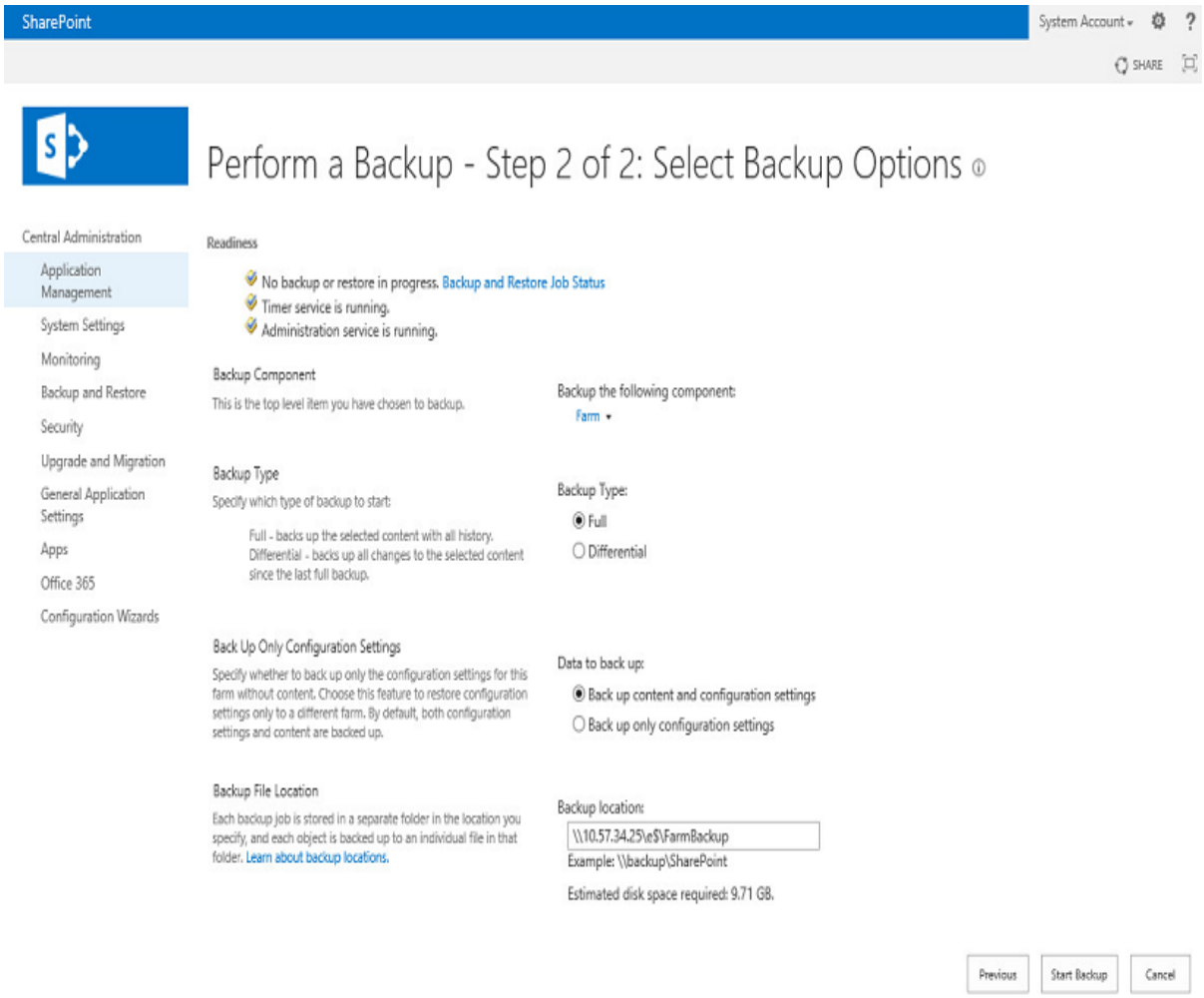
22. Selecione o componente que você deseja restaurar para o farm e clique em **Avançar**.

    Por exemplo, fazer backup do SharePoint de aplicativos web – 80. Expanda o nó Aplicativo web do Microsoft SharePoint Foundation e selecione o componente SharePoint – 80

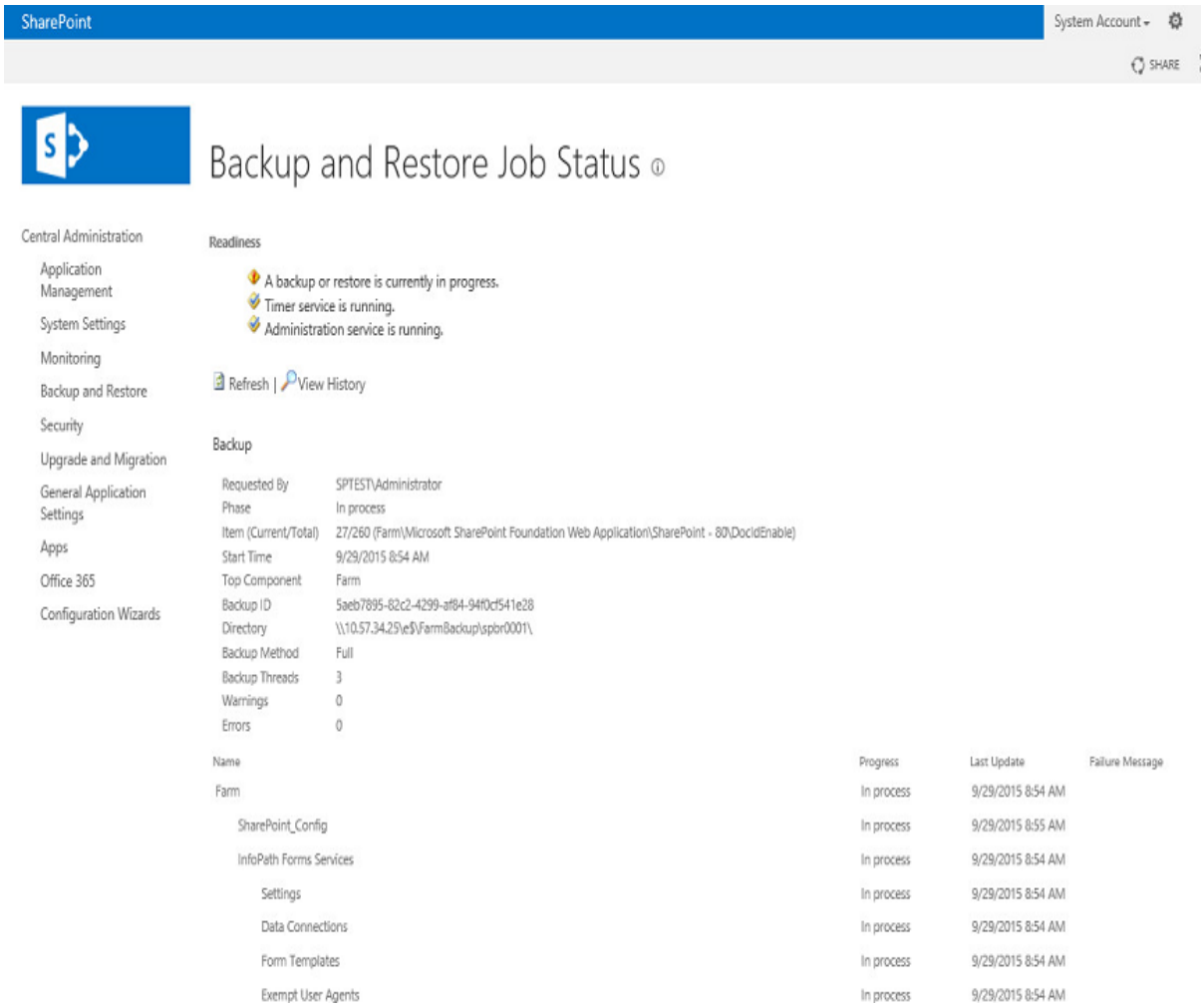
    Faça backup dos serviços de acesso. Expanda o nó Aplicativos de serviços compartilhados em Serviços compartilhados e selecione o componente Serviços de acesso 2010



23. Especifique o tipo de backup como Completo.
24. Crie uma pasta compartilhada na VM instantânea em que o computador é de servidores web front-end para o ambiente do SharePoint.
25. Forneça acesso controle total a todos na pasta compartilhada.
26. Forneça o caminho da pasta compartilhada no local do arquivo de backup para armazenar o arquivo de backup e, em seguida, clique em **Iniciar backup**.

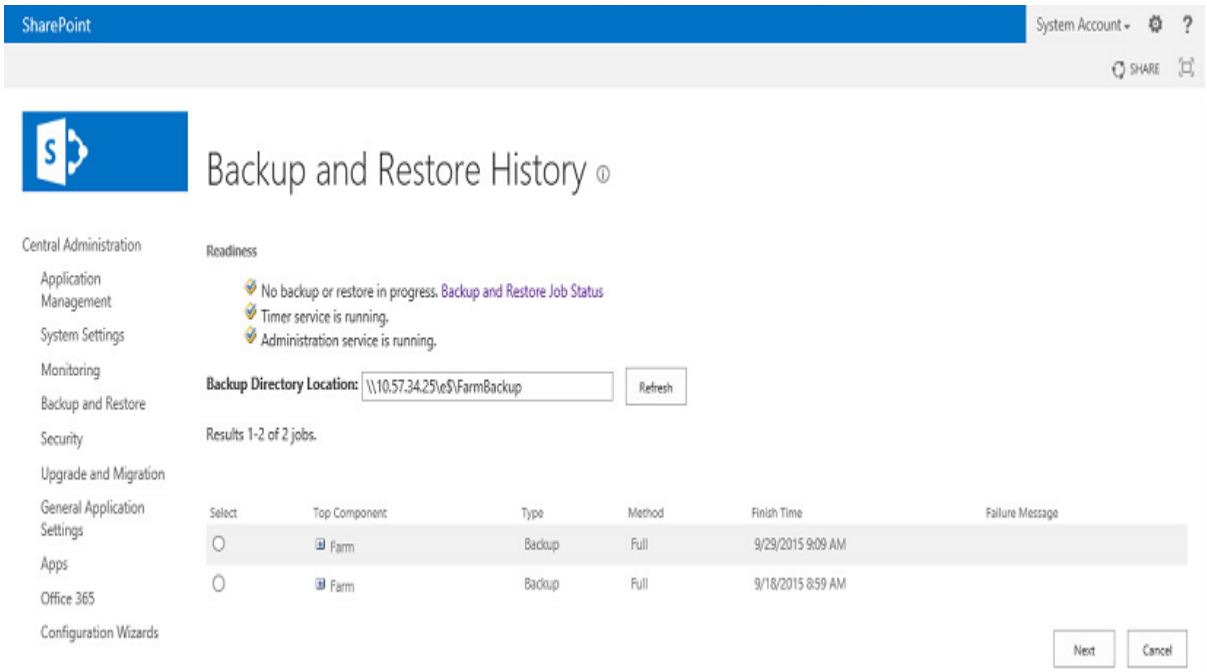


27. Aguarde até que a tarefa de backup seja concluída.



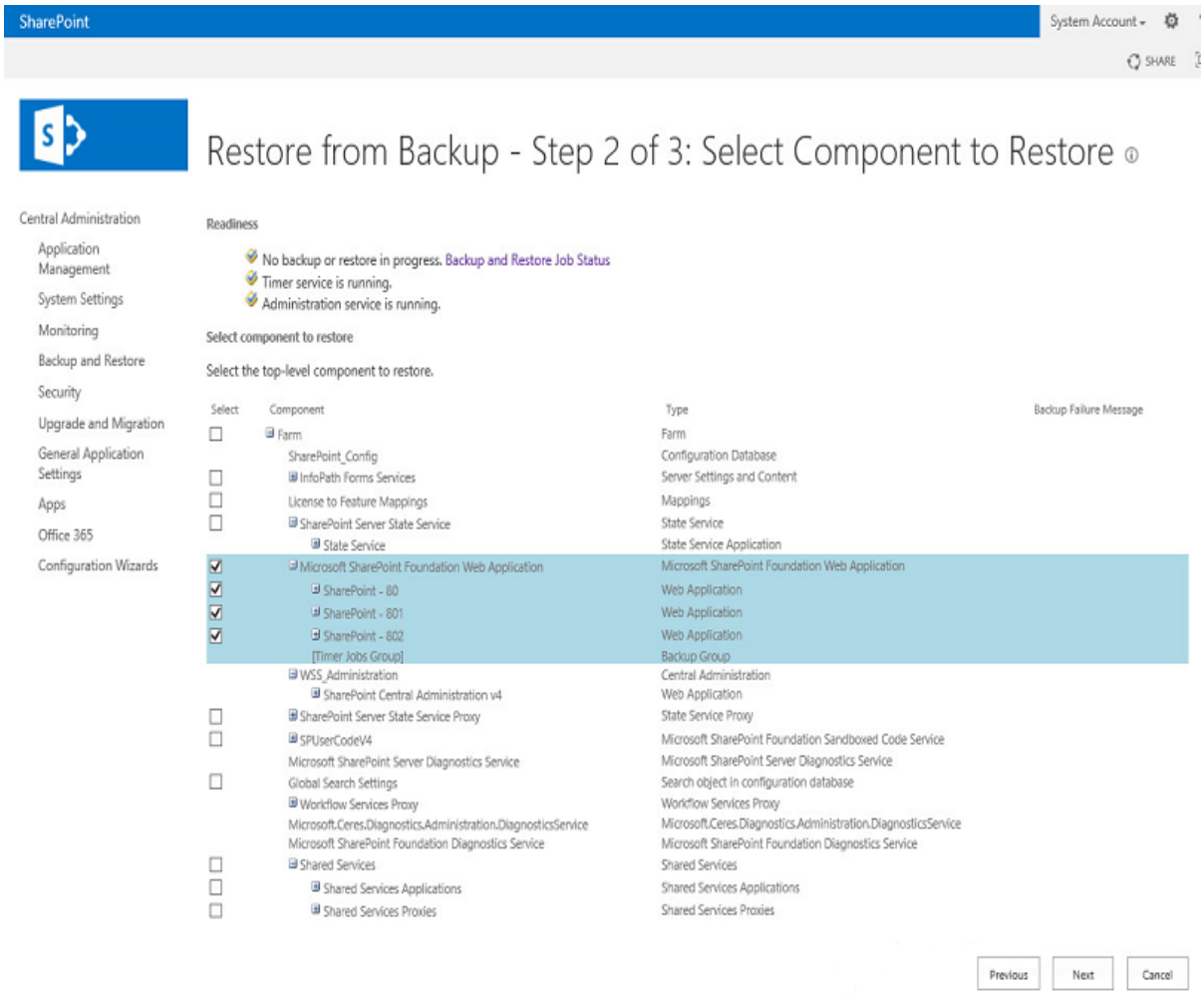
28. Após o conclusão da tarefa de backup de Farm, efetue logon no computador que é de servidores web front-end para o ambiente do SharePoint original.
29. Abra a Administração central, clique em Backup e Restauração e selecione o link Restaurar de um backup.
30. Forneça a pasta compartilhada no campo Local do diretório de backup e clique em **Atualizar**.

    Observação: a pasta compartilhada já é criada em uma das etapas anteriores.
31. Selecione a instância de backup na lista de histórico e clique no botão **Avançar**.



32. Selecione a configuração e o conteúdo no farm a serem restaurados e, em seguida, clique em **Avançar**.

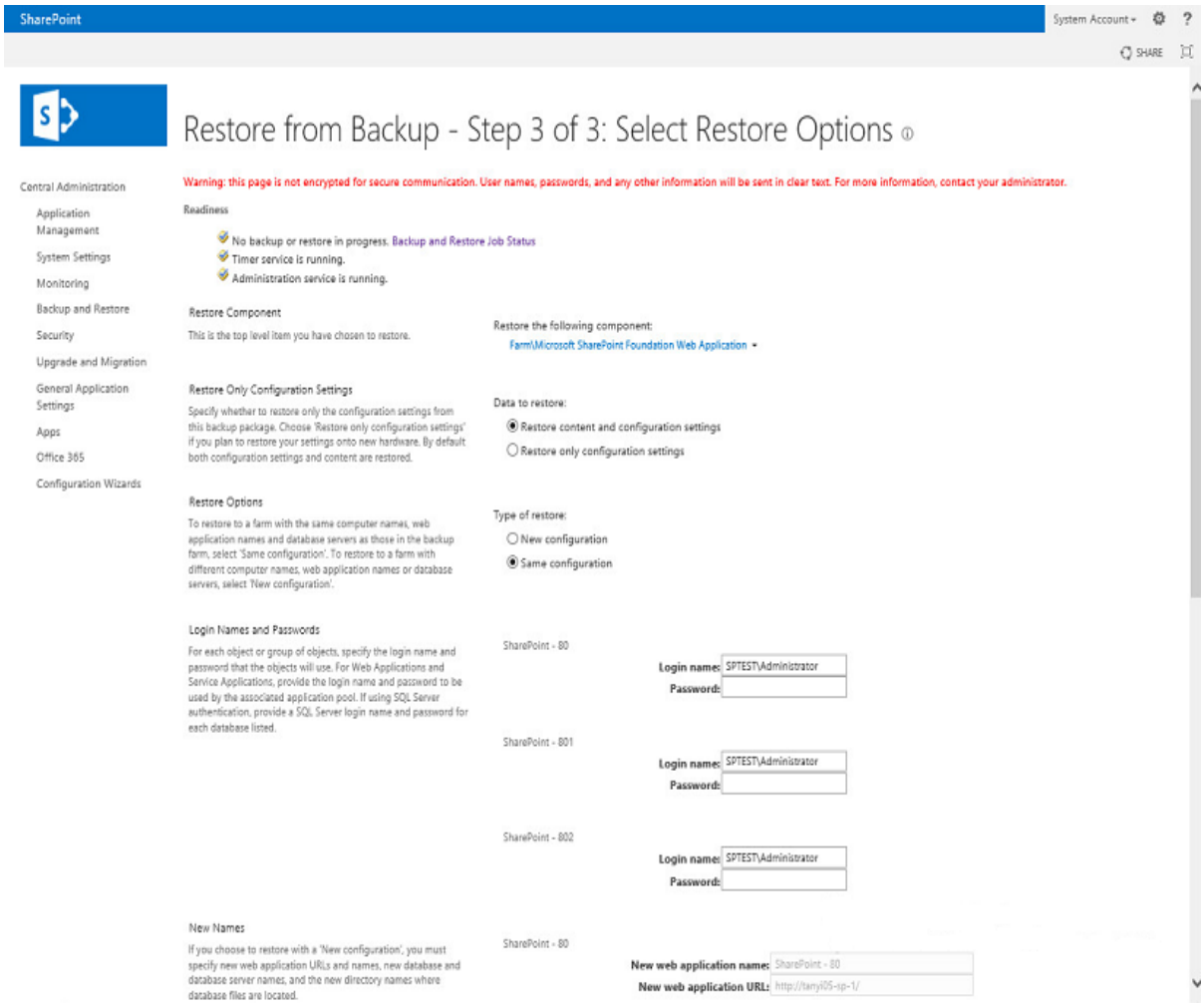
    Por exemplo, selecione todos os componentes do Farm, componentes dos serviços do SharePoint Services ou componentes dos aplicativos web.



A página exibe várias opções para o serviço selecionado e a configuração de conteúdo.

33. Escolha se deseja:

    - Restaurar as definições de conteúdo e de configuração ou Restaurar somente as definições de configuração
    - Substitua a configuração ou crie uma nova nas opções de restauração.



34. Clique no botão **Iniciar restauração** para começar o processo de restauração.

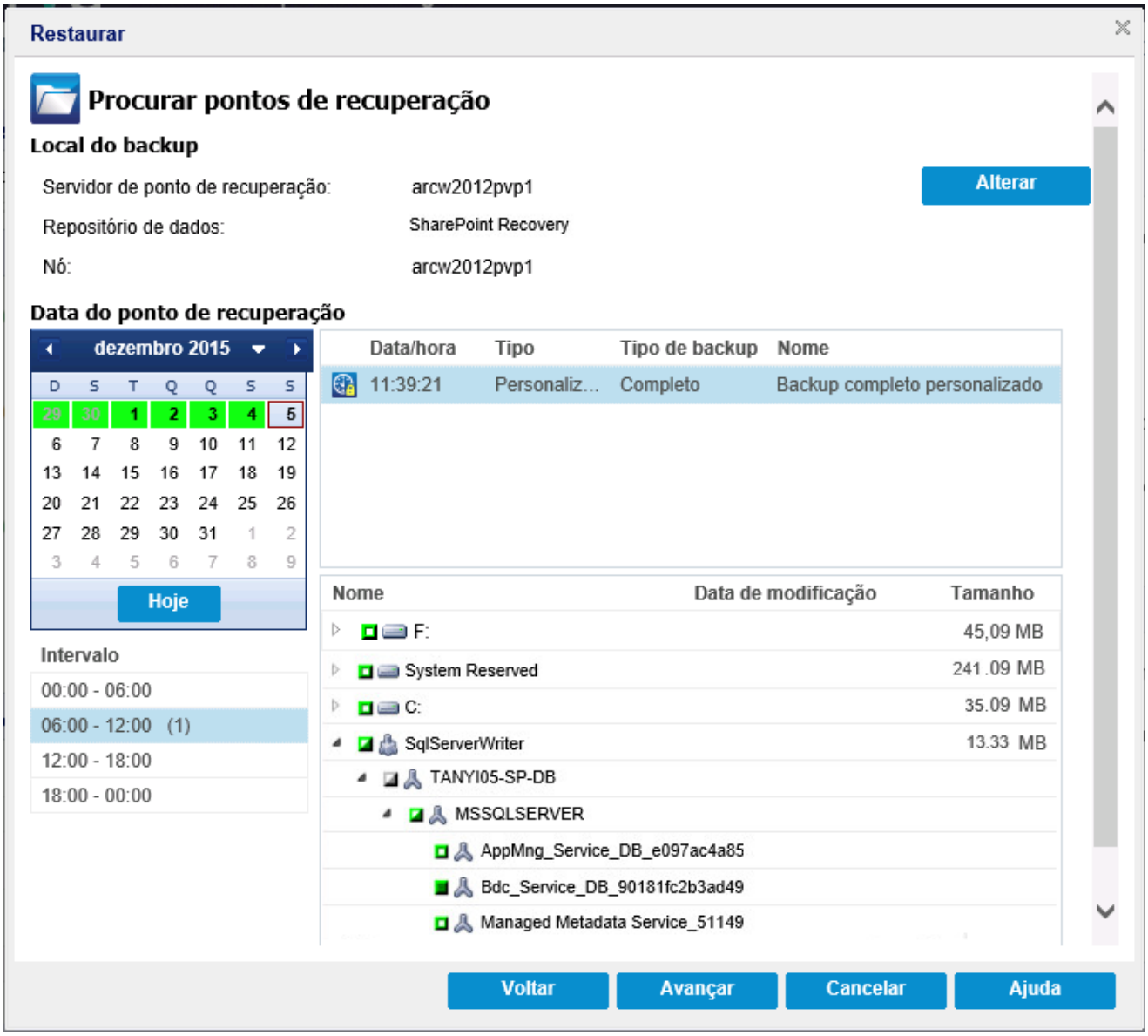
    Após a conclusão da tarefa de restauração, os componentes selecionados no Farm são restaurados.

Restaurar usando a interface de usuário do agente do Arcserve UDP

Siga estas etapas:

1. Efetue logon no console.
2. Clique com o botão direito no nó que é o servidor de banco de dados usado do SharePoint.
3. Clique em Restauração.

   A interface de usuário do agente do Arcserve UDP é aberta e é hospedada no servidor de banco de dados.
4. Selecionar pontos de recuperação do navegador.
5. Clique no ponto de recuperação que inclui o banco de dados, que será restaurado.
6. Selecionar banco de dados em SqlServerWriter/{SqlServerName}/{SqlServerInstantsName} para restaurar.
7. Clique em Avançar.



8. Selecione o destino de recuperação e clique em Avançar.

   Se você selecionar a opção “Restaurar no local original”, o banco de dados será restaurado no local original. Se você selecionar a opção “Restaurar em um local diferente”, o banco de dados será restaurado no local especificado. Nas duas situações, o banco de dados restaurado será anexado automaticamente no SQL Server. Se você selecionar “Apenas arquivo de despejo”, o arquivo de log e o arquivo de dados do banco de dados são salvos com o local especificado.

9. Clique em Concluir e aguarde até que a tarefa de restauração seja concluída.

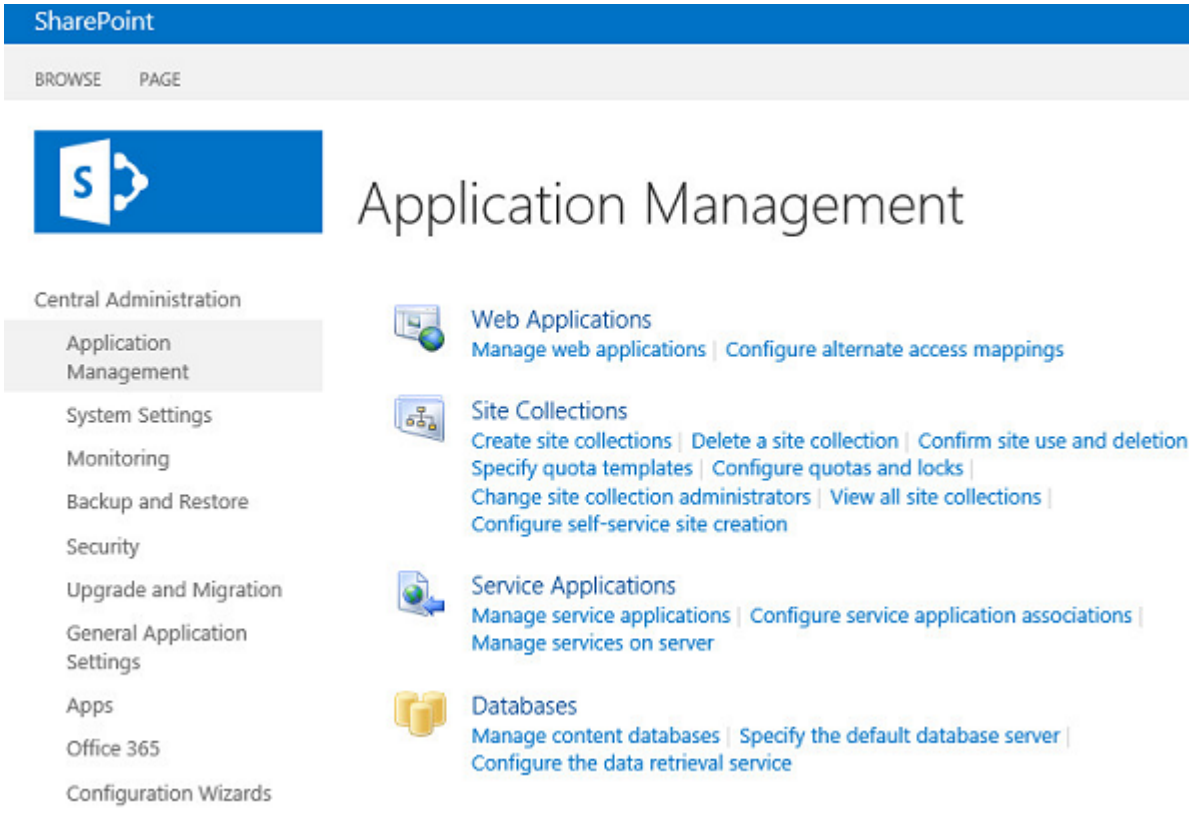
   Observação: Após selecionar "arquivo de despejo somente", conecte o banco de dados primeiro. Siga as etapas descritas em Restaurar usando montar banco de dados do ponto de recuperação e verifique se o novo banco de dados de conteúdo

está associado com seu aplicativo web original. Se não estiver, Adicionar o banco de dados de conteúdo restaurado para o aplicativo web original.

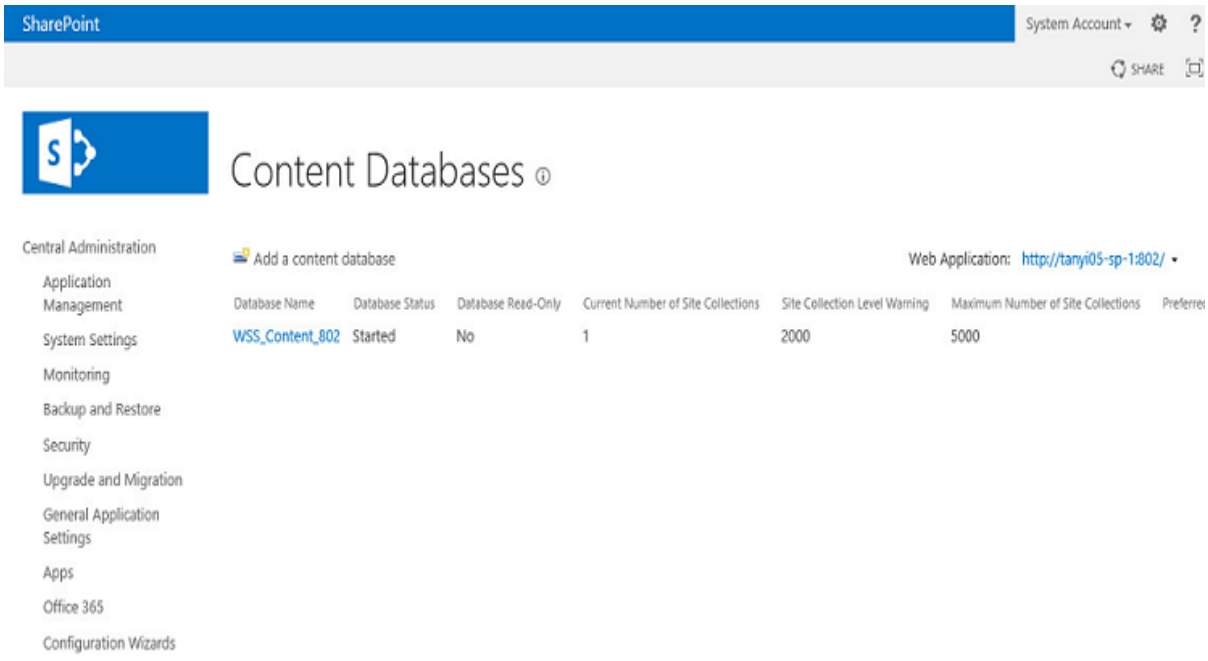
Adicionar o banco de dados de conteúdo restaurado para o aplicativo web original

Siga estas etapas:

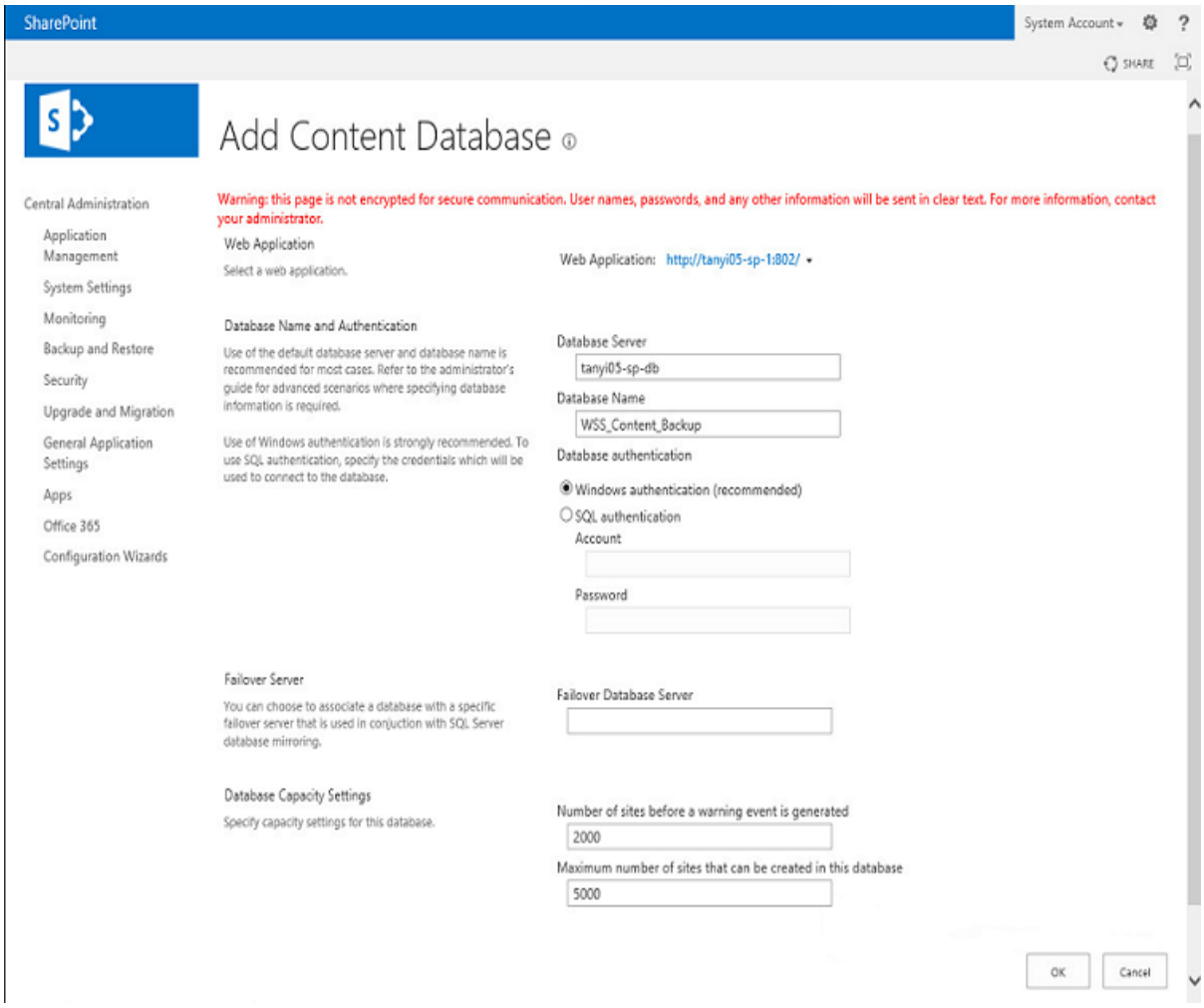
1. Abra a Administração Central do SharePoint e selecione Gerenciamento de aplicativos.



2. Selecione os bancos de dados de conteúdo do gerenciamento.



3. Selecione o aplicativo web e clique em Adicionar um banco de dados de conteúdo.
4. Digite o servidor de banco de dados e o nome do banco de dados, (por exemplo, WSS_Content_Backup) e, em seguida, clique em OK.

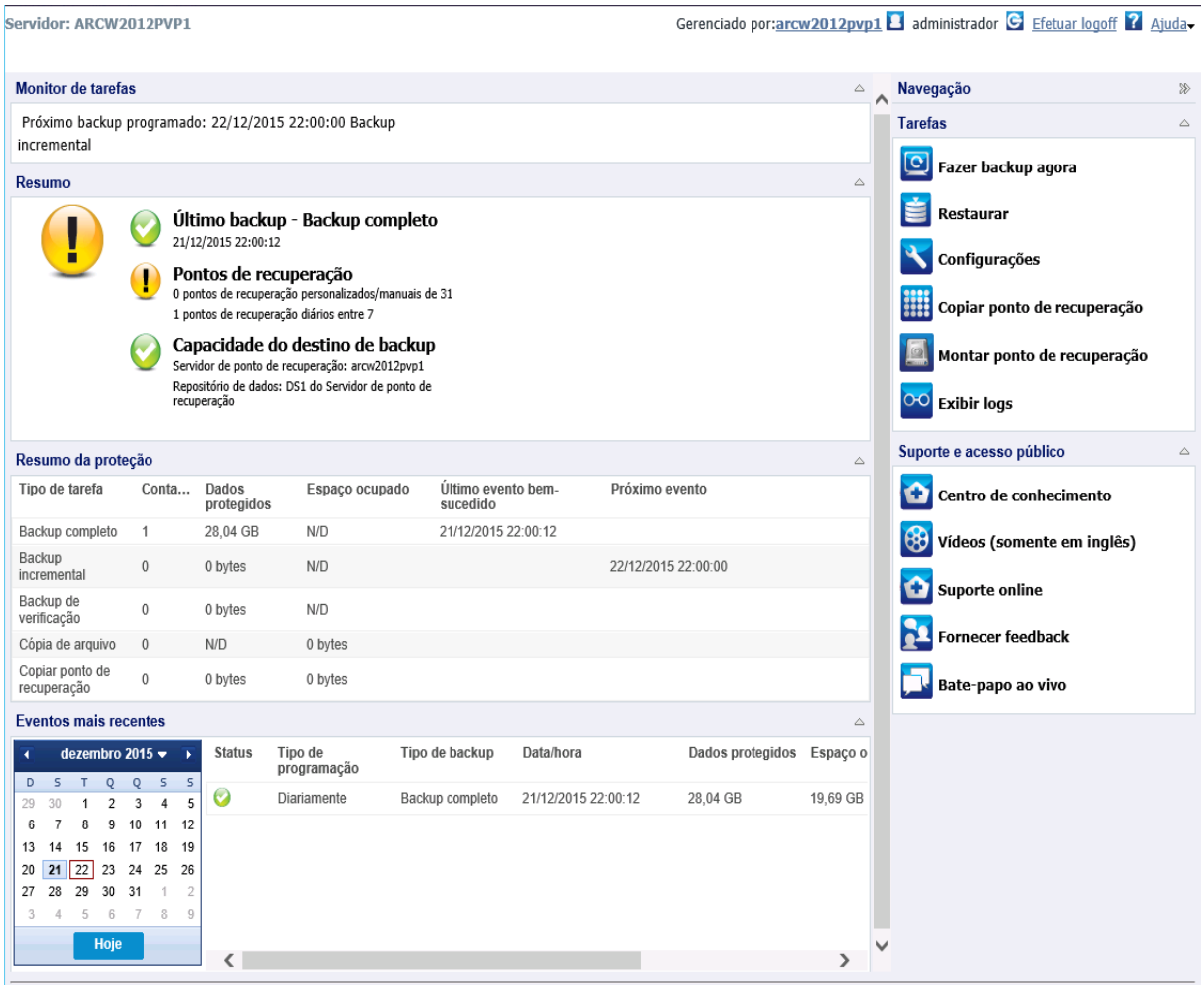


Agora, o banco de dados de conteúdo está associado a seu aplicativo web original.

Restaurar usando Montar banco de dados do ponto de recuperação

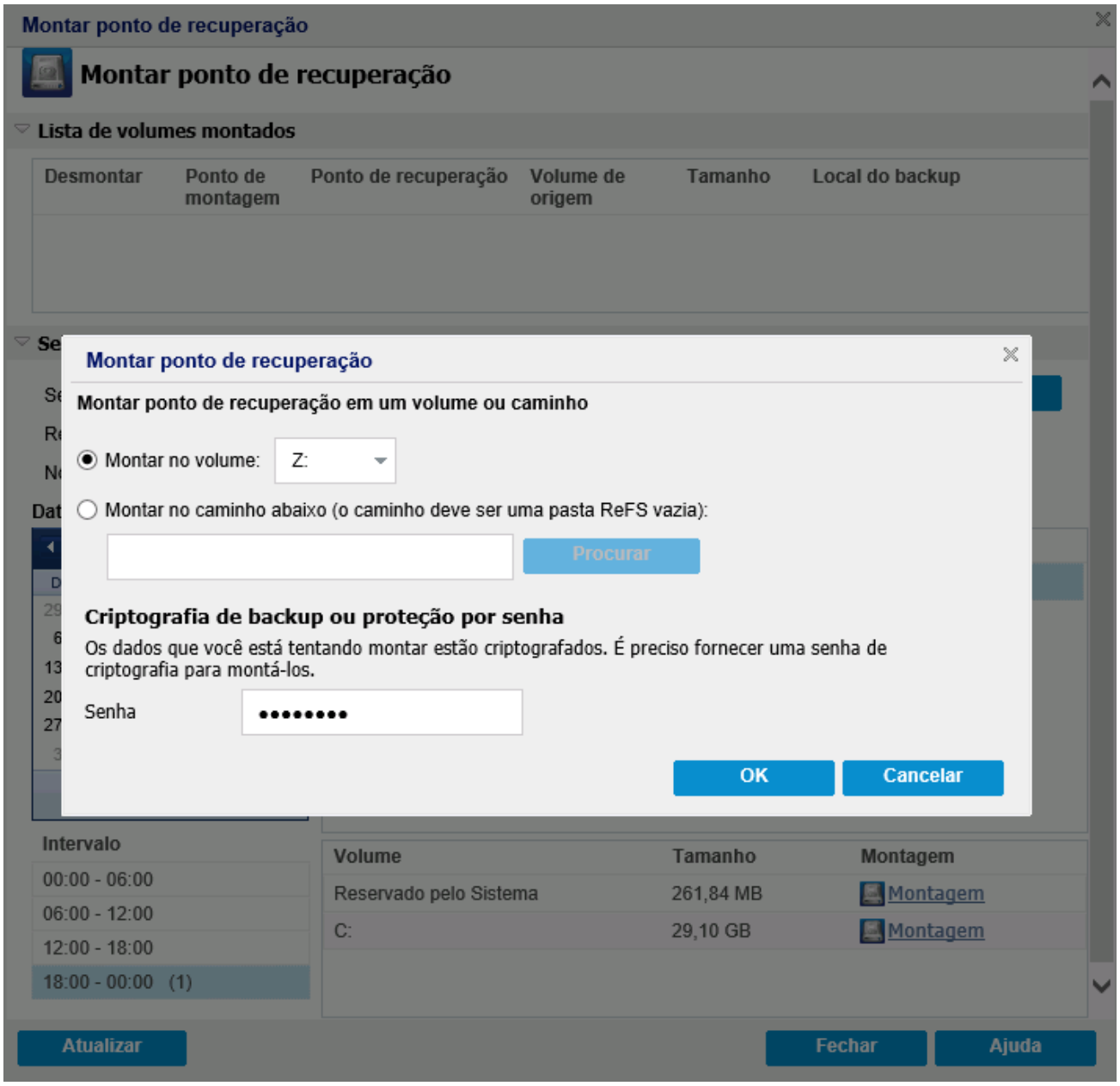
Siga estas etapas:

1. Abra a interface do agente do Arcserve UDP que é hospedada no servidor de banco de dados.

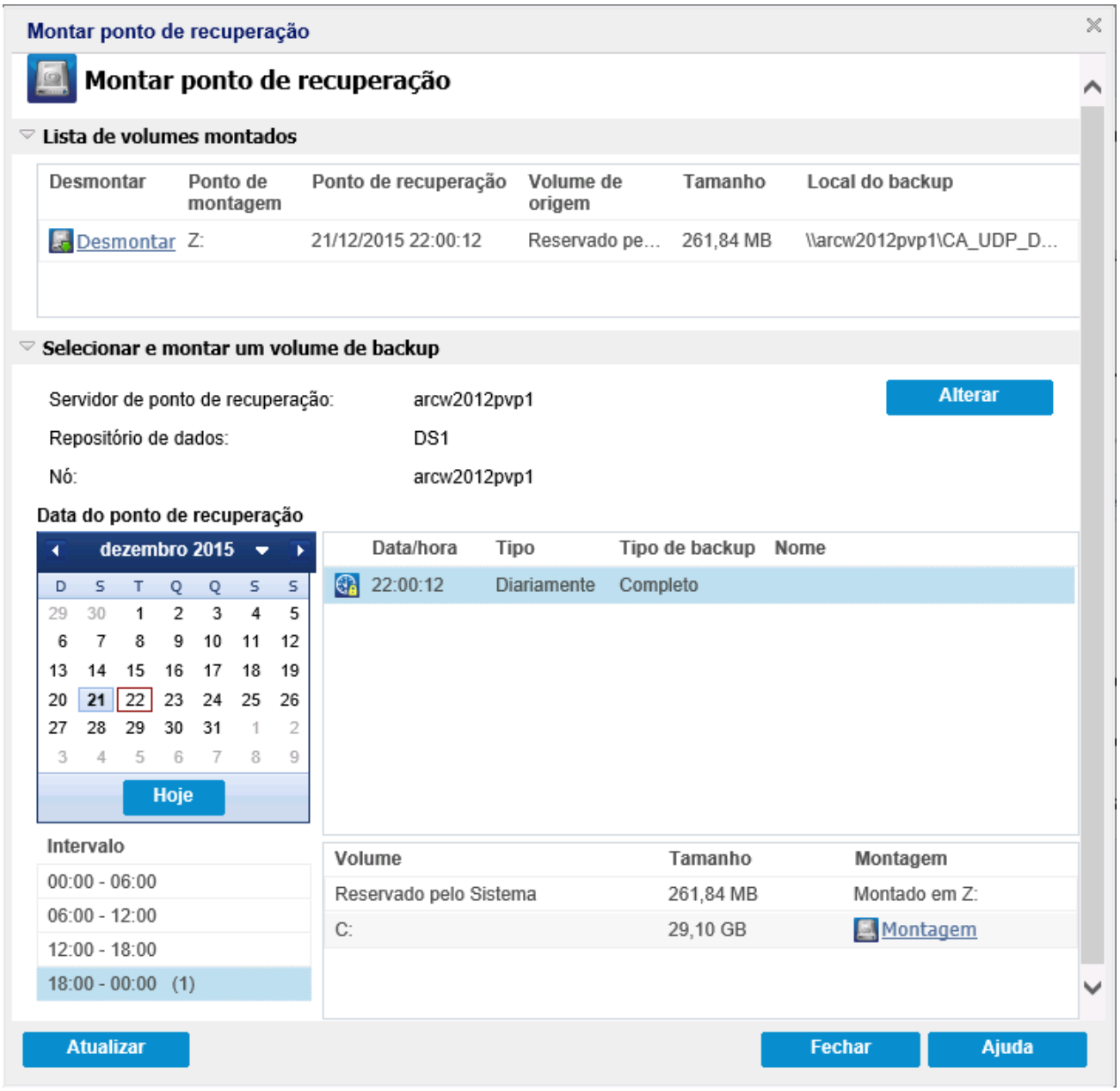


2. Clique em **Montar ponto de recuperação** no painel Tarefas.
3. Selecione o volume que inclui o banco de dados do SQL Server para o SharePoint.

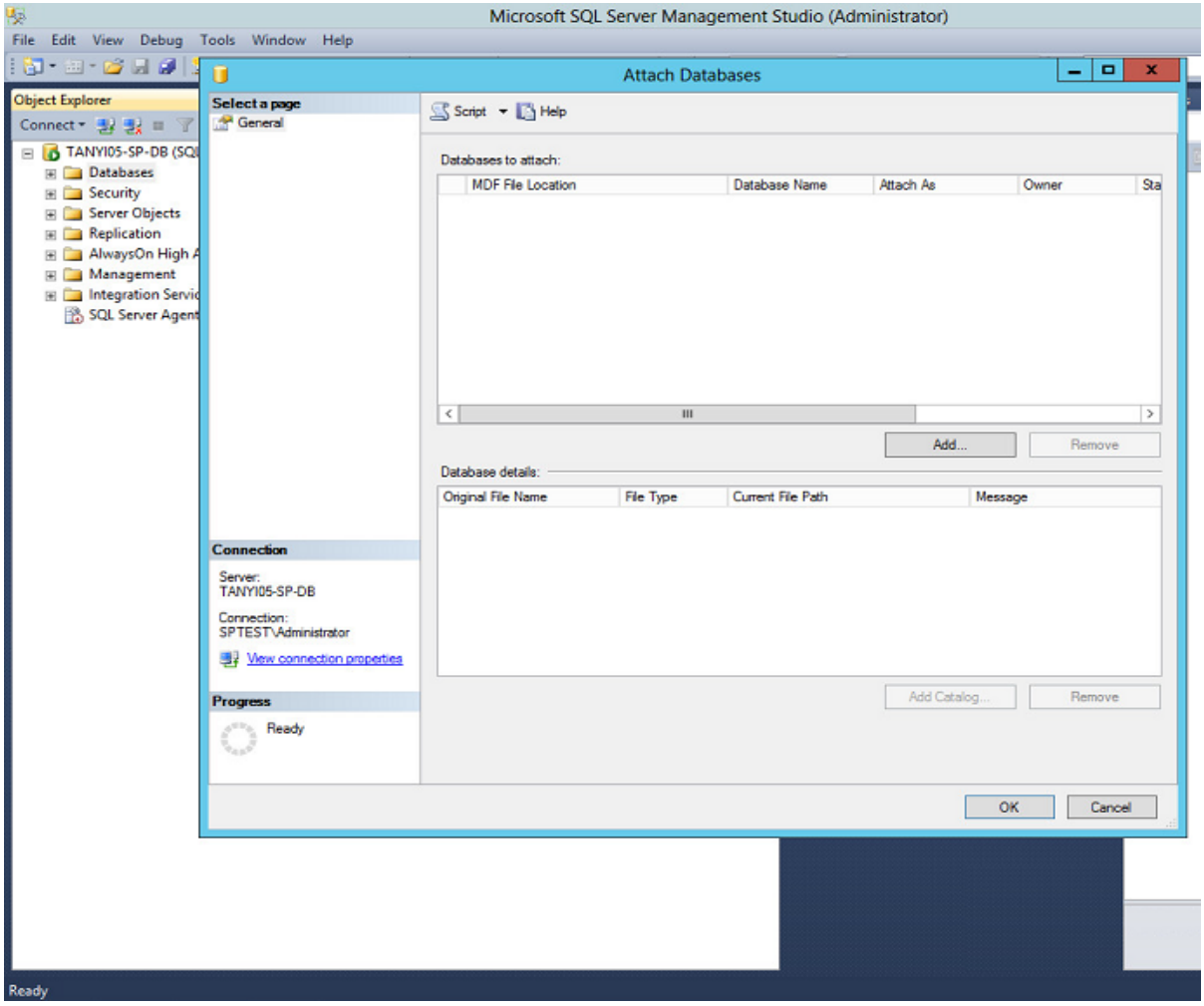
   Por exemplo, por padrão, o arquivo de banco de dados será salvo em "C:\Arquivos de Programas\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA", e você seleciona o volume C.
4. Selecione um novo nome de volume para montar na seguinte caixa de diálogo e clique em **OK**.



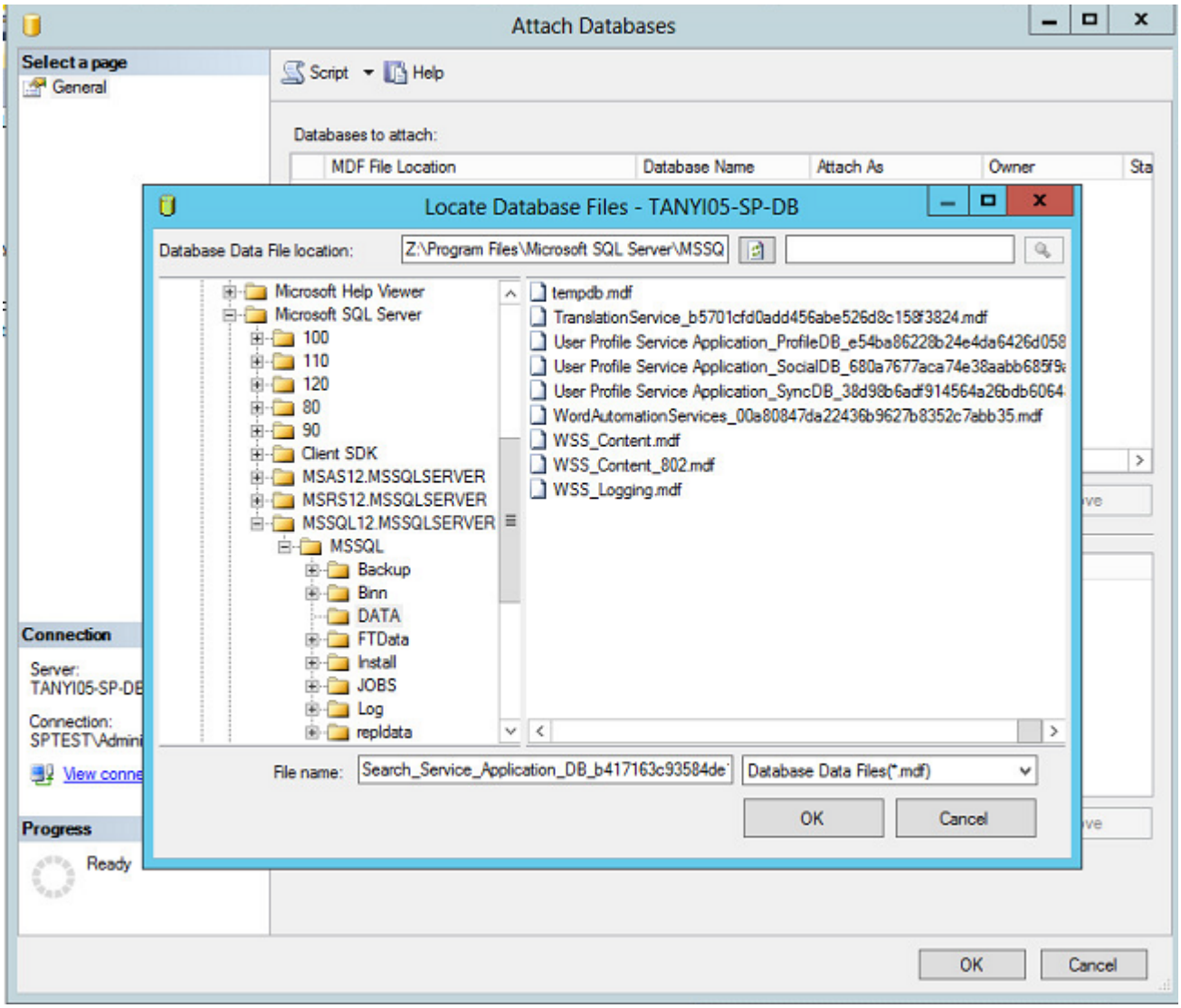
O novo volume é listado nos Volumes montados na interface do usuário.



5. Abra o SQL Server Management Studio para anexar o banco de dados de backup.
6. Clique com o botão direito do mouse na pasta Bancos de dados e selecione Anexar.



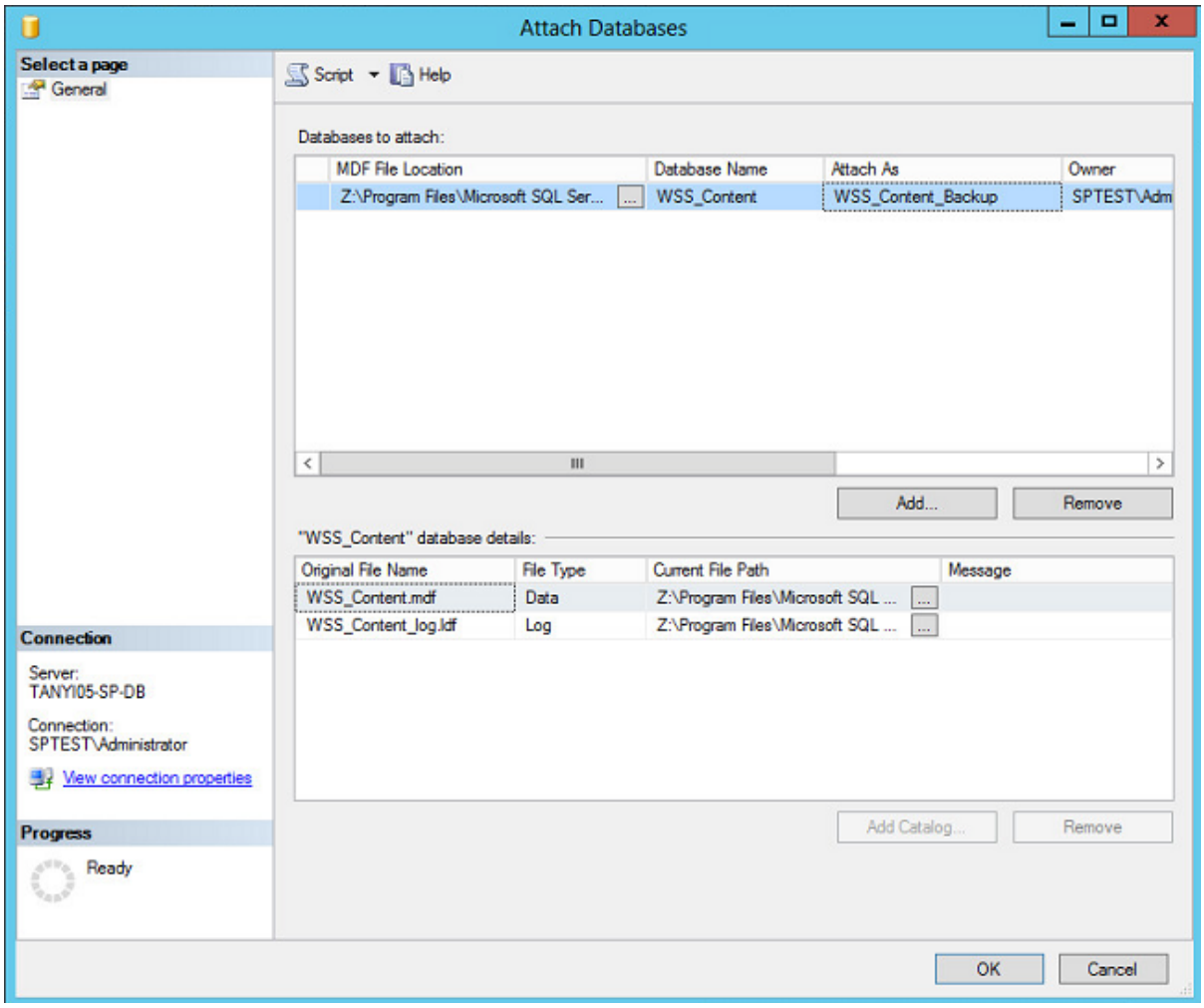
7. Clique em Adicionar para selecionar o arquivo de banco de dados que você deseja anexar.



8. Se o volume montado for Z, selecione o local do arquivo de dados do banco de dados como "Z:\Arquivos de Programas\Microsoft SQL Server\MSSQL12.MSSQLSERVER\MSSQL\DATA".
9. Selecione o arquivo chamado "WSS_Content.mdf" e clique em OK.

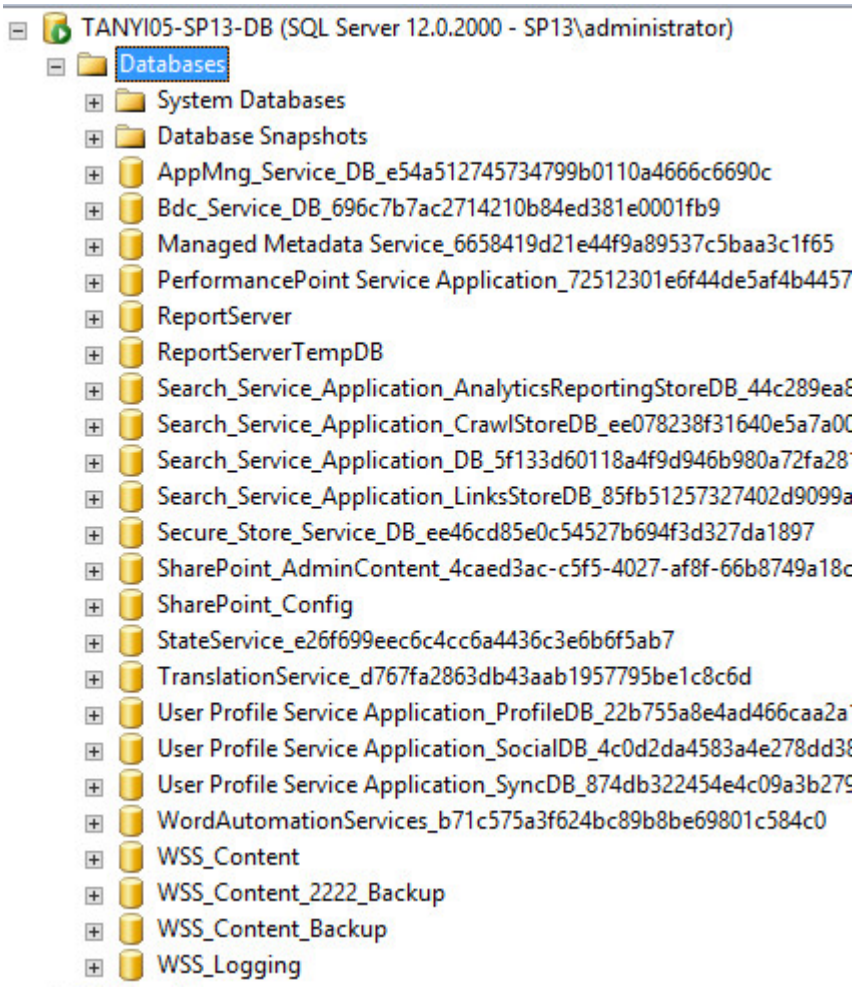
   Observação: “WSS_Content.mdf” é o nome de arquivo do dados de banco de dados padrão para o aplicativo web do SharePoint. Se você deseja restaurar outro banco de dados, criado por um novo aplicativo web, use o nome de arquivo do dados do banco de dados relacionado.
10. Clique na coluna Anexar como para digitar o nome do banco de dados (por exemplo, "WSS_Content_Backup") e clique em OK.

    Observação: antes de restaurar um banco de dados de conteúdo, certifique-se de que seu nome já não exista em outro aplicativo web.

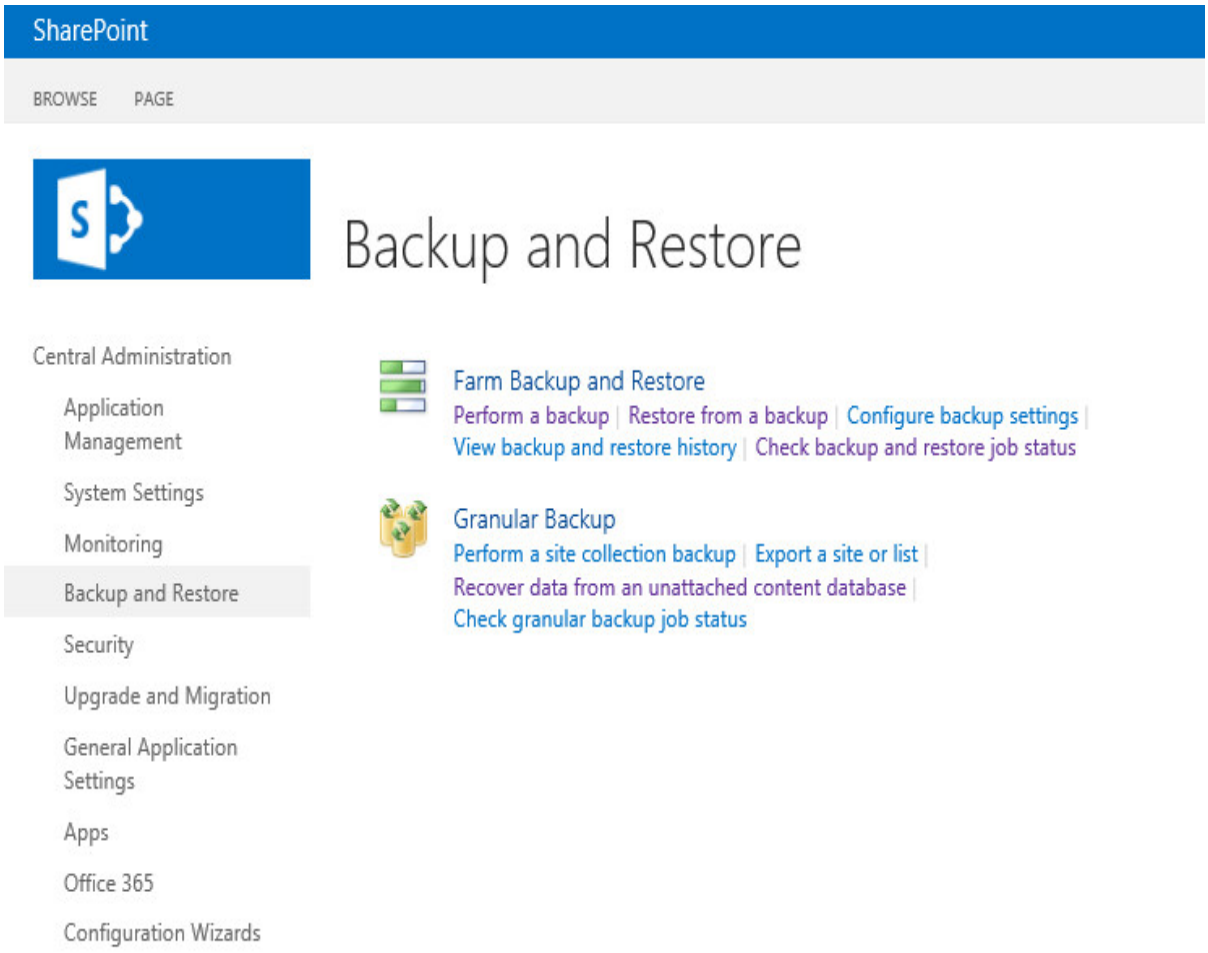


O novo banco de dados é anexado sob a pasta Bancos de dados.

Observação: o novo banco de dados não é associado a qualquer aplicativo web.

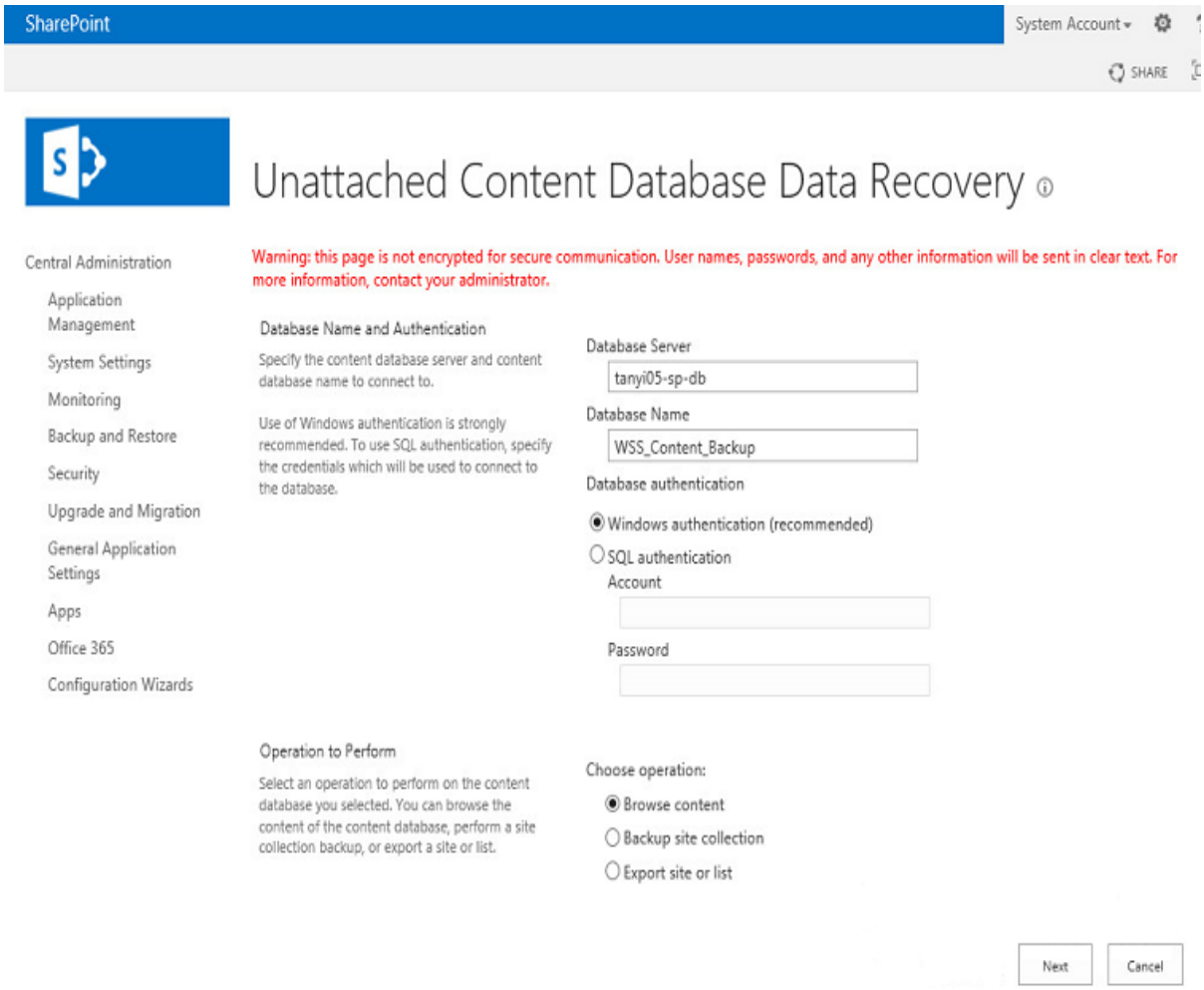


11. Efetue logon no computador que é de servidores web front-end no Farm do Servidor do SharePoint.
12. Abra a Administração central e clique no cabeçalho Backup e Restauração.



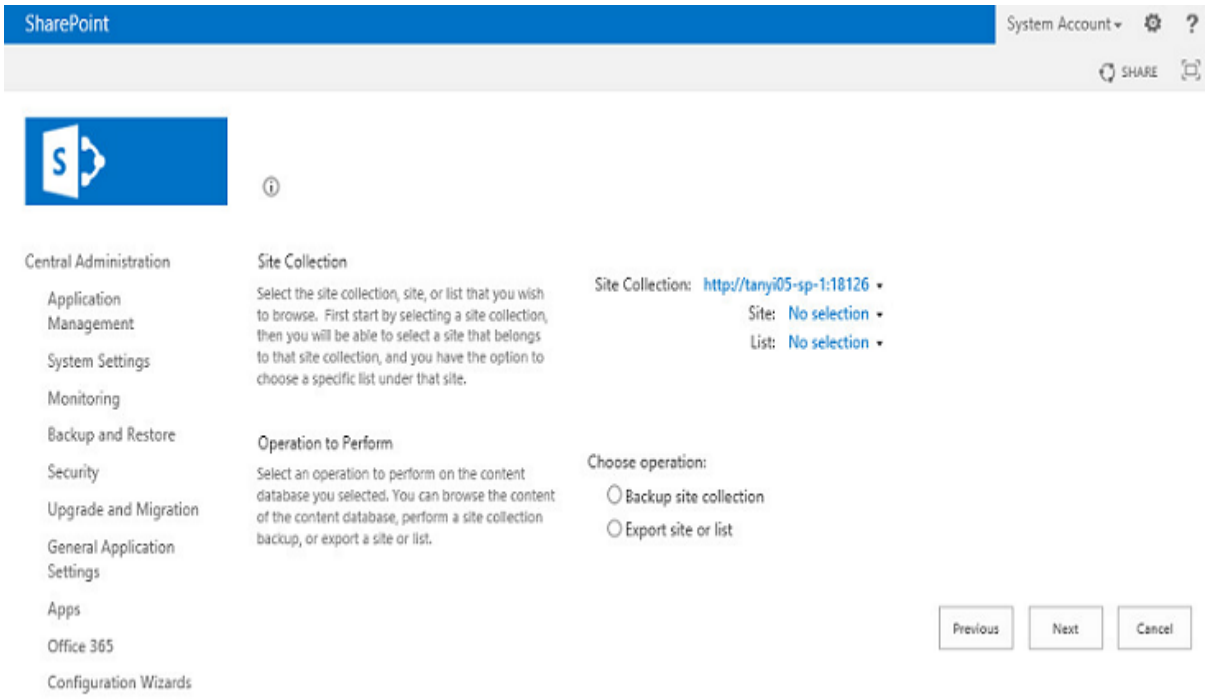
13. Clique em Recuperar dados a partir de um link Banco de dados de conteúdo desanexado e forneça o nome do SQL Server e o nome do banco de dados para o banco de dados desanexado e use a autenticação do Windows.
14. Selecione a opção Procurar conteúdo e clique em **Avançar**.

    Observação: o nome SQL Server é o nome dos servidores de banco de dados usados pelo farm do SharePoint Server, o nome Banco de dados é o nome do banco de dados conectado recentemente.



15. Escolha se deseja fazer backup da coleção de sites ou exportar o site e a lista selecionados.

    Observação: por padrão, se o banco de dados for um banco de dados de conteúdo desanexado, o URL da coleção de sites ainda inclui o número de porta do aplicativo web da administração central.



Você restaurou usando o banco de dados de montagem de um ponto de recuperação.

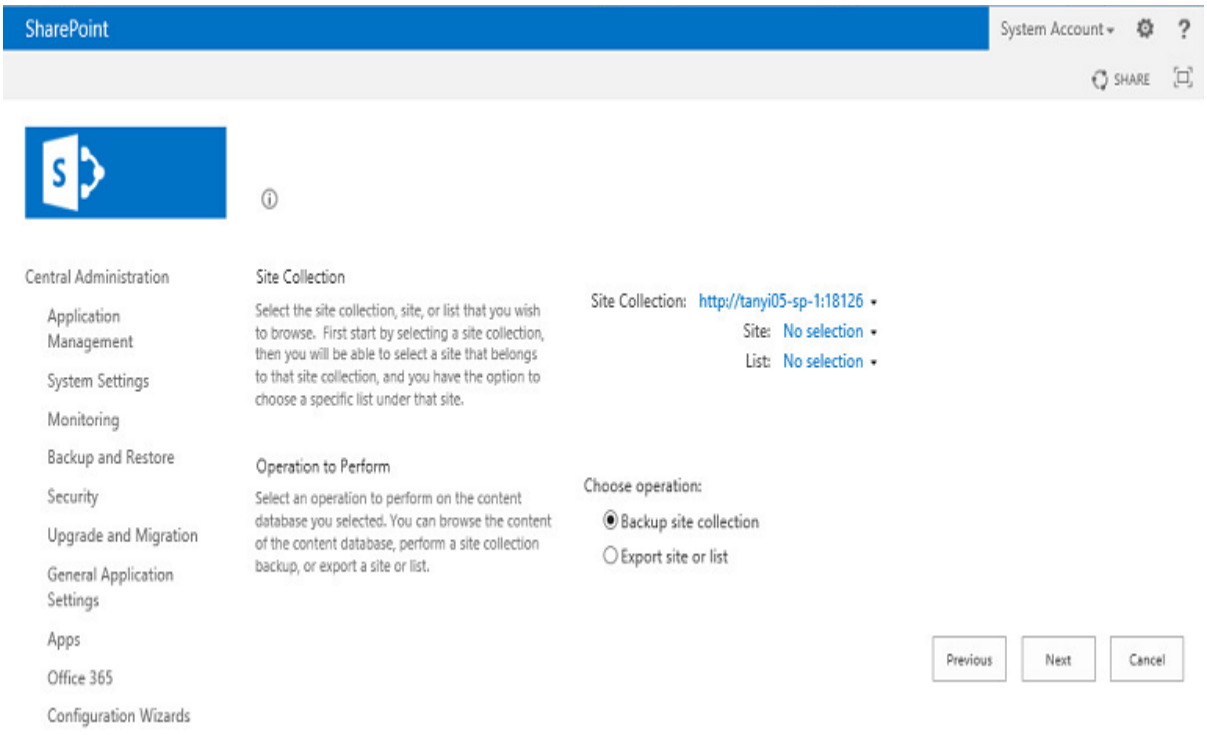
Restaurar uma coleção de sites

Siga estas etapas:

1. Recupere o conteúdo da coleção de sites de um banco de dados de conteúdo desanexado.

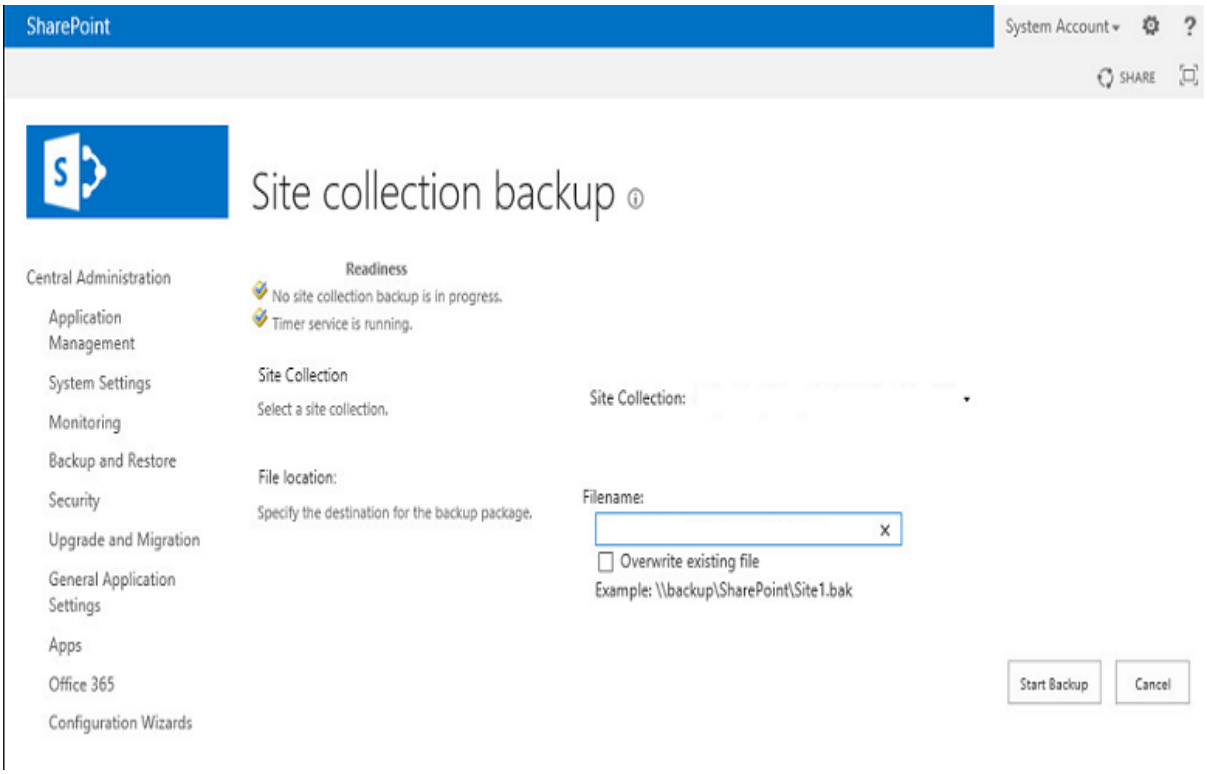
   Em Administração central

   a. Selecione a opção Backup da coleção de sites e clique em Avançar.



   b. Selecione a coleção de sites e forneça o local do arquivo do pacote de backup.

   c. Selecione Substituir arquivo existente.



d. Clique no botão Iniciar backup para iniciar o backup.

   Faz-se backup da coleção de sites em um arquivo.

Use os comandos do PowerShell

a. $database = Get-SPContentDatabase -ConnectAsUnattachedDatabase -DatabaseName xxxx -DatabaseServer xxxx

   ConnectAsUnattachedDatabase: especifica que somente bancos de dados desanexados no farm são retornados.

   DatabaseName: especifica o nome do banco de dados de conteúdo.

   DatabaseServer: especifica o nome do servidor host para o banco de dados de conteúdo especificado no parâmetro DatabaseName.

   Para obter mais informações, consulte o artigo da Microsoft.

b. Backup-SPSite -Identity xxxx -Path xxxx

   Identity: especifica o URL ou o GUID da coleção de sites cujo backup será feito.

   Path: especifica o caminho completo do arquivo de backup (por exemplo, C:\-backup\sitecollection.bak).

   Para obter mais informações, consulte o artigo da Microsoft.

2. Clique em Shell de Gerenciamento do SharePoint para iniciar o console.

3. Use os comandos do PowerShell para restaurar a coleção de sites.

```
Restore-SPSite -Identity xxxx -Path xxxx
```

Identity: especifica o local do URL no qual a coleção de sites será restaurada. (por exemplo, http://www.contoso.com).

Path: especifica um caminho válido do local de backup.(Por exemplo, C:\-backup\sitecollection.bak)

Para obter mais informações, consulte o artigo da Microsoft.

Observação: a restauração de uma coleção de sites no local original falhará. Também é possível executar as seguintes etapas:

a. New-SPContentDatabase -Name xxxx -DatabaseServer xxxx -WebApplication xxxx

   Name: especifica o novo banco de dados de conteúdo a ser criado no farm.

   DatabaseServer: especifica o nome do servidor host para o banco de dados de conteúdo especificado no parâmetro Name.

   WebApplication: anexa o banco de dados de conteúdo ao aplicativo web do SharePoint especificado.

b. Restore-SPSite -Identity xxxx -Path xxxx -GradualDelete -DatabaseServer xxxx -DatabaseName xxxx

   Identity: especifica o local do URL no qual a coleção de sites será restaurada. (por exemplo, http://www.contoso.com).

   Path: especifica um caminho válido do local de backup.(Por exemplo, C:\-backup\sitecollection.bak)

   GradualDelete: especifica que a coleção de sites sendo sobrescrita com o parâmetro Force deve ser gradualmente excluída com o passar do tempo, por uma tarefa de timer, em vez de excluir tudo de uma só vez. Reduz o impacto nos produtos do SharePoint 2010 e no desempenho do SQL Server.

   DatabaseName: especifica o banco de dados de conteúdo do SQL Server no qual os dados da coleção de sites serão armazenados.

   DatabaseServer: especifica o nome do SQL Server que contém o banco de dados de conteúdo especificado pelo parâmetro DatabaseName.

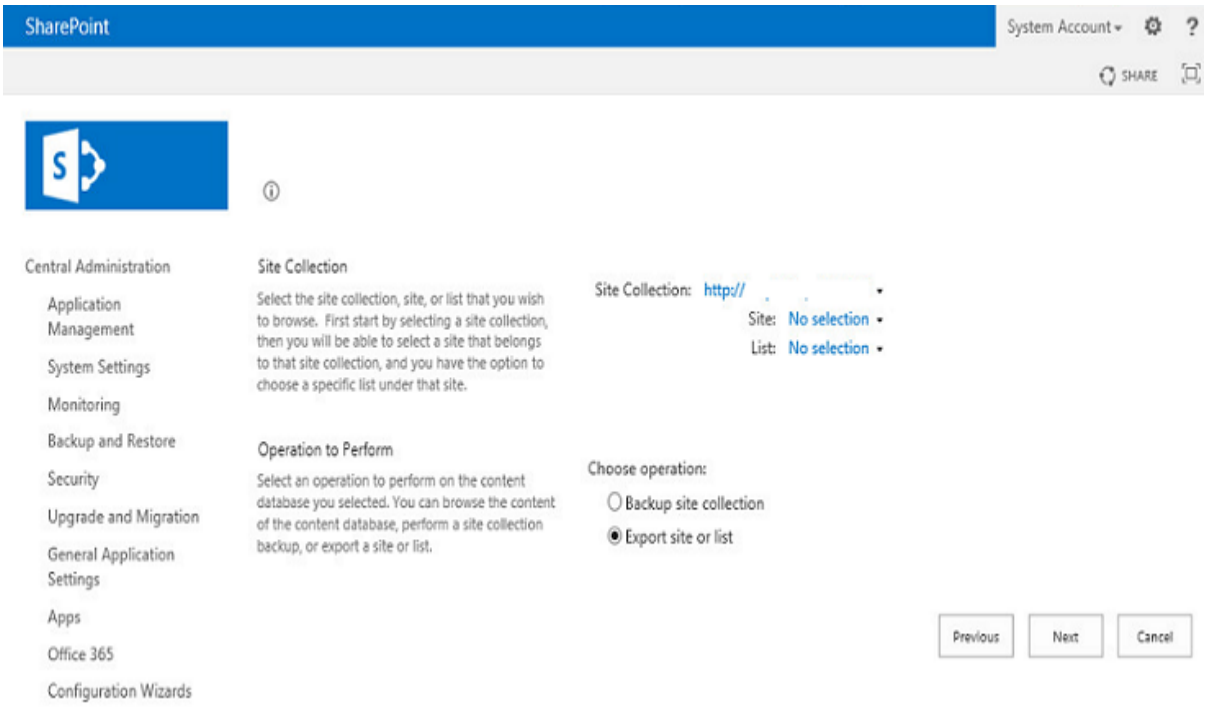
Restaurar um site

Siga estas etapas:

1. Recupere o conteúdo do site de um banco de dados de conteúdo desanexado.

   Usar a Administração central

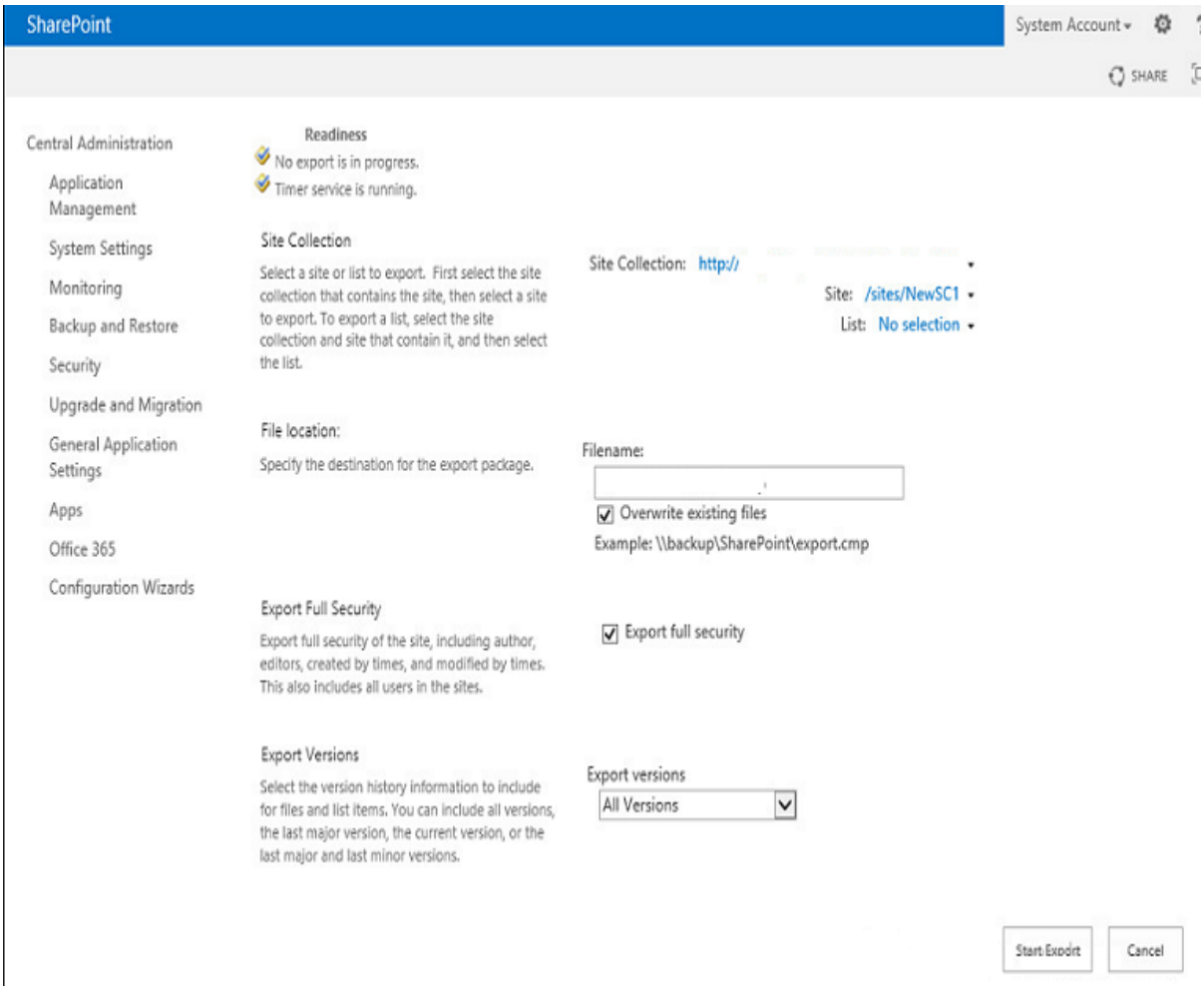
   a. Selecione o local de exportação ou a opção de lista e clique no botão Avançar.



   b. Selecione o local e forneça o local do arquivo do pacote de exportação.

      Exemplo: o nome do local a ser restaurado é LocaldeTeste1 e o URL é /LocaldeTeste1/.

   c. Selecione as opções de segurança e de versões (por padrão Todas as versões).



d. Clique no botão Iniciar exportação para começar a exportação e, em seguida, o local é exportado para um arquivo.

Use os comandos do PowerShell

a. $database = Get-SPContentDatabase -ConnectAsUnattachedDatabase -DatabaseName xxxx -DatabaseServer xxxx

ConnectAsUnattachedDatabase: especifica que somente bancos de dados desanexados no farm são retornados.

DatabaseName: especifica o nome do banco de dados de conteúdo.

DatabaseServer: especifica o nome do servidor host para o banco de dados de conteúdo especificado no parâmetro DatabaseName.

Para obter mais detalhes, consulte o artigo da Microsoft.

b. Objeto de configuração para exportação

$ExportObject = New-Object Microsoft.SharePoint.Deployment.SPExportObject

$ExportObject.Type = [Microsoft.SharePoint.Deployment.SPDeploymentObjectType]::Web

$ExportObject.Url = $SiteUrl

$SiteUrl: especifica a localização do URL no qual será feito backup do site.

c. Definir as configurações de exportação

$ExportSettings = New-Object Microsoft.SharePoint.Deployment.SPExportSettings

$ExportSettings.UnattachedContentDatabase = $database

$ExportSettings.SiteUrl = $CAUrl

$CAUrl: especifica o Url do site de administração central.

$ExportSettings.FileLocation = $ExportPath

$ExportSettings.LogFilePath = $ExportPath

$ExportPath: especifica o caminho para salvar o arquivo de backup (por exemplo, C:\backup).

$ExportSettings.BaseFileName = $ExportFile

$ExportFile: especifica o nome do arquivo do arquivo de backup (por exemplo, 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)

Faça backup do local em um arquivo.

$ExportJob.Run()

Para obter mais detalhes, consulte o artigo da Microsoft.

2. Clique em Shell de Gerenciamento do SharePoint para iniciar o console.
3. Use os comandos do PowerShell para restaurar o local n a localização de origem ou na nova localização.

```
Import-SPWeb -Identity xxxx -Path xxxx -Inclu-
deUserSecurity:$true -UpdateVersions:xxxx
```

Identity: especifica o URL ou o GUID da web no qual importar. Por exemplo, http://www.contoso.com.

Path: especifica o nome do arquivo de importação. Por exemplo, C:\-backup\site.cmp'

IncludeUserSecurity: preserva as configurações de segurança de usuário, exceto SPLists que têm herança desfeita e permissões de nível de item definidas.

UpdateVersions: indica como resolver situações em que uma versão do arquivo a ser importada em um site já existe nesse site. É possível selecionar uma das seguintes opções:

Adicionar: adiciona o arquivo como uma nova versão.

Substituir: substitui o arquivo atual e todas as suas versões (excluir, em seguida, inserir).

Ignorar: ignora o arquivo se ele existir no destino. O novo arquivo não é adicionado.

O valor padrão é Adicionar.

Para obter mais detalhes, consulte o artigo da Microsoft.

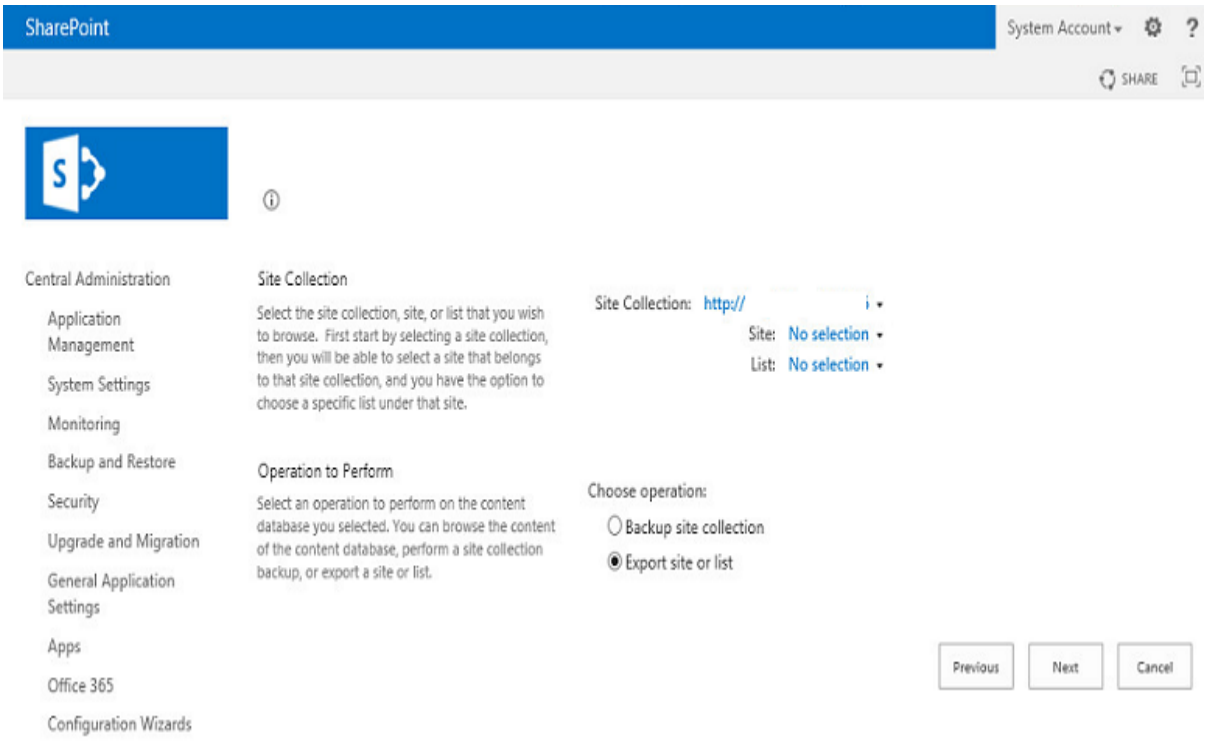
Restaurar uma lista ou uma biblioteca

Siga estas etapas:

1. Recupere de um banco de dados de conteúdo desanexado o conteúdo da lista ou da biblioteca.

   Usar a Administração central

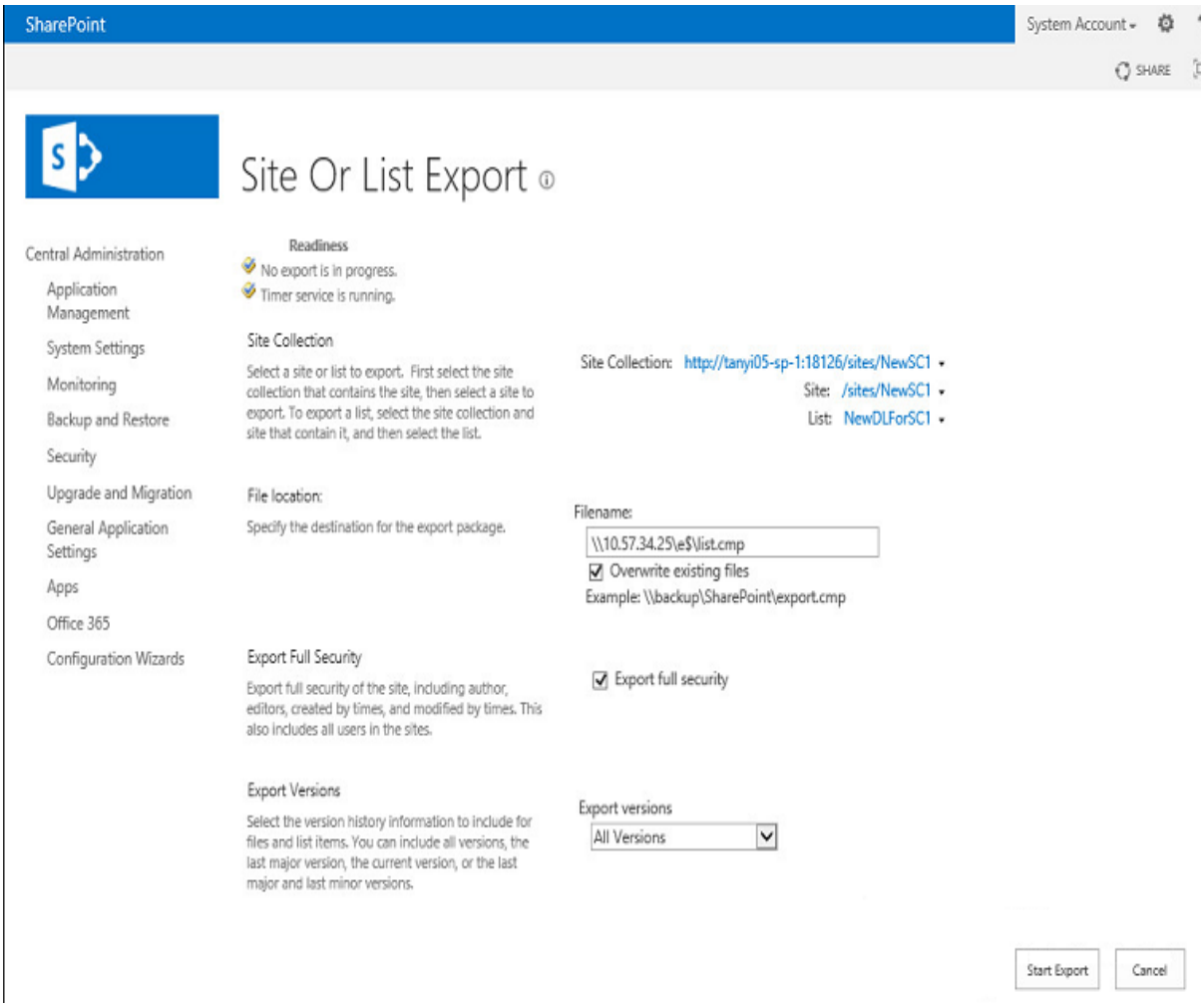
   a. Selecione o local de exportação ou a opção de lista e clique em **Avançar**.



   b. Selecione o local, a lista e forneça o local do arquivo para o pacote de exportação.

      Por exemplo: o nome de lista/biblioteca a ser restaurada é NewList1 e o URL é /TestSite1/NewList1.

   c. Selecione as opções de segurança e de versões (por padrão Todas as versões).



d. Clique em **Iniciar exportação** para começar a exportação.

   A lista ou biblioteca é exportada para um arquivo.

Use os comandos do PowerShell

a. $database = Get-SPContentDatabase -ConnectAsUnattachedDatabase -DatabaseName xxxx -DatabaseServer xxxx

   ConnectAsUnattachedDatabase: especifica que somente bancos de dados desanexados no farm são retornados.

   DatabaseName: especifica o nome do banco de dados de conteúdo.

   DatabaseServer: especifica o nome do servidor host para o banco de dados de conteúdo especificado no parâmetro DatabaseName.

   Para obter mais detalhes, consulte o artigo da Microsoft.

b. Configuração de objeto para exportação.

   $ExportObject = New-Object Microsoft.SharePoint.Deployment.SPExportObject

$ExportObject.Type = [Microsoft.SharePoint.Deployment.SPDeploymentObjectType]::List

$ExportObject.Url = $ListUrl

$ListUrl: Especifica o local do URL no qual se faz o backup da lista ou da biblioteca. Se for uma lista, use o parâmetro "/Lists/{ListName}". Se for uma biblioteca, use o parâmetro "/{LibraryName}"

c. Definir as configurações de exportação

$ExportSettings = New-Object Microsoft.SharePoint.Deployment.SPExportSettings

$ExportSettings.UnattachedContentDatabase = $database

$ExportSettings.SiteUrl = $CAUrl

$CAUrl: especifica o URL do site de administração central.

$ExportSettings.FileLocation = $ExportPath

$ExportSettings.LogFilePath = $ExportPath

$ExportPath: especifica o caminho para salvar o arquivo de backup (por exemplo, C:\backup).

$ExportSettings.BaseFileName = $ExportFile

$ExportFile: especifica o nome do arquivo do arquivo de backup (por exemplo, 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. Faça backup da lista ou da biblioteca em um arquivo.

$ExportJob.Run()

Para obter mais detalhes, consulte o artigo da Microsoft.

2. Clique em Shell de Gerenciamento do SharePoint para iniciar o console.

3. Use os comandos do PowerShell para restaurar a lista ou a biblioteca na localização de origem ou na nova localização.

```
Import-SPWeb -Identity xxxx -Path xxxx -IncludeUserSecurity:$true -UpdateVersions:xxxx
```

Identity: especifica o URL ou o GUID da web no qual importar. Por exemplo, http://www.contoso.com

Path: especifica o nome do arquivo de importação. Por exemplo, C:\-backup\list.cmp'

IncludeUserSecurity: preserva as configurações de segurança de usuário, exceto SPLists que têm herança desfeita e permissões de nível de item definidas.

UpdateVersions: indica como resolver situações em que uma versão do arquivo a ser importada em um site já existe nesse site. É possível selecionar uma das seguintes opções:

Adicionar: adiciona o arquivo como uma nova versão.

Substituir: substitui o arquivo atual e todas as suas versões (excluir, em seguida, inserir).

Ignorar: ignora o arquivo se ele existir no destino. O novo arquivo não será adicionado.

O valor padrão é Adicionar.

Para obter mais detalhes, consulte o artigo da Microsoft.

Restaurar um arquivo

Siga estas etapas:

1. Restaure a lista ou a biblioteca em um novo local. Para obter mais informações, consulte Restaurar uma lista ou uma biblioteca.

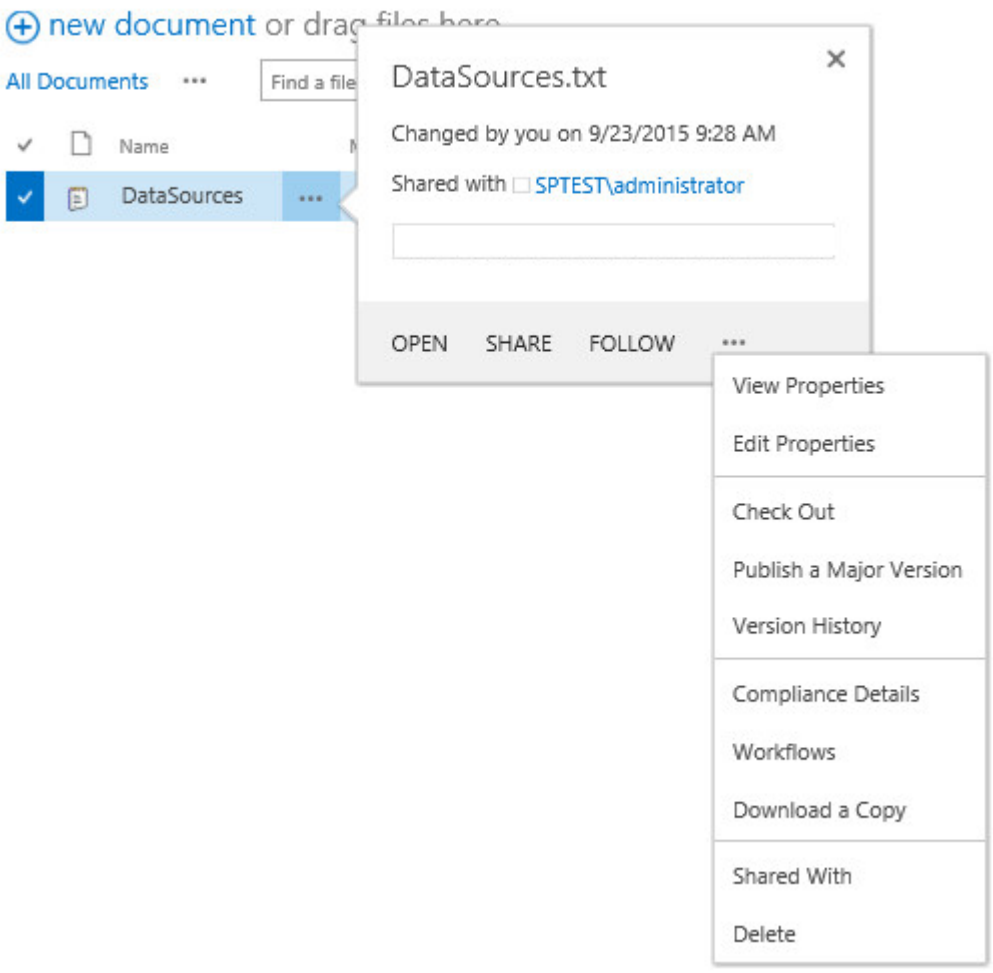
   Por exemplo: A lista de origem ou a biblioteca é chamada NewList1 e o URL é http://contoso.com/TestSite1/NewList1

   - Usando comandos do PowerShell para restaurar a lista ou a biblioteca em um novo local. Exemplo: http://contoso.com/TestSite2

     Import-SPWeb -Identity http://contoso.com/TestSite2 -Path C:\-backup\list.cmp -IncludeUserSecurity:$true -UpdateVersions:Overwrite

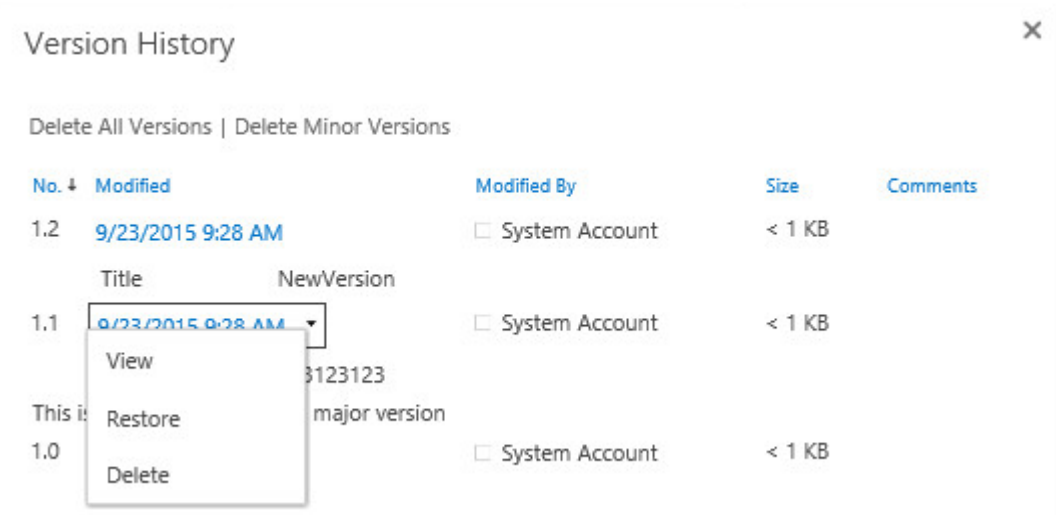
   - Navegue até o novo URL da lista ou da biblioteca. Todos os itens são restaurados em http://contoso.com/TestSite2/NewList1.

2. Navegue até o URL do novo local da lista ou da biblioteca.
3. Verifique o histórico de versão de arquivo na lista ou na biblioteca.



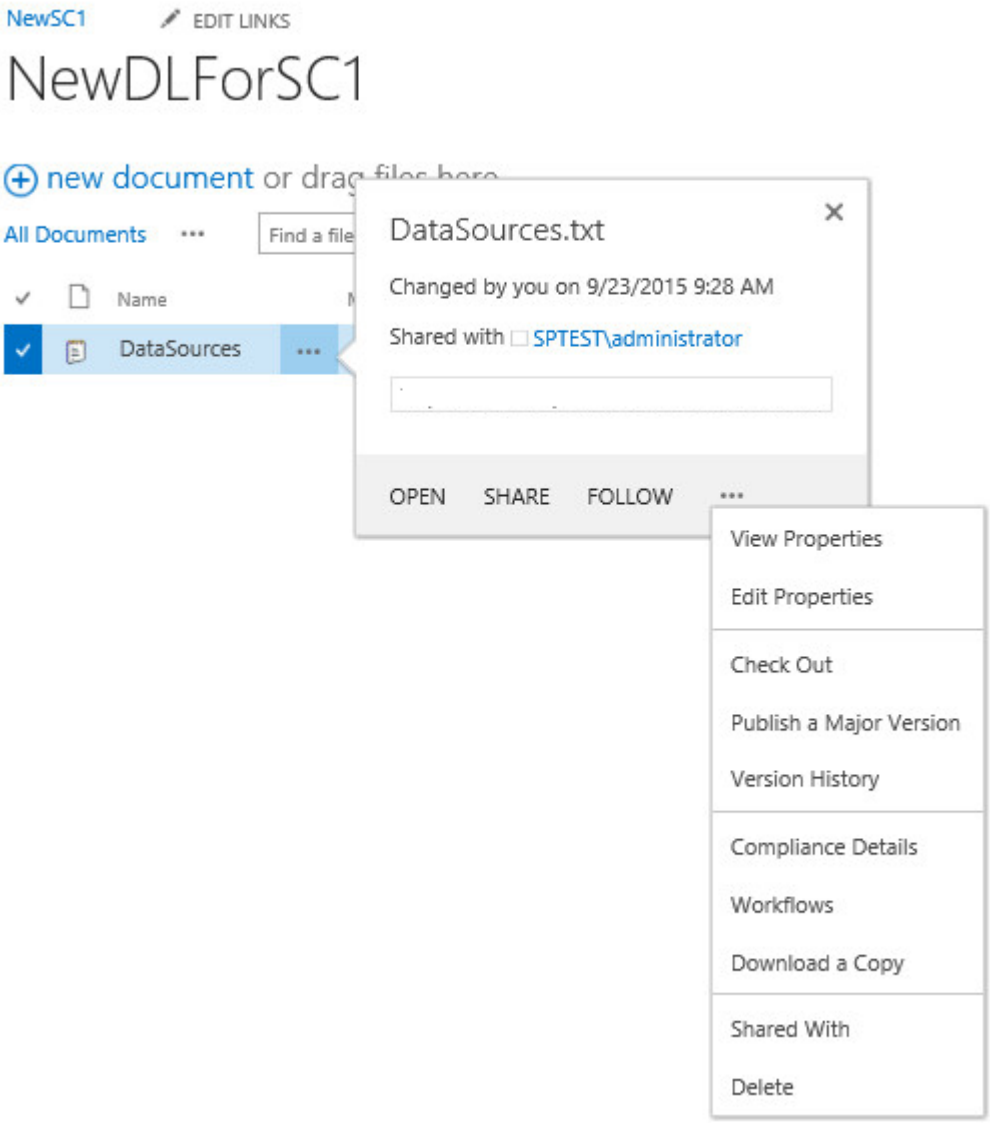
4. Selecione a versão específica do arquivo e clique em Restaurar.

   Por exemplo, restaure a versão 1.1 específica do arquivo.



   O arquivo da versão 1.1 é restaurado.

5. Clique em Fazer download de uma cópia para salvar o arquivo com a versão 1.1 específica em um local.



O arquivo salvo é restaurado na lista de origem ou biblioteca.

Criar uma rede isolada para a recuperação do SharePoint

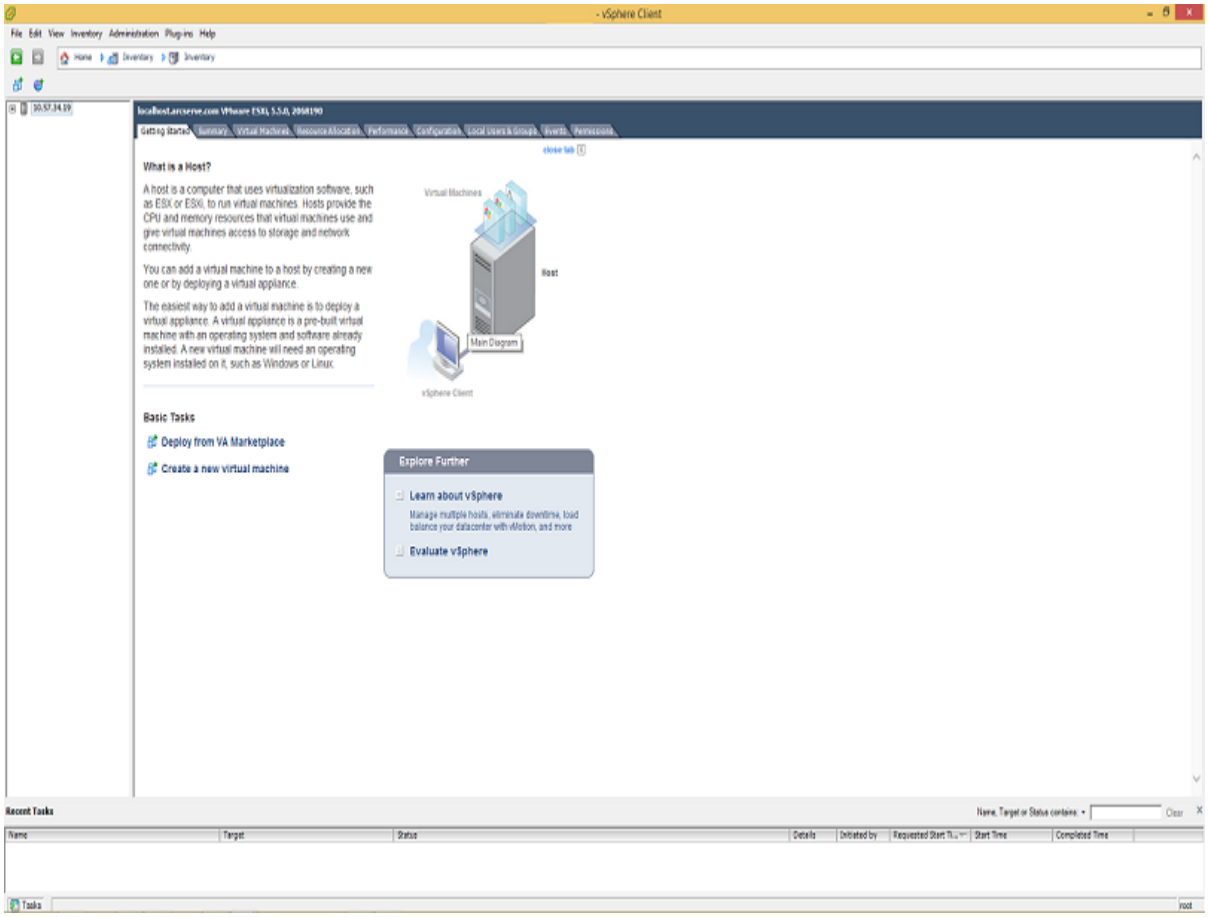
É possível criar uma rede isolada para se recuperar p SharePoint em máquinas da VMware e do Hyper-V.

- Como criar uma rede isolada para recuperação do SharePoint para VM VMware
- Como criar uma rede isolada para a recuperação do SharePoint para VM do Hyper-V

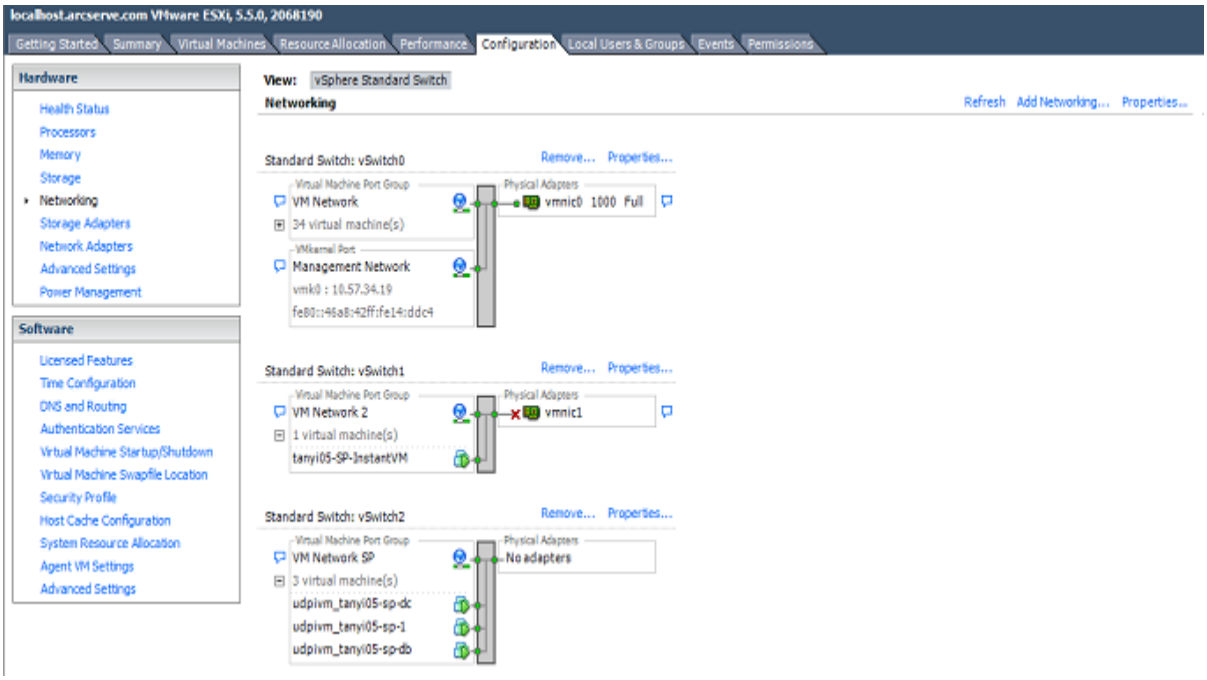
Como criar uma rede isolada para recuperação do SharePoint para VM VMware

Siga estas etapas:

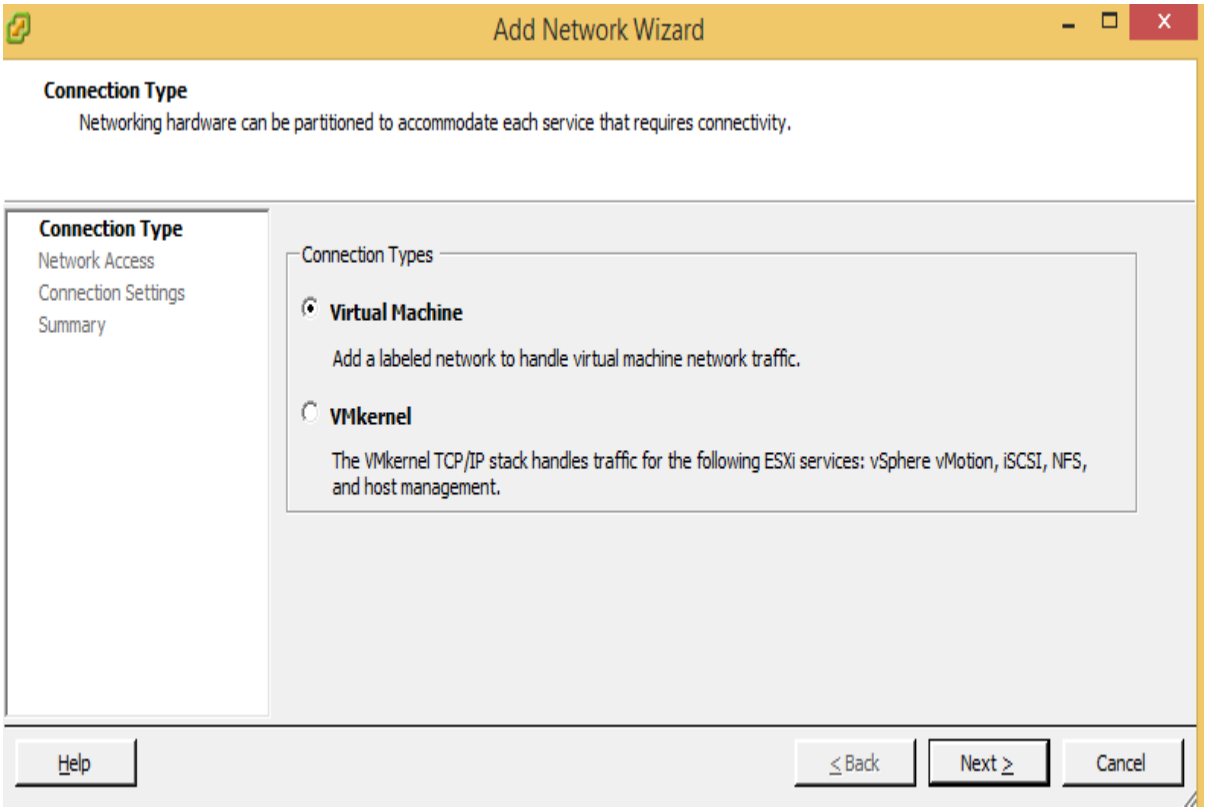
1. Efetue logon no servidor VMware ESXi usando o cliente vSphere.



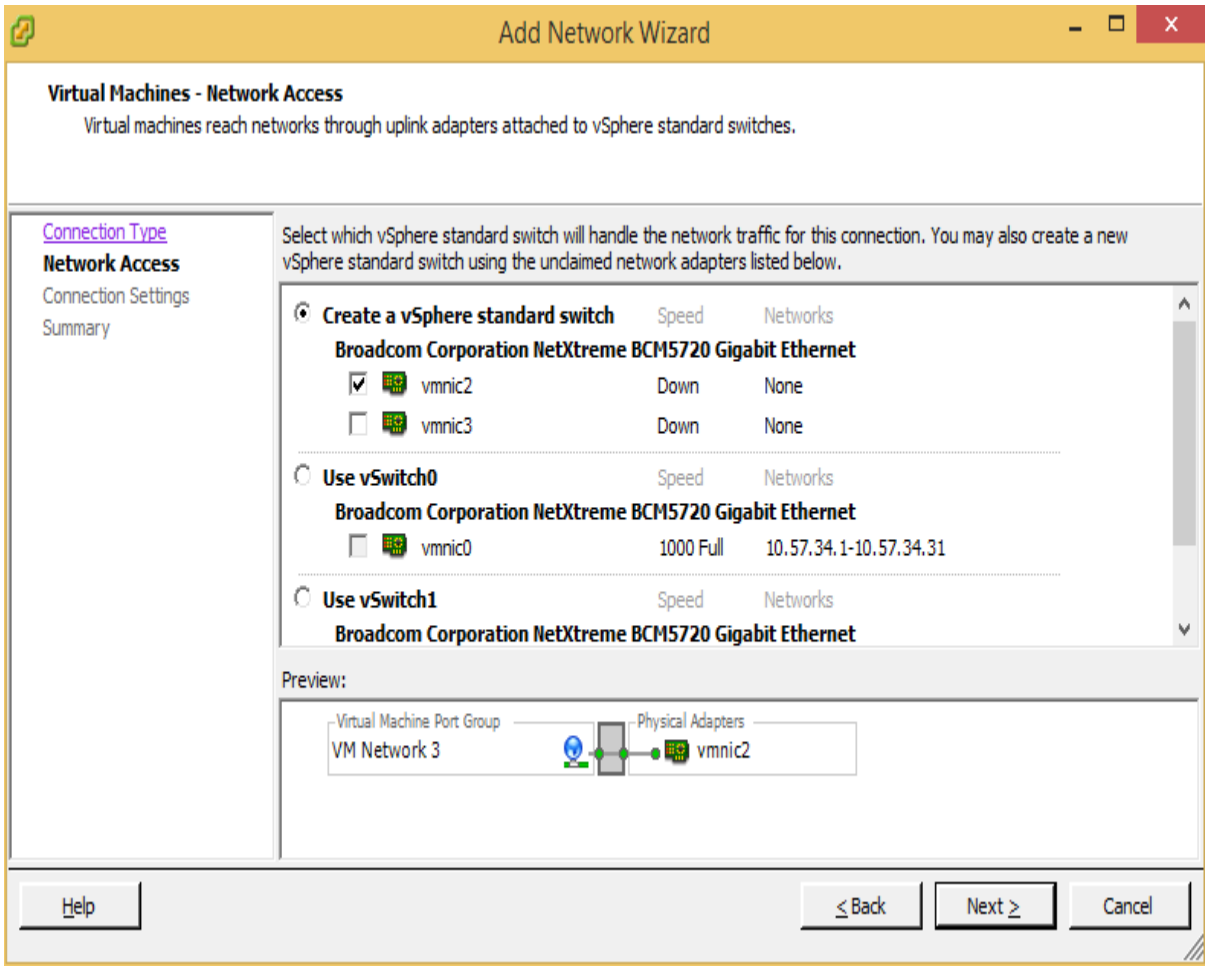
2. Clique na guia Configuração.
3. Selecione Rede no painel Hardware e clique em Adicionar rede.



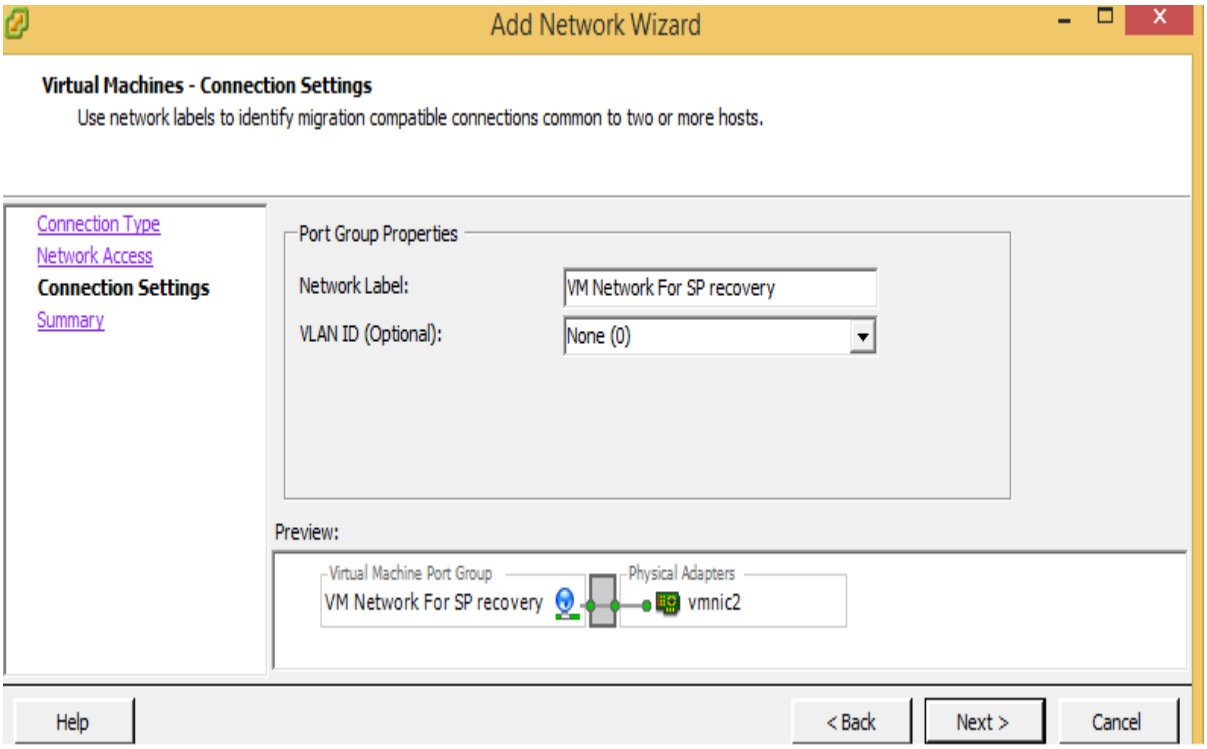
4. Confirme que o botão de opções Máquina Virtual está selecionado e clique em Avançar.



5. Selecione a NIC física que você deve usar para conectar o comutador virtual a outros recursos físicos na rede e clique em Avançar.

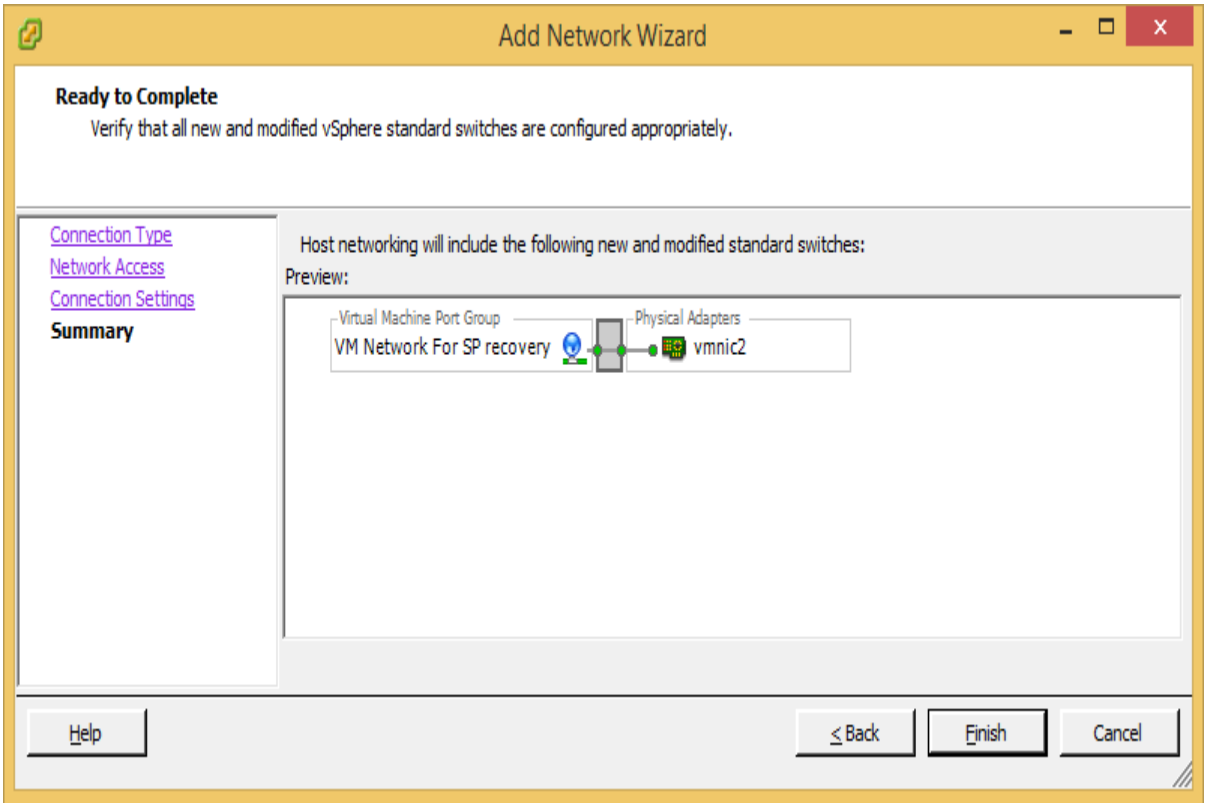


6. Atribua um rótulo de rede ao comutador virtual e uma ID de VLAN, se necessário e clique em **Avançar**.



7. Verifique se suas configurações de comutador virtual estão corretas e clique em **Concluir**.

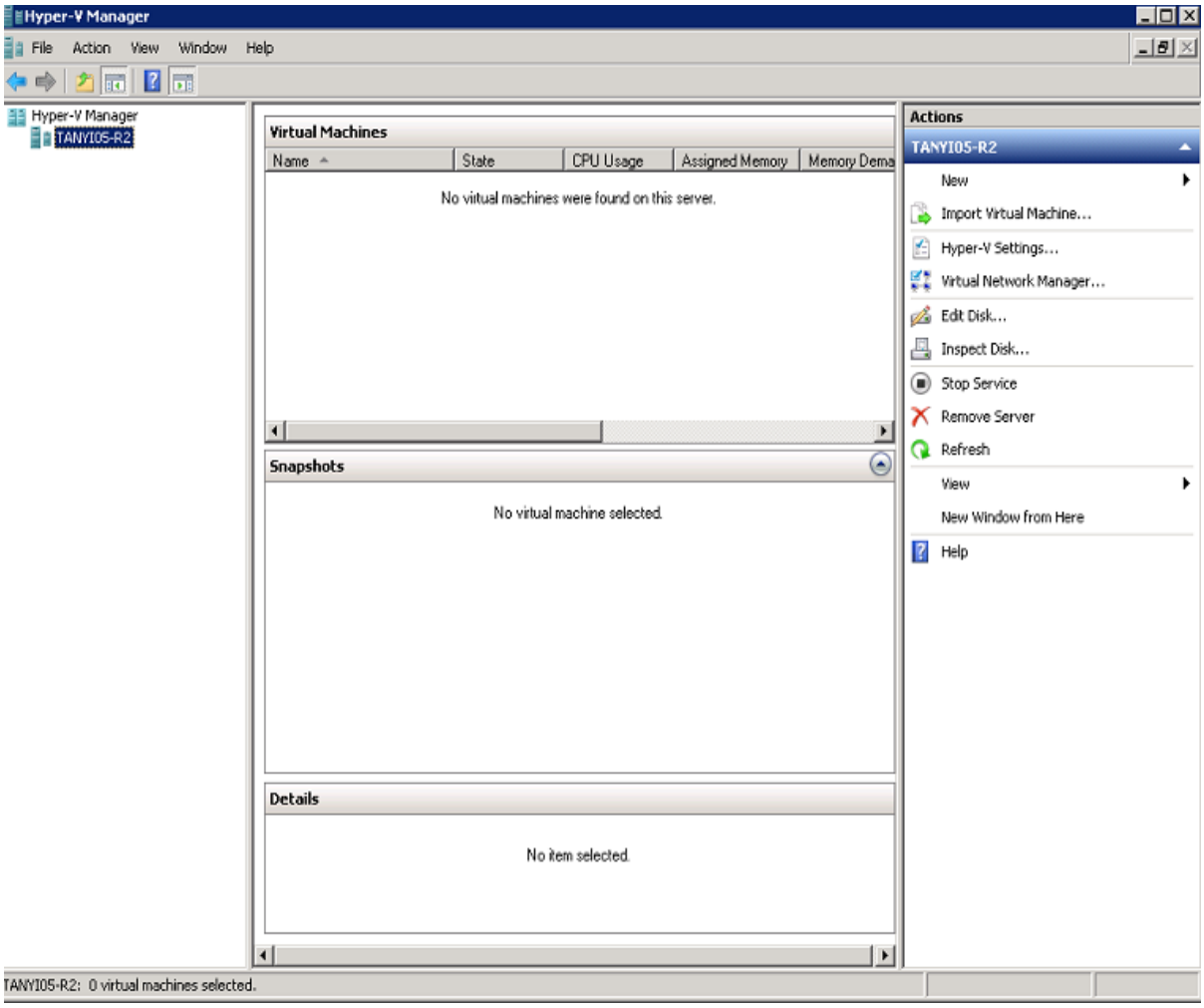
   Quando você voltar para a guia Configuração de rede, é possível ver que o novo comutador Virtual adicionado.


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

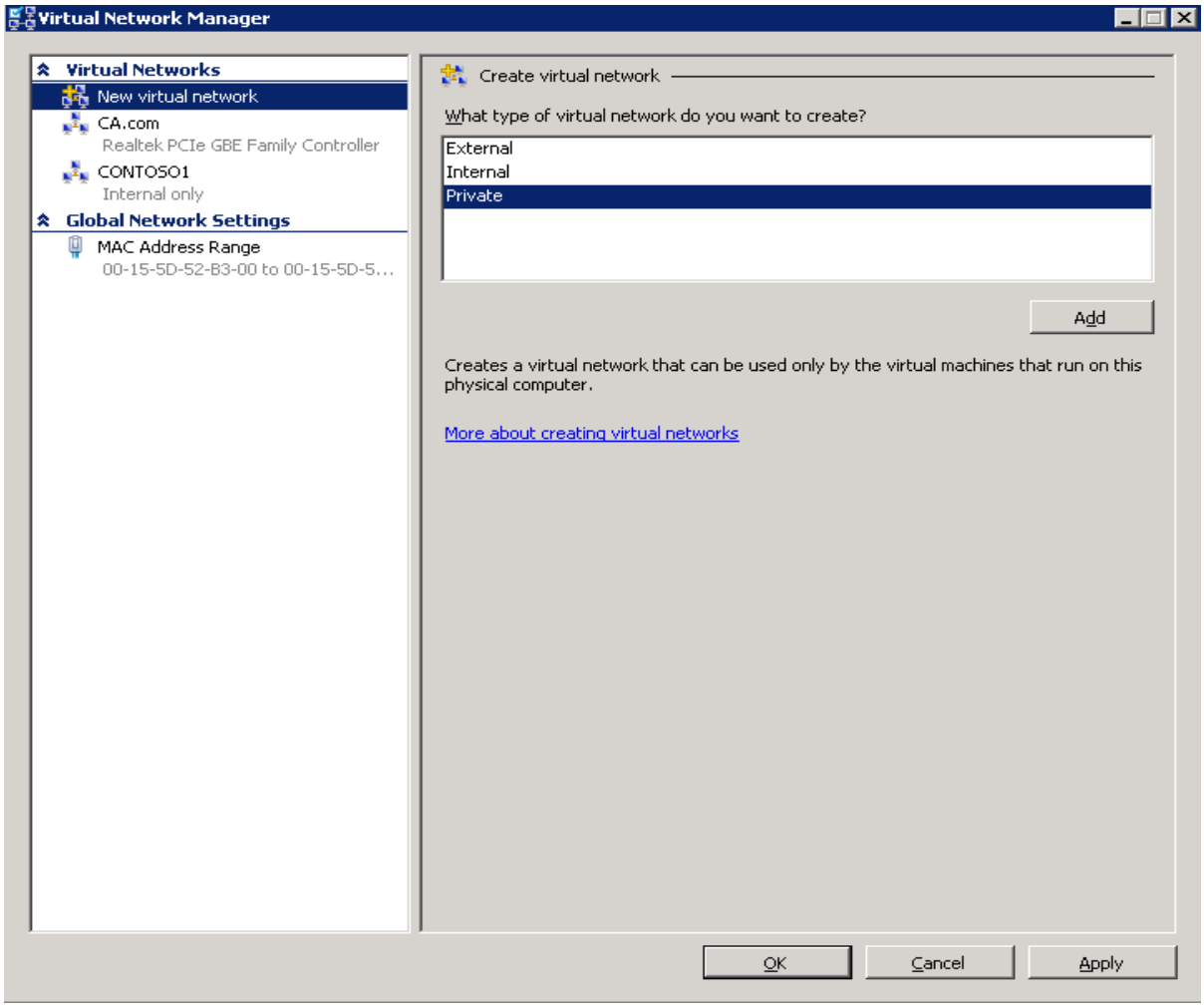
Como criar uma rede isolada para a recuperação do SharePoint para VM do Hyper-V

Siga estas etapas:

1. Efetue logon no Gerenciador Hyper-V.
2. Clique em Gerenciador de rede virtual.

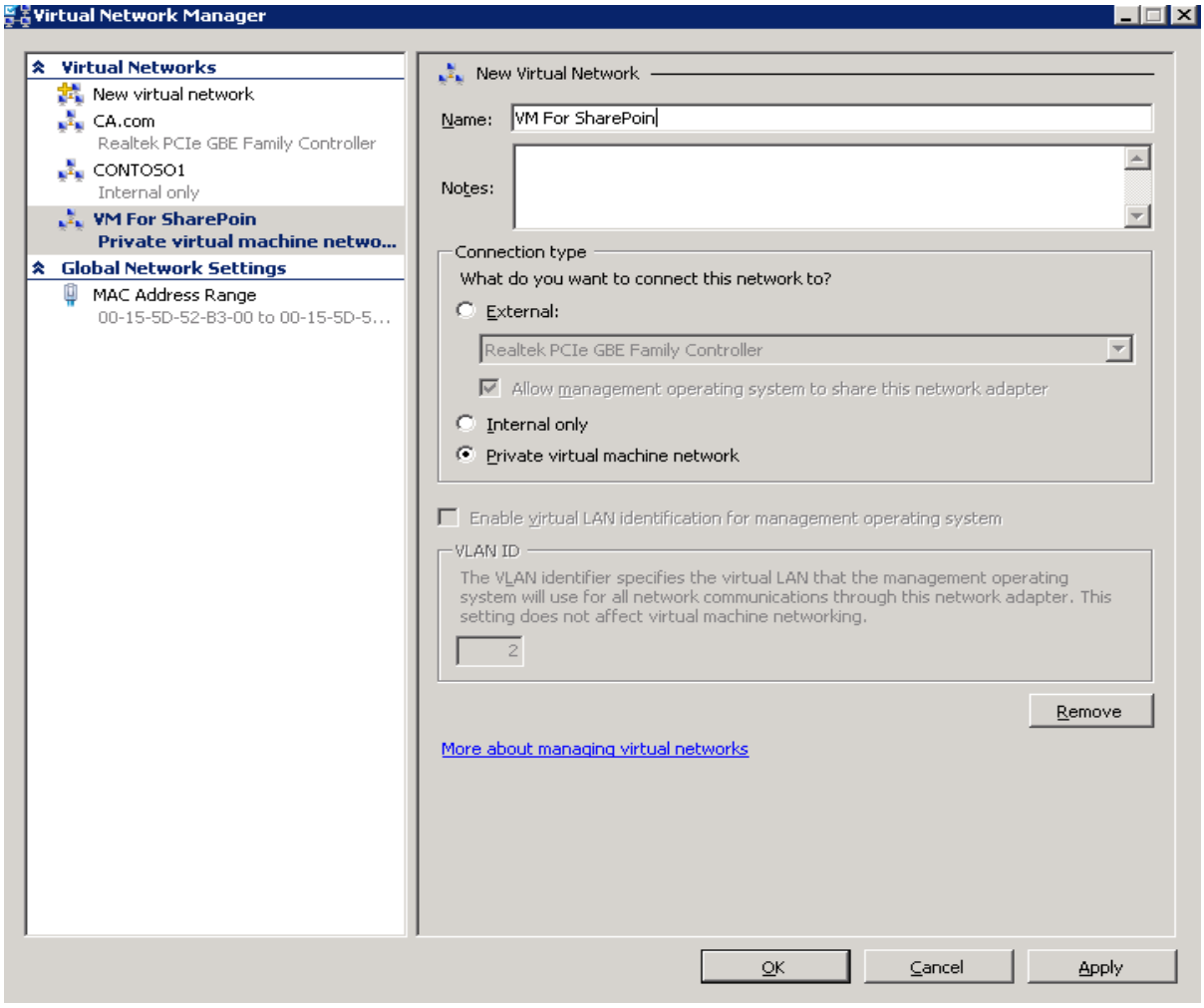


3. Clique em Nova rede virtual, selecione o tipo "Privado" e, em seguida, clique em **Adicionar**.



4. Especifique um nome para a rede virtual privada e clique em OK.

   A nova rede virtual é adicionada.


Virtual Network Manager
Virtual Networks
New virtual network
CA.com
Realtek PCIe GBE Family Controller
CONTOSO1
Internal only
VM For SharePoin
Private virtual machine netwo...
Global Network Settings
MAC Address Range
00-15-5D-52-B3-00 to 00-15-5D-5...
New Virtual Network
Name:
VM For SharePoin
Notes:
Connection type
What do you want to connect this network to?
External:
Realtek PCIe GBE Family Controller
Allow management operating system to share this network adapter
Internal only
Private virtual machine network
Enable virtual LAN identification for management operating system
VLAN ID
The VLAN identifier specifies the virtual LAN that the management operating system will use for all network communications through this network adapter. This setting does not affect virtual machine networking.
2
Remove
More about managing virtual networks
OK
Cancel
Apply

Capítulo 6: Gerando relatórios do Arcserve UDP

Esta seção contém os seguintes tópicos:

Entendendo relatórios do Arcserve UDP

A guia **relatórios** fornece acesso a vários tipos de relatórios, como Alertas, Tendências dos dados, Status do backup, Distribuição de dados e SLA. O painel esquerdo contém a lista de relatórios que podem ser gerados. O painel central exibe os detalhes do relatório selecionado e permite definir várias configurações de relatório. O relatório é gerado para um grupo de nós ou servidores. Também é possível filtrar os relatórios para exibir informações detalhadas para um nó individual.

Para obter mais informações sobre os relatórios, consulte Relatórios do Arcserve UDP.

Este relatório de detalhamento inclui os seguintes itens:

Nós da tarefa

Exibe o nome do nó em que as tarefas de Agentes do Arcserve UDP, da VM com base em host ou no modo de espera virtual são executadas.

Nós protegidos

Exibe o nome do nó do agente e o nó protegido pelo agente do Arcserve Unified Data Protection, backup de VM com base em host, modo de espera virtual ou Arcserve Backup.

Produto

Exibe o produto instalado no nó. O nome do produto poderia ser Agente do Arcserve Unified Data Protection, Servidor de ponto de recuperação do Arcserve Unified Data Protection, VM com base em host ou Arcserve Backup.

Filtros/ações

Exibe as opções globais e locais de filtros e ações relacionadas aos relatórios. Para obter mais informações, consulte Usando filtros e ações.

Relatórios do Arcserve UDP

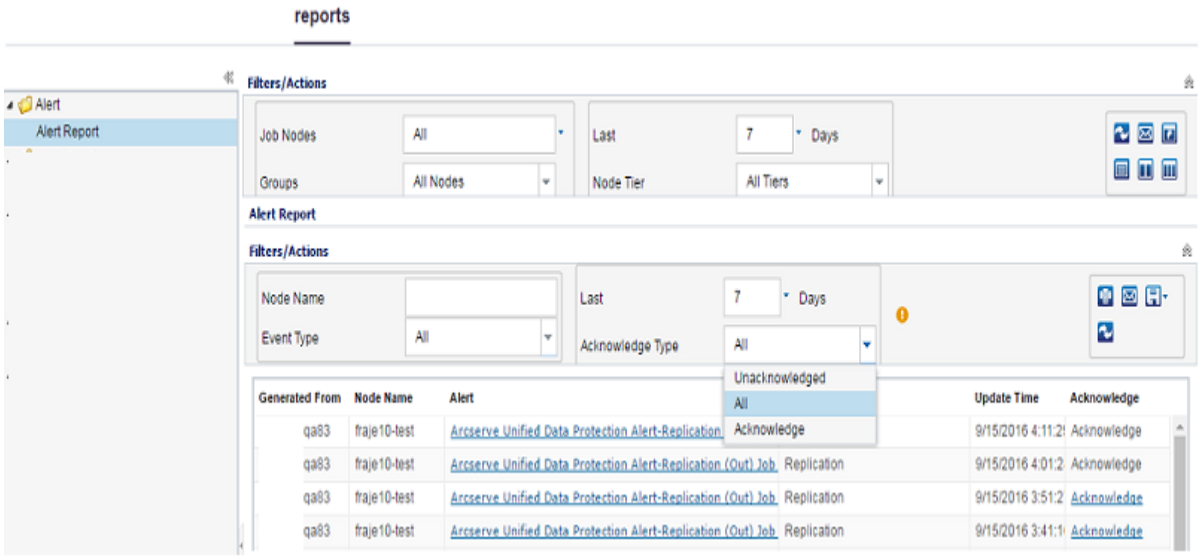
O Arcserve UDP fornece o seguinte tipo de relatório:

- Relatório de alerta
- Relatório de tendências do tamanho dos backups
- **Relatório relacionado a backup:** O Arcserve UDP fornece três tipos de relatórios relacionados a backup:
  - Relatório de status de backup dos nós
  - Relatório de status da proteção da virtualização
  - Relatório de capacidade gerenciada
- Relatório de distribuição de dados em mídias
- **Relatório de SLA:** O relatório de SLA (Service Level Agreement - Contrato de Nível de Serviço) exibe os relatórios de conformidade relacionados ao RPO (Recovery Point Objective - Objetivo do Ponto de Recuperação) e ao RTO (Recovery Time Objective - Objetivo do Tempo de Recuperação)
  - Relatório de RPO
  - Relatório de RTO
- **Relatório do status da tarefa:** O Arcserve UDP ajuda você a gerar o relatório de status da tarefa para recuperar os detalhes sobre todas as tarefas executadas em um período definido.

Relatórios de alerta

O Arcserve UDP exibe as informações de alerta para os nós. Além dos filtros e ações comuns, o relatório de alerta fornece a capacidade de classificação do painel de alertas por confirmação. Por padrão, o painel Relatório de alertas mostra somente os alertas não confirmados. Você pode clicar no link **Confirmar** exibido em cada alerta para removê-lo da exibição do painel. Se você deseja exibir o relatório confirmado, selecione **Confirmar** na opção **Tipo de confirmação** do filtro local.

Relatório de alertas

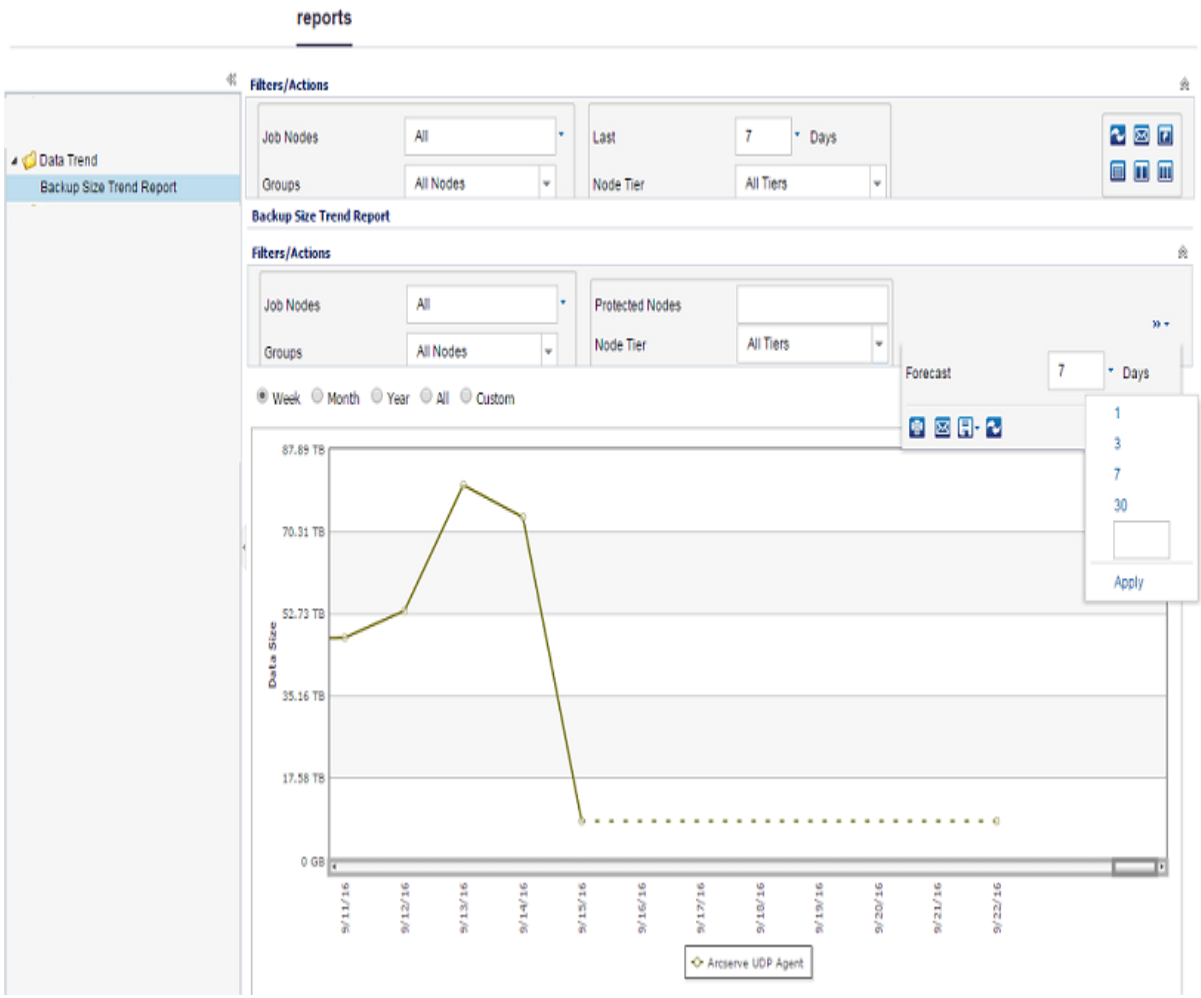


Relatórios de tendência de tamanho de backup

O relatório Tendência de tamanho de backup do Arcserve UDP mostra o tamanho dos dados de backup do Arcserve Backup e do Agente do Arcserve Unified Data Protection em uma exibição histórica e, em seguida, projeta a tendência de crescimento de modo que seja possível se preparar para futuros requisitos de espaço de armazenamento. Esse relatório contém as informações sobre os nós que são executados em sistemas operacionais Windows e Linux suportados e permite uma exibição mais detalhada das informações de um nó individual.

Além dos filtros e ações comuns, o relatório de tendência de tamanho de backup oferece a capacidade de exibir os resultados de acordo com o número de **Dias**. Por padrão, o filtro de **Último(s)** dias não é aplicável. Em vez disso, é possível usar o filtro do modo **Exibir** (semana/mês/ano/personalizado).

Relatório de tendências do tamanho dos backups



Relatórios de status de backup de nó

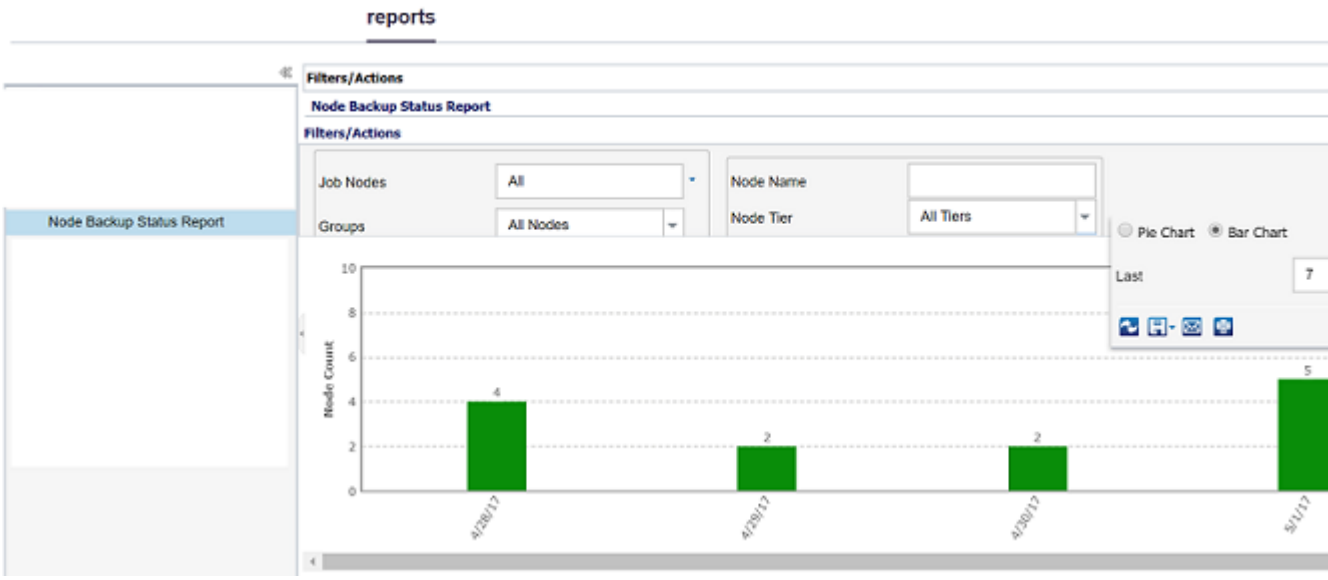
O Arcserve UDP exibe o status do backup mais recente de todos os nós durante o período de tempo específico. Este relatório permite visualizar informações detalhadas sobre nós com base em categorias tais como tipo de grupos e camada do nó selecionados.

Além dos filtros e ações comuns, o relatório de status de backup do nó fornece o recurso para exibir os resultados de acordo com o número de **Dias**. No gráfico de barras, o número de nós fica visível na parte superior de cada barra.

O relatório exibe os seguintes status da tarefa:

- **Bem-sucedida:** fornece uma lista de tarefas que são concluídas com êxito.
- **Falha**: fornece uma lista de tarefas que falharam.
- **Incompleta:** fornece uma lista de tarefas que foram concluídas com status incompleto.
- **Cancelado:** fornece uma lista de tarefas que foram canceladas.
- **Perdido:** fornece uma lista das tarefas que não foram tentadas.
- **Sem backups:** fornece uma lista de nós sem nenhum plano atribuído ou nós com plano atribuído, mas ainda aguardando que backups sejam executados.

Relatório de status de backup dos nós:

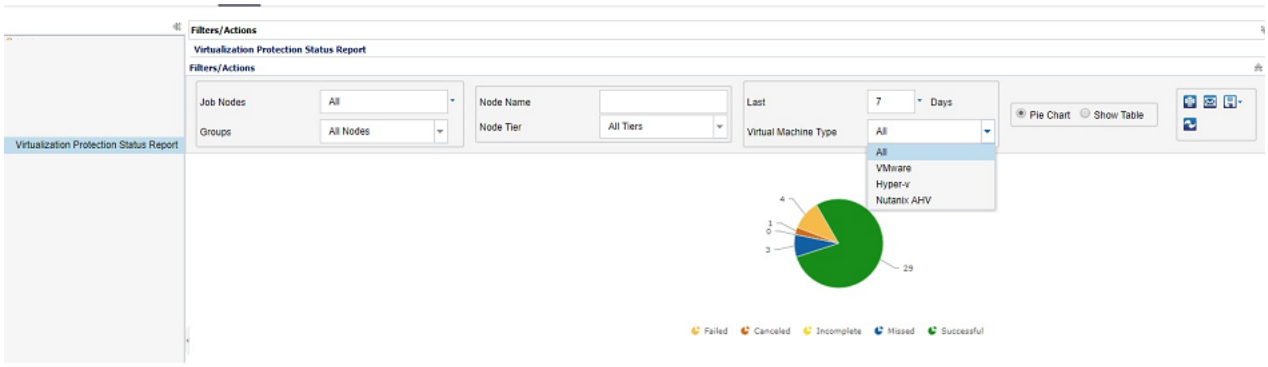


Relatórios de status da proteção da virtualização

Exibe o status do backup mais recente das máquinas virtuais que são protegidas pelo backup de VM com base em host, Modo de espera virtual ou pelo Arcserve Backup. Esse relatório permite exibir informações para um determinado período de tempo e maior aprofundamento em exibição de informações mais detalhadas sobre cada categoria selecionada.

Além dos filtros e das ações comuns, o relatório Status de proteção da virtualização fornece o recurso de exibição de resultados com base no número de **Dias**e de exibição de relatórios em gráfico de pizza ou em tabela.

Relatório de status da proteção da virtualização



Relatórios de capacidade gerenciada

Exibe o tamanho dos dados brutos do último backup completo bem-sucedido para cada nó protegido pelo Arcserve Backup, pelo Agente do Arcserve Unified Data Protection e pelo backup da VM com base em host.

Para obter detalhes sobre os filtros e as ações, consulte os filtros e ações comuns.

Observações:

- digitar um valor no filtro **Últimos dias** não altera o resultado de filtros globais. Independentemente do número de dias que você forneça, a aplicação do filtro exibe os valores mais recentes.
- Os dados relacionados ao backup de nó no repositório de dados excluído poderão aparecer, pois o relatório de capacidade gerenciada não é atualizado, a menos que o backup seja executado no destino de backup mais recente. Por exemplo, se você modificou o plano para executar backups no repositório de dados DS2 e excluiu o repositório de dados DS1, os dados excluídos do DS1 ainda aparecerão no relatório, a menos que você execute o backup no DS2.
- Na área de grade do relatório, as três colunas seguintes são aplicáveis somente para nós de VM que estão protegidos pelo backup sem agente com base em host:

  Espaço usado dos volumes (VM)

  Indica a soma do espaço usado de todos os volumes dentro do sistema operacional convidado da VM.

  Para Windows: refere-se à soma do espaço usado de todos os volumes de NTFS

  Para VM Linux: refere-se à soma do espaço usado de todos os volumes.

  para a VM do Linux, apenas a VM da VMware tem suporte nessa coluna. Nesse caso, é necessário atualizar o nó da VM com credenciais raiz. Seja uma VM do Linux da VMware sem credenciais, seja uma VM do Linux do Hyper-V, essa coluna fica vazia.

  Quanto ao suporte da VM do Linux, o Red Hat da VMware, a máquina CentOS e as VMs do Linux do Hyper-V possuem limitações. Para obter mais detalhes, consulte Problemas conhecidos nas Notas da Versão do Arcserve UDP v6 Update 1.

  Tamanho da leitura sintética

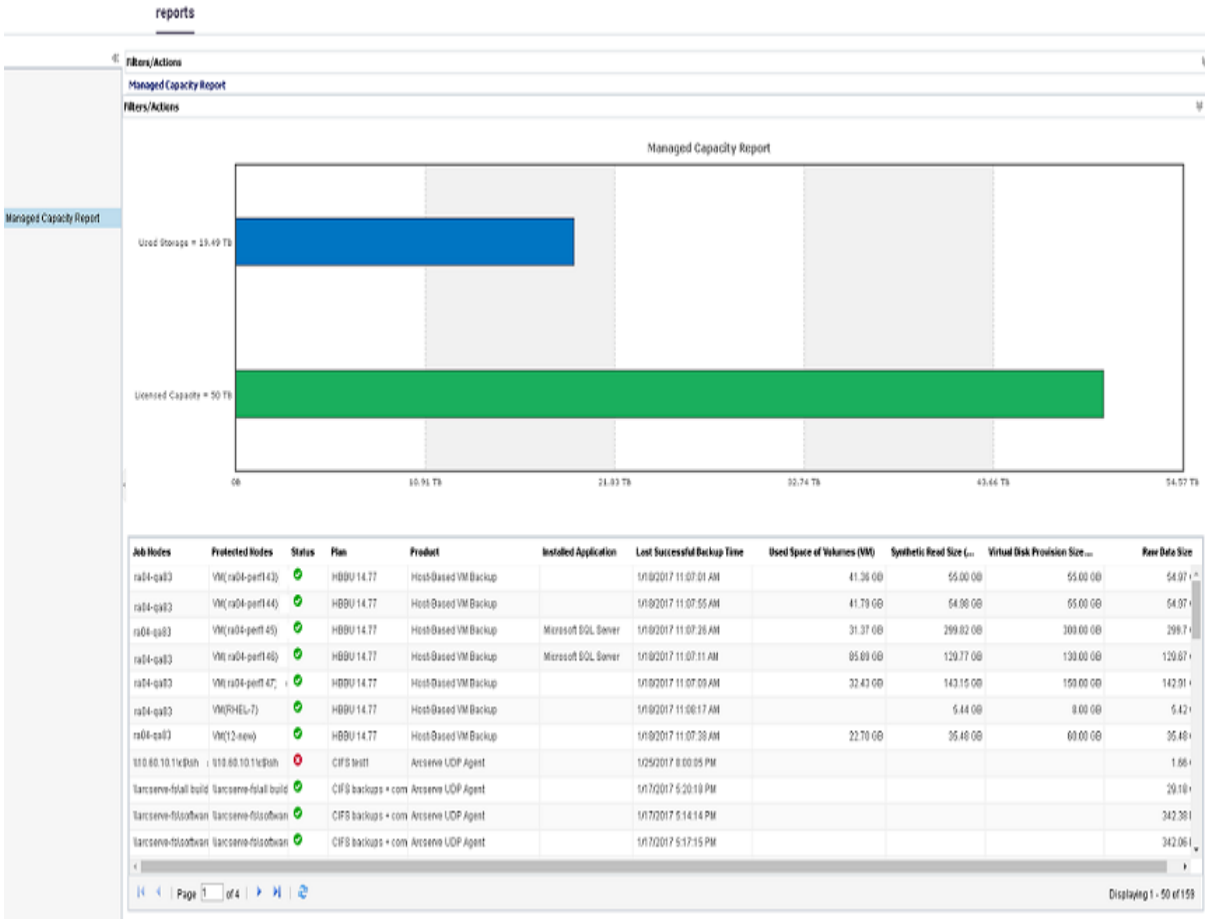
  Indica o tamanho total lido durante o backup.

  Tamanho do provisionamento do disco virtual

Indica a soma do tamanho do provisionamento de todos os discos virtuais da VM.

- Em geral, Tamanho dos dados brutos é o tamanho dos dados gravados no destino do backup. Para backup sem agente com base em host, ele pode ou não ser igual ao tamanho de leitura sintética porque o Arcserve UDP não grava todos os blocos de dados em zero para o destino de backup. Em outras palavras, os blocos de dados em zero são ignorados durante o backup. Além disso, para nós de VM que estão protegidos pelo backup sem agente com base em host, é possível personalizar os dados exibidos para o tamanho dos dados brutos, configurando alguns valores do registro. Para obter mais informações sobre como configurar os valores do registro e comportamentos associados, consulte Entendendo o tamanho dos dados brutos no relatório de capacidade gerenciada para backup da VM sem agente com base em host.

Relatório de capacidade gerenciada

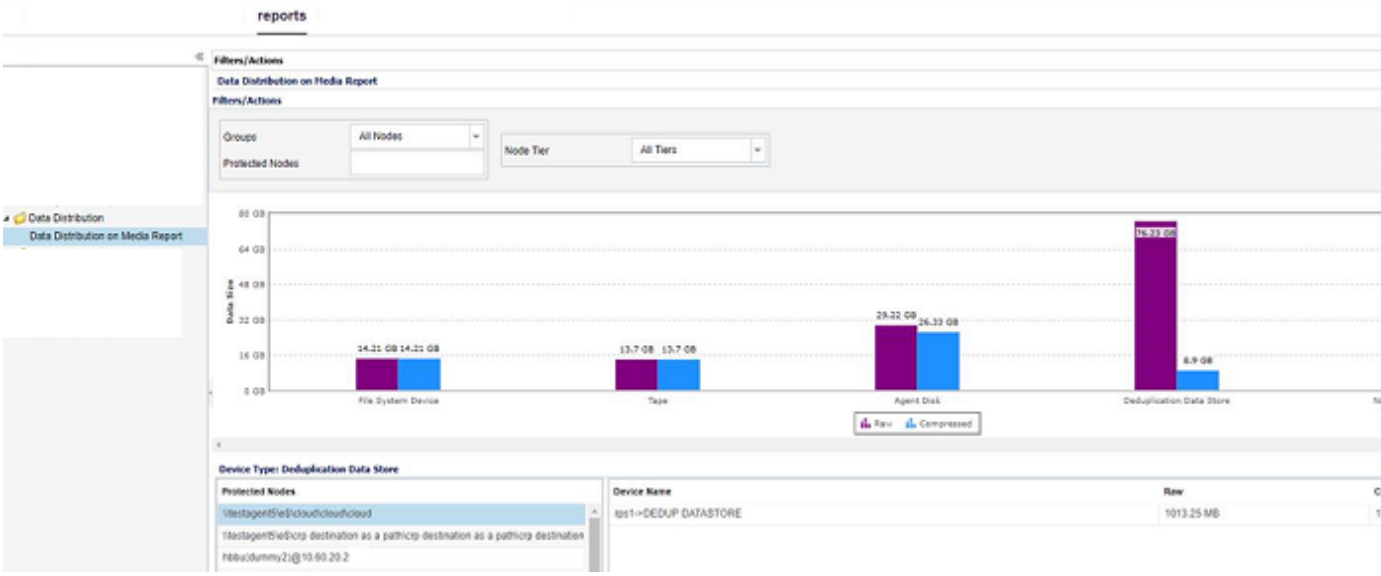


Relatórios de distribuição de dados em mídias

Exibe o tamanho dos dados de backup (brutos) compactados e reais para tipos de destino diferentes (redução de redundância ou não redução de redundância e destino local). Este relatório permite exibir todos os nós, incluindo nós do Arcserve Backup e do agente do Arcserve UDP. Para exibir as informações de dados do Arcserve Backup, ative a **Programação de sincronização de dados do Arcserve Backup** na guia **Configurações**. Para exibir as últimas informações, clique em **Executar agora** na guia Configurações.

Para obter detalhes sobre os filtros e as ações, consulte os filtros e ações comuns.

Relatório de distribuição de dados em mídias



Observação: o relatório de distribuição de dados em mídias depende dos dados do ponto de recuperação disponíveis no destino de backup. É possível usar a opção **Atualizar** para iniciar uma sincronização sob demanda e obter o status mais recente nos relatórios.

Relatórios de RPO

O relatório de RPO (Recovery Point Objective - Objetivo do Ponto de Recuperação) é o relatório de conformidade que exibe como os pontos de recuperação são distribuídos no ambiente de backup. Esse relatório ajuda na avaliação, em caso de falhas, de qual é o momento mais recente e o mais antigo ao qual o nó pode retornar. Como o relatório de RPO é para o destino de backup, o relatório é preenchido com os dados quando houver algum backup pronto. O relatório é preenchido por meio de uma atualização programada ou sob demanda.

Observação: o relatório também é preenchido diretamente no painel do Arcserve UDP. Ao clicar no gráfico de barras de um mês no painel, a tela do relatório de RPO desse mês específico é exibida na página de RPO.

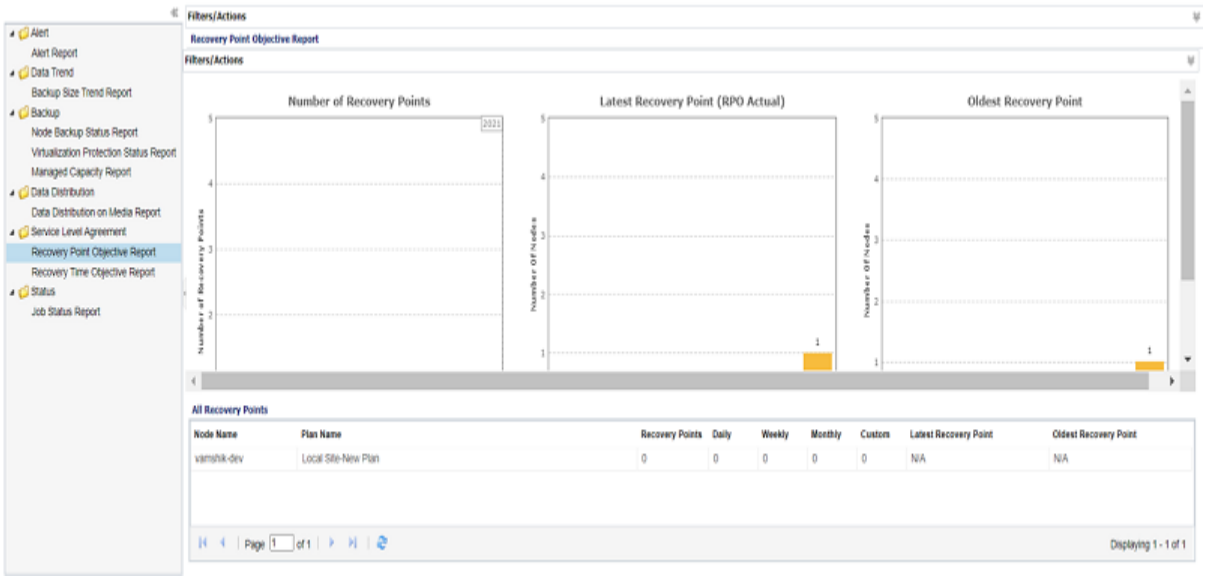
O gráfico de barras de RPO fornece as seguintes informações:

- Distribuição mensal dos pontos de recuperação no destino de backup.
- Tempo de vida do ponto de recuperação mais recente disponível para cada nó.
- Tempo de vida do ponto de recuperação mais antigo disponível para cada nó.
- Números fornecidos na parte superior de cada barra.
- A opção *Tipo de destino* permite selecionar o tipo de destino. Por exemplo, destino na nuvem, servidor de ponto de recuperação e compartilhamento local.
- *Nome de destino* permite selecionar um destino da lista de destinos que aparece como resultado da opção selecionada como Tipo de destino.
- Clicar na barra específica em qualquer um dos três gráficos a seguir exibe resultados específicos: *Número de pontos de recuperação* para cada mês, *Idade do ponto de recuperação mais recente* e *Idade do ponto de recuperação mais antigo*.

No gráfico de barras de RPO, a seção Todos os pontos de recuperação exibe informações como nome do nó, nome do plano, pontos de recuperação, pontos de recuperação diários, semanais, mensais, personalizados e mais recentes, bem como pontos de recuperação antigos.

Além de filtros e ações comuns, os relatórios de RPO oferecem uma opção única de **Atualização** no filtro local.

Relatório de RPO



Observação: o relatório depende dos dados do ponto de recuperação disponíveis no destino de backup. É possível usar a opção **Atualizar** para iniciar uma sincronização sob demanda e obter o status mais recente nos relatórios.

Relatórios de RTO

O relatório de RTO (Recovery Time Objective - Objetivo de Tempo de Recuperação) é o relatório de conformidade que exibe se o objetivo de tempo de recuperação definido foi atendido para todas as tarefas do tipo de recuperação executadas. O relatório de RTO exibe os seguintes tipos de status:

- **RTO atendido:** a tarefa de recuperação atendeu ao objetivo definido.
- **RTO não atendido:** a tarefa de recuperação não atendeu ao objetivo definido.
- **RTO não definido**: o objetivo não foi definido para a tarefa de recuperação.
- **RTO não testado:** o objetivo de tempo de recuperação foi definido, mas a tarefa ainda não foi testada.

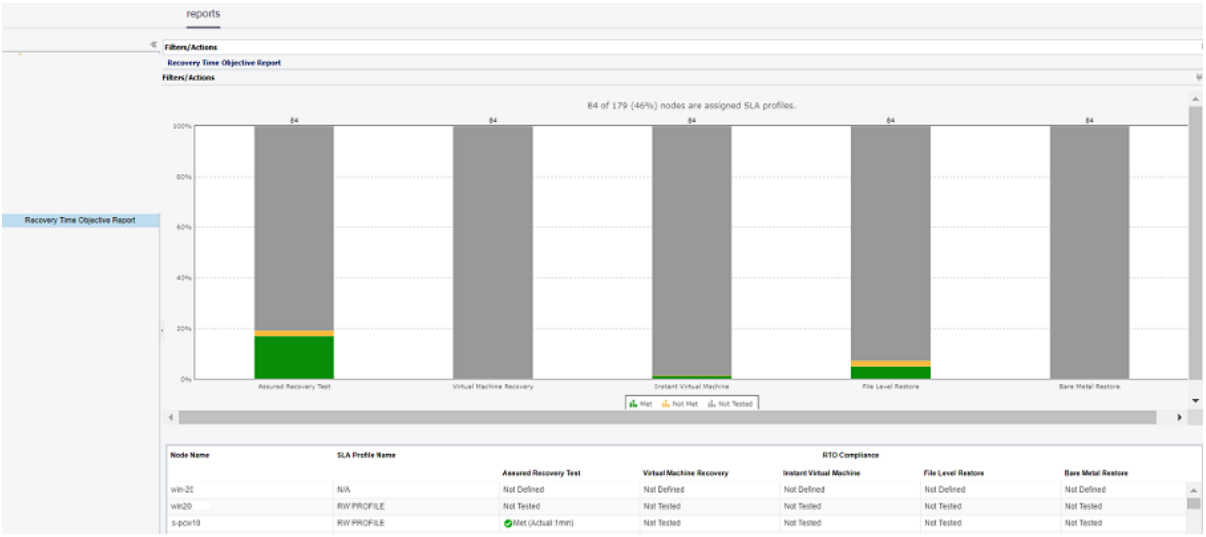
É possível definir os objetivos de tempo de recuperação de todas as tarefas de recuperação. Para obter mais informações, consulte criando o perfil de SLA.

Além dos filtros e ações comuns, os relatórios de RTO fornecem uma opção única de **Perfil de SLA** e Status de RTO no filtro local.

Observação: o relatório de RTO não é suportado para tarefas de restauração Bare Metal que são executadas para tarefas de backup configuradas no local de destino.

Painel do relatório de RTO

Considerações sobre relatório de RTO	Descrição
Parâmetros considerados para gerar o gráfico de RTO	• Atendido • Não atendido • Não testado
Fórmula para definir a porcentagem do status do RTO (%)	Nós atribuídos ao Perfil de SLA/nós totais*100
Codificação de cores usada para o gráfico	• Atendido = verde • Não atendido = vermelho • Não testado = cinza

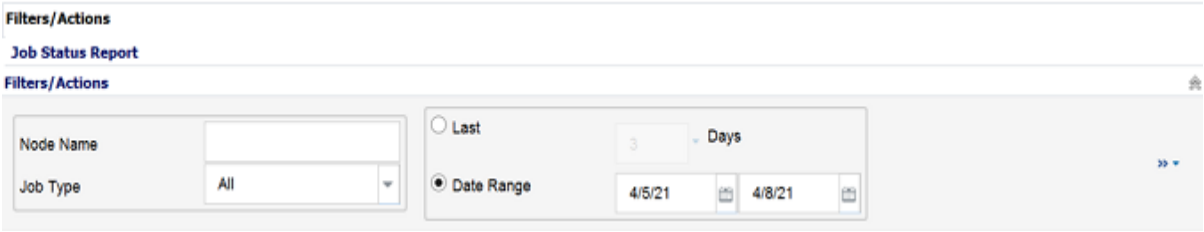

reports
Filters/Actions
Recovery Time Objective Report
Filters/Actions
84 of 179 (46%) nodes are assigned SLA profiles.
Recovery Time Objective Report
Assured Recovery Test
Virtual Machine Recovery
Instant Virtual Machine
File Level Restore
Bare Metal Restore
Met
Not Met
Not Tested
Node Name
SLA Profile Name
RTO Compliance
Assured Recovery Test
Virtual Machine Recovery
Instant Virtual Machine
File Level Restore
Bare Metal Restore
win-2t
N/A
Not Defined
Not Defined
Not Defined
Not Defined
Not Defined
win20
RW PROFILE
Not Tested
Not Tested
Not Tested
Not Tested
Not Tested
s-pcw10
RW PROFILE
Met (Actual 1min)
Not Tested
Not Tested
Not Tested
Not Tested

Relatórios do status da tarefa

O relatório de status da tarefa ajuda você a gerar o status geral de todos os tipos de tarefas que são executados no Console. Esse relatório pode ser útil para atender aos requisitos de auditoria. Além dos filtros e ações comuns, o relatório do status da tarefa fornece a capacidade de exibir os resultados com base no tipo de tarefa, ID da tarefa, status da tarefa e nome do plano (ativo e excluído). Além disso, para duração, exiba o formato de data/hora em horas:-minutos:segundos.

Você pode exibir o relatório de status da tarefa usando os filtros locais. A opção Filtros/ações contém o seguinte:

- **Nome do nó:** filtra o relatório de status da tarefa com base no nome do nó.
- **Tipo de tarefa:** filtra o relatório de status da tarefa com base no tipo de tarefa.
- **Último:** exibe o relatório de status da tarefa referente ao último número de dias.
- **Intervalo de datas:** exibe o relatório de status da tarefa entre o intervalo de datas especificado.



Observação: é possível selecionar entre o filtro Último ou Intervalo de datas, conforme necessário. Por padrão, o filtro Último é selecionado e o status do relatório da tarefa dos últimos 7 dias é exibido.

No log, você pode clicar na ID da tarefa para exibir os detalhes. Também é possível exibir o status de cada tarefa.

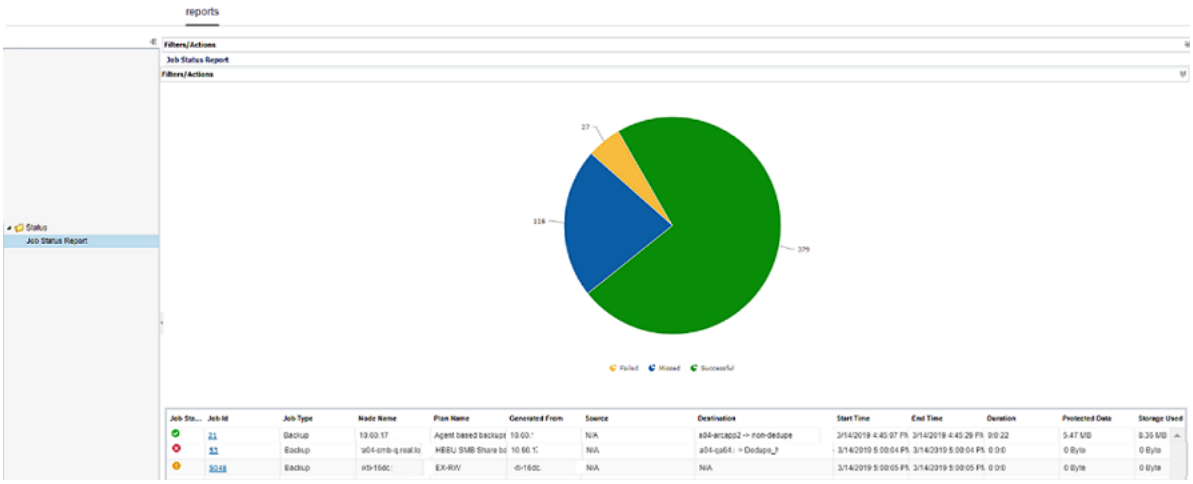
É possível Exibir os valores reais em origem e destino para tipos de tarefas. O relatório exibe os seguintes status da tarefa:

- **Bem-sucedida:** fornece uma lista de tarefas que são concluídas com êxito.
- **Falha**: fornece uma lista de tarefas que falharam.
- **Incompleta**: fornece uma lista de tarefas que foram concluídas com status incompleto.

- **Cancelado:** fornece uma lista de tarefas que foram canceladas.
- **Perdido:** fornece uma lista das tarefas que não foram tentadas.

Observação: a duração de retenção padrão para recuperar o status da tarefa é 180 dias. É possível modificar a configuração para personalizar os dias de retenção padrão para eliminação.

Relatório do status da tarefa



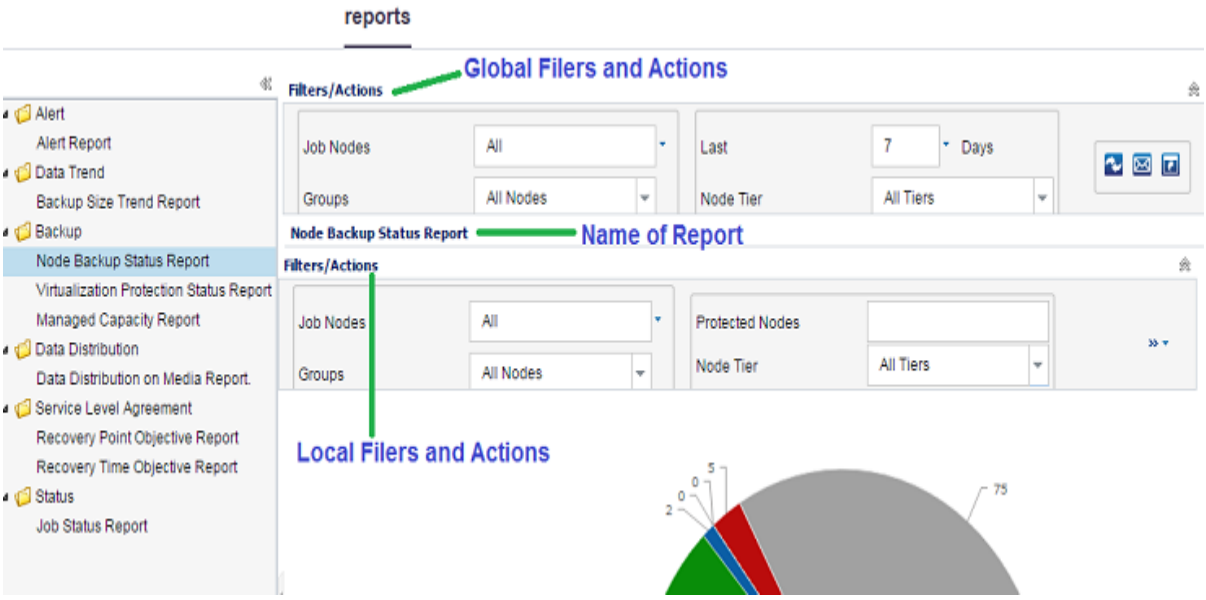
Observação: quando há várias tarefas em execução, o Relatório do status da tarefa é gerado. No entanto, quando você clica no gráfico de pizza, os dados de detalhamento exibidos poderão estar inconsistentes. Para corrigir essa inconsistência, atualize o relatório.

Usando filtros e ações

Cada página de relatório contém duas opções de Filtros/Ações. A primeira opção fica a opção global que aparece na parte superior da página do relatório. A outra opção é a opção local que aparece abaixo do nome do relatório na página do relatório e fornece soluções relacionadas a um relatório específico.

Como pré-requisito, instale o Microsoft .NET Framework (versão 3.5) no computador em que você instalou o console para o recurso de exportação de gráfico de relatório para exportar as imagens em um relatório com êxito.

Observação: o Adobe Flash não é mais necessário e a instalação do .NET Framework como pré-requisito permite exibir os gráficos.



Filtros

Opções global e local contêm filtros nos quais os dados podem ser inseridos para definir opções de exibição de relatório. As opções disponíveis para filtros globais são semelhantes para todos os relatórios. As opções disponíveis para filtros locais variam para relatórios diferentes.

Ações

Para relatórios que usam a opção global:

- **Atualizar:** permite atualizar as informações relacionadas à página.
- **Programar relatórios a serem enviados por email:** permite criar uma programação para enviar relatórios usando email. Para obter mais informações, consulte Programar email.

Observação: um email de agendamento exporta um máximo de 5.000 registros.

- **Redefinir:** permite alterar todos os parâmetros de filtro com os valores padrão.
- **A exibição de relatório mostra apenas um relatório:** permite exibir um relatório em um único painel.
- **A exibição de relatório mostra vários relatórios em duas colunas:** permite dividir o painel de exibição de relatório em duas colunas para exibir vários relatórios.
- **A exibição de relatório mostra vários relatórios em três colunas:** permite dividir o painel de exibição de relatório em três colunas para exibir vários relatórios.

Para relatórios que usam a opção local:

- **Imprimir:** clique no ícone para imprimir o relatório.

  Observação: usando Imprimir, somente é possível acessar os primeiros 50 nós ou alertas da lista completa de dados.
- **Atualizar:** clique para atualizar o relatório de informações relacionadas.
- **Email:** é possível enviar por email o relatório. Para obter mais informações, consulte Enviar relatório por email.

  Observação: um email exporta um máximo de 10.000 registros.
- **Salvar:** é possível usar a opção para exportar um relatório. Selecione um dos formatos de **CSV**, **PDF** e **HTML** e clique em **Abrir** ou em uma das opções de **Salvar**, na caixa de diálogo exibida na parte inferior da página para exportar o relatório.

  Observação: ao usar Salvar, somente é possível acessar os primeiros 10.000 nós ou alertas da lista completa de dados.

Trabalhando com relatórios do Arcserve UDP

Esta seção contém os seguintes tópicos:

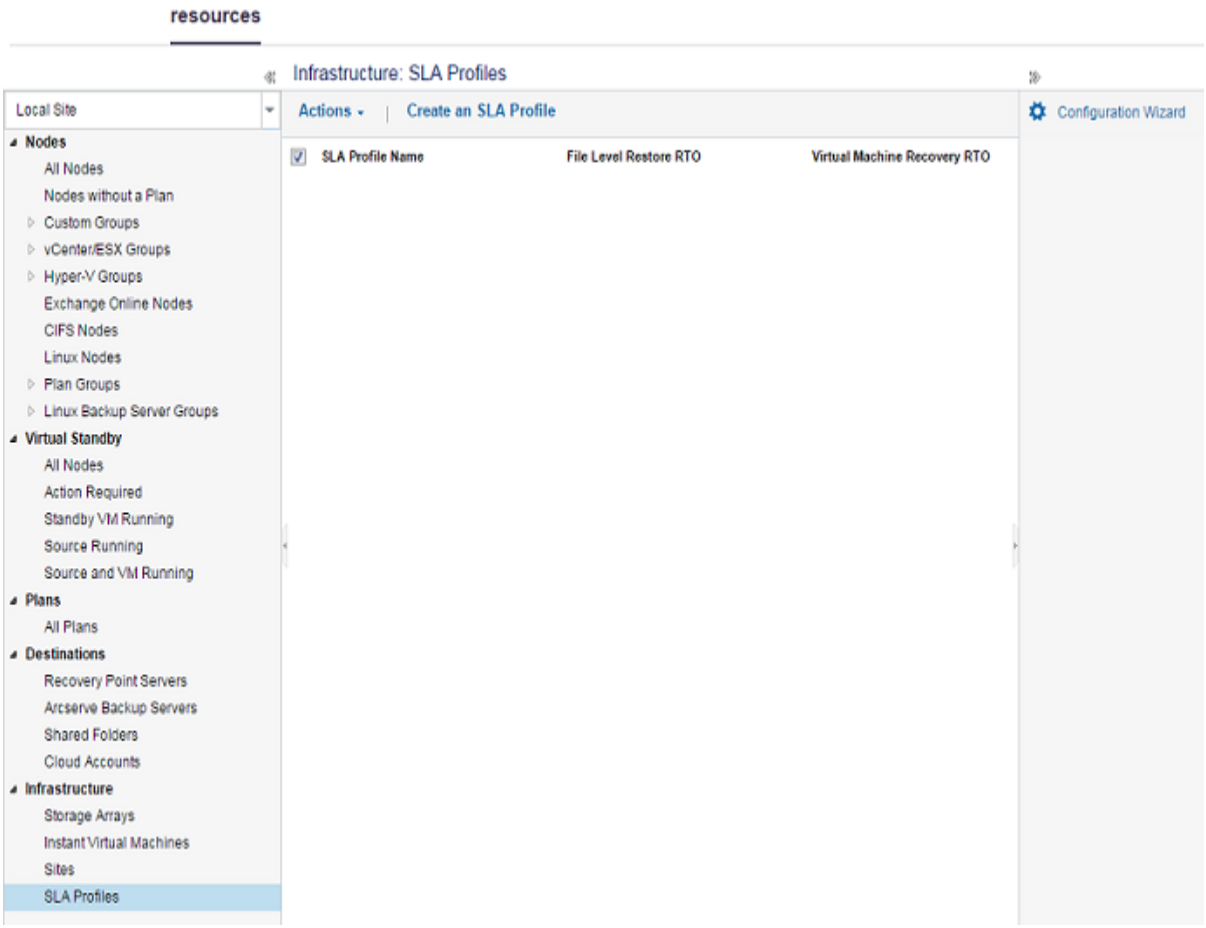
1. Criar um perfil de SLA
2. Programar emails
3. Enviar relatório por email
4. Gerar um relatório
5. Personalizar dias de retenção para um relatório de status de tarefa
6. Tamanho dos dados brutos no relatório de capacidade gerenciado para o backup da VM sem agente com base em host
7. Visualizar valores reais na origem e no destino para tipos de tarefas

Criar um perfil de SLA

Você precisa criar um perfil de SLA para gerar relatórios de RTO.

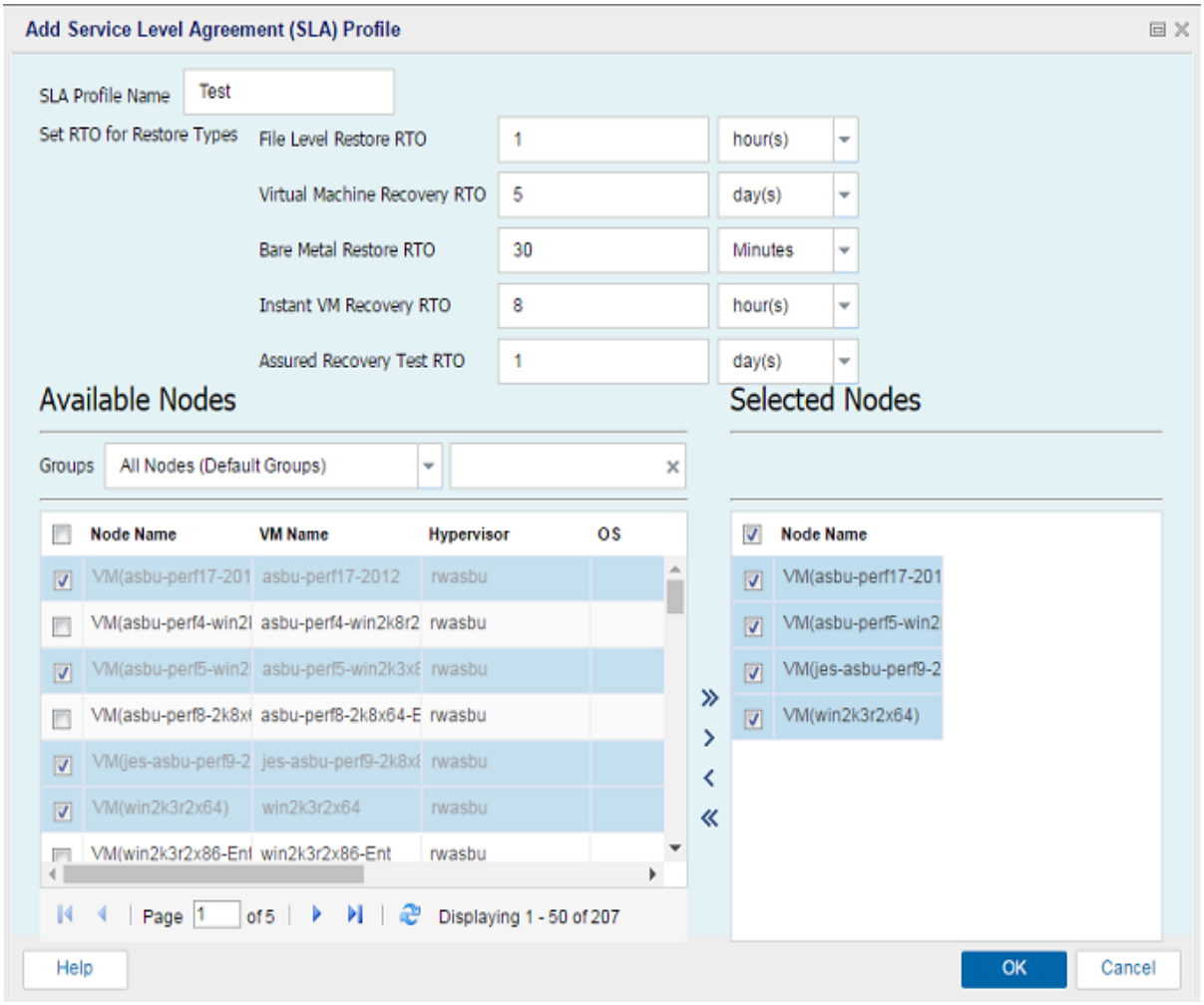
Siga estas etapas:

1. Vá ao painel esquerdo da guia **recursos**, clique em **Infraestrutura** > **Perfil de SLA**.



2. Clique em **Criar um perfil de SLA** no painel central.

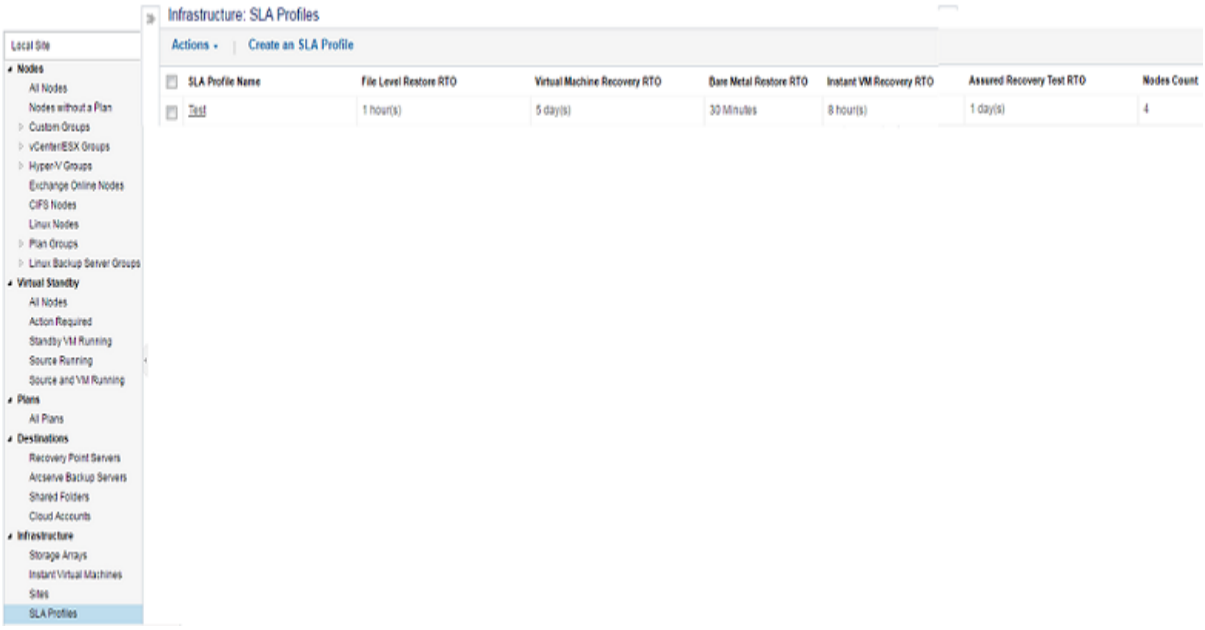
   Adicionar perfil de SLA abre.



3. No painel Adicionar perfil de SLA, execute as seguintes etapas:
   a. Inserir um **Nome de Perfil de SLA**
   b. Digite o tipo de tempo e a duração do tempo das opções desejadas para **Definir RTO para o tipo de restauração**.

      Observação: para todas as opções, é possível selecionar o tempo em dias, horas e minutos.
   c. Na seção **Nós disponíveis**, marque as caixas de seleção dos nós para os quais você deseja gerar relatórios e vá para a seção **Nós selecionados**.
   d. Selecione um ou mais nós em **Nós selecionados** e clique em **OK**.

O perfil de SLA é criado e adicionado sob o Nome de perfil de SLA.



4. Para modificar ou excluir o perfil de SLA existente, selecione a caixa de seleção do perfil desejado e clique em **Ações**.

É possível exibir o relatório de **RTO** usando a guia **relatórios** para entender o status da tarefa de todos os perfis de SLA definidos.

Programar emails

O Arcserve Unified Data Protection permite criar uma programação para enviar relatórios por email a destinatários especificados.

Observação: antes de criar uma programação para enviar um email, defina as configurações de email. Para obter mais informações sobre como configurar, consulte o tópico Configurar emails e alertas.

É possível criar uma programação e editar a programação.

Criar programação

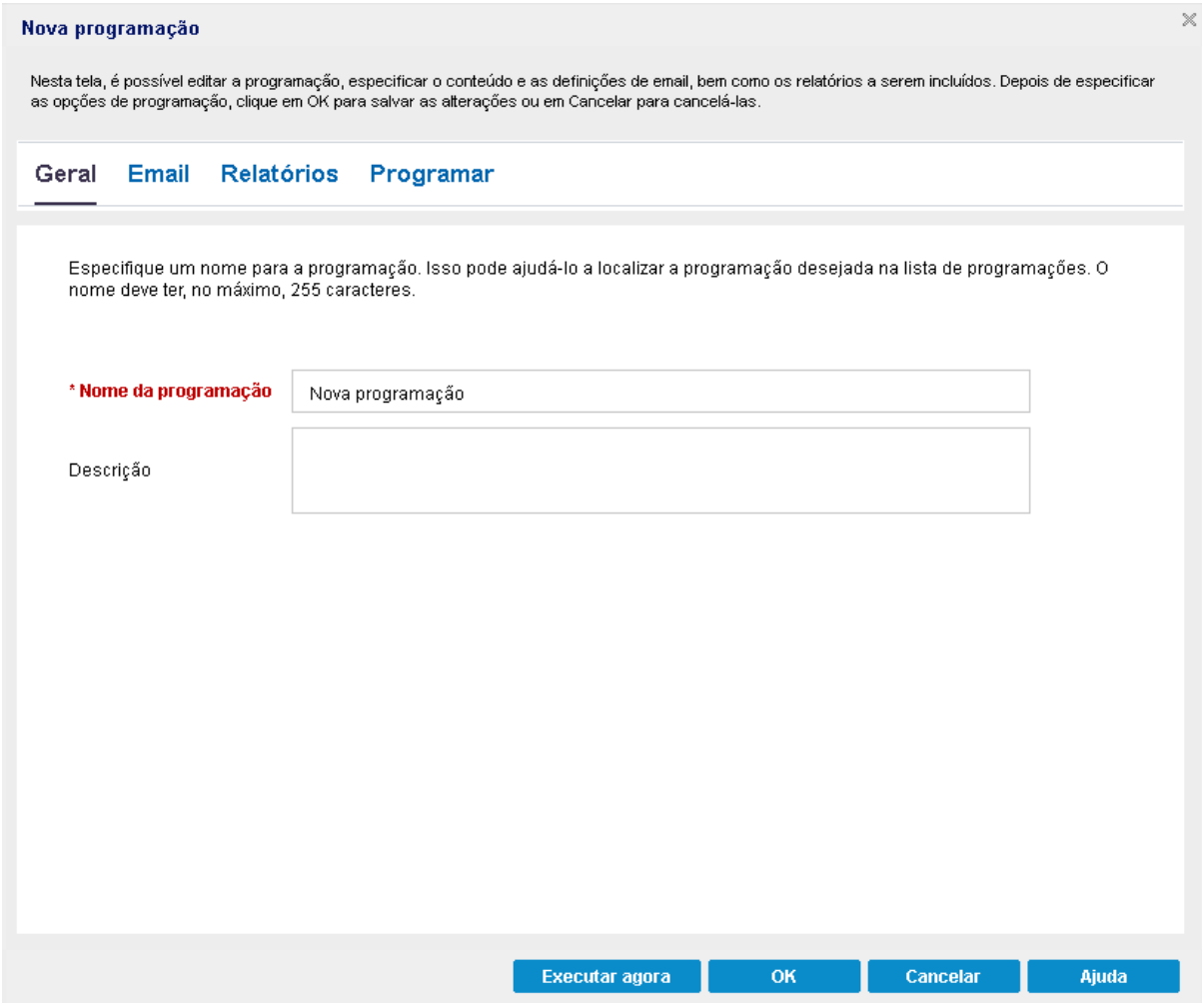
É possível adicionar novas programações aos relatórios de emails. Esses emails de relatório são atualizados, gerados e enviados automaticamente, conforme programado. É possível personalizar a programação das mensagens de email de relatório. O aplicativo permite definir o conteúdo do email, os relatórios a anexar, para quem enviar os relatórios, e a data e hora em que o relatório será enviado. Os relatórios selecionados exibirão informações mais detalhadas em formato de tabela no email.

Siga estas etapas:

1. Efetue logon na interface da web do Arcserve Unified Data Protection.
2. Clique em **Relatórios** na barra de navegação.
3. No canto superior direito dos relatórios, clique na seção global **Filtros/ações**.
4. Na lista expandida, selecione o ícone de email para abrir a caixa de diálogo **Programar relatórios a serem enviados por email**.

   A caixa de diálogo **Programar emails** é exibida.
5. Clique em **Novo**, na caixa de diálogo **Programar emails**.

   A caixa de diálogo **Nova programação** é exibida.



As seguintes guias são exibidas:

- **Geral:** especifique um nome e uma descrição (opcional) para a nova programação.
- **Email**: especifique as configurações de email, o conteúdo e anexo para a programação de email.
- **Relatórios**: selecione os relatórios específicos que deseja incluir no email.
- **Programar**: especifique uma programação para o email.

6. Preencha os campos necessários em cada guia.
7. Clique em **OK** para salvar a programação.

   A nova programação é adicionada à caixa de diálogo **Programar emails**.

   Observação: não clique em **OK**, caso deseje exibir o relatório imediatamente.
8. (Opcional) Para exibir o relatório imediatamente, clique em **Executar agora**.

O relatório é enviado aos destinatários.

Editar programação

O Arcserve UDP permite atualizar uma programação adicionada usando a opção Criar programação.

Siga estas etapas:

1. Efetue logon na interface da web do Arcserve Unified Data Protection.
2. Clique na guia **Relatórios**.
3. Clique na seção global **Filtros/ações**.
4. Na lista expandida, selecione o ícone de email para abrir a caixa de diálogo **Programar emails**.
5. Clique em **Editar** na caixa de diálogo **Programar emails**.

   A caixa de diálogo **Editar programação** é exibida.
6. Atualize os detalhes da programação e clique em **OK**.

   A programação atualizada é exibida na caixa de diálogo **Programar emails**.

   Observação: não clique em **OK**, caso deseje exibir o relatório imediatamente.
7. (Opcional) Para exibir o relatório atualizado imediatamente, clique em **Executar agora**.

   O relatório é enviado aos destinatários.

Enviar relatório por email

O Arcserve Unified Data Protection permite enviar relatórios individuais para destinatários específicos. Se um relatório for enviado por email, o conteúdo será igual ao conteúdo impresso e todos os gráficos serão enviados como imagens incorporadas.

Observação: antes de usar a opção **Enviar relatório por email**, defina as **Configurações de email**. Para obter mais informações sobre como configurar, consulte o tópico Configurar emails e alertas.

Siga estas etapas:

1. Efetue logon na interface da web do Arcserve Unified Data Protection.
2. Clique em **Relatórios** na barra de navegação e selecione um dos relatórios.
3. Clique na seção local **Filtros/ações**, disponível abaixo do nome do relatório selecionado.
4. Na lista expandida, selecione o ícone de email para abrir a caixa de diálogo **Enviar relatório por email**.

   Observação: se a configuração de email não estiver concluída, a caixa de diálogo **Aviso** informa que as configurações de email não foram definidas. Para obter mais informações sobre como configurar, consulte o tópico Configurar emails e alertas.

5. Preencha os seguintes campos:

   - **Para** : especifique o destinatário ao qual o email será enviado.

     Observação: este campo é definido por padrão no endereço de email especificado no módulo Configuração de email.

   - **CC**: especifique outros destinatários, separados por ponto-e-vírgula, aos quais deseja enviar o relatório.
   - **Prioridade**: especifique a prioridade do email. Esse campo é definido por padrão como Normal.
   - **Assunto**: especifique o assunto do email. Esse campo será padrão para o relatório selecionado.
   - **Comentário:** (opcional) especifique qualquer informação que deseja compartilhar.
   - **Anexo**: selecione os formatos para anexar os dados do relatório.

6. Clique em **OK**.

   O email é enviado com êxito.

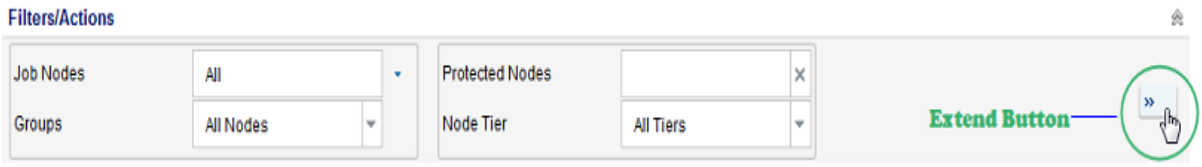
Gerar um relatório

É possível gerar relatórios predefinidos na guia **Relatórios.** É possível gerar os relatórios nos formatos PDF, CSV e HTML.

Siga estas etapas:

1. Navegue até a guia **Relatórios** e selecione um relatório no painel esquerdo.
2. Clique na lista suspensa local **Filtros/Ações**.
3. Forneça ou selecione os detalhes nas opções suspensas **Filtros/ações**.
4. Na lista suspensa do botão **Salvar**, clique em **CSV**, **PDF** ou **HTML**.

   Observação: as imagens grandes ou mais dados em uma página de relatório podem esconder algumas das opções, incluindo o botão Salvar. Para exibir essas opções, clique no botão Estender.



O relatório é gerado no formato selecionado.

Personalizar dias de retenção para um relatório de status de tarefa

Os dias de retenção padrão para o relatório de status da tarefa de recuperação são 180 dias. É possível modificar o número de dias de retenção que estão disponíveis na configuração mencionada em ConsoleConfiguration.xml no seguinte local:

Arquivos de programas\Arcserve\Unified Data Protection\Management\Configuration\ConsoleConfiguration.xml

De acordo com suas necessidades, é possível modificar o número de dias de retenção na configuração.

```
<PurgeConf>
<!-retentionDays, o valor padrão é 180 (180 dias). A unidade está em dias.
Número de dias para retenção de dados para o banco de dados do Console.-->
<retentionDays>180</retentionDays>
<!-purgeHourOfDay, valor padrão é 0 (0h00).
Executar a tarefa de eliminação nesse ponto do tempo todo dia.-->
<purgeHourOfDay>0</purgeHourOfDay>
</PurgeConf>
```

Tamanho dos dados brutos no relatório de capacidade gerenciado para o backup da VM sem agente com base em host

Você pode configurar os seguintes registros no nível de proxy e no nível da VM:

No nível de proxy para todas as VMs protegidas pelo atual do proxy:

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

"CountNtfsVolumeSize"=dword:00000001

"ReportZeroIfHavingNonNtfsVolume"=dword:00000001

"BackupZeroBlock"=dword:00000001

No nível de VM para uma VM específica:

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\{VM UUID}]

"CountNtfsVolumeSize"=dword:00000001

"ReportZeroIfHavingNonNtfsVolume"=dword:00000001

"BackupZeroBlock"=dword:00000001

Observação: o registro de nível de VM tem precedência sobre o registro de nível de proxy.

São observados os comportamentos a seguir:

Chave do Registro	Configuração padrão	Valores possíveis	Finalidade	Informações adicionais
GetVMGuestVolumeUsedSize	0	0 ou 1	Especifica se o espaço usado de todos os volumes de uma VM deve ser contado. 0 - Conta o	

			tamanho do arquivo VMDK da máquina virtual como o tamanho dos dados brutos da VM. 1 - Conta apenas o espaço usado dos volumes. **Observação:** para convidados do Windows, são considerados somente volumes Ntfs. Para convidados do Linux, todos os volumes são considerados.	
ReportZeroIfHavingNonNtfsVolume	0	0 ou 1	Especifica o comportamento da coluna de tamanho de dados brutos do relatório de capacidade de gerenciamento quando há	1. Ignorado quando GetVMGuestVolumeUsedSize=0 2. Aplicável apenas à VM do Windows

			volume(s) não Ntfs nas máquinas virtuais. 0 - O tamanho de volume(s) não Ntfs não é considerado como parte da coluna de tamanho de dados brutos. 1 - O tamanho geral de dados brutos é mostrado como 0 quando há volume(s) não Ntfs na máquina virtual	
BackupZeroBlock	0	0 ou 1	Especifica se deve gravar todos os blocos de dados em zero no destino de backup. 1 - Não grava nenhum bloco de dados no destino do backup. 0-Ignora os "zero" blocos de dados como parte	1. Ignorado quando GetVMGuestVolumeUsedSize=1 2. Se for alterado, o valor entrará em vigor somente após um backup completo

			do backup.	

Exemplo

Uma VM tem um disco virtual de pouco provisionamento com o tamanho provisionado de 1000 GB. O tamanho do arquivo VMDK do disco virtual é 800 GB, entre o qual 200 GB de blocos de dados são todos blocos de dados em zero. No sistema operacional convidado dessa VM, há 2 volumes NTFS cujo espaço usado é de 100 GB e 200 GB, respectivamente, e 1 volume FAT32 com o espaço usado de 1 GB.

Nomes de chaves	Valores padrão	Valores personalizados	Configurações personalizadas	Valores personalizados
GetVMGuestVolumeUsedSize	0	0	1	1
ReportZeroIfHavingNonNtfsVolume	N/D	N/D	1	1
Bloco de BackupZero	0	1	N/D	N/D
DataSize bruto esperado	600 GB (excluindo zero blocos de dados)	800 GB (incluindo "zero" blocos de dados)	300 GB	0

Visualizar valores reais na origem e no destino para tipos de tarefas

A tabela a seguir descreve os valores reais na origem e no destino exibidos para todos os tipos de tarefas para ajudar a compreender o relatório de status da tarefa:

Tipo de tarefa	Valor real na origem	Valor real no destino	Comentários
Backup de FS para repositório de dados (redução de redundância/sem redução de redundância) – nós Windows, nós Linux	Não disponível (N/D)	Exibido como esperado	
Backup de FS para compartilhamento de rede	N/D	Exibido como esperado	
Restauração de FS de compartilhamento de rede	N/D	N/D	
Armazenamento de dados sem redução de redundância de tarefas de backup CIFS	N/D	Exibido como esperado	
Armazenamento de dados sem redução de redundância de tarefas de restauração CIFS	Exibido como esperado	N/D	
Restaurar FS a partir de repositório de dados (redução de redundância/sem redução de redundância)	Exibido como esperado	N/D	
Cópia de arquivo de armazenamento de dados (redução de redundância/sem redução de redundância), cópia de arquivo do Ds de replicação	Exibido como esperado	N/D	**Observação:** aqui, as colunas “Dados protegidos” e “Armazenamento usado” também são exibidas como “N/D"
Arquivamento de arquivo do repositório de dados (redução de redundância/sem redução de redundância), arquivamento de arquivo do repositório de dados de replicação	Exibido como esperado	N/D	**Observação:** aqui, as colunas “Dados protegidos” e “Armazenamento usado” também são exibidas como “N/D"
Cópia de arquivo/arquivamento de arquivo no compartilhamento N\W	N/D	N/D	**Observação:** aqui, as colunas “Dados protegidos” e “Arma-

			zenamento usado" também são exibidas como "N/D"
Cópia de arquivo/restauração do arquivamento de arquivo	N/D	N/D	**Observação:** aqui, as colunas "Dados protegidos" e "Armazenamento usado" também são exibidas como "N/D"
Excluir arquivamento de arquivo	N/D		**Observação:** aqui, as colunas "Dados protegidos" e "Armazenamento usado" também são exibidas como "N/D"
Tarefa de catálogo FS (com base em agente/sem agente)	Exibido como esperado	N/D	
CRP do armazenamento de dados (redução de redundância, sem redução de redundância)	Exibido como esperado	N/D	**Observação:** aqui, as colunas "Dados protegidos" e "Armazenamento usado" também são exibidas como "N/D"
CRP compartilhamento N\W, Local	N/D	N/D	**Observação:** aqui, as colunas "Dados protegidos" e "Armazenamento usado" também são exibidas como "N/D"
Restauração de CRP para compartilhamento N\W, Local	N/D	N/D	**Observação:** aqui, as colunas "Dados protegidos" e "Armazenamento usado" também são exibidas como "N/D"
Tarefas da máquina virtual instantânea	Exibido como esperado	N/D	**Observação:** aqui, as colunas "Dados protegidos" e "Armazenamento usado" também são exibidas como "N/D"

Tarefas da recuperação garantida	Exibido como esperado	N/D	
Recuperação Bare Metal do repositório de dados (redução de redundância/sem redução de redundância)	Exibido como esperado	N/D	**Observação:** aqui, as colunas “Dados protegidos” e “Armazenamento usado” também são exibidas como “N/D"
Tarefas do modo de espera virtual	Exibido como esperado	N/D	**Observação:** aqui, as colunas “Dados protegidos” e “Armazenamento usado” também são exibidas como “N/D"
Tarefas da cópia em fita	Exibido como esperado	N/D	**Observação:** aqui, as colunas “Dados protegidos” e “Armazenamento usado” também são exibidas como “N/D"
Tarefas de replicação, tarefas de replicação entre sites	Exibido como esperado	N/D	**Observação:** aqui, as colunas “Dados protegidos” e “Armazenamento usado” também são exibidas como “N/D"
Tarefas de replicação do MSP	Exibido como esperado	Exibido como esperado	**Observação:** aqui, as colunas “Dados protegidos” e “Armazenamento usado” também são exibidas como “N/D"
Início rápido do RPS a partir do compartilhamento N/W	Exibido como esperado	N/D	**Observação:** aqui, as colunas “Dados protegidos” e “Armazenamento usado” também são exibidas como “N/D"
Início rápido do RPS (armazenamento de dados com redução de redundância / sem redução de redundância)	Exibido como esperado	Exibido como esperado	**Observação:** aqui, as colunas “Dados protegidos” e “Arma-

			zenamento usado” também são exibidas como “N/D"

Capítulo 7: Gerenciando a alta disponibilidade

Esta seção contém os seguintes tópicos:

Como funciona a alta disponibilidade

Usando o Unified Data Protection, é possível monitorar e gerenciar as funções do Arcserve High Availability na guia **alta disponibilidade.** Para gerenciar essas funções, você deve primeiro efetuar logon no Serviço de controle. Quando você primeiro clica na guia **Alta disponibilidade**, a caixa de diálogo **Adicionar serviço de controle** é exibida. Essa caixa de diálogo não será exibida depois.

Gerenciar serviços de controle de alta disponibilidade

Siga estas etapas:

1. Clique na guia **Alta disponibilidade**.

   A caixa de diálogo **Gerenciar serviço de controle** é aberta.

2. Digite os detalhes do Serviço de controle, como o endereço IP, o nome de conta, a senha, o protocolo e o número da porta.

3. Clique em **OK**.

   O serviço de controle especificado é adicionado abaixo do título Cenários e serviços de controle no painel esquerdo. Para modificar ou excluir o serviço de controle, selecione Serviço de controle e clique com o botão direito do mouse para ver as opções. Também é possível selecionar Serviço de controle no painel central e clicar em **Ação** para modificar ou excluir um serviço de controle. Ou, clique com o botão direito do mouse no serviço de controle no painel de navegação

   Observação: expanda o serviço de controle para exibir cenários, grupos e outros detalhes.

Gerenciar licenças de alta disponibilidade

Siga estas etapas:

1. Clique na guia **Alta disponibilidade**.
2. No painel à esquerda, clique em **Cenários e serviços de controle**.

   A página **Serviços de controle e cenários** é exibida.
3. Selecione Serviço de controle e clique em **Registrar**.

   A caixa de diálogo **Registrar** é exibida.
4. Digite a chave de registro
5. Clique em **OK**.

   A licença é registrada.

Gerenciar cenários

O Arcserve Unified Data Protection permite gerenciar os cenários de alta disponibilidade existentes e será possível criar cenários do tipo Sistema completo. Também será possível criar grupos de cenários para organizar seus cenários. As seções a seguir descrevem como gerenciar cenários de HA:

- Gerenciar grupos de cenários
- Criar cenários do tipo Sistema completo
- Gerenciar cenários
- Editar cenários
- Gerenciar hosts de cenário
- Operações em cenários
- BMR e replicação inversa
- Monitorar cenários

Gerenciar grupos de cenários

O Arcserve Unified Data Protection permite gerenciar grupos em um serviço de controle. É possível adicionar, renomear, excluir, sinalizar e publicar comentários para um grupo.

Siga estas etapas:

1. Selecione um serviço de controle gerenciados no painel esquerdo.

   Todos os grupos no serviço de controle são listados no painel central.

2. Clique no menu suspenso **Ações** e, em seguida, clique em um dos seguintes:

   Adicionar grupo de cenários

   Cria um grupo.

   Selecione um grupo para executar as seguintes ações:

   Renomear o grupo de cenários

   Renomeia o grupo.

   Remover o grupo de cenários

   Exclui o grupo. Se o grupo tiver cenários, não será possível removê-lo.

   Sinalizar e comentar

   Sinaliza o grupo em diversas cores e permite adicionar comentários ao sinalizador. Use os sinalizadores para personalizar e identificar facilmente seu grupo.

3. Opcionalmente, clique com o botão direito em um grupo no painel à esquerda para adicionar, excluir ou renomear um grupo do serviço de controle selecionado.

   O grupo é adicionado ou atualizado com base em sua seleção.

Criar cenários do tipo Sistema completo

Siga estas etapas:

1. No painel à esquerda, clique em **Cenários e serviços de controle** e, em seguida, clique em um serviço de controle gerenciado.

   Todos os grupos de cenários do serviço de controle são listados.

2. Clique em um grupo de cenários.

   A página **Cenários** é exibida no painel central.

3. No painel central, clique em **Criar cenário**.

   Observação: como alternativa, no painel esquerdo, clique com o botão direito do mouse e, em seguida, clique em **Criar cenário**.

   O assistente **Criar sistema completo** abre e a caixa de diálogo **Selecionar tipo de servidor e de produto** é exibida.

4. Digite o nome do cenário, selecione o tipo de produto, e especificar se deseja fazer o teste AR.

5. Clique em **Avançar**.

   A caixa de diálogo **Host do mestre e de réplica** é exibida.

6. Digite os detalhes de mestre e réplica.

7. Clique em **Avançar**.

   Os mecanismos serão verificados nos hosts se tiver selecionado a opção **Verificar o mecanismo nos hosts**. Também é possível instalar ou desinstalar mecanismos nos hosts.

8. Clique em **Avançar** após a verificação dos mecanismos.

   A caixa de diálogo **Configurações de volume** é exibida.

9. Selecione os volumes que deseja proteger.

   Observação: quando você seleciona a opção **Permitir a exclusão de diretório e arquivos**, os arquivos e as pastas pagefile.sys, hyberfil.sys, informações do volume do sistema, Reciclador e Reciclado são filtrados por padrão.

10. Clique em **Avançar**.

    A caixa de diálogo **Seleção de pool de recursos** é exibida. É possível selecionar o pool de recursos no qual a VM está localizada após a alternância ou durante o teste AR.

11. Clique em **Avançar**.

    A caixa de diálogo **Seleção de armazenamento** é exibida.

12. Selecione o repositório de dados para armazenar a máquina virtual. Opcionalmente, selecione **Espaço alocado e comprometido sob demanda (usando o disco dinâmico)**. A VM gerada usa provisão dinâmica para seu disco virtual se esta opção for selecionada.
13. Clique em **Avançar**.

    A caixa de diálogo **Propriedades do cenário** é aberta.
14. Expanda as propriedades e modifique conforme desejado, e clique em **Avançar**. Para obter mais informações, consulte o Guia do Administrador do Arcserve RHA.

    A caixa de diálogo **Propriedades do mestre e da réplica** é aberta.
15. Revise as propriedades do mestre e da réplica e, em seguida, use a opção **Clique para editar os mapeamentos de redes físicas**.

    A caixa de diálogo **Mapeamento do adaptador de rede de alta disponibilidade** é exibida.

    Observação: quando há apenas um adaptador de rede virtual nos servidores mestre e de réplica, eles são mapeados automaticamente.
16. Siga as seguintes etapas:
    a. No **Adaptador de rede de réplica**, clique para escolher o adaptador que deseja mapear para o adaptador listado na coluna Adaptador de rede mestre.
    b. Em **Aplicar informações do adaptador mestre** (padrão), selecione se o adaptador mestre estivá no modo DHCP.
    c. Em **Personalizar as informações do adaptador**, selecione para ativar a configuração de IP, gateways, servidores DNS e WINS. Adicionar ou remover endereço IP, gateways, servidores DNS e servidores WINS conforme necessário.
17. Clique em OK para fechar a caixa de diálogo **Mapeamentos do adaptador de rede** e clique em **Avançar** para continuar.

    A caixa de diálogo **Propriedades de alternância** é exibida.
18. Expanda **Redirecionamento do tráfego da rede** e outras propriedades para verificar os valores e, em seguida, clique em **Avançar**.

    A caixa de diálogo **Início da alternância e da replicação inversa** abre.
19. Especifique o tipo de alternância. Para cenários de sistema completo, a replicação inversa é manual.
20. Clique em **Avançar**.

Aguarda enquanto o processo de verificação do cenário é concluído e abre a caixa de diálogo **Verificação do cenário**.

Se o processo de verificação do cenário listar algum erro, será necessário resolvê-lo para poder continuar. Se algum aviso for listado, você também deverá resolvê-lo para poder continuar com êxito. Após fazer as alterações, clique em **Repetir** para repetir a verificação.

21. Clique em **Avançar**.

    A caixa de diálogo **Execução do cenário** é aberta.

22. Clique em **Concluir** para salvar as configurações atuais e executar o cenário mais tarde.

    Como opção, para executar o cenário imediatamente, selecione **Executar agora depois de clicar no botão Concluir** e, em seguida, clique em **Concluir**.

    Para cenários de sistemas completos, selecione **Sincronização de volumes**.

    O cenário é criado.

Gerenciar cenários

Quando você seleciona um serviço de controle gerenciado no painel esquerdo, todos os cenários no serviço de controle são exibidos no painel central. Os cenários são listados com o seu tipo, estado, produto, modo. As estatísticas de RTO /RPO, uso do spool do mestre e o andamento da sincronização também são listados aqui. É possível executar várias operações como excluir, renomear, sinalizar, ou comentar selecionando um cenário.

Siga estas etapas:

1. No painel à esquerda, clique em **Cenários e serviços de controle** e, em seguida, clique em um serviço de controle gerenciado.

   Todos os grupos de cenários no serviço de controle são listados no painel central.

2. No painel à esquerda, clique em um grupo de cenários.

   Os cenários no grupo de cenários são listados no painel central.

3. Selecione um cenário.

4. Clique no menu suspenso **Ações** e, em seguida, clique em um dos seguintes:

   Renomear cenário

   Renomeia o cenário.

   Remover cenário

   Exclui o cenário.

   Se o grupo tiver cenários, não será possível removê-lo.

5. Opcionalmente, no painel esquerdo, clique com o botão direito em um cenário para remover ou renomear um cenário.

   O cenário é atualizado.

Editar cenários

O Arcserve Unified Data Protection permite que você edite as propriedades do cenário enquanto o cenário está no estado interrompido. É possível inserir, renomear ou excluir hosts ou modificar a topologia de um cenário.

Siga estas etapas:

1. No painel à esquerda, clique em **Cenários e serviços de controle** e, em seguida, clique em um serviço de controle gerenciado.

   Todos os grupos de cenários no serviço de controle são listados no painel central.

2. No painel à esquerda, clique em um grupo de cenários e clique em um cenário.

   A página <grupo de cenários>:<cenário> é exibida.

3. Selecione um host do cenário.

4. Clique na guia **Propriedades** e selecione uma das seguintes opções na lista suspensa.

   Propriedades do cenário

   Atualiza as propriedades dos cenários.

   Propriedades de HA

   Atualiza as propriedades de alta disponibilidade.

   Propriedades do host

   Atualiza as propriedades do host.

   Diretórios raiz

   Atualiza os diretórios raiz.

   Observação: isso se aplica somente a cenários de sistema completo.

5. Clique em **Salvar** no menu suspenso **Ação**.

   As propriedades do cenário são atualizadas.

   Edite as configurações de plataforma virtual para um cenário de sistema completo interrompido:

   Siga estas etapas:

1. Selecione o host de réplica do cenário.

2. Clique na guia **Propriedades** e **Propriedades do host** na lista suspensa.

3. Expanda **Máquina virtual** e clique em **Clique aqui para editar a configuração da plataforma virtual.**

   O assistente **Configuração da plataforma virtual** é exibido.

4. Selecione o **Tipo de plataforma virtual** e o endereço IP ou nome de host relacionado.
5. Selecione o pool de recursos para ESX e vCenter ou Host Server para Citrix Xen.
6. Selecione o repositório. No Hyper-V, procure os diretórios e selecione o local da VM no servidor Hyper-V.
7. Clique em **Concluir**.

Edite o mapeamento do adaptador de rede de alta disponibilidade ou a recuperação garantida:

Siga estas etapas:

1. Selecione o host de réplica a partir do cenário.
2. Clique na guia **Propriedades** e selecione **Propriedades do host** na lista suspensa.
3. Expanda a **Máquina virtual** e clique em **Configuração da máquina virtual.**
4. Clique em **Clique aqui para editar mapeamentos da rede física** para a propriedade **Mapeamento do adaptador de rede de alta disponibilidade** ou **Mapeamento do adaptador de rede de recuperação garantida**.

   A caixa de diálogo **Mapeamento do adaptador de rede de alta disponibilidade** é exibida.
5. Selecione os adaptadores de rede da réplica que deseja mapear o adaptador de rede mestre.

   É possível personalizar as informações do adaptador do adaptador de réplica, incluindo o endereço IP, gateway, servidores DNS e WINS.
6. Clique em **OK**.

   Os mapeamentos são modificados e salvos.

Gerenciar hosts de cenário

É possível inserir, excluir e renomear hosts em um cenário.

Siga estas etapas:

1. No painel à esquerda, clique em **Cenários e serviços de controle** e, em seguida, clique em um serviço de controle gerenciado.

   Todos os grupos de cenários no serviço de controle são listados no painel central.

2. No painel à esquerda, clique em um grupo de cenários e clique em um cenário.

   A página <grupo de cenários>:<cenário> é exibida.

3. Selecione um host do cenário.

4. Clique no menu suspenso **Editar** e, em seguida, clique em uma das seguintes opções:

   Inserir o host

   Insere um host filho ao host selecionado no cenário.

   Remover host

   Exclui o host selecionado do cenário.

   Renomear host

   Renomeia o host selecionado no cenário.

   Salvar

   Salva todas as modificações nas propriedades do cenário.

   Parar

   Atualiza todas as modificações.

   As propriedades do cenário são modificadas.

Operações em cenários

É possível executar várias operações nos cenários.

Siga estas etapas:

1. No painel à esquerda, clique em **Cenários e serviços de controle** e, em seguida, clique em um serviço de controle gerenciado.

   Todos os grupos de cenários no serviço de controle são listados no painel central.

2. No painel à esquerda, clique em um grupo de cenários e clique em um cenário.

   A página <grupo de cenários>:<cenário> é exibida.

3. Clique no menu suspenso **Ações** e, em seguida, clique em uma das seguintes opções:

   Executar

   Após criar um cenário, você deve executá-lo para iniciar o processo de replicação. Geralmente, antes que as alterações de dados no mestre possam ser replicadas na Réplica, o mestre e a réplica devem ser sincronizados. Portanto, a primeira etapa ao iniciar uma replicação é sincronizar os servidores mestre e de réplica. Após a sincronização dos servidores, uma replicação online é iniciada automaticamente, atualizando continuamente a réplica com todas as alterações que ocorrem no mestre.

   Executar (Modo de avaliação)

   O modo de avaliação permite que você avalie a utilização exata da largura de banda e o desempenho da taxa de compactação necessária para replicação, sem realmente replicar dados. Nenhuma replicação ocorre quando este comando é executado, mas as estatísticas são obtidas. Um relatório é fornecido após a interrupção do processo de avaliação.

   Interromper

   Você deve interromper a execução de um cenário para definir ou alterar as propriedades. Você poderia interromper os cenários em execução ou o modo de avaliação.

   Sincronizar

   A sincronização é um processo para tornar os dados consistentes no mestre e na réplica. Ativar o processo de sincronização (com a replicação em execução ou não).

   Relatório de diferenças

Um relatório de diferenças compara as diferenças entre o mestre e a réplica em um determinado ponto. A comparação é realizada com os mesmos algoritmos utilizados no processo de sincronização, mas nenhum dado é transferido. O relatório de diferenças é gerado para cada réplica e é enviado ao gerenciador no final do processo. É possível gerar esse relatório a qualquer momento.

Executar a alternância

A alternância (ou tolerância a falhas) é o processo de alteração de funções entre o mestre e a réplica. Isso significa transformar o servidor mestre no servidor em espera e o servidor de réplica no servidor ativo.

Recuperar o servidor ativo

Se o processo de alternância não foi concluído corretamente, será possível selecionar manualmente o servidor que atua como servidor ativo por meio de um processo chamado Recuperar o servidor ativo.

Suspender a verificação de atividade

Suspenda a verificação de atividade que verifica se o servidor ativo está em operação. É possível suspender/retomar manualmente a verificação de atividade de um cenário HA em execução.

Teste de integridade de réplica

A opção Recuperação garantida permite realizar um teste totalmente transparente da capacidade de recuperação dos dados no servidor de réplica. O servidor de réplica que é testado é aquele que assume a função do servidor de produção quando este fica inativo. A opção Recuperação garantida é um verdadeiro teste de servidor, aplicativos e ações reais, o que será necessário caso seja preciso fazer a alternância para o servidor de réplica, torná-lo o servidor ativo e executar suas funções.

Iniciar/interromper a VM

Use esta operação para iniciar ou parar uma máquina virtual a partir do status mais recente do sistema ou a partir de um marcador. É possível iniciar ou interromper uma máquina virtual após a criação de um cenário e sincronizar o mestre e a réplica. Use esse recurso quando o cenário não estiver em execução. O recurso está disponível para cenários Sistema completo de recuperação de falhas e alta disponibilidade. Iniciar/interromper é um item de menu de alternância.

Suspender a replicação

Suspender atualizações no host de réplica, para a realização de uma manutenção do sistema ou alguma outra forma de processamento que não modifica

os dados nele replicados. As alterações continuam sendo registradas para atualização na réplica suspensa, mas não são transferidas efetivamente antes de a replicação ser retomada. Não é possível suspender a replicação durante a sincronização.

Excluir todos os recursos da VM

Ao executar um cenário Sistema completo, alguns recursos temporários são criados, como arquivos de disco, instantâneos e outros arquivos. Essa operação permite excluir tais recursos e está disponível quando o cenário não está em execução.

Restauração de dados

Recuperar dados perdidos ou corrompidos no mestre, a partir de qualquer réplica, por meio da ativação de um processo de direcionamento inverso.

Definir o marcador de retrocesso

Um marcador é um ponto de verificação definido manualmente para marcar um estado anterior para o qual é possível reverter. Essa configuração manual é chamada de marcador de retrocesso de configuração. É recomendável definir um marcador antes de qualquer atividade que possa comprometer a estabilidade dos dados. Os marcadores são definidos em tempo real, e não para eventos já ocorridos.

A operação selecionada será executada.

BMR e replicação inversa

O Arcserve Unified Data Protection permite processar a BMR e a replicação inversa para seu cenário do sistema completo.

Siga estas etapas:

1. Prepare um computador bare metal inicializando-o a partir do CD BMR.
2. Selecione o cenário do sistema completo e clique em **Restaurar** no menu suspenso **Ação.**

   O **Assistente de restauração de dados** é aberto.
3. Siga as instruções exibidas nas telas do assistente para criar e executar o cenário de recuperação.

   Observação: na página **Mapeamento de volume**, se os volumes forem mapeados automaticamente para a origem e para o destino, o mapeamento de volume personalizado estará desativado. Para ativar o mapeamento de volume personalizado, clique em **Limpar** para remover o mapeamento anterior. Clique com o botão direito do mouse no volume selecionado e selecione **Mapeamento de volume personalizado** para abrir a caixa de diálogo **Redimensionar o tamanho do volume** e altere o tamanho, conforme necessário.

Para executar a replicação inversa, siga estas etapas:

1. Prepare um computador bare metal inicializando-o a partir do CD BMR.
2. Selecione o cenário do sistema completo que executou a alternância e a tolerância a falhas e clique em **Executar** no menu suspenso **Ações**.

   O **Assistente de restauração de dados** é aberto.
3. Siga as instruções exibidas nas telas do assistente para criar e executar o cenário de recuperação.

   Os dados são restaurados no computador bare metal. Se selecionou a alternância automática, o processo de alternância será iniciado e o computador bare metal estará pronto. Se selecionou a alternância manual, inicie manualmente o processo de alternância.

Monitorar cenários

O Arcserve Unified Data Protection permite monitorar os cenários de recuperação de falhas e de alta disponibilidade, fornecendo diversas estatísticas e relatórios.

Siga estas etapas:

1. No painel central, selecione um cenário.

   O status do cenário em execução é exibido com detalhes como os dados enviados, arquivos enviados, dados recebidos, arquivos recebidos, etc.

2. Clique na guia **Estatísticas** para ver mais detalhes. A guia tem as seguintes categorias:

   Executando estatísticas

   Exibe os dados estatísticos detalhados dos dados quando o cenário estiver em execução.

   Registro histórico

   Exibe os relatórios de sincronização, relatórios de diferenças e relatórios de teste AR.

3. Clique na guia **Eventos**, para ver todos os eventos de um cenário selecionado. Para copiar ou excluir os eventos, selecione o evento e clique com o botão direito do mouse e, em seguida, selecione **Mostrar eventos** para abrir a caixa de diálogo Mostrar eventos para copiar ou excluir os eventos. Use as teclas Shift+Ctrl para selecionar vários eventos.

   Observação: os eventos são automaticamente atualizados. Os cinco eventos críticos recentes são exibidos no painel quando você seleciona um cenário.

4. Selecione o cenário de cenários no painel esquerdo. Todos os cenários no grupo são listados no painel central. É possível verificar o uso de spool do mestre, RTO/RPO e o andamento da sincronização nesta lista.

5. Os detalhes do painel direito exibem informações do cenário como o nome do cenário, o estado do cenário e o andamento da sincronização.

   Observação: no painel direito, o Uso do spool (% de spool) indica o uso do spool do mestre no cenário.

Instalação remota

O Arcserve Unified Data Protection permite implantar o mecanismo nos hosts remotos a partir de um serviço de controle gerenciado. Também é possível gerenciar a instalação e verificação a partir da lista de hosts.

Siga estas etapas:

1. No painel à esquerda, clique em **Instalação remota**.

   A página **Instalação remota** é exibida no painel central.

2. Na lista suspensa **Serviço de controle**, selecione o serviço de controle que você deseja usar para implantar o mecanismo.

   Os hosts existentes em que o mecanismo foi instalado ou verificado anterior são listados no painel central.

3. No menu suspenso **Ação**, clique em **Adicionar hosts**.

   A caixa de diálogo **Hosts para Instalar o mecanismo** é exibida.

4. Digite o nome do host ou endereço IP do host e clique em **Adicionar**.

   O host é adicionado à lista.

5. Clique em **OK**.

   A caixa de diálogo **Adicionar hosts** é exibida.

6. Selecione uma das seguintes opções:

   Editar hosts

   Abre a caixa de diálogo **Hosts para instalar o mecanismo**, que permite adicionar hosts ou gerenciar os existentes.

   Alterar as configurações de instalação

   Abre a caixa de diálogo **Editar configurações da instalação.** É possível especificar os seguintes detalhes:

   Conta de instalação

   Conta de serviço

   Porta

   Usar configurações anteriores ao reinstalar ou atualizar

   Atualiza ou reinstala um mecanismo existente do RHA.

7. Clique em **OK**.

8. O host é exibido na página **Instalação remota**.

   A coluna **Status** exibe o status de instalação.

Observação: mova o mouse sobre o status para obter os detalhes, em caso de falha na instalação.

Ações de instalação remota

Você pode executar várias operações nos hosts adicionados.

Siga estas etapas:

1. No painel central, selecione um host.
2. Clique na lista suspensa **Ações** e, em seguida, selecione um dos seguintes itens:

Adicionar hosts

Abre a caixa de diálogo **Hosts para Instalar o mecanismo** é exibida. Consulte Instalação remota para obter mais detalhes.

Instalar/atualizar

Instala ou atualiza o mecanismo de HA no host selecionado.

Desinstalar

Desinstala o mecanismo de HA no host selecionado.

Editar configurações

Abre a caixa de diálogo **Editar configurações da instalação**.

Verificar status de hosts

Verifica a existência do host.

Remover hosts

Remove o host da lista.

Exibir logs

Abre a caixa de diálogo **Logs de instalação remota** e exibe os logs de todos os hosts remotos. Clique em Atualizar para exibir os logs mais recentes.

A operação foi concluída com êxito.

Relatórios de alta disponibilidade

O Arcserve Unified Data Protection fornece vários relatórios para monitorar o status de Alta disponibilidade. É possível aplicar filtros para gerar vários tipos de relatórios, conforme necessário.

Siga estas etapas:

1. Clique na guia **Cenários e serviços de controle**.
2. No painel à esquerda, clique em **Relatórios**.
3. A página **Relatórios** é exibida no painel central.
4. No painel central, selecione um serviço de controle da lista suspensa **Serviço de controle**.
5. Digite detalhes e aplique filtros conforme necessário.

   O relatório do HA é gerado.

Capítulo 8: Usando o utilitário VSphereConfig

Esta seção contém os seguintes tópicos:

Ativar ou desativar a marcação VSPhereBackupNFC usando o prompt de comando

Importante: Ative a marcação VSphereBackupNFC no adaptador de kernel específico para backup (em vez da rede de backup específica) quando uma VM de origem hospeda o hipervisor ESXi e o backup usa o VDDK7 ou versões posteriores.

O Arcserve UDP permite ativar ou desativar a marcação *VSphereBackupNFC* usando o prompt de comando. A ferramenta de linha de comando (*AFVSphereConfigTool.exe)* permite ativar ou desativar a marcação VSphereBackupNFC em um adaptador de kernel específico.

Esta seção fornece informações sobre como ativar ou desativar a marcação *VSphereBackupNFC* usando o prompt de comando.

Siga estas etapas:

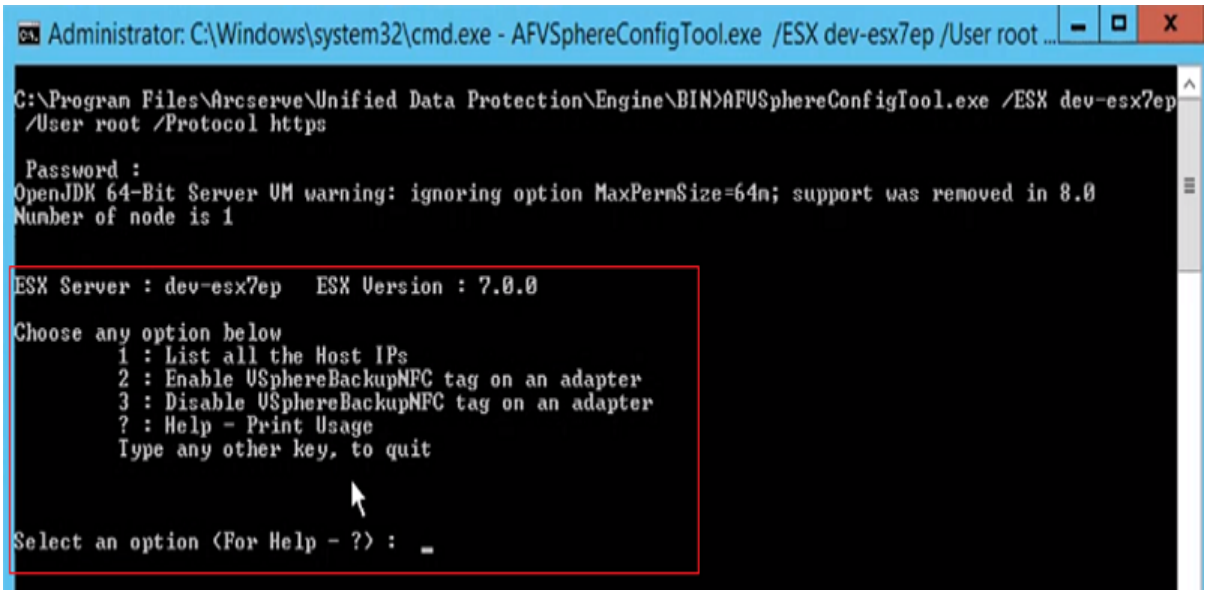
1. Abra o prompt de comando e navegue até <Engine>\BIN>.

   Exemplo: C:\Arquivos de programas\Arcserve\Unified Data Protection\Engine\BIN>

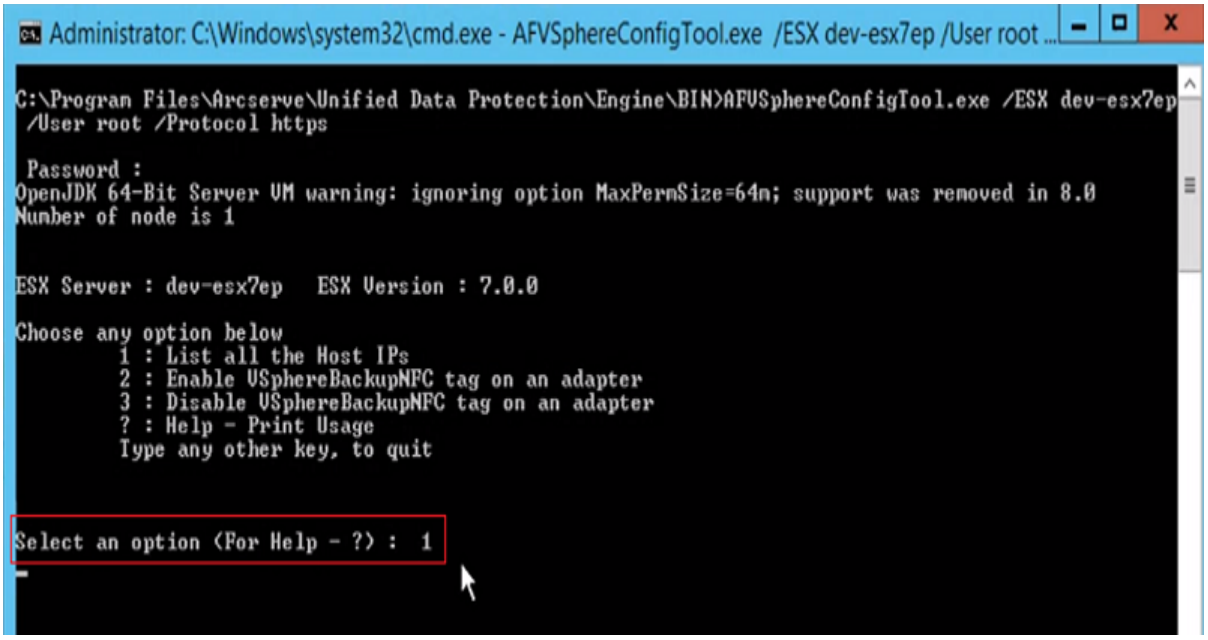
2. Conecte-se ao servidor ESX usando a ferramenta de linha de comando (*AFVSphereConfigTool.exe*) e, em seguida, digite uma senha quando solicitado.

   AFVSphereConfigTool.exe /ESX dev-esx7ep /user root /protocol https

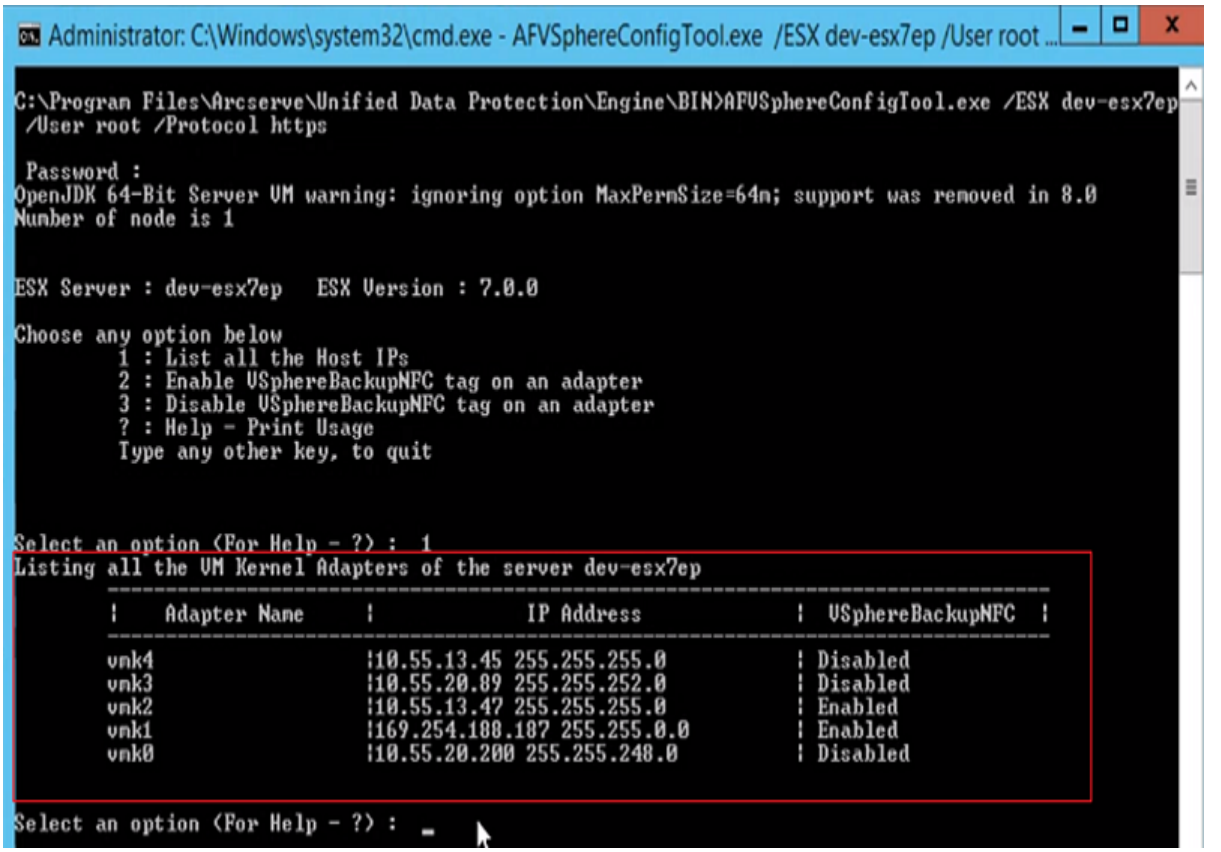
   O servidor ESX selecionado (dev-esx7ep) agora está conectado.



3. Depois de se conectar ao servidor ESX com êxito, quando for solicitado a selecionar uma opção, faça o seguinte:
   - Para listar todos os adaptadores de kernel da VM do servidor ESX, digite o número da opção. Por exemplo, digite 1 para a opção.

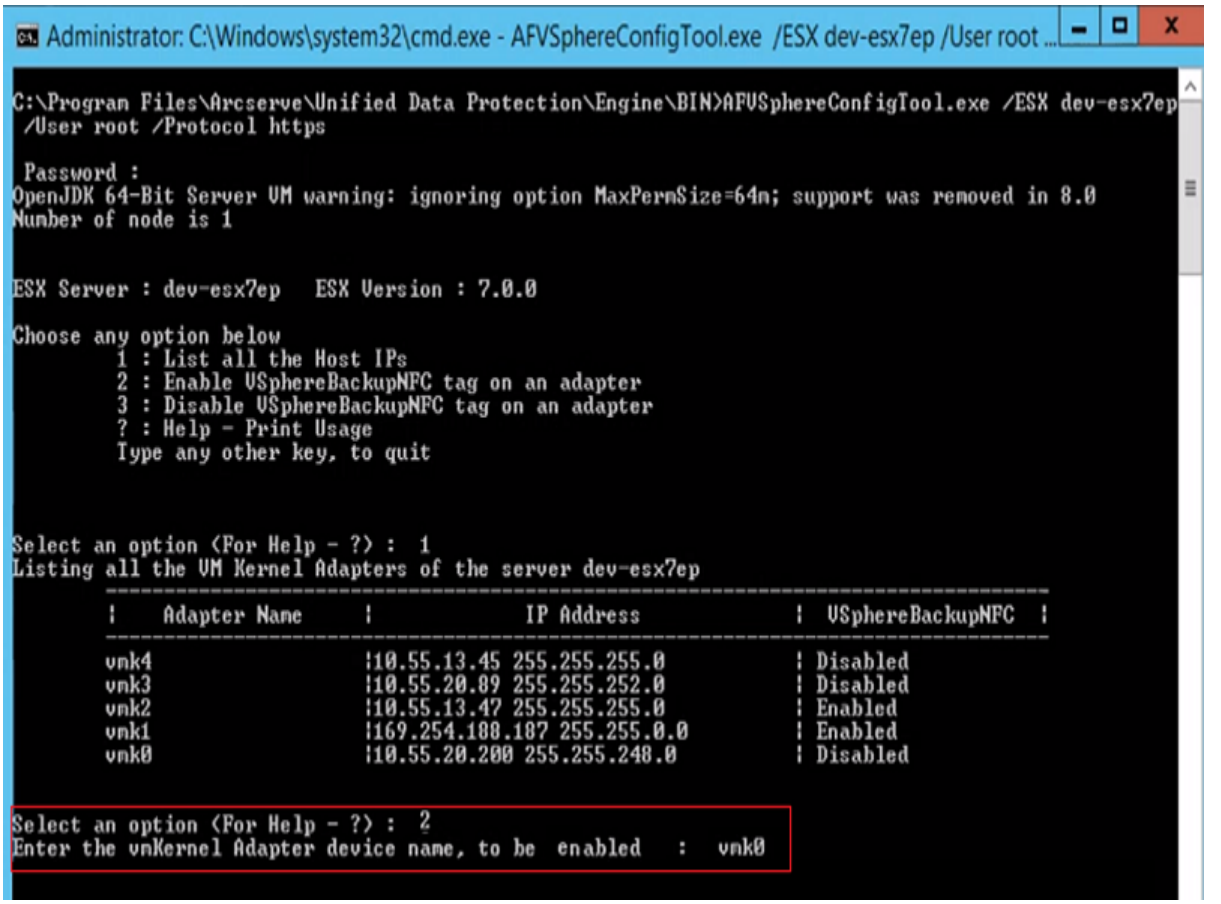


Uma lista de todos os adaptadores de kernel da VM é exibida.

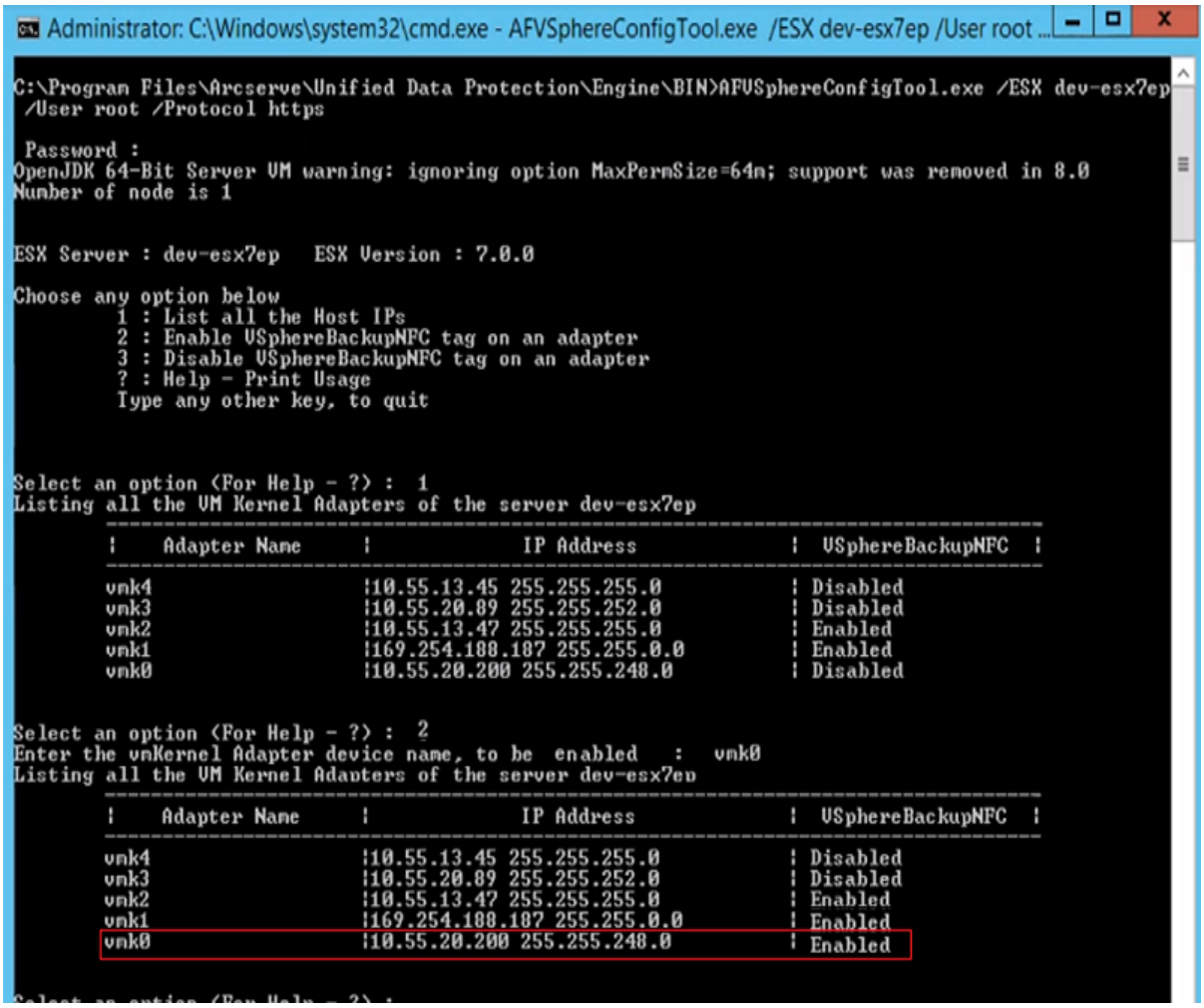


- Para ativar a marcação VSphereBackupNFC em um adaptador, digite o número da opção. Por exemplo, digite 2 para a opção.

  Quando solicitado a inserir o nome do dispositivo adaptador de kernel da VM, digite o nome do dispositivo.

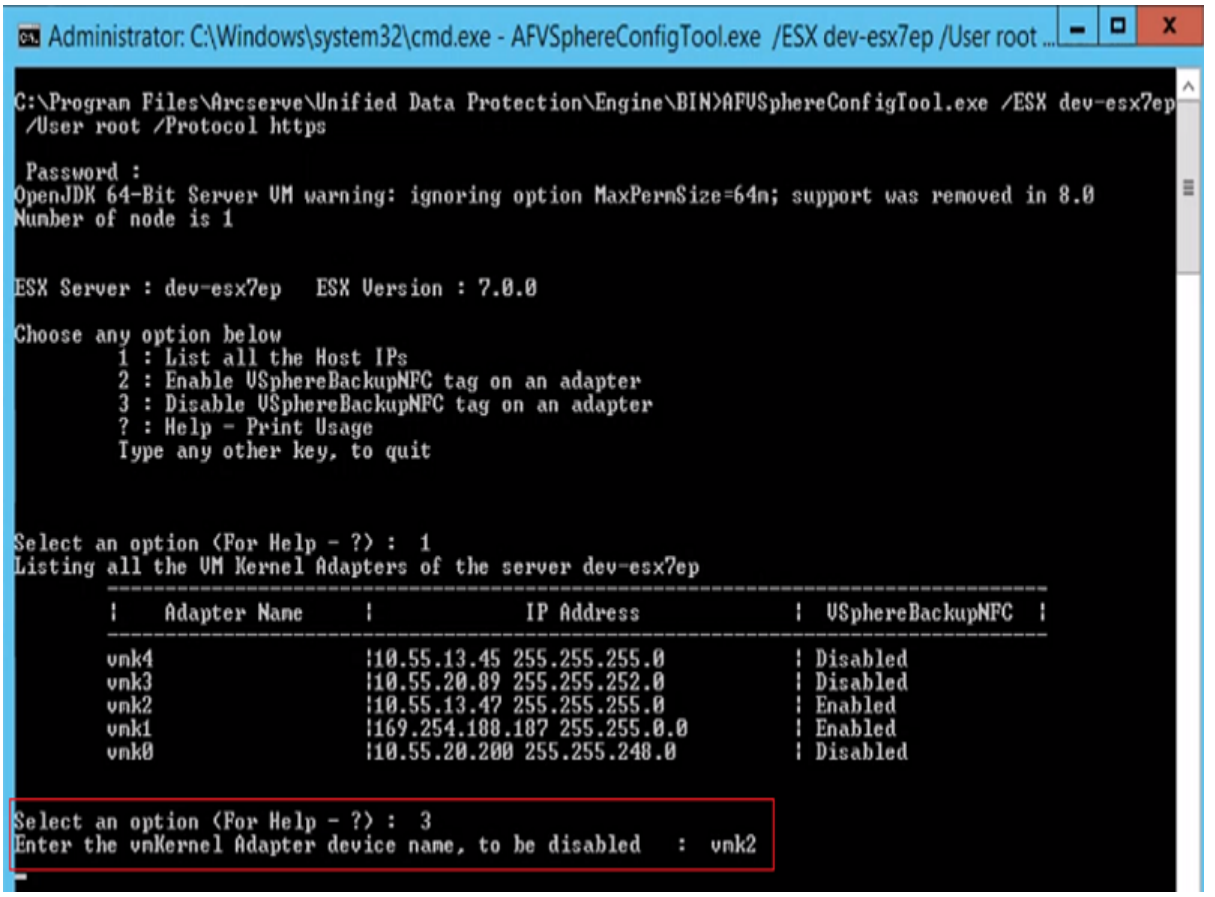


A marcação VSphereBackupNFC é ativada no adaptador selecionado.

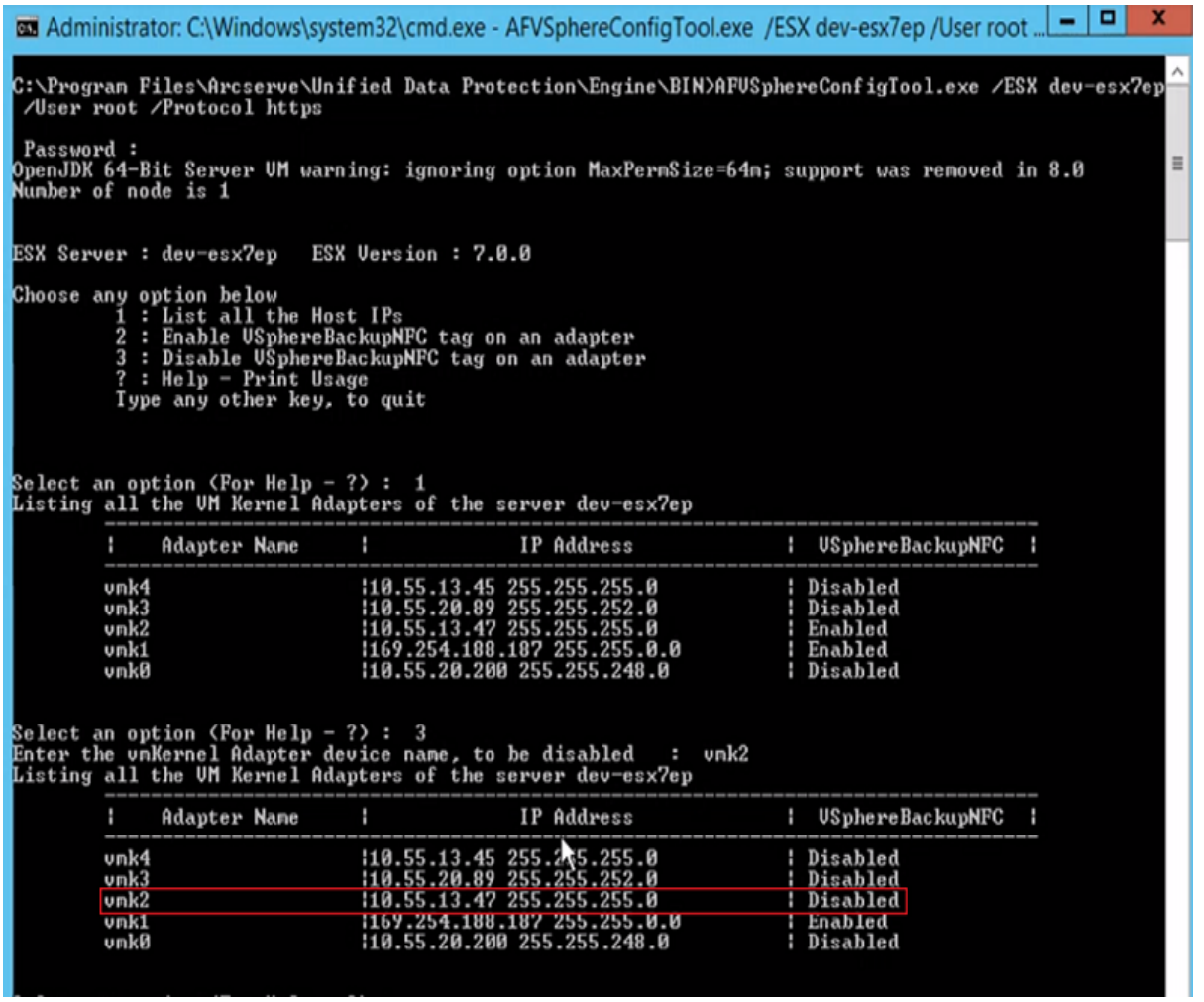


- Para desativar a marcação VSphereBackupNFC em um adaptador, digite o número da opção. Por exemplo, digite 3 para a opção.

  Quando solicitado a inserir o nome do dispositivo adaptador de kernel da VM, digite o nome do dispositivo.



A marcação VSphereBackupNFC é desativada no adaptador selecionado.



4. Digite qualquer chave (exceto 1, 2, 3 e ?) para fechar o prompt de comando.

Capítulo 9: Usando o Utilitário de diagnóstico

O utilitário de diagnóstico permite coletar logs das máquinas. Quando entrar em contato com a equipe de suporte da Arcserve sobre qualquer problema, a equipe de suporte emprega os logs para investigar e corrigir o problema.

Esta seção contém os seguintes tópicos:

Coletar informações de diagnóstico

As informações de diagnóstico são uma coleção de informações de logs, eventos, registros e aplicativos do produto e do sistema, que a equipe de suporte do Arcserve necessita para investigar qualquer erro. O Arcserve UDP permite coletar todas essas informações em um único local; geralmente, um caminho de compartilhamento da rede. Quando você entra em contato com o suporte do Arcserve, você tem essas informações prontamente disponíveis. É possível coletar os dados de diagnóstico para máquinas Windows, Linux, VMware e Hyper-V.

Observação: para servidores de backup Linux, a opção **Coletar informações de diagnóstico** está disponível apenas nos **Nós do <nome_do_site>:** exibição **Grupos de servidores de backup Linux**.

Siga estas etapas:

1. No console, clique em **Recursos**.
2. Execute uma das seguintes etapas, dependendo do tipo de nó:

   Para servidores de backup Linux

   - No painel de navegação à esquerda, vá até **Nós** e clique em **Grupos de servidores de backup Linux**.
   - No painel central, selecione todos os nós Linux.

   Para todos os outros nós e servidores

   - No painel de navegação à esquerda, vá para **Nós** e clique em **Todos os nós**.
   - No painel central, selecione todos os nós necessários.
3. Clique em **Ações**, **Coletar informações de diagnóstico**.

   A caixa de diálogo **Coletar informações de diagnóstico** abre.
4. (Opcional) Marque a caixa de seleção.
5. Forneça o caminho do compartilhamento da rede para armazenar os dados.

   Observações:

   - ao se coletar as informações de diagnóstico para um site remoto, é necessário fornecer o destino como o servidor de gateway ou qualquer outro computador que possa acessar o agente ou o RPS nesse site.
   - Se você desejar especificar o caminho local como o destino, converta o caminho local para o caminho UNC e forneça o caminho UNC. Por exemplo, **C:\teste** pode ser especificado como **\\<Nome_do_computador_local>\C$\test**.

- Para backup sem agente com base em host (VMs), Coletar informações de diagnóstico reúne dados do servidor proxy do Arcserve UDP.
- Coletar informações de diagnóstico reúne dados dos computadores que têm o agente do Arcserve UDP instalado.

6. Clique em **Enviar**.

   Uma tarefa é enviada para coletar os dados.

   Após a conclusão bem-sucedida da tarefa, você verá os dados na pasta compartilhada. O nome do arquivo zip é sufixado com o carimbo de data e hora atual.

Coletar informações de diagnóstico a partir de um agente autônomo

As informações de diagnóstico são uma coleção de informações de logs, eventos, registros e aplicativos do produto e do sistema, que a equipe de suporte do Arcserve necessita para investigar qualquer erro. O agente do Arcserve UDP permite coletar todas essas informações em um único local; geralmente, um caminho de compartilhamento da rede. Quando você entra em contato com o suporte do Arcserve, você tem essas informações prontamente disponíveis.

Siga estas etapas:

1. Usando o prompt de comando, vá até o seguinte caminho:

   ```
   %ProgramFiles% \Arcserve\Unified Data Protection\Engine\BIN\DiagnosticUtility
   ```

2. Execute o comando a seguir para saber como executar o arquivo em lote:

   ```
   arcserveAgentSupport.bat -help
   usage: arcserveAgentSupport.bat [OPTIONS]
   -help print help
   -pass <arg> usrPass (se o caminho de exportação for um compartilhamento remoto, a senha de usuário para acessá-lo)
   -path <arg> export path (pode ser um compartilhamento remoto)
   -usero <arg> usrName (se o caminho de exportação for um compartilhamento remoto, o nome de usuário para acessá-lo)
   -xmlConfig <arg> xmlConfigurationFile (Opcional)
   ```

3. Use o comando a seguir para coletar as informações de diagnóstico:

   ```
   arcserveAgentSupport.bat -path <remote share path> -user <username> -pass <password>
   ```

   Exemplo: arcserveAgentSupport.bat -path \\remote_share\data -user abc -pass xyz

   em que, \\remote_share\data é o caminho, abc é o nome de usuário e xyz é a senha

   É possível encontrar o arquivo zip de informações de diagnóstico no compartilhamento remoto.

Carregar informações de diagnóstico para o site do Arcserve usando FTP

Você pode fazer upload de logs ou arquivos para o FTP de suporte da Arcserve usando um protocolo de transferência de arquivos (FTP). No entanto, os usuários (o solicitante tíquete) podem ativar o link de FTP durante o processo de criação inicial do tíquete ou ao atualizar o tíquete online. Uma vez ativado, o FTP gera o link de FTP com credenciais de logon. Essa informação é fornecida ao usuário por meio de um email automatizado. É possível usar o nome de usuário e a senha enviadas pelo email automatizado para fazer upload e download de arquivos do FTP.

Quando você faz logon no FTP usando ftp://supportftp.arcserve.com, a pasta inicial é exibida. Se você criar um tíquete no portal de suporte da Arcserve, uma subpasta será criada com o número do tíquete na pasta inicial. Por exemplo, se você criar um tíquete com o número Ticket-00XXXX30, uma subpasta denominada Ticket-00XXXX30 será criada na pasta inicial.

ftp://supportftp.arcserve.com/Ticket-00XXXX30/

Nome de usuário e senha: use o nome de usuário e a senha gerados automaticamente que foram enviados a você por meio de um email automatizado.

Pasta: Ticket-00XXXX30

Observação: para usuários japoneses, a senha é o endereço de email do solicitante sem o nome de domínio. Por exemplo, se o endereço de email registrado for abc@yahoo.jp, a senha será abc.

Quando o tíquete é resolvido, o servidor FTP recebe uma notificação. Em seguida, a pasta é compactada, e a pasta original é excluída. A pasta compactada fica disponível para os próximos três meses, depois disso é excluída permanentemente.

Importante: não compartilhe seu nome de usuário com outros usuários.

Siga estas etapas para fazer upload de todos os arquivos para o site da Arcserve usando FTP:

1. O solicitante do tíquete (usuário) ou o agente de suporte da Arcserve efetua logon no portal de suporte da Arcserve e cria um tíquete de suporte.

   O agente de suporte da Arcserve ou o solicitante do tíquete seleciona a caixa de seleção no tíquete de suporte e atualiza o tíquete.

   Um link de FTP é gerado automaticamente para a pasta inicial do FTP. A permissão é definida exclusivamente para o solicitante que abriu o tíquete.

   Por exemplo, a pasta a seguir é sua pasta de FTP:

ftp://supportftp.arcserve.com/<número_do_tíquete>

2. Depois que o link do FTP é criado, o suporte da Arcserve envia automaticamente um email com o link do FTP e as credenciais de logon para o solicitante do tíquete (usuário).
3. O usuário efetua logon no link do FTP e carrega os arquivos.

   Você concluiu com êxito o processo de carregamento de arquivos para o servidor de FTP da Arcserve.

Descompactar logs de agente

Os arquivos de log gerados pelo utilitário de diagnóstico estão em um formato ZIP. Para exibir os arquivos de log, você deve descompactar os arquivos.

Siga estas etapas:

1. Copie o arquivo .arcZIP para o computador que tem o Agente UDP instalado.

   O arquivo .arcZIP é criado usando-se o utilitário de diagnóstico.

2. Usando o prompt de comando, vá até o seguinte caminho:

   ```
   %ProgramFiles% \Arcserve\Unified Data Protection\Engine\BIN\DiagnosticUtility
   ```

3. Execute o comando a seguir para saber como executar o arquivo em lote:

   ```
   arcserveAgentSupportInternal.bat -help
   BaseOperation loadDefaultValue
   INFO: Carregue o caminho de instalação do Agente
   C:\Program Files\Arcserve\Unified Data Protection\Engine\
   usage: arcserveAgentSupportInternal.bat [OPTIONS] rawfile
   -help           imprimir ajuda
   -keepFile Manter desse arquivo temporário
   -path <arg> caminho em que o conteúdo deve ser descompactado
   ```

   A seção de Ajuda é exibida.

4. Use o seguinte comando para descompactar o arquivo:

   ```
   arcserveAgentSupportInternal.bat -path <should_be_the_same_machine_where_you_want_to_unzip> <name_of_the_zip_file>
   ```

   Os logs do agente são descompactados.

Descompactar os logs do console

Os arquivos de log gerados pelo utilitário de diagnóstico estão em um formato ZIP. Para exibir os arquivos de log, você deve descompactar os arquivos.

Siga estas etapas:

1. Copie o arquivo .arcZIP para o computador com o Console do UDP instalado.

   O arquivo .arcZIP é criado usando-se o utilitário de diagnóstico.

2. Usando o prompt de comando, vá até o seguinte caminho:

   ```
   %ProgramFiles% \Arcserve\Unified Data Protection\Management\BIN\DiagnosticUtility
   ```

3. Execute o comando a seguir para saber como executar o arquivo em lote:

   ```
   arcserveConsoleSupportInternal.bat -help
   BaseOperation loadDefaultValue
   INFO: Carregue o caminho de instalação do Agente
   C:\Program Files\Arcserve\Unified Data Protection\Management \
   usage: arcserveConsoleSupportInternal.bat [OPTIONS] rawfile
   -help           imprimir ajuda
   -ignoreFailed Ignorar falha ao importar tabela
   -keepFile Manter arquivo temporário
   -noClean Não limpar o banco de dados
   -path <arg> caminho em que o conteúdo deve ser descompactado
   -u Apenas descompactar o arquivo
   ```

   A seção de Ajuda é exibida.

4. Use o seguinte comando para descompactar o arquivo:

   ```
   arcserveConsoleSupportInternal.bat -path <should_be_the_same_machine_where_you_want_to_unzip> <name_of_the_zip_file>
   ```

   Observação: O comando não substitui o banco de dados do Console. Se você deseja substituir o banco de dados do Console, edite o comando *arcserveConsoleSupportInternal.bat* e remova *-u* do arquivo, em seguida salve o arquivo.

   Os logs do Console são descompactados.

Ignorar conteúdo da pasta de histórico de logs usando o Registro

Você pode usar o agente do UDP para coletar todos os logs, inclusive o histórico de logs, do mecanismo. Às vezes, ao coletar o histórico de logs, o agente do UDP processa os arquivos lentamente e faz com que o tamanho do arquivo pareça maior. Para evitar essas discrepâncias, exclua a pasta LogHistory.

Siga estas etapas:

1. Adicione a chave de Registro no local:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

2. Digite os seguintes detalhes:

   Key Name: *SkipLogHistory*

   type: *DWORD(32-bit)*

   Value: 1 (o valor 1 é usado para ignorar o LogHistory e 0 é usado para coletar o LogHistory)

Coletar o log do computador gateway usando a linha de comando

É necessário ter o produto de gateway do Arcserve UDP instalado para coletar logs a partir da linha de comando.

Siga estas etapas para coletar logs da linha de comando:

1. Abra o prompt de comando e vá até *<Diretório de instalação do gateway>\BIN\Diagnostic Utility*.

   Exemplo: C:\Program Files\Arcserve\Unified Data Protection\Gateway\BIN\Diagnostic Utility\

2. Para compactar os logs, execute o comando abaixo:

   arcserveGatewaySupport.bat -Path "<Caminho de destino>"

3. Para descompactar os logs, execute o comando abaixo:

   arcserveGatewayInternalSupport.bat -Path "<Caminho de destino>" "<caminho de origem>"

Coletar logs do RPS usando a linha de comando

O produto Arcserve UDP deve estar instalado com o componente RPS para que seja possível coletar logs do RPS a partir da linha de comando.

Siga estas etapas para coletar logs da linha de comando:

1. Abra o prompt de comando e vá até *<Diretório de instalação do agente>\BIN\Diagnostic Utility*.

   Exemplo: C:\Program Files\Arcserve\Unified Data ProtectionEngine\BIN\Diagnostic Utility\

2. Para compactar os logs, execute o comando abaixo:

   arcserveAgentSupport.bat -path <remote share path> -user <username> -pass <password>

3. Para descompactar os logs, execute o comando abaixo:

   arcserveAgentSupportInternal.bat –path <destination> <source(rawfile)>

Observações:

- Os logs do RPS possuem os logs das tarefas executadas no RPS.
- Os logs do RPS só podem ser obtidos a partir da linha de comando, e não a partir da interface de usuário do console.
- Alguns logs de tarefas relacionados ao RPS não podem ser obtidos a partir da interface de usuário do console ao coletar logs de VM a partir do console.

Exemplo: quando uma tarefa de replicação do MSP é configurada, você define as tarefas com dois consoles, em que o Console-1 terá Backup como tarefa principal e Replicação como tarefa secundária. No Console-2, a tarefa de replicação gerenciada remotamente é configurada e compartilhada com o Console-1.

Nesse cenário, no Console-2, não é possível coletar logs de tarefas de replicação ao coletar logs de VM a partir do console. É necessário coletar esses logs de replicação a partir da linha de comando na máquina do RPS, que é o destino da tarefa de replicação.

Coletar logs stub do Hyper-V com o agente instalado

É possível coletar logs stub do Hyper-V com o agente instalado. O Hyper-V também pode atuar como proxy para ajudar na coleta de logs stub do Hyper-V.

Quando o próprio Hyper-V atua como um proxy (a máquina do Hyper-V deve ter o agente instalado)

Abra o prompt de comando e vá até *<Diretório de instalação do agente>\BIN\Diagnostic Utility*.

Exemplo: *C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Diagnostic Utility*

- Para compactar os logs: execute *arcserveAgentSupport.bat -Path "Destination"*
- Para descompactar os logs: execute *ArcserveAgentInternalSupport.bat -Path "Destination" "source"*

Quando o Hyper-V não atua como um proxy (coletar toda a pasta Backup de VM com base em host do UDP)

Pré-requisito: o computador deve ter o Java instalado.

Siga estas etapas:

1. Importe o Registro a partir do caminho a seguir na máquina em que o agente está instalado:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine.

2. Copie toda a pasta DiagnosticUtility de um computador que já tenha o agente instalado e cole essa pasta no seguinte caminho:

   C:\Arquivos de Programas\Arcserve\Unified Data Protection\Engine\BIN

   Observação: é necessário criar manualmente essa estrutura de diretório.

3. Crie uma pasta vazia chamada "Logs" no seguinte caminho:

   C:\Arquivos de programas\Arcserve\Unified Data Protection\Engine

4. Copie a pasta Common de um computador que já tenha o agente instalado no seguinte caminho:

   C:\Arquivos de programas\Arcserve\Unified Data Protection

   - Para compactar os logs: execute *arcserveAgentSupport.bat -Path "Destination"*
   - Para descompactar os logs: execute *ArcserveAgentInternalSupport.bat -Path "Destination" "source"*

Coletar mensagens do Visualizador de eventos do Hyper-V

É possível coletar as mensagens do Visualizador de eventos do Hyper-V instalando o agente com um nome de pasta *hyperVEventViewerFiles*.

Siga estas etapas para coletar as mensagens do Visualizador de eventos a partir da linha de comando:

1. Abra o prompt de comando e vá até *<Diretório de instalação do agente>\BIN\Diagnostic Utility*.

   Exemplo: C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\Diagnostic Utility\

2. Para compactar as mensagens do Visualizador de eventos, execute *arcserveAgentSupport.bat -Path "Destination"*
3. Para descompactar as mensagens do Visualizador de eventos, execute *ArcserveAgentInternalSupport.bat -Path "Destination" "source"*

Coletar arquivos OLF e a pasta Ca_lic

Os arquivos CA_LIC e OLF são coletados nos logs ao fazer a coleta no computador com o agente já instalado, com uma pasta chamada CA_LIC.

- Para coletar usando CLI: abra o prompt de comando e vá até *<Diretório de instalação do agente>\BIN\Diagnostic Utility*

  Exemplo: *C:\Arquivos de programas (x86)\Arcserve\SharedComponents\CA_LIC*
- Para coletar usando o Console: vá até o nó do agente, clique com o botão direito do mouse nele e clique em **Coletar informações de diagnóstico**.
- Para compactar os logs: execute *arcserveAgentSupport.bat -Path "Destination"*
- Para descompactar os logs: execute *ArcserveAgentInternalSupport.bat -Path "Destination" "source"*

Coletar listagem de diretório dos diretórios do repositório de dados/destino de backup

Listagem de diretório das pastas de gerenciamento e mecanismo

Mecanismo: este log é coletado na pasta *agentLogs* (após a descompactação de arczip) com o nome *EngineDirectoryBrowseInfo.log*.

Gerenciamento: este log é coletado na pasta *consoleLogs* (após a descompactação de arczip) com o nome *ManagementDirectoryBrowseInfo.log*.

Listagem de diretório dos repositórios de dados:

- **Sem redução de redundância:** este log é coletado para o repositório de dados sem redução de redundância com o nome *CommonStorePathDirectoryBrowseInfo.log* (após a descompactação de arczip) na pasta *agentLogs*
- **Redução de redundância:** quatro logs são coletados para repositórios de dados de redução de redundância (após a descompactação de arczip) na pasta *agentLogs* com os seguintes nomes:
    1. *CommonStorePathDirectoryBrowseInfo.log*
    2. *HashRolePathDirectoryBrowseInfo.log*
    3. *IndexRolePathDirectoryBrowseInfo.log*
    4. *DataRolePathDirectoryBrowseInfo.log*

Capítulo 10: Instalando manualmente o Sophos Intercept X Advanced for Server no Arcserve UDP

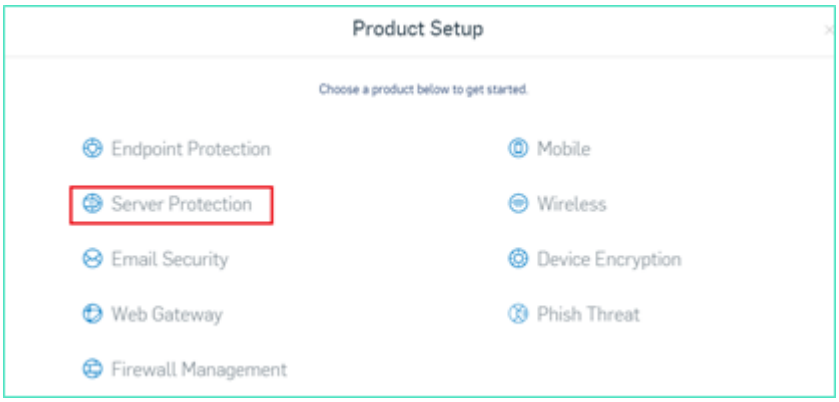
A instalação do Sophos Intercept X Advanced for Server no Arcserve UDP permite o seguinte:

- Proteger os dados e backups do sistema contra ransomware e outros ataques
- Proteção do ponto de extremidade que combina a detecção de malware com base em assinatura e sem assinatura.
- Rede neural de aprendizado profundo
- Tecnologia antiexploração
- O anti-ransomware CryptoGuard, tecnologias WipeGuard e muitas outras capazes de combater uma ampla gama de ameaças ao ponto de extremidade

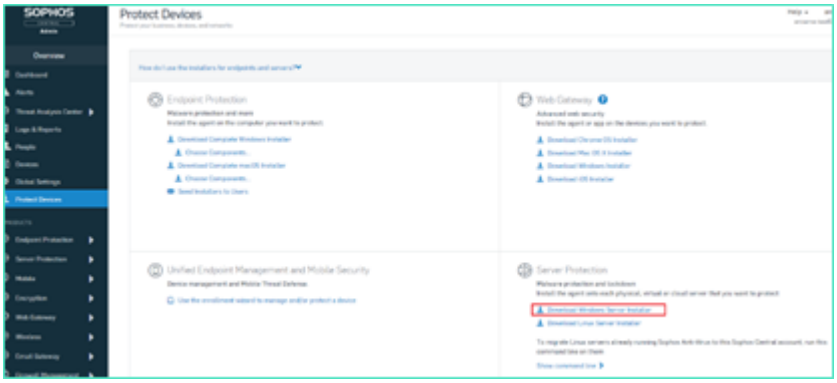
Siga estas etapas:

1. No site de suporte da Arcserve, crie uma conta.
2. Para solicitar uma cópia gratuita do Sophos Intercept X Advanced, forneça todos os detalhes relevantes no Formulário de solicitação do Sophos e envie-o para o suporte da Arcserve. É obrigatório compartilhar os detalhes da ID do email e da ID do pedido. Você receberá uma confirmação de email gerada automaticamente.

   Depois de confirmar seu email, a Arcserve processará sua solicitação, criará uma conta no Sophos Central e enviará um email contendo instruções sobre como criar uma senha.
3. Para criar uma senha para sua nova conta do Sophos Central, siga as instruções no email.
4. Efetue logon no Sophos Central.
5. Abra a caixa de diálogo de configuração do produto e selecione **Proteção do servidor**.



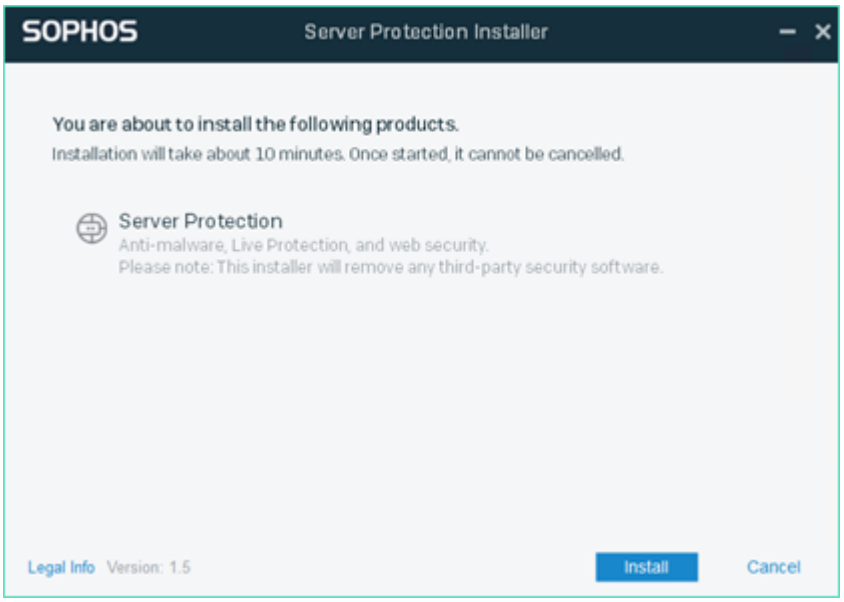
6. Na seção Proteção do servidor, clique em **Fazer download do instalador do Windows Server** e salve o instalador **SophosSetup.exe** em uma pasta no UDP.



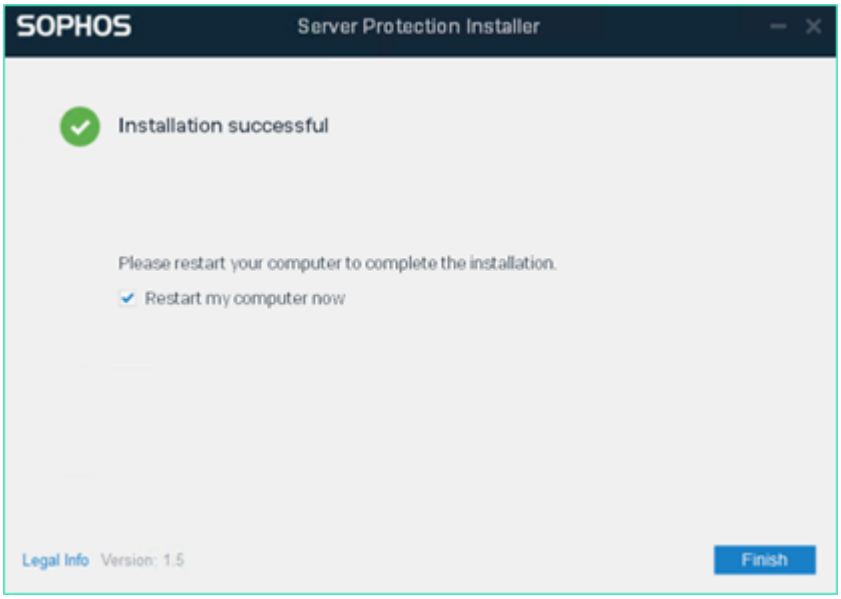
7. Para iniciar o instalador, abra a pasta e clique duas vezes em **SophosSetup.exe**.

   Observação: para evitar comportamento inesperado durante a instalação do Sophos Intercept-X, desative o Windows Defender e\ou outro software antivírus no servidor. O Sophos removerá alguns produtos de segurança que não sejam da Sophos dos servidores Windows. Para obter mais informações, consulte Sophos CRT: lista de software de segurança de terceiros removido pela Sophos.

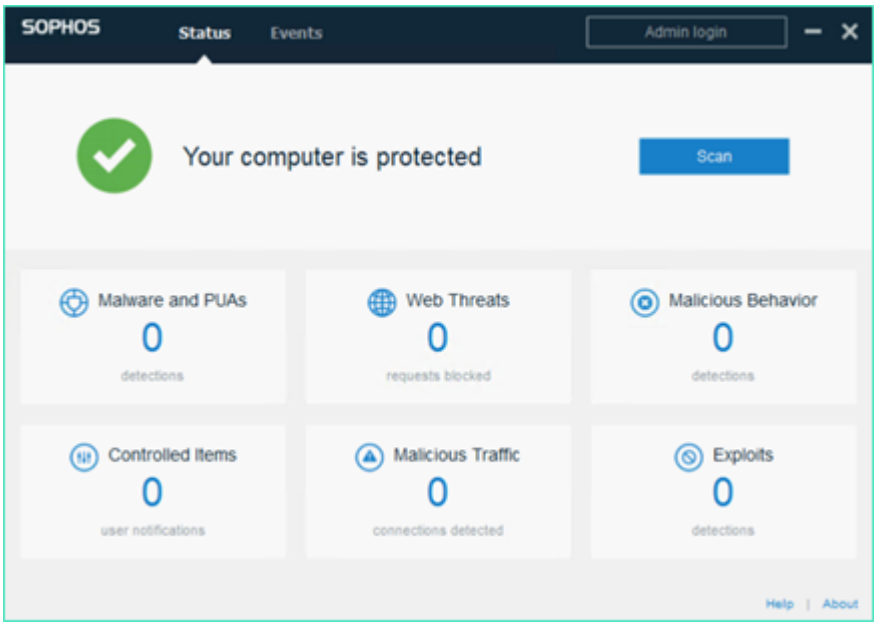
8. Clique em **Instalar**.



9. Para reiniciar o sistema imediatamente, clique em **Concluir**. Para reiniciar o mais tarde, desmarque a opção **Reiniciar meu computador agora**.



10. Para exibir o status de proteção, abra a interface do **Sophos Intercept X**.



O status indica que Arcserve UDP 8.0 está protegido contra ataques de ransomware, malware, ameaças da web e explorações de dia zero.

11. Para acessar o Sophos Central, clique em **Logon do administrador**. Ele permite gerenciar o Sophos Intercept X Advanced Server, definir alertas e políticas e assim por diante.

    Observações:

    - É necessário ter acesso à internet no Arcserve UDP para instalar o *Sophos Intercept X Advanced* e quaisquer atualizações relacionadas. O Sophos Intercept X Advanced tem base na nuvem e não há nenhum instalador offline disponível.
    - Se você já tiver comprado outro UDP e tiver uma conta do Sophos fornecida pela Arcserve, use a mesma conta para todos os seus Arcserve UDP 8.0.
    - Se você já tiver uma conta do Sophos adquirida de alguma outra maneira, como diretamente da Sophos, forneça um endereço de email diferente para uma conta separada no Sophos Central.
    - Se a instalação do Sophos falhar por qualquer motivo, siga as instruções na tela ou no email fornecidas junto com a mensagem de erro.
    - Para receber atualizações do Sophos Intercept X Advanced for Server, como atualizações de definições de malware e atualizações de versão, você deverá ter uma manutenção ou assinatura válida e ativa para seu Arcserve UDP.

Para obter assistência adicional, entre em contato com o suporte técnico da Arcserve pelo telefone (+1.844.765.7043) ou online, ou entre em contato com seu escritório local de suporte da Arcserve.

Capítulo 11: Aplicando práticas recomendadas

Esta seção contém os seguintes tópicos:

Práticas recomendadas para proteger o servidor Arcserve UDP

É possível migrar o console do servidor anterior para um novo servidor sem perder os dados.

- Não há solução de backup no mesmo domínio do Active Directory.
- Use contas de backup.
- Não use contas de administrador de domínio para acessar tarefas relacionadas ao usuário. Por exemplo, o administrador que usa privilégios de administrador para ler emails, navegar online e assim por diante.
- Separe o console UDP do RPS e crie VSB para o console do UDP.
- Se possível, use rede de backup/vlan dedicada.
- Se possível, desative o SMBv1.

  Observação: não é possível desativar ao usar o Red Hat/Centos v6.6 e versões anteriores, pois eles usam o SMB v1.

Excluir arquivos da verificação do antivírus

O software de antivírus pode interferir na execução adequada do processo do modo de espera virtual por meio do bloqueio temporário do acesso aos arquivos ou da quarentena ou exclusão de arquivos que são classificados incorretamente como suspeitos ou perigosos. É possível configurar grande parte dos softwares antivírus para excluir arquivos ou pastas específicas, de modo que seja possível ignorar a verificação de determinados dados. É importante configurar o software antivírus corretamente para que ele não interfira nas operações de backup e de restauração, ou em quaisquer outros tipos de processos.

Em um servidor Hyper-V, o software antivírus corrompe o arquivo de configuração da VM. O servidor Hyper-V altera o estado da máquina virtual para o modo 'de economia' e a VM se torna corrompida e inútil. Nesses casos, é necessário excluir a VM e executar uma conversão completa para criar uma VM.

Para garantir que modo de espera virtual local e remoto funcione corretamente e impedir que a VM entre no modo de economia, exclua os seguintes arquivos que são destinados às máquinas virtuais do Hyper-V:

- Diretório dos arquivos de configuração da máquina virtual:

  (Padrão) C:\ProgramData\Microsoft\Windows\Hyper-V

  Diretório de arquivos de configuração da máquina virtual do modo de espera virtual do Arcserve UDP

- Diretório dos arquivos de disco rígido virtual da máquina virtual:

  (Padrão) C:\Usuários\Público\Documentos\Hyper-V\Virtual Hard Disks

  Diretório de arquivos de disco rígido virtual da máquina virtual do modo de espera virtual da Arcserve UDP

- Diretório dos arquivos de instantâneo:

  (Padrão) %systemdrive%\ProgramData\Microsoft\Windows\Hyper-V\Snapshots

  Diretório de arquivos de instantâneo da máquina virtual do modo de espera virtual do Arcserve UDP

Configurar parâmetros de multitransmissão

Replicações em configurações relacionados a WAN são salvas na seguinte chave do registro:

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\Network]

A lista a seguir exibe a chave do registro e seu valor padrão:

- "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)

A descrição a seguir descreve as configurações de chave do Registro:

WAN_EnableAutoTunning

Especifica a chave para ativar ou desativar o recurso de multitransmissão. Se o valor for 0, a multitransmissão está desativada. Para outros valores, a multitransmissão está ativada. O valor padrão ativar a multitransmissão é 1.

WAN_ChunkSizeByte

Especifica o tamanho do fragmento de dados de cada pacote. Tamanho do pacote afeta a taxa de transferência. Se a largura de banda da WAN for mais alta, o tamanho do fragmento de dados pode ser aumentado.

O valor padrão é de 64 Kbytes. O intervalo é limitado de 512 bytes a 1 Mbyte no código.

WAN_NumberofStreams

Especifica o número de fluxos que precisa para ser criado na WAN, quando a latência é superior ao número de WAN_RTT_Threshhold. O número de fluxos padrão é 5. A faixa de fluxo varia de 1 a 10.

WAN_RTT_Threshold

Quando de RTT é superior a WAN_RTT_Threshold, vários soquetes são criados. A unidade de WAN_RTT_Threshold é milissegundos (ms). O valor padrão é 20 milissegundos. O intervalo é limitado de 20 ms para 600 ms.

WAN_MultiStreamsMaxCacheSize

Especifica que o tamanho da memória será alocado quando a multitransmissão for ativada. Esse buffer de memória será usado para armazenar em cache a memória fragged recebida. O intervalo é de 16 MB a 64 MB. O valor padrão é de 64 MB. Se o valor for igual a zero, o valor será definido como 64 MB. A unidade desse valor é BYTE.

WAN_SendCommandFragDataMerged

Especifica que, se o valor for diferente de zero, a biblioteca de comunicação agrupa arquivos pequenos e os envia em um fragmento. Se o valor for zero, os arquivos pequenos são enviados individualmente. O valor padrão é zero.

Observações:

- Em uma tarefa de replicação, o número de conexões de soquete pode não ser consistente com o registro de WAN_NumberofStreams.

  Tarefa de replicação de não-GDD para não-GDD

  Quando de RTT é mais de WAN_RTT_Threshold, o número de conexão do soquete é igual a WAN_NumberofStreams.

  Tarefa de replicação de não-GDD para GDD ou GDD para GDD

  Existem quatro tipos de conexões. Somente a conexão de bloco de dados funciona com o recurso de multitransmissão. Portanto, quando RTT é mais de WAN_RTT_Threshold, o total de conexão de soquete é 3+WAN_NumberofStreams.

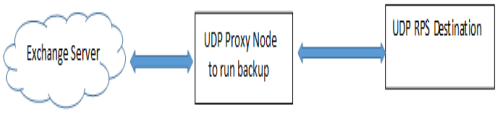
- A tarefa de Replicação detecta o status da rede para determinar se a comunicação está na WAN ou não. Se o status da rede estiver fraco, a LAN pode ser aceita como WAN.

Assuntos relacionados ao Exchange online

Esta seção contém os seguintes tópicos:

Configuração para desempenho ideal

Possível topologia:



Você pode ter o proxy instalado no RPS ou separadamente. No entanto, para um desempenho ideal, recomendamos que você coloque ambos no mesmo nó.

Configuração recomendada para o proxy

- Arquitetura: máquina do Windows de 64 bits. Para obter mais informações sobre os sistemas operacionais suportados para o Arcserve UDP, clique aqui.
- Memória: 8 GB ou superior
- CPU: 2 núcleos

Configuração recomendada para o servidor de ponto de recuperação:

Consulte as Notas da Versão para obter os requisitos do sistema.

Práticas recomendadas de Backup

- Espera mais longa duração do backup no primeiro backup completo que obtém os dados do servidor Microsoft Exchange Online por meio de uma conexão WAN.
- Como a duração do backup para o primeiro backup completo for longo, garantir a configuração necessária de hardware, rede e recursos (por exemplo, espaço em disco no destino, memória, CPU e assim por diante) disponibilidade durante o backup para evitar a interrupção devido a falhas ambientais.
- Prossiga com o backup a partir do ponto de interrupção em qualquer um dos seguintes cenários:
  - Certifique-se de que um backup não esteja em execução durante um período de interrupção de energia ou um tempo de inatividade planejado. Se estiver em execução, será necessário cancelar o backup. Quando você cancela o backup, ele mantém o ponto de recuperação armazenado parcialmente em backup. A próxima programação de backup poderá continuar a partir desse ponto de interrupção.
  - Se, durante o backup, o computador for desligado ou o processo for encerrado inesperadamente, o ponto de recuperação da tarefa em execução será removido. Inicie o backup novamente. O backup não é iniciado a partir do ponto de interrupção. Todos os dados são armazenados em backup novamente.
- É sempre recomendável usar um nó com o mecanismo de proteção automática para proteger todas as caixas de correio, incluindo as criadas recentemente depois da criação do plano.
- No Arcserve UDP, o tamanho dos dados protegidos com suporte é limitado a 8 Terabytes (compactados) por padrão. Para configurar o tamanho, você pode criar o seguinte valor de registro no nó do proxy:

  [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<NodeGUID>]

  " VirtualDiskSize "=dword:00000002

  O exemplo acima define o tamanho de 2 TB.

  Observação: aumentar o tamanho do disco virtual transforma a próxima tarefa de backup incremental em completa e também afeta a velocidade das seguintes tarefas:

Copiar para a fita, replicação, cópia de ponto de recuperação para a nuvem.

- Selecione o tamanho do disco virtual com base em seu tamanho atual de dados fonte e seu crescimento.

  Por exemplo: se o tamanho total de todos os usuários for de 5 TB e o crescimento médio dos dados por dia for de 1% (ou seja, 50 GB), você precisará de 5 TB + 50 GB * 30 dias = 6,5 TB de espaço em disco para acomodar os backups iniciais completos e 30 backups incrementais diários durante um mês.

  Como resultado, o tamanho mínimo do disco necessário é 7 TB (descompactado). Para reter mais pontos de recuperação, use o mesmo método para calcular o tamanho.

- Use as agendas de regulagem corretamente para garantir backup desejada da largura de banda durante horários comerciais. Execute um backup pequeno com apenas alguns usuários para avaliar a utilização da rede, a tarefa de backup e defina os valores de aceleração adequadamente.

- Certifique-se de que a conta de backup atende aos pré-requisitos obrigatórios. Para obter mais informações, consulte o link.

- Se o link de rede usado para conectar o servidor online do Exchange é instável e resulta no cancelamento de backup frequente, configurar a diretiva de retenção de ponto de recuperação para manter um grande número de sessões não mescladas.

  Valor padrão para backups incrementais diários: 7

  Valor padrão para backups manuais: 31

  Configure o backup programação (ões) para manter pelo menos um backup diário, semanal e mensal.

- Certifique-se de que a instalação tenha licenças suficientes. Você pode gerenciar licenças usando o Gerenciador de licenças. Para obter detalhes, consulte a P.4 na seção Perguntas frequentes.

Prática recomendada para restauração

Certifique-se de que a conta usada para restauração tenha as permissões necessárias para representar o usuário de destino selecionado. Para obter mais detalhes, consulte o link.

Perguntas frequentes sobre o Exchange on-line

1. Posso usar o RPS diretamente aos usuários on-line do Exchange backup sem usar qualquer proxy?

   Sim, você pode.

2. Preciso que o administrador /nome da conta de administrador do grupo de caixas de correio do Exchange Online backup?

   Não, a conta de backup precisa apenas de um conjunto específico de permissões. Para obter mais detalhes, consulte o link.

3. Que tipo de taxa de transferência posso esperar para backups on-line do Exchange se a largura de banda da internet é bom?

   Além de largura de banda de rede, Throughput também é limitada pela taxa na qual os dados são lidos do Exchange server é controlado pelo design do Exchange server.

   Às vezes, do Exchange server se recusa a conexão para Arcserve UDP para ler dados. Em tais casos, Arcserve UDP continua tentando até que ele obtém uma conexão bem-sucedida. O tempo de espera maior pode levar a números de taxa de transferência menores.

4. Se eu tiver mais usuários configurados no plano de backup que o número de licenças, é possível executar backups parciais de usuários licenciados?

   Não, você não pode. Se você executar o backup para mais usuários do que o número de licenças disponíveis, o backup falha para todos os usuários. Por exemplo, se você tiver configurado os 100 usuários protejam no console do Arcserve UDP enquanto você tem 90 licenças disponíveis, o backup irá falhar. Para executar o backup com êxito, você precisa remover 10 ou mais usuários da lista de usuários protegidos.

5. Como melhorar o desempenho de throughput de backup?

   Considere os seguintes pontos para garantir o desempenho ideal de taxa de transferência:

   - Divida um grande backup em menores gerenciáveis trabalhos de backup.
   - Exclua as pastas que você não deseja fazer o backup, as configurações de plano. Por exemplo, resíduos, problemas de sincronização e assim por diante.

- Manter uma verificação periódica na infra-estrutura de rede interna e externa.

Assuntos relacionados ao Microsoft Azure

Esta seção contém os seguintes tópicos:

Práticas recomendadas para uma máquina virtual instantânea no Microsoft Azure

Para proteger os nós na rede local, é necessário instalar o Console do UDP no host.

- Selecione o protocolo HTTPS ao instalar os componentes do UDP.
- A maneira mais fácil de criar um grupo de recursos é criando, pelo menos, uma máquina virtual de teste. O Azure guiará você pelas etapas para criar todos os recursos para a máquina virtual de teste que poderão ser usados para a máquina virtual em modo de espera.
- (Opcional) Crie um RPS no Azure.

  Siga estas etapas:

  1. Abra as portas TCP 8014 e 8015 de entrada.
  2. Se o RPS for acessado de um navegador web remoto, resolva o nome do servidor RPS para o IP público.
  3. Para replicar, use a tarefa de plano compartilhado "Replicar para um RPS gerenciado remotamente".

Implantar o Arcserve UDP no Microsoft Azure

Verifique as práticas recomendadas a seguir antes de implantar o Arcserve UDP para Microsoft Azure:

1. Você deve instalar o console do Arcserve UDP no local para proteger os nós que estão na rede local.
2. Selecione o protocolo HTTPS ao instalar componentes do Arcserve UDP.
3. A maneira mais fácil de criar recursos do Azure é criar pelo menos uma máquina virtual de teste que poderá ser usada como sua VM no modo de espera posteriormente.

4. Crie um servidor de ponto de recuperação do Arcserve UDP no Azure.
    - Mantenha as portas TCP 8014 e 8015 abertas para conexões de entrada.
    - Você deve resolver o nome do servidor de ponto de recuperação para o IP público se estiver acessando o servidor de ponto de recuperação a partir de um navegador da web remoto.
    - Use a tarefa de plano compartilhado **Replicar para um RPS gerenciado remotamente** para replicar tarefas.

Capítulo 12: Solução de problemas

Esta seção contém os seguintes tópicos:

Falhas relacionadas com comunicação do Arcserve UDP

Esta seção inclui os seguintes tópicos de solução de problemas relacionados à falha na comunicação do Arcserve UDP:

- O Arcserve UDP não consegue se comunicar com nós do Windows
- Não é possível receber alertas por email da conta do Gmail
- O Arcserve UDP não consegue se comunicar com o servidor de backup Linux do Arcserve UDP em nós remotos
- O Arcserve UDP não consegue se comunicar com o servidor de ponto de recuperação do Arcserve UDP em nós remotos
- O Arcserve UDP não consegue se comunicar com o servidor de backup do Arcserve UDP em nós remotos
- O Arcserve UDP não consegue se comunicar com o site remoto

O Arcserve UDP não consegue se comunicar com nós do Windows

Válido em sistemas operacionais Windows.

Sintoma

O Arcserve UDP não consegue se comunicar com nós do Windows

Solução

A tabela a seguir descreve os motivos pelos quais o Arcserve UDP não consegue se comunicar com nós do Windows e a ação corretiva correspondente:

Causa	Ação corretiva
A rede estava indisponível ou instável ao aplicar os planos.	Verifique se a rede está disponível e estável e tente novamente. O Arcserve UDP pode executar ping no nó remoto e o nó remoto pode executar ping de volta no Arcserve UDP.
O compartilhamento Admin$ da rede do nó remoto não estava disponível quando o Arcserve UDP tentou se comunicar com o nó.	Verifique se Admin$ da rede do nó remoto está disponível e tente novamente.
O nó do Agente do Arcserve Unified Data Protection para Windows não pôde lidar com a carga quando o Arcserve UDP tentou se comunicar com o nó.	Verifique se a CPU no nó remoto do Agente do Arcserve Unified Data Protection para Windows está em um estado normal e tente novamente.
O serviço do Agente do Arcserve Unified Data Protection para Windows no nó remoto não estava em execução quando o Arcserve UDP tentou se comunicar com o nó.	Verifique se o serviço do Agente do Arcserve Unified Data Protection para Windows no nó remoto está em execução e tente novamente.
Protocolo ou porta incorreta utilizada para se comunicar com o nó.	Use o protocolo ou a porta correta para adicionar/atualizar o nó remoto no modo de exibição de nó do Arcserve UDP.
O serviço do Agente do Arcserve Unified Data Protection para Windows não estava se comunicando adequadamente.	Reinicie o serviço do Agente do Arcserve Unified Data Protection para Windows no nó remoto e tente novamente.

Não é possível receber alertas de email da conta do Gmail

A conta do Gmail é bloqueada pelo Google se você usa a conta do Gmail nas configurações de email.

Válido em plataformas Windows.

Sintoma

Ao configurar contas do Gmail, você não receberá alertas por email. Ao tentar configurar a conta do Gmail para alertas por email e clicar em "Enviar um email de teste", você receberá uma das seguintes mensagens de erro:

O email de teste falhou devido a credenciais de usuário incorretas.

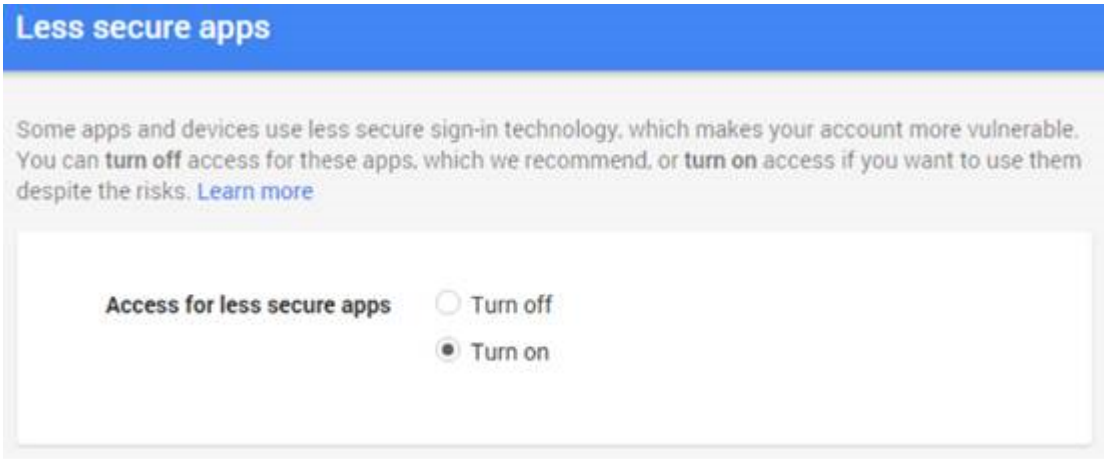
ou

Falha ao enviar o email de teste: credenciais do usuário inválidas.

Solução

1. Forneça as credenciais corretas e tente novamente.
2. A segurança do Google bloqueia emails da conta do Gmail configurada fora do Google. Para evitar isso, no link abaixo, modifique as configurações selecionando "Ativar" para usar o Acesso em aplicativos menos seguros:

   https://www.google.com/settings/security/lesssecureapps



O Arcserve UDP não consegue se comunicar com o servidor de backup Linux do Arcserve UDP em nós remotos

Válido em sistemas operacionais Linux.

Sintoma

O Arcserve UDP não consegue se comunicar com o servidor de backup Linux do Arcserve UDP em nós remotos

Solução

A tabela a seguir descreve os motivos pelos quais o Arcserve UDP não consegue se comunicar com o servidor de backup Linux do Arcserve UDP em nós remotos e a ação corretiva correspondente:

Causa	Ação corretiva
A rede estava indisponível ou instável quando o Arcserve UDP tentou se comunicar com o nó do servidor de backup Linux.	Verifique se a rede está disponível e estável e tente novamente. O Arcserve UDP pode executar ping no nó remoto do servidor de backup Linux e o nó remoto do servidor de backup Linux pode executar ping de volta no Arcserve UDP.
O nó do servidor de backup Linux do Arcserve UDP não conseguiu lidar com a carga quando o Arcserve UDP tentou se comunicar com o nó.	Verifique se a CPU no nó remoto do servidor de backup Linux do Arcserve UDP está em um estado normal e tente novamente.
O serviço de servidor de backup Linux do Arcserve UDP no nó remoto não estava em execução quando o Arcserve UDP tentou se comunicar com o nó.	Verifique se o serviço de servidor de backup Linux do Arcserve UDP no nó remoto está em execução e tente novamente.
O serviço do servidor de backup Linux do Arcserve UDP não estava se comunicando corretamente.	Reinicie o serviço de servidor de backup Linux do Arcserve UDP no nó remoto e tente novamente.

O Arcserve UDP não consegue se comunicar com o servidor de ponto de recuperação do Arcserve UDP em nós remotos

Válido em sistemas operacionais Windows.

Sintoma

O Arcserve UDP não consegue se comunicar com o servidor de ponto de recuperação do Arcserve UDP em nós remotos.

Solução

A tabela a seguir descreve os motivos e a ação corretiva correspondente:

Causa	Ação corretiva
A rede estava indisponível ou instável quando o Arcserve UDP tentou se comunicar com o nó do servidor de ponto de recuperação.	Verifique se a rede está disponível e estável e tente novamente. O Arcserve UDP pode executar ping no nó remoto do servidor de ponto de recuperação e o nó remoto do servidor de ponto de recuperação pode executar ping de volta no Arcserve UDP.
O compartilhamento Admin$ da rede do nó do servidor de ponto de recuperação do Arcserve UDP não estava disponível quando o Arcserve UDP tentou se comunicar com o nó.	Verifique se Admin$ da rede do nó do servidor de ponto de recuperação está disponível e tente novamente.
O nó do servidor de ponto de recuperação do Arcserve UDP não conseguiu lidar com a carga quando o Arcserve UDP tentou se comunicar com o servidor.	Verifique se a CPU no nó remoto do servidor de ponto de recuperação está em um estado normal e tente novamente.
O serviço de agente do Arcserve UDP, o serviço de repositório de dados RPS do Arcserve UDP ou o serviço de compartilhamento de porta do RPS do Arcserve UDP no nó remoto não estava em execução quando o Arcserve UDP tentou se comunicar com o nó.	Verifique se o serviço de agente do Arcserve UDP, o serviço de repositório de dados RPS do Arcserve UDP ou o serviço de compartilhamento de porta do RPS do Arcserve UDP no nó remoto está em execução e tente novamente.
Protocolo ou porta incorreta utilizada para se comunicar com o nó do servidor de ponto de recuperação.	Use o protocolo ou a porta correta para adicionar/atualizar o nó do servidor de ponto de recuperação no modo de exibição de nó de destino do Arcserve UDP.

O serviço de agente do Arcserve UDP, o serviço de armazenamento de dados RPS do Arcserve UDP ou o serviço de compartilhamento de porta do RPS do Arcserve UDP não estava se comunicando corretamente.	Reinicie o serviço de agente do Arcserve UDP, o serviço de repositório de dados RPS do Arcserve UDP ou o serviço de compartilhamento de porta do RPS do Arcserve UDP no nó remoto e tente novamente.

O Arcserve UDP não consegue se comunicar com o servidor de backup do Arcserve UDP em nós remotos

Válido em sistemas operacionais Windows.

Sintoma

O Arcserve UDP não consegue se comunicar com o servidor de backup do Arcserve em nós remotos.

Solução

A tabela a seguir descreve os motivos pelos quais o Arcserve UDP não consegue se comunicar com o servidor de backup do Arcserve em nós remotos e a ação corretiva correspondente:

Causa	Ação corretiva
A rede estava indisponível ou instável quando o Arcserve UDP tentou se comunicar com o nó do servidor de backup do Arcserve.	Verifique se a rede está disponível e estável e tente novamente. O Arcserve UDP pode executar ping no nó remoto do servidor de backup do Arcserve e o nó remoto do servidor de backup do Arcserve pode executar ping de volta no Arcserve UDP.
O nó do servidor de backup do Arcserve não conseguiu lidar com a carga quando o Arcserve UDP tentou se comunicar com o nó.	Verifique se a CPU no nó remoto do servidor de backup do Arcserve UDP está em um estado normal e tente novamente.
O serviço de servidor de backup do Arcserve no nó remoto não estava em execução quando o Arcserve UDP tentou se comunicar com o nó.	Verifique se o servidor de backup do Arcserve no nó remoto está em execução e tente novamente.
Protocolo ou porta incorreta utilizada para se comunicar com o nó do servidor do Arcserve Backup.	Use o protocolo ou a porta correta para adicionar/atualizar o Servidor de backup do Arcserve na exibição do nó de destino do Arcserve UDP.
O serviço relacionado do servidor de backup co Arcserve não estava se comunicando corretamente.	Reinicie o serviço relacionado do servidor de backup do Arcserve no nó remoto e tente novamente.

O Arcserve UDP não consegue se comunicar com o site remoto

Válido em sistemas operacionais Windows.

Sintoma

O Arcserve UDP não consegue se comunicar com o site remoto.

Solução

A tabela a seguir descreve os motivos pelos quais o Arcserve UDP não consegue se comunicar com o site remoto e a ação corretiva correspondente:

Causa	Ação corretiva
A rede está indisponível ou instável.	Verifique se a rede está disponível e estável e tente novamente.
O Arcserve UDP é reinstalado e o site remoto não é registrado no Arcserve UDP.	Registre o site remoto no Arcserve UDP.
O nome do host ou o endereço IP do Arcserve UDP foi alterado e o site remoto não é registrado no Arcserve UDP.	Registre o site remoto no Arcserve UDP.
O nome do host ou o endereço IP do site remoto foi alterado e o site remoto não é registrado no Arcserve UDP.	Registre o site remoto no Arcserve UDP.

Plano, tarefa e configurações relacionadas

Esta seção inclui os seguintes tópicos de solução de problemas relacionados à tarefa e às configurações de backup:

- Falha da tarefa de backup após a alteração do nome do host/endereço IP do console
- Como adicionar senha de criptografia em um destino criptografado existente
- Não é possível aplicar as configurações de backup para o nó
- Falha de implantação do plano após a alteração de senha do computador de proxy de backup sem agente
- Configurações desativadas ao abrir a interface do usuário do agente
- Pausar e retomar falham quando o agente não está conectado à rede
- O serviço do agente do Arcserve UDP é executado lentamente
- Configurar o registro para executar novamente uma tarefa de cópia em fita
- Configurar o registro para copiar em fita vários pontos de recuperação do mesmo tipo na mesma tarefa
- Não inclusão de arquivo/pasta no backup da pasta NFS compartilhada ou conversão de nome de arquivo/pasta em um nome ilegível
- Falha no backup da pasta NFS compartilhada
- Nome de servidor incorreto na solicitação de licença para caminhos UNC
- Redefinir o console do UDP com MFA ativado quando o TOTP não estiver disponível

Falha da tarefa de backup após a alteração do nome do host/endereço IP do console

Sintoma

Instalei o console e servidor RPS na mesma máquina. O backup estava funcionando bem, mas após alterar o nome de host/endereço IP do console, a tarefa de backup falha.

Solução

Esse problema ocorre quando você tem planos atribuídos a nós e modifica o nome de host/endereço IP desse computador.

Para solucionar esse problema, atualize manualmente os nós do agente e execute a tarefa de backup novamente.

Siga estas etapas:

1. Navegar até nós: página Todos os nós.
2. Selecione o nó.
3. Clique com o botão direito do mouse e selecione **Atualizar**.
4. Clique em **OK**.

Os nós são atualizados.

Como adicionar senha de criptografia em um destino criptografado existente

Sintoma

Você esqueceu de adicionar a senha de criptografia no destino Cópia de arquivo.

Solução

É possível adicionar a senha de criptografia agora.

Siga estas etapas:

1. Abra o plano.
2. Abra o destino de cópia de arquivo em que é necessário adicionar a senha de criptografia.
3. Altere o tipo de destino de Armazenamento em nuvem\Compartilhamento de rede para Compartilhamento de rede\Armazenamento em nuvem.
4. Forneça qualquer Compartilhamento de rede ou Armazenamento em nuvem e salve.
5. Mais uma vez, abra o plano e vá para o destino Cópia de arquivo.
6. Altere o destino para Fornecedor da nuvem\Compartilhamento de rede.
7. Selecione o Fornecedor da nuvem\Compartilhamento de rede e, em seguida, selecione o bucket ou Contêiner\Fornecer caminho.
8. Forneça uma senha de criptografia correta.
9. Salve o plano.

Não é possível aplicar as configurações de backup para o nó

Sintoma

Tenho dois consoles, o Console A e o Console B. Adiciono um servidor do ponto de recuperação (RPS) ao console A e crio um plano para o RPS. Em seguida, adiciono o RPS ao Console B. Agora, esse RPS é gerenciado pelo Console B. Mas, quando atualizo o nó do agente do Console A cujo backup foi feito no RPS, recebo o seguinte erro:

Não é possível aplicar configurações de backup ao nó. (Não foi possível localizar o plano do Servidor de ponto de recuperação UDP do Arcserve neste servidor.)

Solução

Para evitar esse erro, siga estas etapas:

1. Selecione o plano do Console A.
2. No painel central, clique em **Ações**, em seguida, selecione **Implantar agora**.

   O plano será redistribuído, e as configurações de backup serão aplicadas ao nó.

Falha de implantação do plano após a alteração de senha do computador de proxy de backup sem agente

Sintoma

Se o Console e o servidor proxy forem computadores diferentes, depois de alterar a senha do computador proxy, a reimplantação do plano falhará. A mensagem de erro informa que as credenciais não estão corretas.

Solução

Siga estas etapas para corrigir o problema:

1. No modo de exibição de nós do Console, atualize o servidor proxy com novas credenciais.
    a. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.
    b. Clique com o botão diteiro no nó e selecione **Atualizar**para atualizar o servidor proxy.
2. Se o servidor RPS e o proxy estiverem na mesma máquina, atualize o RPS com as novas credenciais.
    a. No painel à esquerda, vá para **Destinos** e clique em **Servidores de ponto de recuperação**.
    b. Clique como botão direito no RPS no painel central e selecione **Atualizar**.
3. Reinicie o serviço de agente do Arcserve UDP no computador proxy.
4. Reimplante o plano.

Configurações desativadas ao abrir a interface do usuário do agente

Se os nós do Agente do Arcserve UDP (Windows) não forem removidos da interface do usuário do Arcserve UDP antes da desinstalação do Console do Arcserve UDP, as configurações serão desativadas ao se abrir a interface do usuário do Agente nesses nós do Agente do Arcserve UDP (Windows).

Sintoma

O nó do Agente do Arcserve UDP (Windows) não é notificado de que o Console do Arcserve UDP foi desinstalado. É suposto que ele seja gerenciado.

Solução

Remova os arquivos "RegConfigPM.xml" e "BackupConfiguration.xml" no diretório "<UDP_ENGINE_HOME>\Configuration", no nó do Agente do Arcserve UDP (Windows) e, em seguida, reinicie o "serviço do Agente do Arcserve UDP" do serviço do Windows.

Se o problema persistir, use o Bate-papo ao vivo para entrar em contato com o suporte da Arcserve. O Bate papo ao vivo permite viabilizar uma comunicação inteligente entre você e a equipe do suporte técnico, de modo que suas dúvidas e preocupações sejam atendidas imediatamente, sem interromper o acesso ao produto.

Pausar e retomar falham quando o agente não está conectado à rede

Sintoma

Se o agente não estiver conectado à rede e eu tentar pausar um plano, o plano não será pausado. Similarmente, se o agente não estiver conectado à rede e eu tentar retomar um plano, o plano não será retomado.

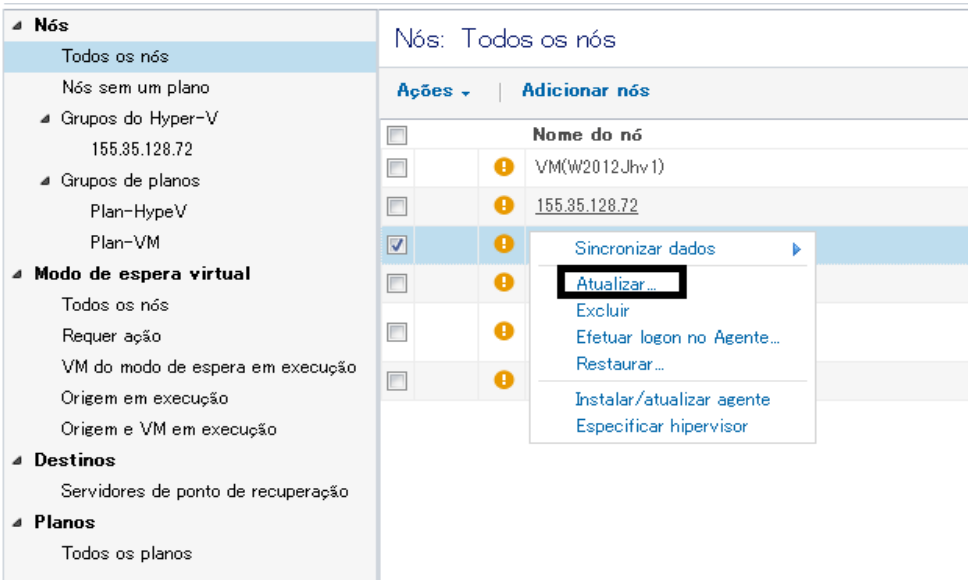
Solução

É possível resolver esse problema atualizando manualmente o nó no console.

Siga estas etapas:

1. Clique na guia de recursos no Console.
2. No painel à esquerda, navegue para **Nós** e clique em Todos os nós.

   Todos os nós adicionados são exibidos no painel central.
3. No painel central, selecione o nó.
4. Clique com o botão direito do mouse e selecione **Atualizar**.



O nó e o plano são atualizados.

O serviço do Agente do Arcserve UDP é executado lentamente

Válido em sistemas operacionais Windows.

Sintoma 1:

O serviço do agente de Arcserve UDP nos sistemas do Agente do Arcserve UDP é executado lentamente. É possível detectar outros sintomas, tais como:

- O serviço do agente do Arcserve UDP para de responder ou ocupa 100% dos recursos da CPU.
- A comunicação dos nós do agente do Arcserve UDP com o serviço da web é insatisfatória ou não existe.

Solução 1:

Em diversas configurações de ambiente, é possível detectar que o serviço do agente do Arcserve UDP ocupa muito tempo da CPU, ou a resposta é lenta. Por padrão, o Tomcat é configurado para alocar uma quantidade limitada de memória para os nós, que talvez não seja adequada para seu ambiente. Para verificar esse problema, revise os arquivos de log a seguir:

<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

Procure a seguinte mensagem:

java.lang.OutOfMemoryError

Para corrigir este problema, aumente a quantidade de memória alocada.

Para aumentar a memória, execute as seguintes etapas:

1. Abra o Registry Editor e acesse a chave a seguir:

   Sistemas operacionais x86:

   - HKEY_LOCAL_MACHINE\SOFTWARE\Apache Software Foundation\Procrun 2.0\CASAD2DWebSvc\Parameters\Java

   Sistemas operacionais x64:

   - HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\CASAD2DWebSvc\Parameters\Java

2. Use uma das seguintes opções:

- Se a mensagem no arquivo de log for:

  java.lang.OutOfMemoryError: PermGen space

  Acrescente o seguinte valor de opções.

  -XX:PermSize=128M -XX:MaxPermSize=128M

  Observação: talvez seja necessário aumentar o valor de -XX:MaxPermSize de acordo com seu ambiente.

- Se a mensagem no arquivo de log for:

  java.lang.OutOfMemoryError: Java heap space
  java.lang.OutOfMemoryError: GC overhead limit exceeded

  Aumente o valor de DWORD a seguir:

  JvmMx

3. Reinicie o serviço do agente do Arcserve UDP.

Sintoma 2

Os backups programados são ignorados e a execução é interrompida.

Solução 2

Ao configurar o valor MAX como 20 ou menos de 20 para backups simultâneos, execute as seguintes etapas:

1. Aumente o valor de DWORD a seguir:

   JvmMx=256

   Observação: esse DWORD é mencionado na Solução 1.

2. Acrescente o seguinte valor de opções.

   -XX:MaxPermSize=128M

   Observação: esse DWORD é mencionado na Solução 1.

Ao configurar o valor MAX como mais de 20, mas menos que 50 para backups simultâneos, execute as seguintes etapas:

1. Aumente o valor de DWORD a seguir:

   JvmMx=512

   Observação: esse DWORD é mencionado na Solução 1.

2. Acrescente o seguinte valor de opções.

   -XX:MaxPermSize=256M

   Observação: esse DWORD é mencionado na Solução 1.

Configurar o registro para executar novamente uma tarefa de cópia em fita

Sintoma

A tarefa de cópia em fita não foi executada para algum erro de mídia e você deseja executar a tarefa novamente.

Solução

É possível controlar o número de tarefas de repetição e o intervalo de tempo das tarefas de repetição para a tarefa de cópia em fita usando as duas chaves de registro a seguir. Ambas as chaves do registro estão no computador em que você instalou o Servidor de backup do Arcserve:

NumberOfRetryCopyToTapeJob

Se uma tarefa de cópia em fita falhar, o Arcserve UDP repetirá a tarefa que falhou. O número de tentativas é configurado usando a chave de registro **NumberOfRetryCopyToTapeJob**. Mas, se as informações de ponto de recuperação ou nó para cópia forem alteradas na tarefa, o Arcserve UDP redefinirá o número de falhas acumuladas como 0. Isso significa que quando nó para copiar ou as informações do ponto de recuperação forem alteradas na tarefa, a tarefa de cópia em fita pode ser executada sem estar limitada pelo número de tentativas. Além disso, se o serviço web de backup do Arcserve for reiniciado, o Arcserve UDP redefinirá o número de falhas acumuladas como 0.

A chave do registro está localizada no Servidor de backup do Arcserve no seguinte local:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\CA ARCServe Backup\WebServiceInfo\NumberOfRetryCopyToTapeJob

Tipo é DWORD.

Padrão: 1

TimeIntervalOfRetryCopyToTapeJob

Controla o intervalo de repetição para a tarefa de cópia em fita que falhou. Esta chave de registro é usada em associação com **NumberOfRetryCopyToTapeJob**.

A chave do registro está localizada no Servidor de backup do Arcserve no seguinte local:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\CA ARCServe Backup\WebServiceInfo\TimeIntervalOfRetryCopyToTapeJob

Tipo é DWORD.

Padrão: 1 horas

Configurar o registro para copiar em fita vários pontos de recuperação do mesmo tipo na mesma tarefa

Sintoma

Por padrão, a tarefa de cópia em fita copia em fita todos os pontos de recuperação qualificados como se fossem do mesmo tipo. Como resultado, o processo de cópia é demorado e o consumo de espaço em fita é maior. Talvez você queira copiar apenas o mais recente dos pontos de recuperação qualificados.

Solução

É possível configurar o registro no nó do servidor do Arcserve Backup para ativar a cópia em fita do ponto de recuperação mais recente do mesmo tipo.

Siga estas etapas:

1. No nó do servidor do Arcserve Backup, adicione o valor DWORD abaixo no registro localizado em:[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ComputerAssociates\CA ARCServe Backup\WebServiceInfo]:

   "CopyLatestRecoveryPointOfSameType"=dword:00000001

2. Reinicie o serviço web do servidor do Arcserve Backup para aplicar as alterações.

   Todas as tarefas de cópia em fita no nó do servidor do Arcserve Backup copiarão em fita o ponto de recuperação mais recente do mesmo tipo.

Não inclusão de arquivo/pasta no backup da pasta NFS compartilhada ou conversão de nome de arquivo/pasta em um nome ilegível

Sintoma

Ao fazer backup da pasta NFS compartilhada, alguns arquivos/algumas pastas não são incluídos nos dados de backup ou o nome de um arquivo ou uma pasta é convertido em um nome ilegível.

Solução

Este problema ocorrerá se um arquivo ou uma pasta na pasta NFS compartilhada tiver um nome com uma codificação de idioma sem suporte. Como uma solução, exporte uma pasta SMB compartilhada em vez da pasta NFS compartilhada. Considere também a adição de um caminho UNC ou NFS com o protocolo SMB.

Para obter mais informações sobre como adicionar um caminho UNC e sobre a codificação de idiomas com suporte, consulte Adicionar um caminho UNC.

Falha no backup da pasta NFS compartilhada

Sintoma

Quando o backup da pasta NFS compartilhada é executado, ocorre falha na tarefa.

Solução

Este problema ocorre se o GID (Group Identifier - Identificador de Grupo) e o UID (User Identifier - Identificador de Usuário) são alterados dos valores padrão. Mantenha sempre apenas os valores padrão do GID e do UID para o cliente NFS e o servidor NFS.

Redefinir o console do UDP com MFA ativado quando o TOTP não estiver disponível

Sintoma

Depois que o processo de logon de autenticação multifator (MFA) for ativado no console do UDP, você poderá:

- Esquecer-se de verificar o código QR
- Perder seu dispositivo móvel que contém um aplicativo autenticador
- Desinstalar o aplicativo autenticador

Solução 1

Se você for um superadministrador ou um usuário administrador ou não administrador, entre em contato com o administrador ou com outros usuários administradores do UDP para redefinir o código QR no console do UDP.

Solução 2

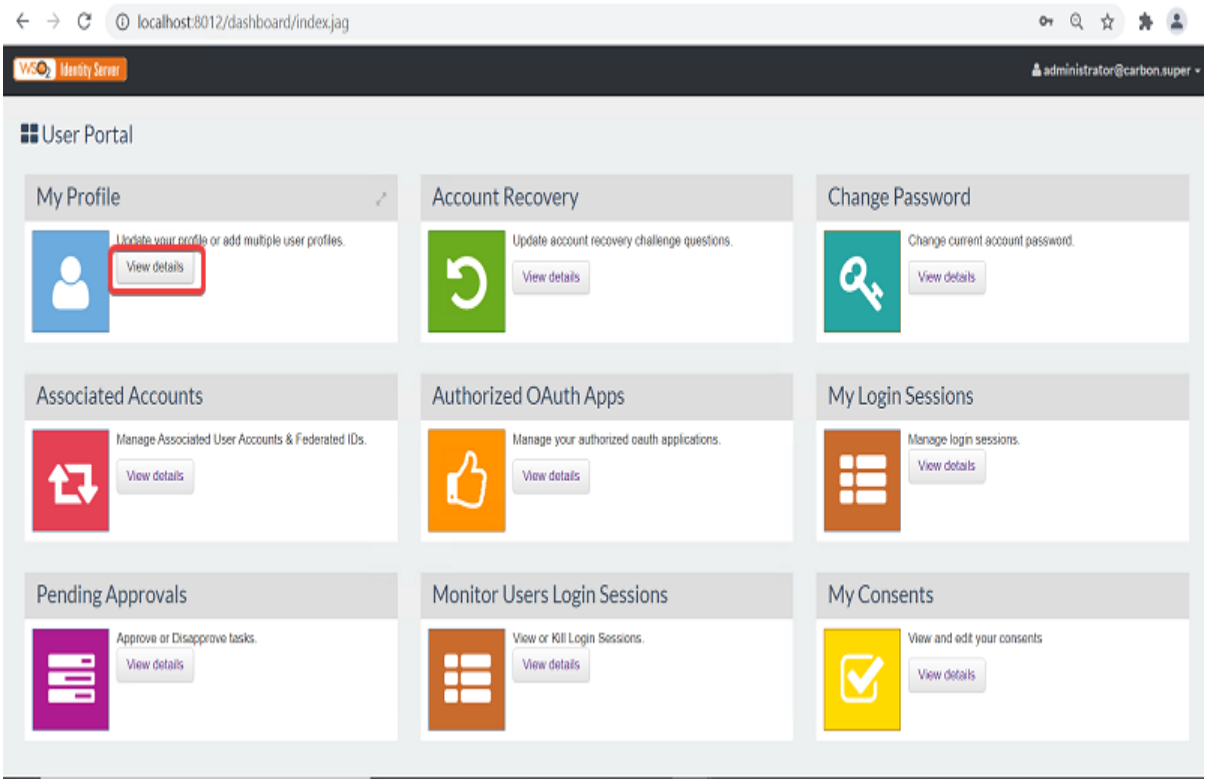
Se você for um superadministrador ou um usuário administrador, poderá verificar a imagem do código QR para obter um novo TOTP usando o portal do painel do servidor de identidade.

Siga estas etapas:

1. Efetue logon no painel do servidor de identidade.

   Por exemplo: *https://localhost:8012/dashboard*

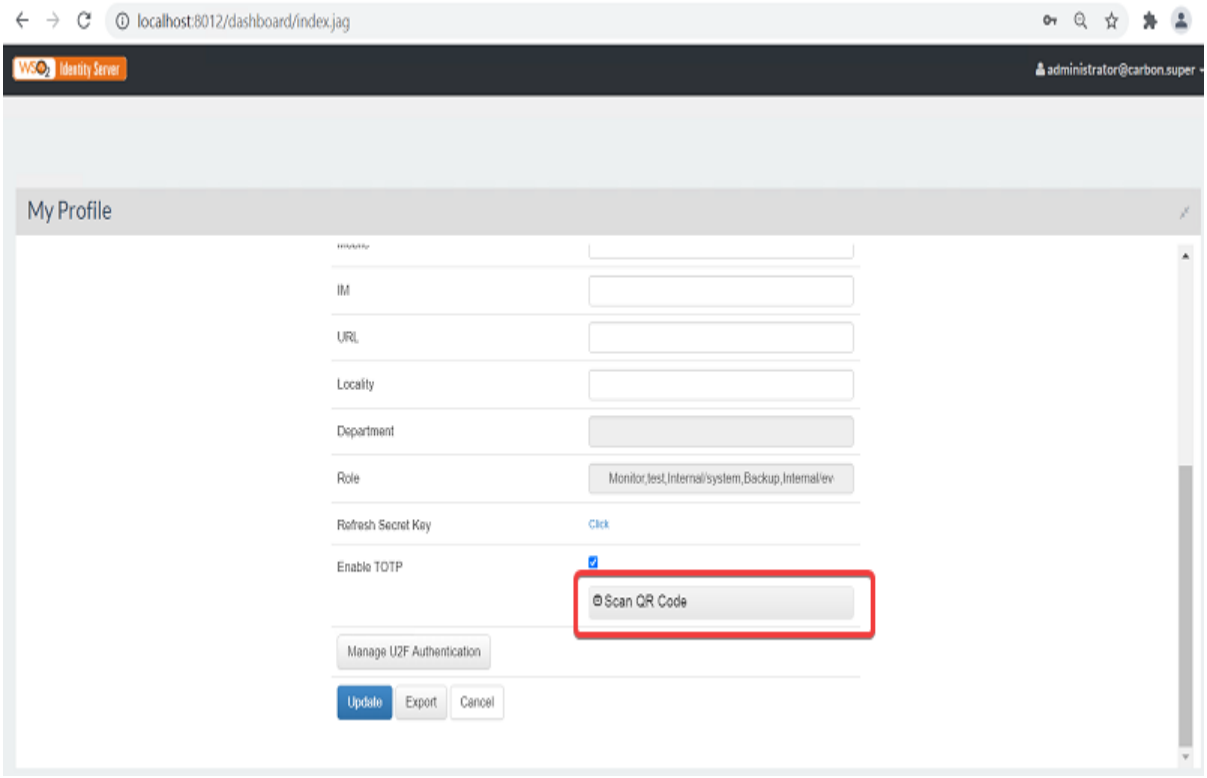
   A página Portal do usuário é exibida.



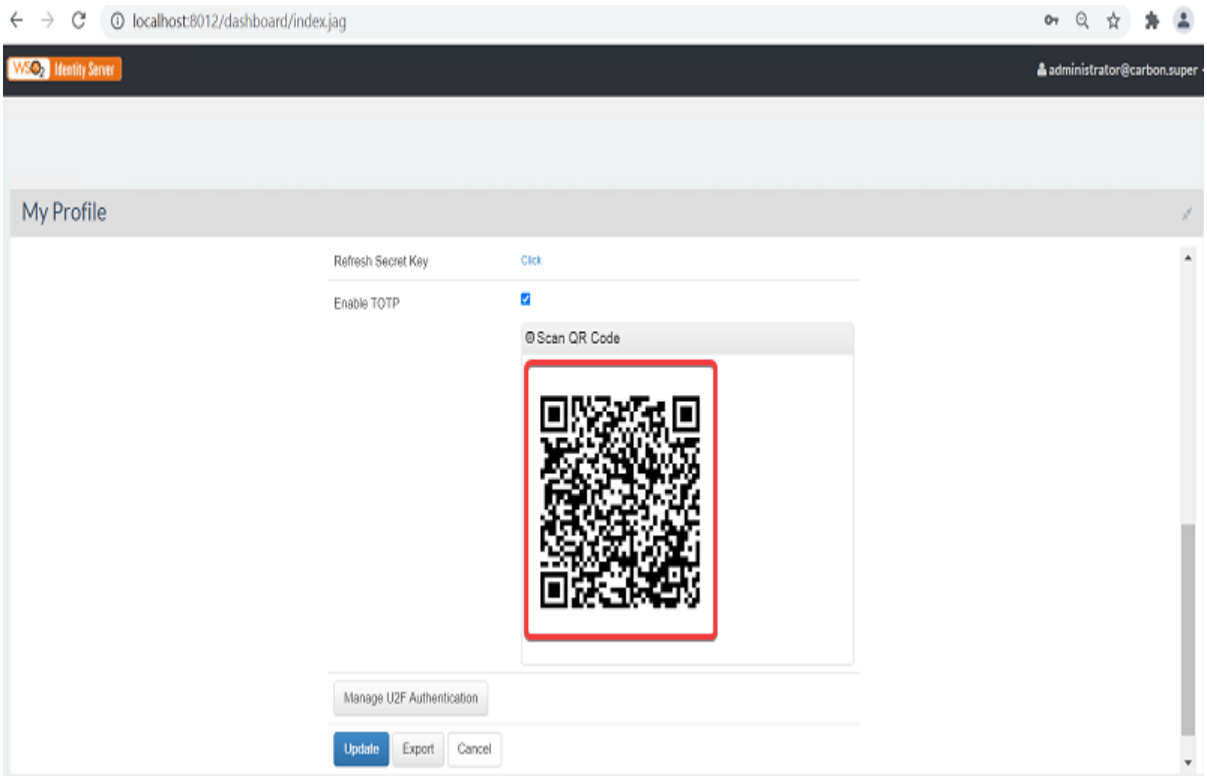
2. Na página Portal do usuário, clique em **Exibir detalhes**.

   A página Meu perfil é exibida.

3. Na página Meu perfil, em Ativar TOTP, clique em **Verificar código QR** para exibir uma imagem do código QR.



4. Para gerar o TOTP, verifique a imagem do código QR usando um aplicativo autenticador.



5. Vá para a página de logon do console do UDP e efetue logon usando o TOTP recém-gerado.

Solução 3

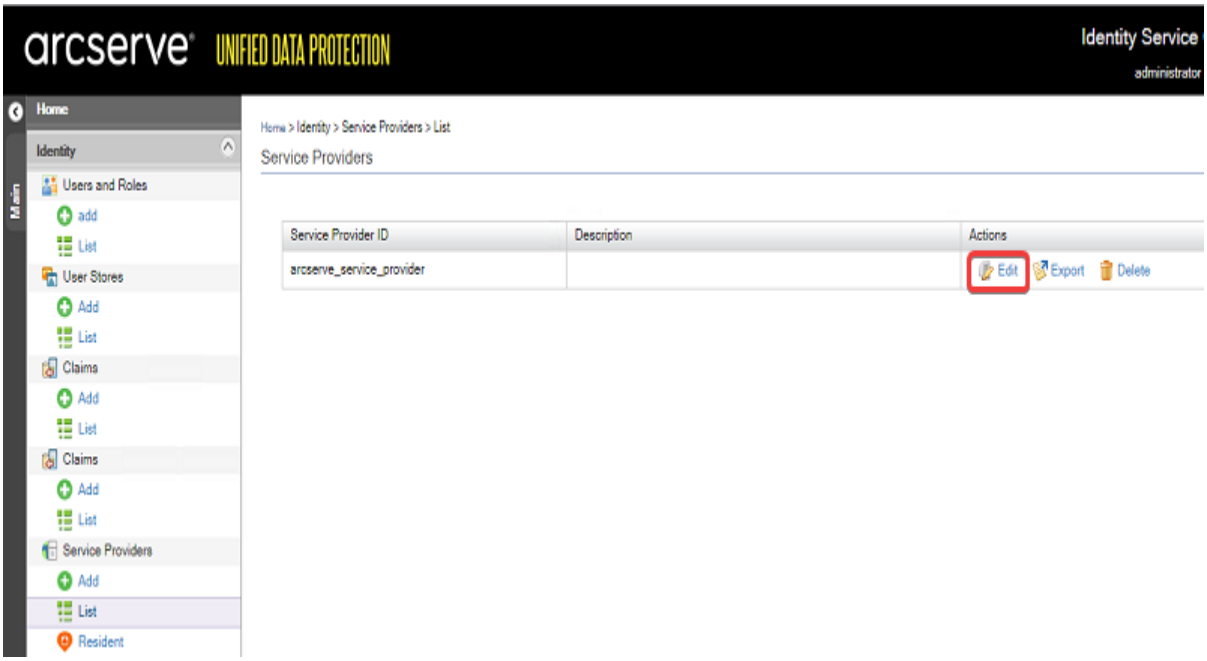
Se você for um usuário superadministrador, poderá remover completamente as configurações existentes.

Siga estas etapas:

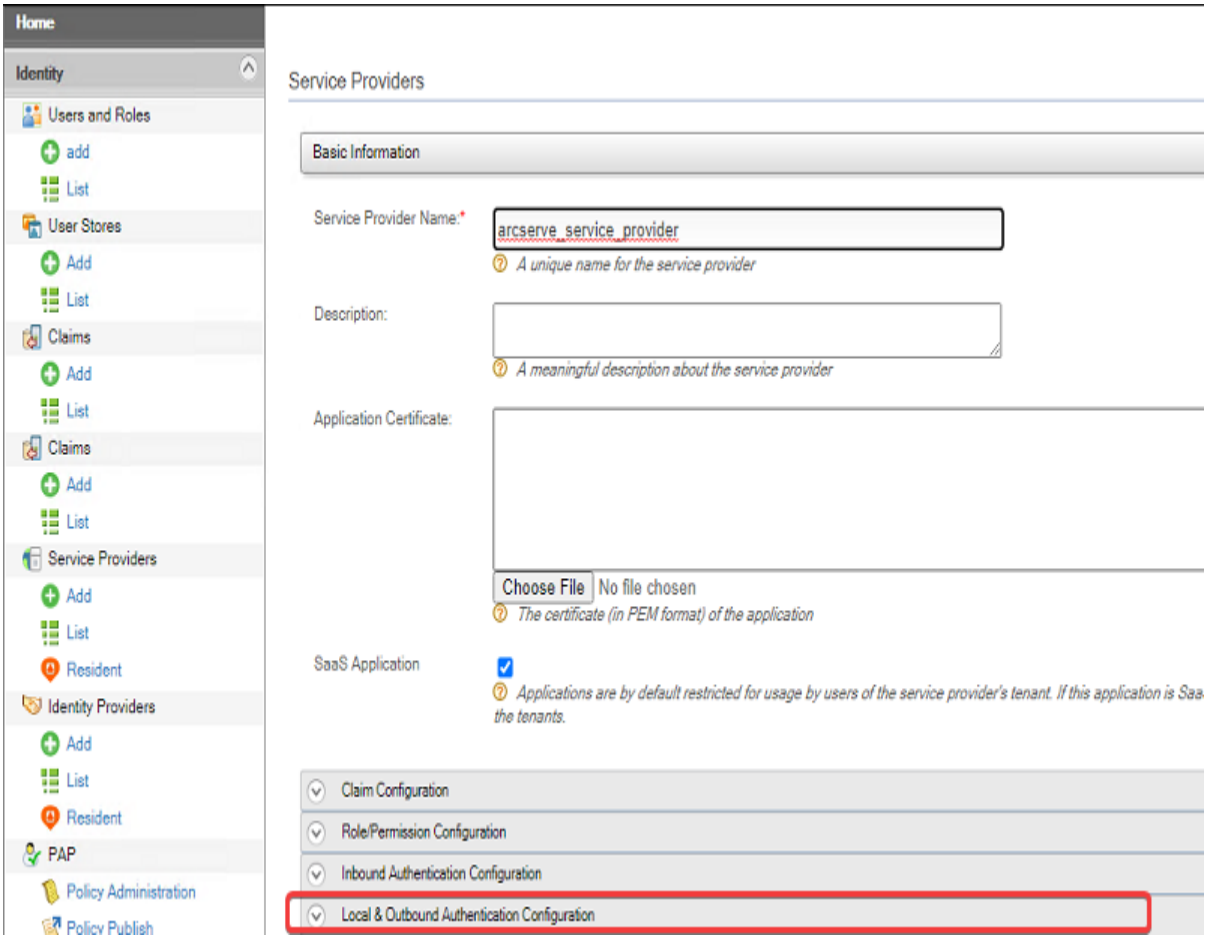
1. Navegue até o caminho *...\Arquivos de programas\Arcserve\Unified Data Protection\Management\IdentityServer\repository\conf* e, em seguida, abra o arquivo *carbon.xml* com um editor.
2. No arquivo carbon.xml, comente as marcações XML *HideMenuItemIds* e salve o arquivo.

3. Reinicie o serviço de identidade do Arcserve UDP.
4. Inicie o console de gerenciamento de usuários. Para obter mais informações, consulte Iniciar o console de gerenciamento de usuários do Arcserve UDP.

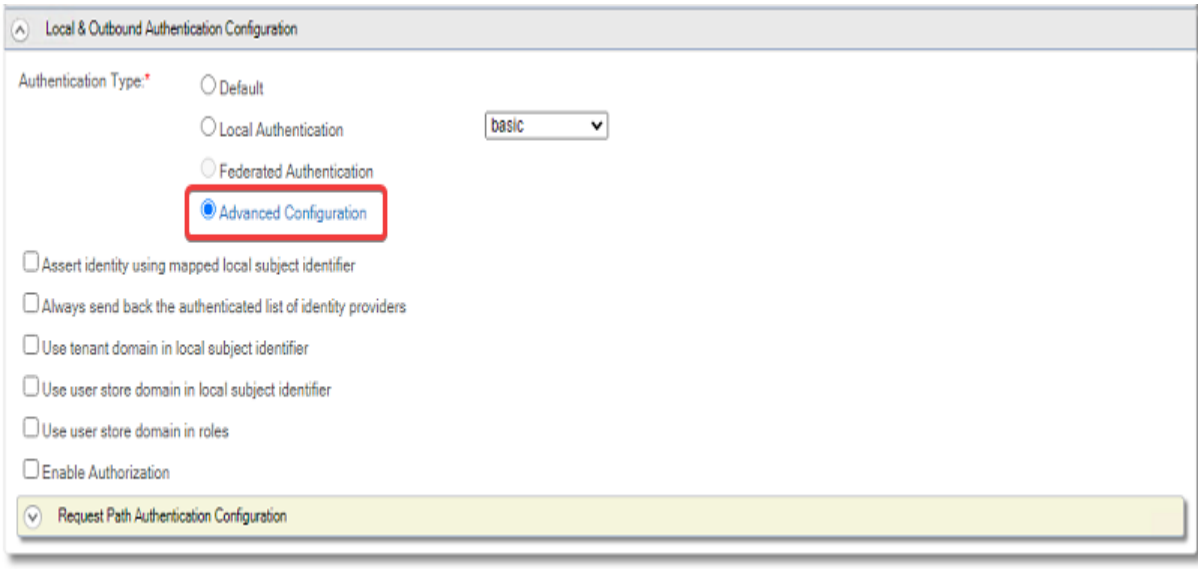
   A página Console do serviço de identidade é exibida.
5. Vá para **Início** > **Identidade** > **Provedores de serviços** > **Listar**.



6. Na lista de provedores de serviços, em *arcserve_service_provider*, clique em **Editar**.



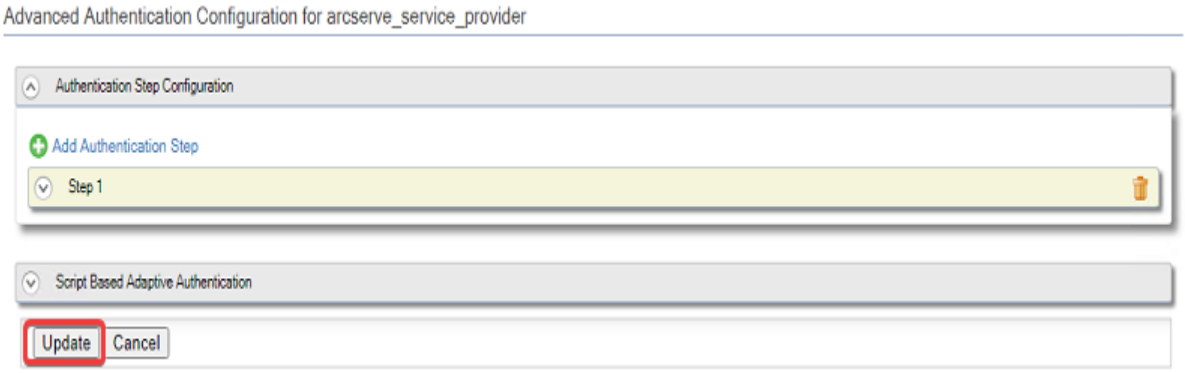
7. Expanda a lista suspensa **Configuração de autenticação local e de saída** e selecione **Configuração avançada**.



A página *Configuração avançada do arcserve_service_provider* é exibida.

8. Na página *Configuração avançada do arcserve_service_provider*, em Configuração da etapa de autenticação, para remover a etapa 2, clique no ícone **Excluir**.

9. Clique em **Atualizar** para salvar as alterações.



As configurações existentes são removidas.

10. Vá para a página de logon do UDP e efetue logon usando o nome de usuário e a senha.
11. Vá para **Configurações** > **Gerenciamento de usuários**.
12. Na seção Autenticação multifator, para desativar MFA, clique na configuração **DESATIVAR**.
13. Clique em **Salvar**.

    As configurações de logon de MFA foram removidas com êxito.

Assuntos relacionados à VM instantânea

Esta seção inclui os seguintes tópicos de solução de problemas relacionados à Máquina Virtual instantânea:

- Falha ao criar uma VM instantânea em VMware devido à duplicação do nome do repositório de dados NFS
- Falha ao criar uma VM instantânea com o Windows 2008 como o servidor de recuperação para o Servidor Hyper-V da VMware ou do Windows 2008 R2
- Falha ao inicializar uma VM instantânea se o computador de origem for um servidor Windows 2008/2012/2016 do AD
- Falha ao ligar VM após restauração do Hyper-V
- Falha na tarefa de VM instantânea devido a um erro de serviço do Windows NFS
- A pasta de arquivo da VM instantânea não pode ser acessada ou excluída mesmo com privilégio de administrador
- Falha da máquina virtual instantânea ao inicializar no Hyper-V após reiniciar o servidor de recuperação
- Falha ao criar o repositório de dados NFS da VMware e exibir Impossível resolver o erro de nome do host
- Não foi possível implantar o serviço de integração na máquina virtual de convidado no Hyper-V
- Falha da VM instantânea do Linux no servidor do Hyper-V em idioma diferente do inglês
- Consumo de licença extra para os caminhos UNC que residem em uma VM sob um Hyper-V licenciado
- É exibido um erro de falha de licença quando você altera a edição/o tipo de licença e cria uma VM instantânea

Falha ao criar uma VM instantânea em VMware devido à duplicação do nome do repositório de dados NFS

Sintoma

A criação da VM instantânea falha e exibe a seguinte mensagem de erro:

Falha ao criar o repositório de dados com base em NFS [arcserve_UDP_<Host-nam/IP>] com o nome do compartilhamento NFS [arcserve_UDP_IVM_ {GUID}]. Código de erro: 12. Mensagem de erro: a chave, o nome ou o identificador especificados já existem (detalhes:).

A razão para esse erro pode ser que um repositório de dados NFS com o mesmo nome já existe e não é removido ou o vCenter/Host ainda tem referências do repositórios de dados NFS em seus registros. No entanto, quando você efetuar logon diretamente no host, verá um repositório de dados NFS. É provável que esse repositório de dados esteja marcado como inativo e esteja esmaecido.

Solução

Para resolver esse problema:

1. Efetue logon no host do ESX e remova o repositório de dados NFS.
2. Reinicie os agentes de gerenciamento nesse host do ESX usando o seguinte comando:

   ```
   /sbin/services.sh restart
   ```

Para obter mais informações sobre como trabalhar no host do ESX, consulte a documentação do VMware.

Falha ao criar uma VM instantânea com o Windows 2008 R2 como o servidor de recuperação para VMware ou Windows 2008 R2 Hyper-V Server

Sintoma

A criação da VM instantânea falha, e o seguinte erro aparece no log de atividades de tarefas:

O Windows não pode verificar a assinatura digital desse arquivo. Uma alteração recente de hardware ou software talvez tenha instalado um arquivo que está assinado incorretamente ou danificado, ou que pode ser software malicioso de origem desconhecida.

Solução

Essa VM instantânea falha ao ser criada porque o driver da VM instantânea é assinado com um certificado digital seguro que não é suportado no Windows 2008 R2, até que você aplique um patch da Microsoft.

Aplique o patch 3033929 da Microsoft e tente criar a VM instantânea novamente.

Falha ao inicializar uma VM instantânea se o computador de origem for um servidor Windows 2008/2012/2016 do AD

Sintoma

Falha ao inicializar a VM instantânea quando ela é um servidor do Active Directory do Windows 2008.

Quando o computador de origem é um servidor do Active Directory do Windows executando a tarefa de VM instantânea, a VM instantânea não consegue inicializar, e uma tela azul aparece exibida com a seguinte mensagem:

INTERROMPER: não foi possível iniciar os serviços de diretório c00002e2 devido ao seguinte erro: um dispositivo conectado ao sistema não está funcionando. Status do erro: 0xc0000001.

Solução 1:

Se o hipervisor de destino for um Hyper-V, adicione a seguinte chave do Registro no hipervisor Hyper-V e, em seguida, dispare a tarefa de IVM.

Se o hipervisor de destino for um ESX/Vcenter, adicione a seguinte chave do Registro ao computador proxy, que é usado para executar a tarefa de VM instantânea e, em seguida, dispare a tarefa de IVM.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\InstantVM
```

Tipo de registro: valor DWORD

Nome: RenameADLog

Valor: 1

Limitações:

- Se o banco de dados e os caminhos do arquivo de log do NTDS estiverem em volumes diferentes, a solução acima não será adequada.
- A partir de agora, a solução acima é válida apenas para o Windows 2008 Active Directory Server.

Solução 2:

Resolvendo o problema manualmente, fazendo logon na VM instantânea.

Siga estas etapas:

1. Ligue a VM instantânea.
2. Ao ligar o computador, pressione F8 antes de o sistema operacional começar a carregar e escolha o modo **Restauração dos serviços de diretório**.
3. Renomeie todos os arquivos *.log na pasta *C:\Windows\NTDS*. Por exemplo, renomeie o arquivo edb.log como edb.log.old.
4. Execute o seguinte comando:

   ```
   esentutl /p "C:\Windows\NTDS\ntds.dit"
   ```

5. Reinicie o sistema.

Observação: a solução acima é válida para todas as versões de servidores Windows com o Active Directory instalado.

Falha ao ligar VM após restauração do Hyper-V

Sintoma

Não é possível ligar a máquina virtual após restaurar a máquina virtual do Hyper-V. O seguinte erro é exibido:

Porta Ethernet Sintética (ID da instância...): falha ao ligar com o erro 'Tentativa de acessar endereço inválido.'

Solução

Esse erro ocorre porque o endereço MAC da VM restaurada entra em conflito com as VMs existentes. Remova o adaptador de NIC da VM restaurada e, em seguida, adicione manualmente um novo para resolver o problema e conseguir ligar com êxito.

Falha na tarefa de VM instantânea devido a um erro de serviço do Windows NFS

Sintoma

Quando o servidor de recuperação de VM instantânea tem Agente do Arcserve UDP e Backup do Arcserve instalados, quando você cria uma VM instantânea para o servidor VMware ESX (i), o serviço do Windows NFS não é iniciado e a tarefa de VM instantânea falha.

Solução

O motivo pelo qual o serviço do Windows NFS falha ao ser iniciado é porque o número da porta padrão do serviço do Windows NFS é 111 e foi usado pelo serviço de backup do Arcserve, **Servidor de chamadas de procedimento remoto**.

Para resolver esse problema, altere o número da porta padrão do serviço de backup do Arcserve, **Servidor de chamadas de procedimento remoto** para outra porta e tente criar a VM instantânea novamente. Para obter mais informações sobre como alterar a porta padrão, consulte Modificar o arquivo de configuração de portas e Portas de comunicação do servidor integrante e servidor principal na documentação de backup do Arcserve.

A pasta de arquivo da VM instantânea não pode ser acessada ou excluída mesmo com privilégio de administrador.

Sintoma

A pasta de arquivo da VM instantânea não pode ser acessada ou excluída devido ao erro "Requer permissão de administrador", mesmo que o usuário tenha privilégios de administrador.

Solução

Esse é um problema do NFS. Primeiro é necessário remover o compartilhamento de NFS para então poder excluir a pasta. Use a seguinte linha de comando para excluir a pasta:

nfsshare /delete [nfs share name]

Falha da máquina virtual instantânea ao inicializar no Hyper-V após reiniciar o servidor de recuperação

Sintoma

Ao iniciar a IVM (Instant Virtual Machine - Máquina Virtual Instantânea) e, em seguida, reiniciar o servidor de recuperação Hyper-V, a IVM falha ao inicializar.

Solução

Para resolver essa falha de inicialização, reinicie a IVM.

Falha ao criar o repositório de dados NFS da VMware e erro Não foi possível resolver o nome do host

Válido para VMware

Sintoma

A criação da VM instantânea falha e exibe a seguinte mensagem de erro:

Falha ao criar o repositório de dados do NFS da VMWARE pelo servidor <nome do host do servidor de recuperação>.

Mensagem de erro: ocorreu um erro durante a configuração do host.

Detalhes: falha na operação, relatório de diagnóstico: Não é possível resolver o nome do host <um nome do host, mas não servidor de recuperação>.

Exemplo

Falha ao criar o repositório de dados do NFS da VMWARE pelo servidor 'host1'.

Mensagem de erro: ocorreu um erro durante a configuração do host.

Detalhes: falha na operação, relatório de diagnóstico: não é possível resolver o nome de host 'host2'.

Solução

O motivo para esse erro é que o servidor ESX lista todos os repositórios de dados NFS ao criar o repositório de dados NFS InstantVM, mesmo quando alguns repositórios de dados não estão mais disponíveis. Por exemplo, o repositório de dados NFS criado pelo **host2** ainda existe, mesmo se **host2** não estiver disponível porque o computador foi excluído. Para que o servidor ESX não é possível resolver o nome do host.

Para resolver esse problema, exclua o repositório de dados indisponível do servidor ESX.

Siga estas etapas:

1. Efetue logon no ESX Server usando SSH.
2. Digite o seguinte comando:

   ```
   esxcfg-nas -l
   ```

   O mesmo erro é exibido na linha de comando.

   ```
   Erro ao executar a operação: não é possível resolver
   o nome de host 'host2'.
   ```

3. Adicione um mapeamento no arquivo **/etc/hosts** do servidor ESX para resolver esse problema.

   <IP address> <hostname>

   Observação: O endereço IP deve estar acessível.

   Exemplo: 10.57.X.X host2

4. Liste todos os repositórios de dados NFS usando o seguinte comando:

   ```
   esxcfg-nas -l
   ```

   ```
   arcserve_UDP_<hostname> is /arcserve_UDP_IVM_{ESX_
   generated_number} from <hostname> unmounted una-
   vailable
   ```

   Exemplo: esxcfg-nas –l

   arcserve_UDP_host2 is /arcserve_UDP_IVM_{991555E6-09A4-4D80-A47E-522831A62Axx} from host2 unmounted unavailable

5. Use o comando a seguir para excluir o repositório de dados indisponível:

   ```
   esxcfg-nas -d arcserve_UDP_host2
   ```

6. Remover o mapeamento <hostname> no arquivo **/etc/hosts** do servidor ESX.

   Agora você pode usar a função do NFS normalmente.

   Observação: Para obter mais informações sobre esse problema, consulte o artigo da base de conhecimento da VMware.

Falha ao implantar o serviço de integração na VM convidada no Hyper-V

Sintoma

Ao fazer backup de uma máquina virtual que tem o aplicativo (SQL ou Exchange) instalado, o ponto de recuperação não inclui as informações de gravador e o log de atividades da tarefa de backup exibe a seguinte mensagem de aviso:

Não foi possível implantar o serviço à VM.

Solução

Esse problema geralmente ocorre quando o Windows Management Instrumentation (WMI) está desativado por firewall na VM convidada. Para resolver esse problema, siga as etapas seguintes:

1. Efetue logon na VM convidada.
2. Abra o Painel de Controle.
3. Abra o Firewall do Windows.
4. Clique em Permitir um aplicativo ou recurso através do Firewall do Windows.
5. Ative a WMI.
6. Clique em OK.

Falha da VM instantânea do Linux no servidor do Hyper-V em idioma diferente do inglês

A VM instantânea do Linux no servidor Hyper-V em idioma diferente do inglês falhou devido à falha de conexão, mesmo quando o firewall estava desativado.

Sintoma

A criação da VM instantânea falha e exibe o seguinte erro:

Falha ao se estabelecer conexão com o host do Hyper-V [ServerName do Hyper-V de destino]. Verifique se o endereço do host está correto ou se as credenciais são válidas.

Solução

A configuração incorreta das informações de conexão do servidor do Hyper-V pode causar esse problema.

Para obter mais detalhes, consulte **Configurar as informações de conexão do servidor do Hyper-V para a VM instantânea** no *Guia do Usuário do Agente do Arcserve UDP para Linux*.

Consumo de licença extra para os caminhos UNC que residem em uma VM sob um Hyper-V licenciado

Sintoma

Os caminhos UNC que residem na VM sob um hipervisor consomem uma licença de soquete extra, mesmo quando a licença já tiver sido aplicada anteriormente para o host do hipervisor. Esse erro resulta no consumo de licenças adicionais.

Solução

O backup do host do hipervisor e os caminhos UNC que residem no mesmo hipervisor consomem a mesmo licença. Mas, ao fazer backup dos caminhos UNC que residem em uma VM que está sob o mesmo hipervisor, os caminhos UNC/-compartilhamentos consomem uma licença extra. Esse problema ocorre apenas se a VM não tiver sido adicionada/importada como um nó para o console e, também, quando os caminhos UNC são adicionados com um nome diferente do nome fornecido ao adicionar a VM ao console.

Siga estas etapas:

1. Adicione o nó (a VM com caminhos UNC) ao console e especifique os detalhes do hipervisor para o nó ou importe o nó a partir do hypervisor.
2. Adicione os caminhos UNC/compartilhamentos com o mesmo nome que aquele definido na etapa 1.

É exibido um erro de falha de licença quando você altera a edição/o tipo de licença e cria uma VM instantânea

Sintoma

Depois de adicionar ou alterar um tipo ou uma edição de licença no console e criar uma VM instantânea sem executar nenhuma tarefa de backup, uma mensagem de erro de falha na licença será exibida. No entanto, na próxima vez que você executar uma VM instantânea, ela identificará com êxito a nova licença e criará uma VM instantânea.

Solução

Siga estas etapas:

1. Depois que uma nova licença for adicionada ao console do UDP, execute a tarefa de backup para o plano existente.
2. Agora, crie uma VM instantânea.

Assuntos relacionados ao agente do Linux

Esta seção inclui os seguintes tópicos de solução de problemas relacionados ao agente do Arcserve UDP Linux:

- Configurações de destino de backup desativadas ao abrir a interface do usuário do agente Linux
- O status de tarefas, histórico de tarefas e o log de atividades não são visíveis

Configurações de destino de backup desativadas ao abrir a interface de usuário do agente do Linux

Se o servidor de backup do Linux não for removido do Console do Arcserve UDP antes de desinstalar o Console, as configurações de destino de backup serão desativadas ao abrir a interface de usuário do servidor de backup.

Sintoma

O servidor de backup não é notificado de que Console do Arcserve UDP está desinstalado. O servidor de backup pressupõe que ainda está sendo gerenciado pelo Console.

Solução

Efetue logon no Servidor de backup e execute o seguinte comando:

```
# /opt/Arcserve/d2dserver/bin/d2dreg --release
```

O servidor de backup é liberado no console e, agora, é possível alterar as configurações de backup a partir na interface de usuário do servidor de backup.

Se o problema persistir, use o Bate-papo ao vivo para entrar em contato com o suporte da Arcserve. O Bate papo ao vivo permite viabilizar uma comunicação inteligente entre você e a equipe do suporte técnico, de modo que suas dúvidas e preocupações sejam atendidas imediatamente, sem interromper o acesso ao produto.

O status de tarefas, histórico de tarefas e o log de atividades não são visíveis

Sintoma

Eu não consigo ver o status de tarefas, o histórico da tarefa e o log de atividades no Console do Arcserve UDP.

Solução

O servidor de backup Linux não pode estabelecer conexão com Arcserve UDP usando o nome do host.

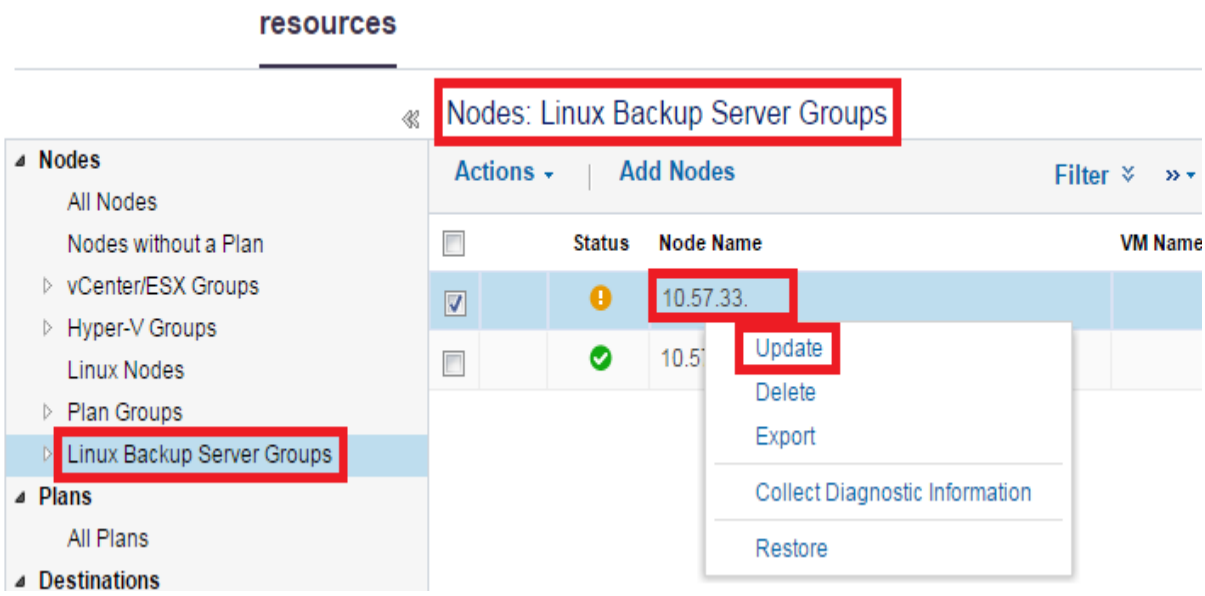
Siga estas etapas:

1. Crie o arquivo server_ip.ini no seguinte local do Arcserve UDP:

   "UDP installation path"\Management\Configuration\server_ip.ini

2. Digite o endereço IP o Arcserve UDP nesse arquivo.
3. Efetue logon no console do Arcserve UDP e atualize o servidor de backup Linux, bem como os nós Linux.

   Observação: o servidor de backup Linux pode ser atualizado apenas nos Grupos de servidores de backup Linux, onde todos os servidores de backup Linux estão listados.



O status de tarefas, o histórico de tarefas e o log de atividades são visíveis.

Falha ao restaurar o volume do sistema do SUSE15 com o sistema de arquivos XFS

O volume do sistema do SUSE15 com o sistema de arquivos XFS falha ao restaurar.

Sintoma

Falha ao executar a tarefa de restauração do nó do SUSE15 com o sistema de arquivos XFS.

Solução

Esse problema ocorre porque o volume do sistema não foi montado. Crie um Live CD do CentOS 7.5 e use-o para realizar a BMR/BMR instantânea.

Se o problema persistir, use o Bate-papo ao vivo para entrar em contato com o suporte da Arcserve. O Bate papo ao vivo permite viabilizar uma comunicação inteligente entre você e a equipe do suporte técnico, de modo que suas dúvidas e preocupações sejam atendidas imediatamente, sem interromper o acesso ao produto.

Relacionado à restauração

Esta seção inclui os seguintes tópicos de solução de problemas relacionados a restauração de:

- Impossível restaurar arquivos
- Adicionar o banco de dados de conteúdo restaurado para o aplicativo web original
- O banco de dados não pode ser montado ao restaurar o banco de dados do Microsoft Exchange
- O campo De não é exibido corretamente para emails enviados por usuários que têm permissões "em nome de" para uma caixa de correio compartilhada
- Falha nas tarefas de restauração após backups leves de integração

Impossível restaurar arquivos

Sintoma

Devido a uma limitação da Microsoft, os dados do arquivo em volumes NTFS com redução de redundância de um sistema Windows 2012 R2 não podem ser lidos de um sistema Windows 2012. Como resultado, se o agente UDP em um sistema Windows 2012 estiver sendo usado para restaurar uma VM com sistema operacional Windows 2012 R2 convidado e contendo volumes NTFS com redução de redundância, os seguintes problemas podem ocorrer. O problema ocorre apenas durante a operação de restauração de um ponto de recuperação em nível de arquivo ou em montagem.

O arquivo ou diretório é corrompido e fica ilegível.

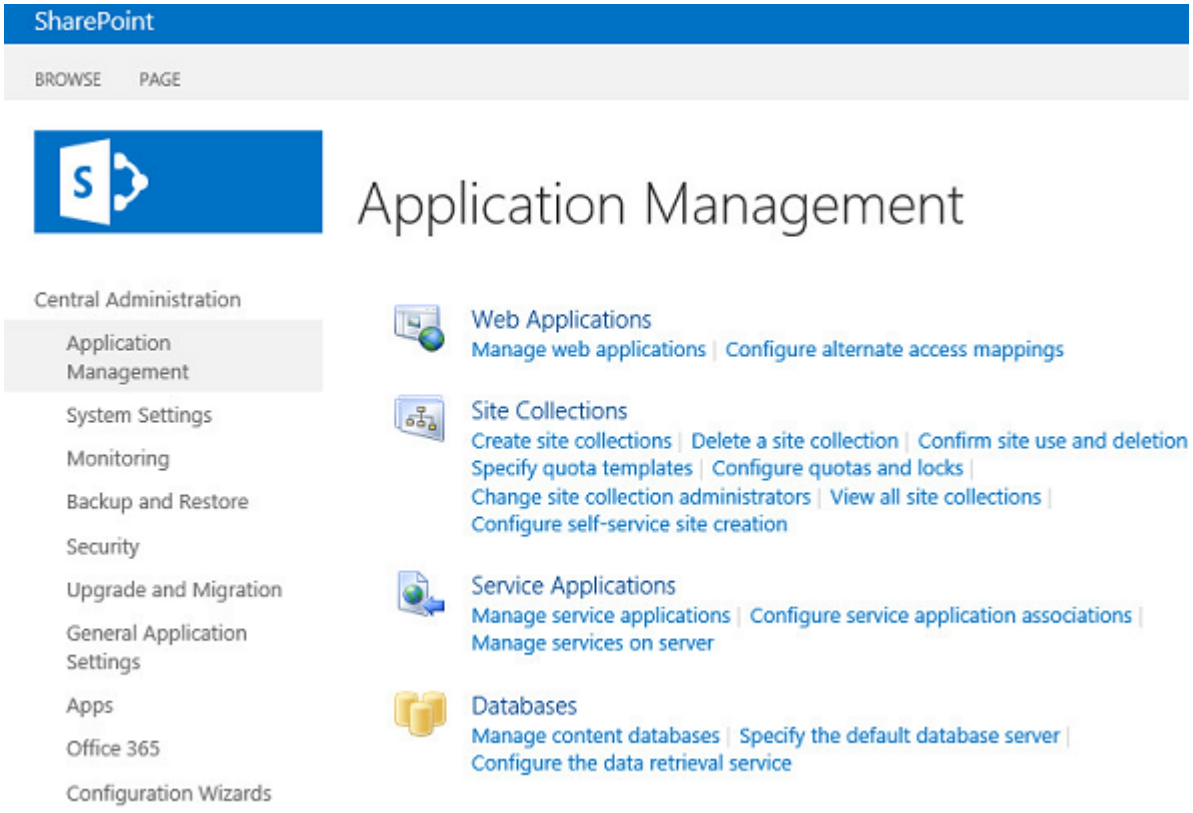
Solução

Quando isso ocorre, inicie o processo de restauração de um agente UDP instalado em um sistema Windows 2012 R2.

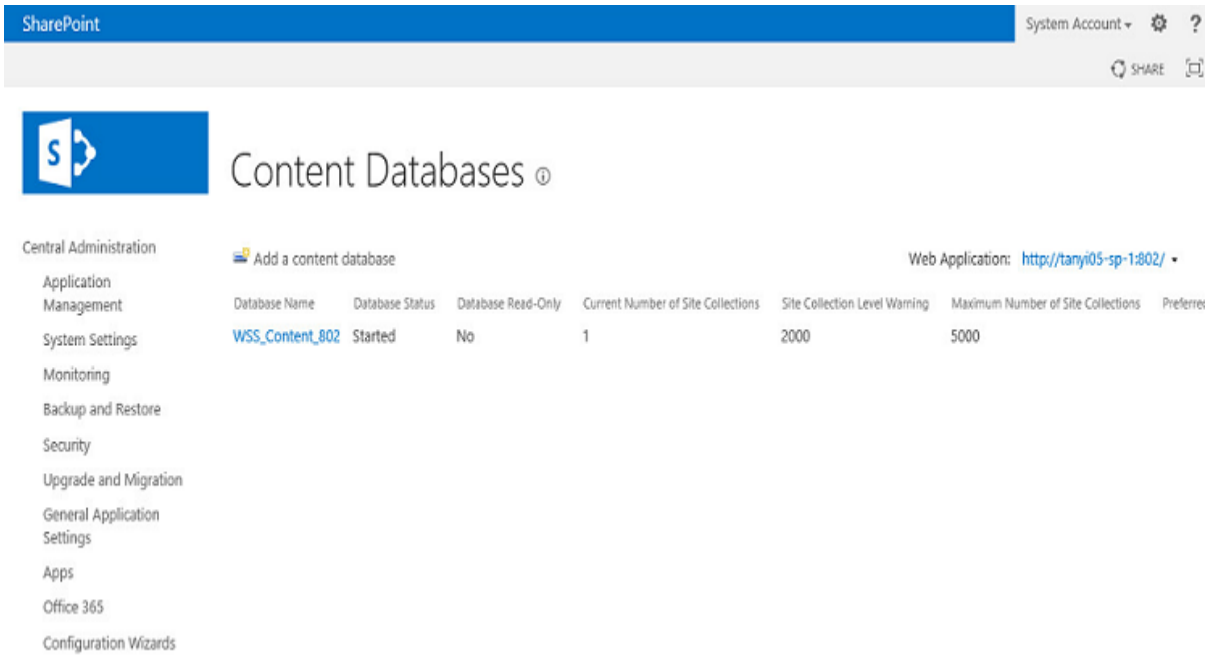
Adicionar o banco de dados de conteúdo restaurado para o aplicativo web original

Siga estas etapas:

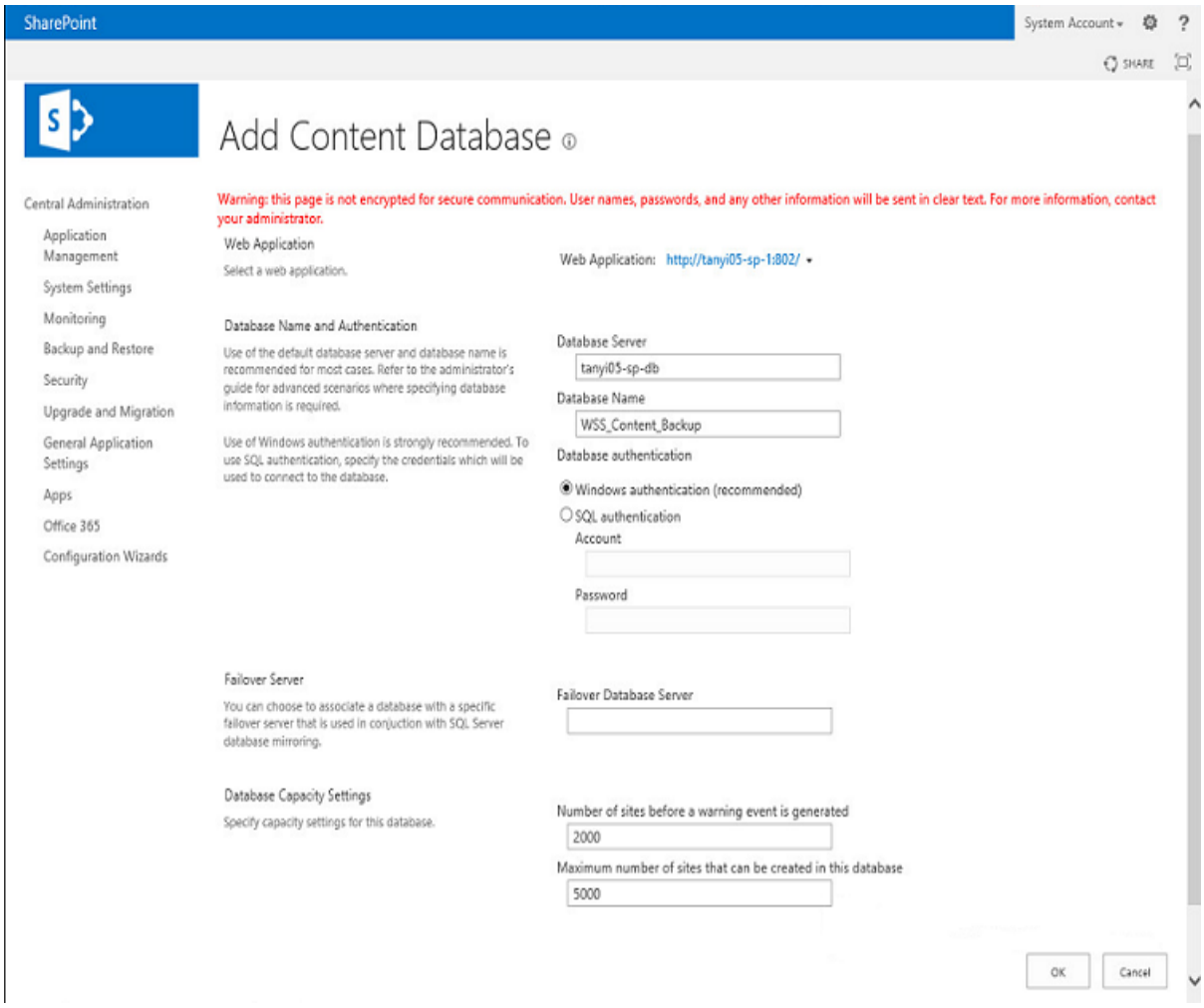
1. Abra a Administração Central do SharePoint e selecione Gerenciamento de aplicativos.



2. Selecione os bancos de dados de conteúdo do gerenciamento.



3. Selecione o aplicativo web e clique em Adicionar um banco de dados de conteúdo.
4. Digite o servidor de banco de dados e o nome do banco de dados, (por exemplo, WSS_Content_Backup) e, em seguida, clique em OK.



Agora, o banco de dados de conteúdo está associado a seu aplicativo web original.

O banco de dados não pode ser montado ao restaurar o banco de dados do Microsoft Exchange

Sintoma

Quando um banco de dados do Microsoft Exchange é restaurado, o banco de dados não pode ser montado. Os logs necessários estão ausentes, ou os logs de transações não estão contíguos. Há erros de eventos, como 454, 455 e 2006, no log de eventos.

Os dois seguintes motivos podem provocar a falha na montagem do banco de dados:

Motivo 1: a opção de limpeza do log do Exchange está ativada nas configurações do UDP e essa configuração exclui os logs de transação depois de cada backup. Em seguida, o usuário tenta restaurar a sessão anterior depois de vários backups em que a operação de limpeza ocorre.

Motivo 2: os usuários excluíram os logs de transação manualmente ou os logs são excluídos por outros programas, como um software antivírus.

Solução

Solução 1: se você ativou a opção de limpeza do log do Exchange e os logs de transação não forem contíguos, restaure todas as sessões uma de cada vez, começando com a sessão mais recente até a sessão com falha na restauração. Se houver falha na restauração da sessão mais recente, tente a Solução 2.

Solução 2: se a Solução 1 não funcionar, use a Solução 2. Essa solução resolve os dois problemas.

Por exemplo, você deseja restaurar o banco de dados Test da sessão 1. As etapas a seguir usam o nome do banco de dados como Test.

1. Efetue logon no servidor do Exchange no qual o banco de dados está localizado.
2. Exclua todos os arquivos (como *.edb, *.log, *.jrs, *.chk) da pasta do banco de dados.
3. Monte o banco de dados para criar um banco de dados vazio.

   Mount-Database -Identity Test
4. Restaure a mesma sessão novamente no local original.

   Se a restauração for bem-sucedida, você não precisará executar as etapas a seguir. Se houver falha na restauração, continue com as etapas a seguir.
5. Monte o banco de dados novamente.

   Mount-Database -Identity Test

6. Crie um novo banco de dados.

   new-mailboxdatabase –name OtherDatabase

7. Mova a caixa de correio para qualquer outro banco de dados.

   get-mailbox –datatbase Test –resultsize unlimited | new-moverequest –targetdatabase OtherDatabse

8. Remova o banco de dados de caixa de correio do computador de destino.

   remove-mailboxdatabase –identity Test

9. Crie um banco de dados de caixa de correio com o mesmo nome.

   new-mailboxdatabase –name Test

10. Restaure a mesma sessão novamente no local original.

    O banco de dados é montado com êxito.

O campo De não é exibido corretamente para emails enviados por usuários que têm permissões "em nome de" para uma caixa de correio compartilhada

Sintoma

Quando restauro emails do Exchange, se o email é enviado por um usuário que tenha o privilégio "em nome de" para uma caixa de correio compartilhado, depois da restauração, as informações do campo De não são exibidas corretamente. O campo De exibe apenas o nome do <host remetente>.

Solução

Siga estas etapas para corrigir o problema:

1. Execute uma das seguintes ações:

   Para backup sem agente

   - No servidor proxy do HBBU, crie um arquivo grtcfg.ini na pasta Configuration:

     [product_installed_path]\ Engine\Configuration

   Para o backup com base em agente

   - Na máquina do agente, crie um arquivo grtcfg.ini na pasta Configurarion:

     [product_installed_path]\ Engine\Configuration

2. Adicione o seguinte conteúdo ao arquivo grtcfg.ini:

   [common]

   0xFF07_enable=1

3. Envie a tarefa de restauração novamente.

Falha nas tarefas de restauração após backups leves de integração

Sintoma

Quando você envia backups leves de integração do gerenciador do Arcserve Backup para fazer backup do nó do Exchange Online a partir do RPS, o nó já passou por backup com a sessão de cópia em fita. As tarefas apresentam falha quando a fonte de dados inclui sessões do Arcserve D2D que já foram armazenadas em backup pelo Arcserve Backup. A mensagem de erro AW0813 aparece no log de atividades.

Solução

O comportamento de design do Arcserve Backup é o responsável por isso. Você precisa modificar esse comportamento para permitir que o Arcserve Backup faça backup das sessões do Arcserve D2D que já foram armazenadas em backup.

Siga estas etapas:

1. No servidor (nó) do Arcserve D2D que você está armazenando em backup, abra o Editor do Registro do Windows.
2. Abra a chave:

   HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\CA ARCserve Backup\ClientAgent\Parameters\AllowRedundantD2DBackups
3. Altere o valor DWORD de AllowRedundantD2DBackups para 1.

   Observação: se a chave de registro descrita acima não estiver presente no nó que você está fazendo backup, é necessário criar a chave.
4. Feche o Editor de registro do Windows.

   Para obter mais detalhes, consulte o artigo da base de conhecimento.

A restauração em uma pasta NFS compartilhada altera o nome de arquivo para um nome ilegível

Sintoma:

Ao executar a restauração em uma pasta NFS compartilhada, os arquivos e as pastas são restaurados com um nome ilegível.

Solução:

O UDP não oferece suporte à restauração de arquivos e pastas em uma pasta NFS compartilhada. É recomendável exportar uma pasta SMB (Server Message Block -

Bloco de Mensagem de Servidor) compartilhada e depois restaurar na mesma pasta.

Observação: se o nome de arquivo/pasta for convertido para um nome ilegível durante a sessão de backup NFS, mesmo após a restauração, o nome de arquivo/pasta permanecerá o mesmo.

Gateway, RPS, repositório de dados, console e bancos de dados relacionados

Esta seção inclui os seguintes tópicos de solução de problemas relacionados ao servidor de ponto de recuperação (RPS), repositório de dados e banco de dados:

- O nome do repositório de dados já está em uso
- Não é possível se conectar ao repositório de dados devido a problema de DNS
- O repositório de dados altera para o modo somente de restauração
- Erro quando a versão do RPS é inferior à versão do Console
- Não há suporte para adicionar o mesmo recurso em sites diferentes
- Como ativar os truncamentos de log quando o banco de dados SQL está no modo de recuperação completa
- Procurar pontos de recuperação não mostra os pontos de recuperação disponíveis quando RPS é configurado com FQDN
- Acesso negado ao se adicionar o RPS
- Não é possível alterar a exibição do UDP para o ponto de recuperação
- Acesso negado ao adicionar ou atualizar nós
- O console do UDP não abre quando a senha de administrador do SQL é alterada
- Falha ao montar os pontos de recuperação pois o tempo limite se esgotou
- Como atualizar as credenciais do servidor de gateway
- Como atualizar o gateway quando as credenciais do proxy do gateway são alteradas
- O console exibe a mensagem Serviço de identidade está iniciando

O nome do repositório de dados já está em uso

Sintoma:

Quando crio um repositório de dados, às vezes, a seguinte mensagem é exibida, apesar de eu especificar um novo nome do repositório de dados:

Este nome já está sendo usado por outro repositório de dados no servidor. Especifique outro nome de repositório de dados.

Solução:

Isso acontece quando tiver um repositório de dados, mas por algum motivo, o UUID no repositório de dados do registro está corrompido. É possível excluir o repositório de dados a partir da interface do usuário, mas o nome continua no Registro do servidor do ponto de recuperação.

Para resolver o problema, especifique um novo nome.

Não é possível se conectar ao repositório de dados devido a problema de DNS

Sintoma:

Durante a BMR, não consigo me conectar à pasta compartilhada exposta ao RPS. Apesar do nome de usuário/senha corretos, não consigo procurar nó no RPS.

Solução:

Quando o UAC do Windows está ativado no servidor de RPS, mesmo uma conta que pertença ao grupo de administradores locais pode não conseguir acessar uma pasta compartilhada do repositório de dados, se a conta não receber acesso a esse compartilhamento de forma explícita.

Usando o administrador interno do RPS, conceda privilégio de leitura/gravação à conta usada na BMR para a pasta compartilhada exposta pelo repositório de dados especificado.

O repositório de dados altera para o modo somente de restauração

Sintoma

Observei que um repositório de dados alterou para o modo somente de restauração, e não permite que eu faça backup de nenhum dado.

Solução

Quando um disco que está sendo usado por um repositório de dados está sem espaço em disco, o repositório de dados alterna para o modo somente de restauração. Neste modo, é possível executar a restauração, mas não é possível fazer backup de dados para o repositório de dados. Além disso, quando a alocação de memória especificada estiver sendo utilizada completamente, aumente a memória de alocação ou altere o repositório de dados do modo de memória para o modo SSD. Mesmo em tais casos, o repositório de dados alterna para o modo somente de restauração.

Para resolver esse problema, transfira o repositório de dados para um disco maior importando o repositório de dados.

Primeiro copie as pastas nas quais o disco está cheio para um disco maior com mais espaço livre e, em seguida, importe o repositório de dados do console.

O recurso **Importar repositório de dados** permite adicionar um repositório de dados para o servidor do ponto de recuperação. É possível importar quaisquer repositórios de dados existentes para um servidor do ponto de recuperação. Os repositórios de dados que você excluiu anteriormente de um servidor do ponto de recuperação estão disponíveis para importar.

Siga estas etapas:

1. No Console, clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Destinos** e clique em **Servidores de ponto de recuperação**.

   A página **Destinos: Servidores de ponto de recuperação** é exibida.
3. Execute uma das seguintes ações:
   - Clique em um servidor do ponto de recuperação.
   - Selecione o servidor do ponto de recuperação e, no menu central, clique no menu suspenso **Ações**.
4. Clique **Importar repositório de dados**.

   A página **Importar um repositório de dados** é exibida.

5. Selecione as opções a seguir e clique em **Avançar**:
   - **Procure** selecionar a **Pasta de destino do backup** a partir da qual você deseja importar o repositório de dados.
   - Digite a **senha criptografada**.

   Observação: deixe em branco se o repositório de dados não for criptografado.

   Após a autenticação da **pasta de Destino do backup**, a página **Importar um repositório de dados** exibe os detalhes do repositório de dados.
6. Modifique os detalhes, se necessário, e clique em **Salvar**.

   Se copiou a pasta Destino de dados, Destino de índice e Destino de hash para o armazenamento de dados de redução de redundância, altere o caminho da pasta.

   Observação: Não é possível ativar ou desativar a opção de criptografia para um repositório de dados existente.

   O repositório de dados é adicionado ao servidor do ponto de recuperação e exibido na caixa de diálogo **Destinos: Servidores de ponto de recuperação**.

   Agora o repositório de dados está disponível para backups.

Erro quando a versão do RPS é inferior à versão do Console

Sintoma

Existe um plano com uma tarefa de backup ou uma tarefa de replicação, e o destino é o RPS (Recovery Point Server - Servidor de Ponto de Recuperação). O RPS é de uma versão mais antiga, e o Console é a versão mais recente. Quando eu crio, modifico, reimplemento, pauso ou retomo um plano, e há uma ou mais versões mais antigas do RPS, o seguinte erro é exibido:

A versão do servidor de ponto de recuperação de destino 'rps1' é menor do que a versão do console atual. Para continuar, é necessário atualizar e também atualizar o servidor de ponto de recuperação.

Solução

Esse erro ocorre quando você planeja usar uma versão mais antiga do RPS. Para resolver esse erro, atualize o RPS usado no plano. Se você atualizar o RPS manualmente (sem usar o Console), não se esqueça de atualizar o RPS do console.

Atualize o RPS na seguinte ordem de preferência:

Replicar para um RPS gerenciado remotamente (RPS3) > Tarefa de replicação (RPS2) > Tarefa de backup (RPS1)

Primeiro, atualize o RPS3, depois atualize o RPS2. Finalmente, atualize o RPS1.

Siga estas etapas para fazer a atualização:

1. na guia **recursos**, vá para os Destinos: página dos Servidores de ponto de recuperação.
2. Selecione o servidor do ponto de recuperação.
3. Clique com o botão direito do mouse em **Instalar/atualizar o servidor de ponto de recuperação**.
4. Clique em **OK**.

Siga estas etapas para fazer a atualização:

1. Da guia **Recursos**, vá para Destinos no painel esquerdo e clique em Servidores de ponto de recuperação.
2. Selecione o servidor do ponto de recuperação.
3. Clique com o botão direito do mouse e selecione **Atualizar**.
4. Clique em **OK**.

Não há suporte para adicionar o mesmo recurso em sites diferentes

Sintoma

Ao adicionar um repositório de dados ao site remoto, recebo a seguinte mensagem de erro:

Não é possível enviar a tarefa para uma VM do Hyper-V ou uma VM do ESX

Solução

O erro ocorre porque o mesmo recurso (nó, servidor RPS, servidor ASBU, servidor Hyper-V, servidor ESX, servidor proxy) já está presente no outro local. Para resolver esse erro, exclua o recurso de todos os sites, em seguida, adicione o recurso somente em um site.

Como ativar os truncamentos de log quando o banco de dados SQL está no modo de recuperação completa

Sintoma

Quando o banco de dados está no modo Completo e um backup completo do banco de dados é executado, o log de truncamento do SQL não pode ser truncado.

Solução

Para resolver esse problema, adicione dois valores de registro para fazer com que o Arcserve UDP execute o comando BACKUP LOG para fazer backup do log de transações. Esse comando marcará espaço, que já foi gravado no arquivo de banco de dados, como reutilizável.

Siga estas etapas para adicionar o valor do registro:

1. Abra o editor de tabela do registro na máquina do agente usando o seguinte comando:

   ```
   regedit
   ```

2. Navegue até as chaves a seguir, de acordo com o backup com base em agente ou sem agente:

   No backup com base em agente para sistema operacional de 32 bits e 64 bits, navegue até a seguinte chave na máquina do agente:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   Ao usar uma versão anterior à Arcserve UDP v6.5, Atualização 2, para o backup sem agente, navegue até a chave a seguir. Crie o valor de tabela de registro na VM da qual você deseja fazer backup no servidor proxy. Se a chave de tabela do Registro não estiver disponível, crie o caminho completo da chave.

   - **Sistema operacional de 32 bits:**

     HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

   - **Sistema operacional de 64 bits:**

     HKEY_LOCAL_MACHINE\SOFTWARE\WoW6432Node\Arcserve\Unified Data Protection\Engine\AFBackupDll

3. Crie os dois valores de registro seguintes e, para ambos, defina o valor como 1:

   - valor dword chamado BackupSQLLog4Purge
   - valor dword chamado ForceShrinkSQLLog

O valor do registro é adicionado.

A solução entrará em vigor quando ocorrer a próxima tarefa de limpeza.

Procurar pontos de recuperação não mostra os pontos de recuperação disponíveis quando RPS é configurado com FQDN

Válido em sistemas operacionais Windows

Sintoma

Quando o RPS não está em um domínio em que você configurou o FQDN (adicionando o sufixo DNS) no Console do UDP, Procurar pontos de recuperação não mostra resultado exato. Embora você tenha feito backup de algumas sessões do RPS, o número de ponto de recuperação é exibido como zero.

O motivo é que, quando o RPS não está em um domínio, não é possível ao RPS identificar a si mesmo usando o FQDN.

Solução

Para resolver esse problema, adicione o sufixo DNS ao host do RPS.

Siga estas etapas:

1. Abra o painel de controle e vá para **Segurança e sistema Sistemas**.
2. Clique em **Alterar configurações** para configurações de nome do computador, domínio e grupo de trabalho.

   A caixa de diálogo Propriedades do sistema é aberta.
3. Na guia **Nome do computador**, clique em **Alterações**.

   A caixa de diálogo **Alterações no domínio/nome do computador** é aberta.
4. Clique em **Mais**.

   A caixa de diálogo **Sufixo DNS e nome do computador NetBIOS** é aberta.
5. No campo Sufixo DNS primário deste computador, adicione o sufixo DNS da rede e clique em **OK**.

   Por exemplo, adicione ABC.com.
6. Reinicie o sistema.

Acesso negado ao se adicionar o RPS

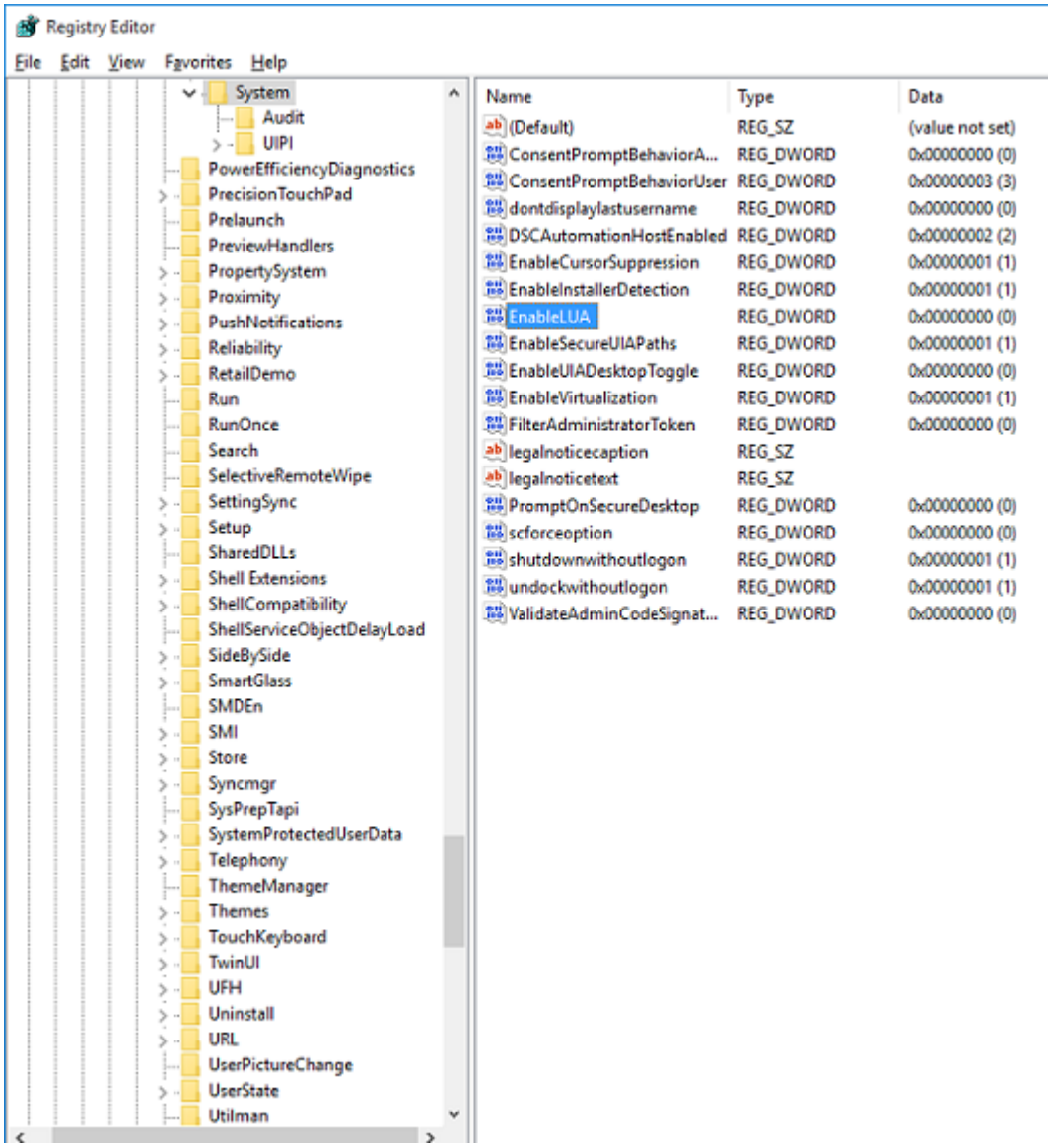
Sintoma:

se você adicionar o Windows 10 como RPS, e mesmo quando o UAC não estiver em execução, uma mensagem de erro será exibida:

Acesso negado. A conta pode não ter privilégios de administrador ou a conta é uma conta de administrador não interno, e o UAC está ativado.

Solução:

para o Windows 10, para desativar o UAC, altere o valor da chave do registro, não apenas alterando o nível para "Nunca notificar" no painel de controle, mas também de acordo com o diagrama de registro fornecido abaixo.



Defina o registro "EnableLUA" como 0 para desativar o UAC completamente e reinicie o computador.

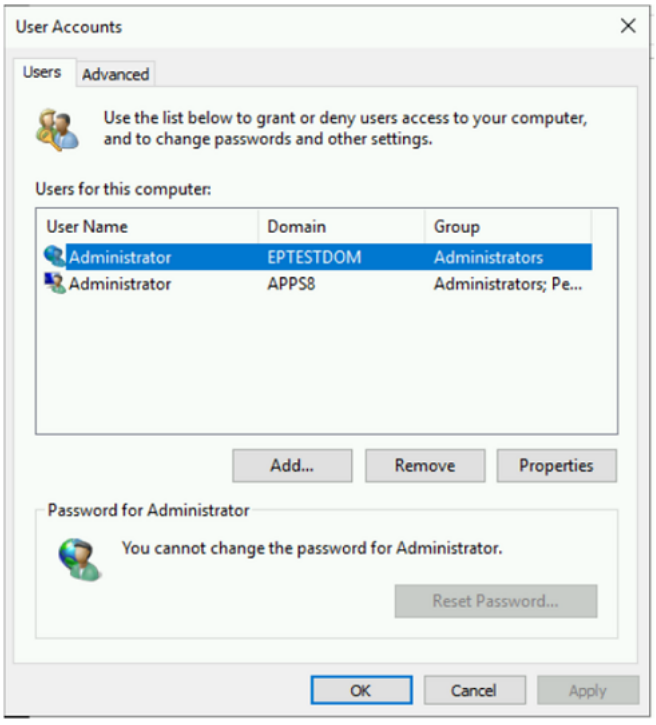
Em seguida, adicione o Windows 10 como RPS no Console.

Atribuindo privilégios e funções de administrador a um usuário de domínio

Esta seção fornece informações sobre como atribuir privilégios e funções de administrador a um usuário de domínio.

Siga estas etapas:

1. Para configurar o computador do console do UDP para o domínio, use as credenciais de logon do administrador.
2. Certifique-se de que o usuário de domínio faça parte do grupo de administradores. Para adicionar um usuário ao grupo de administradores, na janela Contas do usuário, clique no botão **Adicionar**.



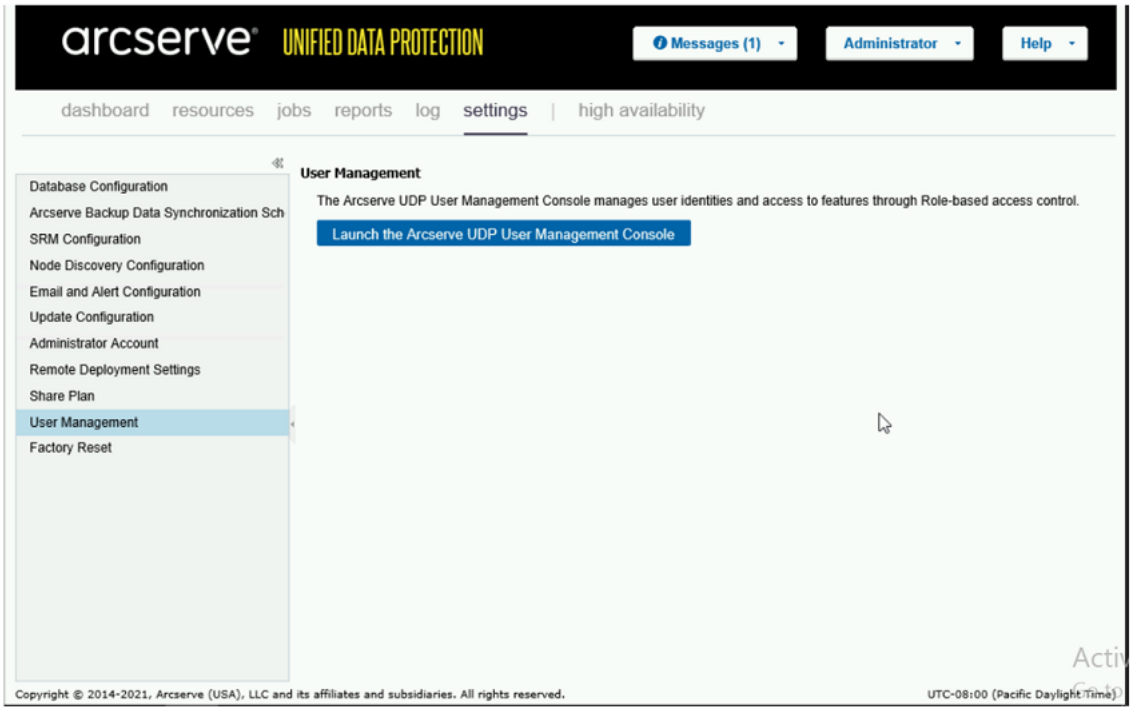
3. Depois de adicionar o usuário ao grupo de administradores, reinicie o serviço de gerenciamento.
4. Para adicionar a função de administrador a um usuário de domínio usando o console de gerenciamento de usuários do Arcserve UDP, faça o seguinte:

a. Efetue logon no console do Arcserve UDP usando as credenciais de administrador.

b. Clique na guia **Configuração**.

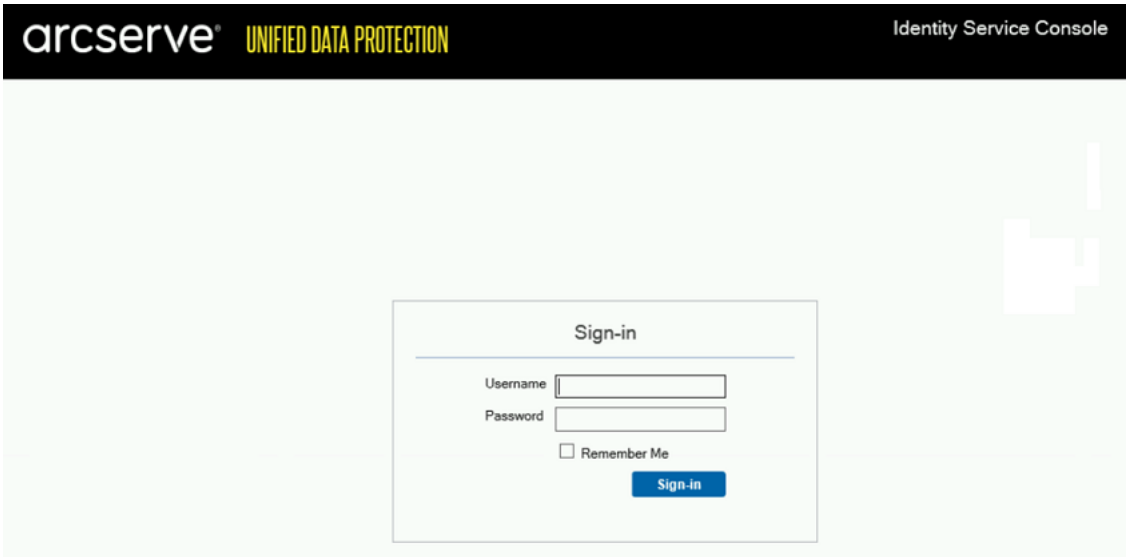
c. No painel esquerdo, clique em **Gerenciamento de usuários**.

   A página Gerenciamento de usuários é aberta.



d. Clique no botão **Abrir o console de gerenciamento de usuários do Arcserve UDP**.

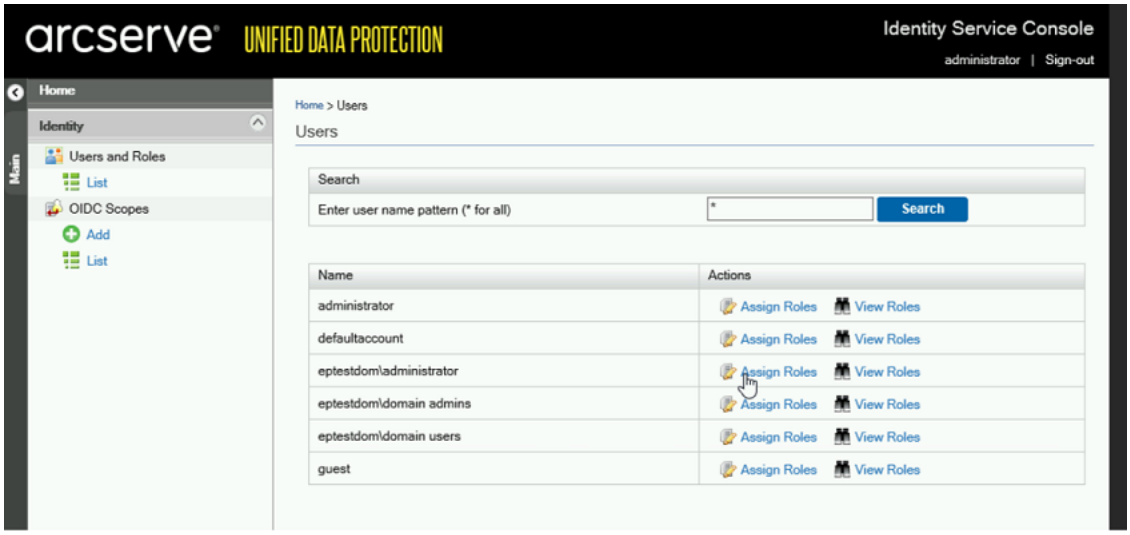
   O Console de serviço de identidade é exibido em uma nova janela.



e. Forneça as credenciais de administrador, como nome de usuário e senha, e clique em **Conectar**.

   A página inicial do Console de serviço de identidade é aberta.

f. Navegue até a página **Usuários** e, em seguida, em uma lista de usuários, selecione um usuário e clique em **Atribuir funções** para aplicar permissões de administrador.



g. Efetue logon no console do UDP usando credenciais de domínio.

Não é possível alterar a exibição do UDP para o ponto de recuperação

Sintoma:

Ao alterar o modo de exibição para exibição do UDP para o ponto de recuperação do RPS, às vezes você recebe mensagens de erro, como acesso negado.

Solução:

Desative o UAC para corrigir o problema. Para obter mais informações, consulte Como desativar um UAC remoto para um administrador não integrado.

Acesso negado ao adicionar ou atualizar nós

Válido em sistemas operacionais Windows

Sintoma

Às vezes, quando você adiciona ou atualiza os nós, obtém o seguinte erro:

Acesso negado. A conta pode não ter privilégios de administrador ou a conta é uma conta de administrador não integrado e UAC está ativado.

Solução

O erro ocorre nos seguintes cenários:

- Você se conectou como um usuário local ou usuário de domínio que não está no grupo de administradores locais do nó para adicionar ou atualizar o nó.
- Você se conectou como um usuário que está nos grupos de administrador local do nó, mas tem uma conta de administrador não integrado do nó para adicionar ou atualizar o nó.

Para resolver esse problema, siga estas etapas:

1. Adicione o usuário local ou de domínio aos grupos de administrador local desse nó.
2. Desative o UAC desse nó.

   Siga estas etapas para desativar o UAC:

   a. Clique em Iniciar, digite regedit no campo Pesquisar programas e arquivos e pressione Enter.

   b. O Editor do registro do Windows é exibido.

      Observação: talvez você precise fornecer credenciais administrativas para abrir o Editor do registro do Windows.

   c. Localize e clique na chave de registro a seguir:

      HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

   d. No menu Editar, clique em Novo e, em seguida, clique em Valor DWORD (32 bits).

   e. Especifique LocalAccountTokenFilterPolicy como o nome da nova entrada e pressione Enter.

   f. Clique com o botão direito do mouse em LocalAccountTokenFilterPolicy e, em seguida, clique em Modificar.

g. Especifique 1 no campo Dados do valor e clique em OK.

h. Feche o Editor do Registro.

Observações:

- Esse procedimento não é semelhante à desativação do UAC. Com esse procedimento, você pode desativar algumas das funcionalidades do UAC.
- Considerando que a tecnologia WMI (Windows Management Instrumentation - Instrumentação de Gerenciamento do Windows) é usada para importação, verifique se a WMI não está bloqueada pelo firewall.

Para obter mais informações sobre o comportamento do Windows, consulte a documentação da Microsoft.

O Console do UDP não abre quando a senha de administrador do SQL é alterada

Sintoma:

O Console do Arcserve UDP usa o SQL Server como banco de dados e usa o administrador do SQL "sa" para se conectar ao banco de dados. Se a senha "sa" for alterada, a página inicial do Console falha ao abrir e a mensagem a seguir é exibida:

SQL Server não está disponível agora. Verifique o status do serviço e, em seguida, reinicie o serviço de gerenciamento do Arcserve UDP.

Solução:

1. Executar <homedir>\Management\BIN\DBAccountUpdate.bat
2. Tipo: updatePassword
3. Digite a nova senha e pressione Enter

Falha ao montar os pontos de recuperação pois o tempo limite se esgotou

Sintoma

Quando o RPS tem uma carga intensa, o sistema operacional leva mais tempo para conectar o volume montado e os pontos de recuperação de montagem falham. Recebo a seguinte mensagem no log de atividades:

A montagem de volume leva mais tempo que o esperado (dois minutos), isso pode acontecer quando o servidor está sob carga pesada. Tente novamente quando a carga do servidor estiver menos pesada ou verifique a solução de problema na documentação online para aumentar o valor do tempo limite.

Solução

Para resolver esse problema, aumente o valor do tempo limite.

Siga estas etapas:

1. Efetue logon no RPS e vá para o seguinte local:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFStorHBAMgmt
   ```

   ```
   "WaitDeviceReadyTimeoutS"=dword:00000078
   ```

   Padrão: 120 segundos

2. Aumente o valor de tempo limite.

   Por exemplo, altere o valor de tempo limite para 600 segundos (10 minutos)

Como atualizar as credenciais do servidor de gateway

Sintoma

Se o nome de usuário de instalação do gateway for alterado ou a senha estiver expirada, você obtém o seguinte erro durante a implantação do plano:

A Implantação de agente falhou.

Falha ao personificar o usuário que instalou o Gateway de gerenciamento remoto do Arcserve usando as credenciais armazenadas. Verifique se as credenciais são válidas ainda e reimplante.

Solução

Para resolver esse problema, atualize o nome de usuário ou a senha da conta do gateway.

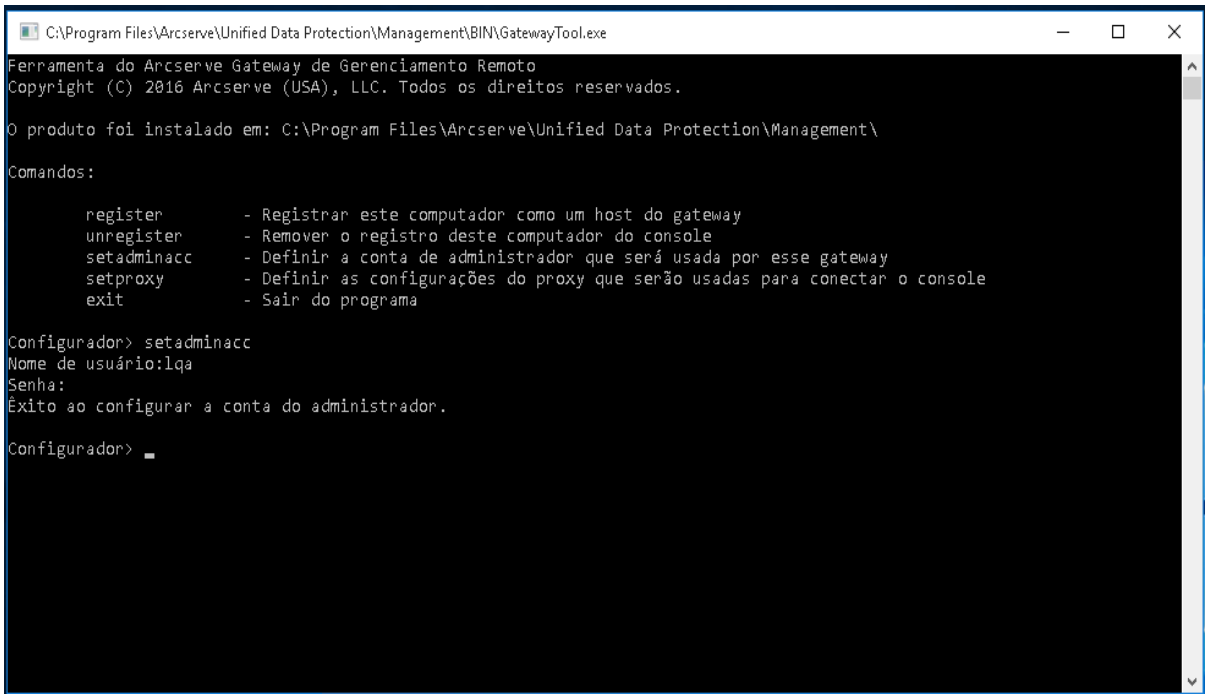
Siga estas etapas:

1. Efetue logon no servidor de gateway.
2. Vá até a pasta BIN na pasta de instalação do Arcserve UDP.

   Por exemplo, C:\Arquivos de programas\Arcserve\Unified Data Protection\Management\BIN\GatewayTool.exe
3. Clique com o botão direito em GatewayTool.exe e clique em Executar como administrador.
4. Na janela do prompt de comando, digite **setadminacc**.
5. Especifique o novo nome de usuário.
6. Especifique a nova senha.

   Se todos os detalhes estiverem corretos, você verá a seguinte mensagem:

   ```
   A configuração de contas de administrador foi bem-sucedida
   ```



7. Reimplante o plano.

Como atualizar o gateway quando as credenciais do proxy do gateway são alteradas

Sintoma

Quando as credenciais do servidor proxy são alteradas, a conexão com o gateway é interrompida. Você obtém a seguinte mensagem de erro ao tentar se conectar ao gateway:

Não é possível conectar-se ao proxy do site do gateway. Verifique o status do site e certifique-se de que o gateway esteja em execução.

Solução

Para resolver esse problema, atualize os parâmetros em GatewayTool.exe set-proxy.

Siga estas etapas para atualizar o servidor de gateway:

1. Efetue logon no servidor de gateway.
2. Vá até a pasta BIN na pasta de instalação do Arcserve UDP.

   Por exemplo, C:\Arquivos de programas\Arcserve\Unified Data Protection\Management\BIN\GatewayTool.exe
3. Clique com o botão direito em GatewayTool.exe e clique em Executar como administrador.
4. Na janela do prompt de comando, digite **setproxy**.
5. Digite **2**para selecionar Proxy personalizado porque o proxy do IE não oferece suporte à credenciais no momento.
6. Especifique o endereço IP do servidor proxy.
7. Especifique a porta do servidor proxy.
8. Digite **Y** para autenticação.

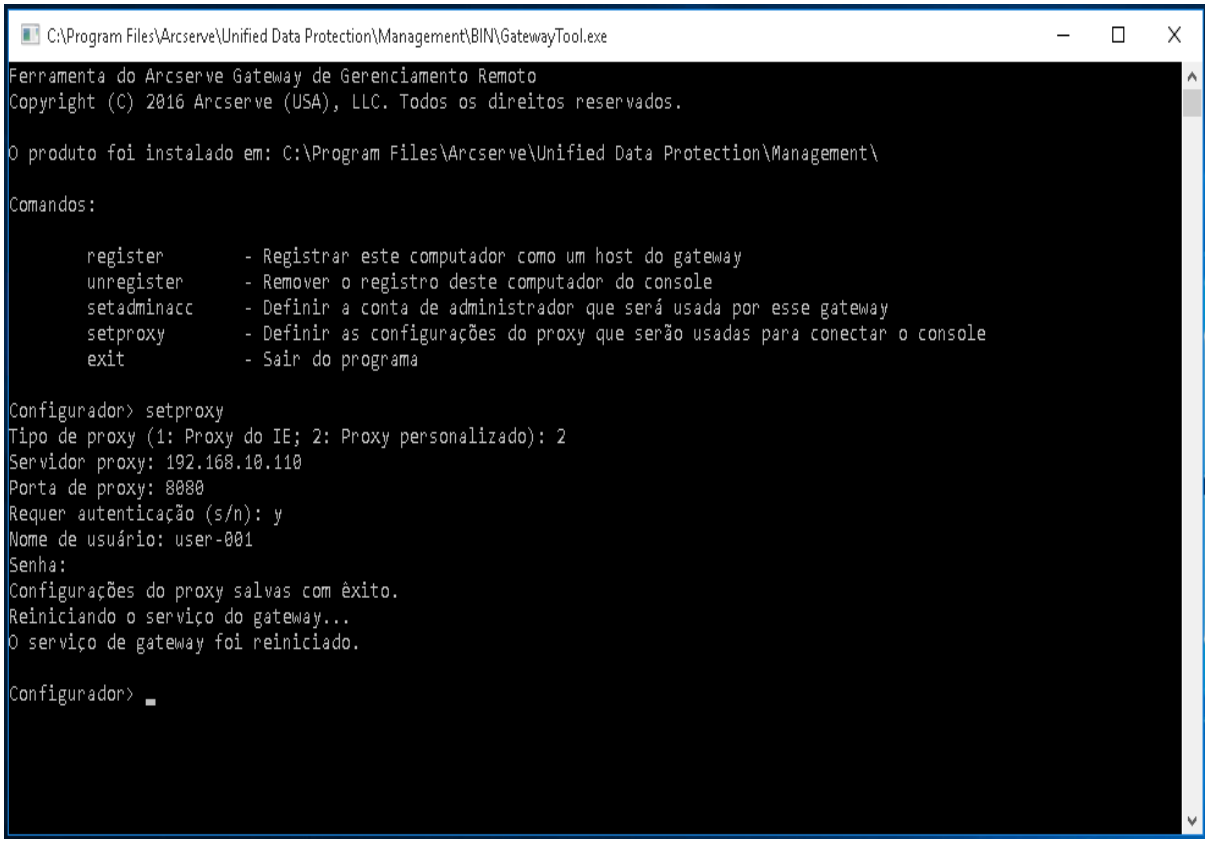
   Observação: se você digitar N, isso desativará as credenciais.
9. Especifique o novo nome de usuário.
10. Especifique a nova senha nova.

    Se todos os detalhes estiverem corretos, você verá a seguinte mensagem:

    ```
    Configurações de proxy foram salvas com êxito. Reiniciando o serviço de gateway.
    ```

Observação: se as credenciais do proxy de gateway estiverem ativadas em um plano, atualize o nome de usuário do proxy e a senha nesse plano.

Da mesma forma, você pode alterar outras configurações, como tipo de Proxy, endereço IP e número da porta no **setproxy**.



Caso encontre a mensagem **Falha ao reiniciar o serviço de gateway, reinicie-o manualmente** na janela do prompt de comando, siga estas etapas:

a. execute **Services. msc** para procurar **serviço de gateway de gerenciamento remoto do Arcserve** e, em seguida, reinicie o serviço de gateway de gerenciamento remoto.

b. Se o serviço remoto parar após a reinicialização, use o Gerenciador de tarefas para finalizar a tarefa **tomcat8.exe** manualmente.

c. Atualize **Services. msc** e reinicie o **Serviço de gateway de gerenciamento remoto do Arcserve**.

O console exibe a mensagem Serviço de identidade está iniciando

Sintoma

Não é possível efetuar logon no Console do Arcserve UDP. O console exibe as seguintes mensagens, mesmo após cinco minutos do logon:

O Serviço de identidade está sendo iniciado

Solução

Para resolver esse problema, abra o console de serviço do Windows e reinicie o serviço do console do Arcserve UDP, **Serviço de Gerenciamento do Arcserve UDP**.

Relacionado à restauração e backup de máquina virtual

Esta seção inclui os seguintes tópicos de solução de problemas relacionados ao servidor de ponto de recuperação (RPS), repositório de dados e banco de dados:

- Adicionar permissões para VDDK no Nível do vCenter Server
- A tarefa de backup para o modelo de VM é sempre convertida em backup completo
- Discos independentes são ignorados pela tarefa de backup do modelo de VM
- A tarefa de backup para a VM no compartilhamento do SMB 3.0 falha com uma mensagem de erro
- A tarefa de recuperação da VM falha ao restaurar a VM para um compartilhamento de arquivos padrão do Windows
- Informações de volume não disponíveis para o ponto de recuperação
- Permissões para o backup sem agente com base em host e o modo de espera virtual no nível do vCenter Server
- Converter backup incremental em backup de verificação, pois o instantâneo da máquina virtual foi alterado desde a última tarefa de backup ou precisa de consolidação
- O backup sem agente para a VM da VMware falha para o dispositivo de CD/DVD da VM
- Falha do backup sem agente com base em host para do Hyper-V após a atualização do Arcserve UDP
- Falha no backup sem agente com base em host no VMware ESXi 6.0
- Falha ao criar um instantâneo para máquinas virtuais do Hyper-V quando várias tarefas estão sendo executadas
- Falha ao fazer backup de um disco virtual. Erro do sistema=[O dispositivo não está pronto (21)]
- Falha na tarefa de backup
- Falha ao importar as VMs da VMware a partir do vCenter
- Não é possível aplicar as configurações de backup para o nó
- Os backups falham devido à licença ESXi

- O backup sem agente com base em host não usa o modo de transporte HotAdd
- O modo de transporte HotAdd não funciona durante a tentativa de fazer backup de uma VM da VMware
- A tarefa de backup sem agente com base em host ou restauração usa o modo de transporte NBD ou NBDSSL mesmo quando o modo SAN é possível
- Controle mais granular de VSS em encerramentos do sistema operacional convidado Windows
- As operações de recuperação falham durante a recuperação de dados usando o modo de transporte HOTADD ou SAN
- Falha na operação de recuperação da VM quando uma porta não padrão é especificada
- A tarefa de backup completo ou incremental programada falha para a VM do Hyper-V
- Falha no gravador de VSS NTDS do Hyper-V ao criar o instantâneo de VSS na VM
- As alterações do endereço MAC não são retidas após a recuperação da VM
- Falha do Hyper-V ao criar um instantâneo VSS
- Não é possível abrir arquivos VMDK
- Problemas causados por UUID da VM duplicado
- Falha na tarefa de catálogo do sistema de arquivos ou falha de verificação do ponto de recuperação para backup sem agente com base em host
- O backup incremental converte para backup de verificação ou o tamanho do backup aumenta no Hyper-V
- Falha no backup sem agente com base em host da VM do Hyper-V que tem uma configuração de disco diferente e especial
- A tarefa de backup falha para uma máquina virtual VMware
- Desativar fazer nova verificação de adaptadores de barramento de host quando a origem e o Proxy estão em diferentes servidores VMware ESX
- Desativar a criação de instantâneo consecutivo na VM do VMware para um backup
- O backup sem agente com base em host trava ao usar o Windows 2003 R2 de 64 bits como proxy de backup

- Quando restaurada de uma versão superior do host ESXi para uma versão anterior do host ESXi, a VM trava na fase de inicialização
- A utilização de RAM atinge 99% quando as tarefas de backup são enviadas para a VM
- Falha na tarefa de restauração do Hyper-V, não é possível se conectar ao utilitário no Host
- A proteção automática falha ao detectar e proteger a VM
- Definir o tamanho do bloco de leitura ao fazer backup do arquivo VMDK

Adicionar permissões para VDDK no Nível do vCenter Server

Se você não tiver as permissões apropriadas, a tarefa de backup para máquinas virtuais com base em host e o modo de espera virtual falhará.

Para evitar esse problema, verifique se possui as permissões apropriadas. Se você for um usuário vCenter, não precisará da permissão de Administrador no nível do vCenter Server, mas deverá ter a permissão de Administrador no nível do Datacenter. Além disso, você deve ter as seguintes permissões no nível do vCenter Server:

- Global, DisableMethods and EnableMethods
- Global, License

Para obter mais informações, consulte o artigo da base de conhecimento da VMware.

Para obter informações sobre a permissão, consulte Permissões para o backup sem agente com base em host e o modo de espera virtual no nível do vCenter Server.

Permissões para o backup sem agente com base em host e o modo de espera virtual no nível do vCenter Server

Ao configurar o vCenter para gerenciar máquinas virtuais, em geral, você configura usuários ou grupos com privilégios de administrador do vCenter. Essa abordagem ajuda a garantir que as contas do vCenter tenham acesso irrestrito à funcionalidade e às tarefas do vCenter. Opcionalmente, é possível criar usuários e grupos do vCenter que podem ser usados para facilitar apenas as operações de backup ou apenas as operações de backup e restauração.

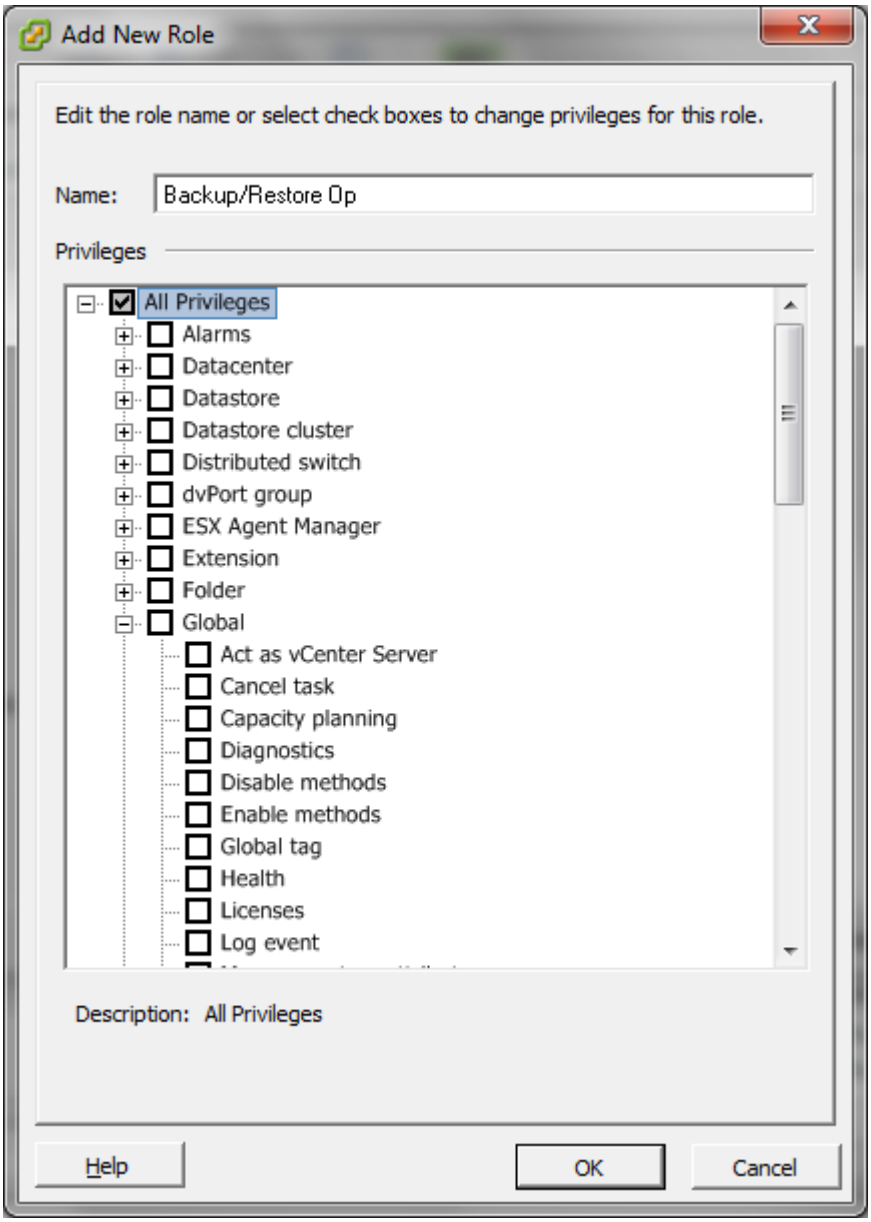
Ao usar contas não administrativas do vCenter para facilitar operações de backup e restauração, você cria funções do vCenter, atribuiu privilégios às funções e, em seguida, aplica a função aos usuários ou grupos individuais.

Observação: como prática recomendada, a VMware recomenda que você permita que as contas de usuário não administrativas do vCenter sejam integrantes do grupo de administradores locais do Windows.

Importante: As etapas abaixo pressupõem que você esteja familiarizado com a configuração de usuários, grupos, funções e permissões do vCenter. Consulte a documentação do vCenter, conforme a necessidade.

Siga estas etapas:

1. Efetue logon no vCenter que está usando o cliente VI.
2. Abra a caixa de diálogo Adicionar novas funções e especifique um nome para a função.



3. Expanda Todos os privilégios.
4. **(Opcional)** Para permitir que a função **facilite apenas as operações de backup**, especifique os seguintes privilégios:

   Importante: para permitir que a função facilite operações de backup e de restauração, vá para a próxima etapa.

   - Expanda Máquina virtual e Configuração e especifique os seguintes privilégios:
     - Controle de alterações de disco
     - Concessão de disco
     - Adicionar disco existente

- Adicionar novo disco
- Adicionar ou remover dispositivo
- Alterar recurso
- Remover disco
- Configurações

- Expanda Máquina virtual e Provisionamento e especifique os seguintes privilégios:
  - Permitir acesso de somente leitura ao disco
  - Permitir download da máquina virtual
- Expanda Máquina virtual e especifique os seguintes privilégios:

  vSphere 4: expanda Estado e especifique Criar instantâneo e Remover instantâneo.

  vSphere 5: expanda Gerenciamento de instantâneos, expanda Estado e, em seguida, especifique Criar instantâneo e Remover instantâneo.
- Expanda Global e especifique os seguintes privilégios:
  - Desativar métodos
  - Ativar métodos
  - Licenças

  Vá para a Etapa 6.

5. Para permitir que a função **facilite as operações de backup e de restauração**, especifique os seguintes privilégios:
   - Expanda Repositório de dados e especifique os seguintes privilégios:
     - Alocar espaço
     - Procurar no repositório de dados
     - Operações de arquivo de baixo nível
   - Expanda Global e especifique os seguintes privilégios:
     - Desativar métodos
     - Ativar métodos
     - Licenças
   - Expanda Host, expanda Operações locais e, em seguida, especifique Reconfigurar máquina virtual.

Observação: esse privilégio é necessário somente quando você precisa executar operações de backup e restauração usando o modo de transporte HotAdd.

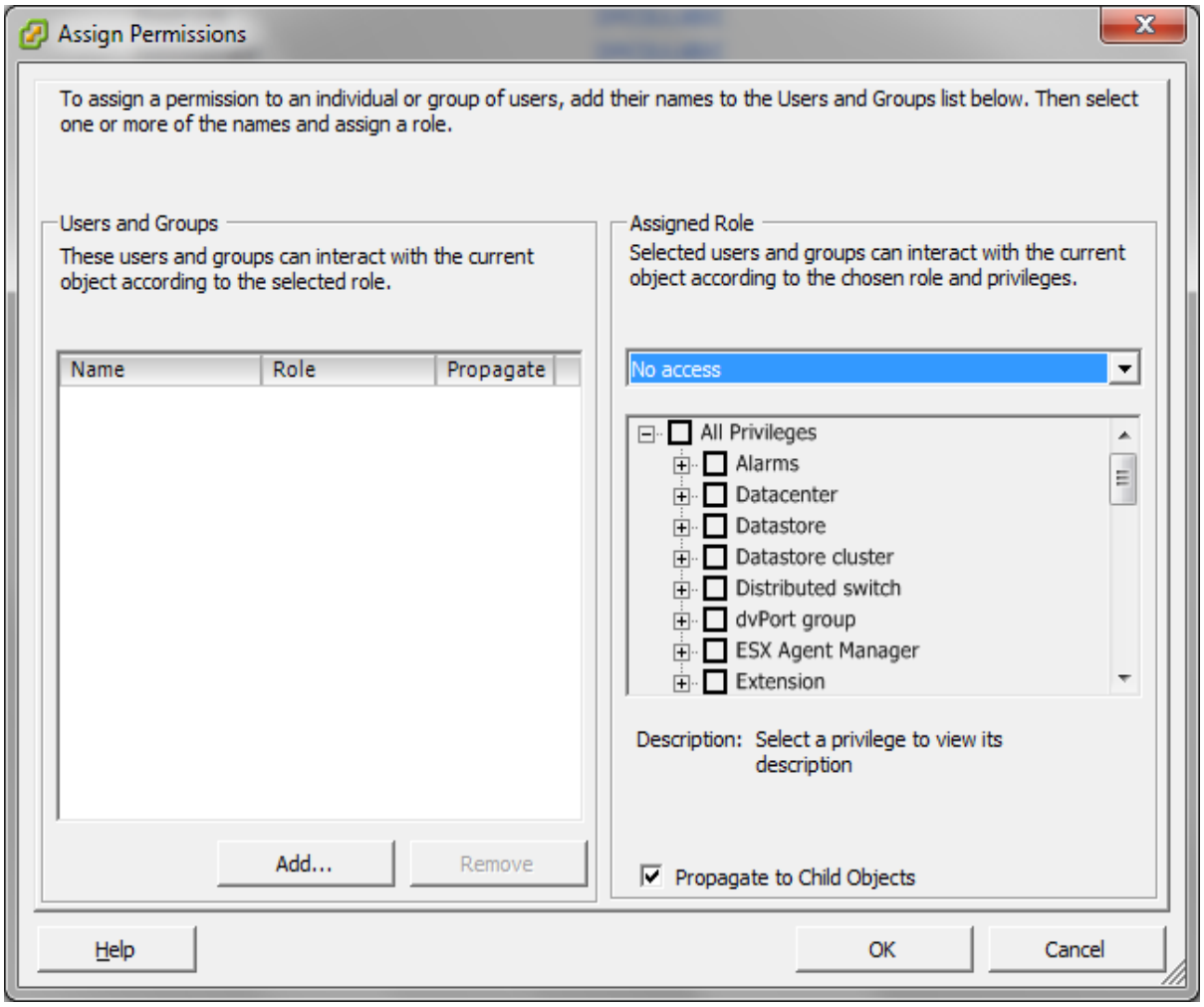
- Expanda Rede e especifique Atribuir rede.
- Expanda Recursos e clique em Atribuir máquina virtual a um pool de recursos.
- Expanda Máquina virtual e Configuração e especifique os seguintes privilégios:
  - Adicionar disco existente
  - Adicionar novo disco
  - Adicionar ou remover dispositivo
  - Avançado
  - Alterar contagem de CPU
  - Alterar recurso
  - Controle de alterações de disco
  - Concessão de disco
  - Dispositivo USB do host
  - Memória
  - Modificar configuração do dispositivo
  - Dispositivo bruto
  - Recarregar a partir do caminho
  - Remover disco
  - Renomear
  - Redefinir informações de convidado
  - Configurações
  - Posicionamento de arquivo de troca
  - Atualização de hardware virtual
- Expanda Máquina virtual e Operações de convidado e especifique os seguintes privilégios:
  - Modificações de operação de convidado
  - Execução do programa de operação de convidado
  - Consultas de operações de convidado (vSphere 5)

- Expanda Máquina virtual e Interação e especifique os seguintes privilégios:
  - Desligar
  - Ligar
- Expanda Máquina virtual e Inventário e especifique os seguintes privilégios:
  - Criar novo
  - Faça o registro
  - Remover
  - Remover o registro
- Expanda Máquina virtual e Provisionamento e especifique os seguintes privilégios:
  - Permitir acesso a disco
  - Permitir acesso de somente leitura ao disco
  - Permitir download da máquina virtual
- Expanda Máquina virtual e especifique os seguintes privilégios:

  vSphere 4: expanda Estado e especifique Criar instantâneo, Remover instantâneo e Reverter para instantâneo.

  vSphere 5: expanda Gerenciamento de instantâneos, expanda Estado e, em seguida, especifique Criar instantâneo, Remover instantâneo e Reverter para instantâneo.

6. Clique em OK para criar a função.
7. Abra a caixa de diálogo Atribuir permissões, para atribuir a função recém-criada a usuários, grupos ou ambos.



8. Na lista Usuários e grupos, selecione o usuário personalizado que você deseja usar para backups e restaurações.

   Na lista suspensa Função atribuída, especifique a função que você deseja aplicar aos usuários ou grupos.

9. Clique em OK para aplicar a função aos usuários ou grupos.

   As permissões estão agora definidas para funções do vCenter.

A tarefa de backup para o modelo de VM é sempre convertida em backup completo, e o tamanho dos dados de backup é o tamanho de provisionamento do disco virtual

Sintoma

Ao fazer backup de um modelo de VM, a tarefa de backup é convertida em backup completo e o tamanho dos dados processados é igual ao tamanho de provisionamento do disco virtual. A seguinte mensagem de aviso aparece no log de atividades:

Como a máquina virtual está configurada como modelo, a tarefa será um backup completo e o backup será feito dos discos virtuais inteiros.

Solução

Esse comportamento é esperado para o backup do modelo de VM. Uma solução alternativa é converter o modelo em VM no início do backup, fazer o backup e convertê-la de volta em modelo no final da tarefa de backup. Se você preferir essa solução alternativa, siga as etapas abaixo para definir um valor de registro na máquina proxy.

1. Faça logon na máquina proxy.
2. Crie um valor de registro no nível de servidor proxy ou VM.

   Observação: se você adicionar o valor de registro no nível de VM e no nível de proxy, a configuração no registro no nível de VM terá prioridade sobre a configuração no registro no nível de proxy.

   No nível do servidor proxy (aplicável a todas as tarefas de backup em execução no servidor proxy)

   a. Abra a chave do registro no seguinte local:

      [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

   b. Adicione um valor DWORD com o nome *TemplateDirectBackup* e especifique seu valor como 0.

   No nível da VM

   a. Abra a chave do registro no seguinte local:

      [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<vm instance uuid>]

b. Adicione um valor DWORD com o nome *TemplateDirectBackup* e especifique seu valor como 0.

Observação: após ativar essa opção, a VM não poderá ser convertida novamente em modelo se o backup for anulado de forma anormal (por exemplo, com travamentos durante a tarefa ou quando a máquina proxy é reinicializada).

Discos independentes são ignorados pela tarefa de backup do modelo de VM

Sintoma

Ao fazer backup de um modelo de VM, a tarefa de backup ignora discos independentes e a seguinte mensagem de aviso aparece no log de atividades:

Unable to backup virtual disk [datastore_720_4] shuli02-t235/shuli02-t235_1.vmdk because it is an independent disk.

Solução

Esse comportamento é esperado para o backup do modelo de VM. A causa-raiz é uma limitação da VMware que impede que o aplicativo de backup abra o VMDK de discos independentes. Uma solução alternativa é definir discos independentes para discos dependentes no início do backup, fazer backup deles e voltar à configuração inicial no fim da tarefa de backup. Se você preferir essa solução alternativa, siga as etapas abaixo para definir um valor de registro na máquina proxy.

1. Faça logon na máquina proxy.
2. Crie um valor de registro no nível de servidor proxy ou VM.

   Observação: se você adicionar o valor de registro no nível de VM e no nível de proxy, a configuração no registro no nível de VM terá prioridade sobre a configuração no registro no nível de proxy.

   No nível do servidor proxy (aplicável a todas as tarefas de backup em execução no servidor proxy)

   a. Abra a chave do registro no seguinte local:

      [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

   b. Adicione um valor DWORD com o nome *ConvertIndependentVMDK* e especifique seu valor como 1.

   No nível da VM

   a. Abra a chave do registro no seguinte local:

      [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<vm instance uuid>]

   b. Adicione um valor DWORD com o nome *ConvertIndependentVMDK* e especifique seu valor como 1.

Observações:

- Depois que você ativar essa opção, não será possível voltar à configuração inicial dos discos independentes se o backup for anulado de maneira anormal (por exemplo, se uma tarefa apresentar falha ou a máquina proxy for reinicializada).
- Essa opção não funciona quando a opção Converter modelo em VM durante o backup está ativada (o registro TemplateDirectBackup é criado com o valor 0).

A tarefa de backup para a VM no compartilhamento do SMB 3.0 falha com uma mensagem de erro

Observação: válida para o Hyper-V.

Sintoma

A VM reside no Hyper-V 2012 ou 2012 R2 e tem arquivos no compartilhamento do SMB 3.0. A tarefa de backup sempre falha com uma das seguintes mensagens de erro:

Falha ao capturar instantâneo de VSS. System error=[VSS_E_VOLUME_NOT_SUPPORTED_BY_PROVIDER]

Falha ao capturar instantâneo de VSS. Erro do sistema=[VSS_E_BAD_STATE]

Solução

1. Se o compartilhamento SMB for hospedado por um servidor de arquivos do Windows, adicione a função de Serviço de agente VSS de servidor de arquivos e certifique-se de que o Serviço de agente de cópia de sombra de servidor de arquivos da Microsoft esteja instalado.
2. Se o compartilhamento SMB for hospedado por appliances NAS de terceiros ou outras soluções semelhantes, verifique se esses appliances ou soluções oferecem suporte ao SMB 3.0 e a protocolos VSS remotos de servidor de arquivos. Para obter detalhes, entre em contato com o fornecedor terceiro.

Observação:

- Para a VM que reside no Hyper-V 2016, o Serviço de agente de cópia de sombra de servidor de arquivos não é necessário.
- É necessário configurar o compartilhamento do SMB 3.0 corretamente antes que o Arcserve UDP possa fazer backup da VM nele. Para encontrar requisitos detalhados do compartilhamento do SMB 3.0, consulte a seção de requisitos e configurações suportadas da documentação da Microsoft.

A tarefa de recuperação da VM falha ao restaurar a VM para um compartilhamento de arquivos padrão do Windows

Observação: válida para o Hyper-V.

Sintoma

Ao restaurar a VM especificando o compartilhamento de arquivos padrão do Windows (por exemplo, \\hostname\C$\abc) como o caminho de destino, a tarefa de restauração falha e a seguinte mensagem de erro aparece:

A tarefa de recuperação da VM não pôde criar a nova máquina virtual.

Solução

A falha da tarefa é esperada, pois arquivos da VM não podem ser armazenados no compartilhamento de arquivos padrão do sistema do Windows. Somente o compartilhamento de arquivos do Microsoft SMB 3.0 é suportado. Para obter detalhes, consulte a *documentação da Microsoft*.

Informações de volume não disponíveis para o ponto de recuperação

Sintoma

No assistente de restauração de arquivos/VM, durante a montagem ou a cópia do ponto de recuperação, não são exibidos volumes nem arquivos na tela do ponto de recuperação. Em vez disso, a seguinte mensagem é exibida:

Não há informações de volume para este ponto de recuperação.

Solução

Esse comportamento é esperado quando a VM de origem não possui o sistema operacional Windows. Dessa forma, o Arcservev UDP não consegue analisar os discos virtuais da VM para obter as informações do volume. É possível restaurar toda a VM ou copiar o ponto de recuperação. Se a VM de origem tiver o sistema operacional de VM Linux, também será possível restaurar arquivos do ponto de recuperação usando um servidor de backup Linux.

Converter backup incremental em backup de verificação, pois os instantâneos da máquina virtual foram alterados desde a última tarefa de backup ou precisam de consolidação

Observação: Válido em plataformas Windows.

Sintoma

Os backups incrementais para máquinas virtuais VMware são convertidos para backups de verificação. O log de atividade exibe a seguinte mensagem:

"Converter backup incremental em backup de verificação, pois os instantâneos da máquina virtual foram alterados desde a última tarefa de backup ou precisam de consolidação."

Solução

Use o cliente do VMware vSphere para consolidar os instantâneos da máquina virtual. Para obter mais detalhes sobre a consolidação de instantâneos, consulte o artigo da Base de dados de conhecimento do VMware.

Observação: a consolidação de instantâneos de uma máquina virtual pode falhar devido a arquivos bloqueados. Se a tarefa de backup usa o modo de transporte HOTADD, então, verifique se as configurações da máquina virtual do proxy de backup no servidor ESXi não contêm os discos rígidos adicionados. Em seguida, consolide os instantâneos da máquina virtual.

Backup sem agente para VM da VMware falha se o dispositivs de CD/DVD da VM estiver conectado a uma imagem ISO que reside em um repositório de dados do NFS desconectado

Sintoma

Execute as seguintes etapas para resolver o problema:

1. Prepare uma imagem de ISO em um repositório de dados do NFS conectado ao host do ESX.
2. Anexe a imagem de ISO ao dispositivo de CD/DVD de uma VM.
3. Desconecte o repositório de dados do NFS da rede.
4. Execute o backup sem agente da VM.

Nesse caso, a tarefa de backup falha com a mensagem de erro como "Não foi possível obter instantâneo da máquina virtual. O ESX Server/vCenter Server relatou o seguinte erro: Ocorreu um erro geral de sistema."

Solução

Devido à limitação do ESX, não é possível tirar um snapshot quando a VM desconecta a imagem ISO anexada. Como alternativa, desanexe a imagem ISO do dispositivo de CD/DVD da VM antes do backup.

Falha do backup sem agente com base em host para VM do Hyper-V após a atualização do Arcserve UDP

Válido para o Hyper-V

Sintoma

Após a atualização do Arcserve UDP da Versão 5.0, Atualização 2, ou anterior à versão mais recente, o backup sem agente com base em host foi iniciado com falha e apresentou a seguinte mensagem de erro:

A tarefa de backup está cancelada. Para um instantâneo do VSS, o gravador de VSS do Hyper-V precisa salvar a máquina virtual e isso não for aplicado no plano atual. Para reiniciar a tarefa de backup, altere a configuração de Método de instantâneo do Hyper-V no plano. Para obter detalhes sobre como definir o Método de instantâneo do Hyper-V em um plano, consulte a documentação do produto.

O backup sem agente com base em host estava funcionando antes da atualização.

Solução

No Arcserve UDP Versão 5.0, Atualização 2, ou anterior, quando o virtual não suporta o método de backup online, o comportamento padrão é adotar o método de backup offline. O método de backup offline salva a máquina virtual ao criar um instantâneo. No estado Salvo, a máquina virtual está inacessível. No entanto, as máquinas virtuais críticas precisam ficar acessíveis o tempo todo.

Na Versão 5.0, Atualização 3, e nas versões posteriores, se a máquina virtual precisar ser colocada no estado Salvo, o comportamento padrão será cancelar a tarefa de backup para evitar qualquer tempo de inatividade da máquina virtual. Se você não quiser que a tarefa de backup seja cancelada, altere a opção **Método de instantâneo do Hyper-V** no plano. Para obter mais detalhes sobre a opção Método de instantâneo do Hyper-V no plano, consulte Como criar um plano de backup da máquina virtual com base em host.

Você também pode consultar o artigo da base de conhecimento do Arcserve para obter mais detalhes sobre esse problema.

Falha no backup sem agente com base em host no VMware ESXi 6.0

Sintoma

Pode haver uma falha nos backups sem agente do Arcserve UD quando você tenta fazer backup de uma máquina virtual no VMware ESXi 6.0 e a função de CBT está ativada.

Esse é um problema conhecido da VMware. Quando há falha no backup, podem ocorrer os dois comportamentos a seguir:

- o Arcserve UDP não pode estabelecer conexão com a função de CBT do host do ESXi. Como resultado, o Arcserve UDP não pode receber as informações de bloco de dados usados ou alterados na máquina virtual.
- Pode haver uma falha no Arcserve UDP ao capturar instantâneos inativos da máquina virtual. (Isso pode ocorrer sempre que o Arcserve UDP captura um instantâneo ou quando você captura um instantâneo manualmente no cliente do vSphere).

Solução

A VMware solucionou esse problema em sua compilação mais recente, o ESXi 6.0 Compilação 2715440. É possível instalar o patch ESXi600-201505001 para resolver esse problema. Para obter mais informações sobre como fazer download e instalar o patch, consulte o artigo da Base de dados de conhecimento da VMware.

Se não for possível aplicar o patch, você poderá resolver o problema fazendo as seguintes alterações na chave do registro:

Solução para falha de conexão do CBT.

Se o Arcserve UDP não puder se conectar ao CBT, em vez de uma falha na tarefa de backup, o Arcserve UDP pode continuar a tarefa de backup. No entanto, em vez de executar um backup incremental, por padrão, o Arcserve UDP executará um backup completo do disco da VM. Se não desejar executar um backup completo automaticamente, você poderá adicionar uma chave do registro para alterar esse comportamento padrão. Se você adicionar a chave e definir o valor como 1, haverá falha na tarefa de backup do Arcserve UDP quando ocorrer um erro de CBT.

É possível adicionar essa chave do registro no servidor Proxy da seguinte maneira:

No nível do servidor proxy (aplicável a todas as tarefas de backup em execução no servidor proxy)

1. Abra a chave do registro no seguinte local:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

2. Insira a seguinte dword:

   "BackupEntireDiskOnCBTBitmapFailure"=dword:00000001

3. Salve a chave do registro.

No nível da VM

1. Abra a chave do registro no seguinte local:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<vm instance uuid>]

2. Insira a seguinte dword:

   "BackupEntireDiskOnCBTBitmapFailure"=dword:00000001

3. Salve a chave do registro.

Observação: se você adicionar ao registro uma chave no nível de VM e outra no nível proxy, a configuração do registro no nível de VM terá prioridade sobre a configuração no nível de proxy.

Solução para falha de instantâneo encerrado

Certifique-se de que a opção **Crie o instantâneo sem quiescência de convidado se a quiescência de instantâneo falhar** esteja selecionada na guia origem do plano de backup sem agente com base em Host.

O backup sem agente com base em host trava ao usar o Windows 2003 R2 de 64 bits como proxy de backup

O Backup sem agente com base em host para VM da VMware trava ao usar o Windows 2003 R2 de 64 bits como proxy de backup.

Válido para VMware

Sintoma

Quando a máquina com Windows 2003 R2 de 64 bits é usada como o servidor proxy de backup para proteger a VM da VMware, às vezes, a tarefa de backup pode travar. É possível ver as mensagens de erro como a seguir no arquivo de log de depuração da tarefa de backup:

[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. Erro de retorno de chamada 18000 em 2439. {AFBackend.exe::AFBackupVirtual.dll (1746.0)}
[2016/01/21 10:19:11:691 00 03820 03336] [VDDKLOG] VixDiskLibVim: Failed to find the VM. Erro 18000 em 2511. {AFBackend.exe::AFBackupVirtual.dll(1746.0)}

Solução

No Arcserve UDP versão 7.0, o VMware VDDK 6.x está integrado. No entanto, oficialmente, o VDDK 6.x não oferece suporte ao Windows 2003 R2. Como alternativa, é possível usar uma das seguintes opções:

- Passe a usar um proxy oficialmente suportado pelo VDDK 6.x. Por exemplo, o proxy do Windows 2008 R2, do Windows 2012 ou do Windows 2012 R2.
- Substitua o VDDK 6.x interno pelo VDDK 5.5, que também é suportado pelo UDP 7.0. Para obter detalhes sobre como substituir o VDDK, consulte *Como aplicar uma versão do VDDK diferente da versão interna no Arcserve UDP.*

O backup sem agente com base em host não usa o modo de transporte hotadd

Sintoma

Para fazer backup de dados, a tarefa de backup com base em host não usa o modo de transporte hotadd, mesmo quando ele estiver disponível. Isso acontece quando a máquina virtual de origem é importada para o console do Arcserve UDP de um host ESX (em vez do servidor vCenter) e o host ESX é gerenciado por um servidor vCenter.

Solução

Para resolver o erro, execute uma das seguintes tarefas:

- Exclua o nó da máquina virtual no console do Arcserve UDP. Importe o nó novamente do vCenter Server que o gerencia o host ESX.
- Desconecte o ESX do vCenter Server.

A tarefa de backup sem agente com base em host ou restauração usa o modo de transporte NBD ou NBDSSL mesmo quando o modo SAN é possível

Válido em plataformas Windows. Válido apenas para VM VMware.

Sintoma

Embora o modo de transporte SAN seja possível, a tarefa de backup ou restauração sem agente ainda usa o modo de transporte NBD ou NBDSSL.

Solução

Os pré-requisitos a seguir devem ser atendidos para utilizar o modo de transporte SAN por tarefas de restauração e backup sem agente.

- A máquina proxy deve ser uma máquina física (não pode ser uma máquina virtual).
- A máquina proxy deve estar conectada à LUN de SAN em que a VM reside.
- Na máquina proxy, a diretiva de SAN do disco de SAN deve ser configurada como OnlineAll.

  Para configurar o disco, faça o seguinte:

  1. Efetue logon no sistema proxy de backup usando uma conta com privilégios administrativos.
  2. Abra a linha de comando do Windows.
  3. Na linha de comando, digite os seguintes comandos
     a. Digite "diskpart" e pressione Enter.
     b. Digite "SAN" e, em seguida, pressione Enter.

        A diretiva atual da SAN é exibida.

     c. Digite "SAN POLICY=OnlineAll" e pressione Enter.
- Se desejar executar a recuperação da VM pelo modo de transporte SAN, o disco de SAN deverá ser configurado para permitir a gravação.

  Para limpar o sinalizador de somente leitura, faça o seguinte:

  1. Efetue logon no sistema proxy de backup usando uma conta com privilégios administrativos.
  2. Abra a linha de comando do Windows.
  3. Na linha de comando, digite os seguintes comandos

a. Digite "diskpart" e pressione Enter.

b. Digite "list disk" e pressione Enter.

   A lista de discos é exibida.

c. Digite "select disk xxx" e pressione Enter para selecionar o disco de SAN que será configurado para permitir gravação.

d. Digite "attribute disk clear readonly" e pressione Enter.

- Para recuperação da VM, o modo de transporte SAN oferece o melhor desempenho em discos thick, mas o pior desempenho em discos thin. Portanto, a recuperação da VM usa o modo de transporte NBD ou NBDSSL para discos thin por padrão. Se você quiser usar o modo de transporte SAN até mesmo para discos thin, é possível adicionar um valor de sequência de caracteres EnforceTransportForRecovery com o valor SAN em HKLM\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFRestoreDll (crie a chave AFRestoreDll se ela não existir).
- Ao obter instantâneos durante o backup, arquivos adicionais são gerados. Por isso, um determinado espaço livre é necessária no dispositivo de armazenamento em que residem os arquivos VMDK da VM. O modo de transporte SAN precisa de mais espaço livre em comparação com o modo de transporte NBD/NBDSSL. Dessa maneira, certifique-se de que haja espaço livre suficiente no LUN de SAN se desejar usar o modo de transporte SAN.

Falha ao criar um instantâneo para máquinas virtuais do Hyper-V quando várias tarefas estão sendo executadas

Sintoma

Ao executar várias tarefas ao mesmo tempo, a criação de instantâneos da máquina virtual de CSV do Hyper-v demora muito e depois ocorre uma falha. A falha persiste mesmo após várias tentativas. A mensagem a seguir é exibida no log de atividades da respectiva máquina virtual.

A criação do instantâneo está em andamento e somente uma operação de criação de instantâneo pode estar em andamento por vez.

Tente novamente após 600 segundos.

Solução

O problema ocorre porque só é possível executar a criação de um instantâneo por vez.

Para resolver o problema, pode-se aumentar o número de tentativas ou aumentar o intervalo entre as tentativas. Você também pode aumentar o número de tarefas simultâneas que pode executar.

Observação: o valor padrão de novas tentativas é 3 e o intervalo de tempo padrão é de 10 minutos.

Para aumentar o número de novas tentativas, execute estas etapas no servidor proxy:

1. Abra o Registro do Windows.
2. Vá para HKLM\SOFTWARE\Arcserve\Unified Data Protection\Engine.
3. Crie uma chave denominada **VSSWrap**.
4. Clique com o botão direito do mouse em **VSSWrap**, selecione **Novo**, em seguida, selecione o valor **DWORD (32 bits)** e especifique o nome como **VssAsynchMaxRetryTimes**.
5. Especifique o valor conforme necessário.

Para aumentar o intervalo entre as tentativas, execute as seguintes etapas no servidor proxy:

1. Abra o Registro do Windows.
2. Vá para HKLM\SOFTWARE\Arcserve\Unified Data Protection\Engine.
3. Crie uma chave denominada **VSSWrap**.

4. Clique com o botão direito do mouse em **VSSWrap**, selecione **Novo**, em seguida, selecione o valor **DWORD (32 bits)** e especifique o nome como **VssAsynchRetryInterval**.
5. Especifique o valor conforme necessário.

Para aumentar o número de tarefas simultâneas, execute estas etapas no servidor proxy:

1. Abra o Registro do Windows.
2. Vá para HKLM\SOFTWARE\Arcserve\Unified Data Protection\Engine.
3. Clique com o botão direito do mouse em **HyperVMaxJobNum**, selecione **Modificar** e especifique o valor, conforme necessário.

Falha do Hyper-V ao criar um instantâneo VSS

O backup da VM com base em host do Hyper-V falha em um host do Hyper-V e exibe a seguinte mensagem:

Falha ao capturar instantâneo de VSS.

Sintoma

Os motivos a seguir são responsáveis pela falha do backup:

- Um ou mais volumes no host do Hyper-V não estão formatados com NTFS/Refs.
- Um ou mais volumes no host do Hyper-V têm menos de 100 MB de espaço livre.
- Atividade em disco excessiva durante o período do backup.

Solução

Resolva os problemas de ambiente e execute o backup novamente.

Falha ao fazer backup de um disco virtual devido a um erro do sistema = [O dispositivo não está pronto (21)]

Válido em plataformas Windows.

Sintoma

Quando ocorre um erro de rede ou um servidor Hyper-V é reiniciado durante o backup em andamento, o log de atividade especifica que o erro pode ser um erro de rede ou um erro do sistema de arquivos.

Solução

Reinicie a tarefa de backup novamente após a reinicialização do servidor do Hyper-V.

Falha na tarefa de backup

Sintoma

Uma tarefa de backup falhou com a seguinte mensagem de erro nos logs de atividades:

A reconfiguração do backup não pode ser executada no estado atual. Desligue a máquina virtual e tente executar a tarefa de backup novamente. (A máquina virtual pode ser ligada durante ou após a fase de criar instantâneo).

Solução

Definir os valores do registro para não reconfigurar o disk.enableUUID.

Siga estas etapas:

Aplica-se ao nível proxy e todas as VMs do VMware são afetadas.

1. Efetue logon no servidor proxy de backup.
2. Abra o editor de registro e procure a seguinte chave:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll
3. Adicionar um valor DWORD com o nome DoNotReconfigDiskUUID e especifique 1 como seu valor.

Aplica-se ao nível de VM específico e somente a VM especificada é afetada.

1. Efetue logon no servidor proxy de backup.
2. Abra o editor de registro e procure a seguinte chave:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<VM-InstanceUUID>

   Observação: substitua o <VM-InstanceUUID> pelo valor UUID da máquina virtual à qual esta configuração se aplica. O valor pode ser encontrado no URL da máquina virtual usada quando estiver conectado ao agente do Arcserve UDP.
3. Adicionar um valor DWORD com o nome DoNotReconfigDiskUUID e especifique 1 como seu valor.

Esteja ciente das seguintes considerações:

- O nível de VM tem precedência no caso de ambos os registros no nível de VM e proxy serem configurados.

- Se o registro não existir, o valor de registro indica 0, isto é, você terá de reconfigurar o disk.enableUUID.
- Se você especificou não reconfigurar o parâmetro disk.enableUUID, os dados de backup poderão não estar em um estado consistente.

Para obter mais informações sobre esse problema, consulte o artigo sobre base de conhecimento da VMware.

Falha ao importar as VMs da VMware a partir do vCenter

Sintoma

O Arcserve UDP não pode importar VMs da VMware a partir do vCenter, embora o servidor vCenter seja funcional e capaz de se conectar tanto com o navegador quanto com o cliente do vSphere. No arquivo ARCAPP-Gateway.log do servidor do Console do Arcserve UDP, a seguinte mensagem de erro é exibida:

com.sun.xml.ws.client.ClientTransportException: HTTP transport error: javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: Certificates does not conform to algorithm constraints

Mas, quando você altera as duas linhas a seguir no arquivo "C:\Arquivos de programas\Arcserve\Unified Data Protection\Common\JRE\lib\security\java.security" e reinicia o serviço de gerenciamento do Arcserve UDP, ele poderá se conectar ao mesmo servidor vCenter pelo Arcserve UDP:

Linhas existentes:

jdk.certpath.disabledAlgorithms=MD2, MD5, RSA keySize < 1024

jdk.tls.disabledAlgorithms=SSLv3, RC4, MD5withRSA, DH keySize < 768

Linhas modificadas:

jdk.certpath.disabledAlgorithms=MD2, RSA keySize < 512

jdk.tls.disabledAlgorithms=SSLv3, RC4, DH keySize < 512

Causa:

O servidor vCenter tem um certificado com um comprimento curto de chave pública ou seu algoritmo foi desativado pelo JRE no Arcserve UDP. Um certificado com comprimento de chave pública inferior a 1024 bits é considerado inseguro (o mesmo se aplica ao algoritmo MD5). Elas são desativadas pelo JRE usado pelo Arcserve UDP.

Solução

Gere um novo certificado para o servidor vCenter. Certifique-se de que o novo certificado tenha uma chave pública com mais de 1024 bits e utilize um algoritmo mais forte.

Os backups falham devido à licença ESXi

Válido em plataformas Windows.

Sintoma

Falha nas tarefas de backup completo, incremental e de verificação. A seguinte mensagem é exibida no log de atividades do Arcserve UDP:

O servidor <server_name> da VM não tem uma licença paga do ESX

Solução

Devido a uma limitação do VMware, as máquinas virtuais em execução em servidores ESXi com uma licença gratuita não podem ser copiadas para backup. Para proteger as VMs, aplique uma licença adquirida.

O modo de transporte HotAdd não funciona durante a tentativa de fazer backup de uma VM da VMware

Sintoma

O modo de transporte HotAdd não é suportado para essa VM e, como resultado, o backup falha no modo NBDSSL (dispositivo de bloqueio de rede criptografado). (A tarefa de backup está sendo executada lentamente). O backup de uma VM do VMware não está usando o transporte HotAdd. Para obter mais detalhes sobre o transporte HotAdd, consulte o link.

Verifique os seguintes pré-requisitos do HotAdd:

- O proxy de backup do HotAdd deve ser uma máquina virtual. O HotAdd envolve anexar um disco virtual ao proxy de backup, como a ação de anexar o disco a uma máquina virtual.
- O proxy com o HotAdd deve ter acesso ao mesmo repositório de dados que a máquina virtual de destino.
- A versão do VMFS e o tamanho do bloco de dados da VM de destino devem ser iguais aos do repositório de dados no qual o proxy do HotAdd reside. Se o proxy do HotAdd for uma máquina virtual que reside em um volume VMFS-3, escolha um volume com tamanho de bloco apropriado de acordo com o tamanho máximo do disco virtual das máquinas virtuais das quais os clientes desejam fazer backup, conforme mostrado em Tamanho de bloco do VMFS-3 para o proxy de backup do HotAdd. Essa limitação não se aplica aos volumes VMFS-5 que sempre tem o tamanho de bloco de arquivo de 1 MB.

  A tabela a seguir exibe o tamanho de bloco do VMFS-3 para o proxy de backup do HotAdd:

Tamanho do bloco do VMFS	Tamanho máximo do disco de destino
1 MB	256 GB
2 MB	512 GB
4 MB	1024 GB
8 MB	2048 GB

- No VSphere 5.1 e versões anteriores, o tamanho máximo com suporte do VMDK é 1,98 TB.
- Os discos a serem implantados com HotAdd devem ser SCSI. As unidades IDE não são compatíveis com o HotAdd.
- O VMware Tools deve ser instalado e atualizado na VM e no proxy de backup.

- O repositório de dados precisa de espaço suficiente para um instantâneo da VM.
- O HotAdd poderá falhar se algum disco tiver sido criado com uma versão de hardware mais recente do que a da VM que está sendo armazenada em backup. Por exemplo, isso poderá ocorrer se um disco for movido de uma VM com versão de hardware 8 para uma VM com versão de hardware 7. Para resolver o problema, atualize a versão do hardware da VM.
- Um único controlador SCSI pode ter um número máximo de 15 discos anexados. Para executar várias tarefas simultâneas com mais de 15 discos, é necessário adicionar mais controladores SCSI a sua máquina proxy de backup.
- No caso de uma conexão ESX autônoma (o ESX Server não é gerenciado pelo vCenter), você poderá fazer o HotAdd dos discos de VMs que estão localizados no mesmo ESX que a máquina proxy de backup.
- O HotAdd poderá falhar se você estiver tentando fazer backup da VM por meio do ESX adicionado como um servidor autônomo ao UDP, mas que, na verdade, está sendo gerenciado pelo vCenter.
- O HotAdd poderá falhar se a VM que você está tentando armazenar em backup e o servidor proxy estiverem em agrupamentos diferentes.

Solução

Desative a opção "automount" na máquina proxy de backup usando o utilitário "diskpart".

Controle mais granular de VSS em encerramentos do sistema operacional convidado Windows

Sintoma

Quero especificar um controle mais granular de VSS durante a criação do instantâneo de encerramento para o sistema operacional convidado Windows.

Solução

No vSphere 6.5, a API de serviço web do vSphere permite os seguintes controles mais granulares para VSS ao criar o instantâneo de encerramento para o sistema operacional convidado Windows:

- É possível configurar em qualquer lugar o tempo limite (padrão de 15 minutos) para encerrar as máquinas virtuais, desde cinco minutos até quatro horas.
- Tipo de backup de VSS – VSS_BT_COPY foi usado anteriormente como padrão durante a criação do instantâneo. Mas, agora, VSS_BT_FULL, VSS_BT_INCREMENTAL, VSS_BT_DIFFERENTIAL e VSS_BT_LOG também estão disponíveis. O truncamento do log é acionado de acordo com as configurações do aplicativo.
- O contexto de backup de VSS foi introduzido para impor o encerramento do aplicativo (VSS_CTX_BACKUP de contexto) ou o encerramento do sistema de arquivos (VSS_CTX_FILE_SHARE_BACKUP de contexto).

Usando o Arcserve UDP, você pode especificar os parâmetros no Registro para implementar o controle.

Observação: para especificar, é necessário que o VMware Tools 10.1.0 ou superior esteja instalado no sistema operacional convidado da VM.

Siga estas etapas:

1. Efetue logon na máquina proxy.
2. Crie um valor de registro no nível de servidor proxy ou VM.

   Observação: se você adicionar o valor de registro no nível de VM e no nível de proxy, a configuração no registro no nível de VM terá prioridade sobre a configuração no registro no nível de proxy.

   No nível do servidor proxy (aplicável a todas as tarefas de backup em execução no servidor proxy)

a. Abra a chave do registro no seguinte local:

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

b. Adicione os seguintes valores DWORD apropriados:

- VssUseEnhancedSnapshot
- VssTimeoutMinute
- VssBackupType
- VssBackupContext
- VssBootableSystemState
- VssPartialFileSupport

No nível da VM

a. Abra a chave do registro no seguinte local:

[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<vm instance uuid>]

b. Adicione os seguintes valores DWORD apropriados:

- VssUseEnhancedSnapshot
- VssTimeoutMinute
- VssBackupType
- VssBackupContext
- VssBootableSystemState
- VssPartialFileSupport

Valores possíveis do Registro:

VssUseEnhancedSnapshot

- 0 – não usar o controle aprimorado, e os valores inferiores do Registro não são efetivos
- 1 - uar o controle aprimorado, e os valores inferiores do Registro são efetivos

VssTimeoutMinute

Intervalo de 5 a 240

VssBackupType

- 0 - VSS_BT_COPY (padrão)
- 1 - VSS_BT_FULL
- 2 - VSS_BT_INCREMENTAL
- 3 - VSS_BT_DIFFERENTIAL
- 4 - VSS_BT_LOG

VssBackupContext

- 0 - ctx_auto
- 1 - ctx_backup (padrão)
- 2 - ctx_file_share_backup

VssBootableSystemState

- 0 – falso
- 1 - verdadeiro (padrão)

VssPartialFileSupport

- 0 - falso (padrão)
- 1 - verdadeiro

Não é possível configurar a máquina virtual para ativar o parâmetro "Disk.EnableUUID"

Sintoma

Ocorre um erro durante a reconfiguração da máquina virtual para ativar o parâmetro 'disk.EnableUUID', necessário para um backup consistente com o aplicativo. Esse problema ocorre quando o ambiente virtual é recuperado de um erro.

Solução

Esse problema é específico do ambiente do VMware. Esse problema ocorre quando o Microsoft VSS tenta executar um instantâneo encerrado pelo aplicativo, mas falha ao ler o valor de UUID do disco ou o número de série de um ou mais discos da máquina virtual.

O parâmetro disk.EnableUUID da VM deve ser ativado. VMs criadas em 4.1 ou posterior têm esse parâmetro ativado por padrão. A tarefa de backup é configurada automaticamente para evitar inconsistência de dados e executar um backup consistente com o aplicativo. Se a tarefa de backup falhar ao ativar o disk.EnableUUID, configure manualmente o parâmetro usando as etapas a seguir:

Siga estas etapas:

1. Desligue a máquina virtual.
2. Efetue logon no vCenter Server ou no host do ESXi/ESX por meio do vSphere Client.
3. Clique com o botão direito do mouse na máquina virtual e clique em Editar configurações.
4. Clique na guia Opções.
5. Navegue até Avançado > Geral > Parâmetros de configuração.
6. Adicione ou modifique o parâmetro bruto disk.EnableUUID e defina-o como Verdadeiro.
7. Clique em OK para salvar.
8. Clique em OK para sair.
9. Reinicialize a máquina virtual para que as alterações entrem em vigor.

   Observação: se o parâmetro já estiver definido como Verdadeiro, existe uma alternativa sem interrupções, que é editar o vmx e definir o valor de disk.enableUUID como Falso e, em seguida, usar o vMotion para mover a VM (para qualquer outro host) a fim de recarregar o vmx na memória do host. Isso desativa efetivamente o encerramento no nível do aplicativo (o encerramento do sistema de arquivos permanece disponível).

As operações de recuperação falham durante a recuperação de dados usando o modo de transporte HOTADD ou SAN

Válido em plataformas Windows.

Sintoma

As operações de recuperação falham ao recuperar dados usando o modo de transporte hotadd ou SAN. A seguinte mensagem é exibida no log de atividades:

Ocorreu um erro desconhecido. Entre em contato com o suporte técnico.

Solução

As operações de recuperação falham ao usar o modo de transporte hotadd ou SAN quando as configurações de disco não estiverem definidas corretamente.

Para configurar o disco, execute as seguintes etapas:

1. Efetue logon no sistema proxy de backup usando uma conta com privilégios administrativos.
2. Abra a linha de comando do Windows.
3. Na linha de comando, digite o seguinte comando:

   diskpart

   Pressione Enter.
4. Digite SAN e, em seguida, pressione Enter.

   A diretiva atual da SAN é exibida.
5. Digite o seguinte comando e pressione Enter:

   SAN POLICY = OnlineAll

   A diretiva da SAN está configurada para não montar automaticamente volumes hospedados pela SAN.
6. Para limpar o atributo de somente leitura do disco específico da SAN, selecione o disco a partir da lista de discos, digite o seguinte comando e pressione Enter:

   attribute disk clear readonly
7. Digite exit e, em seguida, pressione Enter.

   O disco está configurado e é possível enviar a tarefa novamente.

   Se a tarefa falhar novamente, monte os discos hotadd manualmente usando o gerenciamento de discos no sistema proxy.

   Para montar os discos manualmente, faça o seguinte:

1. Efetue logon no sistema proxy de backup usando uma conta com privilégios administrativos.
2. Abra o Painel de Controle do Windows e clique duas vezes em Ferramentas Administrativas.

   A janela Ferramentas Administrativas é exibida.
3. Na lista Favoritos, clique duas vezes em Gerenciamento do Computador.

   O Gerenciamento do computador é exibido.
4. Expanda Armazenamento e clique em Gerenciamento de Disco.

   Os discos são exibidos.
5. Clique com o botão direito no disco que deseja montar e clique em Online.

   O disco está montado e é possível enviar a tarefa novamente.

Falha na operação de recuperação da VM quando uma porta não padrão é especificada

Sintoma

Operação de recuperação da VM falha quando uma porta não padrão é especificada para o VMware vCenter Server.

Solução

Para resolver o problema, defina o número de porta não padrão do vCenter para o valor de VDDKport no registro da máquina proxy de backup.

Para definir o número da VDDKport, execute as seguintes etapas no servidor proxy:

1. Abra o Registro do Windows.
2. Vá para HKLM\SOFTWARE\Arcserve\Unified Data Protection\Engine.
3. Clique com o botão direito do mouse em VDDKport, selecione Modificar e especifique o valor, conforme necessário.

A tarefa de backup completo ou incremental programada falha para a VM do Hyper-V

Sintoma

Às vezes, a tarefa de backup incremental ou completa programada falha para as máquinas virtuais do Hyper-V e os seguintes erros são exibidos no visualizador de eventos no host do Hyper-V:

- Falha ao adicionar a operação DM à máquina virtual <nome da vm>. Memória esgotada (0x8007000E) (ID da máquina virtual <ID da vm>)
- Não foi possível criar o ponto de verificação de backup da máquina virtual <nome da vm>: Esta operação foi retornada porque o tempo limite expirou. (0x800705B4). (ID da máquina virtual <vm ID>)
- Não foi possível criar o ponto de verificação de backup da máquina virtual <nome da vm>: Elemento não encontrado. (0x80070490). (ID da máquina virtual <vm ID>)
- Os gravadores VSS dentro da máquina virtual <nome da vm> não puderam realizar BackupComplete na cópia de sombra (instantâneo de VSS) definida: Chamada de função feita quando o objeto estava em estado incorreto para essa função (0x80042301). (ID da máquina virtual)
- O gravador de VSS do Hyper-V encontrou um erro ao processar essa máquina virtual. (Para obter mais informações sobre erros do gravador de VSS do Hyper-V, consulte a documentação do produto).

Solução 1

A resolução é aumentar o tamanho de RAM no servidor Hyper-V e, então, enviar novamente a tarefa de backup.

Solução 2

Se o gravador VSS que está dentro da máquina virtual não funcionar corretamente, a tarefa de backup falhará. Para resolver o problema, verifique o log de eventos do host Hyper-V e a máquina virtual. Verifique os erros e avisos de VSS e execute as ações apropriadas.

Falha no gravador de VSS NTDS do Hyper-V ao criar o instantâneo de VSS na VM

Sintoma

Em uma VM de controlador de domínio, se o recurso AutoMount não estiver ativado, o gravador de VSS NTDS falha ao fazer o instantâneo de VSS na VM. Como resultado, o gravador de Hyper-V VSS falha ao criar o instantâneo de VSS no host Hyper-V.

A tarefa de backup do Hyper-V HBBU falha com o seguinte log de atividades:

O gravador de VSS do Hyper-V encontrou um erro ao processar essa máquina virtual. (Para obter mais informações sobre erros do gravador de VSS do Hyper-V, consulte a documentação do produto).

Solução

Ativar o recurso *AutoMount* na VM.

Siga estas etapas:

1. Abra uma janela de prompt de comando.
2. Abra o diskpart e execute o seguinte comando:

   automount enable

As alterações do endereço MAC não são retidas após a recuperação da VM

Válido em plataformas Windows e VM VMware

Sintoma

Os endereços MAC de máquinas virtuais não são mantidos após a recuperação de máquinas virtuais.

Solução

Os endereços MAC não são mantidos durante a recuperação, para evitar duplicatas. Para manter as informações de endereços MAC, defina a seguinte chave do Registro no servidor proxy:

Local: HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine
Nome da chave: RetainMACForVDDK
Tipo de valor: Sequência de caracteres

Valor da chave: 1

A recuperação de VM falhou com o erro - não é possível abrir arquivos VMDK

Sintoma

Ocorre uma falha de recuperação da máquina virtual e a seguinte mensagem de erro é exibida nos logs:

Não é possível abrir o arquivo vmdk (nome do arquivo com .vmdk). O VMware relatou o seguinte erro: você não tem direitos de acesso a esse arquivo. Para obter mais informações, consulte o log de depuração de restauração. Se necessário, entre em contato com o suporte da Arcserve.

As mensagens a seguir são encontradas nos logs de depuração de restauração:

- [VDDKLOG] CnxAuthdConnect: Returning false because SSL verification requested and target authd does not support SSL
- [VDDKLOG] CnxConnectAuthd: Returning false because CnxAuthdConnect failed
- [VDDKLOG] Cnx_Connect: Returning false because CnxConnectAuthd failed
- [VDDKLOG] Cnx_Connect: Error message: SSL required

Solução

O motivo pode ser a autenticação SSL desativada no host do ESX. Para solucionar o problema, use um destes métodos:

Usando o cliente do vSphere

1. Efetue logon no vCenter/ESX Server.
2. Navegue até as configurações do ESX Server:

   Configuration, Advanced settings, Configuration, Defaults security

3. Ative a seguinte opção:

   config.defaults.security.host.ruissl

Usando a linha de comando

1. Conecte-se ao host do ESX usando SSH.
2. Abra o seguinte arquivo:

   /etc/vmware/config

3. Defina a entrada security.host.ruissl como VERDADEIRO.
4. Salve o arquivo e reinicie os agentes de gerenciamento.

Problemas causados por UUID da VM duplicado

Sintoma 1

O nó da VM será substituído após a importação de outro nó de VM no Console.

Por exemplo, você tem 2 máquinas virtuais VM1 e VM2 com a mesma UUID (que é chamada UUID de instância para VMware e a UUID da VM para o Hyper-V) nos hosts ESXi que são gerenciados por vCenter VC1 e VC2 diferentes. Você importa a VM1 no console e ela aparece na exibição de lista de nós do console. No futuro, importe a VM2 no console. Na exibição de lista de nós, a VM1 é substituída pela VM2 (em outras palavras, a VM2 é adicionada e a VM1 removida).

Sintoma 2

As informações do nó da VM na coluna do Hypervisor fica mudando quando a detecção automática estiver em execução.

Por exemplo, você tem 2 máquinas virtuais VM1 e VM2 com a mesma UUID (que é chamada UUID de instância para VMware e a UUID da VM para o Hyper-V) nos hosts ESXi que são gerenciados por vCenter VC1 e VC2 diferentes. Você importa a VM1 no console. Além disso, você também importa pelo menos uma VM do vCenter VC2 para que ambos o VC1 e o VC2 sejam adicionados à Lista de detecção do nós (é possível verificar a lista na página Configuração de detecção do nó, na guia Configurações). Enquanto a detecção de nó é executada, ela, primeiramente, conecta-se ao VC1 e detecta a VM1 pela UUID e a coluna Hipervisor é atualizada com as informações do VC1. Posteriormente, quando ela conecta-se ao VC2, ela detecta a VM2 pela mesma UUID e a coluna Hipervisor é atualizada com as informações da VC2.

Solução

O Arcserve UDP usa a UUID da VM (que se chama UUID de instância para a VMware e a UUID da VM para o Hyper-V) para identificar um nó de VM. Embora seja muito raro que as VMs tenham UUID duplicadas, comportamentos problemáticos podem ocorrer no Arcserve UDP neste caso.

Para resolver os problemas, consulte as seguintes etapas para alterar manualmente a UUID da VM (aplicável apenas para a VM da VMware). Após você alterar manualmente a UUID da VM, exclua a VM original do console do Arcserve UDP e importar a VM novamente.

1. Abra a seguinte URL:

   https://<nome do host do vCenter>/mob/

2. Efetue logon como administrador.

3. Pesquise por "conteúdo" na coluna NAME e clique no link na coluna VALOR na mesma linha.
4. Pesquise por "rootFolder" na coluna NOME e clique no link na coluna VALOR na mesma linha.
5. Pesquise por "childEntity" na coluna NOME. Na coluna VALOR na mesma linha, encontre o Datacenter no qual a VM reside e clique no link correspondente.
6. Pesquise por "vmFolder" na coluna NOME e clique no link na coluna VALOR na mesma linha.
7. Pesquise por "childEntity" na coluna NOME. Na coluna VALOR na mesma linha, clique em "mais..." para expandir a lista de VMs. Procure pela VM que você está procurando e clique no link.
8. Pesquise por ReconfigVM_Task da tabela Métodos e clique no link.
9. No novo navegador aberto, remova todos os conteúdos no campo VALOR e digite o seguinte código:

```
<spec>
<instanceUuid>2499952a-6c85-480e-b7df-
4cbd2137eb69</instanceUuid>
</spec>
```

   Observação: A sequência de caracteres 2499952a-6c85-480e-b7df-4cbd2137eb69 mencionada acima é um exemplo de UUID. Você deve substituí-la pela UUID que você deseja aplicar.
10. Clique no link Chamar método para aplicar a nova UUID.
11. Para verificar se a nova UUID foi aplicada, feche o navegador recém-aberto e volte à página da etapa 8.
12. Pesquise por "config" na coluna NOME e clique no link na coluna VALOR na mesma linha.
13. Pesquise por "instanceUuid" na coluna NOME. A UUID da VM é exibida na coluna VALOR na mesma linha.

Falha na tarefa de catálogo do sistema de arquivos ou falha de verificação do ponto de recuperação para backup sem agente com base em host

Válido em plataformas Windows. Válido apenas para VM VMware.

Sintoma

- Falha na tarefa de catálogo do sistema de arquivos para pontos de recuperação de backup sem agente com base em host
- Falha de verificação de ponto de recuperação durante a tarefa de backup sem agente com base em host e o próximo backup incremental é convertido em um Backup de verificação.

Solução

Isso pode ser causado por um problema conhecido do VMware (consulte o VMware no artigo da base de conhecimento). Quando você encerra uma VM VMware, o instantâneo contém dados corrompidos. O backup lê os dados do instantâneo e os dados copiados no backup também são corrompidos.

Observação: esse problema ocorre em todas as versões do VMware ESXi e em uma VM com o sistema operacional convidado executando o Windows 2008 R2 SP1 e o Windows 2012. O Arcserve UDP não pode detectar o problema de corrupção de dados porque a VMware não retorna um erro em tais casos. Você talvez não saiba do problema até tentar restaurar os dados.

Siga o artigo da base de conhecimento da Arcserve para verificar se o problema é causado por esse problema conhecido da VMware. A solução alternativa recomendada pela VMware é desativar os gravadores VSS, como o gravador do serviço MSSearch (ignore-os, se não estiverem instalados) e gravador de otimização de cópia de sombra (normalmente presente em cada máquina virtual Windows), no sistema operacional convidado da VM. Você pode desativar manualmente os gravadores de acordo com VMware artigo da base de conhecimento.

O Arcserve UDP também fornece uma maneira simples para desativar os gravadores, se o método de fechamento de instantâneo do VMware Tools for usado. Siga estas etapas para desativar os gravadores:

No nível do servidor proxy (aplicável para VMs protegidas pelo servidor proxy)

1. Efetue logon no servidor proxy.
2. Abra a chave do registro no seguinte local:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data
Protection\Engine\AFBackupDll]
```

3. Crie um valor de várias sequências de caracteres com o nome *DisableSpecificVSSwriters*.
4. Digite os nomes do gravador VSS que está aguardando para ser desativado (cada nome do gravador ocupa uma única linha).
5. Salve a chave do registro.

No nível da VM

1. Efetue logon no servidor proxy.
2. Abra a chave do registro no seguinte local:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data
Protection\Engine\AFBackupDll\<vm instance uuid>]
```

3. Crie um valor de várias sequências de caracteres com o nome *DisableSpecificVSSwriters*.
4. Digite os nomes do gravador VSS que está aguardando para ser desativado (cada nome do gravador ocupa uma única linha).
5. Salve a chave do registro.

Observações:

- Se você adicionar a chave do registro na VM e no registro de nível de proxy, a configuração do registro no nível da VM terá prioridade sobre a configuração no registro no nível do proxy.
- Essa configuração de registro funciona somente quando é usado o método de fechamento de instantâneo do VMware Tools no plano de backup.
- Se você já tiver configurado gravadores manualmente no sistema operacional convidado da VM de acordo com o artigo da base de dados de conhecimento da VMware, sua configuração será substituída.
- O nome do gravador diferencia maiúsculas de minúsculas e deve ser uma correspondência exata, conforme mostrado na saída de "vssadmin list writers".
- Se você desejar ativar todos os gravadores novamente, não exclua o valor do registro *DisableSpecificVSSwriters*. Em vez disso, mantenha o valor do registro mas remova o conteúdo no registro. Se *DisableSpecificVSSwriters*não existir, o Arcserve UDP presume que nada precisa ser alterado em termos de ativação ou desativação de gravadores VSS.

O backup incremental converte para backup de verificação ou o tamanho do backup aumenta no Hyper-V

Válido em VM do Hyper-V

Sintoma

- Executei uma alteração incremental em uma máquina virtual do Hyper-V. Ao executar um backup incremental, toda a máquina virtual é incluída no backup, em vez de fazer o backup apenas dos dados alterados.
- Eu tenho um servidor proxy com o Arcserve UDP Version 7.0 que faz backup de uma máquina virtual de um host do Hyper-V (exemplo HOST1). Eu tenho outro servidor proxy com uma versão mais antiga do Arcserve UDP que faz o backup de uma máquina virtual a partir do mesmo host do Hyper-V (HOST1). Nesses casos, o CBT está inativo e as tarefas incrementais não serão executadas. O backup incremental se transformará no backup de Verificação.

Solução

As causas raízes dos sintomas acima podem ser um dos seguintes motivos:

- A perda de dados de acompanhamento de bloco de alteração (CBT). As seguintes circunstâncias resultarão em perda de dados de CBT:
  - O host do Hyper-V trava ou pode ser desligado de maneira anormal.
  - O serviço de CBT é interrompido ou o serviço é finalizado inesperadamente.
  - O serviço de CBT não concluiu o trabalho enquanto o host Hyper-V estava encerrando.
- As versões diferentes do CBT no servidor Hyper-V e o servidor proxy.

  Exemplo: considere que haja dois ambientes Arcserve UDP, um é o Arcserve UDP versão 6.0 e o outro é o Arcserve UDP versão 7.0. Esses dois ambientes Arcserve UDP fazem backup de diferentes VMs no mesmo servidor Hyper-V. O ambiente Arcserve UDP Version 7.0 detecta automaticamente o CBT na versão mais antiga do servidor do Hyper-V e fará sua atualização para a versão mais recente. Nesses casos, o ambiente Arcserve UDP Versão 5 converte o restante do backup incremental programado em um backup completo.

  Se o Arcserve UDP detectar as diferentes versões de CBT, o log de atividades exibirá uma mensagem de aviso.

A solução é para atualizar todos os servidores proxy que protegem as máquinas virtuais de um host do Hyper-V para a mesma versão do Arcserve UDP.

Falha no backup com base em host da VM do Hyper-V que tem uma configuração de disco diferencial especial

Válido para a VM do Hyper-V

Sintoma

Se um disco diferencial estiver configurado em uma máquina virtual do Hyper-V, a tarefa de backup para essa máquina virtual falhará. É exibida a seguinte mensagem de erro no log de atividades:

Falha ao preparar para backup da máquina virtual

A seguinte mensagem de erro é exibida no arquivo de log da tarefa de backup, em C:\Arquivos de Programas\Arcserve\Unified Data Protection\Engine\Logs,

O arquivo de disco virtual \\?\UNC\<IP_Address_VM>\HYPERV_HBBU_SNAPSHOT@<snapshot_name>\WIN12-SQL\VIRTUAL HARD DISKS\WIN12-SQL-1.VHDX não foi exposto.

O problema ocorre apenas quando a máquina virtual tem as seguintes configurações de disco diferencial. Todas as configurações devem ser aplicadas.

- A máquina virtual tem um disco rígido virtual regular (tamanho fixo ou dinamicamente expandindo) Disk1 anexado a um controlador IDE ou SCSI da máquina virtual.
- A máquina virtual tem um disco rígido virtual diferencial (Disk2) que também é anexado a um controlador IDE ou SCSI da máquina virtual.
- O disco pai de Disk2 é especificado para Disk1.

Solução

Este erro ocorre devido a uma configuração incorreta ou anormal. Para resolver esse erro, desvincule o disco diferencial ou seu pai da máquina virtual. O Arcserve UDP não suporta tal configuração de disco diferencial.

A tarefa de backup falha para uma máquina virtual VMware

Válido para a VM VMware

Sintoma

Quando faço backup de uma máquina virtual VMware, a tarefa de backup falha com qualquer uma das seguintes mensagens de erro no log de atividades:

Cancele o backup, porque a tarefa de backup foi configurada para usar o método de instantâneo "VSS da Microsoft dentro da VM". No entanto, apenas o método de instantâneo "Ferramentas do VMware" é aplicável, porque o backup da VM com base em host falhou ao implantar as ferramentas necessárias para a VM.

Ou

Cancele o backup, porque a tarefa de backup foi configurada para usar o método de instantâneo "Ferramentas do VMware". No entanto, apenas o método de instantâneo "VSS da Microsoft dentro da VM" é aplicável, porque o backup da VM com base em host falhou ao cancelar a implantação das ferramentas de dentro da VM.

Solução

O primeiro erro pode ocorrer por vários motivos. Você selecionou a opção **VSS da Microsoft dentro da VM** mas:

- Você não atualizou a VM com as credenciais necessárias
- As credenciais não estão corretas
- As Ferramentas do VMware não estão instaladas ou atualizadas.

Neste caso, o Arcserve UDP não pode implantar as ferramentas necessárias para que a máquina virtual use o novo método de instantâneo.

Para resolver esse erro, atualize a máquina virtual com as credenciais corretas. Verifique se as Ferramentas do VMware estão atualizadas e em execução na máquina virtual. Após a verificação, envie a tarefa de backup novamente.

Solução

O segundo erro pode ocorrer no seguinte cenário. Você usou a opção **VSS da Microsoft dentro da VM** nas tarefas de backup anteriores. Agora, você desejar usar a opção **Ferramentas do VMware**, mas as credenciais da máquina virtual foram alteradas (por exemplo, você alterou a senha do sistema operacional convidado, mas não atualizou o nó da máquina virtual no console) ou as Ferramentas do VMware não estão funcionando por algum motivo. Em tais casos, o Arcserve UDP não pode

cancelar a implantação das ferramentas (que foram implantadas pela tarefa de backup anterior) da máquina virtual para usar o novo método de instantâneo.

Para resolver o erro, execute uma das seguintes etapas:

- Atualize a máquina virtual com as credenciais corretas. Verifique se as Ferramentas do VMware estão atualizadas e em execução no sistema operacional convidado da máquina virtual. Após a verificação, envie a tarefa de backup novamente.
- Cancele a implantação manualmente das ferramentas da máquina virtual:
    a. Efetue logon na máquina virtual.
    b. Vá até a seguinte pasta:

        C:\Program Files\ARCServe\ASVMOperationTools\custom-freeze-vmware-snapshot\auto-deploy

    c. Clique com o botão direito do mouse no arquivo em lote auto-undeploy.bat e selecione executar como administrador.
    d. Exclua as seguintes pastas:

        C:\Program Files\ARCServe\as-hbbu-vmwarebackup

        C:\Program Files\ARCServe\ASVMOperationTools

    e. Envie a tarefa de backup novamente.

Desativar nova verificação de adaptadores HBA durante o backup incremental

Aplica-se ao VMware ESX.

Aplica-se somente ao UDP v6.5; não se aplica a atualizações da v6.5.

Sintoma

Quando o nó de origem e o servidor proxy estão em servidores VMware ESX diferentes e eu executo um backup incremental, meu backup demora mais tempo para ser executado. Também recebo diversas mensagens de nova verificação. Desejo desativar as novas verificações de todos os HBAs (Host Bus Adapter - Adaptadores de Barramento do Host) de outros servidores VMware ESX durante os backups incrementais.

Solução

É possível desativar a verificação criando uma chave de registro no servidor proxy e atribuindo um valor a ela.

Siga estas etapas:

1. Efetue logon na máquina.
2. Vá até a seguinte pasta:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine
   ```

3. Crie a seguinte chave de registro (DWORD), se ainda não tiver sido criada:

   ```
   DisableAllESXNodeRescan
   ```

4. Defina o valor da chave do registro como 1.

Desativar a criação de instantâneo consecutivo na VM do VMware para um backup

Na versão anterior do Arcserve UDP, quando várias tarefas de backup de VM do VMware começam ao mesmo tempo, as tarefas criam instantâneos no host do ESX em paralelo com as tarefas. Às vezes, essas operações de criação de instantâneo em paralelo aumentam a entrada e saída do disco no host do ESX. Para evitar esse problema, por padrão o Arcserve UDP versão 7.0 serializa a operação de criação de instantâneo quando as tarefas em execução no mesmo servidor proxy e a operação de criação do instantâneo estão no mesmo host ESX. Em outras palavras, a operação de criação de instantâneo ocorre uma após a outra e o ideal seria apenas um instantâneo criado por vez. Mas isso não é aplicável se as tarefas de backup estiverem em execução em servidores proxy diferentes, ou se as tarefas de backup forem para diferentes hosts ESX.

Para evitar uma situação em que a criação de instantâneos de uma tarefa trava (ou demora muito longo) e as tarefas seguintes são bloqueadas, a próxima tarefa esperará que a operação de criação de instantâneo anterior por até **cinco minutos**. Após cinco minutos, o processo de criação do próximo instantâneo é iniciado.

É possível desativar o comportamento da espera de cinco minutos, siga estas etapas:

1. Efetue logon no servidor proxy.
2. Abra a chave do registro no seguinte local:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

3. Crie um valor DWORD com o nome **CreateSnapshotSequentially**.
4. Defina o valor como 0.

Além disso, você também pode alterar o valor de tempo limite padrão (cinco minutos) seguindo estas etapas:

1. Efetue logon no servidor proxy.
2. Abra a chave do registro no seguinte local:

   [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

3. Crie um valor DWORD com o nome **CreateSnapshotTimeout**.

4. Defina o valor com um número.

   A unidade é segundos.

Quando restaurada de uma versão superior do host ESXi para uma versão anterior do host ESXi, a VM trava na fase de inicialização

Quando restaurada de uma versão superior do host ESXi em um host ESXi de versão anterior, a VM trava na fase de inicialização, depois de ligada.

Válido em plataformas Windows. Válido apenas para VM VMware.

Sintoma

Restaure uma VM de um host do ESXi versão superior para um host ESXi de versão inferior, ligue a VM. A VM trava na fase de inicialização.

Solução

A versão do sistema operacional convidado desta VM pode não ser suportada pela versão anterior do ESXi. Como alternativa, é possível usar uma das seguintes opções:

- Restaure a VM em um ESXi que oferece suporte a essa versão do sistema operacional convidado ou
- Atualize o host ESXi existente para a versão adequada.

Por exemplo, uma máquina virtual do Windows Server 2012 R2 é obtida em backup a partir de um ESXi 5.5 e restaurada para o ESXi 5.0 atualização 1. Quando ESXi 5.0 é iniciado para oferecer suporte ao sistema operacional do Windows Server 2012 R2 convidado, após a atualização 2, esse problema pode ocorrer.

É necessário atualizar ESXi 5.0, atualização 1 para a atualização 2, de forma a ter suporte para o sistema operacional do Windows Server 2012 R2 convidado. Como alternativa, é possível alterar a versão do sistema operacional convidado da VM restaurada para a versão suportada pela versão atual do ESXi (no exemplo acima, altere para o Windows Server 2008 R2).

Observação: essa solução alternativa pode não resolver o problema.

A utilização de RAM atinge 99% quando as tarefas de backup são enviadas para a VM

A utilização da RAM atinge 99% quando as tarefas de backup são enviadas para as VMs no CSV do Hyper-V do Windows 2012.

Sintoma

Durante o backup de VMs que fazem parte do cluster do Hyper-V 2012, a utilização da RAM aumenta gradualmente e atinge os 99% no host do Hyper-V de proprietário de CSV. Como resultado, o host das Máquinas virtuais e do Hyper-V param de trabalhar durante o backup.

Solução

Esse problema é causado por erros conhecidos no código da Microsoft.

Para corrigir esse problema, faça download e aplique o hotfix fornecido pela Microsoft em todos os host do Hyper-V no seguinte link:

https://support.microsoft.com/en-in/kb/2878635

Falha na tarefa de restauração do Hyper-V, não é possível se conectar ao utilitário no Host

A tarefa de restauração da VM do Hyper-V falha e uma mensagem de erro é exibida.

Sintoma

Ao restaurar uma VM do Hyper-V, a tarefa de restauração falha e o seguinte erro é exibido no log de atividades:

Falha ao estabelecer conexão com o utilitário de restauração do Hyper-V no host xxxxx

No log de depuração da tarefa de restauração, aparecem as seguintes mensagens de erro:

Falha ao se conectar a xxxxx:10218. erro:tentativa de conexão atingiu o tempo limite sem estabelecer uma conexão (rc=-536805332)

Falha ao se conectar a xxxxx:10218, erro -536805332

Solução

Normalmente, esse problema é causado porque a conexão entre o host do Hyper-V e o proxy de backup está bloqueada pelo firewall. Se possível, desative o firewall e tente restaurar novamente. Se você não puder desativar o firewall, registre a porta (ou intervalo da porta) usada pela tarefa de restauração para a exceção do firewall.

Por padrão, a tarefa de restauração escolhe aleatoriamente uma porta disponível no intervalo de 1024 e 65535. Você pode especificar manualmente o intervalo pelos valores do registro definidos no host do Hyper-V.

Siga estas etapas:

1. Efetue logon no host do Hyper-V.
2. Execute o comando *regedit* para abrir o editor do registro.
3. Navegue até a seguinte chave do registro (crie chaves se qualquer uma delas não existir):

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\HyperVRestoreStub
4. Crie os seguintes dois valores de registro (DWORD):

   PortMin

   PortMax

5. Especifique os valores com o número de início e fim do intervalo da porta.

   Observações:

   - Intervalo obrigatório de valores especificados: 1024-65535
   - É possível especificar o mesmo número para os dois valores do registro. Nesse caso, o número da porta fixo é usado para a tarefa de restauração. Quando várias tarefas de restauração são executadas simultaneamente e assim que uma tarefa de restauração ocupa esta porta, outras tarefas de restauração falham.

A proteção automática falha ao detectar e proteger a VM

A máquina virtual não é detectada e automaticamente protegida como parte da proteção automática.

Sintoma

Embora uma VM possa ser vista no hipervisor (vCenter/ESX ou Hyper-V) pelo aplicativo cliente nativo (por exemplo, cliente vSphere ou gerenciador do Hyper-V), a proteção automática não detecta e, consequentemente, a VM não pode ser protegida automaticamente.

Os motivos

- A VM não tem um status válido no hipervisor. Por exemplo, a proteção automática ignora as VMs que têm status Desconectado, Órfão ou Inacessível no vCenter/ESX.
- A VM é criada por tarefas do Arcserve UDP, como VSB (Virtual Standby - Modo de espera virtual), IVM (Instant VM - VM instantânea) ou AR (Assured Recovery - Recuperação garantida) (ou clonada da VM VSB/IVM/AR). Arcserve UDP intencionalmente ignora essas VMs devido às considerações a seguir:
  - Arcserve UDP fazendo backup de VMs criadas por IVM/VSB/AR, sem limitação, pode levar à situação de *loop de backup infinito*. Por exemplo, usar proteção automática para proteger todo o ESX. No plano de backup, depois de adicionar uma tarefa de backup, é possível adicionar uma tarefa de VSB que cria VM de VSB no mesmo ESX. Assim, após o primeiro backup, é criada uma nova VM de VSB no ESX. A nova VM de VSB é detectada por proteção automática e adicionada ao plano de backup. Em seguida, durante o próximo backup, uma nova VM de VSB da VM de VSB anterior é criada e adicionada ao plano de backup. O processo continua até que o armazenamento de ESX fique sem espaço livre.
  - Para VM de IVM/AR do Linux, a menos que a migração de armazenamento seja convertida em uma VM normal, o Arcserve UDP não consegue fazer backup da VM. A tarefa de backup pode ser concluída, mas o ponto de recuperação de backup não pode ser restaurado. Essa situação ocorre devido a uma limitação técnica da implementação de IVM do Linux.

Solução

Se você deseja fazer backup de VMs de VSB/IVM/AR, ou se as VMs são convertidas em VMs independentes pela migração de clone ou armazenamento, siga as etapas fornecidas abaixo para a VM do vSphere e a VM do Hyper-V para permitir que a proteção automática faça a detecção e a proteção.

Para a VM do vSphere

1. Efetue logon no cliente web do vSphere e localize a VM.
2. Desligue a VM.
3. Clique com o botão direito na VM e selecione Editar configurações no menu.
4. Selecione a guia **Opções da VM** e expanda Avançado.
5. Clique em **Editar configuração**.
6. Na caixa de diálogo Parâmetros de configuração, localize o parâmetro com qualquer um dos seguintes nomes:
    - VCM
    - UDP_IVM
    - UDP_ARVM
    - UDP_IVM_LINUX
    - UDP_VSBVM
    - UDP_ARVM_LINUX
    - UDP_ARIVM_LINUX
7. Limpe o valor do parâmetro e, em seguida, clique em **OK** para salvar.

Para a VM do Hyper-V

1. Efetue logon no host do Hyper-V e abra o gerenciador do Hyper-V.
2. Localize a VM.
3. Clique com o botão direito na VM e selecione Configurações no menu.
4. Na caixa de diálogo Configurações, selecione Nome no painel esquerdo.
5. Remova todas as linhas que começam com as seguintes cadeias de caracteres:
    - VCM
    - UDP_IVM
    - UDP_ARVM
    - UDP_IVM_LINUX

- UDP_VSBVM
- UDP_ARVM_LINUX
- UDP_ARIVM_LINUX

6. Clique em **OK** para salvar.

Definir o tamanho do bloco de leitura ao fazer backup do arquivo VMDK

Sintoma

Em determinados ambientes, a taxa de transferência de backup da VM da VMware é afetada pelo tamanho do bloco de leitura ao fazer backup do arquivo VMDK.

Solução

Por padrão, o tamanho do bloco de leitura do VMDK é 2 MB. É possível modificar o tamanho.

Siga estas etapas:

1. Efetue logon no proxy de backup sem agente.
2. Execute o comando *regedit* para abrir o editor do registro.
3. Navegue até a seguinte chave do registro:

   HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll
4. Crie os valores de registro (DWORD) usando o seguinte nome:

   ReadVirtualDiskBlockSizeKB
5. Especifique o valor desejado como o tamanho do bloco de leitura (a unidade é KB).

A reserva de espaço de LUN é herdada durante a execução do clone de LUN

Sintoma

Quando o clone de LUN é executado durante o backup usando o instantâneo de hardware, por padrão, a reserva de espaço é herdada do LUN de origem.

Solução

É necessário usar a chave de registro que o Arcserve UDP fornece para desativar a reserva de espaço. A chave de registro está no seguinte local:

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine

DisableLunSpaceReservation =1

Especifica que as reservas de espaço de LUN estão desativadas.

Observação: isso é aplicável somente quando a licença FlexClone é aplicada.

Para obter mais informações, consulte Considerações sobre o suporte a iSCSI/FC do NetApp para VMware.

Assuntos relacionados ao modo de espera virtual

Esta seção inclui os seguintes tópicos de solução de problemas relacionados ao modo de espera virtual:

- Sistema operacional não encontrado
- Falha em tarefas no modo de espera virtual devido a erros internos
- Falha nas tarefas do modo de espera virtual usando o modo de transporte hotadd
- Falha em tarefas de modo de espera virtual para sistemas Hyper-V
- Problema relacionado à UUID duplicada do agente
- A opção recursos de EC2 do terminal não é exibida

Sistema operacional não encontrado

Válido em plataformas Windows.

Sintoma:

A mensagem abaixo é exibida quando há falha ao ligar uma máquina no modo de espera virtual:

Sistema operacional não encontrado.

Solução:

Esse comportamento pode ocorrer em máquinas virtuais que contenham dispositivos SCSI e IDE. Se esse problema ocorrer, examine a maneira como os discos estão configurados na máquina virtual e verifique se a sequência de inicialização da máquina virtual recuperada é igual à da máquina virtual de origem. Se a sequência de inicialização for diferente, atualize o BIOS na máquina virtual recuperada para corresponder ao da origem.

Observação: Use (0:1) para representar o primeiro disco IDE.

Falha em tarefas no modo de espera virtual devido a erros internos

Válido em sistemas operacionais Windows.

Sintoma 1:

Falha nas tarefas do Virtual Standby. Uma das seguintes mensagens é exibida no log de atividades:

Falha ao converter o disco virtual

Erro interno, entre em contato com o suporte técnico

Além disso, o VDDK relata a seguinte mensagem de erro:

Erro desconhecido.

Solução 1:

Para resolver esse problema, considere as seguintes soluções:

- É possível haver falha em operações de conversão quando não há espaço suficiente no repositório de dados especificado na diretiva do Virtual Standby. O VDDK retorna a mensagem, pois a API do VDDK, no momento, não oferece suporte ao recurso para detectar a quantidade de espaço livre em disco no repositório de dados. Para corrigir o problema, libere a quantidade de espaço em disco no repositório de dados original necessária para que a operação seja concluída e, em seguida, envie a tarefa novamente.
- Interferências e excesso de tráfego na rede podem causar falha nas operações de conversão. Para corrigir o problema, certifique-se de que o sistema do nó de origem e do ESX Server ou vCenter Server possam se comunicar pela rede e, em seguida, reenvie a tarefa.
- Várias conexões simultâneas que consistem em tarefas de backup ou de recuperação via VM para o sistema ESX Server ou vCenter Server, que inclui as conexões SDK do vSphere por meio do cliente vSphere para VMware, podem provocar a falha das tarefas. Para corrigir este problema, feche todas as conexões desnecessárias e, em seguida, reenvie a tarefa.

  Este problema é o resultado de uma limitação de conexão do VDDK da VMware. Os limites do protocolo NFC (Network File Copy) a seguir se aplicam:

  ESXi 5: limitado por um buffer de transferência para todas as conexões do NFC e imposto pelo host; a soma de todos os buffers de conexão do NFC a um host ESXi não pode exceder 32 MB. 52 conexões por meio do vCenter Server que inclui o limite por host.

Observação: as conexões não podem ser compartilhadas entre discos. Os limites máximos não se aplicam a conexões SAN e HotAdd. Se o cliente NFC não for desligado corretamente, as conexões podem permanecer abertas por dez minutos.

- Examine as seções de tarefas e eventos do log do cliente VMware vSphere para descobrir erros internos de uma máquina virtual específica. Corrija os erros internos e, em seguida, reenvie a tarefa.

  Exemplo: outro aplicativo ou operação está usando o arquivo VMDK. Para corrigir o problema, libere o arquivo e reenvie a tarefa.

Sintoma 2:

Falha nas tarefas do Virtual Standby. Uma das seguintes mensagens é exibida no log de atividades:

Falha ao converter o disco virtual

Erro interno, entre em contato com o suporte técnico

Além disso, o VDDK relata a seguinte mensagem de erro:

Open vmdk failed with error File not found.

Solução 2:

Esse problema pode ocorrer quando:

- O VDDK não pôde processar um instantâneo corretamente.
- O VDDK não pôde excluir o instantâneo manualmente ou ele é interno para a máquina virtual.

Para corrigir esse problema, envie a tarefa novamente. Caso a tarefa falhe novamente, exclua a máquina virtual recuperada e envie a tarefa novamente.

Sintoma 3:

Falha nas tarefas do Virtual Standby. Uma das seguintes mensagens é exibida no log de atividades:

Não é possível aplicar '<Plan Name>' ao nó '<Node Name>'. O serviço web do agente do Arcserve UDP no conversor "<Converter Name>" está ocupado. Tente novamente mais tarde.

Além disso, o arquivo de log do Console do UDP (ARCApp.log) relata a seguinte mensagem de erro:

[ERROR] deployVsbTask: falha ao chamar a API do serviço web D2D - tempo limite. javax.xml.ws.WebServiceException: java.net.SocketTimeoutException: tempo limite de leitura expirou

Solução 3:

Esse problema pode ocorrer devido ao tempo limite. Para corrigir esse problema, siga estas etapas:

1. Efetue logon no **Console do UDP** usando as credenciais apropriadas.
2. Abra a interface de linha de comando e execute o comando abaixo:

   regedit

   O Registro é aberto.
3. Vá até ***\SOFTWARE\Arcserve\Unified Data Protection\Engine\WebService***.
4. Verifique se a chave **timeoutValue** existe. Se a chave não existir, crie-a manualmente.

   Adicione/modifique a chave conforme abaixo:

   - **Nome da chave:** timeoutValue
   - **Valor:** <informe o valor em minutos>. Por exemplo, para definir o valor do tempo limite como 20 minutos, especifique 20 como o valor.
5. Saia do **regedit**.
6. Navegue até a pasta de instalação do **Console do UDP**. Por exemplo, *C:\Program Files\Arcserve\Unified Data Protection\Management\Configuration*.
7. Abra o arquivo **ConsoleConfiguration.xml** usando o bloco de notas.
8. Localize o texto abaixo na seção **<TimeoutConf>**:

   <webServiceRequestTimeout>600</webServiceRequestTimeout>
9. Altere o valor de **webServiceRequestTimeout** em segundos. Por exemplo, para definir o valor do tempo limite como 20 minutos, especifique 1200 como o valor.
10. **Salve** o arquivo e saia.
11. **Reinicie** o **serviço de gerenciamento do Console do UDP** para permitir a aplicação das configurações.
12. Reimplante o plano e verifique o resultado.

Falha nas tarefas do modo de espera virtual usando o modo de transporte hotadd

Válido em plataformas Windows.

Sintoma:

Falha das operações de recuperação ao recuperar dados usando o modo de transporte hotadd. A seguinte mensagem é exibida no log de atividades:

Ocorreu um erro desconhecido. Entre em contato com o Suporte técnico.

Além disso, o VDDK relata a seguinte mensagem de erro:

Erro desconhecido.

Solução:

As operações de recuperação falham ao usar o modo de transporte hotadd quando as configurações de disco não estiverem definidas corretamente.

Para configurar o disco, siga estas etapas:

1. Efetue logon no sistema proxy de backup usando uma conta com privilégios administrativos.

   Abra a linha de comando do Windows.

2. Na linha de comando, digite o seguinte comando:

   diskpart

   Pressione Enter.

   Digite SAN e, em seguida, pressione Enter.

   A diretiva atual da SAN é exibida.

3. Digite o seguinte comando:

   SAN POLICY = OnlineAll

   Pressione Enter.

   A diretiva da SAN está configurada para não montar automaticamente volumes hospedados pela SAN.

4. Para limpar o atributo de somente leitura do disco específico da SAN, selecione o disco a partir da lista de discos e digite o seguinte comando:

   attribute disk clear readonly

   Pressione Enter.

5. Digite exit e, em seguida, pressione Enter.

O disco está configurado e é possível enviar a tarefa novamente. Se a tarefa falhar novamente, monte os discos hotadd manualmente usando o gerenciamento de discos no sistema proxy.

Para montar os discos manualmente, siga estas etapas:

1. Efetue logon no sistema proxy de backup usando uma conta com privilégios administrativos.

   Abra o Painel de Controle do Windows e clique duas vezes em Ferramentas Administrativas.

   A janela Ferramentas Administrativas é exibida.

2. Na lista Favoritos, clique duas vezes em Gerenciamento do Computador.

   O Gerenciamento do computador é exibido.

3. Expanda Armazenamento e clique em Gerenciamento de Disco.

   Os discos são exibidos.

4. Clique com o botão direito no disco que deseja montar e clique em Online.

   O disco está montado e é possível enviar a tarefa novamente.

Falha em tarefas de modo de espera virtual para sistemas Hyper-V

Válido em sistemas operacionais Windows.

Sintoma:

A seguinte mensagem é exibida no log de atividades:

Falha na tarefa do modo de espera virtual ao obter a VM do Hyper-V.

Solução:

As tarefas do modo de espera virtual falham quando:

- O serviço web de modo de espera virtual não consegue recuperar informações sobre a máquina virtual a partir do sistema Hyper-V. Os problemas de comunicação entre o Arcserve UDP e o sistema Hyper-V ocorrem quando os serviços do Hyper-V necessários não estão em execução no sistema Hyper-V.

  Solução: Verificar se todos os serviços necessários do Hyper-V estão em execução no sistema Hyper-V.

- O sistema Hyper-V não contém a quantidade suficiente de espaço livre em disco necessária para criar a máquina no modo de espera virtual ou para criar seu instantâneo.

  Solução: Considerar a reconfiguração do sistema Hyper-V para liberar o espaço em disco suficiente no volume do sistema.

Observação: Se você detectar outras possíveis causas, entre em contato com o suporte do Arcserve.

Problema relacionado à UUID duplicada do agente

Sintoma:

Um monitor que existe no Console com a mesma UUID de agente precisa substituir a UUID do agente.

Solução:

1. No seu computador, execute o comando *regedit*.
2. Vá para *HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine*
3. Exclua os dados de valor de NodeID.
4. Reinicie o serviço do agente do Arcserve UDP.

As modificações na nuvem privada virtual em tarefas no modo de espera virtual não refletem no Amazon EC2

Sintoma:

Após executar uma tarefa no modo de espera virtual, se é feita uma modificação na VPC (Virtual Private Cloud - Nuvem Privada Virtual) nas configurações de rede da tarefa no modo de espera virtual para usar uma VPC da Amazon diferente para as tarefas subsequentes, as modificações não são atualizadas no Amazon EC2.

Solução

O Amazon EC2 não permite modificar a VPC no Console do UDP depois de executar uma tarefa no modo de espera virtual pelo menos uma vez. Como alternativa, o Arcserve UDP agora permite encerrar a instância antiga e criar uma nova instância com os dados existentes de sessões anteriores.

Siga estas etapas:

1. Configure um plano de backup com o VSB para EC2 como tarefa secundária.
2. Execute algumas tarefas do VSB para AWS com êxito.
3. Modifique as configurações de VPC na tarefa do VSB [configurações de rede].

   As configurações de VPC atualizadas são refletidas na instância depois da próxima tarefa de VSB com êxito.

Observações:

- A instância antiga criada no EC2 será ignorada e a nova instância com o VPC atualizado será criada no EC2 para refletir as alterações de rede.
- A nova configuração de rede também será aplicada aos instantâneos antigos.

A opção recursos de EC2 do terminal não é exibida

Sintoma:

Quando os nós são configurados com um plano que tem a tarefa de Modo de espera virtual para EC2 em UDP 7.0 U1, UDP 7.0 ou UDP 6.5 U4 e, se você atualizar o console para UDP 7.0 U2, a opção **Encerrar recursos do EC2** não será exibida para esses nós específicos.

Solução:

Clique na opção **Modificar** para o plano relacionado e salve.

Assuntos relacionados à cópia dos pontos de recuperação

Esta seção inclui os seguintes tópicos de solução de problemas relacionados à CRP (Copy to Recovery Points - Cópia de Pontos de Recuperação):

- Congestionamento de largura de banda com tarefas de cópia do ponto de recuperação para a nuvem
- Configurar o registro para tarefa de cópia de ponto de recuperação
- Tarefa de mesclagem ignorada

Configurar o registro para tarefa de cópia de ponto de recuperação

Sintoma

A tarefa de cópia de ponto de recuperação não foi executada.

Solução

É possível controlar o número de tarefas de repetição e o intervalo de tempo das tarefas de repetição para a tarefa de cópia para recuperação usando as chaves de Registro a seguir. A chave de Registro está no computador em que você instalou o Agente do UDP.

Tarefa de repetição para CRP

A chave de Registro está localizada no Agente do Arcserve UDP no seguinte local:

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFCopySession\nodename1

Adicione a nova chave conforme mencionado abaixo:

Nome da chave: MaxRetryCount

Tipo de chave: REG_DWORD

Valor: 1 como padrão e máximo (10)

Observação: esta atualização é aplicável a apenas um nó “nodename1”.

Para tarefas de cópia do ponto de recuperação para a nuvem, o Arcserve UDP usa um caminho temporário, que pode ser configurado com as chaves de Registro para o caminho Temp.

Configurar o caminho Temp

A chave do registro está localizada no Servidor de backup do Arcserve no seguinte local:

HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFCopySession

Nome da chave: LocalTempPath

Tipo de chave: REG_SZ

Observação: por padrão, ele armazena no caminho inicial do produto Arcserve.

Congestionamento de largura de banda com tarefas de cópia do ponto de recuperação para a nuvem

Sintoma

A execução de tarefas de cópia de pontos de recuperação (CRP) geralmente torna o computador do agente lento devido ao congestionamento de largura de banda.

Solução

O Arcserve ajuda a definir uma largura de banda específica para tarefas CRP. Como resultado, mesmo se o computador tiver várias tarefas em execução, a largura de banda é controlada automaticamente no computador do agente apenas para tarefas CRP. Usando um processo separado AFCRPBackend.exe para tarefas CRP, é possível configurar a QoS com base em diretiva para AFCRPBackend.exe e acelerar a largura de banda de saída.

Siga estas etapas:

1. Digite MMC na caixa Iniciar e pressione Enter.

   O Console de Gerenciamento Microsoft é aberto.

2. No MMC, pressione CTRL+M.

   A caixa de diálogo Adicionar ou Remover Snap-ins é aberta.

3. Na caixa de diálogo Adicionar ou Remover Snap-ins, selecione Editor de Objeto de Política de Grupo, em Snap-ins disponíveis, e clique em Adicionar.

4. Na caixa de diálogo Selecionar Objeto de Política de Grupo, deixe a configuração padrão do Computador Local e clique em Concluir.

5. Clique em OK.

   A caixa de diálogo Adicionar ou Remover Snap-ins é fechada.

6. No painel esquerdo da janela do MMC, expanda Computador Local, Configuração do Computador, Configurações do Windows e clique com o botão direito do mouse em QoS baseada em diretiva e selecione Criar Nova Política no menu.

7. Na janela de QoS baseada em diretiva, execute as seguintes opções e clique em Avançar:

   - Insira um nome para a nova diretiva.

   - Defina o valor de DSCP como 0.

   - Marque a caixa de seleção de Especificar Taxa de Aceleração de Saída.

   Observação: é recomendável selecionar MBps como opção.

8. Na opção Esta diretiva de QoS se aplica a:, marque a caixa de seleção Somente aplicativos com este nome executável, digite o seguinte caminho exe e clique em Avançar:

   C:\Arquivos de Programas\Arcserve\Unified Data Protection\Engine\BIN\AFCRPBackend.exe

   Observação: AFCRPBackend.exe ajuda a garantir que a restrição de largura de banda é aplicável apenas a tarefas CRP, mesmo que várias tarefas estejam em execução no computador do agente.

9. Prossiga com as configurações padrão na última tela e clique em Concluir.

Tarefa de mesclagem ignorada

Sintoma

- A tarefa de mesclagem foi ignorada porque a sessão está bloqueada pela tarefa de cópia de ponto de recuperação. Verifique se alguma tarefa de cópia de ponto de recuperação está pendente.
- A tarefa de mesclagem foi ignorada porque a sessão está bloqueada pela tarefa de cópia de ponto de recuperação sob demanda. A tarefa de cópia de ponto de recuperação sob demanda está em execução ou aguardando para ser executada.

Solução

Para dar continuidade à tarefa de mesclagem, é preciso remover os arquivos de bloqueio do destino de backup do nó.

Execute a ferramenta de remoção de bloqueio em *C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\AFDeleteLockTool.exe*.

Observação: essa ferramenta remove todos os bloqueios relacionados a CRP (programada e ad hoc), e a mesclagem é iniciada imediatamente. As sessões mescladas não estarão disponíveis para cópia de ponto de restauração no destino.

Utilização:

AFDeleteLockTool.exe -path <BackupDestinationPath> -user <USERNAME> -password <PASSWORD> -type <crp/adhoccrp>

Observações:

-path: especifica o caminho do destino de backup

-type: especifica o tipo da tarefa responsável pelo bloqueio

-crp: remove o bloqueio relacionado às tarefas programadas de CRP.

-adhoccrp: remove o bloqueio relacionado às tarefas ad hoc de CRP.

-user: especifica o nome de usuário para o destino de backup

-password: especifica a senha para o destino de backup

É obrigatório especificar os valores de -path e -type.

A especificação dos valores de -user e - password é opcional. (Ambos devem ser fornecidos ou ignorados, não é possível especificar só um deles.)

Exemplos:

- Se quiser remover apenas os bloqueios impostos por tarefas programadas de CRP, execute a ferramenta da seguinte forma:

  AFDeleteLockTool.exe -path I:/Backup/RPS678 -type crp

- Se quiser remover apenas os bloqueios impostos por tarefas ad hoc de CRP, execute a ferramenta da seguinte forma:

  AFDeleteLockTool.exe -path I:/Backup/RPS678 -user User123 -password "**********" -type crp

- Se quiser remover todos os bloqueios impostos por tarefas de CRP, execute a ferramenta da seguinte forma:

  AFDeleteLockTool.exe -path I:/Backup/RPS678 -user User123 -password "**********" -type crp -type adhoccrp

Relatórios relacionados do Arcserve UDP

Esta seção inclui os seguintes tópicos de solução de problemas relacionados aos relatórios do Arcserve UDP:

Como exibir os gráficos para visualizar relatórios do Arcserve UDP

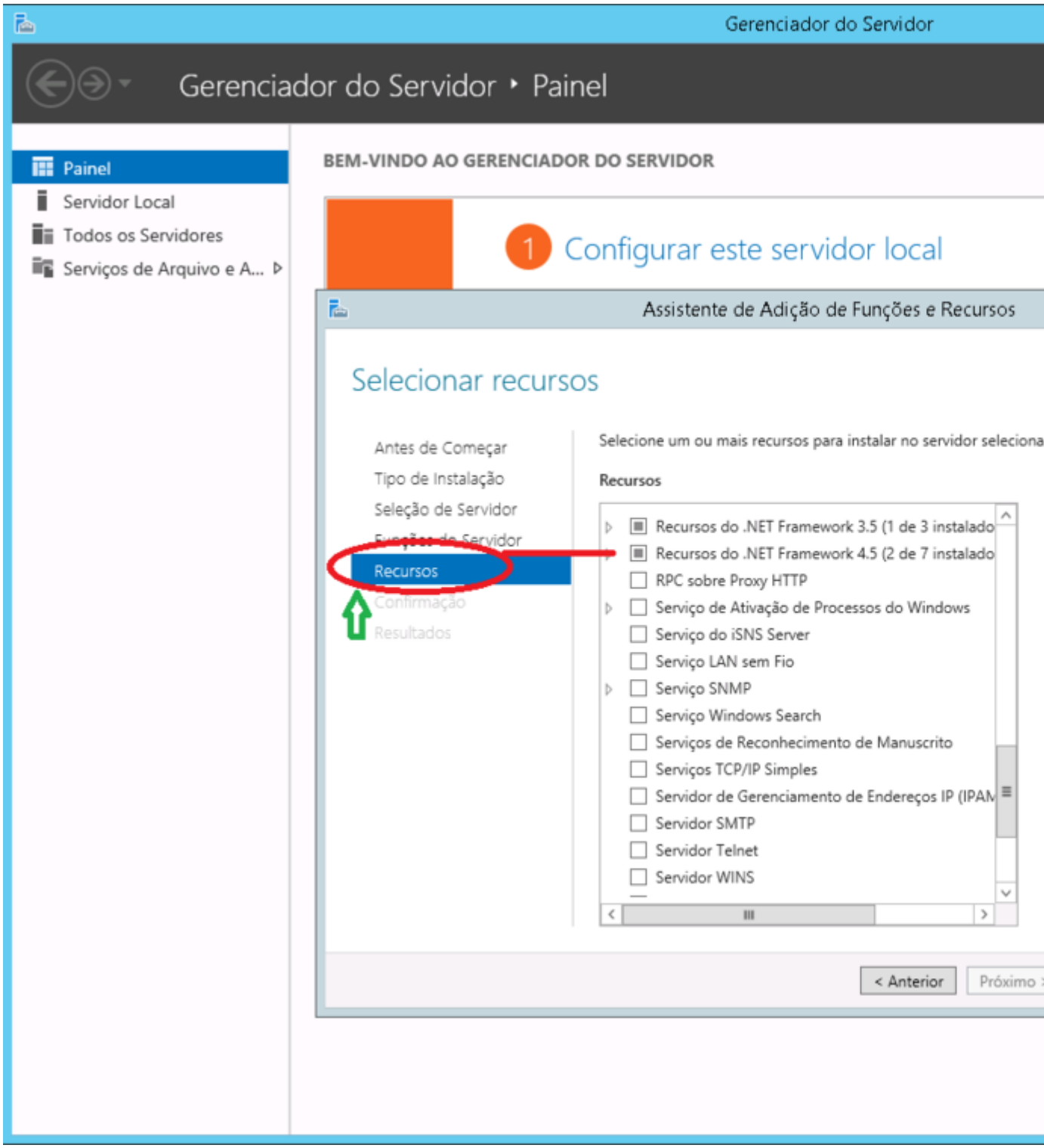
Como exibir os gráficos para visualizar relatórios do Arcserve UDP

Às vezes quando você deseja visualizar os relatórios, os gráficos não podem ser exibidos. Preencha o pré-requisito abaixo para solucionar o problema do Windows 2012/2012r2.

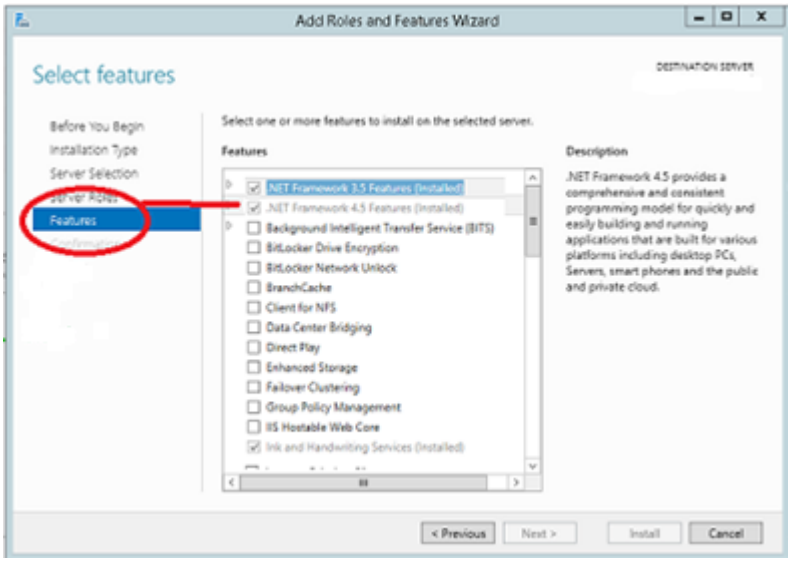
Para exibir os gráficos, é necessário instalar o .NET 3.5 Framework ou uma versão posterior.

Para instalar o .NET Framework, siga estas etapas:

1. Abra o Gerenciador de Servidores.
2. No painel, no canto superior direito, clique em **Gerenciar** e selecione a opção **Adicionar funções e recursos**.



3. Na caixa de diálogo Assistente para adicionar funções e recursos, faça o seguinte:
   a. No painel esquerdo, clique em **Recursos**.
   b. Na guia **Recursos**, marque a caixa de seleção **Recursos do .NET Framework 3.5 (instalados)**.
   c. Clique em **Avançar**.



4. Na tela Confirmar seleções de instalação, clique em **Instalar**.

   A instalação do .NET Framework foi concluída com êxito.

   Importante: mesmo após a implementação dos pré-requisitos, se os gráficos não forem exibidos usando as opções **Imprimir/email/salvar**, verifique se o Editor do Registro tem FCImgExportDll. Para verificar a dll, navegue até o seguinte caminho:

   C:\Arquivos de programas\Arcserve\Unified Data Protection\Management\BIN

   Para cancelar o registro e registrar FCImgExportDLL.dll, siga estas etapas:

   1. Navegue até o seguinte caminho no prompt de comando:

      C:\Windows\Microsoft.NET\Framework64\v4.0.30319

   2. Para cancelar o registro da DLL, execute o seguinte comando:

      C:\Windows\Microsoft.NET\Framework64\v4.0.30319>Regasm.exe /u "C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\FCImgExportDLL.dll"

   3. Para registrar a DLL, execute o seguinte comando:

      C:\Windows\Microsoft.NET\Framework64\v4.0.30319>Regasm.exe "C:\Program Files\Arcserve\Unified Data Protection\Management\BIN\FCImgExportDLL.dll" /codebase

Assuntos relacionados ao Exchange Online do Microsoft Office 365

Esta seção inclui os seguintes tópicos de solução de problemas relacionados ao Microsoft Office 365 Exchange Online:

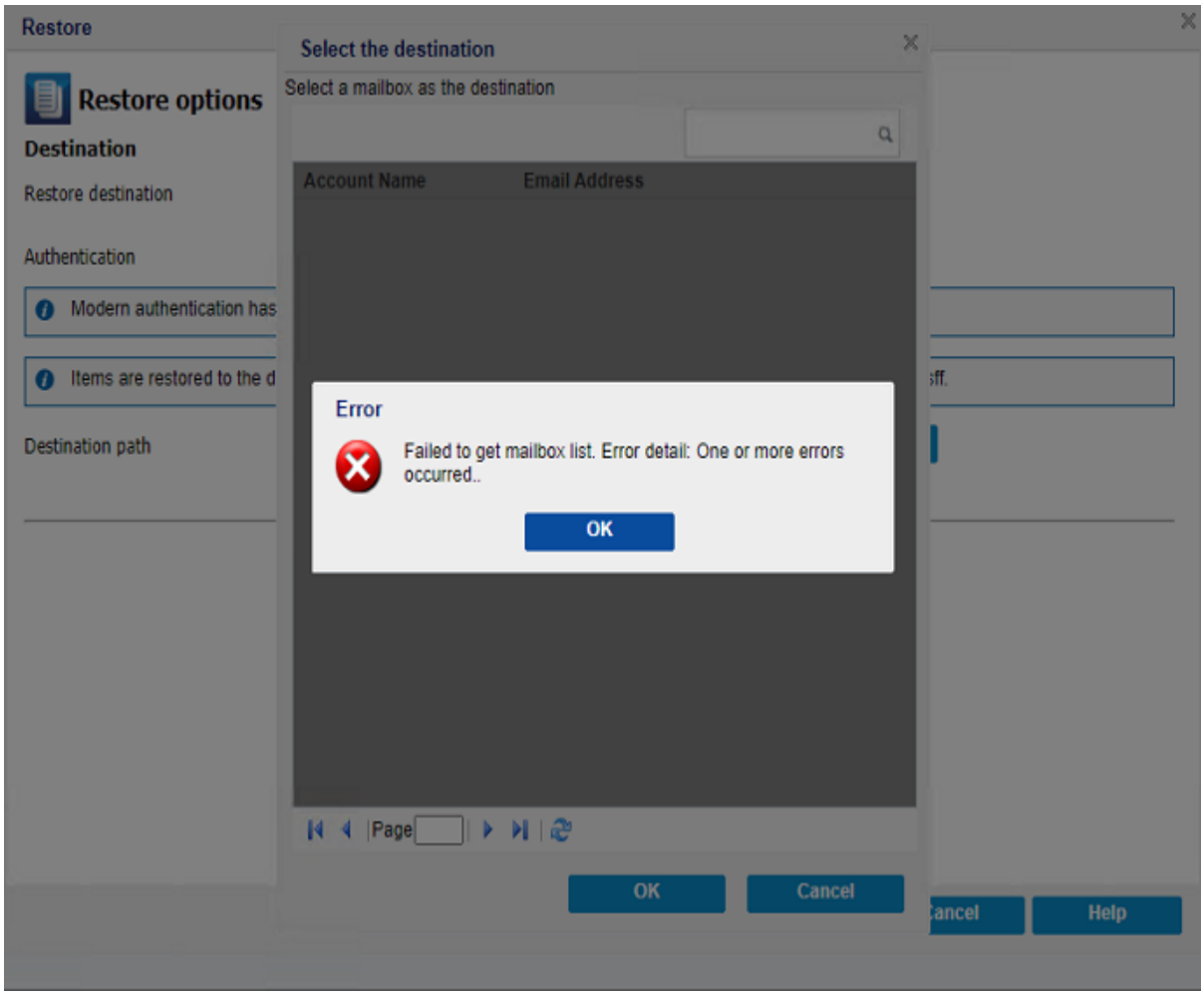
- Não é possível exibir a lista de caixas de correio no diálogo *Selecionar o destino*
- Acesso ou permissão negada para o grupo do Exchange Online

Não é possível exibir a lista de caixas de correio no diálogo *Selecionar o destino*

Sintoma:

Ao definir as opções de restauração, a caixa de diálogo Selecionar o destino não exibe a lista de caixas de correio. Quando você restaura os dados de correio em um local alternativo usando a autenticação existente e clica no botão Procurar para selecionar um destino, a seguinte mensagem de erro é exibida:

Falha ao obter a lista de caixas de correio. Detalhe do erro: ocorreu um ou mais erros.



Solução:

Para resolver esse erro, carregue um certificado válido para o Azure Portal com a ID do aplicativo especificada. Para obter mais informações, consulte Como usar o certificado autoassinado.

Acesso ou permissão negada para o grupo do Exchange Online

Sintoma:

Quando não há caixa de correio anexada ao grupo privado das equipes, a seguinte mensagem de erro é exibida:

Falha de backup da caixa de correio [abcd-pvt-group]: acesso negado

Solução:

Para resolver esse problema, siga estas etapas:

1. Crie uma caixa de correio compartilhada:
    a. Vá para a página de logon da Microsoft e faça logon na conta de administrador do Microsoft Office 365.
    b. Navegue até a página do centro de administração do Exchange Online.
    c. Em Painel, vá para **destinatários** > **compartilhados**.
    d. Clique em **+** para adicionar ou criar uma caixa de correio compartilhada.
2. Defina uma senha e atribua a licença do Office 365 para a caixa de correio compartilhada:
    a. Retorne à conta de administrador do Office 365.
    b. Vá para **Usuários** > **Usuários ativos** e selecione a caixa de correio compartilhada.
    c. Defina a senha e atribua a licença do Office 365.
3. Adicione a caixa de correio compartilhada como o membro do grupo privado:
    a. Navegue até a página do centro de administração do Exchange Online e, em Painel, clique em **Grupos**.
    b. Selecione a caixa de correio privada e clique em **Editar**.
    c. Na página Editar configurações, adicione a caixa de correio compartilhada como o membro do grupo e clique em **Salvar**.
4. Adicione a caixa de correio compartilhada para o administrador global:
    a. Vá para o Portal do Azure.
    b. Navegue até a seção Funções e selecione a função Administrador global.
    c. Clique em **Adicionar atribuições**, selecione a caixa de correio compartilhada e clique em **Salvar**.
5. No console do UDP, atualize o nó com o endereço de email da caixa de correio compartilhada e execute novamente a tarefa de backup.
6. Verifique se a tarefa de backup foi concluída com êxito.

Capítulo 13: Apêndice

Esta seção contém os seguintes tópicos:

Ferramenta de linha de comandos para o repositório de dados de redução de redundância

A ferramenta de linha de comandos (as_gddmgr.exe) permite verificar a integridade dos dados no nível do ponto de recuperação e no nível do repositório de dados para os repositórios de dados de redução de redundância.

Você também pode usar essa ferramenta para recriar um banco de dados de hash, em caso de uma falha do banco de dados de hash. Também é possível usar essa ferramenta para consultar e gerenciar a limpeza de back-end e disco de recuperação para armazenamentos de dados de redução de redundância.

A saída do comando é exibida no console de comando do Windows. A ferramenta também gera um arquivo de log na pasta "Logs". Por exemplo, as_gddmgr_2014-9-4_11-14-22-655.log é um arquivo de log que contém todos os detalhes.

Observação: todos os comandos da ferramenta de linha de comando (as_gddmgr.exe) também oferecem suporte ao armazenamento de dados de volume GUID. Por exemplo, *-scan VerifyAll <armazenamento de dados de volume GUID> [-Password < senha do armazenamento de dados >]*.

Local:

É possível encontrar o arquivo as_gddmgr.exe na pasta "Bin" do caminho de instalação do UDP.

Sintaxe:

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>

Opções:

CheckRecoveryPoint

Reidrata o(s) ponto(s) de recuperação especificado(s) como completo e, em seguida, verifica a integridade dos dados.

O nó <Todos> | <nome do nó do agente do UDP>

Especifica o nome do nó do agente.

RecoveryPoint <Todos> | <número do ponto de recuperação>

Especifica o ponto de recuperação para a verificação de integridade.

Senha <senha do repositório de dados>

Especifica a senha do repositório de dados.

LogLevel <n>

Especifica o número de níveis de log.

VerifyRefCount

Verifica arquivos de índice e arquivos de referência para verificar a contagem de referência registradas no banco de dados de hash. Antes de especificar esta opção, interrompa manualmente o repositório de dados de redução de redundância.

VerifyData

Verifica os arquivos de dados e, em seguida, recria as chaves de hash por meio da comparação delas com o arquivo de referência. Antes de especificar esta opção, interrompa manualmente o repositório de dados de redução de redundância.

VerifyAll

Executa as operações e VerifyRefCount e VerifyData. Antes de especificar esta opção, interrompa manualmente o repositório de dados de redução de redundância.

RebuildHash

Especifique o nome do repositório de dados e, em seguida, gere novamente o banco de dados de hash verificando o índice e os arquivos de referência. Antes de especificar esta opção, interrompa manualmente o repositório de dados de redução de redundância.

RebuildHashWithIndexPath

Especifique o caminho do índice de redução de redundância e, em seguida, gere novamente o banco de dados de hash verificando o índice e os arquivos de referência. A opção é usada apenas quando o repositório de dados não está presente em quaisquer servidores de ponto de recuperação.

Iniciar

Permite executar a eliminação e a recuperação de disco em paralelo com outras tarefas regulares do Arcserve UDP. A execução de eliminação em paralelo pode prejudicar a taxa de transferência de tarefas regulares do Arcserve UDP.

Interromper

Desativa a execução da eliminação e a recuperação de disco em paralelo com outras tarefas regulares do Arcserve UDP.

Status

Consulta o status da eliminação e a recuperação de disco.

StartToReclaim

Permite executar a eliminação e a recuperação de disco em paralelo com outras tarefas do Arcserve UDP regulares. Essa opção ignora a fase de identificação de dados obsoletos, que descobre o bloco de dados obsoletos e inicia diretamente a fase de recuperação de disco, que libera o espaço em disco. O efeito colateral dessa opção é que pode degradar a eficiência da recuperação do disco porque a fase de identificação de dados obsoletos pode descobrir mais blocos de dados obsoletos nos arquivos de dados, mas a recuperação do disco não aguarda a conclusão da fase de identificação de dados obsoletos. Além disso, a execução de eliminação em paralelo pode prejudicar a taxa de transferência de tarefas regulares do Arcserve UDP.

StartToIdentifyObsoletedData

Permite executar a eliminação e a recuperação de disco em paralelo com outras tarefas regulares do Arcserve UDP. Essa opção inicia a fase de identificação de dados obsoletos. A opção será útil se o usuário desejar ignorar a fase de recuperação de disco em andamento.

Observação: lembre-se de que as seguintes opções podem ser executadas por um longo tempo, já que a operação verifica diversos arquivos no repositório de dados de redução de redundância.

- VerifyRefCount
- VerifyData
- VerifyAll

- RebuildHash
- RebuildHashWithIndexPath

Exemplos:

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

Como exibir a opção Verificação de ponto de recuperação

No Arcserve UDP 7.0, a função de verificação de ponto de recuperação é ocultada por padrão pelo assistente de plano. É recomendável usar a tarefa de recuperação garantida para detectar o possível problema de dados. É recomendável usar a tarefa de recuperação garantida para detectar o possível problema de dados. Para obter detalhes, consulte Como configurar a recuperação garantida. Se necessário, você ainda pode usar esta opção para executar a verificação de dados e visualizá-los no assistente de plano.

Siga estas etapas:

1. Efetue logon no Console do UDP.
2. Navegue até a pasta de instalação do Console do UDP. Por exemplo, *C:\Program Files\Arcserve\Unified Data Protection\Management\Configuration*.
3. Abra o arquivo ConsoleConfiguration.xml usando um editor de texto.
4. Localize o texto abaixo na seção <TimeoutConf>:

   <recoveryPointCheck>false</recoveryPointCheck>
5. Altere o valor de false para true.
6. Salve o arquivo e saia.
7. Reinicie o serviço de gerenciamento do console do UDP para permitir a aplicação das configurações.

   Observação: a versão do Arcserve UDP é atualizada a partir da versão anterior, e essa opção já está selecionada em um plano, não estando oculta por padrão.

   Essa opção permite detectar problemas de corrupção de dados por meio da verificação do sistema de arquivos dos volumes. Quando a tarefa de backup é concluída, o Arcserve UDP monta o ponto de recuperação e executa o comando chkdsk do Windows. Se o comando chkdsk detectar um erro, a próxima tarefa de backup será convertida em uma tarefa de backup de verificação. Essa opção se aplica a máquinas virtuais VMware e Hyper-V com o sistema operacional convidado do Windows. Consulte as considerações a seguir antes de ativar essa opção:

   - Os seguintes tipos de volume não são suportados,e são ignorados pela **Verificação do ponto de recuperação**:
     - O volume cujo tipo de sistema de arquivos não é NTFS
     - O volume cujo tipo é listrado com paridade
     - O volume que está naquele pool de armazenamento

- O comando chkdsk não pode detectar todos os problemas do sistema de arquivo. A verificação do ponto de recuperação pode passar, mas o ponto de recuperação ainda pode estar corrompido.
- Dependendo do tamanho do sistema de arquivos do sistema operacional convidado, o comando chkdsk pode demorar mais tempo a ser executado. O chkdsk utiliza uma grande quantidade de memória do sistema no servidor proxy de backup e afeta o desempenho do servidor proxy. Isso resulta em mais tempo para completar a tarefa de backup. *No pior caso, a memória do sistema do servidor proxy de backup poderá se esgotar e o servidor poderá parar de responder, especialmente quando houver várias tarefas simultâneas de backup.* A Verificação do ponto de recuperação em si pode monitorar o uso de memória do sistema e, se o uso de memória atingir um limite, a verificação de ponto de recuperação se suspenderá por algum tempo e liberará alguma memória do sistema. Contudo, como prática recomendada, desative essa opção, a menos que seja ela necessária ou que você tenha um servidor proxy de backup robusto. Como alternativa, você pode distribuir a carga em vários servidores proxy criando vários planos e especificando diferentes servidores proxy em cada plano.
- Se o backup travar de forma consistente, há chances altas de o chkdsk detectar problemas (devido à natureza de um backup consistente travado). Como prática recomendada, não ative essa opção para um backup consistente travado.
- Se você desejar ativar a opção de verificação do ponto de recuperação, mas não desejar que a próxima tarefa de backup seja convertida em uma tarefa de backup de verificação, crie um valor de DWORD chamado CheckRecoveryPointIgnoreError no registro do servidor proxy e defina o valor de DWORD como 1. Crie o valor DWORD no seguinte local:

  [HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll]

  O valor de DWORD é aplicável a todas as tarefas de backup em execução no servidor proxy atual. Se desejar controlar o comportamento de uma máquina virtual específica, você pode definir o valor no seguinte local:

  HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<VM GUID>.

  Observação: se você adicionar ao registro uma chave no nível de VM e outra no nível proxy, a configuração do registro no nível de VM terá prioridade sobre a configuração no nível de proxy.

- Se você deseja interromper a tarefa de backup depois que a verificação do ponto de recuperação detectar o problema (de modo que você possa ficar ciente do problema de dados imediatamente), crie um valor DWORD chamado CheckRecoveryPointDontFailJob no registro do servidor proxy e defina o valor DWORD como 0. Crie o valor DWORD no seguinte local:

  HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll

  O valor de DWORD é aplicável a todas as tarefas de backup em execução no servidor proxy atual. Se desejar controlar o comportamento de uma máquina virtual específica, você pode definir o valor no seguinte local:

  HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine\AFBackupDll\<VM GUID>.

  Observação: se você adicionar ao registro uma chave no nível de VM e outra no nível proxy, a configuração do registro no nível de VM terá prioridade sobre a configuração no nível de proxy.

Como aplicar versão diferente do VDDK da versão integrada no Arcserve UDP

O VDDK (VMware Virtual Disk Development Kit - Kit de Desenvolvimento do Disco Virtual da VMware) 6.7.1 é integrado com o Arcserve UDP 7.0. Ao mesmo tempo, o Arcserve UDP 7.0 é compatível com o VDDK 5.5. Se desejar executar VSB/VM instantânea/Recuperação garantida para o VMware 5.0 ou 5.1, use o VDDK 5.5 em vez do VDDK 6.7.1.

Importante: A Arcserve certifica apenas o VDDK 6.7.1 e 5.5. Não há garantia de que outras versões do VDDK funcionem com a versão 7.0 do Arcserve UDP.

Para alterar o VDDK manualmente, siga estes procedimentos:

- Altere o VDDK para o backup no modo de espera virtual (VSB)
- Altere o VDDK para o backup com base em host (HBBU)

Modificando o VDDK manualmente para o backup no modo de espera virtual (VSB)

Você pode modificar o VDDK manualmente ou usando o arquivo em lotes do Windows. Este tópico explica os procedimentos para ambas as opções.

Considerações:

- Para a VM instantânea e o teste de recuperação garantida, é necessário executar esta ação no servidor proxy/servidor de recuperação.
- Para VSB para VMware, use um servidor do agente dedicado como monitor VSB e configure a tarefa VSB no modo proxy. Em seguida, alterne manualmente o VDDK para a versão 5.5 no servidor do monitor VSB.
- Se a tarefa VSB estiver configurada em um plano do MSP ou em um plano em vários locais, alterne o VDDK no servidor RPS, pois o servidor do monitor não está presente. Como resultado, este servidor RPS não está disponível para uso como um servidor proxy para tarefas de backup sem agente com base em host.

Para alterar o VDDK manualmente, siga estas etapas:

1. Efetue logon no computador no qual o agente do Arcserve UDP está instalado usando uma conta administrativa ou uma conta com privilégios administrativos.
2. Renomeie a pasta *VDDK* para VDDK6.7.
3. Renomeie a pasta *VDDK5.5* para VDDK no seguinte local padrão:

C:\Arquivos de programas\Arcserve\Unified Data Protection\engine\BIN

Observação: o local da pasta BIN pode variar dependendo do local onde você instalou o agente do Arcserve UDP.

4. Execute o seguinte comando para verificar o estado do serviço:

   Observação: você precisa excluir o serviço, mas somente quando ele não estiver no status de execução.

   sc query vstor2-mntapi20-shared

   Se o serviço não existir, exclua usando a próxima etapa. Se o serviço estiver em execução, antes de excluir usando a próxima etapa, execute o seguinte comando para interrompê-lo:

   sc stop vstor2-mntapi20-shared

5. Execute o seguinte comando para excluir o serviço:

   sc delete vstor2-mntapi20-shared

6. Execute o seguinte comando para verificar se o serviço foi excluído com êxito:

   sc query vstor2-mntapi20-shared

   Observação: se o estado do serviço for STOP_PENDING, reinicie o computador.

   Para alterar o VDDK usando um arquivo em lotes do Windows, siga estas etapas:

1. Efetue logon no computador no qual o agente do Arcserve UDP está instalado usando uma conta administrativa ou uma conta com privilégios administrativos.
2. Inicie a ferramenta de utilitário *ChangeToVDDK55.bat* no seguinte local padrão:

   C:\Arquivos de programas\Arcserve\Unified Data Protection\Engine\BIN

   Observação: o local da pasta BIN pode variar dependendo do local onde você instalou o agente do Arcserve UDP.

   O VDDK 5.5 é instalado após a inicialização de uma nova tarefa.

Modificando o VDDK manualmente para o backup com base em host (HBBU)

É possível modificar manualmente o VDDK para o backup com base em host (HBBU).

Modificar o VDDK 6.7 para backup do vSphere 5.5 ou posterior:

Siga estas etapas:

1. Faça download do VDDK do site da VMware.
2. Extraia todos os arquivos para uma pasta temporária.
3. Localize a pasta chamada ***bin***, que está disponível no caminho abaixo e renomeie a pasta (por exemplo, *bin_old*):

   <Caminho de instalação do Arcserve UDP>\Engine\BIN\VDDK\BIN\VDDK64\

   Exemplo: C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\VDDK\BIN\VDDK64\
4. Localize a pasta chamada ***bin*** nos arquivos extraídos na pasta temporária e copie-a no caminho abaixo:

   <Caminho de instalação do Arcserve UDP>\Engine\BIN\VDDK\BIN\VDDK64\.

   O VDDK é modificado com êxito.

Modificar o VDDK 5.5 para backup do vSphere 5.0 e 5.1:

Siga estas etapas:

1. Faça download do VDDK do site da VMware.
2. Extraia todos os arquivos para uma pasta temporária.
3. Localize a pasta chamada ***bin***, que está disponível no caminho abaixo e renomeie a pasta (por exemplo, *bin_old*):

   <Caminho de instalação do Arcserve UDP>\Engine\BIN\VDDK5.5\BIN\VDDK64\

   Exemplo: C:\Program Files\Arcserve\Unified Data Protection\Engine\BIN\VDDK5.5\BIN\VDDK64\
4. Localize a pasta chamada ***bin*** nos arquivos extraídos na pasta temporária e copie-a no caminho abaixo:

   <Caminho de instalação do Arcserve UDP>\Engine\BIN\VDDK5.5\BIN\VDDK64\.

   O VDDK é modificado com êxito.

Como migrar os dados de backup do Arcserve D2D r16.5 dos dois servidores com o mesmo nome de host para o repositório de dados do RPS

Você tem dois servidores com o mesmo nome de host, mas com nomes FQDN DNS diferentes e usa o Arcserve D2D r16.5 para protegê-los. Agora, se você deseja migrar os dados para o repositório de dados RPS do Arcserve UDP, siga estas etapas:

1. Interrompa o serviço do Arcserve D2D no servidor 1.
2. Usando a tarefa de início rápido do Arcserve UDP, migre dados do servidor 1 para o repositório de dados do RPS.
3. Atualize o agente do Arcserve UDP no servidor 1.
4. Crie um plano (ou por meio de um plano existente) para proteger o servidor 1 e escolha o mesmo armazenamento de dados RPS como destino de backup.
5. Implante o plano.
6. Interrompa o serviço do Arcserve D2D no servidor 2.
7. Usando a tarefa de início rápido do Arcserve UDP, migre dados do servidor 2 para o repositório de dados do RPS.
8. No servidor de RPS, vá até a pasta de destino de backup de repositório de dados e localize a pasta para o servidor 2, pesquisando o nome do host do servidor 2.

   Por exemplo, se o nome do host do servidor 2 for "MyServer2", o nome da pasta é "MyServer2".
9. Atualize o agente do Arcserve UDP no servidor 2.
10. No servidor 2, inicie o agente de UDP se não estiver iniciado.
11. Abra o registro (em qualquer servidor específico) e localize a seguinte chave:

    HKEY_LOCAL_MACHINE\SOFTWARE\Arcserve\Unified Data Protection\Engine”
12. Anote o valor de “NodeID”.

    O valor é uma ID exclusiva no formato de GUID, como “e856e0ba-66d7-4da5-8b98-2250173e349a”.
13. No servidor de RPS, localize a pasta de destino de backup do servidor 2 e atualize a ID do nó como **<nome_da_pasta> [valor NodeID]**.

    Exemplo: MyServer2[e856e0ba-66d7-4da5-8b98-2250173e349a]

14. Crie um plano (ou use um já existente) para proteger o servidor 2 e escolha o mesmo repositório de dados RPS como destino de backup.
15. Implante o plano.

Como implantar o Arcserve UDP no Microsoft Azure

É possível implantar o Arcserve UDP no Microsoft Azure ao usar o Arcserve Unified Data Protection v 6.5 Atualização 2 ou superior. O recurso ajuda você a implantar as máquinas do Modo de espera virtual no Microsoft Azure e proteger os dados. Uma máquina do modo de espera é criada no Microsoft Azure e os dados são relacionados com base nos pontos de recuperação do backup local.

O modo de espera virtual converte os pontos de recuperação em formatos de máquina virtual no Microsoft Azure e prepara um instantâneo para recuperar os dados com facilidade quando necessário.

Esse recurso oferece a capacidade de alta disponibilidade, garantindo que a máquina virtual assuma o controle imediatamente quando o computador de origem falhar. A máquina virtual em modo de espera é criada pela conversão dos pontos de recuperação no formato de máquina virtual do Azure.

O que fazer a seguir?

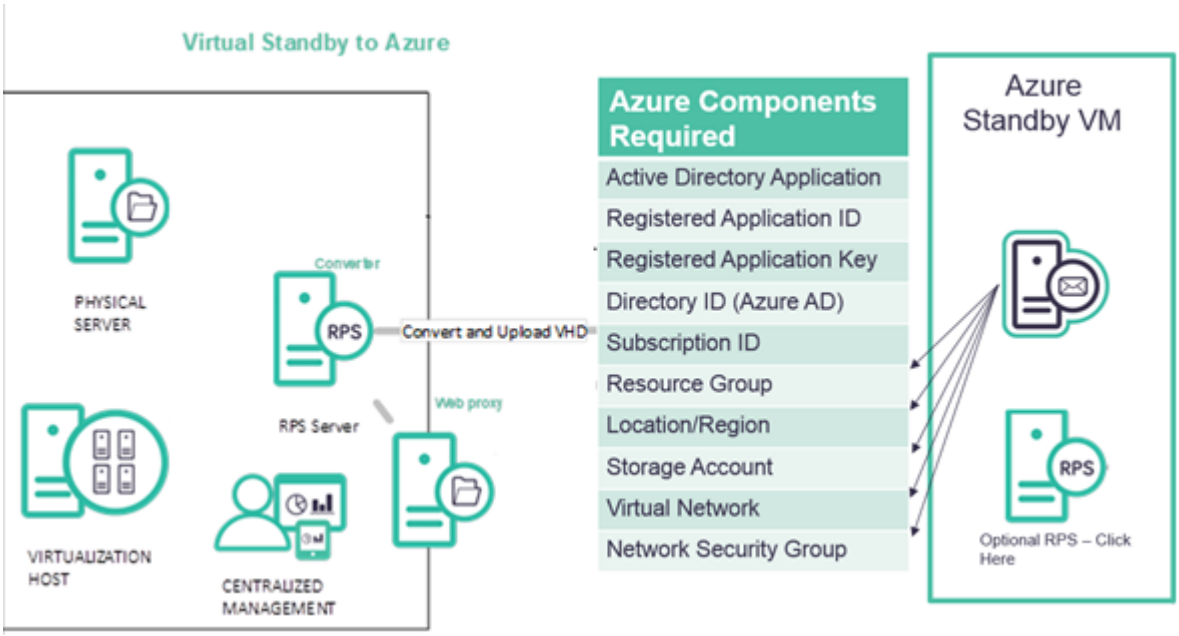
1. Entendendo o fluxo de processos
2. Práticas recomendadas
3. Considerações
4. Planejando a implantação
5. Implantar o Arcserve UDP no Microsoft Azure

Entendendo o fluxo de processos

O Arcserve UDP oferece suporte a máquinas virtuais no modo de espera virtual no Microsoft Azure. Se você já implantou a solução de proteção de dados no local, é possível implantar o Arcserve UDP no Microsoft Azure.

A solução no local é composta pelo console do Arcserve UDP e pelo RPS (Recovery Point Server - Servidor de Ponto de Recuperação) do Arcserve UDP. É possível fazer backup de sistemas do Windows para o RPS local. É possível criar um plano no console do Arcserve UDP para fazer backup dos dados no RPS local e, em seguida, executar a tarefa no modo de espera virtual. O recurso de modo de espera virtual acompanha o sinal de monitoramento do nó de origem. Se o nó de origem estiver desativado, a máquina virtual no Azure assume o controle.

A imagem a seguir mostra o fluxo de processos do Arcserve UDP para o Microsoft Azure:



Considerações

Revise as seguintes considerações antes de implantar o Arcserve UDP para Microsoft Azure:

Observação: para obter mais informações sobre as práticas recomendadas, consulte Implantar o Arcserve UDP no Microsoft Azure.

- No Microsoft Azure, nenhum arquivo VHD pode ter um disco do sistema com mais de 2.048 GB e um disco de dados com mais de 4.095 GB. No modo de espera virtual do Arcserve UDP, a origem não pode ter um disco do sistema com mais de 2.048 GB e um disco de dados com mais de 4.095 GB.
- A VM do Microsoft Azure e o VSB do Arcserve UDP oferecem suporte apenas ao sistema operacional Windows 2008 R2 ou superior.
- O Arcserve UDP não oferece suporte à criação de máquina virtual clássica como VM no modo de espera.
- A VM do Microsoft Azure requer que o volume do sistema e o volume de inicialização estejam no mesmo disco.
- O Microsoft Azure não oferece suporte para a inicialização da máquina a partir do sistema UEFI.
- O Microsoft Azure não oferece suporte para a máquina de origem como o servidor Hyper-V.

- O modo de espera virtual do Arcserve UDP não oferece suporte ao disco do sistema dinâmico da máquina de origem.
- O Arcserve UDP no Microsoft Azure oferece suporte apenas a nós do Windows.

Planejando a implantação do Arcserve UDP no Microsoft Azure

É necessário concluir as tarefas a seguir antes de implantar o Arcserve UDP no Microsoft Azure:

1. Verificar pré-requisitos
2. Preparar uma conta de nuvem no Microsoft Azure
3. Preparar recursos do Microsoft Azure

Pré-requisitos

Revise os pré-requisitos a seguir para o Arcserve UDP e o Servidor de ponto de recuperação antes de implantar o Arcserve UDP no Microsoft Azure:

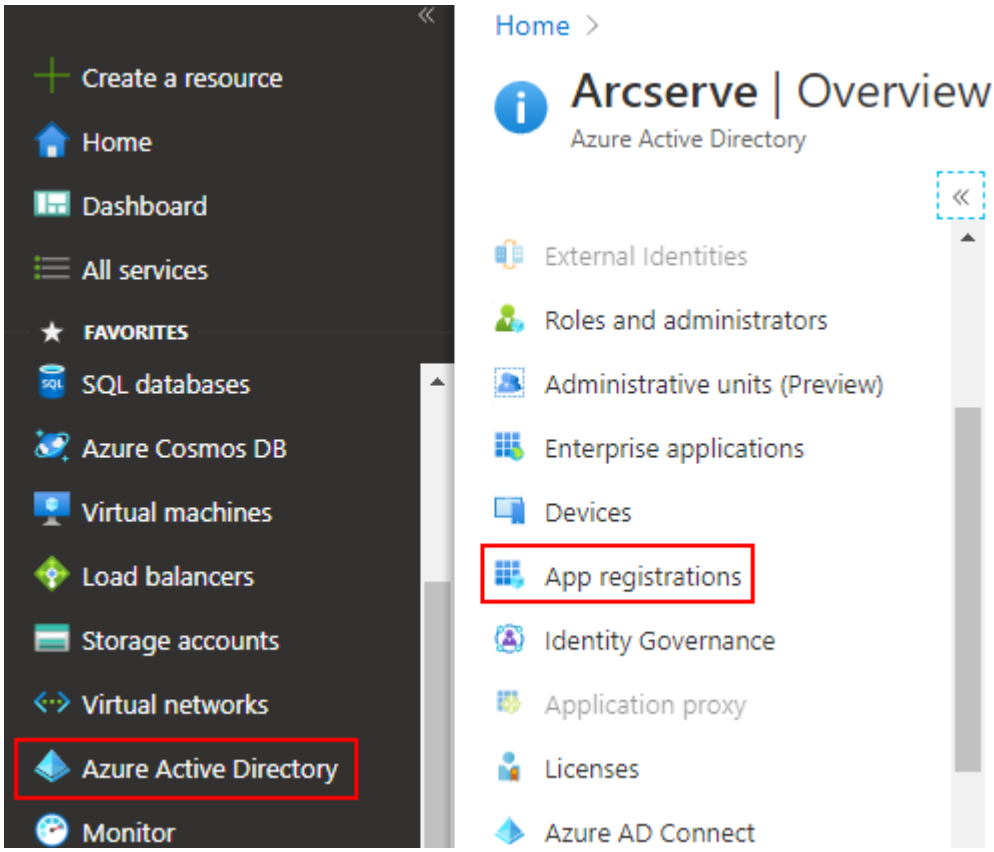
- Consulte a Matriz de compatibilidade para obter informações sobre os sistemas operacionais, os navegadores e os bancos de dados com suporte.
- Prepare os servidores antecipadamente para implantação como servidor de ponto de recuperação e console do Arcserve UDP.
- Os servidores para cada componente devem atender aos seguintes requisitos do sistema:
  - **Servidor:** Windows 2008 R2 Server ou superior
  - **CPU:** 4 Core 2.7 GHz, no mínimo
  - **Espaço em disco:** 40 GB para a instalação do sistema operacional
  - **RAM:** mínimo de 8 GB
  - **Armazenamento de backup para o Servidor de ponto de recuperação:** com base no tamanho dos dados de origem

Preparar uma conta de nuvem no Microsoft Azure

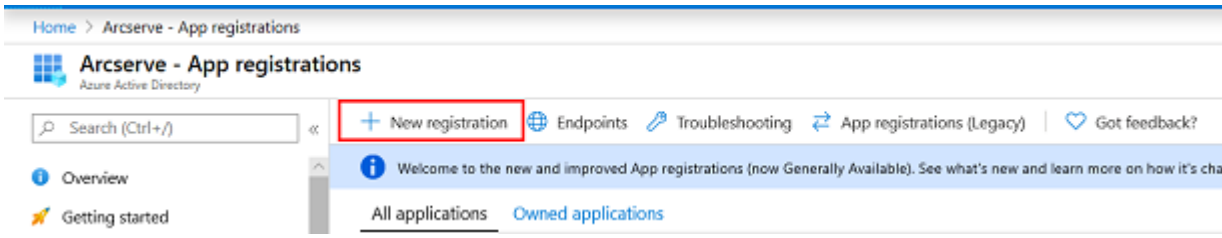
Esta seção fornece informações sobre como criar uma conta de nuvem no Microsoft Azure.

Siga estas etapas:

1. Execute as seguintes etapas para registrar o aplicativo Azure Active Directory usado pelo Arcserve UDP para se comunicar com o Microsoft Azure:
   a. Efetue logon no portal do Azure.
   b. No painel à esquerda, selecione **Azure Active Directory** e clique em **Registros do aplicativo**.

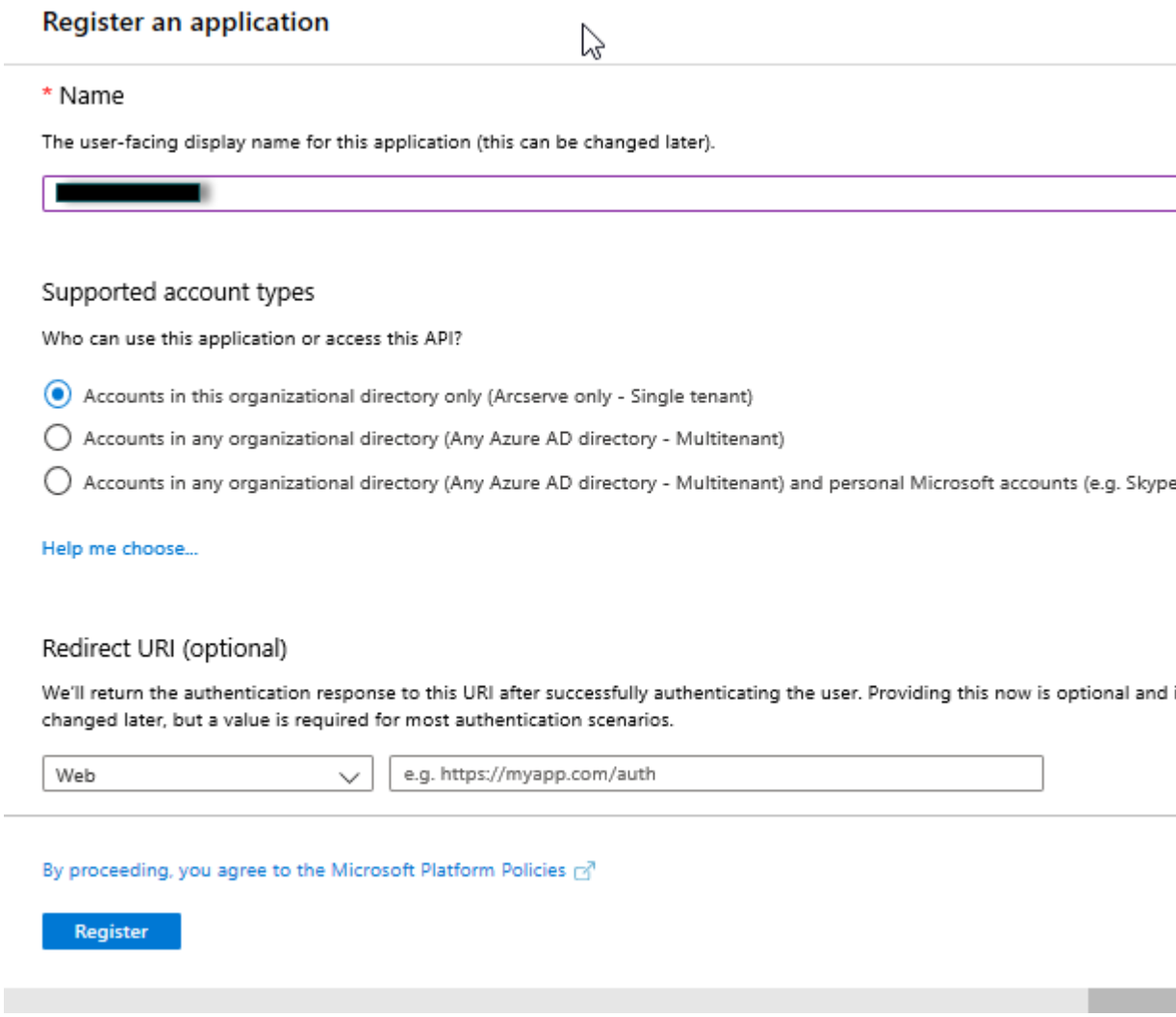


   c. Na página de registros do aplicativo Arcserve, clique em **Novo registro**.

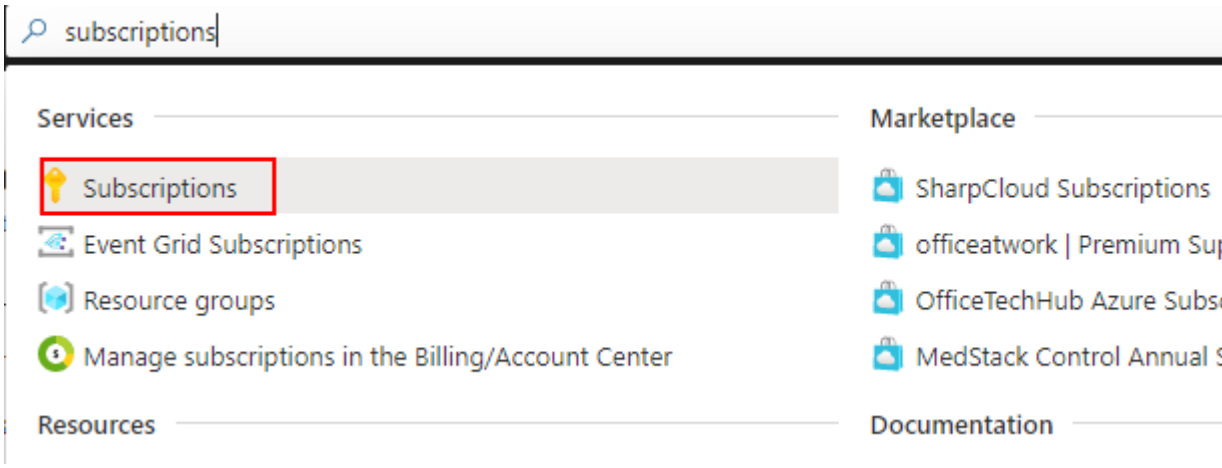


   d. Na página Registrar um aplicativo, siga as etapas abaixo e clique em **Registrar**:

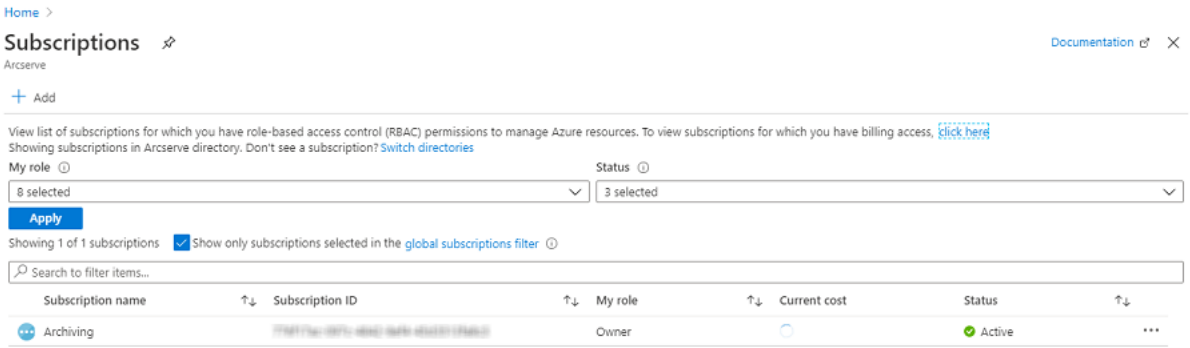
- Nome - Digite um nome para o aplicativo.
- Tipos de conta com suporte - Selecione um tipo de conta com suporte que determina quem pode usar o aplicativo.
- URI de redirecionamento (opcional): selecione **Cliente web ou público (dispositivo móvel e desktop)** para o tipo de aplicativo que você está criando e digite o URI de redirecionamento para o aplicativo.



e. Na barra de pesquisa, digite "assinaturas" e, em seguida, clique em **Assinaturas** na lista.

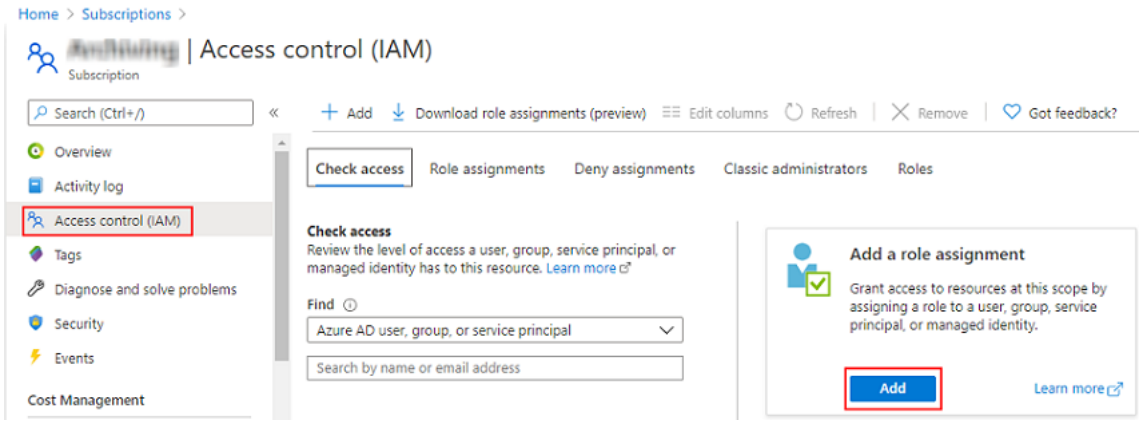


f. Nas páginas Assinaturas, selecione a assinatura do seu aplicativo.



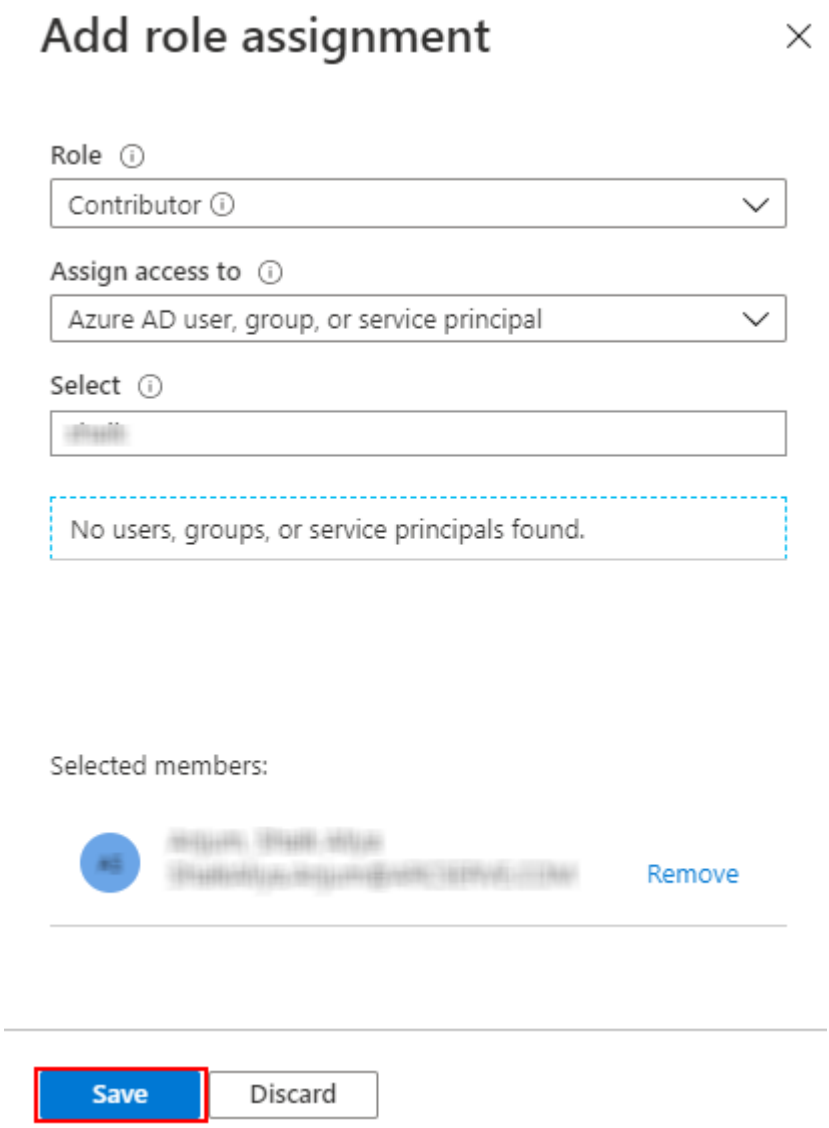
Observação: se a lista de assinaturas não mostrar a assinatura desejada, selecione o **filtro de assinaturas globais**. Certifique-se de que a assinatura desejada esteja selecionada para o portal.

g. Em Assinaturas, vá para **Controle de acesso (IAM) > Verificar acesso** e clique em **Adicionar** na caixa Adicionar uma atribuição de função.



h. Na página Adicionar atribuição de função, siga as etapas abaixo e clique em **Salvar**:

- Função - Selecione a função que você deseja atribuir ao aplicativo.
- Atribuir acesso a - Deixe como padrão.
- Selecionar - Por padrão, os aplicativos do Azure AD não são exibidos nas opções disponíveis. Para localizar o aplicativo, pesquise pelo nome e selecione-o.



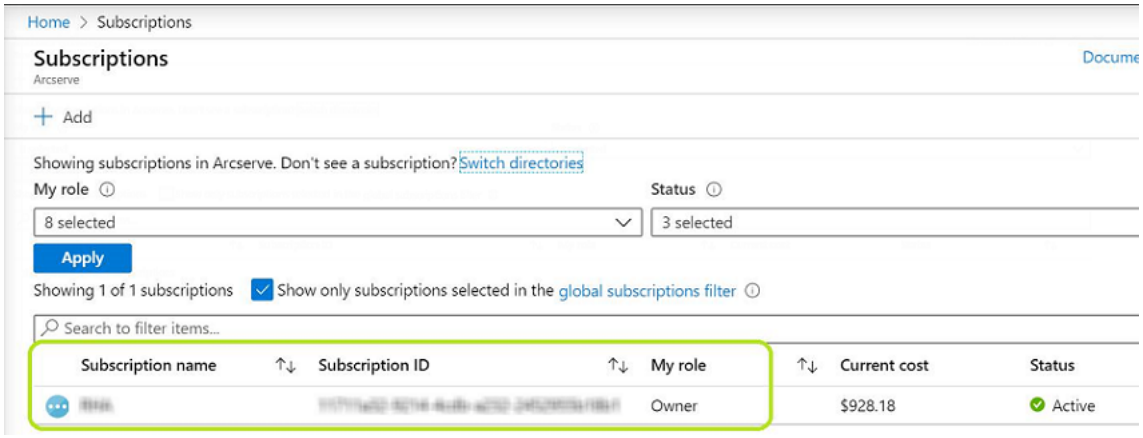
O aplicativo do Active Directory do Azure é registrado, e uma função é atribuída a ele com êxito.

Agora, é possível executar as próximas etapas usando o aplicativo registrado para obter as IDs e chaves necessárias.

2. Para obter a ID da assinatura[1], siga estas etapas:

   a. No painel de navegação esquerdo do portal do Azure, clique em **Assinaturas**.

      A lista de suas assinaturas é exibida juntamente com a ID da assinatura.

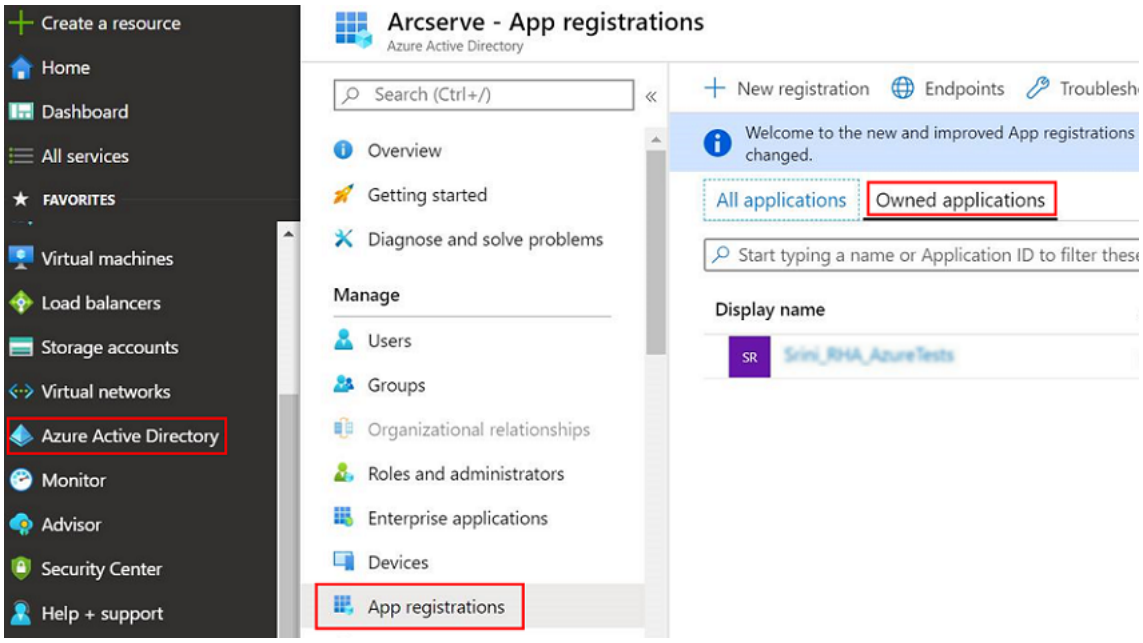


   b. Copie e salve a ID da assinatura, que é usada ao adicionar a conta de nuvem do Microsoft Azure ao Arcserve UDP.

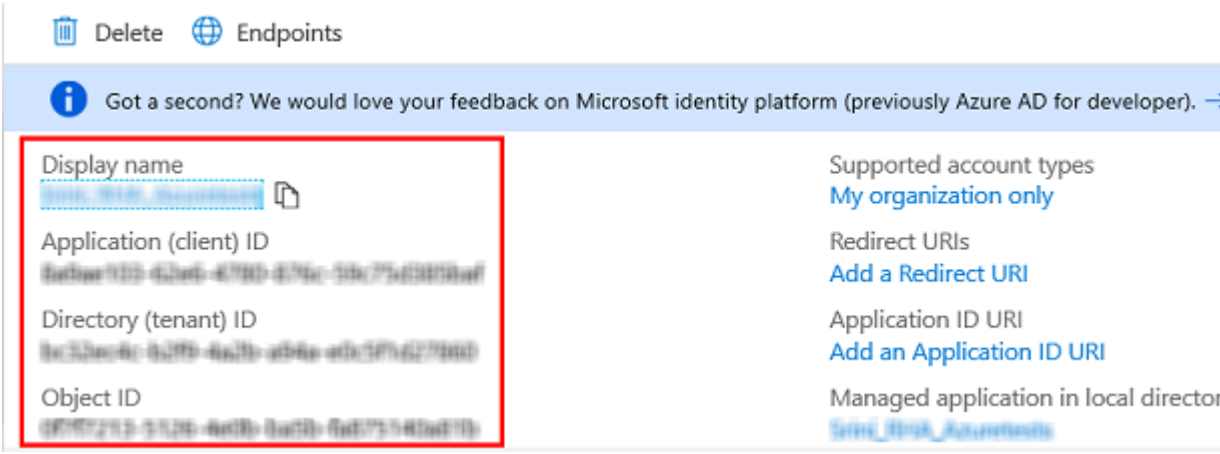
3. Para obter a ID do locatário[2] e ID do aplicativo[3], siga estas etapas:

   a. Vá para o **Azure Active Directory** > **Registros de aplicativo** > **Aplicativos de minha propriedade** e selecione o seu aplicativo.

[1]ID da assinatura refere-se a um GUID (Globally Unique Identifier - Identificador Global Exclusivo) que identifica com exclusividade sua assinatura para usar os serviços do Azure.
[2]ID do locatário refere-se à ID do Azure Active Directory na qual você criou o registro do aplicativo. ID do locatário é chamada de ID de diretório nas propriedades do Azure Active Directory.
[3]Uma ID do aplicativo refere-se a um GUID que identifica com exclusividade o registro do aplicativo no locatário do Azure Active Directory. Às vezes, também é chamada de ID do cliente.



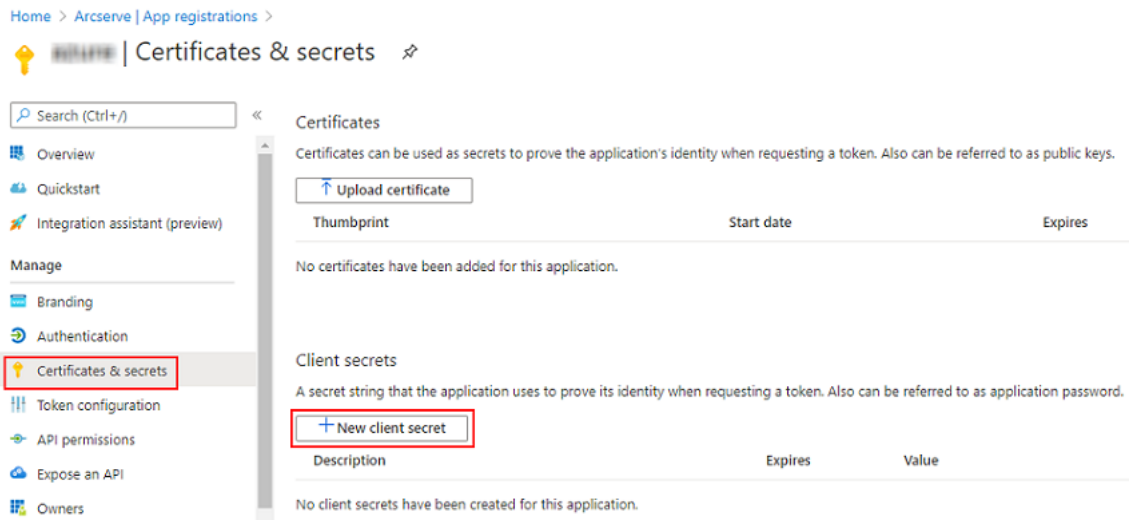
b. Copie e salve a ID do aplicativo (cliente) e a ID do diretório (locatário) em um local seguro.



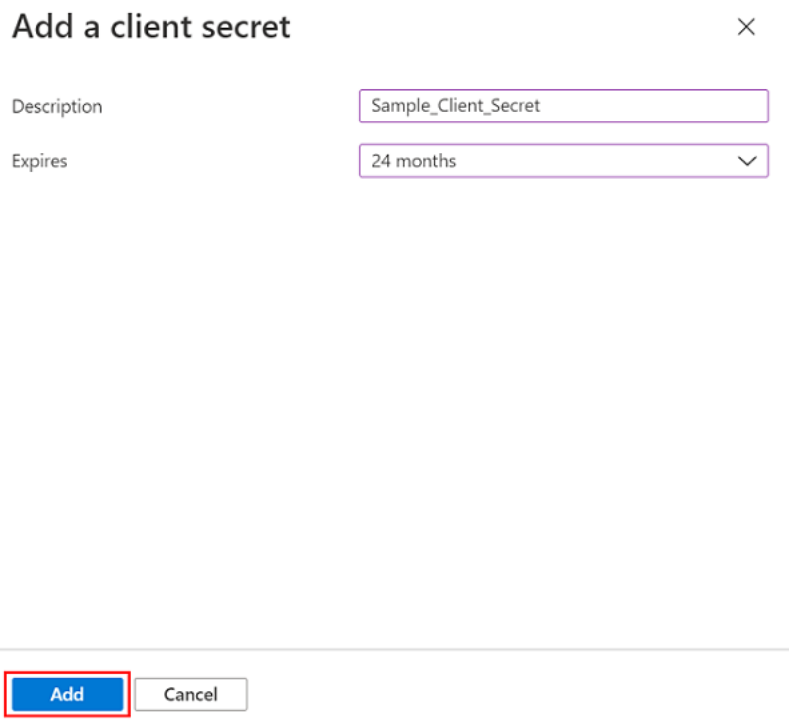
4. Para obter a Chave do cliente[1], siga estas etapas:

   a. Na página registros do aplicativo, selecione o aplicativo, navegue até **Certificados e chaves** no painel esquerdo e clique em **Nova chave do cliente** para adicionar uma chave de cliente.

[1]A chave do cliente é conhecida como a chave de autenticação no Azure.

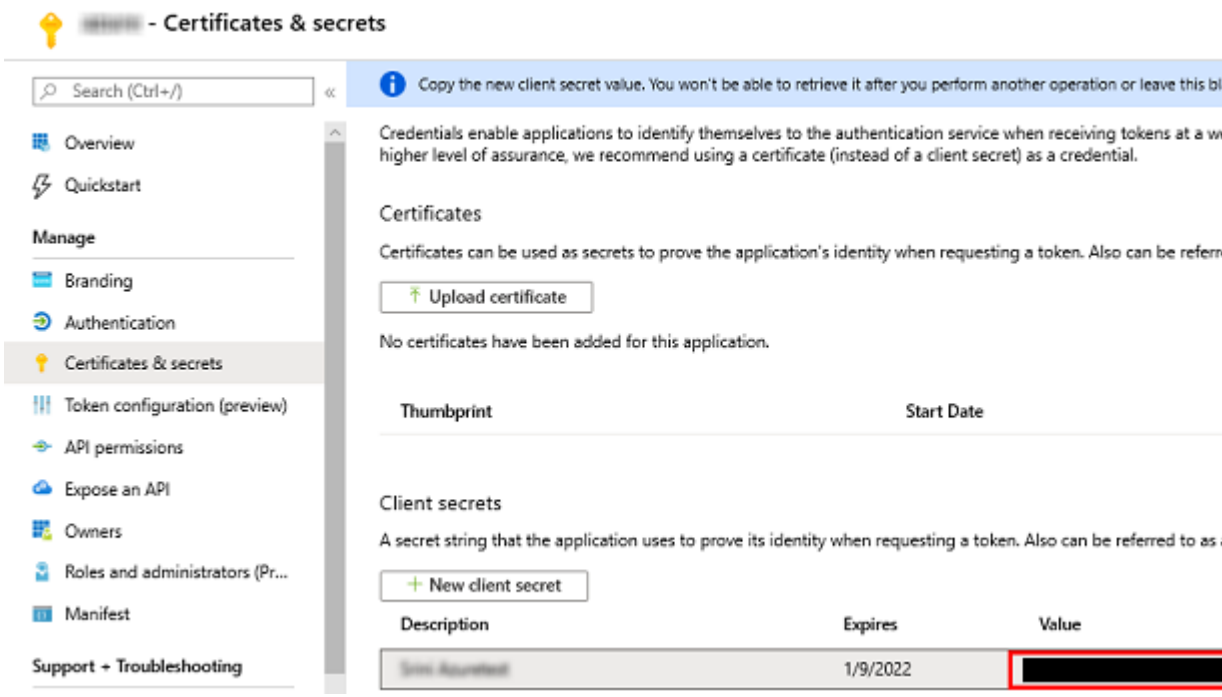


b. Na página Adicionar chave do cliente, digite uma descrição, selecione um intervalo de vencimento na lista suspensa, conforme necessário, e clique em **Adicionar**.



Observação: é recomendável que você selecione a opção de **24 meses** como intervalo de vencimento para evitar ter que gerar uma chave do cliente várias vezes.

O valor da chave do cliente é exibido.



Importante: Copie e salve o valor da chave do cliente, porque não será possível recuperá-lo posteriormente. Se você se esquecer de salvar o valor, exclua a chave do cliente existente e crie uma nova, conforme mencionado na etapa 4.

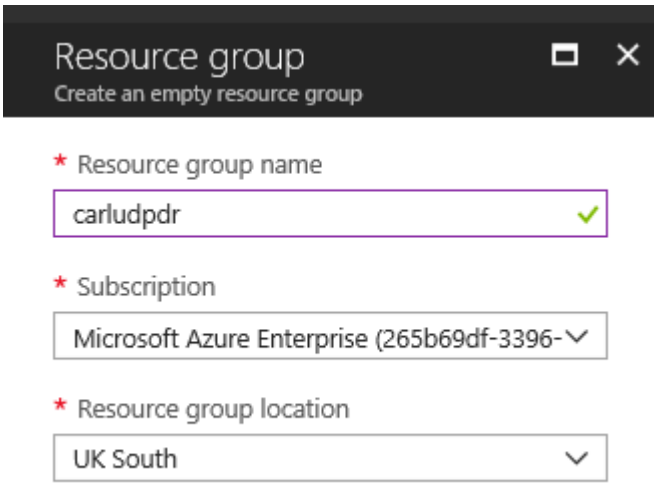
A conta de nuvem será criada com êxito no Microsoft Azure.

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.

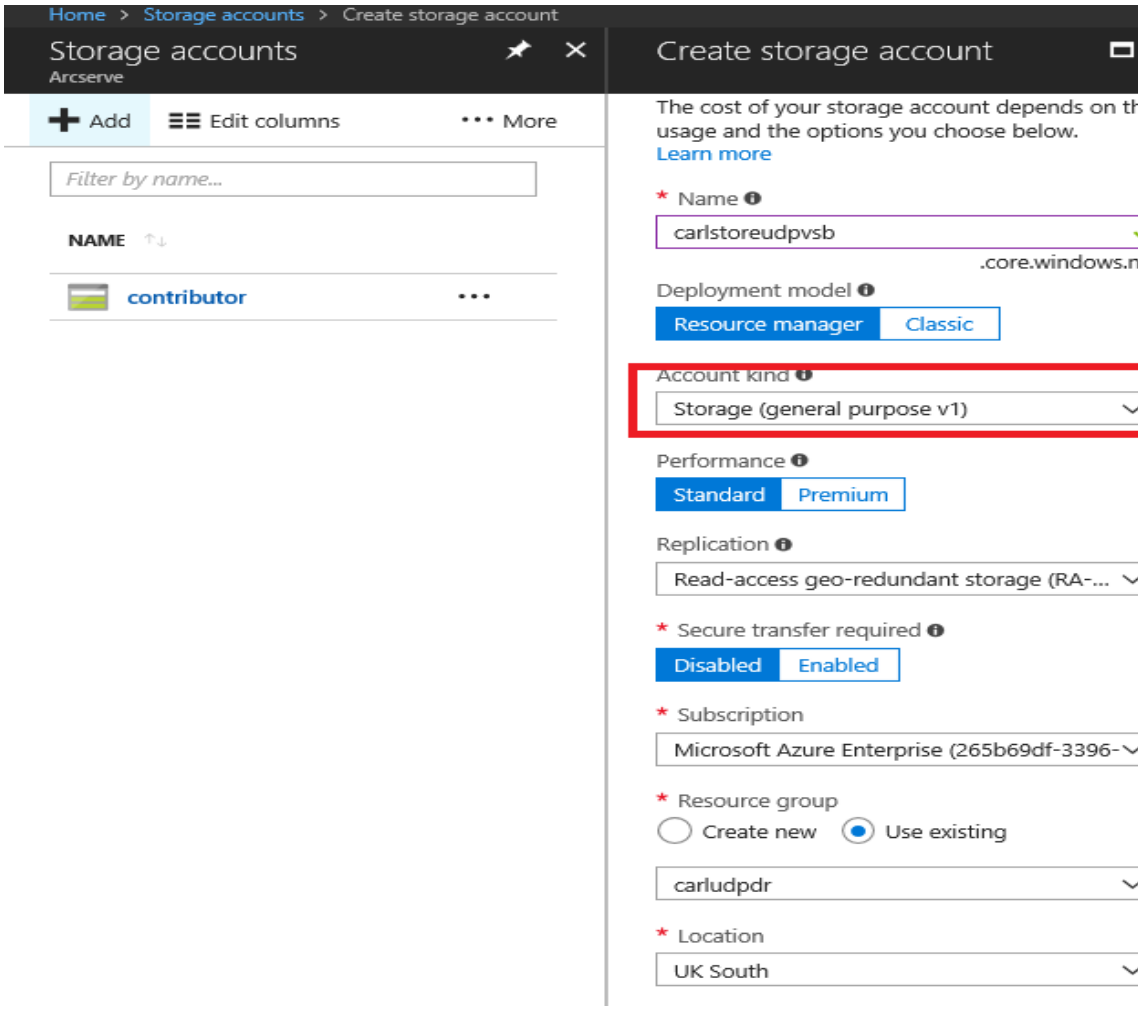
    Deployment model

    Select deployment model based on your requirement.

    Account kind

    Specify **Storage (general purpose v1)** or **StorageV2 (general purpose v2)** as Account kind.

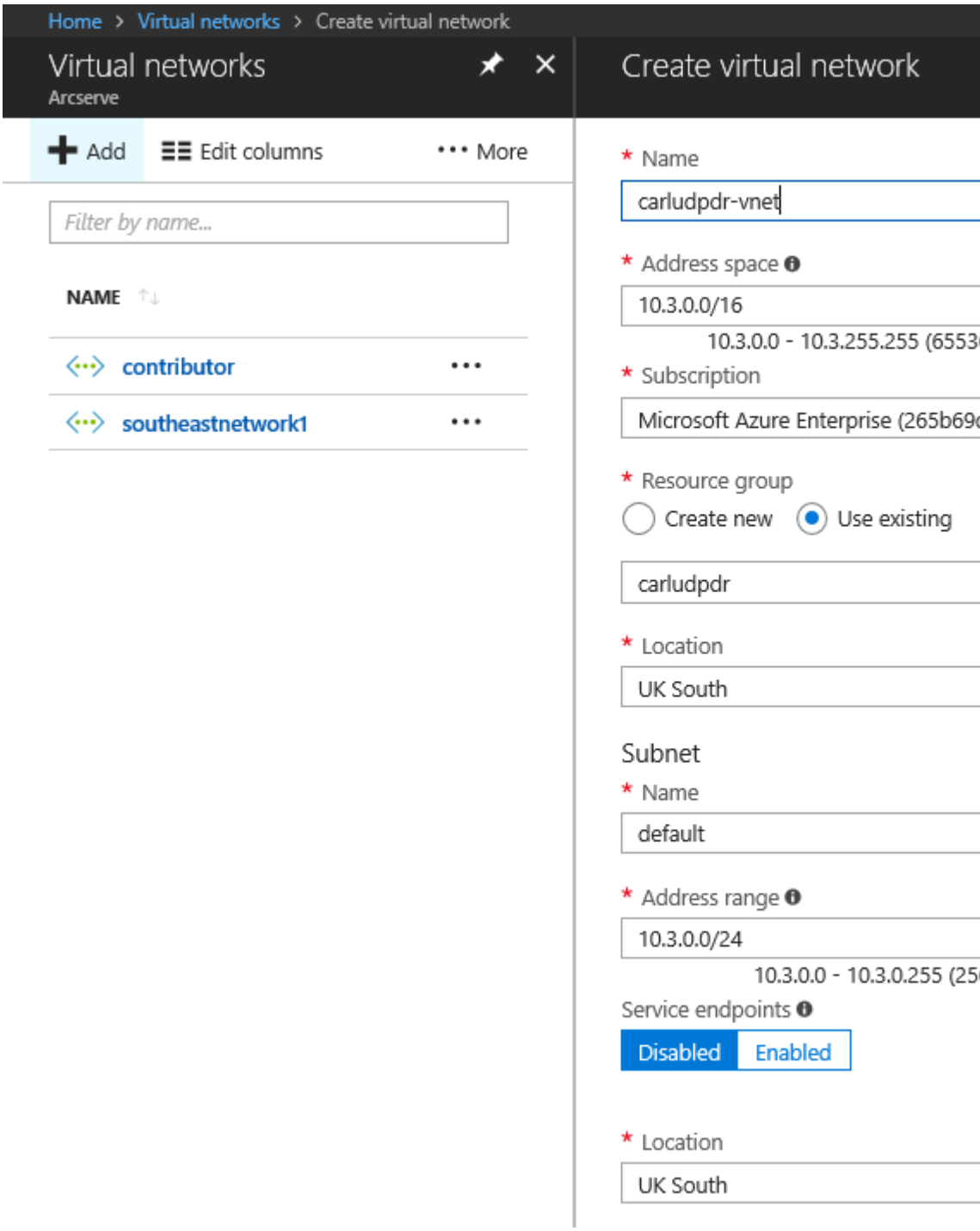
c. Specify other details as required and click **Create**:



3. Perform the following steps to create a Virtual Network and Subnet:

   a. Navigate to Microsoft Azure home, **Virtual networks**, and click **Add**.

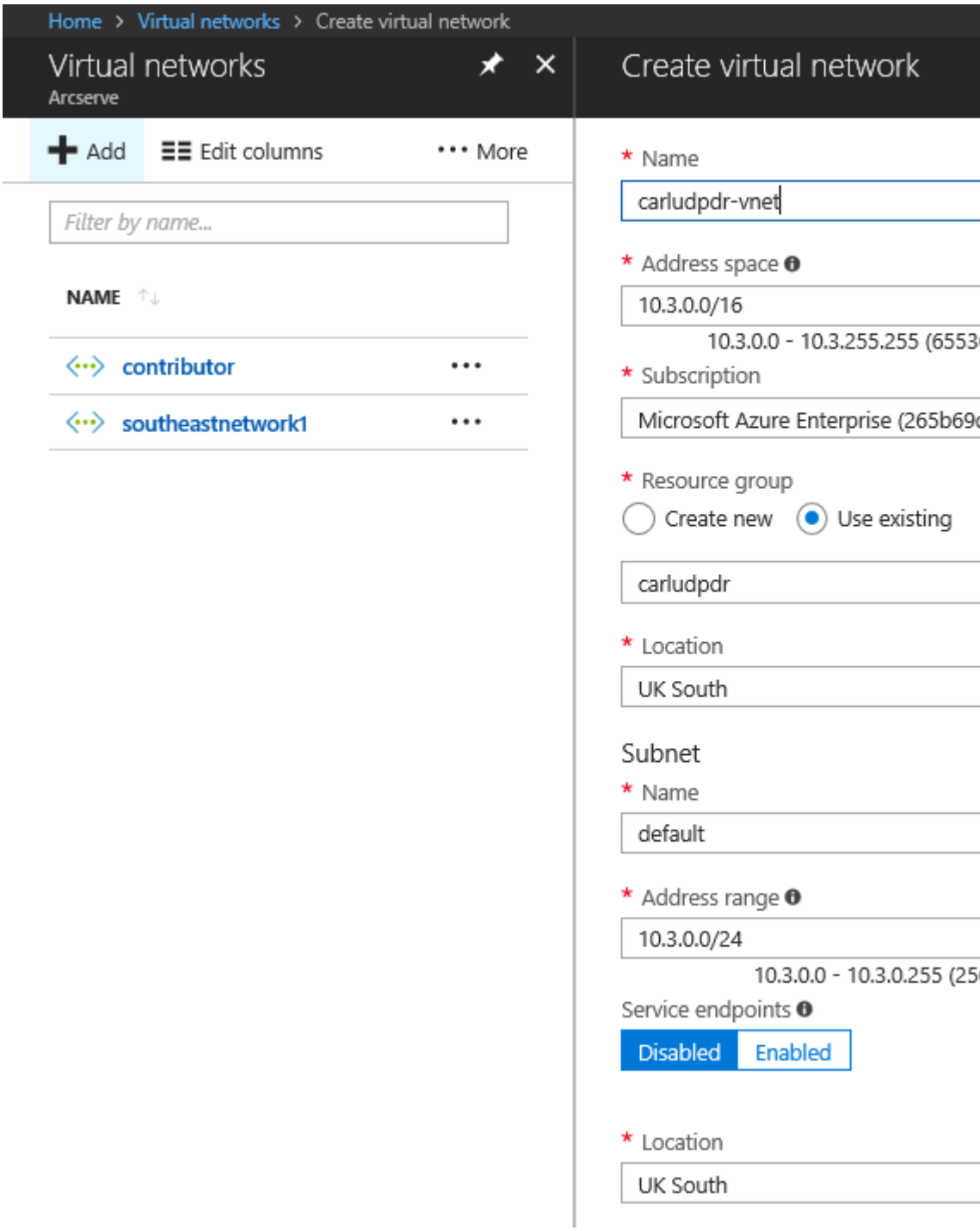
b. Enter the required details and click **Create**.



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.

Implantar o Arcserve UDP no Microsoft Azure

Depois de concluir os pré-requisitos, é possível iniciar a implantação do Arcserve UDP no Microsoft Azure.

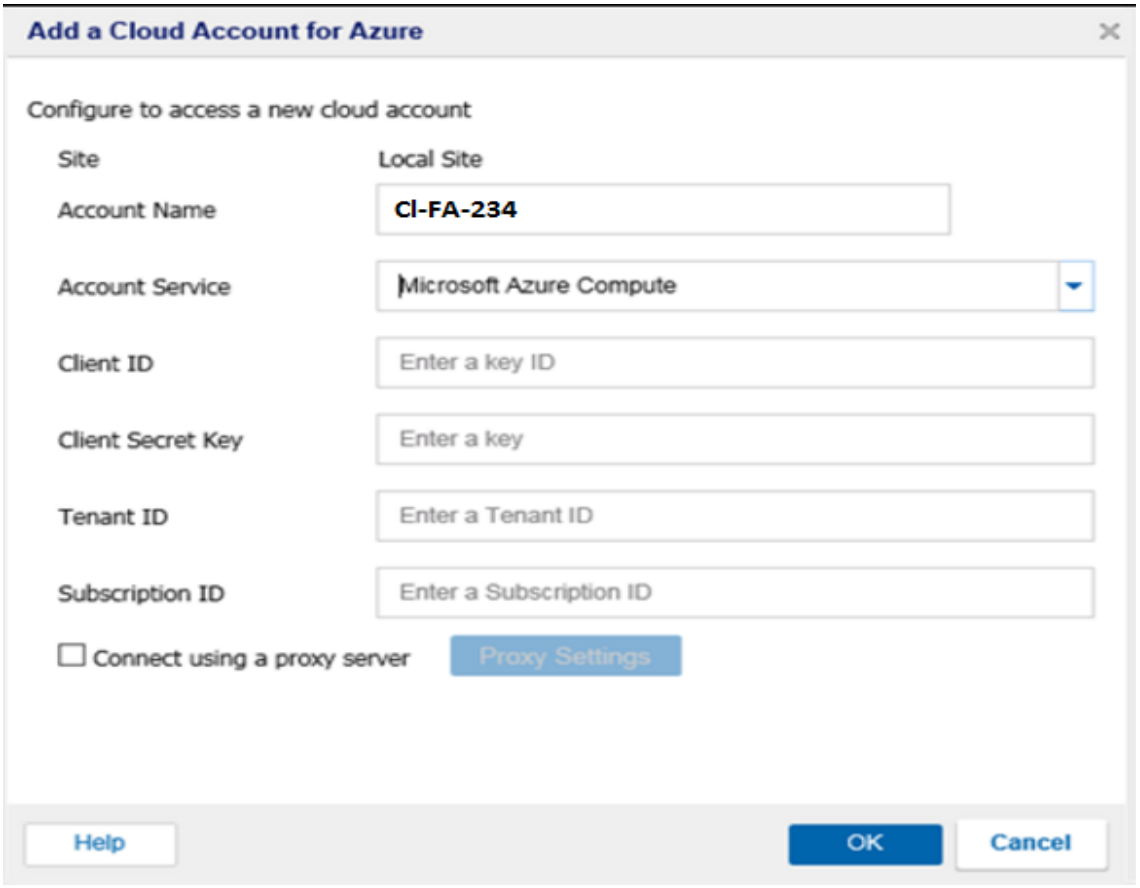
O que fazer a seguir?

1. Adicionar uma conta de nuvem do Azure ao Arcserve UDP
2. Criar um plano com uma tarefa de backup
3. Adicione uma Tarefa no modo de espera virtual ao plano
4. Executar a tarefa do modo de espera virtual manualmente
5. Ligar a VM no modo de espera virtual no Azure
6. Verificar o status da VM no modo de espera virtual

Adicionar conta de nuvem do Azure no Arcserve UDP

Adicione uma conta de nuvem da Computação do Microsoft Azure para copiar arquivos ou pontos de recuperação em um armazenamento na nuvem. É possível usar esta conta ao criar tarefas para os planos de modo de espera virtual para nuvem ou máquina virtual instantânea no Microsoft Azure.

Observação: para adicionar uma conta de nuvem para o Microsoft Azure, é necessário atender aos pré-requisitos. Para obter detalhes, consulte Pré-requisitos.



Siga estas etapas:

1. Efetue logon no Arcserve Unified Data Protection e clique na guia **recursos**.
2. No painel à esquerda, navegue até **Destinos** e clique em **Contas da nuvem**.

A página **Destinos: Contas da nuvem** é exibida no painel central.

3. Clique em **Adicionar uma conta de nuvem**.

   A página **Adicionar uma conta de nuvem** é exibida.

4. Para o **Nome da conta**, forneça um nome exclusivo.

   O nome da conta especifica o nome do armazenamento na nuvem. Esse nome será adicionado ao console para identificar a conta da nuvem. Cada conta de nuvem deve ter um nome de armazenamento exclusivo.

5. Selecione a opção da lista suspensa **Conta de serviço**.

   Vários campos são exibidos para configuração.

6. Insira os detalhes nos campos a seguir para configurar e clique em **OK**:

   ID do cliente

   Refere-se à ID de aplicativo do aplicativo do Azure Active Directory. Copie sua ID de cliente preparada no editor de texto.

   Chave secreta do cliente

   Refere-se à chave de autenticação gerada para o aplicativo do Azure Active Directory que você digita como ID do cliente. Copie sua chave secreta de cliente preparada no editor de texto.

   Importante: Esta chave secreta é fundamental para manter a segurança de suas contas. É necessário manter as chaves e as credenciais da conta em um local seguro. Não incorpore a chave secreta a uma página da web ou a outro código-fonte publicamente acessível e não a transmita por canais não seguros.

   ID do locatário

   Refere-se à ID do Azure Active Directory na qual você criou o aplicativo do Azure Active Directory. Copie sua ID de locatário preparada no editor de texto.

   ID da assinatura

   Refere-se para um GUID (Globally Unique Identifier - Identificador Global Exclusivo) que identifica com exclusividade sua assinatura para usar os serviços do Azure. Copie sua ID de assinatura preparada no editor de texto.

   Configurações de proxy

   Especifica as configurações do servidor proxy. Selecione **Conectar usando um servidor proxy** para ativar essa opção. Caso selecione esta opção, será necessário incluir também o endereço IP (ou nome do computador) do servidor proxy e o número da porta correspondente, usado pelo servidor proxy em conexões com a internet. Pode-se também selecionar esta opção se o servidor proxy

exigir autenticação. Será necessário fornecer as informações de autenticação correspondentes exigidas para usar o servidor proxy.

A conta de nuvem é adicionada ao console.

Criar um plano com uma tarefa de backup

Um plano inclui tipos diferentes de tarefas que você deseja executar. Para criar a máquina no modo de espera virtual, crie um plano que inclui uma tarefa de backup e uma tarefa no modo de espera virtual. Uma tarefa de backup executa um backup dos nós de origem e armazena os dados para o destino especificado. O recurso de modo de espera virtual usa os dados de backup e se converte em um formato de máquina virtual.

Siga estas etapas:

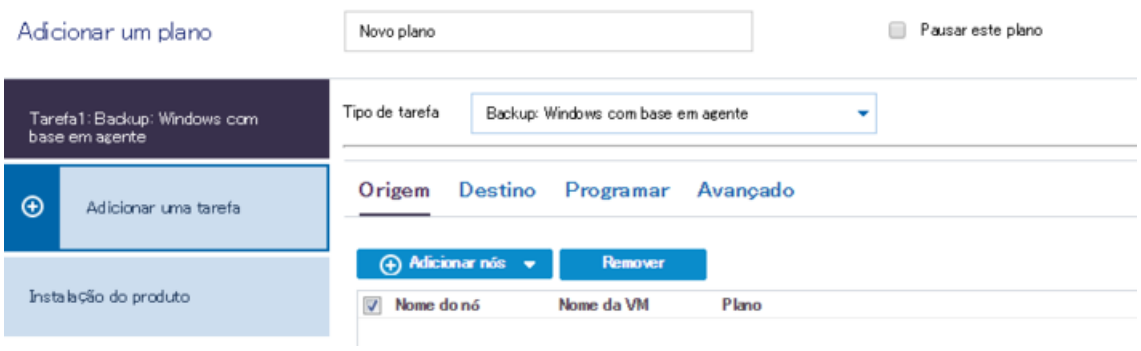
1. Clique na guia **Recursos** no Console.
2. No painel à esquerda, navegue para **Planos** e clique em **Todos os planos**.

   Se tiver criado os planos anteriores, esses planos serão exibidos no painel central.
3. No painel central, clique em **Adicionar um plano**.

   Adicionar um plano é exibido.
4. Digite o nome do plano.
5. (Opcional) Marque a caixa de seleção **Pausar este plano**.

   O plano não será executado até que você desmarque a caixa de seleção para retomar o plano.

   Observação: se um plano for pausado, nenhuma tarefa em andamento será pausada, mas todas as tarefas programadas correspondentes associadas a esse plano serão pausadas. No entanto, você pode executar uma tarefa manualmente. Por exemplo, você pode executar manualmente a tarefa de backup e a tarefa de replicação para um nó mesmo que o respectivo plano esteja pausado. Nesse caso, a tarefa seguinte da tarefa sob demanda (manual) não será executada. Por exemplo, há uma tarefa de replicação após uma tarefa de backup sob demanda, a tarefa de replicação não será executada para a tarefa de backup sob demanda. É necessário executar manualmente a tarefa de replicação. Quando você retomar o plano, as tarefas pendentes não são retomadas imediatamente. Depois de retomar o plano, as tarefas pendentes serão executadas no próximo horário programado.
6. Na lista suspensa **Tipo de tarefa**, selecione **Backup, Windows com base em agente**.



Agora, especifique os detalhes de Origem, Destino, Programação e Avançado.

Adicione uma Tarefa no modo de espera virtual ao plano

Crie um modo de espera virtual na tarefa do Azure para que os dados de backup sejam convertidos em um formato da máquina virtual e a máquina virtual seja criada. O recurso modo de espera virtual também monitora o sinal de monitoramento do nó de origem de modo que, quando o nó de origem estiver desativado, a máquina virtual imediatamente assume o controle como nó de origem.

Observações:

- O modo de espera virtual não pode ligar automaticamente os instantâneos do ponto de recuperação criados a partir de nós de máquina virtual com base em host, nós replicados a partir de um servidor de ponto de recuperação remoto, e a origem da tarefa do modo de espera virtual é aquela replicada para um local diferente. É preciso ativar instantâneos do ponto de recuperação manualmente para esses nós.
- Quando você pausa e retoma o plano novamente, a tarefa do Modo de espera virtual não é retomada automaticamente. É necessário executar manualmente outra tarefa de backup para iniciar a tarefa do Modo de espera virtual. Além disso, quando você pausa o plano, a opção Pausar/retomar o modo de espera virtual fica indisponível. Se não desejar que a máquina virtual inicie automaticamente após você pausar o plano, você deve pausar manualmente o sinal de monitoramento dos nós.

Siga estas etapas:

1. Clique em **Adicionar uma tarefa** no painel esquerdo.

   Uma nova tarefa será adicionada ao painel esquerdo.

2. No menu suspenso, selecione **Tipo de tarefa** do **Modo de espera virtual.**

A tarefa em Modo de espera virtual é adicionada.

3. Na guia **Origem**, selecione uma origem para a tarefa do modo de espera virtual.
4. Clique na guia **Servidor de virtualização** e digite os detalhes e o servidor de monitoramento e do servidor de virtualização.

Tipo de virtualização

Especifique o Azure como o tipo de virtualização.

Nome da conta

Selecione uma conta existente do Azure ou clique em **Adicionar** para criar uma conta.

Para obter mais informações, consulte Como adicionar uma conta de nuvem.

Grupo de recursos

Selecione um grupo de recursos existente ou clique em **Adicionar** para criar um grupo de recursos.

Para obter mais informações, consulte Grupo de recursos no Azure.

Região

Selecione a região na qual deseja que a VM no modo de espera opere no Azure. Para obter mais informações, consulte Regiões no Azure.

Monitor

Especifique o nome do host do servidor que monitora o status do servidor de origem.

Observações:

- Você pode usar qualquer computador físico ou máquina virtual como servidor do monitor.
- Não é possível usar o servidor de origem de backup como servidor do monitor.
- A configuração do servidor do monitor não será necessária se os nós forem replicados a partir de um servidor de ponto de recuperação remoto ou se a origem da tarefa no modo de espera virtual for replicada para um site diferente.
- A configuração do servidor do monitor não será necessária se a fonte do modo de espera virtual for a tarefa replicada e o servidor RPS de destino de replicação estiver no Azure.

Nome de usuário

Especifique o nome de usuário para efetuar logon no sistema de monitoramento.

Senha

Especifique uma senha para o nome de usuário para efetuar logon no sistema de monitoramento.

Protocolo

Especifique HTTP ou HTTPS como o protocolo que você deseja usar para comunicação entre o Arcserve UDP e o servidor de monitoramento.

Porta

Especifique a porta que deseja usar para a transferência de dados entre o Arcserve UDP e o servidor de monitoramento.

5. Clique na guia **Máquina virtual** e insira os detalhes para Configurações básicas da VM, Repositório de dados da VM para VMware, Caminho da VM para Hyper-V e Rede da VM.

Prefixo do nome da VM

Especifique o prefixo que deseja adicionar ao nome de exibição da máquina virtual no Azure.

Valor padrão: UDPVM_

Instantâneos do ponto de recuperação

Especifique o número de instantâneos dos pontos de recuperação (pontos de recuperação) para a máquina virtual no modo de espera. O número máximo de instantâneos do ponto de recuperação é 29.

Valor padrão: 5

Combine todas as sessões não convertidas em um único instantâneo do ponto de recuperação

Especifique se deseja combinar todas as sessões não convertidas em um único instantâneo do ponto de recuperação quando ocorrer a próxima tarefa do VSB programada.

Padrão: Selecionado

Tamanho da máquina virtual

O Microsoft Azure fornece uma ampla seleção de tamanhos de máquina virtual otimizada para atender a diferentes casos de uso. Eles têm várias combinações de CPU, memória, armazenamento e capacidade de rede. Para obter mais informações sobre tamanhos de máquina virtual e como eles atendem às suas

necessidades de computação, consulte Tamanhos de máquinas virtuais do Windows no Azure.

Nome da conta de armazenamento

Selecione um nome de conta de armazenamento existente ou crie uma conta de armazenamento no Azure. Ao criar uma conta de armazenamento no Azure, você deve especificar um dos seguintes como tipo de conta:

- Armazenamento (v1 de finalidade geral)
- Armazenamento V2 (v2 de finalidade geral)

Para obter mais informações, consulte Conta de armazenamento no Azure.

Rede virtual

Selecione uma rede virtual existente ou crie uma rede virtual no Azure. Para obter mais informações, consulte Rede virtual no Azure.

Sub-rede

Selecione uma sub-rede de rede virtual existente com base na rede virtual selecionada ou adicione uma sub-rede no Azure. Para obter mais informações, consulte Adicionar sub-rede no Azure.

Grupo de segurança de rede

Selecione um grupo de segurança de rede existente ou crie um grupo de segurança de rede no Azure. Configure as regras de grupo de segurança para abrir as portas relacionadas, incluindo 3389 para área de trabalho remota, 8014, 8015 para comunicação do Arcserve UDP. Para obter mais informações, consulte Grupo de segurança de rede.

Ativar IP público da atribuição automática

Selecione esta opção para atribuir o IP público à VM no modo de espera automaticamente quando a VM no modo de espera for iniciada no Azure.

6. Clique na guia **Avançado** e forneça os seguintes detalhes:

Iniciar a máquina virtual automaticamente

Especifique se deseja iniciar a máquina virtual automaticamente.

Observação: essa opção não está disponível para nós de máquina virtual com base em host e nós replicados a partir de um servidor de ponto de recuperação remoto e a origem da tarefa no modo de espera virtual é aquela replicada para um local diferente. A fonte do Modo de espera virtual é a tarefa de replicação e o servidor RPS de destino de replicação dentro do Azure.

Timeout

Especifique o tempo que o servidor do monitor deve aguardar por um sinal de monitoramento antes de ligar um instantâneo do ponto de recuperação.

Frequência

Especifique a frequência com que o servidor de origem fará a comunicação dos sinais de monitoramento para o servidor do monitor.

Exemplo: o valor de tempo limite especificado é 60. O valor de frequência especificado é 10. O servidor de origem comunicará sinais de monitoramento em intervalos de 10 segundos. Se o servidor de monitoramento não detectar um sinal de monitoramento em 60 segundos do último sinal detectado, ele ligará a máquina virtual usando o instantâneo do ponto de recuperação mais recente.

Personalizar parâmetros da tarefa

Você pode personalizar os parâmetros da tarefa para as seguintes opções:

- *Número de segmentos sendo carregados para cada tarefa*: valor padrão: 4
- *Tamanho do buffer de cada segmento*: valor padrão: 4096 KB

Ativar alertas por email

Selecione esta opção para ativar alertas por email. Você receberá alertas por email de acordo com as configurações que você fornecer.

- **Sinal de monitoramento faltando para a máquina de origem** – o modo de espera virtual envia notificações de alerta quando o servidor de monitoramento não detecta um sinal de monitoramento no servidor de origem.

  Observação: esta opção não está disponível para os nós de replicação a partir de um servidor de ponto de recuperação remoto ou se a origem da tarefa do modo de espera virtual for aquela que é replicada para um local diferente.

- **VM ligada para a máquina de origem configurada para ser ligada automaticamente** – o modo de espera virtual envia notificações de alerta quando é ligada uma máquina virtual que foi configurada para ligar automaticamente quando um sinal de monitoramento não for detectado.

  Observação: esta opção não está disponível para nós de máquina virtual com base em host e nós replicados a partir de um servidor de ponto de recuperação remoto ou se a origem da tarefa no modo de espera virtual for aquela replicada para um local diferente.

- **VM ligada para a máquina de origem configurada para ser ligada manualmente** -- o modo de espera virtual envia notificações de alerta quando uma máquina virtual é ligada manualmente.

- **Erros/falhas/paralisação na tarefa em modo de espera virtual** -- o modo de espera virtual envia notificações de alerta se um erro for detectado durante o processo de conversão.
- **Modo de espera virtual com êxito** – o modo de espera virtual envia notificações de alerta quando uma máquina virtual é ligada com êxito.
- **O Modo de espera virtual não foi iniciado com êxito a partir do instantâneo do ponto de recuperação** -- o modo de espera virtual envia notificações de alerta se a opção de início automático da recuperação de substituição da máquina virtual for ativada, mas uma máquina virtual não for ligada automaticamente.

7. Clique em **Salvar**.

   As alterações são salvas e a tarefa no modo de espera virtual é automaticamente implantada no servidor do modo de espera virtual.

   Observação: quando a tarefa no modo de espera virtual estiver concluída, o volume da máquina virtual no modo de espera será criado. A máquina virtual no modo de espera será criada apenas depois que a máquina virtual for ativada no Arcserve UDP.

   Você criou com êxito e implantou o modo de espera virtual no plano do Azure.

Executar a tarefa do modo de espera virtual manualmente

Para executar manualmente uma tarefa no modo de espera virtual, você deverá primeiro executar um backup manual. A tarefa no modo de espera virtual está associada a uma tarefa de backup. Se um plano incluir uma tarefa de backup e uma tarefa no modo de espera virtual e você executar a tarefa de backup manualmente, a tarefa do modo de espera virtual será executada automaticamente após a conclusão da tarefa de backup.

Siga estas etapas:

1. Clique na guia **Recursos**.
2. No painel à esquerda, navegue para **Nós** e clique em **Todos os nós**.

   Exibe os planos que você adicionou.
3. Selecione os nós dos quais deseja fazer backup. O nó selecionado deve ter atribuído um plano.
4. No painel central, clique em **Ações**, **Fazer backup agora**.

   A caixa de diálogo **Fazer backup agora** é exibida.

5. Selecione o tipo de backup e forneça um nome para a tarefa de backup.
6. Clique em **OK**.

   A tarefa de backup é executada.

   A tarefa no modo de espera virtual é executada imediatamente após a tarefa de backup ser concluída.

   A tarefa no modo de espera virtual é executada manualmente.

Ligar a VM no modo de espera virtual no Azure

Os volumes da VM no modo de espera são criados no Azure após a conclusão da tarefa do modo de espera virtual. A VM no modo de espera é criada apenas quando ligada a partir do Arcserve UDP.

O Virtual Standby pode ser configurado para ligar máquinas no modo de espera virtual automaticamente a partir de instantâneos de ponto de recuperação quando o servidor de monitoramento não detectar nenhum sinal de monitoramento do servidor de origem. Como alternativa, é possível ligar as máquinas no modo de espera virtual manualmente a partir de instantâneos de ponto de recuperação, caso haja uma emergência ou falha em um servidor de origem ou caso deseje colocá-lo offline para manutenção.

Siga estas etapas:

1. Na guia **Recursos**, navegue até o grupo de nós do **Modo de espera virtual**.

   Os nós no modo de espera virtual são exibidos no painel central.
2. No painel central, selecione o nó e clique em **Colocar a VM no modo de espera**.

   A caixa de diálogo **Colocar a VM no modo de espera** é exibida.
3. Na caixa de diálogo **VM no modo de espera**, execute as seguintes tarefas:
   - Selecione um instantâneo de data e hora do instantâneo do ponto de recuperação para ligar a máquina virtual.
   - Clique em **Ligar VM**.

     A máquina virtual é ligada usando os dados contidos no instantâneo do ponto de recuperação.

   Agora, você pode verificar o status ou desligar a VM no modo de espera virtual. Para obter mais informações, verifique o seguinte:

   - Verificar o status da VM no modo de espera virtual
   - Desligar a VM no modo de espera virtual no Azure

Desligar a VM no modo de espera virtual no Azure

É possível desligar a VM no modo de espera virtual no Azure usando o console do Arcserve UDP.

Siga estas etapas:

1. No console, clique em **Recursos**.
2. Navegue até **Modo de espera virtual**.
3. Selecione e clique com o botão direito do mouse em **VM do Modo de espera virtual** no painel central.

   A caixa de diálogo Colocar a VM no modo de espera é aberta e exibe os instantâneos ativos.
4. Selecione um instantâneo ativo e clique em **Desligar VM**.
5. Clique em **Excluir**.

   Uma caixa de diálogo de confirmação será aberta.
6. Se desejar excluir os discos vinculados à VM do modo de espera virtual, selecione a opção **Excluir os discos anexados**.
7. Clique em **OK**.

   A VM no modo de espera virtual é interrompida com êxito.

Verificar o status da VM no Modo de espera virtual

É possível verificar o status da VM no modo de espera virtual usando o console do Arcserve UDP.

Siga estas etapas:

1. No console, clique em **Recursos**.
2. Navegue até **Modo de espera virtual**.
3. Selecione **VM do Modo de espera virtual** no painel central.
4. O painel do Assistente de configuração exibe o status da VM no modo de espera virtual sob o grupo **Status do modo de espera virtual**.

   O status é exibido como **Em execução** se a VM no modo de espera virtual estiver ligada. Se não estiver ligada, o status será exibido como **N/D** ou **Desligado**.

Termos e definições do Arcserve UDP

Backup com base em agente

Um backup como base em agente é um método de backup de dados usando um componente de agente. O agente é instalado no nó de origem.

Compactação

A compactação é usada para os backups. A compactação geralmente é selecionada para reduzir o uso de espaço em disco, mas também tem um impacto inverso sobre a velocidade do backup devido ao aumento no uso da CPU.

As opções disponíveis são:

Nenhuma compactação

Essa opção exige menos uso da CPU (mais velocidade), mas também mais uso de espaço em disco para a imagem de backup.

Compactação padrão

Alguma compactação será realizada. Essa opção proporciona um bom equilíbrio entre o uso da CPU e o uso do espaço em disco. Essa é a configuração padrão.

Compactação máxima

A compactação máxima será realizada. Essa opção proporciona maior uso da CPU (menos velocidade), mas também menos uso de espaço em disco para a imagem de backup.

Observações:

- Se a imagem de backup contiver dados não compactáveis (como imagens JPG, arquivos ZIP, etc.), pode ser necessário espaço adicional de armazenamento alocado para lidar com esses dados. Como resultado, se selecionar a opção de compactação e tiver dados não compactáveis no backup, isso poderá resultar em um aumento do uso de espaço em disco.
- Caso altere o nível de compactação de Sem compactação para Compactação padrão ou Compactação máxima, ou ainda de Compactação padrão ou Compactação máxima para Sem compactação, o primeiro backup executado após esta alteração do nível de compactação será automaticamente um Backup completo. Após a execução do backup completo, todos os backups futuros (completo, incremental ou de verificação) serão executados conforme a

programação.

Esta opção está disponível apenas para os destinos do compartilhamento local ou remoto. Não é possível alterar a configuração de compactação se o backup do Agente do Arcserve Unified Data Protection for realizado em um repositório de dados.

- Se o destino não tiver espaço livre suficiente, considere aumentar a configuração de compactação do backup. Esta opção está disponível apenas para os destinos do compartilhamento local ou remoto. Não é possível alterar a configuração de compactação se o backup do Agente do Arcserve Unified Data Protection for realizado em um repositório de dados.

configuração

Uma guia no console do Arcserve UDP para definir parâmetros de configuração como alertas por email, configurações de banco de dados e preferências de instalação.

Painel

Uma guia no console do Arcserve UDP que permite ver o status do backup mais recente e o status do armazenamento. É possível exibir o armazenamento de dados reais, brutos e restauráveis mais recente.

Repositório de dados

Um repositório de dados é uma área de armazenamento físico em um disco. É possível criar um repositório de dados em qualquer sistema Windows em que o servidor do ponto de recuperação está instalado. Os repositórios de dados podem ser locais ou em um compartilhamento remoto que o sistema Windows pode acessar.

Destino

Destino é um computador ou servidor onde você deseja armazenar os dados de backup. Um destino pode ser uma pasta local no nó protegido, uma pasta compartilhada remota ou um RPS (Recovery Point Server – Servidor de Ponto de Recuperação).

Nós detectados

Os nós detectados são sistemas físicos ou virtuais adicionados ao console do Arcserve UDP detectando-os no diretório ativo ou no vCenter/ESX server, importando-os de um arquivo ou adicionando-os manualmente usando seu endereço IP.

Criptografia

A solução Arcserve Unified Data Protection fornece o recurso de criptografia de dados.

quando o destino do backup é um servidor do ponto de recuperação, as criptografias disponíveis são Sem criptografia e Criptografar dados com AES-256. É possível definir esta opção para criar um repositório de dados. Quando o destino de backup for local ou de compartilhamento remoto, as opções de formato criptografado disponíveis são Sem criptografia, AES-128, AES-192 e AES-256. É possível definir a opção durante a criação de um plano de backup em pasta local ou compartilhada, ou faça isso na configuração de backup do agente autônomo do Arcserve Unified Data Protection.

Principais recursos de criptografia

1. O método de criptografia AES256 aplica-se a:
   - Repositório de dados
   - Senha salva (no plano de proteção, registro, arquivo de configuração e assim por diante)
2. *Para a tarefa de backup*: se a criptografia estiver ativada, os dados serão criptografados antes de saírem do servidor.
3. *Para a tarefa de replicação:* se o destino da replicação tiver a criptografia ativada, os dados serão criptografados antes de saírem do servidor.

Configurações de criptografia

a. Selecione o tipo de algoritmo de criptografia que deseja usar para os backups.

   A criptografia de dados é a conversão de dados em uma forma ininteligível sem um mecanismo decodificador. A solução Arcserve Unified Data Protection usa algoritmos de criptografia seguros, AES (Advanced Encryption Standard – Padrão de Criptografia Avançada) para atingir o máximo de segurança e privacidade dos dados especificados.

b. Quando um algoritmo de criptografia é selecionado, você deve fornecer (e confirmar) uma senha de criptografia.
   - A senha de criptografia é limitada a um máximo de 23 caracteres.
   - Um backup completo e todos os seus respectivos backups incrementais e de verificação deverão usar a mesma senha para criptografar dados.
   - Se a senha de criptografia para um backup incremental ou de verificação for alterada, um backup completo deverá ser executado. Isso significa que, após

a alteração de senha de criptografia, o primeiro backup será completo, independentemente do tipo de backup.

Por exemplo, se você alterar a senha de criptografia e enviar um backup personalizado incremental ou de verificação manualmente, ele será convertido automaticamente para um backup completo.

Observação: esta opção está disponível apenas para os destinos do compartilhamento local ou remoto. Não é possível desativar a configuração de criptografia se o backup do agente do Arcserve Unified Data Protection for realizado em um repositório de dados.

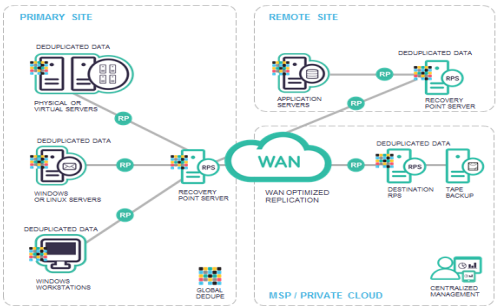
c. A solução Arcserve Unified Data Protection tem a senha de criptografia e a senha de sessão.

- A senha de criptografia é necessária para o repositório de dados.
- A senha de sessão é necessária para o nó.
- Se o repositório de dados estiver criptografado, a senha da sessão será obrigatória. Se o repositório de dados não estiver criptografado, a senha da sessão será opcional.

A senha não será obrigatória caso esteja tentando restaurar no computador em que o backup foi executado. No entanto, caso esteja tentando restaurar em um computador diferente, a senha será necessária. Por padrão, a senha é obrigatória apenas para o primeiro logon. Para informar a senha mesmo após o primeiro logon, o administrador precisará interromper manualmente o serviço Arcserve UDP Agent Explorer Extension.

Redução de redundância global

A redução de redundância global do Arcserve UDP reduz significativamente a quantidade de dados realmente transferida durante ciclos de backup. A capacidade de redução de redundância em todos os clientes do ambiente limita o armazenamento desnecessário e a transferência de dados existentes, tornando-os globais quando os dados passam por redução de redundância em nós, tarefas e sites.



Backup sem agente com base em host

Um backup com base em host sem agente é um método para fazer backup de dados sem o uso de um componente de agente no computador de origem.

Modo de transporte HOTADD

O modo de transporte HOTADD é um método de transporte de dados que permite fazer backup de máquinas virtuais configuradas com discos SCSI. Para obter mais informações, consulte o Guia de Programação da API do disco virtual no site do VMware.

Tarefa

Uma tarefa é uma ação do Arcserve UDP para fazer backup, restaurar, criar no modo de espera virtual ou replicar nós.

tarefas

Uma guia no console do Arcserve UDP na qual é possível monitorar o status de todas as tarefas, como backup, replicação e restauração. Os detalhes incluem tarefas, tipos de tarefas, IDs de nó, pontos de recuperação e nome de plano.

Modo de transporte NBD

O modo de transporte NBD, também conhecido como modo de transporte LAN, usa o protocolo NFC (Network File Copy - Cópia de arquivos de rede) para estabelecer comunicação. Várias operações do VDDK e VCB usam uma conexão para cada disco virtual acessado em cada host ESX/ESXi Server ao usar o NDB.

Modo de transporte NBDSSL

O modo de transporte NBDSSL (Network Block Device Secure Sockets Layer) usa o protocolo NFC (Network File Copy) para se comunicar. O NBDSSL transfere dados criptografados usando redes de comunicação TCP/IP.

Nós

O nó é um sistema físico ou virtual que o Arcserve UDP protege. O Arcserve UDP pode proteger nós físicos e máquinas virtuais em um servidor vCenter/ESX ou servidor Hyper-V da Microsoft.

Plano

Um plano é um grupo de tarefas para gerenciar backup, replicação e criação de computadores no modo de espera virtual. Um plano consiste em uma única ou em várias tarefas. As tarefas são um conjunto de atividades para definir a origem, destino, programação e parâmetros avançados.

Nós protegidos

Nós protegido são os nós que possuem planos de backup programados para fazer backup de dados em intervalos regulares.

Evento recente

Eventos recentes são as tarefas que ainda estão em execução, ou as tarefas que foram recentemente concluídas.

Ponto de recuperação

Um ponto de recuperação é um instantâneo de backup pontual de um nó. Um ponto de recuperação é criado quando você faz backup de um nó. Os pontos de recuperação estão armazenados no destino de backup.

Servidor do ponto de recuperação

Um servidor do ponto de recuperação é um nó de destino onde você instala o servidor. É possível criar repositórios de dados em um servidor do ponto de recuperação. O RPS atua como um repositório de backup para imagens de disco e oferece um conjunto exclusivo de tecnologias com os componentes fundamentais da solução Arcserve UDP. Alguns dos principais recursos do RPS são Redução de redundância global no lado de origem, Replicação de imagens de disco integrada e comprovada, Início rápido do RPS ou Sincronização “Offline” e Armazenamento multilocação.

Replicar

Replicar é uma tarefa que duplica os pontos de recuperação de um servidor para outro servidor.

Recursos

Recursos é uma guia do console da Arcserve UDP. Na guia **Recursos**, é possível gerenciar nós de origem, destinos e planos.

Modo de transporte SAN

O modo de transporte SAN (Storage Area Network) permite transferir dados de backup dos sistemas proxy conectados à SAN para os dispositivos de armazenamento.

Sistemas

Sistemas são todos os tipos de nós, dispositivos e máquinas virtuais que podem ser gerenciados pelo Arcserve Unified Data Protection. Isso inclui físico, virtual, Linux e máquinas virtuais em modo de espera.

Tarefas

Uma tarefa é um conjunto de atividades para definir vários parâmetros para fazer backup, replicar e criar máquinas no modo de espera virtual. Esses parâmetros incluem origem, destino, programação, e alguns parâmetros avançados. Cada tarefa está associada a um plano. É possível ter mais de uma tarefa em um plano.

Nós não protegidos

Nós desprotegidos são os nós adicionados ao Arcserve Unified Data Protection, mas que não têm um plano atribuído. Quando um plano não está atribuído, não é possível fazer backup de dados e o nó permanece desprotegido.

Redução de redundância de dados

A redução de redundância de dados é a tecnologia que elimina cópias duplicadas dos mesmos dados, reduzindo, assim, o espaço de armazenamento. Em uma empresa, pode haver vários motivos para duplicar dados, como um anexo de email específico encaminhado para vários usuários. Quando faz backup desses dados, você salva várias cópias dos mesmos dados na mídia de armazenamento de backup.

A redução de redundância de dados elimina os dados redundantes e salva apenas uma instância dos dados. Todas as outras instâncias são substituídas por uma referência a essa instância. Esse método pode reduzir consideravelmente o espaço de armazenamento necessário para armazenar os dados de backup.

Por exemplo, pode haver um mesmo arquivo de 10 MB que 100 usuários têm armazenado em seus sistemas locais. Ao fazer o backup de todos estes sistemas ou nós locais, você precisaria 1000 MB de espaço de armazenamento. Com a redução de redundância de dados, é possível reduzir o espaço de armazenamento para aproximadamente 10 MB, pois apenas uma instância do arquivo é armazenada no disco. As 99 instâncias restantes se referem a essa instância.

Benefícios de redução de redundância de dados

- Armazena mais dados de backup em um espaço de armazenamento
- Reduz a quantidade de dados enviados pela rede
- Executa o backup mais rapidamente conforme as informações de referência são armazenadas, em vez dos dados reais
- Reduz o custo de largura de banda da rede e a mídia de armazenamento

Tipos de redução de redundância de dados

O Arcserve UDP oferece suporte a dois tipos de redução de redundância de dados.

Redução de redundância de dados do lado da origem

Garante que apenas dados exclusivos do agente são enviados a um servidor de ponto de recuperação para o backup de dados.

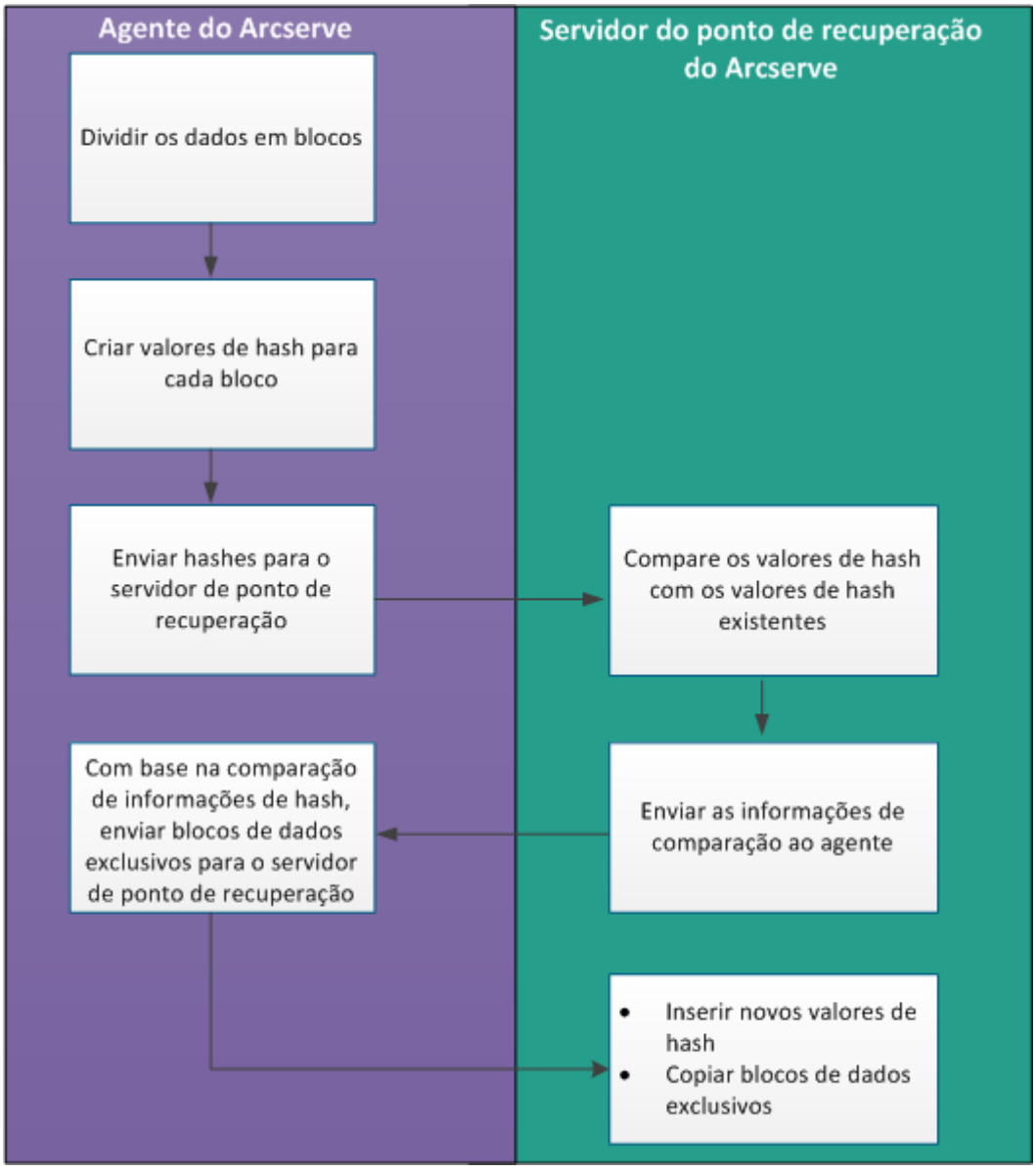
Redução de redundância global

Garante que somente dados exclusivos de vários agentes sejam submetidos a backup em um servidor de ponto de recuperação. Se estiverem presentes blocos de dados semelhantes em vários nós, apenas uma cópia de backup será feita para o servidor de ponto de recuperação.

Como a redução de redundância de dados funciona

O processo de redução de redundância do Arcserve UDP divide os dados em blocos de dados e a cada bloco é atribuído um único identificador denominado hash. O hash é calculado com base no agrupamento de volume. O tamanho do bloco de redução de redundância padrão é de 4 KB (o tamanho do agrupamento do volume padrão é de 4 KB para a maioria dos nós). Esses valores de hash são comparados aos valores de hash dos dados de backup existentes e, se as referências de duplicação forem encontradas, não será feito backup desses blocos de dados. Apenas será feito o backup dos blocos de dados com referências exclusivas.

O diagrama a seguir ilustra como funciona a redução de redundância no Arcserve UDP:



Quando um backup é acionado, o processo de redução de redundância no agente primeiro divide os dados em blocos e atribui uma chave de hash ou valor exclusivo para cada bloco. Em seguida, os valores de hash são enviados para o servidor de ponto de recuperação. No servidor de ponto de recuperação, esses valores de hash são comparados aos valores de hash existentes e os hashes duplicados são filtrados. Os resultados da comparação são enviados de volta para o agente. Com base nessas informações hash duplicadas, o agente envia os blocos de dados exclusivos para o servidor de ponto de recuperação para backup. Os novos valores de hash desses blocos de dados também são inseridos em sua lista de hash existente no servidor de ponto de recuperação.

Quando houver vários agentes, o processo de redução de redundância permanece o mesmo, no entanto, os dados duplicados de vários agentes são filtrados. Isso elimina qualquer duplicação de dados, mesmo que seja de vários agentes.

Abaixo estão os benefícios de usar a redução de redundância de dados no Arcserve UDP.

- **Backup completo mais rápido**
- **Tarefa de mesclagem mais rápida**
- **Suporte a redução de redundância global**
- **Replicação otimizada**

Quando você deve usar a redução de redundância

A seguir estão alguns dos cenários em que o uso de um repositório de dados de redução de redundância pode ser mais efetivo:

- Quando você possui vários nós com dados similares. Nesse cenário, se fizer o backup dos dados de todos os nós para um repositório de dados, deve obter uma boa redução na quantidade de dados que é realmente armazenada no servidor de ponto de recuperação. O espaço de armazenamento necessário pode ser consideravelmente inferior.
- Quando você tem que executar frequentemente um backup completo de um nó. Neste cenário, a maioria dos dados de backup já existe, portanto, o seu tempo de backup pode ser muito pequeno.
- Quando a largura de banda de rede é muito valiosa. Como apenas os blocos de dados exclusivos trafegam pela rede, é possível reduzir o uso da rede.
- Quando os dados de backup se movem com frequência de um nó para outro. Nesse cenário, quando você tenta fazer o backup do novo nó (onde os dados se movem de seu nó original), o destino já contém a cópia e apenas é feito o backup das informações de referência.

Configurando os repositórios de dados da redução de redundância no Arcserve UDP

A seguir, estão os parâmetros importantes de configuração para um repositório de dados de redução de redundância:

Destino de dados

O destino de dados é usado para armazenar os dados protegidos. É preferível usar um disco maior para o destino de dados, pois ele contém os blocos de dados originais da origem.

Destino do índice

O índice de destino é usado para armazenar os arquivos de índice e é melhor usado em um disco diferente para melhorar a taxa de transferência de processamento de redução de redundância.

Destino de hash

O destino de hash é usado para armazenar os arquivos de hash e é melhor usado em unidades de SSD de alta velocidade, as quais podem melhorar a capacidade de redução de redundância com uma menor alocação de memória necessária.

Se o destino de hash estiver configurado em um SSD de alta velocidade, ele pode ser usado para aumentar a capacidade de redução de redundância com menos requisitos de alocação de memória.

Pasta de destino do backup

A pasta de destino na qual os arquivos .D2D e de catálogo residem.

Tamanho do bloco

O "tamanho do bloco de redução de redundância" também afeta a "estimativa da capacidade de redução de redundância". O “tamanho do bloco de redução de redundância” padrão é 16 KB. Se definir esse tamanho como 32 KB, a “previsão de capacidade da redução de redundância” será duplicada. O impacto de aumentar o tamanho do bloco da redução de redundância é que pode diminuir a porcentagem da redução de redundância e, ao mesmo tempo, diminuir também os requisitos de memória.

Alocação de memória

Para estimar o requisito de memória, use a ferramenta "Estimar os requisitos de armazenamento e memória". Se a memória alocada não for suficiente e se quando a memória for totalmente usada, os novos dados não puderem ser inseridos no BD de hash. Portanto, os dados que não puderem ser copiados para

backup depois disso, não poderão ter redução de redundância, fazendo com que a taxa de redução de redundância caia. Se não for possível aumentar a memória por algum motivo, tente aumentar o tamanho do bloco da redução de redundância, pois isso reduziria o requisito de memória.

Observação: o tamanho do bloco não pode ser alterado para um repositório de dados existente.

Lembre-se de que uma nova tarefa de backup não tem permissão para iniciar se a memória hash estiver cheia. Mas, para a tarefa de backup em execução (que foi iniciada antes da memória hash estar cheia), é possível prosseguir concluí-la. Nesse caso, não seriam inseridas nova chave de hash para o banco de dados de hash. Como resultado, há um impacto na porcentagem de redução de redundância.

O motivo é que todos os blocos de dados na tarefa de backup em execução ainda são comparados às chaves de hash existentes no banco de dados de hash.

• Se estiverem duplicados com a chave de hash existente, não serão mais gravados no disco.

• Se não estiverem duplicados com a chave de hash existente, serão gravados em disco. Mas a nova chave de hash não deve ser inserida no banco de dados de hash porque ele está cheio. Como resultado, os blocos de dados consequentes não podem se comparar a essas novas chaves de hash.

Redução de redundância, criptografia e compactação

Além da redução de redundância de dados, é possível aplicar a compactação e a criptografia em um repositório de dados.

Se você ativar a criptografia, o Agente do Arcserve Unified Data Protection para Windows consumirá recursos da CPU para criptografar os dados. Como a criptografia é aplicada somente aos dados exclusivos, os recursos da CPU necessários para criptografia podem ser mínimos onde o percentual de redução de redundância for alto.

- Sem compactação e redução de redundância, a utilização da CPU é menor para a tarefa de compactação e os dados armazenados ficam no formato não compactado.
- Com a compactação padrão e a redução de redundância, a utilização da CPU é ideal para a tarefa de compactação, os dados armazenados estão em um formato compactado e o requisito para o espaço de armazenamento é menor.
- Com a compactação e a redução de redundância máximas, o uso da CPU é máximo para a tarefa de compactação e os dados armazenados são 2-3% maiores, além do requisito para o espaço de armazenamento ser menor

Limitações de redução de redundância

Não é possível modificar o tamanho do bloco de redução de redundância, a configuração de criptografia e o tipo de compactação após ter criado um repositório de dados de redução de redundância.