Rapid Recovery 6.0 em dispositivos DL

Guia do usuário

DELL EMC

Notas, avisos e advertências

NOTA: Uma NOTA indica informações importantes que ajudam você a usar melhor os recursos do computador.

CUIDADO: Um AVISO indica possíveis danos ao hardware ou perda de dados e ensina como evitar o problema.

ATENÇÃO: Uma ADVERTÊNCIA indica possíveis danos à propriedade, risco de lesões corporais ou mesmo risco de vida.

2016 - 09

Rev. A00

Índice

1 Introdução ao dispositivo DL....11
Arquitetura de implantação....11
Smart Agent....13
Dispositivo DL Core....13
Processo de instantâneos....13
Replicação do site de recuperação de desastres ou provedor de serviços....13
Recuperação....14
Recursos do produto....14
Como entender repositórios....14
Desduplicação no Rapid Recovery....16
Compreender as chaves de criptografia....16
Replicação com Rapid Recovery....17
Retenção e arquivamento....21
Virtualização e nuvem....22
Gerenciamento de alertas e eventos....23
Portal de licenças....23
Console Web....23
APIs de gerenciamento de serviço....23

2 Trabalhar com o dispositivo DL Core....24
Noções básicas do Rapid Recovery Core Console....24
Acesso ao Rapid Recovery Core Console....24
Noções básicas sobre o Guia de início rápido....24
Navegar até o Rapid Recovery Core Console....26
Visualização do menu Máquinas protegidas....30
Ver máquinas replicadas no menu de navegação....34
Visualizar o menu Apenas pontos de recuperação....35
Visualizar o menu Grupos personalizados....35
Usar a caixa de diálogo Erro....35
Definições do Core....36
Definições do Rapid Recovery Core....36
Criar cópia de segurança e restaurar definições do Core....65
Ferramentas do nível do Core....66
Roteiro para configurar o Core....69
Repositórios....69
Gerenciamento de um repositório de DVM....69
Gerenciar a segurança....81
Aplicar ou remover criptografia de uma máquina protegida....82
Gerenciar chaves de criptografia....84
Gerenciar contas de nuvem....92
Sobre contas de nuvem....92

Adicionar uma conta de nuvem....92
Editar uma conta de nuvem....94
Configurar as definições da conta de nuvem....94
Remover uma conta de nuvem....94
Archiving....95
Noções básicas sobre arquivos....95
Criar um arquivo....95
Editar um arquivo programado....98
Pausar ou retomar um arquivo programado....100
Forçar um trabalho de arquivo....100
Verificar um arquivo....100
Anexar um arquivo....101
Importar um arquivamento....102
Eventos....104
Eventos Rapid Recovery....104
Como exibir eventos usando tarefas, alertas e registros....105
Como entender as notificações de e-mail....108
Grupos de notificação, configurações de SMTP e modelos de notificação para eventos do sistema....111
Configurar grupos de notificação....111
Sobre a configuração da redução de repetição....114
Configurar retenção de eventos....115
Recuperação automática rápida do dispositivoo....115
Criar a unidade USB RASR....115
Executar a RASR....116
O Local Mount Utility....117
Sobre o Local Mount Utility....117
Trabalhar com máquinas Rapid Recovery Core no Utilitário de montagem local....117
Trabalhar com máquinas protegidas no Local Mount Utility....120
Usar o menu de bandeja do Local Mount Utility....123

3 Gerenciar o dispositivo....125
Como monitorar o status do Dispositivo....125
Backup do Windows....125
Status do backup....126
Política de backup do Windows....127
Armazenamento de provisionamento....128
Apagar a alocação de espaço para um disco virtual....129
Utilitário de recuperação e atualização....129
Fazer upgrade do aparelho....130
Reparar o dispositivo....130

4 Proteger estações de trabalho e servidores....131
Proteger as máquinas....131
Sobre como proteger máquinas com Rapid Recovery....131
Acessar o diagnóstico de máquinas protegidas....193
Gerenciar máquinas....195

Remover uma máquina....195
Cancelar operações em uma máquina....196
Visualizar informações de licença em uma máquina....196
Exportação de VM....196
Sobre a exportação para máquinas virtuais com o Rapid Recovery....196
Gerenciar exportações....208
Como gerenciar dados de classificação por vencimento....221
Sobre retenção e arquivamento de dados do Rapid Recovery....222
Como gerenciar as políticas de retenção....222
Replicação....227
Replicação com Rapid Recovery....227
Cadeias de pontos de recuperação e órfãos....231
Quando a replicação começar....232
Determinar suas necessidades e sua estratégia de seeding....232
Considerações sobre desempenho para transferência de dados replicados....234
Replicação para um core de destino autogerenciado....235
Ver a replicação de entrada e saída....239
Como configurar a replicação....241
Replicar para um Core de destino de terceiros....241
Adicionar uma máquina a uma replicação existente....246
Consumo da unidade de propagação em um Core de destino....247
Gerenciar definições de replicação....249
Remoção da replicação....256
Recuperar dados replicados....258

5 Recuperar dados....259
Gerenciar a recuperação....259
Instantâneos e pontos de recuperação....259
Gerenciar snapshots e pontos de recuperação....259
Ver a página de pontos de recuperação de uma máquina protegida....259
Montar um ponto de recuperação....262
Desmontar pontos de recuperação....263
Trabalhar com pontos de recuperação do Linux....263
Forçar um snapshot....265
Remover pontos de recuperação....266
Excluir uma cadeia de pontos de recuperação órfãos....266
Como migrar pontos de recuperação para um repositório diferente....267
Restaurar dados....268
Sobre como restaurar dados com o Rapid Recovery....268
Noções básicas sobre Live Recovery....268
Restaurar dados de pontos de recuperação....269
Como restaurar volumes a partir de um ponto de recuperação....270
Como realizar uma reversão para clusters e nós de cluster....273
Restauração a partir de um arquivo em anexo....273
Noções básicas sobre bare metal restores em máquinas Windows....274
Restauração sem sistema operacional para máquinas Windows....274

Entender a criação do CD de inicialização para máquinas Windows..... 280
Como usar o Universal Recovery Console para uma BMR..... 282
Realizar uma bare metal restore em máquinas Linux..... 290
Confirmar uma bare metal restore..... 299

6 Gerar e visualizar relatórios..... 303
Sobre os relatórios do Rapid Recovery..... 303
Gerar um relatório no Core Console..... 304
Gerenciar relatórios programados do Core Console..... 307
Como usar o menu Relatórios..... 311
Usar a barra de ferramentas Relatórios..... 312
Noções básicas sobre o relatório do trabalho..... 314
Noções básicas sobre o relatório de resumo dos trabalhos..... 314
Noções básicas sobre o relatório de falhas..... 315
Noções básicas sobre o relatório resumido..... 315
Noções básicas sobre o relatório do Repositório..... 316
O Central Management Console..... 317
Noções básicas sobre o Console de gerenciamento central do Rapid Recovery..... 317
Como configurar o Rapid Recovery Central Management Console..... 318
Como entender relatórios de núcleo do Console de Gerenciamento central..... 322

7 Noções básicas do utilitário Command Line Management do Rapid Recovery..... 324
Comandos..... 325
Arquivo..... 326
CancelActiveJobs..... 327
CheckRepository..... 328
CreateArchiveRepository..... 329
CreateBootCD..... 331
CreateRepository..... 332
DeleteRepository..... 333
Dismount..... 334
DismountArchiveRepository..... 335
EditEsxServer..... 336
Force..... 337
ForceAttach..... 338
ForceChecksum..... 339
ForceLogTruncation..... 340
ForceMount..... 341
ForceReplication..... 342
ForceRollup..... 342
ForceVirtualStandby..... 343
Ajuda..... 344
List..... 345
Montagem..... 347
MountArchiveRepository..... 348
NewCloudAccount..... 349

OpenDvmRepository....350
Pause....351
Protect....353
ProtectCluster....354
ProtectEsxServer....355
RemoveAgent....356
RemoveArchiveRepository....357
RemovePoints....358
RemoveScheduledArchive....359
RemoveVirtualStandby....360
Replicate....360
Replicação....362
RestoreAgent....364
RestoreArchive....365
RestoreUrc....366
Resume....368
SeedDrive....369
StartExport....370
UpdateRepository....373
Versão....374
VirtualStandby....375
Localização....377
Apêndice A: Referências do Core Console....378
Como ver a interface do usuário do Core Console....378
Barra de botões....379
Barra de ícones....380
Menu de navegação à esquerda....382
Como ver o painel Máquinas protegidas....385
Visualizar eventos de uma máquina protegida....387
Como ver o menu Mais para obter uma máquina protegida....389
Apêndice B: Compreender o módulo Rapid Recovery PowerShell....390
Pré-requisitos para usar o PowerShell....391
powershell.exe.config....391
Iniciar o PowerShell e importar o módulo....391
Trabalhar com comandos e cmdlets....391
Obter ajuda e exemplos de cmdlet....392
Cmdlets do módulo PowerShell do Rapid Recovery....392
Edit-EsxiVirtualStandby....395
Edit-HyperVVirtualStandby....396
Edit-ScheduledArchive....397
Edit-VBVirtualStandby....399
Edit-VMVirtualStandby....401
Get-ActiveJobs....402
Get-Clusters....403
Get-CompletedJobs....404

Get-ExchangeMailStores..... 405
Get-Failed..... 406
Get-FailedJobs..... 407
Get-Mounts..... 409
Get-Passed..... 409
Get-ProtectedServers..... 410
Get-ProtectionGroups..... 411
Get-QueuedJobs..... 412
Get-RecoveryPoints..... 413
Get-ReplicatedServers..... 414
Get-Repositories..... 415
Get-ScheduledArchives..... 416
Get-SqlDatabases..... 416
Get-UnprotectedVolumes..... 417
Get-VirtualizedServers..... 418
Get-Volumes..... 419
New-Base..... 420
New-CloudAccount..... 421
New-EncryptionKey..... 422
New-EsxiVirtualStandby..... 423
New-HyperVVirtualStandby..... 425
New-Mount..... 426
Resume-Replication..... 428
New-Repository..... 429
New-ScheduledArchive..... 430
New-Snapshot..... 432
New-VBVirtualStandby..... 432
New-VMVirtualStandby..... 434
Push-Replication..... 435
Push-Rollup..... 436
Remove-Agent..... 437
Remove-Mount..... 438
Remove-Mounts..... 439
Remove-RecoveryPoints..... 440
Remove-Repository..... 441
Remove-ScheduledArchive..... 442
Remove-VirtualStandby..... 443
Resume-Replication..... 444
Resume-Snapshot..... 445
Resume-VirtualStandby..... 446
Resume-VMExport..... 446
Start-Archive..... 447
Start-AttachabilityCheck..... 448
Start-ChecksumCheck..... 450
Start-EsxiExport..... 451

Start-HypervExport ... 452
Start-LogTruncation ... 454
Start-MountabilityCheck ... 455
Start-Protect ... 456
Start-ProtectCluster ... 457
Start-RepositoryCheck ... 458
Start-RestoreArchive ... 459
Start-ScheduledArchive ... 460
Start-VBExport ... 461
Start-VirtualStandby ... 463
Start-VMExport ... 464
Stop-ActiveJobs ... 465
Suspend-Replication ... 466
Suspend-RepositoryActivity ... 467
Suspend-ScheduledArchive ... 468
Suspend-Snapshot ... 469
Suspend-VirtualStandby ... 470
Suspend-VMExport ... 471
Update-Repository ... 472
Localização ... 473
Qualificadores ... 473
Apêndice C: Prolongamento dos trabalhos do Rapid Recovery usando scripts ... 474
Usar scripts PowerShell no Rapid Recovery ... 474
Pré-requisitos para PowerShell Scripting ... 475
powershell.exe.config ... 475
Teste dos scripts do PowerShell ... 475
Localização ... 475
Qualificadores ... 475
Parâmetros de entrada do PowerShell Scripting ... 476
AgentProtectionStorageConfiguration (espaço de nomes Replay.Common.Contracts.Agents) ... 476
AgentTransferConfiguration (espaço de nomes Replay.Common.Contracts.Transfer) ... 477
BackgroundJobRequest (espaço de nomes Replay.Core.Contracts.BackgroundJobs) ... 478
ChecksumCheckJobRequest (espaço de nomes Replay.Core.Contracts.Exchange.ChecksumChecks) ... 478
DatabaseCheckJobRequestBase (espaço de nomes Replay.Core.Contracts.Exchange) ... 479
ExportJobRequest (espaço de nomes Replay.Core.Contracts.Export) ... 479
NightlyAttachabilityJobRequest (espaço de nomes Replay.Core.Contracts.Sql) ... 479
RollupJobRequest (espaço de nomes Replay.Core.Contracts.Rollup) ... 480
TakeSnapshotResponse (espaço de nomes Replay.Agent.Contracts.Transfer) ... 480
TransferJobRequest (espaço de nomes Replay.Core.Contracts.Transfer) ... 480
TransferPrescriptParameter (espaço de nomes Replay.Common.Contracts.PowerShellExecution) ... 482
TransferPostscriptParameter (espaço de nomes Replay.Common.Contracts.PowerShellExecution) ... 482
TransferScriptParameterBase (espaço de nomes Replay.Common.Contracts.PowerShellExecution) ... 484
VirtualMachineLocation (espaço de nomes Replay.Common.Contracts.Virtualization) ... 484
VolumeImageIdsCollection (espaço de nomes Replay.Core.Contracts.RecoveryPoints) ... 484
VolumeName (espaço de nomes Replay.Common.Contracts.Metadata.Storage) ... 485

VolumeNameCollection (espaço de nomes eplay.Common.Contracts.Metadata.Storage)....485
VolumeSnapshotInfo (espaço de nomes Replay.Common.Contracts.Transfer)....485
VolumeSnapshotInfoDictionary (espaço de nomes Replay.Common.Contracts.Transfer)....486
Exemplos de scripts PowerShell....486
PreTransferScript.ps1....486
PostTransferScript.ps1....487
PreExportScript.ps1....487
PostExportScript.ps1....488
PreNightlyJobScript.ps1....488
PostNightlyJobScript.ps1....490
Usar scripts do Bourne Shell no Rapid Recovery....491
Pré-requisitos para scripts do Bourne Shell....492
Parâmetros suportados para scripts de transferência e pós-transferência....492
Testar os scripts do Bourne Shell....492
Parâmetros de entrada para scripts do Bourne Shell....493
TransferPrescriptParameters_VolumeNames....493
TransferPostscriptParameter....493
Exemplos de scripts do Bourne Shell....494
PreTransferScript.sh....494
PostTransferScript.sh....495
PostExportScript.sh....495
Apêndice D: APIs do Rapid Recovery....496
Público-alvo....496
Trabalhar com as APIs REST do Rapid Recovery....496
Fazer download e visualizar as APIs de Core e Agente....496
Leitura adicional recomendada....498
Sobre a Dell....499
Como entrar em contato com a Dell....499
Recursos do suporte técnico....499
Glossário....500

1

Introdução ao dispositivo DL

O dispositivo DL com software Rapid Recovery é uma solução de backup, replicação e recuperação que oferece objetivos de tempo de recuperação quase a zero e objetivos de ponto de recuperação. O Rapid Recovery oferece proteção de dados, recuperação de desastres, migração de dados e gestão de dados. Você precisa da flexibilidade para realizar restaurações sem sistema operacional (para equipamentos similares ou diferentes) e pode restaurar backups para máquinas virtuais ou físicas, independentemente da origem. Com o Rapid Recovery, você pode replicar para um ou mais destinos para maior redundância e segurança.

Seu dispositivo define um novo padrão para proteção de dados unificada ao combinar backup, replicação e recuperação em uma única solução projetada para ser o backup mais rápido e confiável para proteção de máquinas virtuais (MVs), máquinas físicas e ambientes na nuvem. Seu dispositivo é capaz de processar até petabytes de dados com deduplicação global incluída, compressão, criptografia e replicação para qualquer infraestrutura de nuvem pública ou privada. Aplicações de servidor e dados podem ser recuperados em minutos para retenção e conformidade de dados.

O dispositivo suporta ambientes de multi-hipervisor nas nuvens privadas e públicas do VMware vSpheree Microsoft Hyper-V.

O Rapid Recovery oferece:

- **Flexibilidade**. Você pode realizar recuperação universal para múltiplas plataformas, incluindo restauração de físico para virtual, virtual para físico, virtual para virtual e físico para físico.
- **Integração com a nuvem**. Você pode arquivar e replicar para a nuvem, usando provedores de armazenamento na nuvem com suporte para plataformas de código aberto e exclusivas.
- **Deduplicação inteligente**. Você pode reduzir os requisitos de armazenamento ao armazenar dados uma vez e consultá-los depois (uma vez por repositório ou domínio de criptografia).
- **Recuperação instantânea**. Nosso recurso de recuperação em tempo real permite que você acesse dados críticos primeiro, enquanto as operações de restauração restantes são concluídas paralelamente.
- **Recuperação a nível de arquivo**. Você pode recuperar dados a nível de arquivo em premissas, em um local remoto ou pela nuvem.
- **Suporte virtual**. O suporte aprimorado para virtualização inclui proteção sem agente e descoberta automática para VMware® ESXi™ 5 e superiores e exportação para volumes de cluster comum Microsoft® Hyper-V®.

Consulte os recursos a seguir para obter mais informações sobre o Rapid Recovery.

- O site de suporte do produto Dell Rapid Recovery está disponível em https://support.software.dell.com/rapid-recovery/
- O site de documentação em https://support.software.dell.com/rapid-recovery/release-notes-guides/ e http://www.dell.com/support/home/.

Tópicos:

- Arquitetura de implantação
- Recursos do produto

Arquitetura de implantação

O dispositivo é um produto de backup escalonável e recuperação, implantado de maneira flexível em uma empresa ou como um serviço entregue por um fornecedor de serviço gerenciado. O tipo de implantação depende do tamanho e dos requisitos do cliente. A preparação para implantar o dispositivo envolve planejar a topologia do armazenamento de rede, o hardware do núcleo, a infraestrutura de recuperação de desastres e a segurança.

A arquitetura de implantação consiste em componentes locais e remotos. Os componentes remotos podem ser opcionais para os ambientes que não exigem o uso de um local de recuperação de desastres ou um fornecedor de serviço gerenciado para a recuperação

externa. A implantação local básica consiste em um servidor de backup chamado de Core e uma ou mais máquinas protegidas. O componente externo é habilitado usando a replicação, que fornece capacidades de recuperação total no local de DR. O Core usa imagens básicas e instantâneos incrementais para compilar pontos de recuperação das máquinas protegidas.

Além disso, o dispositivo reconhece os aplicativos, pois pode detectar a presença do Microsoft Exchange e do SQL e dos respectivos bancos de dados e arquivos de log e, em seguida, agrupar esses volumes automaticamente com dependência para uma proteção abrangente e uma recuperação eficaz. Isso garante que você nunca terá backups incompletos ao realizar as recuperações. Os backups são realizados com o uso de instantâneos de nível de bloco com reconhecimento do aplicativo. O dispositivo também pode realizar a truncagem de log do Microsoft Exchange e dos SQL Servers protegidos.

O diagrama a seguir descreve uma implantação simples. Nesse diagrama, o software AppAssure Agent é instalado nas máquinas, por exemplo, um servidor de arquivos, servidor de e-mail, servidor de banco de dados ou máquinas virtuais, e conecta-se e é protegido por um único Core, que também consiste em um repositório central. O Portal de licenças gerencia as assinaturas de licenças, os grupos e usuários das máquinas protegidas e núcleos em seu ambiente. O Portal de licenças permite que os usuários façam login, ativem contas, façam download de software, e implantem máquinas protegidas e núcleos conforme a licença referente ao seu ambiente.

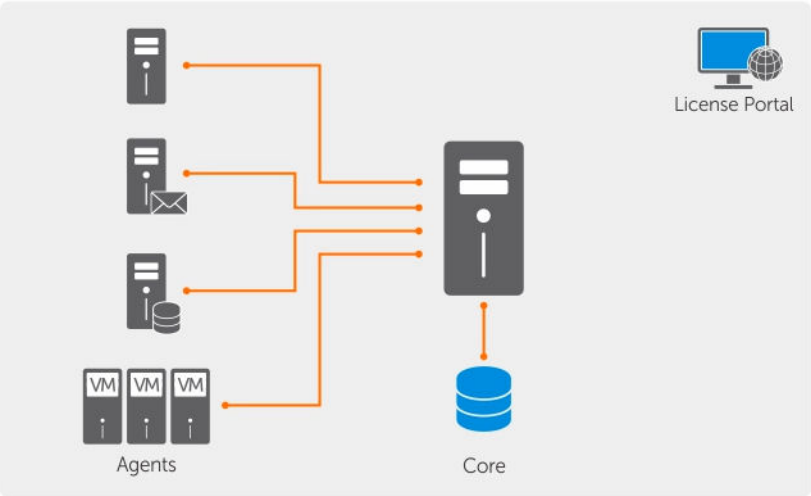


Figura 1. Arquitetura de implantação básica

Você pode também implantar múltiplos núcleos, conforme mostrado no diagrama a seguir. Um console central gerencia múltiplos núcleos.

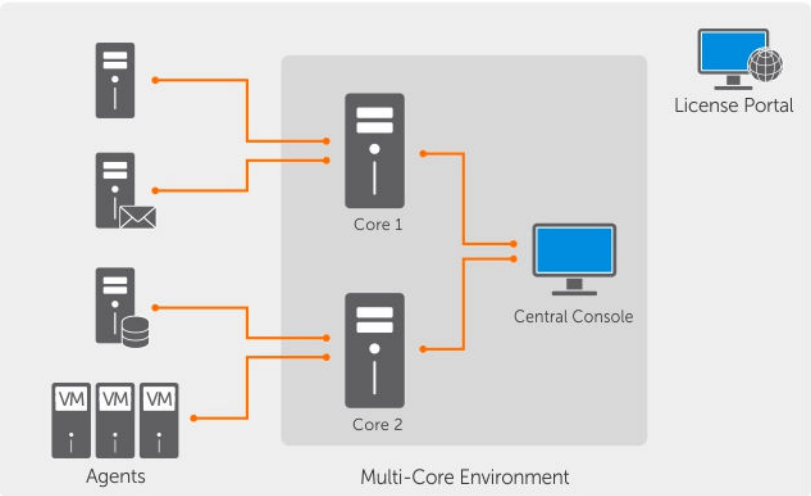


Figura 2. Arquitetura de implantação de múltiplos núcleos

Smart Agent

O Smart Agent rastreia os blocos alterados no volume de disco e depois salva uma imagem dos blocos alterados em um intervalo de proteção pré-definido. A abordagem de instantâneos de nível de bloco perpétua e incremental evita a cópia repetida dos mesmos dados da máquina protegida para o core. O Rapid Recovery Smart Agent é instalado nas máquinas que são protegidas pelo Rapid Recovery Core.

O SmartAgent reconhece aplicativos e detecta o tipo de aplicativo instalado e também o local dos dados. Ele agrupa automaticamente os volumes de dados com dependência, como bancos de dados e, em seguida registra-os juntos para a proteção eficaz e a rápida recuperação. Depois que o software Rapid Recovery Agent é configurado, ele usa a tecnologia inteligente para rastrear os blocos alterados nos volumes do disco protegido. Quando o instantâneo está pronto, é transferido rapidamente para o Coreusando conexões inteligentes de múltiplos threads e baseadas em soquete. Para preservar largura de banda da CPU e memória nas máquinas protegidas, o Smart Agent não criptografa nem deduplica os dados na origem e as máquinas protegidas são emparelhadas comum Core para a proteção.

Dispositivo DL Core

O Core é o componente central da arquitetura de implementação. O Core armazena e gerencia todos os backups de máquina e fornece os serviços de núcleo para backup, recuperação e retenção, replicação, arquivamento e gerenciamento. O Core é um computador autocontido endereçável da rede que executa uma de 64 bits do sistema operacional Microsoft Windows. O dispositivo realiza a compressão in-line baseada no destino, criptografia e deduplicação dos dados recebidos da máquina protegida. Em seguida, o Core armazena os backups do instantâneo em repositórios, como SAN (Storage Area Network) ou DAS (Direct AttachedStorage).

O repositório também pode residir no armazenamento interno dentro do Core. O Core é gerenciado acessando o seguinte URL em um navegador da Web: **https://CORENAME:8006/apprecovery/admin**. Internamente, todos os serviços do Core são acessíveis através de APIsREST. Os serviços do Core podem ser acessados de dentro do próprio Core ou diretamente via Internet, em qualquer aplicativo que possa enviar uma solicitação HTTP/HTTPS e receber uma resposta HTTP/HTTPS. Todas as operações do API são realizadas via SSL e mutuamente autenticadas usando certificados X.509 v3.

Os núcleos são emparelhados com outros núcleos para replicação.

Processo de instantâneos

Um instantâneo é quando uma imagem de base é transferida de uma máquina protegida para o core. Instantâneos capturam e armazenam o estado de um volume de disco em um determinado ponto no tempo quando os aplicativos que geram os dados ainda estão em uso. No Rapid Recovery, você pode forçar um instantâneo, pausar instantâneos temporariamente e visualizar as listas de pontos de recuperação atuais no repositório, além de apagá-las, se necessário. Pontos de recuperação são usados para restaurar máquinas protegidas ou para montar para um sistema de arquivos local. Os instantâneos que são capturados pelo Rapid Recovery são feitos a nível de bloco e possuem conhecimento de aplicativo. Isto significa que todas as transações em aberto e logs de transação em andamento são concluídos e caches são eliminados para o disco antes de criar o instantâneo.

O Rapid Recovery usa um driver de filtro de volume de baixo nível que anexa os volumes montados e depois acompanha todas as mudanças de nível de bloco para o próximo instantâneo iminente. Os serviços de sombra de volume (VSS) da Microsoft são usados para facilitar instantâneos consistentes de travamentos de aplicativos.

Replicação do site de recuperação de desastres ou provedor de serviços

O processo de replicação exige uma relação de origem e destino emparelhados entre dois núcleos. O núcleo de origem copia os pontos de recuperação das máquinas protegidas e, em seguida, os transmite de maneira assíncrona e contínua para um núcleo de destino em um site remoto de recuperação de desastres. O local externo pode ser um data center da empresa (núcleo autogerenciado), um local de um

fornecedor de serviço gerenciado por terceiros (MSPs) ou um ambiente de nuvem. Ao replicar para um MSP, você pode usar os fluxos de trabalho integrados que permitem solicitar conexões e receber notificações automáticas de feedback. Para a transferência inicial dos dados, você pode realizar a propagação de dados usando a mídia externa, o que é útil para grandes conjuntos de dados ou sites com links lentos.

No caso de uma suspensão temporária de força grave, o dispositivo suporta failover e failback em ambientes replicados. No caso de uma suspensão temporária de força abrangente, o núcleo de destino no local secundário pode recuperar instâncias das máquinas protegidas replicadas e iniciar imediatamente a proteção nas máquinas que passaram por failover. Após a restauração do local primário, o núcleo replicado pode realizar o failback dos dados das instâncias recuperadas de volta para as máquinas protegidas no local primário.

Recuperação

A recuperação pode ser feita no local ou no local remoto replicado. Depois que a implantação estiver em estado fixo com a proteção local e a replicação opcional , o Core permitirá que você realize a recuperação usando a Recuperação verificada, Recuperação universal ou Recuperação em tempo real.

Recursos do produto

Você pode gerenciar a proteção e a recuperação de dados críticos usando os seguintes recursos e funcionalidades:

- Repository (Repositório)
- Desduplicação no Rapid Recovery
- Criptografia
- Replicação
- Retenção e arquivamento
- Virtualização e nuvem
- Gerenciamento de alertas e eventos
- Portal de licenças
- Console web
- APIs de gerenciamento de serviço

Como entender repositórios

Um repositório é um local central no qual os dados de instantâneo de backup capturados de suas estações de trabalho e servidor protegidos são armazenados e gerenciados. Os dados são salvos em um repositório na forma de pontos de recuperação.

Um repositório pode residir em diferentes tecnologias de armazenamento, incluindo rede de área de armazenamento (SAN), armazenamento conectado diretamente (DAS) ou armazenamento conectado à rede (NAS).

NOTA: Armazene os repositórios do Rapid Recovery Core em dispositivos de armazenamento primários. A velocidade do volume de armazenamento é o fator mais crítico. Os dispositivos de armazenamento de arquivamento, como domínio de dados, não são compatíveis devido a limitações de desempenho. Da mesma forma, não armazene repositórios em arquivadores NAS com camada para a nuvem, uma vez que esses dispositivos tendem a ter limitações de desempenho quando usados como armazenamento primário.

O DAS oferece a mais alta largura de banda de dados e a mais rápida taxa de acesso, além de proporcionar fácil implementação. Para obter os melhores resultados, use DAS com armazenamento de matriz redundante de discos independentes (RAID) 6. Para obter mais informações, consulte o Artigo de banco de dados Dell 118153, "Opções de repositório: Armazenamento conectado diretamente, rede de área de armazenamento ou armazenamento conectado à rede."

O local de armazenamento para qualquer repositório sempre deve estar em um subdiretório que você especificar (por exemplo, **E:\Repository**), e nunca na raiz do volume (por exemplo, **E:**).

O formato de repositório Rapid Recovery usa o gerenciador de volume de deduplicação (DVM). Os repositórios DVM oferecem suporte para múltiplos volumes, com até 255 repositórios em um único Core, e o uso de extensões. Só é possível criar repositórios DVM em máquinas com sistemas operacionais Windows. Você pode usar esse tipo de repositório ao usar novas instalações do Rapid Recovery. É possível especificar o tamanho de um repositório DVM na criação e posteriormente adicionar extensões.

Entre os recursos e atributos do repositório DVM, estão:

- Suporte para recuperação por pontos de recuperação e arquivamentos Rapid Recovery 6.x
- Suporte para locais de armazenamento apenas no SO Windows. O volume de repositório pode ser local (no armazenamento conectado ao servidor Core) ou em um local de armazenamento em um local compartilhado de sistema de arquivos de Internet comum (CIFS).
- Os tipos de armazenamento compatíveis incluem rede de área de armazenamento (SAN), armazenamento conectado diretamente (DAS) ou armazenamento conectado à rede (NAS).
- Exige 8 GB de memória RAM, preferencialmente a memória de verificação e correção de erros (ECC)
- Exige processador de oito núcleos na máquina Core (esse requisito de longa data agora é obrigatório)
- Oferece suporte para múltiplos repositórios DVM por host
- Nenhum serviço adicional é necessário; o repositório DVM usa serviços nativos do Core para comunicação com o Core e para rastreamento de eventos
- Cada repositório DVM oferece suporte para até 4.096 extensões de repositório (também chamadas de locais de armazenamento)
- O tamanho é fixo; o repositório DVM exige que você especifique o tamanho de repositório em um volume. O tamanho especificado não pode ultrapassar aquele do volume. Cada volume definido como um local de armazenamento deve ter no mínimo 1 GB de espaço livre disponível.
- O local de armazenamento de repositório pode ser um disco dinâmico ou simples, sendo que a velocidade é o fator mais importante
- É possível usar chaves de criptografia padrão criadas e gerenciadas no Core Console (criptografia baseada no Core)
- Deduplica dados em todo o repositório (ou entre domínios de criptografia dentro de cada repositório, se chaves de criptografia forem usadas)
- Usa um cache de deduplicação de DVM redimensionável e exclusivo, com local de armazenamento configurável nas definições do Core
- Otimizado para gravação de dados, armazenando dados de instantâneos em um local de repositório no Core, com todos os dados processados pelo Core
- Não pode ser renomeado após a criação
- Novos repositórios desse tipo podem ser criados usando APIs REST, o utilitário de gerenciamento de linha de comando (cmdutil.exe) do Rapid Recovery ou o cmdlet do Windows PowerShell®

Ao criar um repositório DVM, o Rapid Recovery Core pré-aloca o espaço de armazenamento necessário para os dados e metadados no local especificado. O tamanho mínimo de repositório DVM é de 1 GB, que, para fins práticos, é normalmente muito pouco, exceto para testes.

Uma vez que a deduplicação DVM exige um cache primário e secundário, certifique-se de que o espaço de armazenamento reservado seja duas vezes ao seu cache de deduplicação. Por exemplo, se você reservou 1,5 GB nas configurações de cache de deduplicação DVM no Core, reserve 3 GB no volume de cache. O caminho de instalação padrão para o cache é a unidade C. Para obter mais informações, consulte Noções básicas sobre o cache de deduplicação e locais de armazenamento.

Você pode criar múltiplos repositórios independentes associados a um único Core, com até 255 repositórios DVM. Os repositórios podem englobar diferentes tecnologias de armazenamento.

Você pode ainda aumentar o tamanho de um repositório DVM ao adicionar novas extensões ou especificações de arquivo. Um repositório estendido pode conter até 4.096 extensões que englobam diferentes tecnologias de armazenamento.

Para obter mais informações sobre como trabalhar com repositórios DVM, consulte Gerenciamento de um repositório de DVM.

Desduplicação no Rapid Recovery

A desduplicação é uma técnica de compressão de dados que reduz os requisitos de armazenamento e a carga da rede. O processo envolve armazenar fisicamente os blocos de dados exclusivos somente uma vez no disco. No Rapid Recovery, quando um bloco de dados exclusivo ocorre uma segunda vez em um repositório, em vez de armazenar os dados novamente, uma referência virtual aos dados é armazenada.

A desduplicação ocorre nos snapshots de backup capturados pelo Rapid Recovery Core. As informações do backup são desduplicadas dentro de um único repositório. Elas não podem ser desduplicadas em múltiplos repositórios.

O Rapid Recoveryversão 6.0.2 usa a desduplicação baseada no destino para todos os repositórios de DVM. Nesse modelo, as informações são transferidas para o repositório de DVM (o destino) e, em seguida, são desduplicadas a partir do repositório.

Na maioria das vezes a desduplicação ocorre em linha (durante a transferência das informações de backup).

Para o máximo em ganhos, agora o Rapid Recovery também oferece a desduplicação ocorrendo como pós-processamento. O pós-processamento às vezes é chamado de desduplicação de passagem. Usando esse modelo, os dados no repositório são comparados com referências no cache de dados de DVM. Se um bloco de dados no repositório já foi salvo, cada ocorrência adicional desses dados será substituída por um ponteiro ou referência aos dados.

Esse pós-processamento pode economizar espaço no seu volume de armazenamento do repositório, particularmente se o cache de desduplicação foi preenchido e subsequentemente aumentado para aproveitar as vantagens adicionais da desduplicação. Esse tipo de desduplicação ocorre ao realizar um trabalho de otimização do repositório. Esse recurso é exclusivo dos repositórios de DVM e também é chamado de recuperação do bloco duplicado.

Para obter mais informações sobre o trabalho de otimização do repositório, consulte Sobre o trabalho de otimização do repositório. Para obter mais informações sobre como realizar essa tarefa, consulte Otimização de um repositório de DVM.

Portanto, o Rapid Recovery aproveita as vantagens de todos os tipos de desduplicação descritos aqui: baseada no destino, em linha e pós-processamento.

Para obter mais informações sobre o local em que as referências para os blocos exclusivos estão armazenadas para os repositórios de DVM, consulte Noções básicas sobre o cache de deduplicação e locais de armazenamento.

Compreender as chaves de criptografia

O Rapid Recovery Core pode criptografar dados de instantâneo para todos os volumes em qualquer repositório sem usar chaves de criptografia que você define e gerencia no Core Cosole.

Em vez de criptografar todo o repositório, o Rapid Recovery permite que você especifique uma chave de criptografia para uma ou mais máquinas em um único Rapid Recovery Core. Cada chave de criptografia ativa cria um domínio de criptografia. Não há limite para o número de chaves de criptografia que podem ser criadas no core.

Em um ambiente de múltiplos inquilinos (quando um único core hospeda múltiplos domínios de criptografia), os dados são particionados e deduplicados dentro de cada domínio de criptografia. Como resultado, a Dell recomenda o uso de uma única chave de criptografia para múltiplas máquinas protegidas se você quiser maximizar os benefícios da deduplicação entre um conjunto de máquinas protegidas.

Você também pode compartilhar chaves de criptografia entre os cores usando um dos três métodos. Um método é exportar uma chave de criptografia como um arquivo do Rapid Recovery Core e importá-la para outro core. Um segundo método é arquivar dados protegidos com uma chave de criptografia e depois importar esses dados arquivados para outro Rapid Recovery Core. O terceiro método é replicar pontos de recuperação de uma máquina protegida usando uma chave de criptografia. Depois de replicar as máquinas protegidas, as chaves de criptografia usadas no core de origem aparecem como chaves de criptografia replicadas no core de destino.

Em todos os casos, depois de importada, qualquer chave de criptografia aparece no core com o estado Locked (Bloqueada). Para acessar os dados de uma chave de criptografia bloqueada, você deve desbloqueá-la. Para obter informações sobre como importar, exportar, bloquear ou desbloquear chaves de criptografia, consulte o tópico Gerenciar chaves de criptografia.

Entre os principais conceitos e considerações de segurança, estão:

- A criptografia é realizada usando o padrão de criptografia avançada (AES) de 256 bits no modo CBC (Cipher Block Sequenciamento de blocos de cifras) que está em conformidade com o SHA-3.
- A eliminação de duplicação opera dentro de um domínio de criptografia para garantir a privacidade.
- A criptografia é executada sem afetar o desempenho.
- Você pode aplicar uma única chave de criptografia a qualquer número de máquinas protegidas, mas qualquer máquina protegida só pode ter uma chave de criptografia aplicada por vez.
- Você pode adicionar, remover, importar, exportar, modificar e apagar as chaves de criptografia que estão configuradas no Rapid Recovery Core.

CUIDADO: O Rapid Recovery salva um novo instantâneo sempre que você aplica uma chave de criptografia a uma máquina protegida. Um novo instantâneo também é acionado depois de você desassociar uma chave de criptografia para uma máquina protegida.

Chaves de criptografia geradas do Rapid Recovery Core são arquivos de texto que contêm quatro parâmetros, como descrito na tabela a seguir:

Tabela 1. Componentes de uma chave de criptografia

Componente	Descrição
Nome	Esse valor é equivalente ao nome de chave fornecido ao adicionar uma chave no Rapid Recovery Core Console.
Tecla	Esse parâmetro é composto de 107 caracteres alfabéticos, numéricos e operadores matemáticos americanos gerados aleatoriamente.
ID	A ID é composta de 26 caracteres americanos em letras maiúsculas e minúsculas.
Comment (Comentário)	O Comentário contém o texto da descrição de chave inserido na criação da chave.

Replicação com Rapid Recovery

Esta seção fornece informações conceituais e de procedimentos para ajudá-lo a entender e configurar a replicação no Rapid Recovery.

Replicação é um processo de copiar pontos de recuperação de um Rapid Recovery Core e transmiti-los para outro Rapid Recovery Core visando a recuperação de desastres. O processo exige uma solução com pares de origem/destino entre dois ou mais Cores.

O Core de origem copia os pontos de recuperação de máquinas protegidas selecionadas e então transmite de modo assíncrono e contínuo os dados de snapshot para o Core de destino.

A menos que você a altere o comportamento padrão, definindo um programa de reaplicação, o Core inicia um trabalho de replicação imediatamente após a conclusão de cada snapshot de backup, verificação de soma de verificação, verificação de capacidade de anexação e trabalhos noturnos. Para obter informações, consulte Programar a replicação.

Para obter melhor segurança de dados, os administradores geralmente usam um Core de destino em uma localidade remota de recuperação de desastres. É possível configurar a replicação de saída para um data center de propriedade da empresa ou para uma localidade remota de recuperação de desastres (ou seja, um Core de destino "autogerenciado"). Ou é possível configurar a replicação de saída para um provedor de serviços gerenciados (MSP) terceirizado ou provedor de nuvem que hospede serviços de recuperação após desastres e cópia de segurança em um site externo. Ao replicar para um Core de destino de terceiros, é possível usar fluxos de trabalho incorporados que permitam solicitar conexões e receber notificações automáticas de feedback.

A replicação é gerenciada por máquina protegida. Qualquer máquina (ou todas as máquinas) protegida ou replicada em um Core de origem pode ser configurada para replicar em um Core de destino.

Os possíveis cenários de replicação incluem:

- **Replicação para uma localização local**. O Core de destino situa-se em um datacenter local ou localização no local e a replicação é sempre mantida. Nessa configuração, a perda do Core não impediria a recuperação.
- **Replicação para uma localização externa**. O Core de destino está localizado em uma instalação de recuperação após desastres externa para recuperação em caso de perda.
- **Replicação mútua**. Dois datacenters em locais diferentes, cada um contendo um Core, protegendo máquinas e atuando mutuamente como cópia de segurança externa para recuperação após desastres. Nesse cenário, cada Core replica as máquinas protegidas do Core localizado no outro datacenter.
- **Replicação hospedada e na nuvem**. Os parceiros MSP do Rapid Recovery mantêm vários Cores de destino em um datacenter ou uma nuvem pública. Em cada um desses Cores, o parceiro MSP permite que um ou mais dos seus clientes replique os pontos de recuperação a partir de um Core de origem no local do cliente para o Core de destino do MSP por uma taxa.

NOTA: Nesse cenário, os clientes têm acesso apenas aos seus próprios dados.

As possíveis configurações de replicação incluem:

- **Replicação ponto-a-ponto**. Replica uma ou mais máquinas protegidas de um único Core de origem para um único Core de destino.

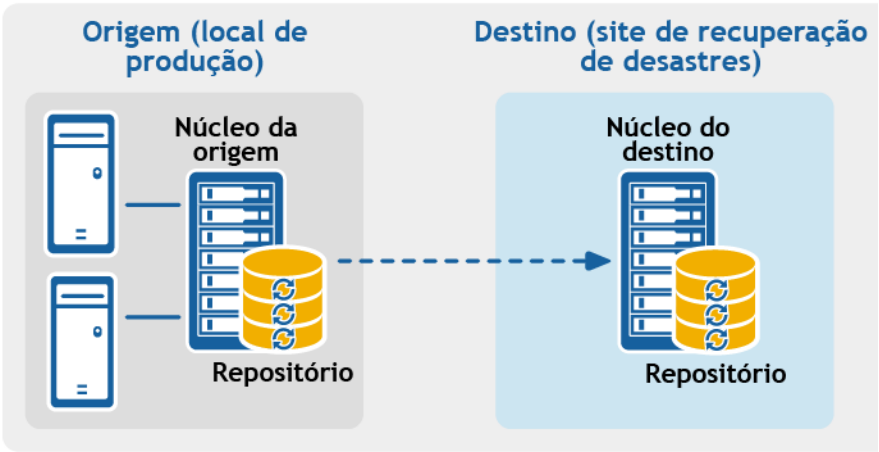


Figura 3. Configuração de replicação ponto-a-ponto

- **Replicação multiponto-a-ponto**. Replica máquinas protegidas de vários Cores de origem para um único Core de destino.

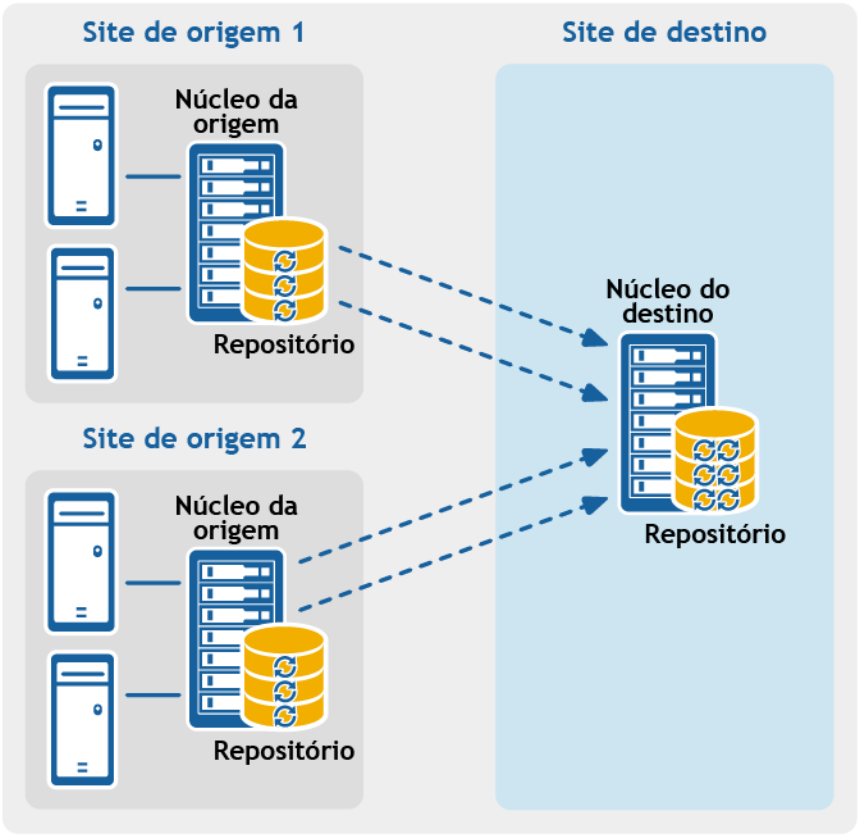


Figura 4. Configuração de replicação de multiponto-a-ponto

- **Replicação de ponto-a-multiponto**. Replica uma ou mais máquinas protegidas de um único Core de origem para mais de um Core de destino.

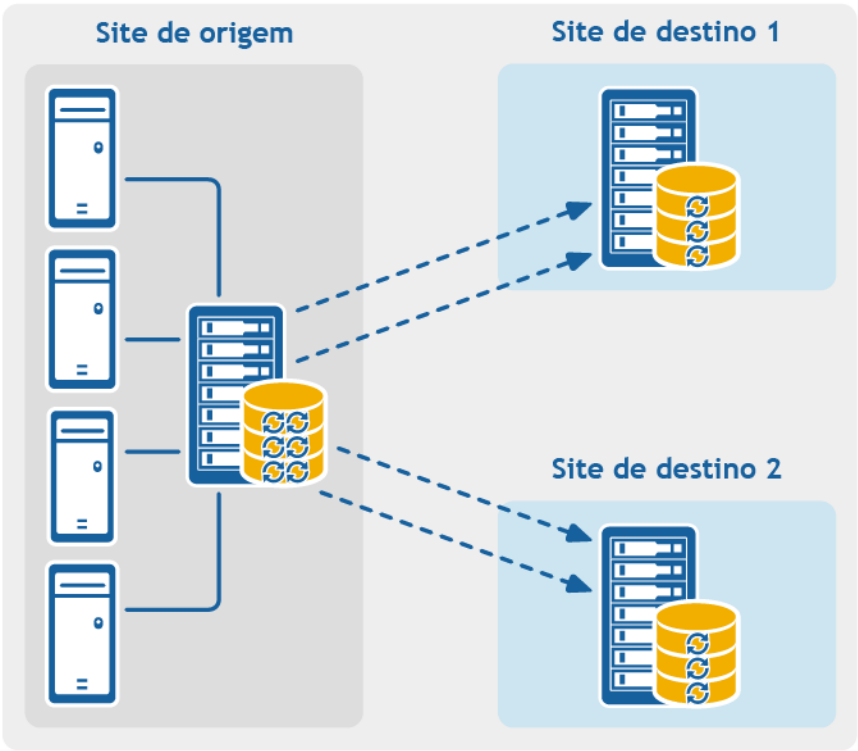


Figura 5. Configuração de replicação ponto-a-multiponto

- **Replicação de saltos múltiplos.** Replica uma ou mais máquinas protegidas de um Core de destino para outro Core de destino, produzindo opções e ativação adicional pós-falha ou recuperação no Core replicado.

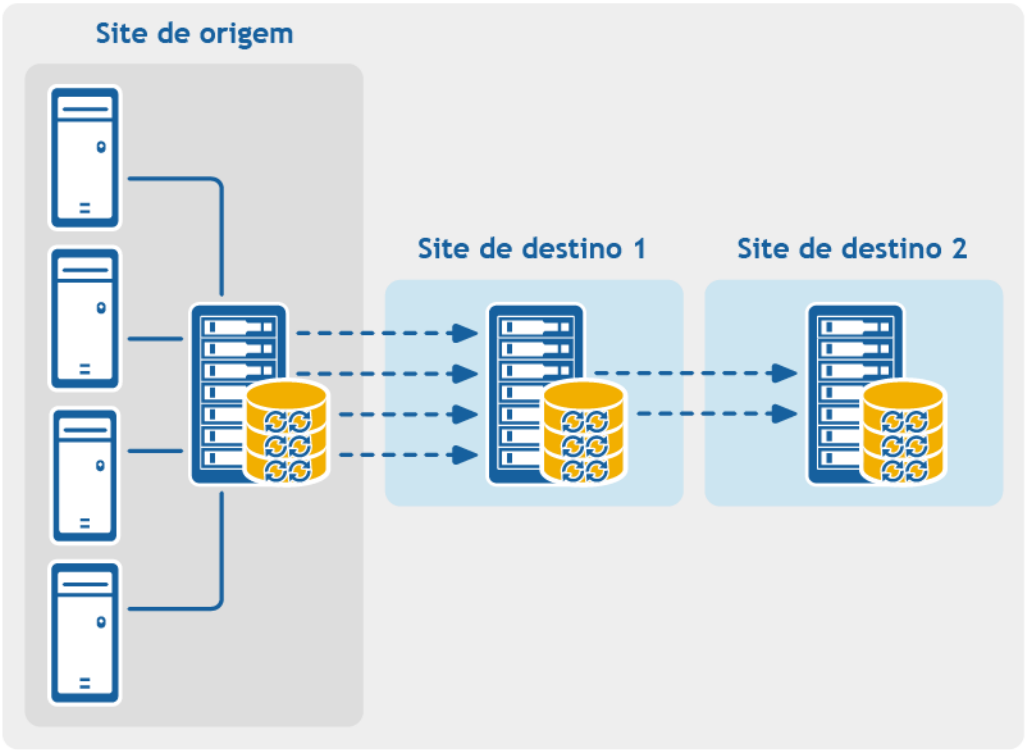


Figura 6. Configuração de replicação de saltos múltiplos

Se o uso dos appliances de backup de proteção de dados Dell como a série DL1x00 ou DL4x00, o Core de destino para o qual você replicar deve ter uma licença de software válida configurada. Esses appliances de hardware incluem uma licença de destino de replicação com a compra. Verifique a chave de licença na mensagem de e-mail de boas-vindas que você recebeu quando adquiriu o appliance. Para obter assistência, visite o site de Assistência à aplicação da licença https://support.software.dell.com/licensing-assistance ou e-mail license@software.dell.com.

Retenção e arquivamento

No dispositivo, as políticas de backup e retenção são flexíveis e, portanto, facilmente configuráveis. A capacidade de adaptar as políticas de retenção às necessidades da organização não apenas ajudam a atender aos requisitos de conformidade, mas o fazem sem comprometer o RTO.

As políticas de retenção impõem os períodos em que os backups são armazenados em mídias de curto prazo (rápidas e caras). Às vezes, certos requisitos técnicos e corporativos obrigam a retenção estendida desses backups, mas o armazenamento rápido tem um custo proibitivo. Portanto, esse requisito cria uma necessidade de armazenamento de longo prazo (lento e barato). Frequentemente, as empresas usam o armazenamento de longo prazo para arquivamento de dados de conformidade e não conformidade. O recurso de arquivamento suporta retenções estendidas para dados de conformidade e não conformidade e também pode ser usado para o seeding dos dados de replicação para um núcleo de destino.

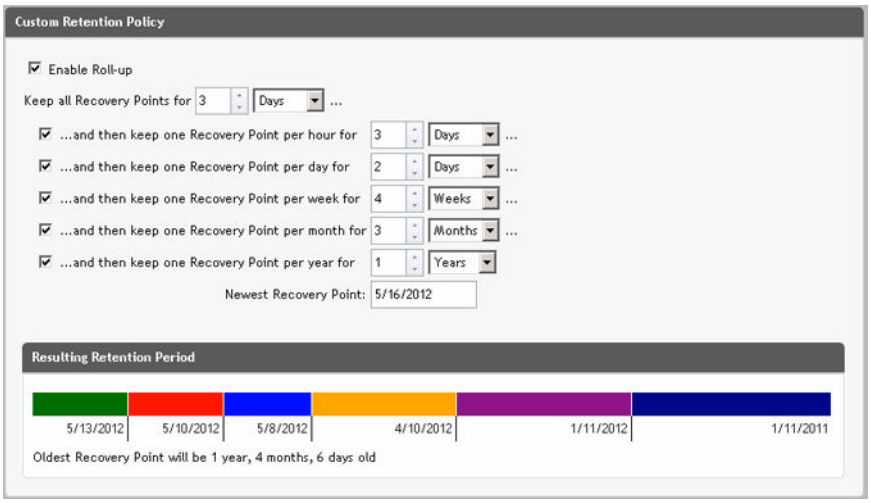


Figura 7. Política de retenção personalizada

No dispositivo, as políticas de retenção podem ser personalizadas para especificar o período em que o ponto de recuperação de backup é mantido. Quando os pontos de recuperação se aproximam do fim do período de retenção, eles tornam-se obsoletos e são removidos do pool de retenção. Tipicamente , esse processo torna-se ineficiente e falham, pois a quantidade de dados e o período de retenção começam a aumentar rapidamente. O dispositivo resolve o problema dos big data gerenciando a retenção de grandes quantidades de dados com políticas de retenção complexas e realizando operações de implantação para os dados que estão se tornando obsoletos, usando operações de metadados eficientes.

Os backups podem ser feitos com um intervalo de alguns minutos. Conforme esses backups envelhecem com os dias, meses e anos, as políticas de retenção gerenciam a obsolescência e o apagamento dos backups antigos. Um simples método de cascata define o processo de obsolescência. Os níveis dentro da cascata são definidos em minutos, horas, dias, semanas, meses e anos. A política de retenção é imposta pelo processo de implantação noturna.

Para o arquivamento de longo prazo, o dispositivo permite criar um arquivamento do núcleo de origem ou destino em qualquer mídia removível. O arquivamento é otimizado internamente e todos os dados no arquivamento são compactados, criptografados e desduplicados. Se o tamanho total do arquivamento for maior que o espaço disponível na mídia removível, o arquivamento ocupa vários dispositivos com base no espaço disponível na mídia. O arquivamento também pode ser bloqueado com uma senha. A recuperação de um arquivamento não exige um novo núcleo; qualquer núcleo pode ingerir o arquivamento e recuperar os dados se o administrador tiver a senha e as chaves de criptografia.

Virtualização e nuvem

O Core é pronto para a nuvem, o que permite que você utilize a capacidade de computação da nuvem para a recuperação.

O dispositivo pode exportar qualquer máquina protegida ou replicada para uma máquina virtual, como versões licenciadas do VMware ou Hyper-V. Você pode realizar uma exportação virtual única ou estabelecer uma MV de espera virtual através de uma exportação virtual contínua. Com a exportação contínua, a máquina virtual é atualizada de forma incremental depois de cada instantâneo. As atualizações incrementais são muito rápidas e fornecem clones de espera que estão prontos para serem ligados, com um clique de um botão. Os tipos suportados de exportação da máquina virtual são a estação de trabalho/servidor VMware de uma pasta; exportação direta para um host vSphere/VMware ESX(i); exportação para Oracle VirtualBox; e exportação para Microsoft Hyper-V Server no Windows Server 2008 (x64), 2008 R2, 2012 (x64) e 2012 R2 (incluindo o suporte para MVs do Hyper-V geração 2)

Além disso, agora você pode arquivar os dados do repositório na nuvem usando Microsoft Azure, Amazon S3, Rackspace Cloud Block Storage ou outros serviços OpenStack baseados em nuvem.

Gerenciamento de alertas e eventos

Além do HTTP REST API, o dispositivo contém um amplo conjunto de recursos de notificação e registro de eventos usando o e-mail, o Syslog ou o Log de eventos do Windows. As notificações de e-mail podem ser usadas para alertar os usuários ou grupos sobre a integridade ou o status de diferentes eventos em resposta a um alerta. Os métodos Log de eventos do Windows e Syslog são usados para fazer o login centralizado em um repositório em um ambiente com múltiplos sistemas operacionais. Nos ambientes com Windows, somente o Log de eventos do Windows é usado.

Portal de licenças

O Portal de licenças fornece ferramentas fáceis de usar para gerenciar os direitos de licença. Você pode fazer o download, ativar, ver e gerenciar as chaves de licença e criar um perfil da empresa para rastrear os seus ativos de licença. Além disso, o portal permite que os provedores de serviços e revendedores rastreiem e gerenciem as licenças de seus clientes.

Console Web

O dispositivo inclui um novo console central baseado na web que gerencia os núcleos distribuídos de um local central. MSPs e clientes corporativos com múltiplos núcleos distribuídos podem implementar o console central para obter uma visão unificada para a gerência central. O console central permite a capacidade de organizar os núcleos gerenciados em unidades organizacionais hierárquicas. Essas unidades organizacionais podem representar unidades de negócios, locais ou os clientes para MSPs com acesso baseado em funções. O console central também pode realizar relatórios nos núcleos gerenciados.

APIs de gerenciamento de serviço

O dispositivo é agregado a um API de gerenciamento de serviço e fornece acesso programático a todas as funcionalidades disponíveis no Central Management Console. O API de gerenciamento de serviço é um REST API. Todas as operações do API são executadas via SSL e mutuamente autenticadas usando certificados X.509 v3. O serviço de gerenciamento pode ser acessado de dentro do ambiente ou diretamente via Internet, de qualquer aplicativo que possa enviar e receber uma solicitação e resposta HTTPS. Essa abordagem facilita a integração com qualquer aplicativo Web, como ferramentas de metodologia de gerenciamento de relacionamentos (RMM) ou sistemas de faturamento. Também é fornecido um cliente SDK para o script PowerShell.

2

Trabalhar com o dispositivo DL Core

Noções básicas do Rapid Recovery Core Console

Esta seção descreve os diferentes elementos da interface de usuário do Rapid Recovery Core Console.

Acesso ao Rapid Recovery Core Console

Conclua as etapas a seguir para acessar o Rapid Recovery Core Console.

- Execute um dos seguintes para acessar o Rapid Recovery Core Console:
  a Faça login localmente no servidor do Rapid Recovery Core e, em seguida, clique duas vezes no ícone do Core Console.
  b Ou digite uma das seguintes URLs no seu navegador da Web:
    - https://<yourCoreServerName>:8006/apprecovery/admin/ ou
    - https://<yourCoreServerIPaddress>:8006/apprecovery/admin/

> **NOTA: Como a interface do usuário do Rapid Recovery Core Console é dependente do JavaScript, o navegador da Web usado para acessar o Core Console deve ter o JavaScript ativado.**
>
> Se você alterou a porta padrão do serviço Rapid Recovery, atualize a porta conforme necessário na URL acima.

Noções básicas sobre o Guia de início rápido

O Guia de Início Rápido é um recurso que oferece a você um fluxo guiado de tarefas sugeridas para configuração e uso do Rapid Recovery Core.

O Guia de início rápido é exibido automaticamente na primeira vez que você atualiza ou instala o Rapid Recovery Core e navega até o Core Console. Clique em **Guia de Inicialização** na página **Bem-Vindo** do guia para ver as várias tarefas de configuração sugeridas. Navegue pelo guia usando as opções **Ignorar etapa** e **Voltar**. Quando tiver visto a última tarefa sugerida, clique em **Concluir** para fechar o guia.

Você pode abrir o Guia de Início Rápido novamente a qualquer momento a partir do menu Ajuda no Core Console. Também é possível ocultar a página **Bem-Vindo** do Guia de início rápido.

A menos que você o oculte, o Guia de início rápido reaparecerá toda vez que você efetuar login no Rapid Recovery Core Console e acessar a página **Início**. Para obter mais informações, consulte Ocultação do Guia de início rápido.

Você não é obrigado a realizar as etapas sugeridas pelo guia. É possível simplesmente visualizar as tarefas sugeridas e navegar por elas usando as opções **Ignorar etapa** e **Voltar**. Opcionalmente, para ocultar o guia para qualquer ponto, clique em **Sair do Guia**.

Se você optar por executar alguma tarefa de configuração sugerida pelo Guia de início rápido, siga os prompts indicados em qualquer etapa do guia e aparecerá o assistente apropriado ou a área relevante da interface do usuário. Os procedimentos para executar cada tarefa sugerida pelo guia estão descritos neste documento, como indicado na tabela abaixo.

> **NOTA: Nem todas as tarefas de configuração sugeridas pelo Guia de início rápido são obrigatórias para todos os usuários. É preciso entender que tarefas deseja realizar para suas necessidades específicas.**

O Guia de início rápido aborda as seguintes tarefas de configuração:

Tabela 2. Tarefas de configuração do Guia de início rápido

Função	Descrição resumida	Resultado da seleção da tarefa/link para o procedimento
Proteção	Proteção de uma única máquina, um cluster de servers ou várias máquinas usando a proteção em massa	Clique em Proteger ou selecione **Proteger máquina** no menu suspenso para abrir o Assistente de proteção de máquina. Para obter informações sobre como executar o Assistente de proteção de máquina, consulte Proteger uma máquina. Selecione **Proteger cluster** no menu suspenso para abrir a caixa de diálogo Conectar-se ao cluster. Para obter mais informações sobre como proteger um cluster, consulte Proteger um cluster. Selecione **Proteção em massa** para abrir o Assistente de proteção de diversas máquinas. Para obter informações sobre como executar o Assistente de proteção de diversas máquinas, consulte Sobre como proteger diversas máquinas.
Replicação	Configuração da replicação de um Core principal (origem) para um secundário (de destino)	Clique em **Replicação** para abrir a página Replicação. É solicitado que um Core de destino seja adicionado usando o Assistente de replicação. Para obter informações sobre o uso do Assistente de replicação para configurar a replicação em um Core autogerenciado, consulte Replicação para um core de destino autogerenciado. Para obter informações gerais sobre replicação, consulte Como configurar a replicação.
Exportação virtual	Realização de uma exportação única ou estabelecimento de exportação contínua de uma máquina protegida para uma máquina virtual	Clique em **Exportar** para realizar uma exportação de dados de sua máquina protegida para uma máquina virtual. É possível realizar uma exportação única ou configurar o standby virtual para exportação contínua para uma VM. Para obter informações sobre exportações virtuais, consulte Sobre a exportação para máquinas virtuais com o Rapid Recovery.
Configuração	Permite definir configurações adicionais do Rapid Recovery Core	Clique em **Mais** para ver funções adicionais que você pode configurar ou gerenciar. Funções inclui arquivos, montagens, CDs de inicialização, repositórios, chaves de criptografia, contas na nuvem, pesquisa de arquivo, políticas de retenção, notificações, relatórios, logs e mais.
Configuração: Criptografia	Como adicionar ou importar chaves de criptografia que você pode usar para uma ou mais máquinas protegidas	Clique em **Chaves de criptografia** para gerenciar a segurança de dados protegidos com a adição ou a importação de chaves de criptografia. Você pode aplicar chaves de criptografia a uma ou mais máquinas protegidas. A criptografia é descrita no tópico Compreender as chaves de criptografia.
Configuração: Notificações	Configuração de notificações de eventos, avisos e alertas	Clique em **Eventos** para especificar os grupos de notificação de eventos, avisos e alertas. Para enviar estas informações por e-mail, você também deve estabelecer as definições do server de SMTP. Para obter informações sobre o gerenciamento de eventos, consulte o tópico Eventos, incluindo os tópicos Configurar grupos de notificação e Configurar um servidor de e-mail.
Configuração: Retenção	Visualização ou alteração da política de retenção padrão do Core	Clique em **Política de retenção** para abrir a página Política de retenção do Core. Daqui, é possível definir quanto tempo manter um ponto de recuperação antes de realizar rollup nele. Para obter informações conceituais sobre políticas de retenção, consulte o tópico Como gerenciar dados de classificação por vencimento. Para obter informações de procedimento, consulte Como gerenciar as políticas de retenção.
Restaurar	Restauração de dados de um ponto de recuperação do Core	Clique em **Restaurar** para abrir o Assistente de restauração de máquinas. Para obter mais informações sobre como restaurar dados, consulte o tópico Como restaurar volumes a partir de um ponto de recuperação.

Ocultação do Guia de início rápido

O Guia de início rápido é exibido automaticamente na primeira vez que você atualiza ou instala o Rapid Recovery Core.

Também aparece quando o Guia de início rápido é selecionado no menu suspenso de Ajuda e toda vez que for acessada a página principal do Core Console.

Use o procedimento abaixo para ocultar o Guia de início rápido.

- No Rapid Recovery Core Console, se a página **Bem-Vindo** do Guia de início rápido estiver aberta, faça o seguinte:
  - Se desejar ocultar a página **Bem-Vindo** do Guia de início rápido, selecione **Não exibir novamente**.

    NOTA: Essa opção ocultará a página Bem-Vindo na próxima vez em que o Guia de início rápido for aberto e em todas as ocasiões subsequentes até que o Rapid Recovery Core seja atualizado.

    Se você optar por ocultar essa página e quiser acessar as opções avançadas no futuro, selecione **Voltar** no assistente para ver essa página oculta.
  - Se desejar ocultar o Guia de início rápido nesta sessão, clique em **Fechar**.

    O Guia de início rápido é fechado. Da próxima vez em que for acessada a página principal no Core Console, o Guia de início rápido será exibido.

    Também é possível abrir o Guia de início rápido no menu Ajuda.
- Em qualquer página do Guia de início rápido, clique em **Sair do guia.**

  O Guia de início rápido é fechado. Se essa opção for selecionada, ainda será possível abrir o Guia de início rápido no menu Ajuda.

Navegar até o Rapid Recovery Core Console.

Ao efetuar o login no Core Console, e ao clicar a qualquer momento no ícone **Início**  , a página **Início** aparecerá. A página **Início** mostra uma visualização do Rapid Recovery Core, com duas opções. Na área de visualização principal, o conteúdo padrão é o novo painel do Core, que apresenta um conjunto de relatórios em tempo real do seu sistema. Os relatórios padrão do painel incluem status de trabalho de transferência recente, transferência por máquina, uma visão geral do repositório e o estado de conectividade de máquinas protegidas, replicadas e "apenas pontos de recuperação". Ou você pode alternar para a visualização Tabelas resumidas clássica. Nessa visualização, o título da página mostra o nome de exibição do seu Rapid Recovery Core e você pode ver tabelas de resumo que mostram máquinas protegidas, repositórios e alertas recentes. Para obter mais informações, consulte Como entender a página Início (visualização de tabelas resumidas) e Noções básicas sobre o painel Core, respectivamente.

Na página **Início** (e em todas as páginas do Core Console), a área de navegação à esquerda mostra os itens protegidos no seu Core. Você pode navegar para outras páginas da interface com um dos procedimentos a seguir:

- Clicando no ícone correspondente da barra de ícones na área de navegação à esquerda. As opções acessíveis a partir da barra de ícones incluem Replicação, Standby virtual, Eventos, Definições e mais.
- Expandir o menu  (Mais) na barra de ícones e selecionando um destino
- Clicando em um botão ou opção de menu da barra de botões. Os botões incluem Proteger, Restaurar, Arquivar e Replicar.

Quando você seleciona um item da área de navegação à esquerda, o foco do Core Console muda para exibir as informações de resumo sobre esse item. Por exemplo, se você clicar no nome de uma máquina protegida, o Core Console mostra informações sobre essa máquina apenas, em vez de todo o Core. Nesse exemplo, o nome de exibição da máquina protegida aparece como o título da página. Um submenu é mostrado à direita, permitindo que você visualize informações específicas sobre a máquina protegida. As opções de menu incluem: Resumo, Pontos de recuperação, Eventos, Definições, Relatórios e mais.

Para voltar a visualizar informações sobre o Core, incluindo relatórios de painel ou uma exibição resumida de várias máquinas protegidas ou replicadas, clique no ícone **Início**  no canto superior esquerdo da UI. Na página **Início**, você pode alternar entre a visualização do painel e a da página de resumo clicando no link vermelho na parte superior direita da página.

O título na parte superior do Core Console oferece contexto para as informações que você está vendo no Core. Por exemplo:

- A qualquer momento que você vir o nome de exibição ou endereço IP do Core como título da página, você estará vendo as informações de resumo sobre o Core.

- Se o título for Painel, você estará vendo o painel do Core.
- Se você vir o nome de exibição ou o endereço IP de uma máquina protegida ou um painel Resumo na parte superior da página, você estará vendo informações sobre uma única máquina protegida pelo ou replicada no Core.
- Se você vir o título Máquinas protegidas, você estará vendo informações sobre todas as máquinas protegidas no Rapid Recovery Core.
- Se você vir o título Máquinas replicadas de..., você estará vendo informações sobre todas as máquinas replicadas no Rapid Recovery Core.
- Se você vir o título Apenas pontos de recuperação, você estará vendo informações sobre todas as máquinas "apenas pontos de recuperação" nesse Core.

Para obter informações sobre os recursos e funções disponíveis em cada página, consulte a seção apropriada a seguir.

Para obter mais informações sobre a visualização de máquinas protegidas, consulte Visualização do menu Máquinas protegidas. Para obter mais informações sobre o gerenciamento de máquinas protegidas, consulte Gerenciar máquinas protegidas.

Para obter mais informações sobre a visualização de máquinas replicadas, consulte Ver a replicação de entrada e saída.

Para obter mais informações sobre a visualização de máquinas "apenas pontos de recuperação", consulte Visualizar o menu Apenas pontos de recuperação

Compreensão da área de navegação esquerda

A área de navegação esquerda do Console do Core é exibida no lado esquerdo daquela interface de usuário. O conteúdo deste área de navegação pode variar de acordo com o tipo de objetos protegidos no seu Rapid Recovery Core.

A área de navegação esquerda sempre contém o seguinte:

- **Barra de ícones.** Para navegação entre as principais páginas do Console do Core.
- **Filtro de texto.** O filtro de texto é um campo de texto que permite filtrar os itens exibidos nos vários menus que aparecem abaixo dele. Quando você clicar na seta à direita do filtro de texto, cada um dos menus que aparecem abaixo dele se expandirá ou será minimizado.

Seguindo esses elementos, a área de navegação esquerda tipicamente exibe menus para ajudá-lo a navegar, filtrar e visualizar os objetos protegidos em seu Core. Isso inclui máquinas protegidas, máquinas replicadas e assim por diante.

Cada menu é sensível ao contexto; ou seja, cada menu só aparece no Console do Core se ele for relevante. Por exemplo, se você proteger pelo menos uma máquina, o menu de máquinas protegidas será exibido e assim por diante.

Para obter mais informações, consulte as tabelas da área de navegação à esquerda em Como ver a interface do usuário do Core Console.

Visualização da página Início do Rapid Recovery Core Console

Sempre que você fizer login no Rapid Recovery Core Console ou sempre que você clicar no ícone **Início** da barra de ícones, a página **Início** é exibida.

A página **Início** Core Console oferece uma nova visualização de **painel** e a visualização familiar de **tabelas de resumo**. O painel é a visualização padrão.

Você pode alternar entre visualizações na página **Início** clicando no link vermelho na parte superior direita da página **Início**.

Da página Início, e de todas as outras páginas do Core Console, você pode navegar para as funções desejadas usando a área de navegação à esquerda.

Para obter mais informações, consulte os seguintes tópicos:

- Compreensão da área de navegação esquerda
- Noções básicas sobre o painel Core
- Como entender a página Início (visualização de tabelas resumidas)

Como entender a página Início (visualização de tabelas resumidas)

A página **Início** aplica-se apenas ao Core. Na visualização de painel, ela mostra relatórios gráficos em tempo real. Ao alternar para a visualização de tabelas resumidas, a página **Início** exibe todas as máquinas que o Core protege ou replica, os repositórios associados ao seu Core e alertas de máquinas nesse Core.

A visualização de cada painel na página **Início** pode ser expandida ou contraída. Por exemplo, se você clicar no ícone  (contrair visualização) no lado superior direito do painel Máquinas protegidas, a visualização de máquinas protegidas é contraída e apenas o nome do painel fica visível. Para expandir a exibição para ver todas as máquinas protegidas novamente, clique no ícone  (Expandir exibição).

A tabela a seguir descreve os vários elementos da página **Início** na visualização de tabelas resumidas.

Tabela 3. Opções da página Início

Elemento de UI	Descrição
Máquinas protegidas	O painel Máquinas protegidas mostra uma lista das máquinas que este Core protege. Esse painel é exibido independentemente de haver alguma máquina adicionada ao Core para proteção. Essa seção inclui as seguintes informações sobre cada máquina protegida: · **Tipo de máquina.** Um ícone indica se a máquina é uma máquina física, virtual ou um cluster protegido. · **Status.** Círculos coloridos na coluna Status indicam se a máquina protegida está acessível, em pausa ou offline e inalcançável. · **Nome de exibição.** O nome de exibição ou endereço IP da máquina protegida. · **Nome do repositório.** O nome do repositório onde os pontos de recuperação da máquina estão armazenados. · **Último snapshot.** A data e a hora em que o Rapid Recovery criou o snapshot de ponto de recuperação mais recente para essa máquina. · **Pontos de recuperação.** O número de pontos de recuperação armazenados no repositório e o uso de espaço para cada máquina protegida. · **Versão**. A versão do software do agente Rapid Recovery instalada na máquina. Se você clicar no nome de uma máquina específica mostrada nesse painel, uma página Resumo é exibida com as informações de resumo da máquina selecionada. Para obter mais informações sobre o que você pode realizar na página Resumo, consulte Visualização das informações de resumo de uma máquina protegida.
Máquinas replicadas	O painel Máquinas replicadas lista as máquinas que este Core replicou de outro Core. Esse painel não é mostrado a menos que seu Core replique máquinas de outro Core. Essa seção inclui as seguintes informações sobre cada máquina replicada: · **Tipo de máquina.** Um ícone indica se a máquina é uma máquina física, virtual ou um cluster protegido. · **Status.** Círculos coloridos na coluna Status indicam se a máquina replicada está acessível, em pausa ou offline e inalcançável. · **Nome de exibição.** O nome de exibição ou endereço IP da máquina replicada. · **Nome da replicação.** O nome de exibição do Core de origem de qualquer máquina replicada neste Core de destino. Você pode definir esse nome ao configurar a replicação. · **Nome do repositório.** O nome do repositório onde os pontos de recuperação da máquina estão armazenados. · **Último snapshot replicado.** A data e a hora em que o Rapid Recovery criou a réplica mais recente da máquina protegida original. · **Pontos de recuperação.** O número de pontos de recuperação armazenados no repositório e o uso de espaço para cada máquina replicada. · **Versão**. A versão do software do agente Rapid Recovery instalada na máquina. Se você clicar no nome de uma máquina específica mostrada nesse painel, a página Resumo é exibida com as informações de resumo da máquina replicada.

Elemento de UI	Descrição
Máquinas "apenas pontos de recuperação"	O painel Máquinas "apenas pontos de recuperação" lista das máquinas removidos da proteção ou replicação, se os pontos de recuperação forem mantidos. Essas máquinas podem ser usadas para recuperação em nível de arquivo, mas não para bare metal restore, restauração de volumes inteiros ou adição de dados de snapshot. Esse painel não é mostrado, a menos que você tenha alguma máquinas que atenda essa definição. A seção inclui as seguintes informações sobre cada máquina apenas com pontos de recuperação: · **Tipo de máquina.** Um ícone indica se a máquina é uma máquina física, virtual ou um cluster protegido. · **Status.** Círculos coloridos na coluna Status indicam se a máquina "apenas pontos de recuperação" está acessível, em pausa ou offline e inalcançável. · **Nome de exibição.** O nome de exibição ou endereço IP da máquina cujos pontos de recuperação você manteve. · **Nome do repositório.** O nome do repositório onde os pontos de recuperação restantes da máquina estão armazenados. · **Pontos de recuperação.** O número de pontos de recuperação armazenados no repositório e o uso de espaço para cada máquina "apenas pontos de recuperação". Se você clicar no nome de uma máquina específica mostrada nesse painel, a página Resumo aparece para essa máquina "apenas pontos de recuperação".
Repositórios do DVM	Esse painel é exibido para DL1000, independentemente se algum Repositório de DVM foi criado. Esse painel não é mostrado a menos que seu Core tenha um ou mais repositórios de DVM. São incluídas as seguintes informações sobre cada Repositório de DVM: · **Tipo.** Um ícone retrata um repositório. · **Status.** Círculos coloridos na coluna Status mostram se o repositório está montado e se pode aceitar transferências de pontos de recuperação, ou se está inalcançável ou em estado de erro. · **Nome do repositório.** O nome de exibição do repositório. · **Uso de espaço.** A quantidade total de espaço usado no repositório e o tamanho ou extensão do volume de armazenamento. · **Dados protegidos.** A quantidade de espaço usado no repositório. · **Máquinas.** O número de máquinas cujos pontos de recuperação o repositório armazena. · **Pontos de recuperação.** O número de pontos de recuperação armazenados no repositório. · **Taxa de compressão.** A taxa com que o repositório comprime os dados protegidos para economizar espaço. Para obter mais informações, consulte Como entender repositórios.
Alertas	Esta seção mostra os alertas importantes do Core e de todas as máquinas que ele protege. A seção inclui as seguintes informações: · **Ícones.** A coluna de ícones indica a natureza do alerta. Eles incluem mensagens informativas, erros · **Data.** Exibe a data e a hora em que o Rapid Recovery gerou o alerta. · **Mensagem.** Descreve o alerta. Você também pode ver esses detalhes na página Eventos do Core. Para obter mais informações, consulte Como exibir eventos usando tarefas, alertas e registros.

Noções básicas sobre o painel Core

A exibição do painel Core de um conjunto de relatórios gráficos em tempo real de dados relevantes para o Core e as máquinas protegidos. O painel inclui os seguintes relatórios:

- **Trabalho de transferência**. Esse relatório mostra todas as transferências de dados do snapshot (inclusive imagem de base e snapshots incrementais) concluídas nas últimas 24 horas. Entre os snapshots estão imagem de base e snapshots incrementais. Esse relatório de painel é exibido como um gráfico de círculo.
- **Trabalho de transferência por máquina**. Esse trabalho mostra, por máquina protegida, o número de trabalhos de transferência com falha e bem-sucedidos nas últimas 24 horas. Esse relatório de painel é exibido como um gráfico de linha.

- **Repositório**. Esse relatório mostra os repositórios associados ao Core. Ele mostra o número de repositórios, quantas máquinas estão protegidas, o número de pontos de recuperação e a porcentagem de compressão ou deduplicação. Esse relatório é atualizado a cada minuto.
- **Conectividade da máquina**. Esse relatório mostra o estado de conectividade de máquinas protegidas e replicadas no Core. Ele também mostrar a conectividade de dados em máquina apenas com pontos de recuperação.

Você pode minimizar ou expandir a visualização de todos os relatórios no painel clicando na seta para cima ou para baixo no cabeçalho do relatório. Alguns relatórios de painel (conectividade da máquina e repositório) têm um sinal de adição próximo à seta, em que você pode adicionar outra máquina protegida ou outro repositório, respectivamente.

Você também pode arrastar e soltar para mover o local de um dos relatórios em outro lugar no relatório para ordenar os relatórios de uma maneira mais efetiva para o uso.

Visualização do menu Máquinas protegidas

Na interface de usuário do Rapid Recovery, um menu Máquinas protegidas aparece na área de navegação esquerda. Assim como todos os rótulos de menu na área de navegação, o rótulo desse menu é exibido em letras maiúsculas. Por padrão, esse menu está totalmente expandido e mostra uma lista de máquinas protegidas por esse Core. Se houver clusters do servidor protegidos, eles são incluídos nessa lista.

Para expandir ou retrair a exibição de máquinas protegidas e clusters do servidor no Core, clique na seta no lado esquerdo desse menu.

O menu Máquinas protegidas inclui um menu suspenso no lado direito relacionando as funções que podem ser realizadas em todas as máquinas protegidas. Clique na seta à direita de **Máquinas protegidas** para ver o menu e executar um dos seguintes:

- Forçar um snapshot incremental de todas as máquinas
- Forçar uma imagem de base de todas as máquinas
- Pausar a proteção de todas as máquinas (se estiver ativa)
- Retomar a proteção de todas as máquinas (se estiver em pausa)
- Atualizar os metadados para todas as máquinas protegidas
- Remover a proteção de todas as máquinas do Core

Cada máquina relacionada no menu Máquinas protegidas também tem um menu suspenso que controla as funções apenas daquela máquina. No menu suspenso de qualquer máquina, é possível fazer o seguinte:

- Forçar um snapshot incremental da máquina selecionada
- Pausar a proteção da máquina selecionada (se estiver ativa)
- Retomar proteção (se estiver em pausa)
- Atualizar metadados
- Remover a proteção da máquina selecionada do Core
- Navegar até a página Resumo da máquina selecionada
- Navegar até a página Pontos de recuperação da máquina selecionada
- Navegar até a página Eventos da máquina selecionada
- Navegar até a página Definições da máquina selecionada
- Gerar relatórios específicos para a máquina
- Acessar mais funções específicas para a máquina selecionada, incluindo informações do sistema, montagens, política de retenção, notificações ou um log específico da máquina
- Criar um rótulo personalizado exibido na lista de Máquinas protegidas

Se você estiver gerenciando clusters do servidor no Rapid Recovery Core, o cluster também aparecerá no menu de navegação esquerdo. No menu suspenso de qualquer cluster, também é possível:

- Navegar até a página **Nós protegidos** do cluster selecionado

Se você clicar na seta à esquerda do menu Máquinas protegidas, será exibida a lista de contratos de máquinas protegidas e clusters do servidor, e não a de máquinas. Clicar novamente nessa seta faz com que a lista de máquinas seja expandida novamente.

Clique no nome de qualquer máquina do menu Máquinas protegidas para abrir a página Resumo dessa máquina. Para obter mais informações sobre o que você pode realizar na página Resumo, consulte Visualização das informações de resumo de uma máquina protegida.

Por fim, clicar diretamente no menu **Máquinas protegidas** faz com que a página **Máquinas protegidas** seja mostrada na área de conteúdo principal, com um único painel mostrando máquinas protegidas desse Core. Para obter mais informações sobre o que você pode realizar no painel **Máquinas protegidas** da página Máquinas protegidas, consulte Como ver o painel Máquinas protegidas.

NOTA: Na página Máquinas protegidas, você pode voltar a uma visualização da perspectiva do Core clicando no ícone Início da barra de ícones.

Visualização das informações de resumo de uma máquina protegida

Quando você clica no nome de uma máquina protegida do Core Console, a página **Resumo** é mostrada. Ela contém, no mínimo, um painel de Resumo e um painel de Volumes. Se uma máquina for adicionada a replicação, um painel Replicação também é mostrado.

Se você tiver um ou mais servers Exchange protegidos, você também verá um painel de Informações do Exchange Server que contém informações sobre seu server Exchange protegido.

Se você tiver um ou mais servers SQL protegidos, você também verá um painel de Informações do SQL Server que contém informações sobre seu server SQL protegido.

No topo desta página há um menu de ações que você pode realizar na máquina protegida. Abaixo dela há, no mínimo, um painel de Resumo e um painel de Volumes. Se uma máquina for adicionada a replicação, um painel Replicação também é mostrado.

Ao mostrar informações sobre uma máquina protegida — na página de Resumo e todas as outras visualizações — há um menu na parte superior da página com funções que você pode executar. Esse menu é exibido imediatamente abaixo do nome da máquina protegida.

Links relacionados

- Visualizar o painel Resumo
- Visualização de volumes em uma máquina protegida
- Exibindo informações de replicação
- Visualizar o painel de informações do Exchange Server
- Visualização do painel de informações do SQL Server

Visualizar o painel Resumo

O painel **Resumo** contém informações resumidas sobre a máquina protegida, incluindo o nome do host, a data e a hora do último snapshot, a data e a hora do próximo snapshot agendado, as informações sobre a chave de criptografia e as informações de versão do software do agente Rapid Recovery. Há também um link para uma página Informações do sistema detalhada para a máquina.

Visualização de volumes em uma máquina protegida

Para qualquer máquina protegida, na página Resumo, no painel Volumes, é possível realizar as seguintes ações para qualquer um dos volumes listados:

- Definir ou modificar uma programação de proteção para um volume selecionado. Os cronogramas de proteção são normalmente estabelecidos quando você protege uma máquina primeiro. Para obter mais informações sobre a modificação de uma programação de proteção, consulte Modificar programações de proteção.
- Forçar uma imagem de base ou snapshot. Os snapshots ocorrem normalmente dependendo da programação de proteção. Contudo, a qualquer momento, é possível forçar uma imagem de base ou um snapshot incremental para os volumes selecionados. Para obter mais informações consulte Forçar um snapshot.

Exibindo informações de replicação

O painel **Replicação** contém informações de resumo sobre a máquina replicada, inclusive o nome da replicação, o estado da replicação, o progresso e o espaço disponível.

Visualizar o painel de informações do Exchange Server

O painel **Informações do Exchange Server** aparece somente para as máquinas protegidas que forem Exchange Servers.

Esse painel contém informações resumidas sobre o Exchange Server protegido, incluindo a versão instalada do Microsoft Exchange, o caminho no qual o Exchange está instalado e o caminho definido para os dados da caixa de correio do Exchange.

A grade Armazenamentos de e-mail mostra o nome do Exchange Database (EDB), o caminho do arquivo do EDB, o caminho no qual os arquivos de log estão armazenados, o prefixo do log, o caminho do sistema, o Grupo de Disponibilidade do Bancos de Dados (DAG) e o tipo de armazenamento de e-mail.

Visualização do painel de informações do SQL Server

O painel **Informações do SQL Server** é exibido somente para máquinas protegidas que são SQL servers.

Este painel contém informações de resumo sobre os SQL servers protegidos. Você pode expandir as informações do database para ver detalhes para cada tabela no database. Você também pode ver o database ou o nome da tabela e o caminho do banco de dados.

Como ver pontos de recuperação para uma máquina

A página Pontos de recuperação mostra uma lista dos pontos de recuperação coletados para essa máquina protegida, além de dados pertinentes sobre a máquina e o repositório. Nessa página, você pode montar, exportar e restaurar pontos de recuperação específicos ou excluir pontos de recuperação.

A página está dividida em dois painéis: Resumo dos pontos de recuperação e Pontos de recuperação. O painel Resumo não contém links de ações. Ele exibe os dados relacionados a seguir sobre a máquina.

Tabela 4. Dados do painel Resumo dos pontos de recuperação

Elemento de UI	Descrição
Total de pontos de recuperação	O número de pontos de recuperação coletados para essa máquina protegida específica.
Total de dados protegidos	A quantidade de dados da máquina protegida armazenados no repositório.
Repositório	O nome do repositório no qual o Rapid Recovery armazena os pontos de recuperação dessa máquina protegida.
Status do repositório	A barra de progresso exibe a porcentagem do espaço total usada no repositório. A quantidade de dados usada e o tamanho total do repositório aparecem abaixo da barra de progresso.

Para obter mais informações, consulte Como ver o painel Máquinas protegidas.

Visualizar eventos de uma máquina protegida

Na página **Eventos**, você pode visualizar os trabalhos que ocorreram ou estão em progresso na máquina protegida selecionada. Os botões na parte superior da página permitem navegar para listas de trabalhos em cada uma das três categorias de atividades:

- **Tarefas.** Um trabalho que deve ser realizado pelo Rapid Recovery para que funcione corretamente.
- **Alertas.**Ama notificação relacionada a uma tarefa ou evento que inclui erros e aviso.
- **Registro.**Uma combinação de todas as tarefas e alertas de máquinas protegidas.

A tabela a seguir contém descrições de cada elemento da página **Eventos**.

Tabela 5. Elementos da página Eventos

Elemento de UI	Descrição
Pesquisar palavra-chave	Permite pesquisar um item específico dentro de cada categoria. Disponível somente para tarefas.
De	Para restringir os resultados, você pode inserir uma data de início da pesquisa. Disponível somente para tarefas.
Para	Para restringir os resultados, você pode inserir uma data de término da pesquisa. Disponível somente para tarefas.
Ícones de status	Cada ícone representa um status diferente do trabalho. Para alertas e tarefas, clicar em um dos ícones permite filtrar a lista por esse status, gerando, essencialmente, um relatório. Quando você clica no ícone uma segunda vez, o filtro desse status é removido. Você pode filtrar por mais de um status. Os status são: • **Ativo.**Um trabalho em progresso. • **Enfileirado.** Um trabalho que está aguardando a conclusão de outro trabalho para poder começar. • **Aguardando.**Um trabalho que está aguardando sua aprovação ou conclusão, como uma unidade de propagação. (Para obter mais informações sobre unidades de propagação, consulte Replicação.) • **Concluído.**Um trabalho que foi concluído com êxito. • **Com falha.** Um trabalho que teve uma falha e não foi concluído.
Ícone de serviço	Este botão adiciona trabalhos de serviços à lista de trabalhos. Quando você clica nesse ícone, um ícone de serviço menor aparece em cada ícone de status, permitindo filtrar por trabalhos de serviço que possuam esses status (se houver). Exemplos de trabalhos de serviços são a exclusão de arquivos de índice ou a remoção de uma máquina da proteção.
Lista suspensa Tipo de exportação	A lista suspensa inclui os formatos para os quais você pode exportar o relatório de eventos. Disponível somente para tarefas. Ela inclui os seguintes formatos: • PDF • HTML • CSV • XLS • XLSX
Ícone (Exportar)	Converte o relatório de eventos para o formato selecionado. Disponível somente para tarefas.
Seleção de página	Os relatórios de eventos podem incluir vários trabalhos em múltiplas páginas. Os números e as setas na parte inferior da página **Eventos** permitem navegar pelas páginas adicionais do relatório.

O página **Eventos** exibe todos os eventos em uma tabela. A seguinte tabela lista as informações exibidas para cada item.

Tabela 6. Informações detalhadas da tabela de resumo de eventos

Elemento de UI	Descrição
Status	Exibe o status da tarefa, alerta ou item de registro. Disponível para alertas ou itens de registro, clique no cabeçalho para filtrar os resultados por status.
Nome	Nome está disponível somente para tarefas. Esse campo de texto lista o tipo de tarefa que foi concluída nessa máquina protegida. Os exemplos incluem transferência de volumes, manutenção de repositório, execução, realização de verificação de capacidade de montagem, realização de verificação de soma de verificação e assim por diante.
Hora inicial	Disponível para tarefas, alertas e itens de registro. Exibe a data e a hora de início do trabalho ou da tarefa.
Hora final	Disponível somente para tarefas. Exibe a data e a hora de conclusão do trabalho ou da tarefa.
 Detalhes do trabalho	Disponível somente para tarefas. Abra a caixa de diálogo **Monitorar tarefa ativa** de maneira que você possa visualizar os detalhes do trabalho ou da tarefa específico(a). Esses detalhes incluem um ID do trabalho, taxa de transferência de dados do core (se relevante), tempo decorrido para conclusão do trabalho, trabalho total em quantidade de gigabytes e tarefas subordinadas associadas ao trabalho.
Mensagem	Disponível para alertas e itens de registro. Esse campo de texto fornece uma mensagem descritiva do alerta ou do item de registro.

Visualização de relatórios para uma máquina protegida

O menu suspenso **Relatórios**  permite gerar relatórios sob demanda para a máquina protegida selecionada.

O relatório do trabalho fornece um relatório sobre o status d e trabalhos bem-sucedidos e trabalhos com falha para a máquina selecionada. Trabalhos com falha podem ser visualizados em um relatório de falhas. Para obter mais informações sobre esse tipo de relatório, consulteNoções básicas sobre o relatório do trabalho.

O relatório de falhas fornece informações sobre trabalhos de Core com falha e cancelados para a máquina especificada. Para obter mais informações sobre esse tipo de relatório, consulteNoções básicas sobre o relatório de falhas.

Para obter informações sobre como gerar esses relatórios, consulteGerar um relatório de Core sob demanda.

Ver máquinas replicadas no menu de navegação

Se o seu Core replica máquinas de outro Rapid Recovery Core, o nome de exibição do Core de origem aparece como um menu minimizado na navegação à esquerda do Console do Core. Assim como acontece com todos os rótulos de menu na área de navegação, esse nome de menu das máquinas replicadas aparece com todas as letras maiúsculas, abaixo do menu de Máquinas Protegidas. Por padrão, o menu de máquinas replicadas é totalmente expandido, e mostra a lista de todas as máquinas provenientes do Core de origem que são replicadas em seu Core de destino.

Para expandir ou minimizar a exibição de máquinas replicadas a partir do Core de origem, clique na seta no lado esquerdo desse menu.

Cada menu de máquinas replicadas inclui um menu suspenso no lado direito relacionando as funções que podem ser realizadas simultaneamente em todas as máquinas replicadas a partir daquele Core. Clique na seta à direita do menu de máquinas replicadas para ver uma lista suspensa de funções que você pode executar. Essas ações incluem:

- Pausar replicação. Se a replicação estiver atualmente ativa, para a ação até você retomá-la.
- Retomar replicação. Se a replicação tiver sido pausada, ela será iniciada novamente.

- Forçar replicação. Replica sob demanda, em vez de em um momento agendado.
- Remover a replicação. Remove a relação de replicação entre o core de origem e seu core de destino. Opcionalmente, você pode apagar os pontos de recuperação armazenados neste Core. Para obter informações, consulteRemoção da replicação.

Clicar diretamente no nome do Core de origem no menu de navegação faz com que a página **Máquinas replicadas de [Nome do Core de Origem]** seja exibida na área de conteúdo principal. Para obter mais informações sobre o que você pode realizar nesta página, consulteVer a replicação de entrada e saída.

Links relacionados

Pausar e retomar a replicação
Forçar a replicação
Remoção da replicação

Visualizar o menu Apenas pontos de recuperação

O menu Apenas pontos de recuperação é exibido na área de navegação à esquerda se uma das seguintes condições for verdadeira:

- Se o seu Rapid Recovery Core mantém alguns pontos de recuperação de uma máquina que estava anteriormente protegida
- Se você removeu a replicação, mas manteve os pontos de recuperação.

Assim como acontece com todos os rótulos de menu na área de navegação, o rótulo para este menu é exibido com todas as letras maiúsculas.

Para expandir ou retrair a exibição de máquinas apenas com pontos de recuperação, clique na seta à esquerda desse menu.

O menu inclui um menu suspenso no lado direito relacionando as funções que podem ser realizadas simultaneamente em todas as máquinas apenas com ponto de recuperação. Nesse caso, a única função que você pode realizar é remover os pontos de recuperação do Core.

CUIDADO: Essa ação remove todas as máquinas apenas com pontos de recuperação em seu Rapid Recovery Core, excluindo-os permanentemente e impedindo a restauração das informações desses pontos de recuperação a partir desse Core.

Visualizar o menu Grupos personalizados

O menu Grupos personalizados aparecerá na área de navegação esquerda apenas se você tiver definido um ou mais grupos personalizados. Assim como acontece com todos os rótulos de menu na área de navegação, o rótulo desse menu é exibido em letras maiúsculas.

Para expandir ou retrair a exibição dos itens desse menu, clique na seta à sua esquerda.

O menu Grupos personalizados inclui um menu suspenso no lado direito relacionando as funções que podem ser realizadas simultaneamente em todos os itens semelhantes desse grupo.

Para obter mais informações, consulte Noções básicas sobre grupos personalizados.

Usar a caixa de diálogo Erro

Quando um erro ocorre na interface de usuário do Rapid RecoveryRapid Recovery Core Console, como a tentativa de inserir um parâmetro inválido, uma caixa de diálogo Erro aparece. A caixa de diálogo geralmente indica a causa do erro, fornece alguns links para informações adicionais sobre o erro e inclui um botão Fechar. Você precisa fechar a caixa de diálogo Erro para continuar, mas talvez queira visualizar mais informações sobre o erro.

Na caixa de diálogo Erro, escolha entre as opções a seguir:

Os erros da interface de usuário que causam o aparecimento da caixa de diálogo Erro não são rastreados na guia Eventos do Rapid Recovery, pois são apenas erros de validação ou inserção de dados. No entanto, quando você clica na opção Pesquisar base de conhecimento referente a algum erro, a URL do link fornecido é registrada no arquivo CoreAppRecovery.log. Você pode pesquisar a cadeia de caracteres de texto "KB article url generated" no log para ver a URL de cada erro que foi visualizado em um navegador. Para obter mais informações sobre download ou visualização de logs de erros do Core, consulte os tópicos Como baixar e exibir o arquivo de log do Core ou Acesso aos logs do Core, respectivamente.

Definições do Core

Esta seção descreve como gerenciar e alterar as configurações do seu Rapid Recovery Core a partir do ícone de Configurações  .

Definições do Rapid Recovery Core

Por padrão, as definições do Rapid Recovery Core são configuradas para proporcionar um desempenho ideal para a maioria dos usuários. Essas definições afetam o desempenho do Rapid Recovery Core, ou, em alguns casos, a exibição de informações no Rapid Recovery Core Console. Na barra de ícones, clique em  (Definições) para acessar as configurações do Core. Uma lista de todas as definições do Core é mostrada à esquerda. Você pode clicar no título de qualquer definição dessa lista para ir para a configuração completa dessa definição à direita. Ou você pode navegar por todas as definições do Core à direita para ver todas as opções de configuração. Para obter informações, consulte Definições do Rapid Recovery Core.

Você pode também acessar as ferramentas do Core, como ver um resumo das informações do sistema ou fazer download dos arquivos de log do Core. Para obter informações, consulte Ferramentas do nível do Core.

A tabela a seguir relaciona o conjunto abrangente de definições do Rapid Recovery Core que você pode configurar.

Tabela 7. Definições configuráveis do Rapid Recovery Core

Definição de configuração	Descrição
Configuração de Backup e restauração do Core	O Rapid Recovery permite criar uma cópia de segurança das definições de configuração do Core em um arquivo XML. Você pode usar um arquivo de cópia de segurança para restaurar ou migrar as definições do Core. Para obter mais informações sobre a criação de backup e a restauração das definições do Core, consulte Criar cópia de segurança e restaurar definições do Core.
Geral	As definições gerais incluem opções de configuração que se aplicam geralmente ao Rapid Recovery Core, incluindo opções de exibição e portas do servidor da Web e do serviço Rapid Recovery. Para obter mais informações sobre as definições gerais do Rapid Recovery Core, incluindo como configurá-las, consulte Configurar definições gerais do Core.
Atualizações	As definições de atualização controlam os aspectos relacionados ao recurso de atualização automática, que verifica se há versões atualizadas do software Rapid Recovery. Para obter mais informações sobre as definições de atualização do Rapid Recovery Core, incluindo como configurá-las, consulte Configuração das definições de atualização.
Trabalhos noturnos	As definições de trabalhos noturnos referem-se às tarefas automatizadas que o Core realiza diariamente. Você pode configurar o horário de início e quais trabalhos são executados. A Dell recomenda programar os trabalhos fora do horário de expediente normal para reduzir a carga no sistema quando a demanda por recursos está alta. Para obter mais informações, consulte Compreender trabalhos noturnos, Configurar trabalhos noturnos para o Core e Como personalizar os trabalhos noturnos para uma máquina protegida.

Definição de configuração	Descrição
Fila de transferência	As definições de fila de transferência controlam o número de tentativas de transferência quando os trabalhos falham devido à indisponibilidade de recursos. Você pode estabelecer o número máximo de transferências simultâneas e o número máximo de tentativas de transferência de dados. Para obter mais informações sobre as definições da fila de transferência, consulte Modificar definições de fila de transferência.
Tempo limite do cliente	As definições de tempo limite do cliente determinam por quanto tempo serão realizadas tentativas de solicitações de conexão específicas ou de operações de leitura e gravação. Para obter mais informações sobre as definições de tempo limite do cliente, consulte Ajustar definições de tempo limite do cliente.
Cache de deduplicação DVM	A deduplicação garante que cada bloco de informações seja armazenado apenas uma vez no repositório, criando referências para blocos de dados repetidos. As referências são armazenadas em um cache de deduplicação. Quando chaves de criptografia são usadas, a deduplicação ocorre dentro de cada domínio de criptografia. As definições do cache de deduplicação do DVM permitem configurar o tamanho e especificar os locais dos caches primário e secundário, bem como do cache de metadados. Para obter mais informações sobre cache de deduplicação, consulte Noções básicas sobre o cache de deduplicação e locais de armazenamento. Para obter mais informações sobre ajuste de definições, consulte Configuração das definições de cache de deduplicação DVM.
Mecanismo Replay	As configurações do mecanismo Replay controlam as informações referentes ao canal de comunicação do mecanismo Replay, tais como endereços IP e configurações de tempo limite, para ajudar a ajustar o desempenho específico às suas necessidades de rede. Para obter mais informações sobre as definições do mecanismo do Rapid Recovery, consulte Configurar as definições do mecanismo Replay.
Implantação	As definições de implantação permitem definir opções para implantar o software do agente do Rapid Recovery de seu Core nas máquinas que você deseja proteger. Para obter mais informações sobre a configuração de definições de implantação, consulte Configurar as definições do implantação.
Conexão de banco de dados	O Rapid Recovery armazena as informações transacionais em um banco de dados de serviço MongoDB que, por padrão, é instalado localmente na máquina Core. Você pode configurar essas definições para alterar o tempo de retenção de informações no banco de dados ou o tamanho do pool de conexões para permitir mais ou menos conexões simultâneas. Para obter mais informações sobre a configuração ou modificação de definições de conexão do banco de dados de serviço, consulte Configurar definições de conexão de banco de dados.
Banco de dados local	O Rapid Recovery exibe informações sobre tarefas, eventos e alertas do Core na página Eventos. O Rapid Recovery armazena essas informações transacionais em um banco de dados de serviço MongoDB, que é instalado localmente na mesma máquina do Rapid Recovery Core. Você pode configurar informações de credencial (nome de usuário e senha) para o banco de dados de serviço Mongo local usando as definições de Banco de dados local. Para obter mais informações sobre como ajustar as definições do banco de dados local, consulte Modificação das definições locais de conexão do banco de dados.
Server de SMTP	Ao configurar as definições de server de SMTP (simple mail transfer protocol) no Core, você também poderá enviar as informações de evento do Core por e-mail. Para obter mais informações sobre como configurar um server de SMTP para e-mail, consulte Configurar um servidor de e-mail.

Definição de configuração	Descrição
	NOTA: Para enviar informações sobre eventos por e-mail, você também deve configurar as definições de grupo de notificação. Para obter mais informações sobre especificação de eventos para recepção de alertas de e-mail, consulte Configurar grupos de notificação.
Configuração da nuvem	Os parâmetros de configuração da nuvem permitem que você especifique os parâmetros de configuração das contas de armazenamento na nuvem suportadas. Essas definições não criam contas de nuvem. Em vez disso, elas associam contas existentes de armazenamento em nuvem ao Rapid Recovery Core para facilitar ações tais como o arquivamento de informações do Rapid Recovery. Para obter mais informações sobre o gerenciamento de informações de conta de armazenamento em nuvem no Rapid Recovery Core, consulte Gerenciar contas de nuvem.
Relatórios	As definições de relatório incluem um único parâmetro de configuração que permite selecionar a fonte usada quando um relatório é gerado a partir do Rapid Recovery Core. Para obter mais informações sobre como alterar as definições de relatórios, consulte Gerenciamento de definições de relatórios.
Capacidade de anexação	As definições de Capacidade de anexação permitem especificar se você deseja realizar Verificação de capacidade de anexação do SQL na máquina protegida ou se a instância do SQL Server deve ser usada no Core. Se você especificar SQL no Core, é preciso fornecer as informações de credencial. Para obter mais informações sobre como gerenciar as definições de capacidade de anexação do SQL para o Core, consulte Gerenciamento das definições de Capacidade de anexação SQL do Core.
Trabalhos	Os trabalhos do Core são criados automaticamente quando você inicia operações, como replicação. Você pode especificar as definições de cada trabalho usando as configurações do Core para Trabalhos. Você pode configurar o número de trabalhos executados simultaneamente. Caso um erro de rede ou outro erro de comunicação impeça que o trabalho seja bem-sucedido de início, você pode definir o número de novas tentativas a serem feitas usando a definição de Contagem de tentativas. Para obter mais informações sobre trabalhos do Core, quais trabalhos estão disponíveis e como configurá-los, consulte Definições de trabalhos do Core.
Aplicação de licença	No Core Console, o Rapid Recovery permite alterar a licença associada ao Core, limitar o número de snapshots diários, visualizar informações sobre o conjunto de licenças e contatar o servidor de licenças. Para obter mais informações sobre o gerenciamento de licenças no Core, consulte Gerenciar licenças. Para obter mais informações sobre como gerenciar licenças, consulte o guia Dell Data Protection | Portal de licenças do Rapid Recovery. **NOTA: O Dell Data Protection | Portal de licenças do Rapid Recovery tem um ciclo de lançamento diferente do software Rapid Recovery. Para obter a documentação mais recente do produto, consulte o Site de documentação técnica da Dell.**
Configuração de SNMP	O Protocolo Simples de Gerenciamento de Rede (SNMP) é um protocolo para gerenciar dispositivos em uma rede IP. Você pode configurar o Rapid Recovery Core como um agente SNMP. Assim o Core pode enviar informações como alertas, status do repositório e máquinas protegidas. Para obter mais informações sobre como usar SNMP com o Rapid Recovery, consulte Noções básicas das definições do SNMP.
vSphere	As definições do vSphere Core são aplicadas somente aos usuários com proteção sem agentes em máquinas virtuais. Se você estiver usando um host vSphere, essas definições incluem configurações que se aplicam às VMs. Para obter mais informações sobre as definições de vSphere para a proteção sem agentes VMware ou ESXi, consulte Configuração das definições do vSphere.

Definição de configuração	Descrição
Carregamentos de logs	Quando esta opção está definida como Sim, o Rapid Recovery Core carrega os arquivos de log para a Dell para análise em um esforço contínuo para melhorar a qualidade geral do produto. Essa configuração é opcional.

Configurar definições gerais do Core

As definições gerais para o Rapid Recovery Core incluem o nome de exibição do Core, a porta do servidor da web, a porta de serviço e a localidade (o idioma de exibição do Core Console).

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Definições), e, em seguida, realize um dos seguintes procedimentos:
- Na lista de Definições do Core, no lado esquerdo da página de Definições, clique em **Geral**.
- Role a tela para baixo no lado direito da página de Definições até que consiga ver o cabeçalho "Geral".

  As Definições gerais do Core serão exibidas.

3 Clique na definição geral que deseja alterar.

A definições selecionada se tornará editável, como um campo de texto ou um menu suspenso.

4 Insira as informações de configuração conforme descrito na tabela a seguir.

Tabela 8. Informações sobre as definições gerais

Caixa de texto	Descrição
Nome de exibição	Insira um novo nome de exibição para o Core. Esse é o nome que será exibido no Rapid Recovery Core Console. Você pode inserir até 64 caracteres.
Porta do servidor da Web	Insira um número de porta para o servidor da Web. A porta padrão é 8006.
Porta de serviço	Insira um número da porta para o serviço Rapid Recovery Core. A porta padrão é 8006.
Localidade	Na lista suspensa Localidade, selecione o idioma que você deseja usar. Você pode escolher entre inglês, francês, alemão, japonês, coreano, português, chinês simplificado e espanhol. **NOTA: Se você alterar o idioma, confirme a mensagem indicando que o serviço Rapid Recovery Core deve ser reiniciado para que o idioma atualizado possa ser exibido no Core Console. Você pode reiniciar este serviço no Gerenciador de Tarefas do Windows.**

5 Para todas as definiões, quando estiver satisfeito com suas alterações, clique em ✔ para salvar a alteração e sair do modo de edição, ou clicar em ✖ para sair do modo de edição sem salvar.

Configuração das definições de atualização

O Rapid Recovery inclui o recurso de atualização automática. Ao instalar o Rapid Recovery Core, é possível optar por atualizar automaticamente o software Rapid Recovery Core quando houver novas atualizações disponíveis e a frequência com que o sistema deve verificar se há atualizações.

Os números de versão do Rapid Recovery normalmente incluem quatro blocos de informações, separados por pontos decimais: o número da versão principal, o número da versão secundário, a revisão e número de compilação. Por exemplo, a primeira versão remarcada do Rapid Recovery foi a 6.0.1.609. A versão seguinte foi a 6.0.2.142.

O recurso de atualização automática faz uma comparação entre todos os dígitos de um número de versão. Se você ativar a atualização automática, o software Core é apenas atualizado sem intervenção quando os números de versão principal e secundário são idênticos. Por exemplo, uma atualização automática ocorreria da versão de Core 6.0.1.609 para 6.0.2.142 (as duas versões começam com 6.0). Na mesma máquina, o Core não atualizaria automaticamente de 6.0.2.142 para 6.1.1.XXX, pois os dígitos após o primeiro decimal não são iguais. Em vez disso, você será notificado (através de um banner no topo do Core Console) de que há uma atualização para o software Core disponível. Esta notificação dá a você uma oportunidade para rever as notas de versão e determinar se atualizar para a versão mais recente do Core é adequado às suas necessidades.

NOTA: Para obter informações sobre como instalar o software do Rapid Recovery Core, consulte o Guia de instalação de atualização do Dell Data Protection | Rapid Recovery.

É possível visualizar e alterar as definições que o sistema utiliza para verificar se há atualizações a qualquer momento.

CUIDADO: Ao usar replicação, a configuração do sistema para instalar atualizações automaticamente pode fazer com que o Core de origem seja atualizado antes do Core de destino, o que pode acarretar falha de replicação ou impedir o estabelecimento de uma nova replicação entre os Cores. Para usuários de replicação, a Dell recomenda que os administradores apliquem atualizações automáticas apenas ao Core de destino, depois atualizem manualmente o Core de origem e, por fim, atualizem as máquinas protegidas.

Execute as etapas deste procedimento para configurar as definições de atualização.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Definições) e, em seguida, faça o seguinte:
- Na lista de definições do Core no lado esquerdo da página Definições, clique em **Atualizações**.
- Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Atualizações.

  As definições de Atualizações do Core são mostradas.

3 Clique na definição que você deseja alterar.

  A definição selecionada se torna editável.

4 Insira as informações de configuração conforme descrito na tabela a seguir.

Tabela 9. Informações das definições de atualização

Caixa de texto	Descrição
Verificar se há novas atualizações	Selecione a frequência com que o Rapid Recovery deve procurar e instalar as atualizações. Você pode selecionar dentre as seguintes opções: • Nunca • Diariamente • Semanalmente • Mensalmente Se você optar por atualizações automáticas, depois que o limite de tempo selecionado passar, se uma atualização estiver disponível ela é instalada depois que os trabalhos noturnos forem concluídos.
Instalar atualizações	Especifique como as atualizações disponíveis serão tratadas escolhendo uma das seguintes opções: • Nunca procurar por atualizações • Notificar-me sobre atualizações, mas não instalá-las automaticamente • Instalar atualizações automaticamente
Status	O estado indica se há novas atualizações disponíveis.
Última verificação	O campo Última verificação indica a data e a hora em que o sistema verificou se há novas atualizações pela última vez.

Caixa de texto	Descrição
	Clique em**Verificar agora** para verificar imediatamente se há alguma atualização de software disponível. Esta verificação ocorre independentemente da frequência definida.

5 Para cada definição, quando estiver satisfeito com suas alterações, clique na para salvar a alteração e sair do modo de edição, ou clique em para sair do modo de edição sem salvar.

Compreender trabalhos noturnos

Trabalhos noturnos são tarefas automatizadas diárias que ocorrem em um horário pré-determinado fora do expediente normal. Esses trabalhos utilizam muita memória e incluem diversas tarefas de verificações de integridade e consolidação de dados melhor realizadas quando o Rapid Recovery Core está menos ativo.

Todos os trabalhos noturnos, e o escopo para o qual são aplicados, são descritos na tabela a seguir. Trabalhos noturnos podem ser gerenciados a nível de core (que se aplica a todas as máquinas protegidas no core). Esses trabalhos noturnos também podem ser aplicados para uma lista de máquinas protegidas específicas, no escopo como "Máquina protegida".

Tabela 10. Informações de trabalhos noturnos

Nome do trabalho	Escopo	Descrição
Alterar	N/A	Esse controle abra a caixa de diálogo Nightly Jobs (Trabalhos noturnos), onde você pode ativar, desativar ou alterar as configurações de cada trabalho noturno.
Horário de trabalhos noturnos	All (Todos)	Essa configuração representa o horário no qual os trabalhos noturnos estão programados para começar. A Dell recomenda que seu cre execute trabalhos noturnos durante um horário de pouca atividade. O horário padrão é 00:00.
Implantação	Core ou máquina protegida	Aplica a política de retenção aos seus dados de backup ao combinar ou "implementar" pontos de recuperação no cronograma configurado na política. Você pode personalizar a política no core, que se aplica por padrão a todas as máquinas protegidas. Por padrão, o trabalho de implementação é executado em todo o core; ou clique em (Ampliar) para definir em quais máquinas protegidas você deseja realizar a implementação usando a política de core. Para obter mais informações sobre como usar uma política de retenção em uma máquina protegida que se diferente da política padrão definida no core, consulte Como personalizar as configurações de uma política de retenção para uma máquina protegida.
Verificar a conectabilidade de bancos de dados SQL	Máquina protegida	Verifica a integridade de pontos de recuperação que contêm bancos de dados SQL. Processo: • Monte o ponto de recuperação mais recente para grupos de proteção que contenham bancos de dados. • Conecte o banco de dados do SQL Server. • Abra o banco de dados. • Feche o banco de dados. • Desmonte o ponto de recuperação. Para ativar essa verificação noturna, especifique uma instância do SQL Server para usar na realização de verificações de conectabilidade para bancos de dados do SQL Server em máquinas protegidas. **NOTA: Essa opção não aparece se você não estiver protegendo um SQL Server em seu core.**

Nome do trabalho	Escopo	Descrição
Baixar logs de máquinas protegidas	Núcleo	Baixa logs para máquinas protegidas ao core para que possam ser enviados para um servidor de registro.
Consolidar instantâneos VMware para máquinas virtuais protegidas	Core ou máquina protegida	Esse trabalho noturno é relevante se você usar APIs VMware para proteger máquinas sem o software de agente Rapid Recovery. Você deve consolidar instantâneos do VMware periodicamente. Ativar esse trabalho noturno permite que você realize essas consolidações diariamente. Esse trabalho noturno contém um parâmetro (Número máximo de consolidações simultâneas) que deve ser definido entre 1 e 100.
Verificar a integridade dos pontos de recuperação	Core ou máquina protegida	Verifica a integridade dos pontos de recuperação para cada máquina protegida. Por padrão, a opção `Check integrity of recovery points` não é ativada. Processo: • Monte o ponto de recuperação mais recente para todo grupo de proteção. • Enumere os arquivos e pastas de cada volume. • Examina os pontos de recuperação para garantir que sejam válidos. • Desmonte o ponto de recuperação.
Verificar a soma de verificação de bancos de dados Exchange	Máquina protegida	Verifica a integridade de pontos de recuperação que contêm arquivos de bancos de dados Exchange. **NOTA: Essa opção não aparece se você não estiver protegendo um Exchange Server em seu core.**
Truncar logs de SQL (apenas no modelo de recuperação simples)	Máquina protegida	Mantém o tamanho dos logs de SQL Server ao truncar o log de transação de banco de dados para atender ao último ponto de recuperação. **NOTA: Essa opção não aparece se você não estiver protegendo um SQL Server em seu core.**
Truncar logs do Exchange	Máquina protegida	Mantém o tamanho dos logs de Exchange ao truncar o log de transação de banco de dados Exchange para atender ao último ponto de recuperação. **NOTA: Essa opção não aparece se você não estiver protegendo um Exchange Server em seu core.**
Registrar estatísticas de repositório	Núcleo	Envia estatísticas de repositório para um servidor de registro.
Apagar eventos e trabalhos antigos	Núcleo	Mantém a escala do banco de dados de eventos ao remover eventos antigos. O número de dias é configurável, sendo definido, por padrão, para 30 dias.

Configurar trabalhos noturnos para o Core

Quando qualquer opção de trabalho noturno é ativada no Rapid Recovery Core, o trabalho selecionado é executado uma vez por dia, no horário especificado, com todas as máquinas protegidas pelo Core. Da mesma forma, se você desabilita algum trabalho noturno no nível do Core, o trabalho especificado deixa de ser executado em todas as máquinas protegidas pelo Core.

NOTA: Se o escopo de um trabalho noturno, conforme descrito no tópico Compreender trabalhos noturnos, inclui máquinas protegidas, você pode configurar esse trabalho para ser aplicado apenas a uma ou mais máquinas protegidas individualmente. Para obter mais informações sobre como aplicar definições de trabalhos noturnos específicas a uma máquina protegida, consulte Como personalizar os trabalhos noturnos para uma máquina protegida.

Como os trabalhos noturnos usam muita memória, a Dell recomenda configurar o Core para executá-los durante um período de baixa atividade. Por padrão, os trabalhos noturnos são programados para serem executados à meia-noite. Se outro horário for mais adequado, altere essa definição no campo Horário dos trabalhos noturnos usando este procedimento.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em (Definições) e, em seguida, faça o seguinte:
- Na lista de definições do Core no lado esquerdo da página **Definições**, clique em **Trabalhos noturnos**.
- Role a tela para baixo no lado direito da página **Definições** até ver o cabeçalho Trabalhos noturnos.

  As definições de Trabalhos noturnos do Core são mostradas.

3 Para alterar qualquer trabalho noturno ou alterar a hora em que trabalhos noturnos começam a ser executados, clique em **Alterar**.

  A caixa de diálogo **Trabalhos noturnos** é exibida.

4 Para alterar o horário em que os trabalhos noturnos são executados, insira um novo horário no campo **Horário dos trabalhos noturnos**.

5 Na primeira coluna, clique para selecionar cada opção de trabalhos noturnos que você deseja definir para o Core. Clique em qualquer opção selecionada para desmarcá-la.

6 Clique em **OK**.

  A caixa de diálogo **Trabalhos noturnos** é fechada e suas definições de trabalho noturno do Core são salvas.

Modificar definições de fila de transferência

As definições da fila de transferência são no nível do Core e estabelecem o número máximo de transferências simultâneas e de novas tentativas de transferência de dados.

Execute as etapas deste procedimento para modificar as definições da fila de transferência.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em (Definições) e execute um dos procedimentos a seguir:
- Na lista de definições do Core no lado esquerdo da página Definições, clique em **Fila de transferência**.
- Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Fila de transferência.

  As definições de Fila de transferência do Core são mostradas.

3 Clique na definição que você deseja alterar.

  A definição selecionada se torna editável.

4 Insira as informações de configuração conforme descrito na tabela a seguir.

Tabela 11. Informações das definições de fila de transferência

Caixa de texto	Descrição
Máximo de transferências simultâneas	Digite um valor para atualizar o número de transferências simultâneas. Defina um número de 1 a 60. Quanto menor o número, menor a carga sobre a rede e outros recursos do sistema. À medida que o número de agentes processados aumenta, o mesmo acontece com a carga sobre o sistema.
Número máximo de tentativas	Digite um valor para definir o número máximo de tentativas antes de cancelar a operação de transferência. Defina um número de 1 a 60.

5 Para cada configuração, quando estiver satisfeito com as alterações, clique em para salvar as alterações e sair do modo de edição, ou clique em para sair do modo de edição sem salvar.

Ajustar definições de tempo limite do cliente

As definições de tempo limite do cliente controlam por quanto tempo diferentes operações serão tentadas antes que o tempo se esgote.

NOTA: A Dell recomenda manter as definições padrão de tempo limite, a menos que você tenha problemas específicos em seu ambiente e um representante do Suporte Dell recomende a modificação das definições.

Execute as etapas deste procedimento para ajustar as definições de tempo limite do cliente.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Definições) e, em seguida, faça o seguinte:
- Na lista de definições do Core no lado esquerdo da página Definições, clique em **Tempo limite do cliente**.
- Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Tempo limite do cliente.

  As definições de Tempo limite do cliente do Core são mostradas.

3 Clique na definição que você deseja alterar.

A definição selecionada se torna editável.

4 Insira as informações de configuração conforme descrito na tabela a seguir.

5

Tabela 12. Informações das definições de tempo limite do cliente

Definição	Descrição
Tempo limite de conexão	Controla o tempo limite da conexão entre o Core e as máquinas protegidas ao enviar dados usando o protocolo de transferência de hipertexto (HTTP). Insira a quantidade de tempo que deve passar antes que um tempo limite de conexão ocorra. Usa o formato HH:MM:SS. **NOTA: A definição padrão é 0:05:00 ou cinco minutos.**
Tempo limite de leitura/gravação	Controla o tempo limite da conexão entre o Core e as máquinas protegidas ao ler ou gravar dados de fluxo através por HTTP. Um exemplo é o recebimento pelo Core de blocos de dados alterados de uma máquina protegida para criar um snapshot incremental. Insira a quantidade de tempo que deve passar antes que um tempo limite ocorra durante um evento de leitura/gravação. Usa o formato HH:MM:SS. **NOTA: A definição padrão é 0:05:00 ou cinco minutos.**
Tempo limite da UI	Controla o tempo limite da conexão entre a interface gráfica de usuário e o serviço Rapid Recovery Core por HTTP. Insira a quantidade de tempo que deve passar antes que um tempo limite de UI de conexão ocorra. Usa o formato HH:MM:SS. **NOTA: A definição padrão é 0:05:00 ou cinco minutos.**
Tempo limite da UI de leitura/gravação	Controla o tempo limite da conexão para leitura e gravação de fluxos de dados entre a interface gráfica de usuário e o serviço Rapid Recovery Core por HTTP. Insira a quantidade de tempo que deve passar antes que um tempo limite ocorra durante eventos de leitura ou gravação. Usa o formato HH:MM:SS. **NOTA: A definição padrão é 0:05:00 ou cinco minutos.**

6 Para cada definição, quando estiver satisfeito com suas alterações, clique na ✔ para salvar a alteração e sair do modo de edição, ou clique em ✖ para sair do modo de edição sem salvar.

Noções básicas sobre o cache de deduplicação e locais de armazenamento

A deduplicação global reduz a quantidade de espaço de armazenamento em disco necessário para os dados salvos em cópias de segurança pelo Core. Cada repositório é deduplicado, armazenando cada bloco único uma vez fisicamente em disco, e utilizando referências virtuais ou indicadores a esses blocos em cópias de segurança subsequentes. Para identificar blocos duplicados, o Rapid Recovery inclui um cache de deduplicação em repositórios de gerenciador de volume de deduplicação (DVM). O cache mantém referências a blocos exclusivos.

Por padrão, para repositórios de DVM, essa cache de deduplicação é de 1,5 GB. Esse tamanho é suficiente para vários repositórios. Até esse cache ser excedido, seus dados são deduplicados em todo o repositório. Quando a quantidade de informações redundantes for tão grande que o cache de deduplicação fique cheio, seu repositório não poderá mais tirar total vantagem de deduplicação adicional para dados recém-adicionados. A quantidade de dados salvos em seu repositório antes que o cache de deduplicação encha varia por tipo de dados salvos em cópias de segurança e é diferente para cada usuário.

É possível aumentar o tamanho do cache de deduplicação DVM alterando as definições do cache de deduplicação no Rapid Recovery Core. Para obter mais informações sobre como aumentar o tamanho do cache, consulte o tópico Configuração das definições de cache de deduplicação DVM.

Quando você aumentar o tamanho do cache de deduplicação DVM, há dois fatores a considerar: espaço em disco e uso de RAM.

Espaço em disco. Duas cópias do cache de deduplicação DVM são armazenadas em disco: um cache primário, e um cache secundário, que é uma cópia paralela. Portanto, se você estiver usando o tamanho de cache padrão 1,5 GB para um repositório de DVM, 3 GB de armazenamento em disco são usados no seu sistema. À medida que você aumenta o tamanho do cache, a quantidade de espaço em disco utilizado continua proporcionalmente o dobro do tamanho do cache. Para garantir o desempenho adequado e resistente a erros, o Core altera de forma dinâmica a prioridade desses caches. Ambos são necessários, a única diferença é que o cache designado como principal é salvo primeiro.

Uso de RAM. Quando o Rapid Recovery Core inicia, ele carrega o cache de deduplicação para a memória RAM. O tamanho do cache, portanto, afeta o uso de memória do seu sistema. A quantidade total de memória RAM usada pelo Core depende de muitos fatores. Esses fatores incluem quais operações estão em execução, o número de usuários, o número de máquinas protegidas e o tamanho do cache de deduplicação. Toda operação realizada pelo Core (transferência, replicação, rollup e assim por diante) consome mais RAM. Depois que uma operação é concluída, o consumo de memória diminui cada vez mais. Contudo, os administradores devem considerar o requisito mais alto do carregamento de RAM para obterem operações eficientes.

As definições padrão do Rapid Recovery Core colocam o cache principal, o cache secundário e o cache de metadados de repositórios de DVM no diretório AppRecovery. Essa pasta é instalada na máquina do Core.

NOTA: Dependendo de suas configurações, o diretório do AppRecovery pode não estar visível no Rapid Recovery Core. Para ver esse diretório, você pode precisar alterar as Opções de pasta no painel de controle para exibir arquivos, pastas e unidades ocultas.

Supondo que o Rapid Recovery Core esteja instalado na unidade C, esses locais são normalmente os seguintes:

Tabela 13. Os locais de armazenamento padrão para configurações do cache de deduplicação DVM

Definição	Local de armazenamento padrão
Local do cache principal	C:\ProgramData\AppRecovery\RepositoryMetaData\PrimaryCache
Local do cache secundário	C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache
Local do cache de metadados	C:\ProgramData\AppRecovery\RepositoryMetaData\CacheMetadata

Você pode alterar o local de armazenamento desses caches. Por exemplo, para aumentar a tolerância a erros, é possível alterar o local do seu cache secundário para uma unidade física diferente do cache principal, supondo que o Rapid Recovery Core tenha acesso ao local.

Para obter mais informações sobre como alterar os locais de armazenamento para qualquer dessas definições, consulte o tópico Configuração das definições de cache de deduplicação DVM.

A Dell recomenda que você planeje o armazenamento da deduplicação separadamente. A deduplicação ocorre apenas em um único repositório (não em vários repositórios). Se você estiver usando criptografia baseada em Core, a deduplicação é limitada aos dados protegidos por uma única chave, visto que, por motivos de segurança, cada chave funciona para um único domínio de criptografia.

Para obter mais informações sobre deduplicação, consulte Desduplicação no Rapid Recovery.

Configuração das definições de cache de deduplicação DVM

Execute as etapas deste procedimento para configurar as definições de cache de deduplicação de repositórios de DVM.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Definições) e execute um dos procedimentos a seguir:

- Na lista de definições do Core no lado esquerdo da página Definições, clique em **Cache de deduplicação DVM**. Essa definição é mostrada apenas se o seu Core tiver um ou mais repositórios de DVM.
- Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Cache de deduplicação DVM.

  As definições de Cache de deduplicação DVM do Core são mostradas.

3 Se você quiser restaurar as definições do cache de deduplicação DVM para o padrão a qualquer momento, faça o seguinte:

   a Na parte superior da área de definições do cache de deduplicação, clique em **Restaurar padrão**.

     A caixa de diálogo Restaurar padrão é exibida

   b Clique em **Sim** para confirmar a restauração.

4 Clique na definição que você deseja alterar.

  A definição selecionada se torna editável.

5 Para alterar definições individuais de cache de deduplicação, digite as informações de definição conforme descritas na tabela a seguir.

Tabela 14. Informações de definição do cache de deduplicação DVM

Definição	Descrição
Restaurar padrão	Esse controle redefine os locais de cache de DVM para os locais padrão do sistema, que são descritos para cada definição.
Local do cache principal	Se você desejar alterar o local do cache primário para repositórios de DVM, na caixa de texto Local de cache primário, insira o caminho para um local de armazenamento acessível ao Core. O local padrão é: C:\ProgramData\AppRecovery\RepositoryMetaData\PrimaryCache Uma vez que o cache principal e o secundário têm o mesmo tamanho, o armazenamento coletivo para esses dois caches exige duas vezes a quantidade de espaço da quantidade alocada para o tamanho do cache de deduplicação. Por exemplo, se você especificar a quantidade padrão de 1,5 GB para o tamanho do cache de deduplicação, garanta que cada um dos dois locais de armazenamento tenha, pelo menos, 1,5 GB. Em especial, se ambos os locais pertencerem à mesma unidade (por exemplo, a unidade C), deve haver pelo menos 3 GB de espaço livre em disco.
Local do cache secundário	Se você desejar alterar o local do cache secundário para repositórios de DVM, na caixa de texto Local de cache secundário, insira o caminho para um local de armazenamento acessível ao Core. O local padrão é: C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache

Definição	Descrição
Local de metadados de cache	Se você desejar alterar o local de metadados de cache para repositórios de DVM, na caixa de texto Local de metadados de cache, insira o caminho para um local de armazenamento acessível ao Core. O local padrão é: C:\ProgramData\AppRecovery\RepositoryMetaData\CacheMetadata
Tamanho do cache de deduplicação (GB)	Se você quiser alterar o tamanho do cache para deduplicação de repositórios de DVM, na caixa de texto Tamanho do cache de deduplicação, digite um novo valor (em GB). O local padrão é: C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache A definição mínima de tamanho do cache é de 1,5GB. Além disso, o tamanho do cache não pode exceder 50% da RAM instalada.

6 Para cada configuração, quando estiver satisfeito com as alterações, clique em ✔ para salvar as alterações e sair do modo de edição, ou clique em ✖ para sair do modo de edição sem salvar.

Configurar as definições do mecanismo Replay

Você pode configurar as informações relacionadas ao mecanismo Replay, que é o canal de comunicação do Rapid Recovery. Esses parâmetros determinam as definições do Core para proporcionar uma comunicação eficaz.

Em geral, a Dell recomenda usar as definições padrão. Em alguns casos, o Suporte da Dell pode solicitar que você modifique essas definições para ajustar o desempenho às suas necessidades de rede.

Conclua as etapas deste procedimento para configurar as definições do mecanismo Replay.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Definições) e, em seguida, faça o seguinte:
- Na lista de definições do Core no lado esquerdo da página Definições, clique em **Replay Engine**.
- Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Replay Engine.
  As definições do Replay Engine do Core são mostradas.

3 Clique na definição que você deseja alterar.
A definição selecionada se torna editável.

4 Insira as informações de configuração conforme descrito na tabela a seguir.

Tabela 15. Informações de definições do mecanismo Replay

Caixa de texto	Descrição
Endereço IP	O Core usa esse endereço IP para montar e restaurar um ponto de recuperação, para permitir o feedback entre máquinas protegidas e o Core. O endereço IP do mecanismo Replay é preenchido automaticamente com o endereço IP da máquina do Core. Se você inserir manualmente o endereço IP do servidor, esse valor é utilizado nos casos em que a máquina protegida não pode resolver automaticamente o endereço IP fornecido.

Caixa de texto	Descrição
	Você não precisará definir esse valor manualmente, a menos que tenha problemas com a conexão entre máquinas protegidas e o Core.
Porta de preferência	Insira um número de porta ou aceite a definição padrão. A porta padrão é 8007. A porta é usada para especificar o canal de comunicação do mecanismo Replay.
Porta em uso	Representa a porta em uso para a configuração do mecanismo Replay.
Permitir atribuição automática de porta	Clique para permitir a atribuição automática de porta TCP.
Grupo de administradores	Insira um novo nome para o grupo de administração. O nome padrão é BUILTIN\Administrators.
Comprimento de I/O assíncrono mínimo	Insira um valor ou escolha a definição padrão. Descreve o comprimento mínimo assíncrono de entrada/saída. A definição padrão é 65536.
Tempo limite de leitura	Insira um valor de tempo limite de leitura ou escolha a definição padrão. A definição padrão é 00:05:00.
Tempo limite de gravação	Insira um valor de tempo limite de gravação ou escolha a definição padrão. A definição padrão é 00:05:00.
Tamanho da memória intermediária de recebimento	Insira um tamanho de memória intermediária de entrada ou aceite a definição padrão. A definição padrão é 8192.
Tamanho da memória intermediária de envio	Insira um tamanho de memória intermediária de saída ou aceite a definição padrão. A definição padrão é 8192.
Sem atraso	Recomendamos deixar essa caixa de seleção desmarcada visto que, se isso não for feito, a eficiência da rede poderá ser afetada. Se for determinado que é preciso modificar essa configuração, entre em contato com o Suporte da Dell para obter orientações de como fazer isso.

5 Para cada definição, quando estiver satisfeito com suas alterações, clique na ✔ para salvar a alteração e sair do modo de edição, ou clique em ✖ para sair do modo de edição sem salvar.

Configurar as definições do implantação

O Rapid Recovery permite baixar instaladores do Rapid Recovery Core para as máquinas que você deseja proteger.

Você pode configurar definições relacionadas à implantação do software do agente do Rapid Recovery do seu Core para as máquinas que deseja proteger.

Conclua as etapas deste procedimento para configurar as definições de implantação.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Definições) e execute um dos procedimentos a seguir:
- Na lista de definições do Core no lado esquerdo da página Definições, clique em **Implantar**.
- Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Implantar.

As definições de Implantar do Core são mostradas.

3 Clique na definição que você deseja alterar.

A definição selecionada se torna editável.

4 Insira as informações de configuração conforme descrito na tabela a seguir.

Tabela 16. Informações das definições de implantação

Caixa de texto	Descrição
Nome do Agent installer	O nome padrão do arquivo é Agent-Web.exe. Se você quiser alterar esse nome de arquivo por qualquer motivo, você pode usar essa definição para especificar um novo nome para o arquivo executável do Core Web Installer. Esse arquivo gera um fluxo de download da versão mais recente do Rapid Recovery Core Installer, que é executada diretamente da Web e permite pausar e retomar o processo conforme necessário.
Endereço do Core	Insira o endereço do seu servidor Core. Geralmente isso consiste no protocolo, nome e porta do servidor Core e diretório em que os arquivos do Core residem. Por exemplo, se o servidor fosse Sample, a definição seria https://sample:8006/apprecovery/admin/Core
Tempo limite de falha de recebimento	Por quanto tempo a implantação do software Agent deve ser tentada antes de atingir o tempo limite. A definição padrão é 00:25:00 ou vinte e cinco minutos. Se você quiser alterar essa definição, digite o intervalo de tempo em que você quer que o sistema tente implantar o software do agente antes que um tempo limite ocorra durante eventos de leitura ou gravação. Usa o formato HH:MM:SS.
Máximo de instalações paralelas	Essa definição controla o número máximo de implantações do software Agent que o Core deve tentar ao mesmo tempo. A definição padrão é 100.

5 Para cada configuração, quando estiver satisfeito com as alterações, clique em ✔ para salvar as alterações e sair do modo de edição, ou clique em ✖ para sair do modo de edição sem salvar.

Configurar definições de conexão de banco de dados

O Rapid Recovery exibe informações sobre tarefas, eventos e alertas do Core na página Eventos. O Rapid Recovery armazena essas informações transacionais em um banco de dados de serviço MongoDB que, por padrão, é instalado localmente na máquina Core. Você pode configurar essas definições para alterar o tempo de retenção de informações no banco de dados ou o tamanho do pool de conexões para permitir mais ou menos conexões simultâneas.

Se estiver usando um segundo Rapid Recovery Core, você pode configurar as definições de conexão de banco de dados no primeiro Core para apontar para a segunda máquina Core. Dessa maneira, os dados de eventos dos dois Cores serão armazenados no MongoDB do segundo Core.

Você também pode configurar as definições de conexão de banco de dados do Core para apontar para outra máquina que possua um MongoDB instalado separadamente e esteja acessível ao Rapid Recovery Core através da rede. Nesse caso, os dados de transação de evento do seu Core são salvos nesse banco de dados de serviço e não localmente. Para obter mais informações sobre a configuração ou modificação de definições de conexão do banco de dados de serviço, consulte Configurar definições de conexão de banco de dados.

NOTA: Para obter mais informações sobre como visualizar informações de eventos do Rapid Recovery Core, consulte Como exibir eventos usando tarefas, alertas e registros.

Os clientes podem optar por especificar a instalação do banco de dados de serviço MongoDB em outra máquina que seja acessível ao Rapid Recovery Core na rede. Se o banco de dados de serviço do Rapid Recovery Core estiver instalado em uma máquina diferente daquela que hospeda o Rapid Recovery Core, você deverá fornecer credenciais de banco de dados (nome de usuário e senha) nessas definições.

Conclua as etapas deste procedimento para modificar as definições de conexão do banco de dados de serviço usado pelo Rapid Recovery Core.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Definições) e, em seguida, faça o seguinte:

- Na lista de definições do Core no lado esquerdo da página Definições, clique em **Conexão do banco de dados**.
- Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Conexão do banco de dados.
  As definições de Conexão do banco de dados do Core são mostradas.

3 Na parte superior da área de definições de Conexão do banco de dados, você pode fazer o seguinte:

- Clique em **Testar conexão** para confirmar as definições.
  É recomendável testar a conexão se você alterar qualquer uma das definições da conexão do banco de dados.
- Clique em **Restaurar padrão** para restaurar todas as definições padrão de conexão do banco de dados.
  Você será solicitado a confirmar esta ação, o que resulta em abandonar qualquer definição personalizada de conexão do banco de dados.

4 Clique na definição que você deseja alterar.
A definição selecionada se torna editável.

5 Insira as informações de configuração conforme descrito na tabela a seguir.

Tabela 17. Informações das definições de conexão do banco de dados

Caixa de texto	Descrição
Nome do host	Insira um nome de host para a conexão de banco de dados. **NOTA: Quando localhost é o parâmetro especificado como host, o MongoDB é instalado localmente na máquina que hospeda o Core.**
Port	Insira o número da porta para a conexão do banco de dados. **NOTA: A definição padrão é 27017.**
Nome de usuário	Insira o nome de um usuário com privilégios administrativos para o banco de dados de serviço MongoDB. **NOTA: Se o parâmetro do nome do host é localhost, esse campo não é necessário.**
Senha	Insira a senha associada ao nome de usuário que você especificou. **NOTA: Se o parâmetro do nome do host é localhost, esse campo não é necessário.**
Período de retenção (dia)	Insira o número de dias de retenção do histórico de eventos e trabalhos no banco de dados de serviço.
Tamanho máximo do pool de conexão	Define o número máximo de conexões de banco de dados em cache para permitir a reutilização dinâmica. **NOTA: A definição padrão é 100.**
Tamanho mínimo do pool de conexão	Define o número mínimo de conexões de banco de dados em cache para permitir a reutilização dinâmica. **NOTA: A definição padrão é 0.**

6 Para cada definição, quando estiver satisfeito com suas alterações, clique na  para salvar a alteração e sair do modo de edição, ou clique em  para sair do modo de edição sem salvar.

Modificação das definições locais de conexão do banco de dados

Você pode ver eventos do sistema relacionados ao Rapid Recovery Core na página Eventos. O Rapid Recovery Core armazena essas informações transacionais em um banco de dados de serviço MongoDB. Por padrão, esse banco de dados é instalado localmente na máquina do Core e o nome do host nas definições de conexão do banco de dados é padronizado como localhost. Nessa situação, a interface loopback ignora o hardware de interface de rede local e as credenciais do banco de dados não são necessárias.

Opcionalmente, para aumentar a segurança, você pode especificar as credenciais do banco de dados explicitamente (um nome de usuário e senha) para o banco de dados MongoDB usado pelo Rapid Recovery Core.

NOTA: Para obter mais informações sobre como visualizar informações de eventos do Rapid Recovery Core, consulte Como exibir eventos usando tarefas, alertas e registros. Para obter informações sobre as definições de conexão do banco de dados, consulte Configurar definições de conexão de banco de dados.

Execute as etapas deste procedimento para modificar as definições de conexão do banco de dados local para especificar as credenciais do banco de dados.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Definições) e execute um dos procedimentos a seguir:
- Na lista de definições do Core no lado esquerdo da página Definições, clique em **Definições do banco de dados local**.
- Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Definições do banco de dados local.

  As definições de Banco de dados local do Core são mostradas.

3 Clique na definição que você deseja alterar.

A definição selecionada se torna editável.

4 Digite as credenciais adequadas para se conectar ao banco de dados do serviço, conforme descrito na tabela a seguir.

Tabela 18. Informações das definições do banco de dados local

Caixa de texto	Descrição
Nome de usuário	Insira o nome de um usuário com privilégios administrativos para o banco de dados de serviço MongoDB.
Senha	Insira a senha associada ao nome de usuário que você especificou.

5 Para cada configuração, quando estiver satisfeito com as alterações, clique em ✓ para salvar as alterações e sair do modo de edição, ou clique em ✕ para sair do modo de edição sem salvar.

Gerenciamento das definições do servidor de SMTP

Se você configurar as definições do servidor de SMTP (simple mail transfer protocol) no Core, poderá enviar notificações de tarefas, eventos e alertas por e-mail.

As informações sobre a configuração de um servidor de e-mails SMTP são descritas no tópico Configurar um servidor de e-mail.

NOTA: Para enviar informações sobre eventos por e-mail, você também deve configurar as definições de grupo de notificação. Para obter mais informações sobre especificação de eventos para recepção de alertas de e-mail, consulte Configurar grupos de notificação.

Gerenciamento dos parâmetros de configuração da nuvem

No Rapid Recovery, você pode associar contas de armazenamento que você tem com provedores de armazenamento em nuvem ao Rapid Recovery Core. Isso permite a você arquivar as informações de máquinas protegidas quando os dados se tornarem obsoletos.

O Rapid Recovery se integra com Amazon™ S3, Microsoft Azure e provedores de nuvem gerenciada usando a tecnologia de código aberto OpenStack.

Para obter mais informações sobre o gerenciamento de informações de conta de armazenamento em nuvem no Rapid Recovery Core, consulte Gerenciar contas de nuvem.

Gerenciamento de definições de relatórios

Você pode gerar relatórios para o Rapid Recovery Core ou para máquinas protegidas. Para obter informações sobre os relatórios que você pode gerar, consulte Gerar e visualizar relatórios.

Execute as etapas deste procedimento para gerenciar as definições de relatórios do Core.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Definições) e execute um dos procedimentos a seguir:

- Na lista de definições do Core no lado esquerdo da página Definições, clique em **Relatórios**.
- Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Relatórios.

  As definições de **Relatórios** do Core são mostradas. As Definições de relatórios são descritas na tabela a seguir.

Opção	Descrição
Restaurar padrão	Esta opção restaura todas as definições de relatório com as definições padrão. Os padrões de cada definição são listados abaixo.
Fonte	Esta opção controla a fonte padrão usada nos relatórios. O padrão é a fonte tipográfica Trebuchet MS. Você pode alterar essa definição para qualquer fonte tipográfica disponível em seu sistema.
Tamanho do papel	Esta opção controla o tamanho de papel padrão para a impressão de relatórios. O padrão é A4. Você pode selecionar dentre os seguintes tamanhos de papel: • Carta • Tabloide • Ledger • Ofício • A3 • A4 • Executivo • B4 • C3Envelope • C4Envelope
Orientação da página	Esta opção controla a orientação da página para relatórios exportados. A orientação padrão é Retrato. Você pode selecionar dentre as seguintes opções de layout: • Retrato • Paisagem

3 Para alterar qualquer uma das definições para os Relatórios, clique no campo da definição apropriada.
O campo da definição é mostrado como um menu suspenso configurável.

4 Clique no menu suspenso e selecione um dos valores disponíveis.
Por exemplo, no campo Fonte, clique em **Times New Roman**.

5 Para cada configuração, quando estiver satisfeito com as alterações, clique em ✔ para salvar as alterações e sair do modo de edição, ou clique em ✖ para sair do modo de edição sem salvar.
A opção selecionada agora aparece como a nova definição do parâmetro selecionado dos Relatórios.

Gerenciamento das definições de Capacidade de anexação SQL do Core

As verificações de capacidade de anexação do SQL ocorrem como parte dos trabalhos noturnos do Rapid Recovery. Para reduzir os custos de licenciamento, o Rapid Recovery oferece duas opções para executar verificações de capacidade de anexação: usando uma instância licenciada do SQL Server instalada na máquina do Rapid Recovery Core ou usando a instância do SQL Server já instalada na sua máquina protegida. Esta segunda opção agora é a definição padrão. No entanto, se sua máquina protegida já estiver ativa quando os trabalhos noturnos ocorrerem, considere realizar das verificações com uma instância do SQL Server no Core.

No resumo, o processo de gerenciamento das configurações de capacidade de anexação do SQL do Core envolve as seguintes tarefas:

- Montar o último ponto de recuperação de grupos de proteção que contêm bancos de dados.
- Conectar ao banco de dados a partir do SQL Server.
- Abrir o banco de dados.
- Fechar o banco de dados.
- Desmontar o ponto de recuperação.
  Para ativar essa verificação noturna, especifique uma instância do SQL Server a ser usada para realizar verificações de capacidade de anexação de bancos de dados SQL Server em máquinas protegidas.

NOTA: Esta opção aparece apenas quando há um SQL Server sendo protegido no Core.

Para configurar o Core para executar as verificações de capacidade de anexação do SQL como parte dos trabalhos noturnos, siga as seguintes etapas.

NOTA: Se você selecionar a opção padrão para usar a instância do SQL Server instalada na máquina protegida, essa instância do SQL Server gerenciará a capacidade de anexação de SQL em todas as máquinas SQL protegidas. Se você não quiser que essa configuração se aplique a todas as máquinas SQL protegidas, selecione Usar o SQL Server no core. Para realizar verificações de capacidade de anexação no Core, você precisa instalar ou usar uma versão licenciada do SQL Server na máquina do Core.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Definições) e, em seguida, faça o seguinte:
- Na lista de definições do Core no lado esquerdo da página Definições, clique em **Capacidade de anexação**.
- Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Capacidade de anexação.

3 Para usar a instância do SQL Server instalada na máquina SQL Server protegida, selecione **Usar o SQL Server na máquina protegida**. Essa é a opção padrão.

4 Para usar a instância do SQL Server instalada no Rapid Recovery Core, selecione **Usar o SQL Server no core** e insira as informações de autenticação, conforme descrito na tabela a seguir.

Tabela 19. Informações de credenciais do SQL Server

Caixa de texto	Descrição
SQL Server	No menu suspenso do SQL Server, selecione a instância adequada do SQL Server no servidor do Core.
Tipo de credencial	Selecione o método de autenticação adequado para suas credenciais entre as opções a seguir: • Windows • SQL
Nome de usuário	Especifique um nome de usuário para acessar o SQL Server no Core com base no tipo de credencial selecionado.
Senha	Especifique uma senha para acessar o SQL Server no Core com base no tipo de credencial selecionado.

5 Clique em **Testar conexão**.

NOTA: Se as credenciais forem inseridas de forma incorreta, será exibida uma mensagem para alertá-lo de que as credenciais falharam. Corrija as informações de credenciais e teste novamente a conexão.

6 Quando estiver satisfeito com as alterações, clique em **Aplicar**.

Noções básicas sobre trabalhos do Core

Trabalhos do Core são processos que o Rapid Recovery Core executa para dar suporte às suas operações, incluindo backup para pontos de recuperação, replicação de dados, arquivamento de dados, exportação de dados para VMs, manutenção de repositórios, etc. Os trabalhos do Core são iniciados automaticamente para algumas operações, como replicação ou arquivamento, de acordo com a programação estabelecida. Você também pode chamar alguns trabalhos sob demanda de vários elementos do Core Console.

- Ao visualizar ou editar as definições de trabalho do Core, cada trabalho tem dois parâmetros: Máximo de trabalhos simultâneos e Contagem de tentativas.
  - O parâmetro Máximo de trabalhos simultâneos determina quantos trabalhos desse tipo podem ser executados ao mesmo tempo.
  - O parâmetro Contagem de tentativas determina quantas vezes o trabalho deve ser tentado antes de ser abandonado, caso erros de rede ou outros erros evitem a conclusão na primeira vez.
- Na tabela Trabalhos do Core, a coluna Definições indica se o trabalho listado está incluído nas definições de trabalho do Core por padrão ou precisa ser explicitamente adicionado.

A tabela a seguir descreve os principais trabalhos do Core disponíveis e suas funções.

Tabela 20. Trabalhos do Core

Nome do trabalho	Descrição	Máximo de trabalhos simultâneos	Contagem de tentativas	Definições
Verificar a capacidade de anexação de bancos de dados SQL em snapshots	Permite que o Core verifique a consistência dos bancos de dados SQL e garante que todos os arquivos de apoio MDF (dados) e LDF (log) estejam disponíveis no snapshot de backup. Processo: • Montar o último ponto de recuperação de grupos de proteção que contêm bancos de dados SQL. • Montar o banco de dados. Se você estiver realizando a capacidade de anexação do servidor SQL protegido, monte usando o caminho de UNC. • Conectar ao banco de dados a partir do SQL Server. • Realizar a verificação de capacidade de anexação.	1	0	Padrão

Nome do trabalho	Descrição	Máximo de trabalhos simultâneos	Contagem de tentativas	Definições
	• Realizar operações limpeza. • Fechar o banco de dados. • Desmontar o banco de dados. • Desmontar o ponto de recuperação.			
Verificar a soma de verificação dos bancos de dados do Exchange	Verifica a integridade de pontos de recuperação que contêm bancos de dados do Exchange. Processo: • Montar o último ponto de recuperação de grupos de proteção que contêm bancos de dados SQL. • Conectar ao banco de dados a partir do SQL Server. • Abrir o banco de dados. • Fechar o banco de dados. • Desmontar o ponto de recuperação.	1	0	Padrão
Verificar a montabilidade de bancos de dados do Exchange	Verifica se os bancos de dados do Exchange são montáveis.	1	0	Padrão
Replicar dados de máquinas protegidas a partir da origem remota	Transfere uma cópia dos pontos de recuperação para uma máquina protegida de um Core de origem para um Core de destino. Este trabalho é executado no Core de destino que recebe os pontos de recuperação replicados de entrada.	3	0	Padrão
Replicar dados de máquinas protegidas no destino remoto	Transfere uma cópia dos pontos de recuperação para uma máquina protegida de um Core de origem (no qual foram salvos originalmente) para um Core de destino. Este trabalho é executado no Core de origem e controla a replicação de saída.	1	3	Padrão
Realizar rollup dos pontos de recuperação	Aplica a política de retenção aos seus dados de backup com a combinação de pontos de recuperação "em execução" na programação definida pela política de retenção.	1	0	Padrão
Verificar pontos de recuperação	Verifica a integridade dos pontos de recuperação.	1	0	Adicionar
Excluir todos os pontos de recuperação	Exclui todo o conjunto de pontos de recuperação em uma máquina protegida.	1	0	Adicionar
Excluir cadeia de pontos de recuperação	Exclui toda uma cadeia de pontos de recuperação em uma máquina protegida.	1	0	Adicionar
Excluir intervalo de pontos de recuperação	Exclui um conjunto de pontos de recuperação em uma máquina protegida, por identificação do ponto de recuperação ou período.	1	0	Adicionar
Implantar o software Agent em máquinas	Implanta o software do agente Rapid Recovery na máquina ou nas máquinas especificadas.	1	0	Adicionar
Baixar bibliotecas do Exchange	Baixa as bibliotecas do Microsoft Exchange da máquina protegida para a máquina do Core no caminho **C:\ProgramData\AppRecovery\ExchangeLibraries**.	1	0	Adicionar

Nome do trabalho	Descrição	Máximo de trabalhos simultâneos	Contagem de tentativas	Definições
Exportar para arquivo	Cria um backup no caminho especificado com um arquivamento dos pontos de recuperação selecionados. Processo: • Montar pontos de recuperação. • Gravar dados nos backups. • Desmontar o ponto de recuperação.	1	0	Adicionar
Exportar para máquina virtual	Exporta dados do ponto de recuperação especificado da máquina protegida para o caminho de destino como uma máquina virtual. Processo: • Montar ponto de recuperação. • Criar máquina virtual a partir dos dados do ponto de recuperação no caminho de destino. • Desmontar o ponto de recuperação.	1	0	Adicionar
Importar arquivos	Importa o ponto de recuperação a partir do backup especificado em um arquivamento do Core criado anteriormente.	1	0	Adicionar
Manter repositório	Realiza uma verificação do repositório. Processo: • Verificar o sistema de arquivos do repositório. • Montar ponto de recuperação. • Recalcular cache de deduplicação do repositório. • Carregar pontos de recuperação do repositório.	1	0	Adicionar
Montar snapshots de pontos de recuperação	Realiza a montagem do ponto de recuperação para o caminho especificado.	1	0	Adicionar
Proteger máquinas virtuais ESX®	Adiciona todas as máquinas virtuais especificadas a uma proteção sem agentes. O trabalho é realizado imediatamente depois de adicionar a proteção sem agentes de uma ou mais VMs ao Core usando o Assistente de proteção de diversas máquinas. O trabalho define um número de identificação para cada VM especificada, grava informações sobre o Core em um arquivo de configuração e recupera metadados a partir do arquivo.	1	0	Adicionar
Restaurar do ponto de recuperação	Realiza uma restauração a partir de um ponto de recuperação para uma máquina de destino especificada. Processo: • Montar ponto de recuperação. • Gravar todos os dados do ponto de recuperação na máquina especificada. • Desmontar o ponto de recuperação.	1	0	Adicionar
Carregar logs	Carrega logs no servidor especificado.	1	0	Adicionar

Alguns trabalhos do Core estão incluídos em Definições. As Definições de trabalhos permitem que você especifique quantos trabalhos simultâneos do mesmo tipo o Core pode realizar e quantas novas tentativas devem ser realizadas se a primeira tentativa falhar.

Para obter mais informações sobre essas Definições, consulte Definições de trabalhos do Core.

Para obter informações sobre como adicionar trabalhos às Definições do Core, consulte Adição de trabalhos do Core às definições.

Para obter informações sobre como editar as definições de trabalhos na lista Definições, consulte Editar as definições de trabalhos do Core.

Definições de trabalhos do Core

Ao selecionar  (Definições) na barra de ícones, você pode acessar as definições de alguns trabalhos do Core. A área **Trabalhos** da página de definições do Core permite que você determine duas definições para cada tipo de trabalho listado:

1 O número máximo de trabalhos desse tipo que o Core deve tentar por vez. O valor deve ser definido entre 1 e 50.

2 O número de vezes que um trabalho deve ser tentado se um erro de rede ou outro erro de comunicação impedir a conclusão do trabalho na primeira vez. O valor deve ser definido entre 0 e 10.

Vários trabalhos são incluídos automaticamente nas definições do Core. Esses trabalhos incluem um valor de "Padrão" na coluna Definições (conforme mostrado no tópico Noções básicas sobre trabalhos do Core).

Você pode adicionar alguns outros trabalhos às definições se quiser configurar essas definições para controlar o número máximo de trabalhos ou novas tentativas para essas funções. Esses trabalhos incluem um valor de "Adicionar" na coluna Definições. Para obter informações sobre como adicionar esses trabalhos para à tabela Definições, consulte Adição de trabalhos do Core às definições.

Não é possível definir esses dois parâmetros em trabalhos do Core indisponíveis nas Definições.

No caso de trabalhos mostrados nas definições, você pode editar as definições existentes. Isso permite que você personalize os dois parâmetros, exclua um tipo de trabalho da lista Definições de trabalho ou restaure as definições padrão. Para obter informações mais detalhadas, consulte o tópico Editar as definições de trabalhos do Core.

Adição de trabalhos do Core às definições

As definições de trabalhos do Core permitem definir, para cada tipo de trabalho, o número máximo de trabalhos que o Core deve tentar de cada vez e quantas vezes o trabalho deve ser repetido se a primeira tentativa falhar.

Cada tipo de trabalho do Core tem valores padrão para esses dois parâmetros, conforme descrito no tópico Definições de trabalhos do Core. Esta lista também indica que tipos de trabalho são incluídos por padrão nas definições do Core.

A adição de um trabalho do Core às definições permite alterar esses parâmetros para o tipo de trabalho adicionado.

Execute as etapas do procedimento a seguir para adicionar um trabalho às definições do Core.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Definições) e execute um dos procedimentos a seguir:
- Na lista de definições do Core no lado esquerdo da página Definições, clique em **Trabalhos**.
- Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Trabalhos.
  As definições de Trabalhos do Core são mostradas.

3 Na página de Definições do Core, em Trabalhos, clique em **Adicionar**.
A caixa de diálogo Definições de trabalho é exibida.

4 Na caixa de diálogo **Definições de trabalho**, no campo **Trabalhos**, selecione o nome de um trabalho que você deseja adicionar às definições do Core.

Esses trabalhos são descritos no tópico Definições de trabalhos do Core.

5 Para definir o número máximo de trabalhos que o Core pode realizar ao mesmo tempo, na caixa de texto **Máximo de trabalhos simultâneos**, insira um novo valor entre 1 e 50.

6 Para definir o número de tentativas que o Core deve fazer antes de abandonar o trabalho, na caixa de texto **Contagem de tentativas**, insira um novo valor entre 0 e 10.

7 Clique em **Salvar**.

A caixa de diálogo Definições de trabalho é fechada e as novas definições de trabalho são aplicadas.

Editar as definições de trabalhos do Core

As definições de trabalhos do Core permitem definir, para cada tipo de trabalho, o número máximo de trabalhos que o Core deve tentar de cada vez e quantas vezes o trabalho deve ser repetido se a primeira tentativa falhar.

Cada tipo de trabalho do Core tem valores padrão para esses dois parâmetros, conforme descrito no tópico Noções básicas sobre trabalhos do Core. Esta lista também indica que tipos de trabalho são incluídos por padrão nas definições do Core. Ao editar as definições de trabalhos do Core, você pode fazer o seguinte:

- Você pode personalizar as definições de cada tipo de trabalho do Core.
- Você pode excluir um tipo de trabalho da lista de definições do Core. Esse recurso não está disponível se o tipo de trabalho estiver incluído nas definições por padrão.

NOTA: Excluir um trabalho das definições do Core simplesmente remove o tipo de trabalho dessa lista. Para editar as definições do Core para esse tipo de trabalho novamente no futuro, você pode adicioná-lo à lista como descrito no tópico Adição de trabalhos do Core às definições.

- Você pode restaurar as definições de qualquer tipo de trabalho para as definições padrão.

NOTA: Embora você possa usar esse recurso apenas para os tipos de trabalho incluídos por padrão nas definições do Core, você pode definir outros tipos de trabalho nos padrões removendo da lista e adicionando novamente.

Execute as etapas do procedimento a seguir para editar as definições de um trabalho.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Definições) e execute um dos procedimentos a seguir:

- Na lista de definições do Core no lado esquerdo da página Definições, clique em **Trabalhos**.
- Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Trabalhos.

As definições de Trabalhos do Core são mostradas.

3 Na grade Trabalho, selecione um trabalho que você deseja remover da lista. No menu suspenso  do trabalho, selecione **Excluir**.

O trabalho é removido da lista.

4 Na grade Trabalho, selecione um trabalho na lista para o qual você quer redefinir as configurações. No menu suspenso  do trabalho, selecione **Redefinir com os padrões**.

As definições desse trabalho são redefinidas com as definições padrão.

5 Na grade Trabalho, selecione o trabalho que você deseja alterar. No menu suspenso  do trabalho, selecione **Editar**.

6 A caixa de diálogo Definições de trabalho [NomedoTrabalho] é aberta.

7 Para alterar o número máximo de trabalhos que o Core pode realizar ao mesmo tempo, na caixa de texto Máximo de trabalhos simultâneos, insira um novo valor entre 1 e 50.

8 Para alterar a definição relativa ao número de tentativas adicionais que o Core deve fazer antes de abandonar o trabalho, na caixa de texto Contagem de tentativas, insira um novo valor entre 0 e 10.

9 Clique em **Salvar**.

A caixa de diálogo Definições de trabalho é fechada e as novas definições de trabalho são aplicadas.

Gerenciar licenças

Muitos usuários do Rapid Recovery Core começam com uma licença de teste, que tem recursos limitados. Uma licença de teste é válida por 14 dias e pode ser estendida uma única vez pelo administrador do grupo para 28 dias. Quando o período de teste expira, o Rapid Recovery Core para de criar snapshots até você obter e registrar uma licença válida que não seja de teste.

NOTA: Para obter informações sobre como inserir uma chave de licença ou as informações do arquivo (por exemplo, atualizar ou alterar uma licença de teste para uma licença válida de longo prazo), consulte Atualização ou alteração de uma licença.

As licenças são validadas usando arquivos de licença ou chaves de licença.

Arquivos de licença são arquivos de texto que terminam com a extensão de arquivo **.lic**. Exemplos de arquivos de licença incluem os seguintes:

- Os arquivos de licença podem aparecer com comprimento de 9 caracteres, que consistem de três grupos de números arábicos separados por um hífen, por exemplo: `123-456-789.lic`.
- Licenças baseadas em software podem aparecer no formato Software-<nome do grupo>.lic, com o nome do grupo após o nome do cliente ou conta, por exemplo: `Software-YourCompany.lic`.
- Licenças de dispositivos Dell podem aparecer no formato <Série do dispositivo>-<nome do grupo>.lic, com o nome do grupo após a conta do nome do cliente, por exemplo: `DL4X00 Series-YourCompany.lic`.

Chaves de licença têm 30 caracteres e consistem de seis grupos de caracteres alfanuméricos ingleses separados por um hífen. Por exemplo, um formato de chave de licença de amostra é `ABC12-DEF3G-H45IJ-6K78L-9MN10-OPQ11`.

O Rapid Recovery gerenciar licenças ou entrar em contato com o servidor de licenças diretamente a partir do Core Console selecionando  (Definições) na barra de ícones e clicando em **Aplicação de licença**.

As definições de Aplicação de licença incluem as seguintes informações:

Detalhes da licença:

- **Alterar licença**. Permite a você alterar uma licença existente associada ao Core carregando um arquivo de licença ou inserindo uma chave de licença.
- **Adicionar licença**. Esta opção está disponível somente para dispositivos de backup da Dell e permite que você carregue um arquivo de licença ou insira uma chave de licença.
- **Grupo de portal de licenças**. Esta opção abre o portal de licenças para gerenciamento do grupo.
- **Tipo de licença**. Os tipos de licenças incluem Teste, Assinatura e Empresa. Para obter mais informações, consulte o tópico Sobre Dell Data Protection | Portal de licenças do Rapid Recovery Tipos de licença de software no Guia do usuário do Dell Data Protection | Portal de licenças do Rapid Recovery.
- **Status da licença**. Indica o status da licença. Um status ativo garante que os snapshots podem continuar conforme programado. Se a licença estiver bloqueada ou expirada ou se o Core não conseguir se comunicar com o Dell Data Protection | Portal de licenças do Rapid Recovery após o período de avaliação, os snapshots serão pausados até que o status da licença seja corrigido.

Limitações de licença:

- **Número máximo de snapshots por dia**. Indica o número de backups limitados pela licença específica.

Conjunto de licenças:

- **Tamanho do conjunto**. O conjunto de licenças é o número de licenças que não são de teste disponíveis para alocação entre grupos e subgrupos no Dell Data Protection | Portal de licenças do Rapid Recovery. O tamanho do conjunto indica quantas licenças podem ser alocadas. Para obter mais informações, consulte o tópico “Noções básicas dos conjuntos de licenças” no*Guia do usuário doDell Data Protection | Portal de licenças do Rapid Recovery*.
- **Protegido por este Core**. Indica o número de máquinas deste conjunto de licenças que são protegidas por este Core.

- **Total protegido no grupo**. Indica o número total de máquinas protegidas no mesmo grupo de licenças deste Core.

Servidor de licenças. Essas definições se aplicam a licenças padrão (phone home). Essas definições não se aplicam a appliances e a outras licenças que não sejam do tipo phone home:

- **Endereço do servidor de licenças**. Exibe uma URL ativa do servidor de licenças associado a este Core.
- **Última resposta do servidor de licenças**. Indica se a última tentativa de comunicação com o portal do servidor de licenças teve êxito.
- **Último contato com o servidor de aplicação de licença**. Exibe a data e hora do último contato bem-sucedido com o servidor de aplicação de licença.
- **Próxima tentativa de contato com o servidor de aplicação de licença**. Indica a próxima data e hora programada para a tentativa de comunicação com o servidor de aplicação de licença.
- **Entrar em contato agora**. Este botão entra em contato com o servidor de licenças sob demanda. Use esta opção após fazer alterações em sua configuração de licenças para registrá-las imediatamente em vez de aguardar a próxima tentativa programada.

Para obter mais informações sobre as licenças, consulte o *Guia do usuário do Dell Data Protection | Portal de licenças do Rapid Recovery*.

Para obter mais informações sobre como adicionar ou alterar uma chave ou arquivo de licença, consulte Atualização ou alteração de uma licença.

Para obter mais informações sobre como entrar em contato com o servidor do portal de licenças, consulte Contato com o servidor do Dell Data Protection | Portal de licenças do Rapid Recovery

Você também pode visualizar as informações de aplicação de licença relativas a uma única máquina protegida. Para obter informações, consulte Visualizar informações de licença em uma máquina.

Atualização ou alteração de uma licença

Depois de ou comprar uma licença de longo prazo do Rapid Recovery, você receberá por e-mail um arquivo de licença ou uma chave de licença.

Execute as etapas descritas neste procedimento para atualizar sua licença de teste ou alterar sua licença existente e associá-la ao Rapid Recovery Core Console.

NOTA: Os usuários de dispositivos de backup da Dell também podem adicionar licenças ao Core se necessário. Para obter mais informações, consulte Adição de uma licença.

Para obter informações sobre como adquirir uma chave de licença ou obter mais detalhes sobre como usar o portal de licenças para fazer baixar software, registrar dispositivos, gerenciar assinaturas e grupos de licença e gerar relatórios do portal de licenças, consulte o Guia do usuário do *Dell Data Protection | Portal de licenças do Rapid Recovery*.

Se você tiver acabado de instalar um novo Core e for solicitado a escolher um arquivo ou uma chave de licença, vá para a Etapa 5.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Definições).

3 Role a tela para baixo no lado direito da página **Definições** até ver o cabeçalho Aplicação de licença.
As definições de aplicação de licença do Core são exibidas.

4 Para atualizar ou alterar a licença existente associada ao Core, na parte superior da área de definições Detalhes da licença do Core, clique em  **Alterar licença**.
A caixa de diálogo **Change License** (Alterar licença) aparece.

5 Para inserir uma chave de licença ou carregar um arquivo de licença, selecione uma das opções a seguir:
   a Se você quiser *inserir manualmente* a chave de licença, na caixa de diálogo Alterar licença, digite a chave com cuidado e clique em **Continuar**.
   A caixa de diálogo é fechada, o arquivo de licença que você selecionou é autenticado e essa licença é associada ao Core.
   b Se você quiser *fazer upload* de um arquivo de licença, na caixa de diálogo Alterar licença, clique em **Escolher arquivo**.

Na caixa de diálogo **Carregamento de arquivo**, navegue pelo sistema de arquivos e localize o novo arquivo de licença que você quer usar. Por exemplo, localize`Software-YourCompany.lic`.

c Clique no arquivo de licença e em **Abrir**.

A caixa de diálogo Carregamento de arquivo é fechada. O arquivo de licença selecionado aparece na caixa de diálogo Alterar licença.

d Na caixa de diálogo **Alterar licença**, clique em **Continuar**.

A caixa de diálogo é fechada, o arquivo de licença que você selecionou é autenticado e essa licença é associada ao Core.

6 Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Servidor de licenças.

As definições de Aplicação de licença do Core são mostradas.

7 Na área Servidor de licenças, clique em **Entrar em contato agora**.

Assim que a licença é aplicada ao servidor de licenças, todas as máquinas protegidas associadas são atualizadas automaticamente com a nova licença.

Adição de uma licença

Os proprietários de dispositivos de backup da Dell podem adicionar uma ou mais licenças ao Rapid Recovery Core Console.

Assim que você tiver atualizado ou adquirido sua licença do Rapid Recovery, você receberá um arquivo de licença ou uma chave de licença por e-mail.

Você também pode atualizar ou alterar uma licença existente no Core Console. Para obter mais informações, consulte Atualização ou alteração de uma licença.

NOTA: Somente usuários de dispositivos de backup da Dell podem ver o botão Adicionar dispositivo.

NOTA: Para obter informações sobre como obter uma chave de licença, consulte o *Guia do usuário do* Dell Data Protection | Portal de licenças do Rapid Recovery.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Definições).

3 Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Aplicação de licença.

As definições de aplicação de licença do Core são exibidas.

4 Para adicionar uma licença e associá-la ao Core, na parte superior da área de definições Detalhes da licença do Core, clique em **Adicionar licença**. **Na**caixa de diálogo **Adicionar licença**, realize um dos procedimentos a seguir:

a Se você quiser *inserir manualmente* a chave de licença, na caixa de diálogo Alterar licença, digite a chave com cuidado e clique em **Continuar**.

A caixa de diálogo é fechada, o arquivo de licença que você selecionou é autenticado e essa licença é associada ao Core.

b Se você quiser *fazer upload* de um arquivo de licença, na caixa de diálogo Alterar licença, clique em **Escolher arquivo**.

Na caixa de diálogo **Carregamento de arquivo**, navegue pelo sistema de arquivos e localize o novo arquivo de licença que você quer usar. Por exemplo, localize`Software-YourCompany.lic`.

c Clique no arquivo de licença e em **Abrir**.

A caixa de diálogo Carregamento de arquivo é fechada. O arquivo de licença selecionado aparece na caixa de diálogo Alterar licença.

d Na caixa de diálogo **Alterar licença**, clique em **Continuar**.

A caixa de diálogo é fechada, o arquivo de licença que você selecionou é autenticado e essa licença é associada ao Core.

5 Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Servidor de licenças.

As definições de Aplicação de licença do Core são mostradas.

6 Na área Servidor de licenças, clique em **Entrar em contato agora**.

Assim que a licença é aplicada ao servidor de licenças, todas as máquinas protegidas associadas são atualizadas automaticamente com a nova licença.

Contato com o servidor do Dell Data Protection | Portal de licenças do Rapid Recovery

O Rapid Recovery Core Console entra em contato com o servidor do portal frequentemente para permanecer atualizado com as mudanças feitas no Dell Data Protection | Portal de licenças do Rapid Recovery.

No caso de licenças que não são de teste, o Rapid Recovery Core entra em contato com o portal de licenças a cada hora. Se não consegue se conectar ao portal de licenças após o período de avaliação de 10 dias, o Core para de criar snapshots.

Normalmente, a comunicação com o server do portal de licenças ocorre automaticamente em intervalos designados. No entanto, é possível iniciar a comunicação sob demanda.

Execute as etapas deste procedimento para entrar em contato com o server do portal de licenças.

1 Navegue até o Rapid Recovery Core Console.
2 Na barra de ícones, clique em **Definições** e role a tela para baixo no lado direito da página **Definições** até ver o cabeçalho Servidor de licenças.
3 Na área Server de licenças, clique em **Entrar em contato agora**.

Noções básicas das definições do SNMP

O Protocolo Simples de Gerenciamento de Rede (SNMP) é um protocolo para gerenciar dispositivos em uma rede IP. O SNMP é usado principalmente para monitorar dispositivos em uma rede a fim de detectar condições que exigem atenção. O protocolo usa componentes de software (agentes) para enviar informações para computadores administrativos (gerentes). Um agente SNMP processa as solicitações do gerente para obter ou definir certos parâmetros. O agente SNMP pode enviar interceptações (notificações sobre eventos específicos) ao gerente.

Os objetos de dados gerenciados por agentes SNMP são organizados em um arquivo de Base de Informações de Gerenciamento (MIB) que contém Identificadores de Objeto (OIDs). Cada OID identifica uma variável que pode ser lida ou definida usando SNMP.

O Rapid Recovery inclui suporte para SNMP versão 1.0.

Você pode configurar o Rapid Recovery Core como um agente SNMP. Assim o Core pode enviar informações como alertas, status do repositório e máquinas protegidas. Um host SNMP pode ler essas informações usando um aplicativo independente conhecido como navegador de SNMP. Você pode instalar o navegador de SNMP em qualquer máquina que o Rapid Recovery Core possa acessar pela rede.

Para certificar-se de que as notificações de eventos de SNMP do Core podem ser recebidas pelo navegador de SNMP, verifique se as opções de notificação de um grupo de notificação estão corretamente configuradas para notificar por interceptação SNMP.

NOTA: Você pode usar o grupo padrão ou criar um grupo de notificação personalizado. O processo é idêntico.

Abra o grupo de notificação, selecione a guia **Opções de notificação** e certifique-se de que a opção **Notificar por interceptação SNMP** está ativada. O grupo de notificação especifica a interceptação número 1 por padrão. Se necessário, você pode alterar o número da interceptação para garantir que ele coincide com a definição esperada pelo navegador de SNMP.

Para obter mais informações e detalhes específicos sobre como configurar as opções de notificação, consulte Configurar grupos de notificação.

Como alternativa, você pode baixar um arquivo MIB do Rapid Recovery Core. Um navegador de SNMP pode ler esse arquivo de forma mais acessível ao usuário que os dados recebidos diretamente do Core.

Esta seção inclui os seguintes tópicos:

- Definir as configurações do SNMP
- Download do arquivo MIB SNMP

Definir as configurações do SNMP

Use as definições de SNMP para controlar a comunicação entre o Core e o navegador de SNMP. Isso inclui a porta SNMP, a porta do receptor do trap e o nome do host do receptor do trap.

Use este procedimento para configurar as definições do SNMP no Core.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Definições) e execute um dos procedimentos a seguir:
- Na lista de definições do Core no lado esquerdo da página Definições, clique em **Configuração do SNMP**.
- Role a tela para baixo no lado direito da página Definições até ver o cabeçalho Configuração do SNMP.
  As definições de Configuração do SNMP são exibidas.

3 Modifique as definições do SNMP conforme descrito na tabela a seguir.

Tabela 21. Informações das definições de conexão do SNMP

Caixa de texto	Descrição
Porta de entrada	Insira um número de porta para a conexão do SNMP. **NOTA: A definição padrão é 8161.**
Porta do receptor do trap	Insira um número de porta para o receptor do trap. A definição padrão é 162.
Nome do host do receptor do trap	Insira um nome de host para a conexão do SNMP. **NOTA: O nome de host padrão é localhost.**

4 Para cada configuração, quando estiver satisfeito com as alterações, clique em  para salvar as alterações e sair do modo de edição, ou clique em  para sair do modo de edição sem salvar.

Download do arquivo MIB SNMP

O SNMP (Simple Network Management Protocol) é usado para monitorar dispositivos em uma rede a fim de detectar condições que exigem atenção. Quando o Rapid Recovery Core está definido como um agente SNMP, o Core relata informações como alertas, status de repositório e máquinas protegidas. Um host SNMP pode ler essas informações usando um aplicativo independente, conhecido como navegador de SNMP.

Os objetos de dados gerenciados por agentes SNMP são organizados em um arquivo Base de Informações de Gerenciamento (MIB) que contém Identificadores de Objeto (OIDs). Cada OID identifica uma variável que pode ser lida ou definida usando SNMP.

Você pode baixar um arquivo MIB do Rapid Recovery Core. Um navegador de SNMP pode ler esse arquivo, denominado dell-aa-core.mib, de forma mais acessível ao usuário que os dados recebidos diretamente do Core.

Use esse procedimento para baixar o arquivo MIB SNMP do Rapid Recovery Core.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Mais) e clique em **Downloads**.
A página **Downloads** aparece.

3 Role para baixo até o painel Outros arquivos.

4 Para baixar o arquivo MIB, clique no link de download do **Arquivo MIB SNMP**.

As definições de Configuração do SNMP são exibidas.

5 Na caixa de diálogo **Abrir dell-aa-core.mib**, realize um dos procedimentos a seguir:

- Para abrir o arquivo de log, selecione Abrir com, selecione um navegador de SNMP para visualizar o arquivo MIB baseado em texto e, por último, clique em **OK**.

  O arquivo dell-aa-core.mib é aberto no aplicativo selecionado.

- Para salvar o arquivo localmente, selecione **Salvar arquivo** e clique em **OK**.

  O arquivo dell-aa-core.mib é salvo na sua pasta Downloads. Ele pode ser aberto usando um navegador de SNMP ou um editor de texto.

Configuração das definições do vSphere

VMware vSphere é um conjunto de software de virtualização com o qual você pode gerenciar máquinas virtuais ESXi ou vCenter Server. Se você estiver usando vSphere, não é necessário carregar o software do agente Rapid Recovery em VMs individuais para protegê-las. Esse recurso é chamado de proteção sem agentes, que se aplica somente a máquinas virtuais.

Use este procedimento para configurar as definições do vSphere no Core.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Definições) e, em seguida, faça o seguinte:

- Na lista de definições do Core no lado esquerdo da página Definições, clique em **vSphere**.
- Role a tela para baixo no lado direito da página Definições até ver o cabeçalho vSphere.

  As definições do vSphere são exibidas.

3 Modifique as definições do vSphere conforme descrito na tabela a seguir.

Tabela 22. Informações das definições do vSphere Core

Elemento de UI	UI Type	Descrição
Duração da conexão	Caixa de número	Estabelece o tempo antes do qual ocorre um tempo limite da conexão com o ESXi Server. Usa o formato HH:MM:SS. **NOTA: A definição padrão é 00:10:00 ou dez minutos.**
Máximo de consolidações simultâneas	Campo de texto	Define o número máximo de consolidações simultâneas para máquinas virtuais protegidas. **NOTA: A definição padrão é 0.**
Máximo de novas tentativas	Campo de texto	Define o número máximo de tentativas de conexão com um disco virtual ou de operações de leitura e gravação antes do tempo limite. **NOTA: A definição padrão é 10.**
Permitir restauração paralela	Booleano (caixa de seleção)	Quando esta opção está marcada, ela permite a restauração paralela de uma máquina virtual sem agentes. Quando esta opção está desmarcada, a função está desabilitada. **NOTA: A definição padrão é Não (desmarcada).**

4 Para cada definição, quando estiver satisfeito com suas alterações, clique na marca de seleção para salvar a alteração e sair do modo de edição, ou clique em **X** para sair do modo de edição sem salvar.

Criar cópia de segurança e restaurar definições do Core

Você pode criar uma cópia de segurança em arquivo das informações de definição e, posteriormente, restaurar essas definições caso haja problemas com a máquina Core você queira migrar essas definições para uma máquina diferente. As informações incluídas na cópia de segurança incluem os metadados do repositório (como o nome do repositório, o caminho de dados e o caminho de metadados); as máquinas protegidas no Core; os relacionamentos de replicação (destinos e origens); quais máquinas estão configuradas para standby virtual; e informações sobre chaves de criptografia.

Esse processo restaura apenas as definições de configuração, não os dados. Informações de segurança (como credenciais de autenticação) não são armazenadas no arquivo de configuração. Salvar um arquivo de configuração de Core não acarreta riscos de segurança.

NOTA: Você deve primeiramente criar uma cópia de segurança das informações de definição do Core para poder usar esse processo para restaurar as definições.

Use este procedimento para criar uma cópia de segurança das definições do Core e restaurá-las.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Configurações).

A página **Configuration** (Configuração) aparece. Na parte superior do painel de Configurações, acima das categorias de definições, você verá dois botões, Definições da cópia de segurança e Definições de restauração.

3 Caso queira criar uma cópia de segurança das definições do Core, vá para a Etapa 4. Caso queira restaurar definições do Core, vá para a Etapa 6.

4 Para fazer uma cópia de segurança das definições atuais em um arquivo XML, na parte superior da página Definições, clique em **Definições da cópia de segurança**.

Aparece a caixa de diálogo Configuração da cópia de segurança do Core.

5 Na caixa de texto Caminho local, digite o caminho de um diretório acessível localmente à máquina Core no qual você deseja armazenar as definições do Core em um arquivo XML e clique em **Cópia de segurança**.

Por exemplo, digite `C:\Users\Your_User_Name\Documents\AA5CoreSettings` e clique em **Cópia de segurança**.

Um arquivo chamado AppRecoveryCoreConfigurationBackup.xml é salvo no destino local que você especificou.

6 Para restaurar as definições do Core a partir de um arquivo XML de cópia de segurança salvo anteriormente usando esse método, execute as etapas a seguir.

NOTA: Quando você restaura as definições de configuração do Core, o serviço Rapid Recovery Core é reiniciado.

a Na parte superior da página **Definições**, clique em **Restaurar**.

A caixa de diálogo **Configuração da restauração do núcleo** é mostrada.

b Na caixa de texto **Caminho local**, digite o caminho local onde você armazenou as definições de configuração do Core.

Por exemplo, digite `C:\Users\Your_User_Name\Documents\AA5CoreSettings`.

c Caso não queira restaurar as informações de repositório, vá para a Etapa g.

d Opcionalmente, caso queira restaurar as informações de repositório para a configuração do arquivo de cópia de segurança, selecione **Restaurar repositórios** e clique em **Restaurar**.

A caixa de diálogo **Restaurar repositórios** é exibida.

Se você optar por restaurar as informações de repositório a partir da cópia de segurança dos dados de configuração, os repositórios configurados quando as definições do Core foram salvas serão exibidos para confirmação. Por padrão, todos os repositórios existentes estão selecionados.

e Confirme as informações de repositório que você deseja restaurar. Se vários repositórios aparecerem nas listas para confirmação e você quiser restaurar as informações de apenas alguns deles, desmarque a seleção dos repositórios que não deseja restaurar.

f Quando você estiver satisfeito com a seleção de repositórios que deseja restaurar, clique em **Salvar**.

A caixa de diálogo **Restaurar repositórios** é fechada.

g Na caixa de diálogo **Restaurar repositórios**, clique em **Restaurar**.

A caixa de diálogo **Restaurar repositórios** é fechada e o processo de restauração é iniciado. Um alerta aparece, indicando que a configuração do serviço de repositório foi alterada.

h Caso não tenha sido possível restaurar alguma definição de configuração, uma mensagem de erro será exibida. Confira os detalhes do erro para ver se há alguma ação necessária da sua parte. Para obter informações, consulte Como exibir eventos usando tarefas, alertas e registros. Para continuar, clique em **Fechar** para limpar a caixa de diálogo de erro.

i Depois de restaurar a configuração, verifique o seguinte:

- Desbloqueie todas as chaves de criptografia. Para obter informações, consulte Desbloquear uma chave de criptografia.
- Se o standby virtual estiver configurado para atualizar continuamente uma VM para um destino de rede, você precisa especificar as credenciais da rede nas definições do standby virtual antes de uma sincronização bem-sucedida. Para obter informações, consulte Exportação de VM.
- Se o arquivamento programado estiver configurado para arquivar em uma conta de armazenamento na nuvem, você precisa especificar as credenciais para que o Core possa se conectar à conta de nuvem. Para obter mais informações sobre a conexão do Core com uma conta de armazenamento na nuvem, consulte Adicionar uma conta de nuvem.
- Se a replicação estiver configurada e você quiser restaurar para um Core de destino, confirme as definições do Core de destino (particularmente do host) no Core de origem. Para obter mais informações, se você estiver gerenciando seu próprio Core, consulte Replicação para um core de destino autogerenciado. Se estiver replicando para um núcleo gerenciado por terceiros, consulte Replicar para um Core de destino de terceiros.
- Se a verificação de capacidade de anexação do SQL estiver configurada e a instância do SQL Server estiver realizando as verificações na máquina do Core, especifique as credenciais do SQL nas definições de Capacidade de anexação. Para obter informações, consulte Gerenciamento das definições de Capacidade de anexação SQL do Core.

  Verifique se a configuração do mecanismo de reprodução foi restaurada e atualize as definições se elas não garantirem uma comunicação eficaz. Para obter informações, consulte Configurar as definições do mecanismo Replay.

Ferramentas do nível do Core

Além de configurar as definições do Core, você também pode usar as ferramentas do nível do Core descritas na tabela a seguir.

Tabela 23. Outras ferramentas do nível do Core

Elemento de UI	Descrição
Informações do sistema	O Rapid Recovery permite visualizar informações sobre o Rapid Recovery Core, incluindo informações do sistema, volumes locais e montados e conexões do mecanismo de reprodução. Para obter mais informações sobre as informações mostradas da página Informações do sistema, consulte Noções básicas sobre as informações do sistema do Core. Para obter mais informações sobre como visualizar as Informações do sistema, consulte Como visualizar informações do sistema do Core.
Download dos arquivos de log do Core	Informações sobre várias atividades do Rapid Recovery Core são salvas no arquivo de log do Core. Para diagnosticar possíveis problemas, você pode baixar e visualizar logs do Rapid Recovery Core. Para obter mais informações sobre como acessar e visualizar os logs do Core, consulte Acesso aos logs do Core. Cada máquina protegida também salva um log de atividade. Esse log pode ser carregado para o Core se você selecionar o trabalho noturno chamado Baixando os logs das máquinas protegidas. Para obter mais informações sobre trabalhos noturnos, consulte Compreender trabalhos noturnos. Para obter mais informações sobre como configurar as definições de trabalho noturno do Core, consulte Configurar trabalhos noturnos para o Core. Para obter mais informações sobre a configuração de trabalhos noturnos para máquinas protegidas específicas, consulte Como personalizar os trabalhos noturnos para uma máquina protegida.

Noções básicas sobre as informações do sistema do Core

O Rapid Recovery permite que você visualize informações sobre o Rapid Recovery Core. Você pode visualizar informações gerais, informações sobre volumes locais e informações sobre volumes montados.

No painel **Geral**, você pode ver as informações descritas na tabela a seguir.

Tabela 24. Informações do sistema

Elemento de UI	Descrição
Nome do host	O nome da máquina do Rapid Recovery Core.
Versão de OS	A versão do sistema operacional instalado no Rapid Recovery Core.
Arquitetura de OS	Relaciona a estrutura subjacente e o design da máquina que hospeda o Rapid Recovery Core. Pode incluir o chipset e listar um sistema de 64 bits. O Rapid Recovery Core dá suporte apenas a sistemas de 64 bits.
Memória (física)	Mostra a quantidade de memória de acesso aleatório (RAM) instalada na máquina Core.
Nome de exibição	Mostra o nome de exibição do Core, que pode é configurável (consulte Configurar definições gerais do Core).
Nome de domínio totalmente qualificado	Mostra o nome de domínio totalmente qualificado da máquina Core.
Local do cache de metadados	Mostra o caminho do local do cache de metadados. Para obter mais informações, consulte Noções básicas sobre o cache de deduplicação e locais de armazenamento.
Local do cache principal	Mostra o caminho do local do cache de deduplicação principal. Para obter mais informações, consulte Noções básicas sobre o cache de deduplicação e locais de armazenamento.
Local do cache secundário	Mostra o caminho do local do cache de deduplicação secundário. Para obter mais informações, consulte Noções básicas sobre o cache de deduplicação e locais de armazenamento.

O painel **Volumes** inclui as seguintes informações sobre volumes de armazenamento da máquina do Core: Nome, ID do dispositivo, sistema de arquivos, capacidade bruta, capacidade formatada, capacidade usada e pontos de montagem.

O painel **Conexões do mecanismo de reprodução** exibe informações detalhadas sobre os pontos de recuperação montados atualmente. Essas informações incluem ponto final local, ponto final remoto, ID de agente de imagem montada, ID da imagem montada e nome de exibição da imagem montada. Você pode ver se a montagem é gravável e visualizar o usuário autenticado, os bytes lidos e os bytes gravados.

Você pode desmontar pontos de recuperação montados localmente em um Core a partir da página Montagens. Para obter mais informações sobre desmontagem de pontos de recuperação, consulte Desmontar pontos de recuperação.

Para obter mais informações, consulte Como visualizar informações do sistema do Core.

Como visualizar informações do sistema do Core

As informações do sistema do Core incluem informações gerais, informações sobre volumes locais e informações sobre volumes montados do Core. Para obter uma descrição detalhada das informações disponíveis nessa página, consulte Noções básicas sobre as informações do sistema do Core.

Conclua as etapas nesse procedimento para exibir informações do sistema do Core.

NOTA: Você também pode ver informações do sistema de uma máquina protegida específica. Para obter mais informações, consulte Visualização das informações do sistema de uma máquina protegida.

1 Navegue para o Rapid Recovery Core Console.

2 Na barra de ícones, clique em (Mais) e clique em **Informações do sistema**.
A página Informações do sistema é exibida.

Acesso aos logs do Core

Informações sobre várias atividades do Rapid Recovery Core são salvas no arquivo de log do Core. Esse arquivo, AppRecovery.log, é armazenado por padrão no caminho C:\ProgramData\AppRecovery\logs.

NOTA: Dependendo de suas configurações, o diretório do AppRecovery pode não estar visível no Rapid Recovery Core. Para ver esse diretório, você pode precisar alterar as Opções de pasta no painel de controle para exibir arquivos, pastas e unidades ocultas. Se essas definições incluírem a opção de ocultar as extensões dos tipos de arquivo conhecidos, o arquivo de log do Core pode ser mostrado como AppRecovery sem extensão .log.

O log do Core inclui informações sobre trabalhos do Core concluídos, falhas de conexão, resultados de tentativas do Core em entrar em contato com o Portal de licenças e outras informações. Cada declaração armazenada no arquivo de log do Core é precedida por um de quatro qualificadores: INFO, DEBUG, ERROR e WARN. Esses qualificadores ajudam classificar a natureza das informações armazenadas no log ao diagnosticar um problema.

NOTA: Da mesma forma, um arquivo de log também é armazenado em cada máquina protegida que contém informações relacionadas às tentativas de comunicação com o Core. Para obter mais informações sobre logs de máquina, consulte Acessar o diagnóstico de máquinas protegidas.

A capacidade de acessar logs pode ser útil para solucionar um problema ou trabalhar com o Suporte do Rapid Recovery da Dell. Para acessar os logs, consulte os procedimentos a seguir:

- Como baixar e exibir o arquivo de log do Core
- Download e visualização do arquivo de log de uma máquina protegida

Como baixar e exibir o arquivo de log do Core

Caso encontre algum erro no Core, você pode baixar os logs de Core para exibi-los ou compartilhá-los com o representante do Suporte da Dell.

1 Na barra de ícones do Rapid Recovery Core Console, clique em (Mais) e, em seguida, clique em **Log do Core**.

2 Na página **Baixar log do Core**, clique em **Clique aqui para começar o download**.

3 Caso precise abrir ou salvar o arquivo`CoreAppRecovery.log`, clique em **Salvar**.

4 Caso você veja a caixa de diálogo **Abrindo CoreAppRecovery.log**, faça o seguinte:

- Para abrir o arquivo de log, selecione **Abrir com** e um aplicativo (como Bloco de Notas) para visualizar o arquivo de log com base em texto e, por fim, clique em **OK**.
  O arquivo CoreAppRecovery.log é aberto no aplicativo selecionado.
- Para salvar o arquivo localmente, selecione **Salvar arquivo** e clique em **OK**.
  O arquivo CoreAppRecovery.log é salvo na pasta **Downloads**. Ele pode ser aberto usando-se qualquer editor de texto.

Links relacionados

Como baixar e exibir o arquivo de log do Core
Download e visualização do arquivo de log de uma máquina protegida

Roteiro para configurar o Core

A configuração contém tarefas como criar e configurar o repositório para armazenar instantâneos do backup, definir chaves de criptografia para a segurança dos dados protegidos e configurar alertas e notificações. Depois de concluir a configuração do Core, você pode proteger os agentes e realizar a recuperação.

A configuração do Core envolve entender certos conceitos e realizar as seguintes operações iniciais:

- Criar um repositório
- Configurar as chaves de criptografia
- Configurar a notificação de eventos
- Configurar a política de retenção
- Configurar a capacidade de conexão do SQL

Repositórios

Essa seção descreve como trabalhar com repositórios. Ela debate o repositório do gerenciador do volume de deduplicação e descreve os recursos e os atributos. Ela descreve tipos de deduplicação usados no Rapid Recovery e como a deduplicação é usada em todo o aplicativo. Em seguida, essa seção descreve como gerenciar repositórios DVM, inclusive criando um repositório, exibindo e editando detalhes e excluindo um repositório. Você pode aprender a abrir um repositório de um Core em outro Core. Por fim, essa seção descreve como migrar pontos de recuperação manualmente de um repositório para outro.

Gerenciamento de um repositório de DVM

Antes de poder usar o Rapid Recovery, é preciso configurar um ou mais repositórios no server do Rapid Recovery Core. Um repositório armazena seus dados protegidos; mais especificamente, armazena os snapshots capturados de suas máquina protegidas em seu ambiente.

O gerenciamento de um repositório de DVM envolve as seguintes operações:

1 **Criação de um repositório de DVM**. Antes de criar um repositório, considere o tipo de tecnologia adequada.

Para obter mais informações sobre repositórios, consulte Como entender repositórios.

Para obter mais informações sobre como criar um repositório DVM, consulte Como criar um repositório DVM.

2 **Adicionando um novo local de armazenamento**. Para obter mais informações sobre a adição de um novo local de armazenamento em um repositório de DVM, consulte Adicionar um local de armazenamento a um repositório de DVM existente.

3 **Modificando as definições do repositório**. Para obter mais informações sobre como modificar as definições do repositório para um repositório, consulte Ver ou modificar detalhes de repositório

4 **Verificando um repositório**. Para obter mais informações sobre a verificação de repositório de DVM, consulte Verificar um repositório.

5 **Executar um trabalho de otimização do repositório**. Para obter mais informações sobre o trabalho de otimização do repositório, consulte Sobre o trabalho de otimização do repositório. Para as etapas de otimização de um repositório de DVM existente, consulte Otimização de um repositório de DVM.

6 **Excluindo um repositório**. Para obter mais informações sobre a exclusão de repositórios, consulte Excluir um repositório.

Como criar um repositório DVM

Este processo descreve como criar um repositório no seu Core usando a tecnologia de repositório de gerenciador de volume de deduplicação (DVM).

- Você precisa ter acesso administrativo à máquina na qual você deseja criar um repositório DVM.
- Esse tipo de repositório exige no mínimo 150 GB de espaço de armazenamento disponível no volume definido como o local de armazenamento.

- O local de armazenamento para um repositório DVM precisa estar em uma unidade local conectada ao servidor Core.
- O servidor Core pode ser um dispositivo série DL (incluindo o DL1000) ou pode ser qualquer servidor Windows baseado em software que atenda aos requisitos do sistema.

NOTA: [E recomendado criar o repositório através da guia Appliance (Dispositivo). Para obter mais informações, consulte a seção Armazenamento de provisionamento.

Conclua as etapas a seguir para criar um repositório DVM.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em (Mais), e, em seguida, selecione **Repositories (Repositórios)**.
A página **Repositories (Repositórios)**Repositórios é mostrada.

Na página **Repositories (Repositórios)**, o painel Repositórios DVM é mostrado.

3 No topo da página, clique em **Add New DVM Repository (Adicionar novo repositório DVM)**.
A caixa de diálogo **Add New Repository (Adicionar novo repositório)** é mostrada.

4 Digite as informações, conforme descrito na tabela a seguir.

Tabela 25. Configurações para adicionar novo repositório

Caixa de texto	Descrição
Nome do repositório	Insira o nome de exibição do repositório. Por padrão, essa caixa de texto é composta da palavra Repositório e um número, que corresponde ao número de repositórios deste Core. Por exemplo, se esse é o primeiro repositório, o nome padrão é Repositório 1. Altere o nome conforme necessário. Os nomes de repositório devem conter entre 1 e 40 caracteres alfanuméricos, incluindo espaços. Não use caracteres proibidos nem frases proibidas.
Operações simultâneas	Defina o número de solicitações simultâneas que você quer que o repositório suporte. Por padrão, o valor é 64.
Comentários	Opcionalmente, insira uma observação descritiva sobre esse repositório. É possível digitar até 254 caracteres. Por exemplo, digite **Repositório DMV 2**

5 Clique em **Add Storage Location (Adicionar local de armazenamento)** para definir o local de armazenamento específico ou volume para o repositório. Esse volume deve ser um local de armazenamento primário.

CUIDADO: Defina uma pasta exclusiva dentro do diretório raiz para o local de armazenamento de seu repositório. Não especifique o diretório raiz. Por exemplo, use E:\Repository\, não E:\. Se o repositório que você estiver criando nessa etapa for removido posteriormente, todos os arquivos no local de armazenamento de seu repositório serão apagados. Se você definir seu local de armazenamento no diretório raiz, todos os outros arquivos no volume (por exemplo, E:\) são apagados, o que pode resultar em uma perda catastrófica de dados

A caixa de diálogo **Add Storage Location (Adicionar local de armazenamento)** é mostrada.

6 Clique em **Add Storage Location (Adicionar local de armazenamento)** para definir o local de armazenamento específico ou volume para o repositório. Esse volume deve ser um local de armazenamento primário.

7 Na área **Storage Location (Local de armazenamento)**, especifique como adicionar o arquivo para o local de armazenamento. Você pode optar por adicionar um volume de armazenamento conectado localmente (como armazenamento conectado diretamente, uma rede de área de armazenamento ou armazenamento conectado de rede). Você também pode especificar um volume de armazenamento em um local compartilhado de sistema de arquivo de Internet comum (CIFS)

- Selecione **Add file on local disk (Adicionar arquivo em disco local)** para especificar uma máquina local e depois insira as informações conforme descrito na tabela a seguir.

Tabela 26. Configurações de disco local

Caixa de texto	Descrição
Caminho de dados	Digite o local para armazenar os dados protegidos. Por exemplo, digite `X:\Repository\Data`. Ao especificar o caminho, use somente caracteres alfanuméricos, o hífen e o ponto final (apenas para separar os nomes de host e domínios). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Caminho de metadados	Digite o local para armazenar os metadados protegidos. Por exemplo, digite `X:\Repository\Metadata`. Ao especificar o caminho, use somente caracteres alfanuméricos, o hífen e o ponto final (apenas para separar os nomes de host e domínios). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

- Ou selecione **Add file on CIFS share (Adicionar arquivo no compartilhamento CIFS)** para especificar um local de compartilhamento de rede e depois insira as informações conforme descrito na tabela a seguir.

Tabela 27. Credenciais de compartilhamento de CIFS

Caixa de texto	Descrição
Caminho UNC	Digite o caminho para o local de compartilhamento de rede. Se esse local estiver no diretório raiz, defina um nome de pasta exclusivo (por exemplo, `Repository`). O caminho deve começar com \\. Ao especificar o caminho, use somente caracteres alfanuméricos, o hífen e o ponto final (apenas para separar os nomes de host e domínios). As letras a a z não diferenciam maiúsculas de minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Nome de usuário	Especifique um nome de usuário para acessar o local de compartilhamento da rede.
Password (Senha)	Especifique uma senha para acessar o local de compartilhamento da rede.

8 Na área **Storage Configuration (Configuração de armazenamento)**, clique em **More Details (Mais detalhes)** e insira os detalhes para o local de armazenamento como descrito na tabela a seguir.

Tabela 28. Detalhes de configuração de armazenamento

Caixa de texto	Descrição
Tamanho	Defina o tamanho ou a capacidade do local de armazenamento. O tamanho mínimo é de 1 GB. O padrão é de 250 GB. Você pode escolher entre: • GB • TB **NOTA: O tamanho que você especificar não pode exceder o tamanho do volume.** Se o local de armazenamento for um volume New Technology File System (NTFS) usando o Windows XP ou Windows 7, o limite do tamanho do arquivo é 16 TB. Se o local de armazenamento for um volume NTFS usando o Windows 8, 8.1, Windows 10, Windows Server 2012 ou 2012 R2, o limite do tamanho do arquivo é de 256 TB. **NOTA: Para que o Rapid Recovery valide o sistema operacional, o Windows Management Instrumentation (WMI) precisa ser instalado no local de armazenamento pretendido.**
Política do cache de gravação	A política do cache de gravação controla o modo como o Windows Cache Manager é usado no repositório e ajuda a ajustar o repositório para obter o desempenho ideal em configurações diferentes.

Caixa de texto	Descrição
	Configure o valor como uma das seguintes opções: • Ligado • Apagado • Sincronizar Se ativada, que é a configuração padrão, o Windows controla o cache. Isso é adequado para o Windows 10 e para versões do Windows Server 2012 e mais recentes. **NOTA: Ativar a política de cache de gravação pode melhorar o desempenho. Se estiver usando o Windows Server 2008 SP2 ou Windows Server 2008 R2 SP2, recomenda-se a configuração desligado.** Se desativar a configuração, o Rapid Recovery controla o cache. Se configurado como Sync (Sincronizar), o Windows controla o cache e a entrada/saída síncrona.
Bytes por setor	Especifique o número de bytes que você quer que cada setor contenha. O valor padrão é 512.
Média de bytes por registro	Especifique o número médio de bytes por registro. O valor padrão é 8192.

9 Clique em **Salvar**.

A caixa de diálogo **Add Storage Location (Adicionar local de armazenamento)** se fecha e suas configurações são salvas. A caixa de diálogo **Add New Repository (Adicionar novo repositório)** mostra seu novo local de armazenamento.

10 Opcionalmente, repita as etapas 6 a 9 para acrescentar locais de armazenamento adicionais para o repositório.

11 Quando todos os locais de armazenamento que você deseja criar para o repositório no momento tiverem sido definidos, na caixa de diálogo **Add New Repository (Adicionar novo repositório)**, clique em **Create (Criar)**.

A caixa de diálogo **Add New Repository (Adicionar novo repositório)** se fecha e suas alterações são aplicadas. A página **Repositories (Repositórios)** é aberta, mostrando seu repositório recém-adicionado na tabela resumida de repositórios DVM.

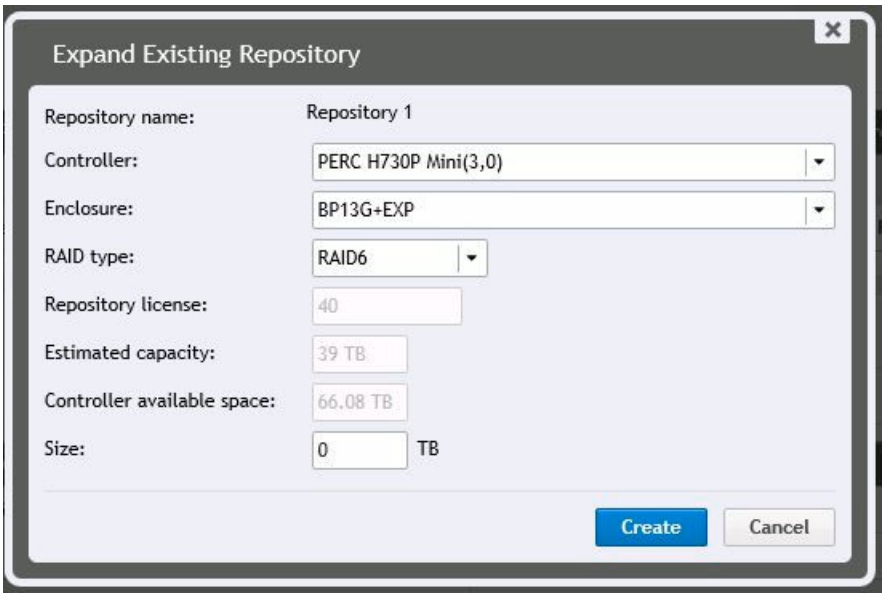
Ampliar o repositório

O recurso Expand Repository (Ampliar repositório) está disponível em todos os modelos DL (1300, 4300, 4000), exceto o DL 1000. O tipo de licença aplicado restringe o tamanho do repositório. Para ampliar o repositório usando armazenamento interno não utilizado e armazenamento no gabinete externo, atualize a licença. Para alterar a chave de licença, consulte a seção Atualização ou alteração de uma licença. Para ampliar o repositório existente:

1 Clique em **Appliance** > **Provisioning** (Dispositivo, Provisionamento).

2 Na seção **Repositories (Repositórios)**, clique em  → **Expand Existing Repository (Ampliar repositório existente)** ao lado do repositório que você quer expandir.

A caixa de diálogo **Expand Existing Repository (Ampliar repositório existente)** é mostrada.



3 Na caixa **Expand Existing Repository (Ampliar repositório existente)**, especifique as seguintes informações:

Tabela 29. Expandir o repositório existente

Caixa de texto	Descrição
Nome do repositório	O nome do repositório que deve ser ampliado.
Controlador	Selecione o controlador de armazenamento adequado dependendo se você está criando um repositório em armazenamento interno ou gabinete de armazenamento conectado diretamente.
Gabinete	Selecione o gabinete de armazenamento adequado.
RAID Type (Tipo de CPU)	Selecione a configuração de RAID adequada. Você tem as seguintes opções para configurações de RAID: 1, 5 ou 6.
Licença de repositório	A licença de repositório é mostrada.
Estimativa de capacidade	Mostra a capacidade estimada disponível para criar um repositório.
Espaço disponível para controlador	Mostra o espaço disponível para controlador.
Tamanho	Insira o tamanho do repositório que deve ser criado.

4 Clique em **Criar**.
Um novo local de armazenamento é adicionado ao repositório existente.

O repositório é ampliado para o tamanho especificado.

Ver ou modificar detalhes de repositório

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em (Mais), e, em seguida, selecione **Repositories (Repositórios)**.
A página **Repositories (Repositórios)**Repositórios é mostrada.

O painel **DVM Repositories (Repositórios DVM)** é mostrado.

3 No menu da página **Repositories (Repositórios)**, você pode executar as seguintes ações gerais:

Opção	Descrição
Adicionar novo repositório DVM	Adicionar um novo repositório DVM.
Abrir repositório DVM existente	Abra um repositório DVM existente por outro Core, o que muda a propriedade do repositório para este Core. Para obter mais informações, consulte Abrir um repositório de DVM existente.
Atualizar	Ver ou atualizar a lista de repositórios.

4 No painel **DVM Repositories (Repositórios DVM)**, no menu suspenso (Ações) para qualquer repositório DVM, você pode executar as seguintes ações adicionais:

Opção	Descrição
Adicionar local de armazenamento	Estender o repositório existente adicionando um local de armazenamento **NOTA: Ao estender um volume de repositório DVM, primeiro pause a proteção. Em seguida, estenda o volume e, por fim, retome a proteção. Essa ação impede que um raro erro que possa ocorrer apenas ao estender um volume simultâneo com uma fase de transferência específica.**
Verificar	Executar uma verificação de repositório
Configurações	Exibir ou modificar configurações de repositório. Essas configurações incluem: • Ver o nome do repositório • Ver ou alterar o máximo de operações simultâneas • Ver ou alterar uma descrição para o repositório • Ativar ou desativar a deduplicação • Ativar ou desativar a compressão dos dados armazenados no repositório
Executar trabalho de otimização	Executar um trabalho de otimização no repositório
Apagar	Apagar um repositório

NOTA: Ao estender um volume de repositório DVM, primeiro pause a proteção. Em seguida, estenda o volume e, por fim, retome a proteção. Essa ação impede que um raro erro que possa ocorrer ao estender em uma fase de transferência específica.

Você pode executar as seguintes ações gerais na página Repositories (Repositórios):

- Ver ou atualizar a lista de repositórios
- Adicionar um novo repositório
- Abrir um repositório existente por outro Core, o que muda a propriedade para este repositório

Adicionar um local de armazenamento a um repositório de DVM existente

NOTA: É recomendado expandir a repositório por meio da guia Dispositivo. Para obter mais informações, consulte Ampliar o repositório

Adicionar um local de armazenamento a um repositório de DVM permite definir onde você deseja que o repositório ou o volume seja armazenado.

Execute as etapas do procedimento a seguir para especificar o local de armazenamento do repositório ou do volume.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em (Mais) e, em seguida, selecione **Repositórios**.
A página Repositórios é exibida.

A página Repositórios de DVM é exibida.

3 Na tabela de resumo de repositórios, a partir da linha que representa o repositório de DVM ao qual você deseja adicionar um local de armazenamento, clique em **Configurações** e selecione **Adicionar local de armazenamento**.

A caixa de diálogo **Adicionar local de armazenamento** é exibida.

4 Especifique a forma de adicionar o arquivo ao local de armazenamento. Você pode selecionar adicionar o arquivo no disco local ou no compartilhamento de CIFS.

- Selecione **Adicionar arquivo no disco local** para especificar uma máquina local e, depois, insira as informações conforme descrito na tabela a seguir.

Tabela 30. Definições de disco local

Caixa de texto	Descrição
Caminho de dados	Insira o local para armazenar os dados protegidos. Por exemplo, digite `X:\Repository\Data`. As mesmas limitações do caminho se aplicam; use somente caracteres alfanuméricos, hífen ou ponto, sem espaços ou caracteres especiais.
Caminho de metadados	Insira o local para armazenar os metadados protegidos. Por exemplo, digite `X:\Repository\Metadata`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

- Ou selecione **Adicionar arquivo no compartilhamento de CIFS** para especificar um local de compartilhamento de rede e, depois, insira as informações conforme descrito na tabela a seguir.

Tabela 31. Credenciais de compartilhamento de CIFS

Caixa de texto	Descrição
Caminho de UNC	Insira o caminho para o local de compartilhamento de rede. Se esse local estiver na raiz, defina um nome de pasta dedicada (por exemplo, `Repository`). O caminho precisa começar com \\. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Nome de usuário	Especifique um nome de usuário para acessar o local de compartilhamento de rede.
Senha	Especifique a senha para acessar o local de compartilhamento de rede.

5 No painel Configuração de armazenamento, clique em **Mais detalhes** e insira os detalhes do local de armazenamento, como descrito na tabela a seguir.

Tabela 32. Detalhes do local de armazenamento

Caixa de texto	Descrição
Tamanho	Defina o tamanho ou capacidade do local de armazenamento. O tamanho padrão é de 250 GB. Você pode selecionar dentre os seguintes: • GB • TB **NOTA: O tamanho mínimo é 1 GB. O tamanho que você especificar não pode exceder o tamanho do volume.** Se o local de armazenamento for um volume NTFS (Sistema de arquivos de nova tecnologia) usando o Windows XP ou Windows 7, o limite de tamanho do arquivo é 16 TB. Se o local de armazenamento for um volume NTFS usando o Windows 8, Windows 8.1 ou Windows Server 2012, 2012 R2, o limite de tamanho do arquivo é 256 TB.

Caixa de texto	Descrição
	NOTA: Para que o Rapid Recovery valide o sistema operacional, a Instrumentação de gerenciamento do Microsoft Windows (WMI) deve estar instalada no local de armazenamento pretendido.
Política de cache de gravação	A política de cache de gravação controla como o Gerenciador de cache do Windows é usado no repositório e ajuda a ajustar o repositório para que o melhor desempenho seja obtido com diferentes configurações. Defina o valor para um dos seguintes: • Ligado • Desligado • Sincronizar Se definido como Ligado, que é o padrão, o Windows controla o armazenamento em cache. Isso é apropriado para o Windows 10 e para versões do Windows Server 2012 e posterior. **NOTA: Definir a política de cache de gravação como Ligado pode resultar em desempenho mais rápido. Se você estiver utilizando o Windows Server 2008 SP2 ou Windows Server 2008 R2 SP2, a recomendação de configuração será Desligado.** Se configurado para Desligado o, Rapid Recovery controlará o cache. Se definido como Sincronizar, o Windows controla o armazenamento em cache, além da entrada/saída síncrona.
Bytes por setor	Especifique o número de bytes que você deseja incluir em cada setor. O valor padrão é 512.
Média de bytes por registro	Especifique a média de bytes por registro. O valor padrão é 8192.

6 Opcionalmente, se desejar executar o trabalho de otimização do repositório para o repositório selecionado, selecione **Executar trabalho de otimização do repositório para [Nome do repositório]**.

A Dell recomenda a execução do Trabalho de otimização do repositório ao adicionar locais de armazenamento a um repositório existente. Esse trabalho otimiza o espaço livre ao aplicar a deduplicação dos dados armazenados no repositório.

Com base em fatores como tamanho do repositório, quantidade de dados no repositório, largura da banda de rede disponível e carga local na entrada e na saída do sistema, a execução de um Trabalho de otimização do repositório poderá demorar e utilizar grande quantidade da largura da banda de seu ambiente.

Para obter mais informações sobre o trabalho de otimização do repositório, consulte Sobre o trabalho de otimização do repositório.

7 Clique em **Salvar**.

A caixa de diálogo é fechada e o local de armazenamento, salvo. Na tabela de resumo de repositórios, o local de armazenamento criado será visível ao expandir os detalhes do repositório.

Sobre como verificar a integridade dos repositórios DVM

No Rapid Recovery Core, os usuários podem definir diferentes políticas de retenção entre cores de origem e destino. Para que a replicação funcione adequadamente com diferentes políticas de retenção, o core de destino precisa ter a mesma versão do software (ou mais recente) do que o core de origem.

NOTA: Os cores precisam compartilhar os mesmos três dígitos para o número de versão (por exemplo, ambos começando com 6.0.1.xxxx ou 5.4.3.xxxx). O número de versão (representado por xxxx) pode ser diferente apenas se o core de destino for mais recente.

Os administradores podem agora configurar a implementação em um core de destino em uma taxa diferente no core de origem. Da mesma forma, você pode agora definir uma política de retenção personalizada para qualquer máquina replicada. Por exemplo, é possível implementar pontos de recuperação no core de destino em uma taxa mais rápida e com menor granularidade do que o core de origem, economizando espaço. Ou é possível ainda implementar pontos de recuperação para qualquer máquina replicada selecionada em uma taxa

inferior no core de destino, mantendo maior granularidade, o que pode ser útil para fins de conformidade. Para obter mais informações sobre como usar uma política de retenção que se difere do padrão no core, consulte Como personalizar as configurações de uma política de retenção para uma máquina protegida.

Se o core tiver sido atualizado a qualquer ponto do AppAssure 5.3.x e você tiver utilizado a replicação, é necessário executar esse trabalho antes que possa configurar diferentes políticas de retenção entre cores de origem e de destino, ou configurar uma política de retenção personalizada em uma máquina replicada.

Você não vai conseguir ver ou executar esse trabalho se não possuir um ou mais repositórios que se qualifiquem para tal (criados antes da versão 5.4.x e ainda não realizados).

Executar esse trabalho verifica a integridade de todos os dados armazenados no repositório especificado, garantindo que você possa recuperar dados de cada instantâneo ou imagem de base. Se a verificação de integridade detectar qualquer problema com os dados em seu repositório, o trabalho é encerrado imediatamente. Os detalhes do evento para esse trabalho no core solicitam que você entre em contato com o suporte Dell para que possa agendar um horário para trabalhar com um representante de suporte e realizar procedimentos adicionais a fim de identificar e solucionar inconsistências de dados.

CUIDADO: A execução desse trabalho deve levar um período prolongado de tempo. A quantidade de tempo se difere com base na quantidade e no tipo de dados em seu repositório e no sistema de armazenamento subjacente. Enquanto o trabalho é executado, nenhuma outra transação pode ser realizada no repositório, incluindo transferências (instantâneo e backups de imagem de base, além de replicação), trabalhos noturnos e assim por diante.

Você pode realizar outras operações nos outros repositórios enquanto esse trabalho é executado.

NOTA: Esse trabalho verifica a integridade de todos os conteúdos dentro de um repositório. Para obter informações sobre o trabalho de `Integrity Check`, que você pode usar para garantir que um repositório possa ser montado e usado, consulte Verificar um repositório.

Verificar um repositório

O Rapid Recovery permite realizar uma verificação de diagnóstico de um volume de repositório de DVM quando um erro ocorre. Os erros no Core podem resultar de desligamento incorreto, falha de hardware ou outros fatores ambientais de pilha de IP inferior que podem ser expostos na funcionalidade do Rapid Recovery.

NOTA: Este procedimento deve ser executado somente para fins de diagnóstico. Por exemplo, execute essa verificação no caso de falha de hardware, desligamento inapropriado do Core ou falha de importação de um repositório.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em (Mais) e selecione **Repositórios**.
A página **Repositórios** é exibida.

A página Repositórios de DVM é exibida.

3 Para verificar um repositório de DVM, no painel **Repositório de DVM**, em qualquer linha da tabela de resumo representando um repositório de DVM, clique em e selecione **Verificar**.
A caixa de diálogo **Check Repository** (Verificar repositório) é mostrada.

4 Na caixa de diálogo **Verificar repositório**, confirme que você entendeu que todas as tarefas ativas associadas a esse repositório serão canceladas e que você deseja prosseguir.
Os trabalhos ativos são cancelados e o Trabalho de verificar o repositório é iniciado.

5 Opcionalmente, você pode monitorar o status do trabalho clicando no menu suspenso **Tarefas em execução** na barra de botões e selecionando Mantendo trabalho do repositório.

Sobre o trabalho de otimização do repositório

Durante o uso de um repositório de DVM, os dados capturados em cada snapshot são deduplicados. Essa deduplicação ocorre de maneira incremental, desde que os snapshots sejam salvos no repositório. Uma ocorrência de cada string de informações é salva no repositório. Quando uma string de informações é duplicada, uma referência para a string original no cache de deduplicação é usada, economizando espaço de armazenamento no repositório.

Caso o cache de deduplicação DVM esteja cheio, somente dados de snapshot já referenciados no cache são deduplicados. À medida que ocorre deduplicação, o cache continua sendo atualizado com valores exclusivos, substituindo os valores mais antigos no cache. Isso resulta em uma deduplicação inferior à ideal.

Para obter mais informações sobre deduplicação, consulte Noções básicas sobre o cache de deduplicação e locais de armazenamento.

Você pode escolher aumentar o cache de deduplicação DVM antes que ele esteja cheio, o que garante a deduplicação ideal continuada dos dados nesse repositório. Para obter mais informações, consulte Configuração das definições de cache de deduplicação DVM.

Você também pode aumentar o cache de deduplicação depois de estar cheio. Caso queira recuperar espaço no repositório depois de aumentar o cache, você pode otimizar o repositório. Essa ação força uma comparação dos dados nos snapshots com as informações no cache de deduplicação. Caso alguma string repetida seja encontrada no repositório, esses dados são substituídos por referências aos dados, o que economiza espaço de armazenamento no repositório. Às vezes, isso é conhecido como deduplicação off-line, pois esse processo de deduplicação ocorre mediante a solicitação, e não de maneira incremental à medida que os dados do snapshot são transferidos.

O processo de otimização utiliza muito o processador. O tempo necessário para executar esse trabalho depende de vários fatores. Entre esses fatores estão o tamanho do repositório, a quantidade de dados no repositório, a largura da banda da rede disponível e a carga existente na entrada e na saída do sistema. Quanto mais dados houver no repositório, por mais tempo esse trabalho será executado.

As ações a seguir são substituídas ou canceladas quando o trabalho de otimização do repositório ocorre.

- Trabalho de excluir pontos de recuperação
- Trabalho de manter o repositório
- Trabalho de verificar a integridade do repositório

As ações a seguir são substituídas ou canceladas quando o trabalho de otimização ocorre.

- Trabalho de excluir todos os pontos de recuperação
- Trabalho de cadeia excluir pontos de recuperação
- Trabalho de manter o repositório
- Base do trabalho de excluir pontos de recuperação
- Trabalho de verificar a integridade do repositório

Para etapas sobre como otimizar um repositório de DVM existente, consulte Otimização de um repositório de DVM.

Você pode interromper o trabalho de otimização do repositório durante um período limitado, caso necessário. Para obter mais informações, consulte Interromper ou retomar o trabalho de otimização do repositório.

Otimização de um repositório de DVM

Você precisa ter um repositório de DVM no seu Core para executar este procedimento.

Você pode executar a deduplicação offline de dados salvos em um repositório de DVM existente. Isso é realizado com a abertura do Trabalho de otimização do repositório.

NOTA: A Dell recomenda executar o trabalho de otimização de repositório apenas depois de ter aumentado o tamanho do cache de deduplicação. Essa ação permite que você recupere o espaço do repositório e use mais efetivamente o cache de deduplicação do DVM.

Execute as etapas deste procedimento para otimizar um repositório de DVM.

1 Navegue até o Console do Rapid Recovery Core.

2 Na barra de ícones, clique em (Mais) e, em seguida, selecione **Repositórios**.
A página **Repositórios** será exibida.

3 No painel Repositórios de DVM, na linha que representa o repositório que você deseja otimizar, clique em e, em seguida, selecione **Executar trabalho de otimização**.
Um prompt de aviso é exibido pedindo que você confirme a otimização.

4 Clique para confirmar a otimização.
O trabalho de otimização tem precedência sobre a maioria dos outros trabalhos. Se necessário, você pode interromper um trabalho otimização em andamento. Para obter mais informações sobre a interrupção ou a retomada este trabalho, consulte Interromper ou retomar o trabalho de otimização do repositório.

Interromper ou retomar o trabalho de otimização do repositório

Ao iniciar o Trabalho de otimização do repositório, o repositório de DVM selecionado é deduplicado. Essa otimização de deduplicação é um trabalho que exige muito do processador e tem a finalidade de economizar espaço no repositório. Para obter mais informações, consulte Sobre o trabalho de otimização do repositório.

Assim que esse trabalho for iniciado, você poderá interromper o trabalho utilizando o seguinte procedimento. Isso pausa a deduplicação. Se você já tiver interrompido uma otimização, você poderá retomar o processo utilizando esse procedimento.

NOTA: Esse procedimento é aplicável somente a repositórios de DVM e somente quando o trabalho de otimização do repositório tiver sido iniciado.

Complete as etapas desse procedimento para interromper ou retomar um trabalho de otimização do repositório.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em (Mais) e selecione **Repositórios**.
A página **Repositórios** é exibida.

A página Repositórios de DVM é exibida.

3 Se desejar interromper um trabalho de otimização, faça o seguinte:

a Na tabela de resumo de repositórios, na linha representando o repositório apropriado, clique em e selecione **Interromper trabalho de otimização**.
Um prompt de aviso aparece, solicitando a confirmação da interrupção.

b Clique para confirmar a otimização.

4 Se desejar retomar um trabalho de otimização interrompido, faça o seguinte:

a Na tabela de resumo de repositórios, na linha representando o repositório apropriado, clique em e selecione **Continuar trabalho de otimização**.
Um prompt de aviso aparece, solicitando a confirmação da interrupção.

b Na caixa de diálogo, selecione a opção **Continuar o trabalho a partir do ponto da interrupção,** e clique em **Sim**.

A caixa de diálogo é fechada, e o trabalho de otimização do repositório é retomado a partir do ponto em que ele foi interrompido pela última vez.

Abrir um repositório de DVM existente

Como a tecnologia de repositório principal do Rapid Recovery, o repositório de DVM contém dados de instantâneo (em forma de pontos de recuperação) das máquinas protegidas em um Rapid Recovery Core específico. Você pode abrir um repositório existente de um Core (por exemplo, Core A) em um segundo Core (Core B).

NOTA: Abrir um repositório de outro Core muda a propriedade do repositório. Quando você abrir um repositório existente, a informação fica acessível somente para o segundo Core.

No caso de um repositório DVM, o Core original (Core A) não pode estar em uso. Por exemplo, a máquina deve estar desligada, estar inacessível a uma rede ou os serviços do Core devem ser interrompidos.

O repositório pode estar em um local de rede compartilhado ou em um dispositivo de armazenamento acessível para o segundo Core.

Execute o procedimento a seguir para abrir um repositório existente.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em (Mais) e, em seguida, selecione **Repositórios**.
A página **Repositórios** é exibida.

O painel Repositórios de DVM também é exibido.

3 Para abrir um repositório DVM existente, na parte superior da página, clique em **Abrir repositório DVM existente**.
A caixa de diálogo **Abrir o repositório DVM existente** é exibida.

4 Na caixa de diálogo **Abrir o repositório DVM existente**, digite as seguintes informações sobre o repositório que deseja abrir e clique em **Abrir**.

Tabela 33. Opções para abrir o repositório DVM existente

Caixa de texto	Descrição
Caminho	O caminho do repositório (por exemplo, **D:\work\machine** para um caminho local ou **\\10.10.99.155\repositories** para endereço IP ou \\servername\sharename para um caminho de rede).
Nome de usuário	Se o repositório tiver um caminho de rede, insira o nome de usuário para efetuar login no compartilhamento de rede.
Senha	Se o repositório tiver um caminho de rede, insira a senha para efetuar login no compartilhamento de rede.

A caixa de diálogo é fechada e o repositório selecionado é adicionado ao seu Core atual.

Excluir um repositório

Execute as etapas deste procedimento para excluir um repositório.

1 Navegue para o Rapid Recovery Core Console.

2 Na barra de ícones, clique em (Mais) e selecione **Repositórios**.
A página **Repositórios** é exibida.

Na página **Repositórios**, o painel Repositórios DVM é exibido.

3 Na tabela de resumo dos repositórios, na linha que representa o repositório que você deseja excluir, clique em para expandir o menu suspenso e selecione **Excluir**.
Aparece uma mensagem de aviso pedindo para confirmar a exclusão.

4 Clique em **Sim** para confirmar a exclusão do repositório.

CUIDADO: Quando um repositório é excluído, os dados contidos nele são descartados e não podem ser recuperados.

Executar o trabalho de verificar o repositório em um repositório de DVM

Execute este procedimento para verificar a integridade um repositório DVM completo. Ele é recomendado para cores de destino replicados durante a atualização do AppAssure 5.3.x para a versão 5.4. Durante a execução da verificação de integridade, que pode ser prolongada, nenhuma outra ação pode ser executada no repositório.

Se você tiver vários repositórios de DVM para um Core de destino, execute este processo uma vez para cada repositório.

NOTA: Se você tiver outro repositório DVM no Core de destino para o qual o trabalho de verificação de integridade já foi concluído ou se criou um novo repositório adicional para este core de destino, você poderá executar operações em um repositório secundário enquanto o trabalho de integridade está sendo executado no repositório DVM que você especificou.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em (Mais), e selecione **Repositórios**.
A página **Repositórios** é exibida.

O painel Repositórios de DVM é exibido.

3 Na tabela resumo de repositórios, na fileira que representa o repositório que você deseja verificar, clique em e no menu suspenso, selecione **Trabalho de verificar o repositório**.
É exibida uma mensagem de confirmação.

CUIDADO: Antes de confirmar que deseja realizar o trabalho, você deve pensar bem sobre o tempo de duração necessário. Enquanto o trabalho está em execução, nenhuma outra transação pode ser executada naquele repositório, incluindo transferências (cópias de segurança do Snapshot e da imagem de base, e replicação), trabalhos noturnos e assim por diante.

4 Na caixa de diálogo **Trabalho de verificar o repositório**, para executar a verificação de integridade, clique em **Sim**.
A caixa de diálogo é fechada. Todos os trabalhos enfileirados em andamento são cancelados e começa o trabalho de verificação da integridade.

5 Para monitorar o andamento do trabalho de verificar o repositório de um repositório, incluindo a determinação das etapas adicionais necessárias depois da verificação, na barra de ícones, clique na guia (Eventos).

6 Na página **Eventos**, clique em **Detalhes do trabalho** para o trabalho para visualizar mais informações sobre o status do trabalho.
- Se você vir um erro em alguma tarefas subordinada, observe o erro e forneça as informações para o representante do suporte técnico da Dell.
- Se o trabalho de verificar o repositório concluir todas as tarefas subordinadas com sucesso, você poderá estabelecer uma política de retenção personalizada para este repositório.

Gerenciar a segurança

O Core pode criptografar dados do instantâneo da máquina protegida dentro do repositório. Em vez de criptografar todo o repositório, você pode especificar uma chave de criptografia durante a proteção de uma máquina, em um repositório que permite que as chaves sejam reutilizadas para diferentes máquinas protegidas. A criptografia não afeta o desempenho, uma vez que cada chave de criptografia ativa cria um domínio de criptografia, permitindo assim que um único núcleo suporte múltiplos locatários, hospedando múltiplos domínios de criptografia. Em um ambiente de múltiplos locatários, os dados são particionados e desduplicados dentro dos domínios de criptografia. Como você gerencia as chaves de criptografia, a perda do volume não pode vazar as chaves. As considerações e conceitos referentes à segurança da chave são:

- A criptografia é realizada usando o AES de 256 bits no modo Encadeamento de Blocos de Cifras (CBC), em conformidade com o SHA-3.
- A desduplicação opera dentro de um domínio de criptografia para garantir a privacidade.

- A criptografia é realizada sem afetar o desempenho.
- Você pode adicionar, remover, importar, exportar, modificar e apagar as chaves de criptografia que estão configuradas no Core.
- Não há limite para o número de chaves de criptografia que você pode criar no Core.

Aplicar ou remover criptografia de uma máquina protegida

Você pode proteger os dados protegidos no seu Core a qualquer momento definindo uma chave de criptografia e aplicando-a a uma ou mais máquinas protegidas no seu repositório. Você pode aplicar uma única chave de criptografia a qualquer número de máquinas protegidas, mas uma máquina protegida só pode usar uma única chave de criptografia a qualquer momento.

O escopo da deduplicação no Rapid Recovery é limitado às máquinas protegidas que usam o mesmo repositório e a mesma chave de criptografia. Por isso, para maximizar o valor da deduplicação, a Dell recomenda aplicar uma única chave de criptografia a tantas máquinas protegidas quanto seja viável. No entanto, não há limite para o número de chaves de criptografia que podem ser criadas no Core. Portanto, se a conformidade legal, as regras de segurança, as políticas de privacidade ou outras circunstâncias o exigirem, você pode adicionar e gerenciar qualquer número de chaves de criptografia. Nesse caso, você pode aplicar cada chave a apenas uma máquina protegida ou a qualquer conjunto de máquinas no seu repositório.

Quando você aplica uma chave de criptografia a uma máquina protegida ou separa uma chave de criptografia de uma máquina protegida, o Rapid Recovery cria uma nova imagem de base para aquela máquina no próximo snapshot programado ou forçado. Os dados armazenados nessa imagem de base (e em todos os snapshots incrementais subsequentes criados enquanto a chave de criptografia está aplicada) são protegidos por um padrão de criptografia avançado de 256 bits. Não existem métodos conhecidos para violar esse método de criptografia.

Se você alterar o nome ou a frase de acesso para uma chave de criptografia existente atualmente utilizada para uma máquina protegida, no próximo snapshot programado ou forçado, o Rapid Recovery Core captura e reflete as propriedades atualizadas da chave. Os dados armazenados nessa imagem (e em todos os snapshots incrementais subsequentes criados enquanto a chave de criptografia está aplicada) são protegidos por um padrão de criptografia avançado de 256 bits. Não existem métodos conhecidos para violar esse método de criptografia.

Depois que uma chave de criptografia é criada e aplicada a uma máquina protegida, há dois conceitos envolvidos na remoção dessa criptografia. O primeiro é desassociar a chave da máquina protegida. Opcionalmente, depois que a chave de criptografia é desassociada de todas as máquinas protegidas, é possível excluí-la do Rapid Recovery Core.

Esta seção inclui os seguintes tópicos:

- Associar uma chave de criptografia a uma máquina protegida
- Aplicar uma chave de criptografia a partir da página Máquinas protegidas
- Desassociar uma chave de criptografia de uma máquina protegida

Associar uma chave de criptografia a uma máquina protegida

Você pode aplicar uma chave de criptografia a uma máquina protegida usando um de dois métodos:

- **Como parte da proteção de uma máquina.** Usando esse método, você pode aplicar criptografia a uma ou a várias máquinas simultaneamente. Esse método permite adicionar uma nova chave de criptografia ou aplicar uma chave existente à máquina ou máquinas selecionadas.

  Para usar criptografia ao definir inicialmente a proteção de uma máquina, você deve selecionar as opções avançadas no assistente de proteção de máquinas relevante. Essa seleção adiciona uma página Criptografia ao fluxo de trabalho do assistente. Nessa página, selecione **Ativar criptografia** e depois selecione uma chave de criptografia existente ou especifique parâmetros para uma nova chave. Para obter mais informações, consulte Proteger uma máquina ou Sobre como proteger diversas máquinas, respectivamente.
- **Modificando as definições de configuração de uma máquina.** Esse método aplica uma chave de criptografia a uma máquina protegida por vez. Há duas abordagens para modificar as definições de configuração de uma máquina na UI do Rapid Recovery:
  - Modificar os parâmetros de configuração de uma máquina protegida específica. A chave de criptografia que você quer usar para essa abordagem já precisa existir no Rapid Recovery Core, ser um tipo de chave universal e precisa estar no estado desbloqueado. A criptografia é parte das Definições gerais. Para obter mais informações, consulte Visualização e modificação das definições de máquina protegida.

- Clique no ícone **Não criptografado** na página Máquinas protegidas. Usando esta abordagem, você pode criar e aplicar uma nova chave de criptografia ou atribuir uma chave universal desbloqueada existente à máquina protegida especificada. Para obter mais informações, consulte Aplicar uma chave de criptografia a partir da página Máquinas protegidas.

Aplicar uma chave de criptografia a partir da página Máquinas protegidas

Assim que uma chave de criptografia for adicionada a um Rapid Recovery Core, ela poderá ser utilizada para qualquer número de máquinas protegidas.

Se você selecionar uma chave de criptografia durante a proteção inicial de uma ou mais máquinas, a chave será automaticamente aplicada às máquinas que você proteger usando esse assistente. Nesses casos, este procedimento não é necessário.

Execute esse procedimento:

- Se desejar aplicar uma chave de criptografia desbloqueada universal existente a qualquer máquina protegida em seu Core.
- Se tiver acabado de adicionar uma nova chave de criptografia utilizando o processo descrito no tópico Adicionar uma chave de criptografia e desejar aplicar essa chave a uma máquina protegida.
- Se a criptografia já tiver sido aplicada a uma máquina protegida em seu Core, mas você desejar alterar a chave para uma chave desbloqueada universal diferente disponível em seu Core.

CUIDADO: Depois de aplicar uma chave de criptografia a uma máquina protegida, o Rapid Recovery obtém uma nova imagem de base para essa máquina no próximo snapshot programado ou forçado.

1 Navegue até o Rapid Recovery Core e clique em **Máquinas protegidas**.

A página **Máquinas protegidas** é exibida, listando todas as máquinas protegidas por esse Core. Um cadeado aberto aparece para as máquinas que não têm uma chave de criptografia aplicada. Um cadeado fechado indica que a máquina protegida está com a criptografia aplicada.

2 No painel Máquinas protegidas, clique no ícone de cadeado da máquina protegida que deseja configurar.

A caixa de diálogo **Configuração de criptografia** é exibida.

3 Realize um dos procedimentos a seguir:

- Se desejar aplicar uma chave de criptografia existente a essa máquina, selecione **Criptografar dados utilizando criptografia com base no Core com uma chave existente** e selecione a chave apropriada no menu suspenso. Clique em **OK** para confirmar.
- Se desejar alterar uma chave de criptografia existente para uma chave desbloqueada universal diferente, selecione **Criptografar dados utilizando criptografia com base no Core com uma nova chave** e selecione a chave apropriada no menu suspenso. Clique em **OK** para confirmar.
- Se deseja criar uma nova chave de criptografia e aplicá-la a essa máquina protegida, selecione **Criptografar dados utilizando criptografia com base no Core com uma nova chave**. Em seguida, insira os detalhes da chave, como descrito na tabela a seguir.

Tabela 34. Detalhes de nova chave de criptografia

Caixa de texto	Descrição
Nome	Insira um nome para a chave de criptografia. Os nomes de chaves de criptografia devem ter entre 1 e 64 caracteres alfanuméricos. Não utilize caracteres proibidos nem frases proibidas.
Descrição	Insira um comentário descritivo para a chave de criptografia. Essas informações aparecem no campo Descrição ao visualizar uma lista de chaves de criptografia no Rapid Recovery Core Console. As descrições podem conter até 254 caracteres. A melhor prática é evitar o uso de caracteres proibidos e frases proibidas.
Frase de acesso	Insira a frase de acesso usada para controlar o acesso. A melhor prática é evitar o uso de caracteres proibidos.

Caixa de texto	Descrição
	Armazene a frase de acesso em um local seguro. O Suporte da Dell não consegue recuperar uma frase de acesso. Depois de criar uma chave de criptografia e aplicá-la a uma ou mais máquinas protegidas, você não poderá recuperar os dados caso perca a frase de acesso.
Confirmar frase de acesso	Insira novamente a frase de acesso. Usado para confirmar a entrada da frase de acesso.

4 Clique em **OK**.

A caixa de diálogo é fechada. A chave de criptografia que você especificou será aplicada às cópias de segurança futuras dessa máquina protegida e o cadeado agora aparece fechado.

Opcionalmente, se quiser que a chave de criptografia seja aplicada imediatamente, force um snapshot. Para obter mais informações, consulte Forçar um snapshot.

CUIDADO: O Rapid Recovery a criptografia AES de 256 bits no modo encadeamento de blocos de codificação (CBC) com chaves de 256 bits. Embora o uso de criptografia seja opcional, a Dell recomenda que você estabeleça uma chave de criptografia e que proteja a frase de acesso definida. Armazene a frase de acesso em um local seguro, pois ela é essencial para a recuperação dos dados. Sem a frase de acesso, não é possível executar a recuperação dos dados.

Desassociar uma chave de criptografia de uma máquina protegida

Depois que uma chave de criptografia é aplicada a uma máquina protegida, todos os dados de snapshot subsequentes armazenados no Rapid Recovery Core são criptografados.

Você pode desassociar uma chave de criptografia de uma máquina protegida. Essa ação não descriptografa as cópias de segurança existentes, mas gera uma nova imagem de base da máquina no momento do próximo snapshot programado ou forçado.

NOTA: Se desejar remover uma chave de criptografia do Core, conforme descrito no tópico Remover uma chave de criptografia, deverá primeiramente desassociar essa chave de criptografia de todas as máquinas protegidas.

Realize este procedimento para desassociar uma chave de criptografia de uma máquina protegida específica.

1 Navegue até o Rapid Recovery Core e clique em **Máquinas protegidas**.

A página Máquinas protegidas é exibida, listando todas as máquinas protegidas por esse Core. Um cadeado aberto aparece para as máquinas que não têm uma chave de criptografia aplicada. Um cadeado fechado indica que a máquina protegida está com a criptografia aplicada.

2 No painel Máquinas protegidas, clique no ícone **Criptografado** da máquina protegida que deseja configurar.

A caixa de diálogo **Configuração de criptografia** é exibida.

3 Selecione **Criptografar dados usando criptografia baseada em Core com uma chave existente** e, no menu suspenso, selecione **(Nenhum)** e clique em **OK**.

4 Se desejar remover a chave de criptografia do Rapid Recovery Core, repita este procedimento em todas as máquinas protegidas que usam essa chave. Em seguida, execute o procedimento descrito no tópico Remover uma chave de criptografia.

Gerenciar chaves de criptografia

Para gerenciar chaves de criptografia do Rapid Recovery Core, na barra de ícones, clique em (Mais) e selecione **Chaves de criptografia**. A página **Chaves de criptografia** é exibida. Para cada chave de criptografia adicionada ao Rapid Recovery Core (caso alguma já tenha sido definida), você vê as informações descritas na tabela a seguir.

Tabela 35. Informações sobre cada chave de criptografia

Elemento de UI	Descrição
Selecione um item	Para cada chave de criptografia, você pode marcar a caixa de seleção para realizar ações na lista de opções do menu acima da tabela.
Nome	O nome associado à chave de criptografia.
Impressão digital	Esse parâmetro é uma cadeia de caracteres gerada aleatoriamente com as 26 letras maiúsculas e minúsculas do alfabeto inglês, que ajuda a identificar exclusivamente cada chave de criptografia.
Tipo	Tipo descreve o ponto de origem de uma chave de criptografia e a possibilidade de ser aplicada. Uma chave de criptografia conter um de dois tipos possíveis: **Universal**. O tipo Universal é a condição padrão quando você cria uma chave de criptografia. Uma chave com um tipo Universal, combinada com um estado Desbloqueado, indica que a chave pode ser aplicada a uma máquina protegida. Você não pode bloquear manualmente um tipo de chave universal; em vez disso, você deve primeiro alterar o tipo conforme descrito no procedimento Como alterar tipos de chave de criptografia. **Replicação**. Quando uma máquina protegida em um Core de origem tem criptografia ativada e os pontos de recuperação dessa máquina são replicados em um Core de destino, qualquer chave de criptografia usada na origem é exibida automaticamente no Core de destino com um tipo de Replicação. O estado padrão após receber uma chave replicada é bloqueado. Você pode desbloquear uma chave de criptografia com um tipo de Replicação fornecendo a frase de acesso. Caso uma chave tenha um tipo Desbloqueado, você pode bloqueá-la manualmente. Para obter mais informações, consulte o tópico Desbloquear uma chave de criptografia.
Estado	O estado indica se uma chave de criptografia pode ser usada. Os dois estados possíveis são: • **Desbloqueado**. Um estado Desbloqueado indica que a chave pode ser usada imediatamente. Por exemplo, você pode criptografar snapshots de uma máquina protegida ou recuperar dados de um ponto de recuperação replicado no Core de destino. • **Bloqueado**. Um estado Bloqueado indica que a chave não pode ser usada até ser desbloqueada por meio de uma frase de acesso. Bloqueado é o estado padrão de uma chave de criptografia recém-importada ou replicada. Quando o estado de uma chave de criptografia é bloqueado, ela deve ser desbloqueada para ser usada. Caso você tenha desbloqueado anteriormente uma chave de criptografia bloqueada e a duração de desbloqueio tenha expirado, o estado muda de desbloqueado para bloqueado. Depois que a chave é bloqueada automaticamente, você deve desbloqueá-la novamente para usá-la. Para obter mais informações, consulte o tópico Desbloquear uma chave de criptografia.
Descrição	A descrição é um campo opcional, no qual recomendamos incluir informações úteis sobre a chave de criptografia, como o uso pretendido ou uma dica sobre a frase de acesso.

No nível superior do painel Chaves de criptografia, você pode adicionar uma chave de criptografia ou importar uma chave usando um arquivo exportado de outro Rapid Recovery Core. Você também pode excluir chaves selecionadas na tabela de resumo.

Desde que haja uma chave de criptografia para um Core, você pode gerenciar as chaves existentes editando as propriedades de nome ou descrição, alterando a frase de acesso, desbloqueando uma chave de criptografia bloqueada ou removendo a chave do Rapid Recovery Core. Você também pode exportar uma chave para um arquivo, que pode ser importado para outro Rapid Recovery Core.

Quando você adiciona uma chave de criptografia na página **Chaves de criptografia**, a chave é exibida na lista de chave de criptografia, mas não é aplicada a uma máquina protegida específica. Para obter informações sobre como aplicar uma chave de criptografia criada no painel **Chaves de criptografia** ou para excluir uma chave por completo do Rapid Recovery Core, consulte Aplicar ou remover criptografia de uma máquina protegida.

No painel **Chaves de criptografia**, você pode gerenciar a segurança dos dados de backup no Core de qualquer máquina protegida no repositório fazendo o seguinte:

- Adicionar uma chave de criptografia
- Importar uma chave de criptografia

- Desbloquear uma chave de criptografia
- Editar uma chave de criptografia
- Alterar a frase de acesso de uma chave de criptografia
- Exportar uma chave de criptografia
- Remover uma chave de criptografia
- Como alterar tipos de chave de criptografia

Adicionar uma chave de criptografia

ORapid Recovery usa a criptografia AES de 256 bits no modo encadeamento de blocos de codificação (CBC) com chaves de 256 bits. Embora o uso de criptografia seja opcional, a Dell recomenda que você estabeleça uma chave de criptografia e que proteja a frase de acesso definida.

CUIDADO: Armazene a frase de acesso em um local seguro. Sem uma frase de acesso, não é possível recuperar os dados dos pontos de recuperação criptografados.

Depois de definir uma chave de criptografia, você pode usá-la para proteger seus dados. As chaves de criptografia podem ser usadas em qualquer número de máquinas protegidas.

Esta etapa descreve como adicionar uma chave de criptografia no Console do Rapid Recovery Core. Esse processo não aplica a chave a nenhuma máquina que esteja sendo protegida atualmente no Core. Você também pode adicionar uma chave de criptografia durante o processo de proteção de uma máquina. Para obter mais informações sobre como adicionar criptografia como parte da proteção de uma máquina, consulte Proteger uma máquina. Para obter mais informações sobre como adicionar criptografia a duas ou mais máquinas ao protegê-las inicialmente, consulte Sobre como proteger diversas máquinas.

Execute as etapas deste procedimento para adicionar uma chave de criptografia.

1 Navegue até o Console do Rapid Recovery Core.

2 Na barra de ícones, clique em (Mais) e, em seguida, selecione **Chaves de criptografia**.
A página **Chaves de criptografia** será exibida.

3 Clique em **Adicionar chave de criptografia**.
A caixa de diálogo **Criar chave de criptografia** será exibida.

4 Na caixa de diálogo **Criar chave de criptografia**, insira os detalhes da chave, como descrito na tabela a seguir.

Tabela 36. Criar detalhes da chave de criptografia.

Caixa de texto	Descrição
Nome	Insira um nome para a chave de criptografia. Os nomes de chaves de criptografia devem ter entre 1 e 64 caracteres alfanuméricos. Não use caracteres proibidos ou frases proibidas.
Descrição	Insira um comentário para a chave de criptografia. Essas informações aparecem no campo Descrição ao visualizar as chaves de criptografia no Core Console. Você pode inserir até 254 caracteres. A prática recomendada é evitar o uso de caracteres proibidos e frases proibidas.
Frase de acesso	Insira a frase de acesso usada para controlar o acesso. A prática recomendada é evitar o uso de caracteres proibidos.

Caixa de texto	Descrição
	CUIDADO: Armazene a frase de acesso em um local seguro. Dell O suporte não pode recuperar uma frase de acesso. Depois de criar uma chave de criptografia e aplicá-la a uma ou mais máquinas protegidas, você não poderá recuperar os dados caso perca a frase de acesso.
Confirmar frase de acesso	Insira novamente a frase de acesso. Usado para confirmar a entrada da frase de acesso.

5 Clique em **OK**.

A caixa de diálogo é fechada e a chave de criptografia criada fica visível na página Chaves de criptografia.

6 Para aplicar uma chave de criptografia a uma máquina protegida, consulte Aplicar uma chave de criptografia a partir da página Máquinas protegidas.

Importar uma chave de criptografia

Você pode importar uma chave de criptografia de outro Rapid Recovery Core e usar essa chave para criptografar dados para uma máquina protegida no Core. Para importar a chave, é necessário que ela possa ser acessada pela máquina Core, localmente ou através da rede. Você também deve saber a frase de acesso da chave de criptografia.

Execute as etapas deste procedimento para importar uma chave de criptografia.

NOTA: Este procedimento não aplica a chave a nenhuma máquina protegida. Para obter mais informações sobre como aplicar a chave, consulte Aplicar uma chave de criptografia a partir da página Máquinas protegidas.

1 Navegar para o Rapid Recovery Core.

2 Na barra de ícones, clique em (Mais) e selecione **Chaves de criptografia**.

A página **Chaves de criptografia** é exibida.

3 Clique em **Importar**.

A caixa de diálogo **Upload de arquivo** é exibida.

4 Na caixa de diálogo**Upload de arquivo**, navegue para a rede ou o diretório local contendo a chave de criptografia que você deseja importar.

Por exemplo, navegue para a pasta **Downloads** do usuário conectado.

O nome de arquivo da chave começa com "EncryptionKey-", seguido do ID da chave e terminando com a extensão .key. Um exemplo de nome de chave de criptografia é EncryptionKey-RandomAlphabeticCharacters.key.

5 Selecione a chave que você deseja importar e clique em **Abrir**.

6 Na caixa de diálogo **Importar chave**, clique em **OK**.

A caixa de diálogo é fechada e a chave de criptografia importada permanece visível na página **Chaves de criptografia**. Se a chave de criptografia foi usada para proteger um volume antes de ser exportada, o estado da chave é Bloqueado.

Desbloquear uma chave de criptografia

Chaves de criptografia podem estar em estado bloqueado ou desbloqueado. Uma chave de criptografia desbloqueada pode ser aplicada a uma máquina protegida para proteger os dados de cópia de segurança dessa máquina salvos no repositório. Em um Rapid Recovery Core, usando uma chave de criptografia desbloqueada, você também pode recuperar dados de um ponto de recuperação.

Quando você importa uma chave de criptografia para um Rapid Recovery Core, o estado padrão é Bloqueado. Isso é válido quer você tenha importado a chave de criptografia explicitamente, quer ela tenha sido adicionada ao Rapid Recovery Core pela replicação de máquinas protegidas criptografadas ou pela importação de um arquivo de pontos de recuperação criptografados.

No caso de chaves de criptografia adicionadas ao Rapid Recovery Core somente por replicação, ao desbloquear uma chave, você pode especificar um período de tempo (em horas, dias ou meses) durante o qual ela continuará desbloqueada. Cada dia é baseado em um período de 24 horas começando no momento em que a solicitação de desbloqueio é salva no Rapid Recovery Core. Por exemplo, se a chave for desbloqueada às 11h24 na terça-feira e a duração selecionada for de dois dias, a chave será bloqueada outra vez, automaticamente, às 11h24 de quinta-feira.

NOTA: Não é possível usar uma chave de criptografia bloqueada para recuperar dados nem aplicá-la a uma máquina protegida. Você deve primeiro fornecer a frase de acesso, desbloqueando assim a chave.

Você também pode bloquear uma chave de criptografia desbloqueada, garantindo que ela não possa ser aplicada a uma máquina protegida até ser desbloqueada. Para bloquear uma chave de criptografia com o estado Universal, primeiramente, é necessário alterar o tipo para Replicado.

Se uma chave de criptografia desbloqueada está sendo usada atualmente para proteger uma máquina no Core, é preciso primeiro desassociá-la da máquina protegida para poder bloqueá-la.

Conclua as etapas deste procedimento para desbloquear uma chave de criptografia bloqueada.

1 Navegue até o núcleo do Rapid Recovery.

2 Na barra de ícones, clique em (Mais) e selecione **Chaves de criptografia**.
A página **Chaves de criptografia** é exibida. A coluna Estado indica quais chaves de criptografia estão bloqueadas.

3 Localize a chave de criptografia que você deseja desbloquear, clique no respectivo menu suspenso e selecione **Desbloquear**.
A caixa de diálogo **Editar chave de criptografia** é exibida.

4 Na caixa de diálogo, no campo Frase de acesso, insira a frase de acesso para desbloquear esta chave.

5 Para especificar o período em que a chave permanecerá desbloqueada, na opção Duração, execute um destes procedimentos:
- Para especificar que a chave continuará desbloqueada até você bloqueá-la explicitamente, no Rapid Recovery selecione **Até o bloqueio manual**.
- Para especificar que a chave permaneça bloqueada por uma duração especificada que você pode configurar em horas, dias ou meses, faça o seguinte:
  - Selecione o campo de número e digite um valor entre 1 e 999.
  - Especifique horas, dias ou meses, respectivamente.
  - Depois, clique em **OK**.
    Essa opção está disponível para chaves de criptografia adicionadas por replicação.

    A caixa de diálogo é fechada e as alterações da chave de criptografia selecionada ficam visíveis na página de Chaves de criptografia.
- Para especificar que a chave permaneça bloqueada até a data e hora escolhidas, faça o seguinte:
  - Selecione a opção **Até**.
  - No campo de texto ou usando os widgets calendário e relógio, especifique explicitamente os dados e a hora em que você deseja que a chave de criptografia seja travada.
  - Depois, clique em **OK**.
    Essa opção está disponível para chaves de criptografia adicionadas por replicação.

    A caixa de diálogo é fechada e as alterações da chave de criptografia selecionada ficam visíveis na página de Chaves de criptografia.

Bloquear uma chave de criptografia

Quando uma chave de criptografia estiver bloqueada, ela não pode ser aplicada a qualquer máquina protegida até que seja desbloqueada. Para bloquear uma chave de criptografia com o tipo Universal, é necessário primeiramente alterar o tipo para Replicado.

Conclua as etapas deste procedimento para bloquear uma chave de criptografia.

1 Navegue até o núcleo do Rapid Recovery.

2 Na barra de ícones, clique em (Mais) e selecione **Chaves de criptografia**.
A página **Chaves de criptografia** é exibida. A coluna Estado indica quais chaves de criptografia estão desbloqueadas e mostra o tipo de cada chave.

3 Localize a chave de criptografia que você deseja bloquear. Se o tipo dela for Universal, clique em seu menu suspenso e selecione **Alterar o tipo para Replicado**.
A caixa de diálogo **Alterar tipo da chave de criptografia** é exibida.

4 Na caixa de diálogo, confirme que você deseja alterar o tipo de chave para **Replicated**.

5 Se você alterou com sucesso o status da chave de criptografia para Replicado, clique em seu menu suspenso e selecione **Bloquear**.
A caixa de diálogo **Bloquear chave de criptografia** é exibida.

6 Na caixa de diálogo, confirme que deseja bloquear a chave.
A caixa de diálogo é fechada e o estado da chave de criptografia selecionada agora é bloqueado.

NOTA: Essa opção está disponível para chaves de criptografia adicionadas por replicação.

Editar uma chave de criptografia

Depois que uma chave de criptografia é definida, você pode editar o nome ou a descrição da chave. Essas propriedades aparecem quando você visualiza a lista de chaves de criptografia no painel Chaves de criptografia.

Execute as etapas deste procedimento para editar o nome ou a descrição de uma chave de criptografia desbloqueada existente.

CUIDADO: Depois de editar o nome ou a descrição de uma chave de criptografia usada para proteger uma ou mais máquinas, o Rapid Recovery tira uma nova imagem de base. Esse snapshot da imagem de base ocorre para essa máquina no próximo snapshot programado ou forçado.

1 Navegue até o núcleo do Rapid Recovery.

2 Na barra de ícones, clique em (Mais) e selecione **Chaves de criptografia**.
A página **Chaves de criptografia** é exibida.

3 Localize a chave de criptografia que você quer editar e faça o seguinte:
- Se a chave estiver bloqueada, é necessário desbloqueá-la. Consulte Desbloquear uma chave de criptografia
- Se a chave estiver desbloqueada, proceda conforme descrito abaixo.

4 Clique, no menu suspenso para a chave de criptografia especificada e selecione **Editar**.
A caixa de diálogo **Edit Encryption Key** (Editar chave de criptografia) é mostrada.

5 Na caixa de diálogo, edite o nome ou a descrição da chave de criptografia e clique em **OK**.
A caixa de diálogo é fechada e as alterações da chave de criptografia selecionada ficam visíveis na página de **Chaves de criptografia**.

Alterar a frase de acesso de uma chave de criptografia

Para manter máxima segurança, você pode alterar a frase de acesso de qualquer chave de criptografia existente. Execute as etapas deste procedimento para alterar a frase de acesso de uma chave de criptografia.

CUIDADO: Depois que você edita a frase de acesso de uma chave de criptografia usada para proteger uma ou mais máquinas, o Rapid Recovery Core captura um snapshot incremental dessa máquina no próximo snapshot programado ou forçado.

1 Navegar para o Rapid Recovery Core.

2 Na barra de ícones, clique em (Mais) e, em seguida, selecione **Chaves de criptografia**.
A página **Chaves de criptografia** é exibida.

3 Localize a chave de criptografia que você deseja atualizar, clique no menu suspenso e selecione **Alterar senha**.
A caixa de diálogo **Change Passphrase** (Alterar senha) é mostrada.

4 Na caixa de diálogo, no campo **Frase de acesso**, digite a nova frase de acesso da criptografia.

5 No campo **Confirmar frase de acesso**, digite novamente a frase de acesso idêntica.

6 Clique em **OK**.
A caixa de diálogo é fechada e a frase de acesso é atualizada.

7 Como opcional, caso você use uma dica no campo Descrição, edite a chave de criptografia para atualizar a dica. Para obter mais informações, consulte Editar uma chave de criptografia.

CUIDADO: Rapid Recovery usa criptografia AES de 256 bits em modo Cipher Block Chaining (CBC) com chaves de 256 bits. A Dell recomenda gravar a frase de acesso em um local seguro e manter essas informações atualizadas. O Suporte da Dell não consegue recuperar uma frase de acesso. Sem a frase de acesso, você não pode recuperar informações dos pontos de recuperação criptografados.

Exportar uma chave de criptografia

Você pode exportar uma chave de criptografia de qualquer Rapid Recovery Core com a finalidade específica de usá-la em outro Core. Quando você executa esse procedimento, a chave é salva na pasta **Downloads** da conta de usuário do Windows ativa.

Execute as etapas deste procedimento para exportar uma chave de criptografia.

1 Navegue até o núcleo do Rapid Recovery.

2 Na barra de ícones, clique em (Mais) e selecione **Chaves de criptografia**.
A página **Chaves de criptografia** é exibida.

3 Localize a chave de criptografia que você deseja exportar, clique no respectivo menu suspenso e selecione **Exportar**.
A caixa de diálogo **Abrir chave de criptografia-[nome.chave]** é exibida.

4 Na caixa de diálogo, selecione **Salvar arquivo** para salvar e armazenar as chaves de criptografia em um local seguro e clique em **OK**.
O download da chave de criptografia é feito em forma de arquivo de texto no local padrão, como a pasta **Downloads** da conta de usuário do Windows ativa.

5 Como opção, se desejar importar essa chave para um Core diferente, copie o arquivo para um local acessível no Core escolhido.

Remover uma chave de criptografia

Quando você remove uma chave de criptografia na página Chave de criptografia, a chave é excluída do Rapid Recovery Core.

NOTA: A remoção de uma chave de criptografia não descriptografa os pontos de recuperação já salvos usando a chave. Você ainda precisa manter e fornecer a frase de acesso para a chave para recuperar dados para os pontos de recuperação criptografados existentes.

Você não pode remover uma chave de criptografia que já esteja associada a uma máquina protegida. Você deve primeiramente visualizar as definições de criptografia de cada máquina protegida que use a chave e desassociar a chave de criptografia que deseja remover. Para obter mais informações, consulte o tópico Desassociar uma chave de criptografia de uma máquina protegida.

Execute as etapas deste procedimento para remover uma chave de criptografia.

1 Navegue até o Rapid Recovery Core.

2 Na barra de ícones, clique em (Mais) e, em seguida, selecione **Chaves de criptografia**.
A página **Chaves de criptografia** será exibida.

3 Localize a chave de criptografia que você quer remover. Clique em seu menu suspenso, e selecione **Remover**.
A caixa de diálogo **Remover a chave de criptografia** será exibida. Você verá uma mensagem confirmando a ação de remover a chave de criptografia.

4 Na caixa de diálogo, confirme que deseja remover a chave de criptografia.

NOTA: A remoção de uma chave de criptografia não descriptografa os pontos de recuperação já salvos usando a chave. Você ainda precisa manter e fornecer a chave para recuperar dados para os pontos de recuperação criptografados existentes.

A caixa de diálogo é fechada e a chave de criptografia removida não aparece mais na página **Chave de criptografia**.

Como alterar tipos de chave de criptografia

As chaves de criptografia listam um dos dois tipos possíveis no painel Chaves de criptografia: Universal ou Replicação. O tipo indica a provável origem da chave de criptografia e determina se você pode alterar os detalhes ou as frase de acesso. Você só pode modificar atributos caso o tipo seja Universal. Caso precise modificar esse atributos para uma chave com tipo Replicado, você deve alterar o tipo para Universal usando esse procedimento. Quando você alterar o tipo de uma chave de criptografia para Universal, ela é desbloqueada manualmente e pode ser usada para criptografar outras máquinas protegidas.

NOTA: Você deve saber a frase de acesso para alterar o tipo de Replicado para Universal.

As chaves de criptografia também têm dois estados possíveis: Bloqueado ou Desbloqueado. O estado determina se é possível aplicar uma chave de criptografia a uma máquina protegida ou restaurar dados de um ponto de recuperação criptografado. Você só pode alterar o tipo de uma chave de criptografia manualmente caso o estado seja Desbloqueado.

Quando você cria primeiro uma chave de criptografia, o tipo é Universal, e o estado é Desbloqueado. Você pode usar essa chave imediatamente (por exemplo, para criptografar cópias de segurança de uma máquina protegida). No entanto, um tipo de chave Universal não pode ser bloqueado manualmente. Caso queira bloquear manualmente uma chave de criptografia com um tipo de Universal, você deve alterar o tipo para Replicado usando esse procedimento.

Você não pode alterar um tipo da chave de criptografia caso esteja já em uso pontos de recuperação de criptografia para uma o mais máquinas protegidas.

Siga esse procedimento para alterar um tipo da chave de criptografia.

1 Navegar para o Rapid Recovery Core.

2 Na barra de ícones, clique em (Mais) e selecione **Chaves de criptografia**.
A página **Chaves de criptografia** é exibida. Chaves de criptografia acessíveis ao Core são exibidas em uma tabela de resumo. Cada uma lista um tipo de Universal ou Replicado.

3 Localize a chave de criptografia que você deseja atualizar.

4 Caso você queira alterar uma chave de criptografia Universal para Replicação, faça o seguinte:

a Clique no menu suspenso e selecione **Alterar o tipo para Replicado**.
A caixa de diálogo **Alterar o tipo da chave de criptografia** é exibida. Você vê uma mensagem confirmando que você deseja alterar o tipo para Replicado.

- Na caixa de diálogo, confirme se você deseja alterar o tipo para Replicado.

A caixa de diálogo é fechada, e o tipo de chave de criptografia é atualizado para Replicação.

5 Caso você queira alterar uma chave de criptografia Replicação para Universal, faça o seguinte:

a Clique no menu suspenso e selecione **Alterar o tipo para Universal**

A caixa de diálogo **Alterar o tipo da chave de criptografia** é exibida. Você vê uma mensagem confirmando que você deseja alterar o tipo para Universal.

- Na caixa de diálogo, no campo **Frase de acesso**, digite a frase de acesso e clique em **OK** para confirmar se você deseja alterar o tipo para Universal.

A caixa de diálogo é fechada, e o tipo de chave de criptografia é atualizado para Universal.

Gerenciar contas de nuvem

Esta seção descreve como definir links para contas existentes de provedores de armazenamento em nuvem e como gerenciar essas contas para uso com o Rapid Recovery. Por exemplo, você pode arquivar os dados do Rapid Recovery na nuvem ou importar dados arquivados da nuvem.

Sobre contas de nuvem

Rapid Recovery permite arquivar dados em diversos provedores de nuvem ou importar dados arquivados armazenados em uma conta de nuvem. Entre as nuvens compatíveis estão Microsoft Azure, Amazon™, Rackspace, e qualquer fornecedor com base em OpenStack.

Você pode adicionar uma conta de nuvem ao Rapid Recovery Core Console. Depois de adicioná-la, você poderá editar as informações, configurar as opções de conexão da conta ou remover a conta do Rapid Recovery.

Adicionar uma conta de nuvem

Antes que você possa mover os dados em qualquer direção entre uma conta de nuvem e o seu Core, você precisa adicionar os dados da conta do provedor da nuvem ao Rapid Recovery Core Console. Essas informações identificam a conta de nuvem no Core Console enquanto armazena em cache, seguramente, as informações da conexão. Esse processo então permite que o Rapid Recovery Core se conecte à conta de nuvem para executar as operações que você especificar.

Para adicionar uma conta em nuvem, execute as etapas do procedimento a seguir.

1 Na barra de ícones do Rapid Recovery Core Console, clique no ícone **Mais** e, em seguida, selecione **Contas de nuvem**.
A página **Contas de nuvem** é exibida.

2 Na página **Contas de nuvem**, clique em **Adicionar nova conta**.
A caixa de diálogo **Add New Account** (Adicionar nova conta) é mostrada.

3 Selecione um provedor de nuvem compatível da lista suspensa Tipo de nuvem.

4 Digite os detalhes conforme descrito na tabela a seguir com base no tipo de nuvem selecionado na etapa 3.

Tabela 37. Detalhes da conta de nuvem

Tipo de nuvem	Caixa de texto	Descrição
Microsoft Azure	Nome da conta de armazenamento	Insira o nome de sua conta de armazenamento do Microsoft Azure.

Tipo de nuvem	Caixa de texto	Descrição
		NOTA: O nome deve corresponder precisamente ao nome da conta de armazenamento no Azure. Deve conter apenas letras minúsculas e números, e ter entre 3 e 24 caracteres.
	Chave de acesso	Insira a chave de acesso para sua conta. **NOTA: Você pode digitar a chave principal ou secundária. Para obter a chave de acesso da conta do Azure, verifique Chaves em Configurações.**
	Usar o protocolo https	Selecione esta opção para usar o protocolo https seguro em vez do protocolo http padrão.
	Nome de exibição	Digite um nome de exibição para essa conta de nuvem para a exibição no Rapid Recovery Core Console; por exemplo, Microsoft Azure 1.
Amazon™ S3	Chave de acesso	Digite a chave de acesso para sua conta de nuvem da Amazon™.
	Chave secreta	Insira a chave secreta para esta conta.
	Nome de exibição	Digite um nome de exibição para essa conta de nuvem para a exibição no Rapid Recovery Core Console; por exemplo, Amazon 1.
Fornecido pelo OpenStack	Região	Digite a região para sua conta de nuvem.
	Nome de usuário	Insira o nome de usuário para sua conta em nuvem baseada no OpenStack.
	Senha ou chave de API	Selecione se deseja usar uma senha ou uma chave de API e digite sua seleção para esta conta.
	ID do locatário	Insira seu ID do locatário para esta conta.
	URL de autenticação	Insira a URL de autenticação para esta conta.
	Nome de exibição	Digite um nome de exibição para essa conta de nuvem para a exibição no Rapid Recovery Core Console; por exemplo, OpenStack 1.
Arquivos do Rackspace Cloud	Região	Use a lista suspensa para selecionar a região para a sua conta.
	Nome de usuário	Insira o nome de usuário para sua conta em nuvem do Rackspace.
	Senha ou chave de API	Selecione se deseja usar uma senha ou uma chave de API e digite sua seleção para esta conta.
	ID do locatário	Insira seu ID do locatário para esta conta.
	URL de autenticação	Insira a URL de autenticação para esta conta.
	Nome de exibição	Digite um nome de exibição para essa conta de nuvem para a exibição no Rapid Recovery Core Console; por exemplo, Rackspace 1.

5 Clique em **Salvar**.

A caixa de diálogo fecha e sua conta aparece na página **Contas de nuvem** do Core Console.

Editar uma conta de nuvem

Caso precise alterar as informações para se conectar à conta de nuvem, por exemplo, para atualizar a senha ou editar o nome de exibição, você pode fazer isso na página Contas de nuvem do Rapid Recovery Core Console. Execute as etapas do procedimento a seguir para editar uma conta em nuvem.

1 Na barra de ícones do Rapid Recovery Core Console, clique no ícone  **Mais** e, em seguida, selecione **Contas de nuvem**.
A página **Contas de nuvem** é exibida.

2 Ao lado da conta em nuvem que desejar editar, clique no menu suspenso, e depois clique em **Editar**.
A janela **Editar conta** é aberta.

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

NOTA: Não é possível editar o tipo de nuvem.

Configurar as definições da conta de nuvem

As definições de configuração da nuvem permitem determinar o tempo que deve ser decorrido entre as tentativas do Rapid Recovery de se conectar à sua conta de nuvem antes que o tempo expire. Execute as etapas do procedimento a seguir para configurar as definições da conexão para sua conta em nuvem.

1 Na barra de ícone do Rapid Recovery Core Console, clique em  **Configurações**.
A pagina Definições é exibida.

2 No menu à esquerda, clique em **Contas de nuvem**.

3 Na tabela Contas de nuvem, clique no menu suspenso ao lado da conta de nuvem que você deseja configurar e realize os passos a seguir:

- Para alterar as configurações de conexão da conta de nuvem, clique em **Editar**.
  1 Na caixa de diálogo Configuração da nuvem, realize um dos procedimentos a seguir:
    - Para **Solicitar tempo limite**, utilize as setas para cima e para baixo para determinar o período, em minutos e segundos, a ser utilizado pelo Rapid Recovery sobre uma tentativa única de se conectar à conta de nuvem quando houver um atraso. As tentativas de conexão irão parar depois da quantidade de tempo inserida.
    - Para **Tamanho do buffer de gravação**, insira o tamanho do buffer que deseja reservar para gravar dados arquivados na nuvem.
    - Para **Tamanho do buffer de leitura**, insira o tamanho do bloco que deseja reservar para ler dados arquivados da nuvem.
  2 Clique em **OK**.
- Para retornar a configuração da nuvem para o seguinte padrão, clique em **Redefinir**.
  - **Solicitar tempo limite:**01:30 (minutos e segundos)
  - **Tamanho do buffer de gravação:** 8388608 (bytes)
  - **Tamanho do buffer de leitura:** 8388608 (bytes)

Remover uma conta de nuvem

Se você interromper seu serviço em nuvem, ou decidir parar de usá-lo em um Core específico, você pode desejar remover sua conta em nuvem do Core Console. Execute as etapas do procedimento a seguir para remover uma conta em nuvem.

1 Na barra de ícones do Rapid Recovery Core Console, clique no ícone  **Mais** e, em seguida, selecione **Contas de nuvem**.

A página **Contas de nuvem** é exibida.

2 Ao lado da conta em nuvem que desejar editar, clique no menu suspenso, e depois clique em **Remover**.

3 Na caixa de diálogo **Apagar conta**, clique em **Sim** para confirmar que quer remover a conta.

4 Se a conta de nuvem estiver atualmente em uso, uma segunda caixa de diálogo solicita que você confirme se você ainda deseja removê-la. Clique em **Sim** para confirmar.

NOTA: Remover uma conta atualmente em uso faz com que todos os trabalhos de arquivamento para esta conta falhem.

Archiving

Esta seção descreve casos de negócios para a criação de um arquivo, como criar um arquivo usando o Rapid Recovery e onde você pode armazená-lo.

Noções básicas sobre arquivos

As políticas de retenção impõem períodos em que as cópias de segurança são armazenadas em mídias de curto prazo (rápidas e caras). Às vezes, certos requisitos técnicos e de negócios exigem a retenção prolongada desses backups, mas o armazenamento rápido tem um custo proibitivo. Portanto, esse requisito gera uma necessidade de armazenamento de longo prazo (lento e barato). As empresas frequentemente usam o armazenamento de longo prazo para arquivar dados de conformidade e não conformidade. O recurso de arquivo do Rapid Recovery é usado para oferecer suporte à retenção estendida de dados compatíveis e não compatíveis. Também é usado para executar replicação de dados de replicação para um core de réplica remota.

Quando um arquivo é criado, ele pode ser usado das seguintes maneiras:

- Um arquivo pode ser montado como um sistema de arquivos para recuperação de arquivos simples ou pastas.
- Um arquivo pode ser usado como fonte para uma restauração sem sistema operacional.
- Um arquivo pode ser importado para um repositório.

Criar um arquivo

Você pode usar esse procedimento para criar um arquivo único ou um arquivamento programado.

Se você planejar a criação de um arquivo em um local da nuvem, adicione, em primeiro lugar, sua conta de nuvem ao Rapid Recovery Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.

Um arquivo único é um arquivo criado sob demanda para um máquina específica. Um arquivo programado é um arquivo que reaparece automaticamente na data e na hora especificadas no assistente. A capacidade de programar um arquivo recorrente acomoda situações nas quais você desejaria que arquivos frequentes de uma máquina fossem salvos sem a inconveniência de precisar criar manualmente os arquivos todas as vezes.

1 Na barra de botões do Rapid Recovery Core Console, clique em  **Arquivar**.
O assistente de arquivo é aberto.

2 Na página **Tipo de arquivo** do assistente, selecione uma das opções a seguir:
- Arquivo único
- Arquivo contínuo (por programa)

3 Clique em **Avançar**.

4 Na página **Local**, selecione uma opção na lista suspensa **Tipo de local** e insira as informações conforme descritas na seguinte tabela.

Tabela 38. Opções de tipo de local de arquivo

Opção	Caixa de texto	Descrição
Local	Local	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, d:\work\archive.
Rede	Local	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, \\servername\sharename.
	Nome de usuário	Insira um nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira uma senha para o caminho de rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA: Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.**
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados devem ser salvos.

5 Clique em **Avançar**.

6 Na página **Máquinas** do assistente, selecione a(s) máquina(s) protegida(s) que você desejar arquivar.

7 Clique em **Avançar**.

8 Realize um dos procedimentos a seguir:

- Se você optar pela criação de um arquivo único, pule para a Etapa 15.
- Se você optar pela criação de um arquivamento programado, pule para a Etapa 9

9 Na página **Programa**, selecione uma das seguintes opções na lista suspensa **Enviar dados**:

- Diariamente
- Semanalmente
- Mensalmente

10 Insira as informações descritas na seguinte tabela com base em sua seleção na Etapa 9.

Tabela 39. Opções de Enviar dados

Opção	Caixa de texto	Descrição
Diariamente	Na hora	Selecione a hora do dia que você deseja criar o arquivo diário.
Semanalmente	No dia de semana	Selecione um dia da semana no qual deseja criar automaticamente o arquivo.
	Na hora	Selecione a hora do dia na qual você deseja criar um arquivo.
Mensalmente	No dia do mês	Selecione o dia do mês no qual deseja criar automaticamente o arquivo.
	Na hora	Selecione a hora do dia na qual você deseja criar um arquivo.

11 Opcionalmente, se você não quiser que o trabalho de arquivo seja iniciado na próxima hora programada depois de concluir o assistente, selecione **Pausar o arquivamento inicial**.

NOTA: Talvez você deseje pausar o arquivo agendado se precisar de tempo para preparar o local de destino antes de arquivar os resumos. Se você não selecionar essa opção, o arquivamento começa no horário agendado.

12 Clique em **Avançar**.

13 Na página **Opções** de um arquivo contínuo, selecione uma das ações de reciclagem descritas na seguinte tabela.

Tabela 40. Opções de reciclagem de arquivo contínuo

Caixa de texto	Descrição
Incremental	Permite que você adicione pontos de recuperação a um arquivo existente. Compara pontos de recuperação para evitar duplicação de dados que já existem no arquivo.
Substitua esse core	Substitui quaisquer dados arquivados preexistentes pertencentes a este core, porém deixa os dados de outros cores intactos.
Apagar completamente	Apaga todos os dados arquivados do diretório antes de gravar o novo arquivo.

14 Opcionalmente, selecione **Criar cadeias de pontos de recuperação (corrigir órfãos)** e pule para a Etapa 18.

15 Na página **Opções** de um arquivo único, insira as informações descritas na seguinte tabela.

Tabela 41. Opções de arquivo único

Caixa de texto	Descrição
Tamanho máximo	Grandes arquivos de dados podem ser divididos em vários segmentos. Selecione a quantidade máxima de espaço que você deseja reservar para criar o arquivo efetuando uma das seguintes ações: • Selecione **Destino inteiro** para reservar todo o espaço disponível no caminho fornecido para o destino fornecido na Etapa 4. (por exemplo, se o local for D:\work\archive, todo o espaço disponível na unidade D: será reservado). • Selecione a caixa de texto em branco, use as setas para cima e para baixo para inserir uma quantidade e depois selecione uma unidade de medida na lista suspensa para personalizar o espaço máximo que você deseja reservar. **NOTA: Os arquivos na nuvem Amazon™ são automaticamente divididos em segmentos de 50 GB. Os arquivos da nuvem Microsoft Azure são automaticamente divididos em segmentos de 200 GB.**
Reciclar ação	Selecione uma das seguintes opções de ação de reciclagem: • Não reutilizar. Não substitui ou apaga nenhum dado arquivado existente no local. Se o local não estiver vazio, o Rapid Recovery permitirá a seleção de um local diferente. • Substituir este Core. Substitui quaisquer dados arquivados preexistentes pertencentes a este core, porém deixa os dados de outros cores intactos. • Apagar completamente. Apaga todos os dados arquivados do diretório antes de gravar o novo arquivo. • Incremental. Permite que você adicione pontos de recuperação a um arquivo existente. Compara pontos de recuperação para evitar duplicação de dados que já existem no arquivo.
Comentários	Insira qualquer informação adicional necessária para o arquivo. O comentário será exibido se você importar o arquivo mais tarde.
Criar cadeias de pontos de recuperação (corrigir órfãos)	Selecione essa opção para arquivar toda a cadeia de pontos de recuperação. Esta opção é selecionada por padrão.

16 Clique em **Avançar**.

17 Na página **Período**, insira manualmente a data inicial e a data final dos pontos de recuperação a serem arquivados ou selecione a data/hora clicando no ícone de calendário e, depois, no ícone abaixo da janela do calendário.

18 Clique em **Concluir**.

O assistente é fechado.

Arquivar na nuvem

Quando os dados atingirem o final de um período de retenção, você pode desejar ampliar essa retenção criando um arquivo dos dados antigos. Quando você arquiva dados, há sempre uma dúvida de onde armazená-los. ORapid Recovery permite que você carregue seus arquivos em uma variedade de provedores de nuvem diretamente do Console do Core. As nuvens compatíveis incluem Microsoft Azure, Amazon™, Rackspace e qualquer provedor baseado em OpenStack.

Exportar um arquivo a uma nuvem utilizando o Rapid Recovery envolve os seguintes procedimentos:

- Adicione sua conta de nuvem ao Console do Rapid Recovery. Para obter mais informações, consulte Adicionar uma conta de nuvem.
- Arquive seus dados e exporte-os para sua conta em nuvem. Para obter mais informações, consulte Criar um arquivo.
- Retomar dados arquivados importando-os do local da nuvem. Para obter mais informações, consulte Importar um arquivamento.

Editar um arquivo programado

O Rapid Recovery permite que você altere os detalhes de um arquivamento programado. Para editar um arquivo agendado, execute as etapas do procedimento a seguir.

1 No Console do Rapid Recovery Core, clique no menu suspenso  **Mais** na barra de ícones e, em seguida, selecione **Arquivos**.

2 Na página Arquivos, sob Arquivos programados, clique no menu suspenso ao lado do arquivo que você deseja alterar, e depois clique em **Editar**.

O **Assistente de adição de arquivo** será aberto.

3 Na página **Local** do Assistente de arquivo, selecione uma das seguintes opções a partir na lista suspensa **Tipo de local**:

- Local
- Rede
- Nuvem

4 Digite os detalhes para o arquivamento conforme descrito na tabela a seguir com base no tipo de local selecionado na Etapa 3.

Tabela 42. Detalhes do arquivo

Opção	Caixa de texto	Descrição
Local	Local	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, d:\work\archive.
Rede	Local	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, \\servername\sharename.
	Nome de usuário	Insira um nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira uma senha para o caminho de rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA: Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter informações, consulte Adicionar uma conta de nuvem.**
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.

Opção	Caixa de texto	Descrição
	Nome da pasta	Digite um nome para a pasta na qual você quer salvar os dados arquivados; por exemplo, Rapid-Recovery -Archive- [DATA DE CRIAÇÃO] - [HORA DE CRIAÇÃO].

5 Clique em **Avançar**.

6 Na página **Máquinas** do assistente, selecione quais máquinas protegidas ou máquinas que contêm os pontos de recuperação que você deseja arquivar. Limpar as máquinas que você não quer arquivar.

7 Clique em **Avançar**.

8 Na página **Programa**, selecione uma das seguintes opções na lista suspensa **Enviar dados**:

- Diariamente
- Semanalmente
- Mensalmente

9 Insira as informações descritas na tabela a seguir dependendo de sua seleção da Etapa 8.

Tabela 43. Enviar as opções de dados

Opção	Caixa de texto	Descrição
Diariamente	Na hora	Selecione a hora do dia que você deseja criar o arquivo diário.
Semanalmente	No dia de semana	Selecione um dia da semana no qual deseja criar automaticamente o arquivo.
	Na hora	Selecione a hora do dia que você deseja criar o arquivo diário.
Mensalmente	No dia do mês	Selecione o dia do mês no qual deseja criar automaticamente o arquivo.
	Na hora	Selecione a hora do dia que você deseja criar o arquivo diário.

10 Opcionalmente, para adiar o arquivamento e retomar posteriormente, selecione **Pausar o arquivamento inicial**.

NOTA: Talvez você deseje pausar o arquivo agendado se precisar de tempo para preparar o local de destino antes de arquivar os resumos. Se você não selecionar essa opção, o arquivamento começa no horário agendado.

11 Clique em **Avançar**.

12 Na página **Opções**, use a lista suspensa **Reciclar ação** para selecionar uma das opções descritas na tabela a seguir:

Tabela 44. Opções de reciclagem de arquivo

Caixa de texto	Descrição
Incremental	Permite que você adicione pontos de recuperação a um arquivo existente. Compara pontos de recuperação para evitar duplicação de dados que já existem no arquivo.
Substituir este Core	Substitui quaisquer dados arquivados preexistentes pertencentes a este core, porém deixa os dados de outros cores intactos.
Apagar completamente	Apaga todos os dados arquivados do diretório antes de gravar o novo arquivo.

13 Você pode opcionalmente selecionar **Criar cadeias de pontos de recuperação (corrigir órfãos)**.

14 Clique em **Concluir**.

O Rapid Recovery aplica-se às suas alterações no arquivo.

Pausar ou retomar um arquivo programado

Se você já tiver um trabalho de arquivamento programado, você pode pausar ou retomar esta ação, conforme necessário.

Pode haver vezes que deseje pausar um trabalho de arquivamento programado, como quando precisar alterar o local do arquivo de destino. Se você optou anteriormente por pausar o arquivamento, ao executar o procedimento Criar um arquivo, você pode retomar o arquivamento programado mais tarde. Execute as etapas do procedimento a seguir para pausar ou retomar o arquivo agendado.

1 No Console do Rapid Recovery Core, clique no menu  **Mais** na barra de ícones e, em seguida, selecione **Arquivos**.
2 Na página **Arquivos**, sob Arquivos programados, realize um dos procedimentos a seguir:
   - Selecione o arquivo de preferência, e depois clique em uma das seguintes ações disponíveis:
     - Pause
     - Resume
   - Ao lado do arquivo de preferência, clique no menu suspenso e em uma das seguintes ações disponíveis, conforme adequado:
     - Pause
     - Resume

   O status do arquivo é exibido na coluna Programar.

Forçar um trabalho de arquivo

Usando esse procedimento, você pode forçar o Rapid Recovery a realizar um trabalho de arquivo programado a qualquer momento.

Para forçar um trabalho de arquivo, você precisa ter um arquivo programado no Core.

1 No Rapid Recovery Core Console, na barra de ícones, clique no menu suspenso  **Mais** e, em seguida, selecione **Arquivos**.
2 Na página Arquivos, em Arquivos programados, clique no menu suspenso ao lado do arquivo que deseja forçar e clique em **Forçar**.
   O Rapid Recovery arquiva os pontos de recuperação de acordo com as configurações que você escolher para o arquivo, independentemente da hora definida para o arquivo programado.

Verificar um arquivo

A verificação de um arquivo verifica se um arquivo e seu conteúdo estão suficientemente íntegros para recuperação.

Você pode examinar um arquivo quanto à integridade de sua estrutura, dos segmentos de dados e dos arquivos do índice pela realização de uma verificação de arquivo. A verificação de arquivo verifica a presença de todos os arquivos necessários dentro do arquivo e a integridade dos arquivos. Para realizar uma verificação do arquivo, execute as etapas do procedimento a seguir.

1 No Rapid Recovery Core Console, clique no menu suspenso  **Mais** na barra de ícone e selecione **Arquivos**.
2 Na página **Arquivos**, clique em **Verificar**.
   A caixa de diálogo **Check Archive** (Verificar arquivamento) é exibida.
3 Para **Tipo de local**, selecione uma das seguintes opções a partir da lista suspensa:
   - Local
   - Rede
   - Nuvem

4 Com base no tipo de local selecionado na Etapa 3, insira os detalhes do arquivo, conforme descrito na seguinte tabela.

Tabela 45. Detalhes do arquivo

Opção	Caixa de texto	Descrição
Local	Local	Insira o caminho para o arquivo.
Rede	Local	Insira o caminho para o arquivo.
	Nome de usuário	Insira o nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira a senha para o caminho da rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA: Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter informações, consulte Adicionar uma conta de nuvem.**
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Selecione a pasta na qual os dados arquivos estão salvos; por exemplo, Rapid Recovery -5-Arquivo-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

5 Marque ou desmarque as verificações descritas na seguinte tabela. Por padrão, todas as opções são selecionadas.

NOTA: Não desmarque todas as verificações. Você deve selecionar pelo menos uma opção.

Opção	Descrição
Offsets de mapeamento de arquivos de índice	Essa opção verifica se todos os dados na estrutura interna do arquivo estão no local correto.
Integridade da estrutura	Essa opção verifica a presença de determinados arquivos internos e a estrutura da pasta do arquivo. Se algum arquivo ou pasta estiver ausente, a verificação apresentará falha.
Integridade da soma de verificação	Essa opção verifica a integridade dos segmentos de dados no arquivo para garantir a integridade dos segmentos.

6 Clique em **Verificar arquivo**.

O Rapid Recovery verifica o arquivo de acordo com suas seleções.

Anexar um arquivo

Anexar um arquivo permite ver os pontos de recuperação do arquivo.

Você deve ter um arquivo preexistente criado no Rapid Recovery Core 6.0.1 ou posterior para concluir esse procedimento. Para obter mais informações, consulte Criar um arquivo.

Quando você anexa um arquivo, o nome do arquivo fornecido aparece como um menu do arquivo no menu de navegação à esquerda do Core Console. Cada máquina protegida com pontos de recuperação do arquivo é listada separadamente abaixo do menu do arquivo. Você pode clicar em qualquer nome da máquina no arquivo e navegar em seus pontos de recuperação. Você pode também realizar as mesmas ações como quaisquer outros pontos de recuperação visíveis no seu Core.

Anexar o arquivo também armazena em cache as credenciais para acessar as informações. Até que você exclua a definição do arquivo anexado, pode facilmente reanexar e destacar o arquivo, tornando seus pontos de recuperação facilmente acessíveis.

Use esse procedimento para anexar um arquivo.

1 No Rapid Recovery Core Console, clique no menu  **Arquivo** e, em seguida, selecione  **Anexar arquivo**.

A caixa de diálogo **Anexar arquivo** é exibida.

2 Na caixa de texto **Nome**, insira um nome para este arquivo anexado.

O valor que você digita neste campo é mostrado no menu de navegação à esquerda como o nome do menu do arquivo.

Segundo as melhores práticas de nomes de exibição, o nome do arquivo deve conter entre 1 e 64 caracteres alfanuméricos, incluindo espaços. Não use caracteres proibidos. nem frases proibidas.

3 Na lista suspensa **Tipo de local**, selecione o tipo de local do arquivo entre as seguintes opções:

- Local
- Rede
- Nuvem

4 Digite os detalhes para o arquivamento conforme descrito na tabela a seguir com base no tipo de local selecionado na Etapa 3.

Tabela 46. Detalhes do tipo do local

Opção	Caixa de texto	Descrição
Local	Local	Digite o caminho para o arquivo; por exemplo, **D:\Work\Archive**.
Rede	Local	Digite o caminho para o arquivo; por exemplo, **\\servername\sharename**.
	Nome de usuário	Insira o nome de usuário para o login no compartilhamento de rede.
	Senha	Insira a senha para o login no compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA: Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.**
	Contêiner	Selecione o contêiner do arquivo associado à sua conta no menu suspenso.
	Nome da pasta	Insira o nome da pasta dos dados arquivados; por exemplo, Rapid-Recovery-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

5 Clique em **Anexar**.

O arquivo é anexado a este Core e monta o conteúdo como um sistema de arquivos.

Importar um arquivamento

Você pode usar esse procedimento para importar um arquivo por vez, ou agendar a importação de um arquivo de modo recorrente.

Quando quiser recuperar dados arquivados, é possível importar todo o arquivo para um local especificado.

CUIDADO: Realize essa etapa apenas após uma análise cuidadosa. Importar um arquivo repreenche o repositório com os conteúdos do arquivo, substituindo novos dados no repositório desde que o arquivo foi obtido.

Para importar um arquivo, realize as etapas do procedimento a seguir.

1 Na barra de menu do Rapid Recovery Core Console, clique no menu suspenso  **Archive (Arquivo)** e depois selecione **Import Archive (Importar arquivo)**.

O **assistente Import Archive (Importar arquivo)**.

2 Na página **Import Type** (Tipo de importação) do assistente, selecione uma das opções a seguir:

- One-time import (Importação única)
- Continuous import (by schedule) (Importação contínua, por programação)

3 Clique em **Avançar**.

4 Na página **Location (Local)**, selecione o local do arquivo que você deseja importar na lista suspensa e depois insira as informações como descrito na tabela a seguir:

Tabela 47. Opções de tipo de local de arquivo importado

Opção	Caixa de texto	Descrição
Local	Local	Digite o local para a saída. É usado para definir o caminho do local onde você quer salvar o arquivamento; por exemplo, d:\trabalho\arquivamento.
Rede	Local	Digite o local para a saída. É usado para definir o caminho do local onde você quer salvar o arquivamento; por exemplo, \\nome_do_servidor\nome_de_compartilhamento.
	Nome de usuário	Digite um nome de usuário. Ele será usado para determinar as credenciais de login para o compartilhamento de rede.
	Password (Senha)	Digite uma senha para o caminho de rede. Ela será usada para determinar as credenciais de login para o compartilhamento de rede.
Cloud (Nuvem)	Account (Conta)	Selecione uma conta na lista suspensa. **NOTA: Para selecionar uma conta na nuvem, você deve adicioná-la no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.**
	Container (Contêiner)	Selecione no menu suspenso um contêiner associado à sua conta.
	Folder Name (Nome da pasta)	Insira um nome para a pasta na qual você deseja salvar os dados arquivos.

5 Clique em **Avançar**.

6 Na página **Archive Information (Informações de arquivo)** do assistente, se quiser importar toda máquina incluída no arquivo, selecione **Import all machines (Importar todas as máquinas)**.

7 Realize uma das opções a seguir com base em sua seleção:

- Se você selecionou a opção **One-time import (Importação única)** na etapa 2, a opção **Import all machines (Importar todas as máquinas)** na etapa 6) e todas as máquinas estão presentes no Core (como máquinas protegidas, replicadas ou apenas de pontos de recuperação), prossiga para a etapa 12
- Se você selecionou a opção **Continuous import (Importação contínua)** na etapa 2, a opção **Import all machines (Importar todas as máquinas)** na etapa 6) e no mínimo uma máquina não está presente no Core (como máquina protegida, replicada ou apenas de pontos de recuperação), clique em **Next (Avançar)** e prossiga para a etapa 9
- Se você não importou todas as máquinas na etapa 6, clique em **Next (Avançar)** e continue para a etapa 8.

8 Na página **Machines (Máquinas)**, selecione as máquinas que você deseja importar do arquivo.

- Se você selecionou a opção **One-time import (Importação única)** na etapa 2 e no mínimo uma máquina não está presente no Core (como máquina protegida, replicada ou apenas de pontos de recuperação), use as listas suspensas para selecionar um repositório para cada máquina que deseja importar e depois prossiga para a etapa 12.
- Se todas as máquinas estiverem presentes no Core (como máquinas protegidas, replicadas ou apenas de pontos de recuperação), prossiga para a etapa 12.

9 Clique em **Avançar**.

10 Na página **Repository (Repositório)**, realize uma das seguintes opções:

- Se um repositório estiver associado ao Core, selecione no mínimo uma das opções na tabela a seguir.

Tabela 48. Opções de repositório

Opção	Descrição
Use an existing repository (Usar um	Selecione um repositório atualmente associado a esse Core na lista suspensa.

Opção	Descrição
repositório existente).	
Create a Repository (Criar um repositório)	Na caixa de texto Server (servidor), insira o nome do servidor no qual você deseja salvar um novo repositório (por exemplo, nome de servidor ou host local) e depois consulte Como criar um repositório DVM.

- Se nenhum repositório estiver associado ao Core, insira o nome do servidor no qual você deseja salvar um novo repositório (por exemplo, nome de servidor ou host local) e depois consulte Como criar um repositório DVM.

11 Se você escolheu a opção **Continuous import (by schedule) (Importação contínua, por programação)** na etapa 2, na página **Schedule (Programação)**, selecione as opções descritas na tabela a seguir.

Tabela 49. Schedule import options (Opções de importação programada)

Opção	Descrição
Daily (Diariamente)	Clique no ícone de relógio acima e use as setas para cima e para baixo para selecionar quando você deseja que o trabalho de arquivamento comece. Se estiver usando um sistema de 12 horas, clique no botão AM ou PM para especificar o momento do dia.
Weekly (Semanalmente)	Selecione o dia da semana e depois o horário no qual você deseja que o trabalho de arquivamento comece. Se estiver usando um sistema de 12 horas, clique no botão AM ou PM para especificar o momento do dia.
Monthly (Mensalmente)	Selecione o dia do mês e o horário no qual você deseja que o trabalho de arquivamento comece. Se estiver usando um sistema de 12 horas, clique no botão AM ou PM para especificar o momento do dia.
Pause initial importing (Pausar importação inicial)	Selecione essa opção se você não deseja que o trabalho de importação comece no próximo horário programado depois de concluir o assistente. **NOTA: Você pode pausar a importação agendada se precisar de um tempo para preparar o local de destino antes que a importação seja reiniciada. Se você não selecionar essa opção, a importação iniciará no horário agendado.**

12 Clique em **Concluir**.

Eventos

O Rapid Recovery Core contém conjuntos predefinidos de eventos. Esses eventos podem ser usados para notificar os administradores de problemas críticos no Core ou com problemas em trabalhos relacionados a backups, exportação virtual, replicação e assim por diante.

Esta seção descreve como visualizar os eventos mostrados no Rapid Recovery Core Console. Você pode também aprender sobre os métodos de notificação de evento e a configuração, incluindo como configurar as notificações por e-mail. Por fim, você pode configurar as notificações para alterar por quanto tempo os logs de evento são mantidos e reduzir a notificação de eventos repetitivos.

Eventos Rapid Recovery

O Rapid Recovery Core inclui conjuntos predefinidos de eventos, que podem ser usados para notificar os administradores sobre problemas críticos no Core ou nos trabalhos de backup.

- Você define os tipos de eventos que acionam os alertas, bem como com os métodos o sistema usa para essas notificações (e-mail, alertas, e assim por diante), configurando grupos de notificação. Para obter mais informações, consulte Configurar grupos de notificação.
- Se você quiser que os administradores recebam notificações através de e-mail, além de configurar um grupo de notificação, você precisa configurar um servidor de e-mail, e configurar um modelo de notificação por e-mail. Para obter mais informações, consulte Configurar um servidor de e-mail e Configurar um modelo de notificação por e-mail, respectivamente.

- Você pode reduzir o número de eventos do mesmo tipo e escopo que aparecem na página Events (Eventos), usando o recurso de redução a repetição. O recurso de redução a repetição está ativado por padrão. Você pode desativar esse recurso, ou você pode controlar o período de tempo para o qual os eventos são combinados em uma única ocorrência no log de eventos. Para obter mais informações, consulte Sobre a configuração da redução de repetição.
- Você pode controlar como as informações de eventos longos e o históricos são retidos na página Eventos do Core console. Para obter mais informações, consulte Configurar retenção de eventos.

Como exibir eventos usando tarefas, alertas e registros

No Core Console, você pode mostrar eventos do Core e ver eventos de uma máquina protegida ou replicada específica.

A página **Eventos** no Core Console exibe um registro de todos os eventos relacionados ao Rapid Recovery Core. Para acessar e exibir eventos do Core, clique em  (Eventos).

A página **Eventos** de uma máquina replicada ou protegida específica exibe um log de eventos relacionados a essa máquina específica. Para acessar e mostrar eventos de uma máquina selecionada, clique no nome da máquina no menu Máquinas protegidas e, na página **Resumo** da máquina, clique no menu **Eventos**.

O conteúdo da página Eventos (no Core ou em uma máquina especificada) é dividido em três seções: Tarefas, Alertas e Registro. Essas visualizações permitem filtrar detalhes sobre diversos eventos conforme apropriado.

É possível definir a forma de notificação de vários eventos configurando os grupos de notificação. Para obter mais informações, consulte Configurar grupos de notificação.

Conclua as etapas nos procedimentos abaixo para exibir tarefas, alertas ou todos os registros de todos os eventos:

- Visualizar tarefas
- Visualizar alertas
- Visualizar todos os eventos

Visualizar tarefas

Uma tarefa é um trabalho que o Rapid Recovery Core deve realizar, como transferir dados em uma cópia de segurança programada regular ou executar uma restauração a partir de um ponto de recuperação.

Quando uma tarefa está em execução, ela é relacionada no menu suspenso **Tarefas em execução** no alto do Core Console. Clicar em uma tarefa em execução abre a caixa de diálogo Monitorar tarefa ativa.

Também é possível visualizar todas as tarefas do Rapid Recovery Core ou todas as tarefas associadas a uma máquina específica.

1. Para visualizar todas as tarefas para o Rapid Recovery Core, na barra de ícones, clique em  (Eventos).
   Se desejar visualizar as tarefas de uma máquina protegida específica, acesse a página **Resumo** da máquina especificada e clique no menu **Eventos**.
2. Para visualizar apenas as tarefas, no canto superior esquerdo da página, clique em **Tarefas**. Essa é a exibição padrão.
   A lista de eventos é filtrada para exibir apenas as tarefas do Core ou da máquina selecionada.
3. Como opção, para filtrar a lista de tarefas por palavra-chave, data inicial, data final ou qualquer combinação, faça o seguinte:
   a. Para filtrar por palavra-chave, insira-a na caixa de texto **Pesquisar palavra-chave**.
      Por exemplo, você pode filtrar por palavras-chave como "executando," "arquivo" ou "transferência".
   b. Para filtrar por data e hora inicial, insira-as utilizando uma das seguintes opções:
      - Na caixa de texto **De**, digite a data e hora em formato MM/DD/AAAA HH:MM AM/PM. Por exemplo, para pesquisar a partir do primeiro dia de janeiro de 2016 às 8h da manhã, insira 01/01/16 08:00 AM.

- Para selecionar a data e a hora atuais, clique em widget **Calendário** na caixa de texto **De** e clique na data atual. A hora atual será exibida automaticamente.
- Clique em widget **Calendário**, selecione a data e clique em widget relógio e selecione o tempo desejado usando os controles. Clique fora do calendário para aceitar as alterações selecionadas.

c Para refinar ainda mais a lista de tarefas que aparece, você também pode definir uma data e hora final no mesmo formato.

A lista de tarefas é filtrada imediatamente com base nos critérios selecionados.

4 Como opção, você pode filtrar as tarefas que aparecem na lista da seguinte forma:

Opção	Descrição
	Para ver somente as tarefas ativas, clique no ícone **Tarefas ativas**.
	Para ver somente as tarefas que estão na fila para serem executadas, clique no ícone **Tarefas em fila**.
	Para ver somente as tarefas que estão esperando para serem executadas, clique no ícone **Tarefas em espera**.
	Para ver somente as tarefas que foram concluídas, clique no ícone **Tarefas concluídas**.
	Para ver somente as tarefas com falha, clique no ícone **Tarefas com falha**.

5 Para exportar a lista de tarefas, selecione um formato na lista e clique em **Exportar**. Na caixa de diálogo resultante, confirme a exportação e clique em **OK**.

É possível exportar usando os seguintes formatos:

Tabela 50. Formatos de exportação

Formato	Descrição
PDF	Formato portátil de documento (padrão formato de exportação)
HTML	Formato de página da Web
CSV	Valores separados por vírgula
XLS	Pasta de trabalho do Microsoft Excel 1997 - 2003
XLSX	Pasta de trabalho do Excel

O arquivo do tipo selecionado é baixado para o local padrão no servidor Core.

6 Clique em ícone **Detalhes do trabalho** de qualquer tarefa para iniciar uma nova janela com os detalhes da tarefa, incluindo:

- Status
- Trabalho total (tamanho ou porcentagem concluída)
- Data e hora de início
- Data e hora de término
- Taxa
- Tempo decorrido
- Fase (para filhos tarefas)

Visualizar alertas

Um alerta é uma notificação relacionada a uma tarefa ou evento. Os tipos de alertas incluem erros, avisos ou informações.

Você pode visualizar um registro de alertas importantes do Rapid Recovery Core ou associados a uma máquina específica.

1 Para visualizar os alertas do Rapid Recovery Core, na barra de ícones, clique em  (Eventos) e, em seguida, clique em **Alertas**.

Se você deseja visualizar os alertas de uma máquina protegida específica, navegue até a página **Resumo** da máquina especificada, clique no menu **Eventos** e clique em **Alertas**.

A lista de eventos é filtrada para exibir apenas os alertas importantes do Core ou da máquina selecionada.

2 Como opção, para filtrar a lista dos alertas importantes por data inicial, data final, descrição da mensagem de alerta ou qualquer combinação, faça o seguinte:

a Para filtrar por data e hora inicial, insira-as utilizando uma das seguintes opções:

- Na caixa de texto **De**, digite a data e hora no formato MM/DD/AAAA HH:MM AM/PM. Por exemplo, para pesquisar a partir do primeiro dia de janeiro de 2016 às 8h da manhã, insira 01/01/16 08:00 AM.
- Para selecionar os dados atuais e a hora, clique no widget  na caixa de texto **De** e, em seguida, clique na data atual. A hora atual aparecerá automaticamente.
- Clique no widget  **Calendário**, selecione a data e, em seguida, clique no widget  Relógio e selecione a hora desejada usando os controles. Clique fora do calendário para aceitar as alterações selecionadas.

b Para filtrar por descrição da mensagem de alerta, insira a descrição na caixa de texto **Pesquisar mensagem**.

Por exemplo, para ver apenas alertas relacionados aos agentes, digite "agente;' para ver alertas relacionados às transferências, digite "transferência" e assim por diante.

c Para refinar ainda mais a lista de alertas exibida, você também pode definir uma data e hora final no mesmo formato.

A lista de alertas é filtrada imediatamente com base nos critérios selecionados.

3 De forma opcional, se você quiser remover todos os alertas, clique em **Descartar tudo**.

Visualizar todos os eventos

Você pode visualizar todos os eventos do Rapid Recovery Core ou todos os eventos associados a uma máquina específica.

1 Para visualizar um registro de todos os eventos do Rapid Recovery Core, na barra de ícones clique em  (Eventos) e, em seguida, clique em **Registro**. Para visualizar todos os eventos do Rapid Recovery Core, navegue até a página inicial do Rapid Recovery Core e, em seguida, clique em  (Eventos).

Se você deseja visualizar um registro de todos os eventos de uma máquina protegida específica, navegue até a página **Resumo** da máquina especificada, clique no menu **Eventos** e clique **Registro**.

2 Como opção, para filtrar a lista de todos os eventos por data inicial, data final, descrição da mensagem de alerta ou qualquer combinação, faça o seguinte:

a Para filtrar por data e hora inicial, insira-as utilizando uma das seguintes opções:

- Na caixa de texto **De**, digite a data e hora no formato MM/DD/AAAA HH:MM AM/PM. Por exemplo, para pesquisar a partir do primeiro dia de janeiro de 2016 às 8h da manhã, insira 01/01/16 08:00 AM.
- Para selecionar os dados atuais e a hora, clique no widget  na caixa de texto **De** e, em seguida, clique na data atual. A hora atual aparecerá automaticamente.
- Clique no widget  **Calendário**, selecione a data e, em seguida, clique no widget  Relógio e selecione a hora desejada usando os controles. Clique fora do calendário para aceitar as alterações selecionadas.

b Para filtrar por descrição da mensagem de alerta, insira a descrição na caixa de texto **Pesquisar mensagem**.

Por exemplo, para ver apenas alertas relacionados aos agentes, digite "agente;' para ver alertas relacionados às transferências, digite "transferência" e assim por diante.

c Para refinar ainda mais a lista de eventos exibida, você também pode definir uma data e hora final no mesmo formato.

A lista de eventos é filtrada imediatamente com base nos critérios selecionados.

Como entender as notificações de e-mail

Você pode configurar o Rapid Recovery Core para notificar você sobre eventos específicos, enviando uma mensagem de e-mail para um endereço de e-mail que você especificar. Os eventos que acionam os alertas estão definidos no grupo de notificação, assim como os outros métodos de notificação.

NOTA: Os grupos de notificação precisam ser estabelecidos independentemente do fato de você usar e-mail como um método de notificação. Para obter mais informações, consulte Configurar grupos de notificação.

Se você optar por e-mail como uma das opções de notificação, você precisa também configurar um servidor de e-mail SMTP. O Rapid Recovery Core usa o servidor que você definir para enviar alertas com base nos parâmetros no grupo de notificação.

Além disso, você também precisa definir um modelo de notificação por e-mail . O Core usa este modelo para definir a linha de assunto do e-mail para cada alerta, e o conteúdo no corpo da mensagem. O modelo tem configurações padrão; você pode usar o padrão como está, ou você pode testar e fazer modificações para atender às suas necessidades.

Esta seção inclui os seguintes tópicos:

- Configurar um servidor de e-mail
- Configurar um modelo de notificação por e-mail

Configurar um servidor de e-mail

Execute as etapas deste procedimento para configurar um server de e-mail.

NOTA: Você também deve configurar as definições de grupo de notificação, incluindo a ativação da opção Notificar por e-mail antes que as mensagens de alertas de e-mail sejam enviadas pelo sistema. Para obter mais informações sobre especificação de eventos para recebimento de alertas de e-mail, consulte Configurar grupos de notificação.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Configurações) e siga uma das seguintes opções:

- Na lista de configurações do Core no lado esquerdo da página Configurações, clique em **Servidor de SMTP**.
- Role para baixo no lado direito da página Configurações até visualizar o cabeçalho **Servidor de SMTP**.

As configurações do core do servidor de SMTP são exibidas.

3 Clique na configuração que deseja alterar.

A configuração selecionada se torna editável.

4 Insira as informações de configuração conforme descrito na tabela a seguir.

Opção	Descrição
Server de SMTP	Digite o nome do server de e-mail a ser usado pelo modelo de notificação de e-mail. A convenção de nomenclatura inclui o nome do host, domínio e sufixo; por exemplo, smtp.gmail.com.
De	Insira o endereço de e-mail de devolução. Usado para especificar o endereço de e-mail de devolução para o modelo de notificação de e-mail; por exemplo, noreply@localhost.com.
Nome de usuário	Insira um nome de usuário do server de e-mail.
Senha	Insira a senha associada ao nome de usuário necessário para acessar o server de e-mail.
Port	Insira um número de porta. Utilizado para identificar a porta do server de e-mail; por exemplo, porta 587 para o Gmail. O padrão é 25.

Opção	Descrição
Tempo limite (segundos)	Insira um valor de número inteiro para especificar quanto tempo deve-se tentar se conectar ao server de e-mail. Utilizado para estabelecer o tempo em segundos antes de ocorrer o tempo limite. O padrão é 60 segundos.
TLS	Selecione essa opção se o server de e-mail usar uma conexão segura, como Transport Layer Security (TLS) ou Secure Sockets Layer (SSL).

5 Para cada configuração, quando estiver satisfeito com suas alterações, clique em Para salvar a alteração e sair do modo de edição ou clique em Para sair do modo de edição sem salvar.

CUIDADO: Se você não confirmar cada alteração, suas configurações não serão alteradas.

6 Clique em **Enviar e-mail de teste** e faça o seguinte:

a Na caixa de diálogo **Enviar e-mail de teste**, insira um endereço de e-mail de destino para a mensagem de teste e clique em **Enviar**.

b Se a mensagem de teste falhar, saia da caixa de diálogo de erro e da caixa de diálogo **Enviar e-mail de teste** e revise suas configurações de servidor de e-mail. Em seguida, envie a mensagem de teste novamente.

c Quando a mensagem de teste for bem-sucedida, clique em **OK** para confirmar o êxito da operação.

d Verifique a conta de e-mail para a qual você enviou a mensagem com o e-mail de teste.

Configurar um modelo de notificação por e-mail

Ao ativar as notificações de eventos do Rapid Recovery por e-mail, um modelo padrão é criado para você automaticamente. O servidor de e-mail SMTP definido para o core usa esse modelo para enviar notificações sobre eventos do Rapid Recovery por e-mail.

Esse tópico descreve o processo de configurar o modelo de notificação de e-mail padrão ou de personalização do conteúdo. Usando a opção Restore Default (Restaurar padrão) é possível restaurar as alterações ao modelo de notificação padrão a qualquer momento.

CUIDADO: Modifique o modelo por sua conta e risco. Você é responsável por testar quaisquer modificações ao modelo. Só o modelo padrão é compatível.

Realize as etapas neste procedimento para configurar um modelo de notificação por e-mail.

NOTA: Você também deve configurar um servidor de e-mail e definições de grupo de notificação, incluindo ativar a opção Notify by email (Notificar por e-mail), antes que mensagens de alerta de e-mail sejam enviadas. Para obter mais informações sobre como configurar um servidor de e-mail para enviar alertas, consulte Configurar um servidor de e-mail. Para obter mais informações sobre como especificar eventos para receber alertas por e-mail, consulte Configurar grupos de notificação.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em (Mais), e, em seguida, selecione **Notificações**
A página **Notifications (Notificações)** é mostrada.

3 No painel Email Settings (Configurações de e-mail), clique em **Alterar**.
A caixa de diálogo **Edit Email Notification Configuration (Editar configuração de notificação por e-mail)** é mostrada.

4 Selecione **Ativar notificações por e-mail**.
O modelo de e-mail é ativado e fica visível. Os valores do modelo de e-mail padrão são descritos na etapa a seguir.

5 Confira o conteúdo da caixa de diálogo Edit Email Notification Configuration (Editar configuração de notificação de e-mail) e determine se o conteúdo padrão atende às suas necessidades.

Opção	Descrição
Ativar notificações por e-mail	Essa configuração ativa ou desativa o modelo de notificação por e-mail. • Para ativar as notificações por e-mail, marque essa opção.

Opção	Descrição
	• Para desativar as notificações por e-mail, desmarque essa opção.
Email Subject (Assunto do e-mail)	Os conteúdos desse campo de texto controlam a linha de assunto para mensagens de e-mail enviadas como notificações de eventos do sistema. A linha de assunto de e-mail padrão é: `<hostName> <level>: <name> for <agentName>`

E-mail	Os conteúdos dessa área de texto controlam o corpo para mensagens de e-mail enviadas como notificações de eventos do sistema. A mensagem do corpo de e-mail padrão é:
	`<shortCompanyName> <coreProductName> on <hostName> has reported the <level> event "<name>"`
	
	`Date/Time: <localTimestamp>`
	
	`<message>`
	
	`<if(details.errorDetails)>`
	`<details.ErrorDetails.Message>`
	
	`<details.ErrorDetails.Details>`
	`<endif>`
	`---`
	
	`About this event: <description>`
	
	`<coreAdminUrl>`

Enviar de e-mail de teste	Clicar neste botão envia uma mensagem de e-mail de teste para o endereço de e-mail especificado na caixa de diálogo **Send Test Email (Enviar e-mail de teste)** resultante.
Restore Defaults	Clicar neste botão remove quaisquer alterações personalizadas do modelo de e-mail e restaura os campos Email Subject (Assunto de e-mail) e Email (E-mail) com os conteúdos padrão descritos nesta tabela.
OK	Clicar neste botão confirma e salva as configurações na caixa de diálogo Edit Email Notification Configuration (Editar configuração de notificação de e-mail).
Cancelar	Clicar neste botão cancela quaisquer alterações na caixa de diálogo Edit Email Notification Configuration (Editar configuração de notificação de e-mail).

6 Se quiser personalizar o modelo de e-mail, faça alterações no texto ou variáveis descritas na etapa precedente. As variáveis usadas no padrão são descritas na tabela a seguir.

Opção	Descrição
nome de host	O nome de host do core
detalhes	Os detalhes do objeto do evento específico.
nome do agente	O nome da máquina protegida associada a esse evento, se o evento possuir um escopo de máquina protegida única.
nome do repositório	O nome do repositório associado a esse evento, se o evento possui escopo de repositório.
resumo de trabalho	O resumo do trabalho associado a esse evento, se o evento possui escopo de trabalho.
nome de core escravo remoto	O nome do repositório de destino remoto associado a esse evento, se o evento possui escopo de core de destino.
nome de core mestre remoto	O nome do repositório de origem remoto associado a esse evento, se o evento possui escopo de core de origem.
nome do produto	O nome do produto, 'Rapid Recovery Core'. Esse nome de produto pode ser alterado para personalização de marca usando etiquetas brancas.
nome da empresa	O nome da empresa que vende o produto.

7 Na caixa de texto **Email Subject (Assunto do e-mail)**, insira um assunto para o modelo do e-mail.

O assunto do e-mail é usado para definir o assunto do modelo de notificação de e-mail, por exemplo, <nomedehost> - <nível> <nome>.

8 Na caixa de texto **Email (E-mail)**, insira as informações do corpo do modelo que descrevam o evento, quando ocorreu e sua gravidade.

9 Clique em **Send Test Email (Enviar e-mail de teste)** e depois faça o seguinte:

a Na caixa de diálogo Send Test Email (Enviar e-mail de teste), digite um endereço de e-mail de destino para a mensagem de teste e depois clique em **Send (Enviar)**.
b Se a mensagem de teste falhar, feche a caixa de diálogo de erro e da caixa de diálogo Send Test Email (Enviar e-mail de teste), clique em **OK** para salvar as configurações de modelo de e-mail atual. Em seguida, modifique suas configurações de servidor de e-mail como descrito no procedimento Configurar um servidor de e-mail. Lembre-se de digitar novamente a senha para a conta de e-mail. Salve essas configurações e depois retorne para esse procedimento.
c Depois que a mensagem for enviada com sucesso, clique em **OK** para confirmar que tudo correu bem.
d Verifique a conta de e-mail para a qual você enviou a mensagem de e-mail de teste.

Depois que estiver satisfeito com os resultados de seus testes, retorne para a caixa de diálogo Edit Email Notification Configuration (Editar configuração de notificação de e-mail) e clique em **OK** para fechar a caixa de diálogo e salvar suas configurações.

Grupos de notificação, configurações de SMTP e modelos de notificação para eventos do sistema

Os grupos de notificação permitem que você defina conjuntos de eventos específicos para os quais os usuários são alertados, e a forma como qual ocorra a notificação. Para configurar ou editar grupos de notificação, consulte Configurar grupos de notificação.

Você precisa também configurar as configurações do servidor SMTP se você quer enviar alertas por e-mail. Para obter mais informações sobre a definição das configurações do servidor de e-mail, consulte Configurar um servidor de e-mail.

Ao enviar notificação de eventos, o sistema usa uma notificação por e-mail. Você pode personalizar este modelo. Para obter mais informações sobre como configurar ou personalizar a notificação por e-mail, consulte Configurar um modelo de notificação por e-mail.

Configurar grupos de notificação

NOTA: Deve-se também configurar as definições do server SMTP se desejar enviar alertas como mensagens de e-mail, conforme descrito neste procedimento. Para obter mais informações sobre como definir as configurações do servidor de e-mail, consulte Configurar um servidor de e-mail.

Os grupos de notificação permitem definir conjuntos de eventos específicos sobre os quais os usuários são alertados e a maneira como essa notificação ocorre. Você pode configurar os seguintes métodos para o envio de alertas:

- Por e-mail
- No log de eventos do Windows
- Uso de syslogd
- Uso de alertas do sistema
- Usar alertas
- Usar trap de SNMP

Você pode configurar mais de um grupo de notificação com diferentes parâmetros de notificação.

Os grupos de notificação podem ser definidos no nível do Core ou para cada máquina protegida específica.

Execute as etapas deste procedimento para configurar os grupos de notificação para alertas.

1 Realize um dos procedimentos a seguir:

- Para definir as notificações no nível do Core, a partir da barra de ícone, clique em (Mais) e selecione **Notificações**.
  A página **Notificações** é exibida.
- Para definir as notificações para uma máquina protegida específica, faça o seguinte:
  1 No menu Máquinas protegidas, clique na máquina em relação à qual deseja especificar notificações.

A página **Grupos de notificação personalizados** é exibida.

2 Na página Resumo da máquina protegida, no menu suspenso Mais, selecione **Notificações**.

A página **Grupos de notificação personalizados** é exibida.

2 Clique em **Adicionar grupo**

A caixa de diálogo **Adicionar grupo de notificação** é exibida.

Os grupos de notificação permitem definir conjuntos de eventos específicos sobre os quais os usuários são alertados e a maneira como essa notificação ocorre. Você pode configurar os seguintes métodos para o envio de alertas:

A caixa de diálogo **Adicionar grupo de notificação** contém uma área de descrição geral e duas guias:

- Habilitar alertas
- Opções de notificação

3 Na área de descrição geral, insira as informações básicas para o grupo de notificação, conforme descrito na tabela a seguir.

Opção	Descrição
Nome	Insira um nome para o grupo de notificação de eventos. Estas informações são obrigatórias. **CUIDADO: O valor inserido para o nome do grupo de notificação não poderá ser alterado posteriormente.**
Descrição	Insira uma descrição que explique a finalidade do grupo de notificação de eventos. Estas informações são opcionais.

4 Na guia **Habilitar alertas**, defina o conjunto de eventos do sistema que deseja registrar em log, criar relatórios e para o qual deseja ser alertado, como segue:

Opção	Descrição
Todos os alertas	Para criar alertas para todos os eventos, selecione **All Alertas** (Todos os alertas).
Erros	Para criar alertas para erros, no menu **Selecionar tipos**, clique em **Erro**. Isso é representado por um X vermelho.
Aviso	Para criar alertas para erros, no menu **Selecionar tipos**, clique em **Aviso**. Isso é representado por um ícone amarelo de ponto de exclamação.
Informações	Para criar alertas para mensagens informativas, no menu **Selecionar tipos**, clique em **Informações**. Isso é representado por um i azul.
Restaurar padrão	Para restaurar os tipos de alerta para o padrão, no menu **Selecionar tipos**, clique em **Restaurar padrão**. Isso é representado por uma seta azul-escura virada para a esquerda.

5 Para criar alertas para um tipo de evento específico (erro, aviso ou mensagem informativa), faça o seguinte:

a Se a opção **Todos os alertas** não exibir grupos de alerta, clique no símbolo de ângulo para a direita **>** que precede o rótulo Todos os alertas. O símbolo muda para uma seta voltada para baixo, e a visualização se expande para exibir os grupos.

b Em seguida, clique no símbolo de ângulo para a direita **>** ao lado de qualquer grupo de alerta específico para exibir os eventos relacionados no grupo.

As categorias de grupo de eventos incluem:

- Arquivo
- Relatório automático
- Capacidade de anexação
- Atualização automática
- Repositório de backup
- CD de inicialização
- Nuvens
- Clusters
- Serviço do Core
- Retenção do banco de dados
- Cache de deduplicação

- Repositório de DVM
- Exchange
- Exportar
- Trabalhos
- Aplicação de licença
- Montagem local
- Truncamento de log
- Metadados
- Trabalhos noturnos
- Notificação
- Persistir estado do core
- PowerShell Scripting
- Proteção
- Instalação de envio por push
- Verificação de ponto de recuperação
- Montagem remota
- Repositório comum
- Replicação
- Restaurar
- Rollup
- Arquivos programados
- Segurança
- Logs de servidor
- vSphere

- Para definir alertas para todos os eventos em cada grupo, marque a caixa de seleção **Todos os alertas**.
- Para definir alertas para todos os eventos dentro de qualquer grupo de alerta, marque a caixa de seleção ao lado desse grupo.
- Para selecionar somente alguns tipos de alerta dentro de um grupo de alerta, expanda o grupo e selecione somente os eventos específicos em relação aos quais você desejar registrar, criar relatório e definir alertas.

6 Clique na guia **Opções de notificação**.

7 Na guia **Opções de notificação**, especifique como lidar com o processo de notificação.

Opção	Descrição
Notificar por e-mail	Designe os destinatários da notificação de e-mail. É possível optar por especificar vários endereços de e-mail separados, bem como cópias carbono e ocultas. Você pode selecionar: • Para: • CC: • BCC:
Notificar pelo Log de eventos do Windows	Selecione essa opção se deseja que os alertas sejam comunicados por meio do Log de Eventos do Windows.
Notificar por syslogd	Selecione essa opção se deseja que os alertas sejam comunicados por meio de syslogd. Especifique os detalhes do syslogd nas seguintes caixas de texto: • Host: • Porta:
Notificar por alertas do sistema	Selecione esta opção se você deseja que o alerta seja exibido como uma pop-up na parte inferior direita da tela.
Notificar por meio de alertas	Selecione essa opção se desejar que os alertas sejam exibidos como janelas pop-up localizadas no lado inferior direito do Core Console.

Opção	Descrição
Notificar por trap SNMP	O Rapid Recovery Core funciona como um agente de SNMP, enviando interrupções (notificações sobre eventos específicos) para o gerenciador de SNMP. Isso permite que o Core transmita certas informações, como alertas, status do repositório e máquinas protegidas. Selecione essa opção se quiser que os eventos do Core sejam comunicados por trap de SNMP. Você também especificar um número de trap. Por exemplo, o número de interrupção padrão utilizado pelo Rapid Recovery Core é 162.

8 Clique em **OK**.

Você verá uma mensagem indicando que o nome do grupo de notificação definido não pode ser alterado após a criação do grupo. Outras propriedades dentro do grupo de notificação podem ser alteradas a qualquer momento.

- Se você estiver satisfeito com o nome do grupo, confirme essa mensagem e salve o seu trabalho.
- Se quiser alterar o nome do grupo, clique em **Não** para voltar à janela Criar grupo de notificação, atualize o nome do grupo e outras definições de grupo de notificação e salve seu trabalho.

O grupo de notificação é exibido na tabela de resumo. Você pode criar diferentes grupos de notificação usando qualquer conjunto de parâmetros.

Sobre a configuração da redução de repetição

É essencial que os administradores recebam alertas sobre certos eventos. No entanto, em certas circunstâncias, pode ser frustrante ou inconveniente receber notificações repetidas sobre um evento do qual você está ciente. Mesmo que um alerta seja gerado devido a uma falha ambiental sobre a qual você deseja saber imediatamente, é possível que a mesma condição de erro gere centenas ou milhares de eventos no log de eventos. Para reduzir a repetição no log de eventos e reduzir a inconveniência de receber repetidas notificações por e-mail para o mesmo evento no Console do Core, o Rapid Recovery inclui uma definição de redução de repetição, que é habilitada por padrão e configurada em 5 minutos. Essa definição pode ser ajustada entre 1 e 60 minutos. Também é possível desabilitá-la completamente.

Quando a redução de repetição está desabilitada, cada vez que ocorre um evento do mesmo tipo e escopo, ele é registrado no banco de dados. Independentemente do tempo decorrido desde a ocorrência anterior do evento, cada nova ocorrência é mostrada na seção Alertas da guia Eventos.

Quando a redução de repetição está habilitada (por exemplo, com o tempo padrão de cinco minutos), o evento é registrado no banco de dados de eventos e mostrado no log de alertas quando ocorre pela primeira vez. Se subsequentemente um evento do mesmo tipo e escopo é novamente registrado dentro do limite de tempo estabelecido, a contagem do evento no banco de dados aumenta em 1 para cada ocorrência repetida dentro do limite. O log mostra na parte de Alertas da página Eventos. No entanto, ele mostra o evento apenas uma vez, com a data e a hora da ocorrência mais recente. O log de eventos não é atualizado com o mesmo evento até a expiração do limite de tempo a partir da primeira ocorrência. Por exemplo, se definido para 5 minutos e o evento ocorrer novamente 6 minutos mais tarde, ele será exibido no log e você receberá outra mensagem de e-mail.

Configurar redução de repetição

Execute as etapas deste procedimento para configurar a redução de repetição dos eventos.

1 Navegue para o Rapid Recovery Core Console. Na barra de ícones, clique em  (Mais) e selecione **Notificações**.

A página **Notificações** é exibida.

2 No painel Redução de repetição, veja as definições existentes.

3 Para ativar, desativar ou alterar o tempo limite de eventos armazenados, clique em  **Alterar**.

A caixa de diálogo **Editar redução de repetição** é exibida

4 Realize um dos procedimentos a seguir:

- Para desativar a redução de repetição, desmarque a opção **Habilitar redução de repetição**.
- Para ativar a redução de repetição, marque a opção **Habilitar redução de repetição**.

- Para alterar o limite de tempo (em minutos) para os quais os eventos idênticos repetidos são ignorados, na caixa de texto **__ minuto(s)**, insira um número entre 1 e 60.

NOTA: A opção Habilitar redução de repetição deve ser marcada para alterar esse valor.

5 Clique em **OK** para salvar as configurações e fechar a caixa de diálogo.

Configurar retenção de eventos

Eventos e trabalhos rastreados no Core são salvos por um período determinado de tempo. A definição padrão é 30 dias. Este número pode ser definido entre 0 dias e 3652 dias (aproximadamente 10 anos).

Execute as etapas deste procedimento para configurar a retenção de eventos.

1 Navegue até o Console do Rapid Recovery Core.

2 Na barra de ícones, clique em (Definições), e, em seguida, faça o seguinte:
- Na lista de definições do Core no lado esquerdo da página Definições, clique em **Conexão do banco de dados**.
- Role a tela para baixo no lado direito do da página Definições até que você possa ver o cabeçalho **Conexão do banco de dados**.

As definições de conexão do database serão exibidas.

3 Para alterar a quantidade de dias durante os quais as informações de evento serão salvas no banco de dados, clique no campo de texto **Período de retenção (dias)**, insira um valor entre 0 e 3652, e, em seguida, clique em para salvar a alteração.
O período de retenção de eventos é ajustado conforme especificado.

Recuperação automática rápida do dispositivoo

Rapid Appliance Auto Recuperação (RASR) é um processo de restauração sem sistema operacional que rapidamente restaura o seu aparelho a um estado operacional.

RASR oferece duas opções de recuperação:

- Restaurar as configurações de fábrica
- Recuperar o seu aparelho a um estado antes da falha (SO, configurações, e definições são recuperadas)

Criar a unidade USB RASR

Para criar um pen drive USB RASR:

1 Navegue até a guia **Appliance (Dispositivo)**.

2 Usando a navegação no painel esquerdo, selecione**Appliance (Dispositivo)** > **Backup**.
A janela **Create RASR USB Drive (Criar unidade USB RASR)** é mostrada.

NOTA: Insira um pen drive USB de 16 ou mais GB antes de tentar criar a chave RASR.

3 Após inserir um pen drive USB de 16 GB ou mais, clique em **Create RASR USB Drive now (Criar unidade USB RASR agora)**.
A mensagem **Prerequisite Check (Verificação de pré-requisitos)** é mostrada.
Depois dos pré-requisitos serem verificados, a janela **Create the RASR USB Drive (Criar a unidade USB RASR)** mostra o tamanho mínimo necessário para criar a unidade USB e uma **Lista de possíveis caminhos de destino**.

4 Selecione o destino e clique em **Create (Criar)**.
Uma caixa de diálogo de aviso é mostrada.

5 Clique em **Yes (Sim)**.

A chave da unidade USB RASR é criada.

6 **NOTA: Certifique-se de utilizar a função Windows Eject Drive (Unidade de ejeção do Windows) para preparar o pen drive USB para remoção. Caso contrário, o conteúdo do pen drive USB pode ser danificado e o pen drive USB não irá funcionar como o previsto.**

Remova a chave USB RASR criada para cada dispositivoo DL, etiqueta, e armazenar para uso futuro.

Executar a RASR

NOTA: A Dell recomenda que você crie uma chave USB RASR depois de configurar o dispositivoo. Para criar uma chave USB RASR, consulte a seção Como criar a chave USB RASR.

NOTA: Certifique-se de que você tem os RUU mais recentes disponíveis e podem ser acessados tanto no seu dispositivoo.

.

NOTA: Para executar a recuperação do sistema usando RASR, consulte *Como recuperar uma Dell™ DL Backup and Recovery Appliance usando Rapid Appliance Auto Recuperação (RASR)* no site Dell.com/support/home.

Para executar uma redefinição de fábrica:

1 Insira a chave USB RASR criada.
2 Reinicie o dispositivoo e selecione **Boot Manager (F11) (Gerenciador de Inicialização (F11)).**
3 No **Boot Manager Main Menu (Menu principal do Gerenciador de Inicialização)**, selecione **One-shot BIOS Boot Menu (Menu de inicialização única do BIOS)**.
4 No **Boot Manager Boot Menu (Menu de inicialização do Gerenciador de Inicialização)**, selecione a unidade USB conectada.
5 Selecione o layout de teclado.
6 Clique em **Troubleshoot (Solucionar problemas)** > **Rapid Appliance Self Recovery (Recuperação automática rápida do dispositivoo)**.
7 Selecione o sistema operacional (SO) de destino.
A RASR é aberta e a tela de **boas-vindas** é mostrada.
8 Clique em **Next (Avançar)**.
A tela de verificação **Prerequisites (Pré-requisitos)** é mostrada.

NOTA: Confirme que todo o hardware e os outros pré-requisitos foram verificados antes de executar a RASR.

9 Clique em **Next (Avançar)**.
A tela **Recovery Mode Selection (Seleção do modo de recuperação)** é mostrada com três opções:
- **System Recovery (Recuperação do sistema)**
- **Windows Recovery Wizard (Assistente de recuperação do Windows)**
- **Factory Reset (Redefinição de fábrica)**

10 Selecione a opção **Factory Reset (Redefinição de fábrica)**.
Esta opção irá recuperar o disco do sistema operacional a partir da imagem de fábrica.
11 Clique em **Next (Avançar)**.
A seguinte mensagem de advertência é mostrada em uma caixa de diálogo: `This operation will recover the operating system. All OS disk data will be overwritten.`
12 Clique em **Yes (Sim)**.
O disco do sistema operacional começa a ser restaurado de volta à redefinição de fábrica.
13 A página **RASR Concluído** é mostrada na conclusão do processo de recuperação. Clique em **Finish (Concluir)**.
14 Inicializar o sistema após restaurar.
15 **NOTA: Continue apenas se você vê o Assistente de configuração da AppAssure Appliance, caso contrário, vá para a etapa 17.**

Aguarde o Assistente de configuração AppAssure Appliance carregar, você precisafechá-lo. Feche o assistente usando o Gerenciador de tarefas do Windows.

16 Execute **launchRUU.exe** o arquivo no pacote de RUU. Siga as instruções e selecione a opção para continuar com a instalação de RUU e conclua a instalação.

17 O **dispositivoo DL Assistente de configuração é iniciado** e será o seu guia através do resto dos o processo de restauração.

O seu equipamento funciona normalmente agora.

O Local Mount Utility

Esta seção descreve como fazer download, instalar e usar o Utilitário de montagem local (LMU) do Rapid Recovery baseado no Windows para montar pontos de recuperação e explorar o conteúdo de um nível de arquivo usando uma máquina que não hospeda o Rapid Recovery Core.

Sobre o Local Mount Utility

O LMU é um aplicativo com base em Windows que pode ser obtido por download e que permite que você monte um ponto de recuperação do Rapid Recovery em um dos três modos disponíveis em qualquer máquina com Windows. Esse pequeno utilitário pode ser instalado sistemas operacionais Windows de 32 e 64 bits, e inclui os drivers rapidrecovery-vdisk (antigo aavdisk) e aavstor, mas não é executado como um serviço. Quando o utilitário é instalado, por padrão, ele é instalado no diretório **C:\Program Files\AppRecovery\Local Mount Utility**, e um atalho aparece na área de trabalho da máquina.

Embora o utilitário tenha sido projetado para acesso remoto a uma máquina Rapid Recovery Core, também é possível instalar o LMU na mesma máquina de um Rapid Recovery Core. Quando executado em um Core, o aplicativo reconhece e exibe todas as montagens desse Core, incluindo montagens realizadas por meio do Rapid Recovery Core Console. Da mesma forma, as montagens realizadas no LMU também aparecem no Core Console.

Quando o LMU é instalado na mesma máquina, como um Mailbox Restore, o LMU inicia automaticamente o Mailbox Restore quando você o usa para abrir um banco de dados do Exchange. O Mailbox Restore é o aplicativo Dell Rapid Recovery usado para restaurar itens e armazenamento de dados do Microsoft Exchange. Você pode instalá-lo no momento da instalação do LMU ou do Rapid Recovery Core. Para obter mais informações sobre o Mailbox Restore, consulte o *Guia do Usuário do Mailbox Restore do Dell Data Protection | Rapid Recovery para Microsoft Exchange*.

NOTA: As máquinas Linux usam um utilitário de linha de comando, local_mount, para consultar o Core de máquinas protegidas e seus respectivos pontos de recuperação. Da mesma forma, essa ferramenta permite que os usuários montem remotamente um volume de ponto de recuperação; permite que os usuários explorem o conteúdo do volume no nível de arquivo; e permite que os usuários restaurem arquivos individuais ou um volume inteiro a partir do ponto de recuperação, incluindo BMR do volume do sistema. Para obter mais informações, consulte Montar um volume de ponto de recuperação em máquina Linux, Restaurar volumes em uma máquina Linux usando a linha de comando e Realizar uma bare metal restore em máquinas Linux, respectivamente.

Trabalhar com máquinas Rapid Recovery Core no Utilitário de montagem local

O Utilitário de montagem local (LMU) permite que você trabalhe com um número ilimitado de máquinas Core local ou remotamente. Se você instalar o LMU em uma máquina Rapid Recovery Core, essa máquina será mostrada automaticamente no LMU como o localhost. Todos os Cores remotos adicionais aparecem como seus nomes de máquinas ou endereços IP, dependendo das informações que foram inseridas ao serem adicionadas. Com o LMU, você pode adicionar, editar e remover máquinas Core. Para obter mais informações, consulte os procedimentos a seguir:

Links relacionados

Adicionar uma máquina Core ao Local Mount Utility
Alterar as opções do Local Mount Utility
Como editar definições de conexão do Core no Local Mount Utility
Reconectar a um Core
Como remover uma máquina Rapid Recovery Core do Local Mount Utility

Adicionar uma máquina Core ao Local Mount Utility

Para montar um ponto de recuperação, é necessário adicionar uma máquina Core ao LMU. Não há limite ao número de Cores que podem ser adicionados.

Conclua o procedimento a seguir para configurar o LMU adicionando um Core.

1 Na máquina em que o LMU está instalado, inicie o LMU clicando duas vezes no ícone na área de trabalho.
2 Realize um dos procedimentos a seguir:
   - No menu Local Mount Utility, no canto superior esquerdo, clique em **Adicionar Core**.
   - Clique com o botão direito do mouse no espaço em branco do painel esquerdo e clique em **Adicionar Core**.

   A caixa de diálogo **Adicionar Core** é exibida.
3 Na caixa de diálogo **Adicionar Core**, insira as credenciais solicitadas, descritas na tabela a seguir.

Tabela 51. Credenciais do Rapid Recovery Core

Opção	Descrição
Nome do host	O nome ou o endereço IP do Core a partir do qual você deseja montar pontos de recuperação. **NOTA: Se você estiver instalando o LMU em uma máquina Rapid Recovery Core, o LMU adicionará automaticamente a máquina localhost.**
Port	O número da porta usada para se comunicar com o Core. O número de porta padrão é 8006.
Use minhas credenciais de usuário do Windows	Selecione esta opção se as credenciais que você usa para acessar o Core forem iguais às credenciais do Windows.
Use credenciais específicas	Selecione essa opção se as credenciais que você usa para acessar o Core forem diferentes das credenciais do Windows.
Nome de usuário	O nome de usuário utilizado para acessar a máquina do Core. **NOTA: Essa opção só permanecerá disponível se você escolher usar credenciais específicas.**
Senha	A senha usada para acessar a máquina do Core. **NOTA: Essa opção só permanecerá disponível se você escolher usar credenciais específicas.**

4 Clique em **Conectar.**
5 Se você estiver adicionando vários Cores, repita todas as etapas conforme necessário.

Alterar as opções do Local Mount Utility

Conclua o procedimento a seguir para alterar as opções de todos os Cores do Rapid Recovery conectados ao LMU.

1 Na interface do usuário do Local Mount Utility, clique em **Opções**.

2 Na caixa de diálogo **Opções**, você pode alterar a definição descrita na tabela a seguir.

Tabela 52. Definições do Core

Opção	Descrição
Repositório do ponto de montagem padrão	Use o botão **Procurar** ou insira um caminho para o local que você deseja usar nos pontos de recuperação de montagem.
Use minhas credenciais de conta de usuário do Windows	Selecione essa opção para usar sempre as credenciais do Windows por padrão ao se conectar a um Core.
Use credenciais específicas	Selecione essa opção para usar as seguintes credenciais para cada Core conectado: • **Nome de usuário**: digite o nome de usuário a ser usado para todas as cores. • **Senha**: digite a senha a ser usada para todas as cores.
Tempo limite de conexão (seg)	Digite o tempo em que a LMU deve continuar tentando se conectar a um Core antes da conexão expirar (em minutos : segundos : milissengundos).
Idioma	Selecione o idioma no qual você deseja que a LMU seja exibida. Você pode selecionar dentre as seguintes opções: • Inglês • Francês • Alemão • Português • Espanhol • Chinês simplificado • Japonês • Coreano

Como editar definições de conexão do Core no Local Mount Utility

Para editar as definições que você estabeleceu quando adicionou um Core ao LMU, conclua o procedimento a seguir.

NOTA: Esse procedimento não se aplica ao Core localhost. Ele só se aplica a máquinas Core remotas.

1 Na interface do usuário do Local Mount Utility, clique com o botão direito do mouse no Core cujas definições você deseja editar e em **Editar Core**.

2 Na caixa de diálogo **Editar Core**, você pode alterar as definições descritas na tabela a seguir.

Tabela 53. Definições do Core

Opção	Descrição
Nome do host	O nome do Core a partir do qual você deseja montar pontos de recuperação.

Opção	Descrição
	NOTA: Se você estiver instalando o LMU em uma máquina Rapid Recovery, Core, o LMU adicionará automaticamente a máquina localhost.
Port	O número da porta usada para se comunicar com o Core. O número de porta padrão é 8006.
Use minhas credenciais de usuário do Windows	Selecione esta opção se as credenciais que você usa para acessar o Core forem iguais às credenciais do Windows.
Use credenciais específicas	Selecione essa opção se as credenciais que você usa para acessar o Core forem diferentes das credenciais do Windows.
Nome de usuário	O nome de usuário utilizado para acessar a máquina do Core. **NOTA: Essa opção só permanecerá disponível se você escolher usar credenciais específicas.**
Senha	A senha usada para acessar a máquina do Core. **NOTA: Essa opção só permanecerá disponível se você escolher usar credenciais específicas.**

3 Depois que você fizer as alterações, clique em **OK**.

Reconectar a um Core

Se você perder a conexão com uma máquina Rapid Recovery Core, você pode atualizar a conexão com a seguinte etapa.

Na interface do usuário do Local Mount Utility, faça o seguinte:

- Se o Core estiver off-line, clique duas vezes no Core cuja conexão você quer restabelecer.
  O LMU tentará restabelecer a conexão com o Core.
- Se o Core estiver on-line, clique com o botão direito no Core e, em seguida, clique em Reconectar ao Core.
  O LMU atualiza a conexão.

Como remover uma máquina Rapid Recovery Core do Local Mount Utility

Conclua o procedimento a seguir para remover um Core do LMU.

NOTA: Essa opção não está disponível para um Rapid Recovery Core localizado em e rotulado como o localhost.

1 Na interface do usuário do Local Mount Utility, clique com o botão direito do mouse que você deseja remover e clique em **Remover Core**.

2 Para confirmar um comando, clique em **Sim** na caixa de diálogo.
A LMU remove o Core e as máquinas protegidas na árvore de navegação.

Trabalhar com máquinas protegidas no Local Mount Utility

Com o Local Mount Utility (LMU), você pode montar e procurar pontos de recuperação em máquinas protegidas sem precisar estar conectado no Rapid Recovery Core Console associado a essa máquina. Para obter mais informações, consulte os procedimentos a seguir:

- Montar um ponto de recuperação usando o Local Mount Utility
- Usar o Local Mount Utility para explorar um ponto de recuperação montado

- Atualizar pontos de recuperação
- Usar o Local Mount Utility para desmontar pontos de recuperação individuais
- Desmontar todos os pontos de recuperação de um Rapid Recovery Core único ou de uma máquina protegida
- Usar o Utilitário de montagem local para desmontar todos os pontos de recuperação

Montar um ponto de recuperação usando o Local Mount Utility

Com o LMU, você pode montar qualquer ponto de recuperação associado a uma máquina Core conectada, inclusive máquinas protegidas, máquinas replicadas e máquinas "apenas pontos de recuperação".

Antes de montar um ponto de recuperação, o Local Mount Utility (LMU) precisa se conectar ao Core no qual o ponto de recuperação está armazenado. Como descrito no procedimento Adicionar uma máquina Core ao Local Mount Utility, o número de Cores que podem ser adicionados ao LMU é ilimitado; no entanto, o aplicativo pode ser conectado somente a um Core por vez. Por exemplo, se você montar um ponto de recuperação de uma máquina protegida por um Core e depois montar um ponto de recuperação de outra máquina protegida por um Core diferente, o LMU se desconectará automaticamente do primeiro Core para estabelecer uma conexão com o segundo Core.

1 Na interface do usuário do Local Mount Utility, expanda o Core na árvore de navegação para revelar as máquinas protegidas.

2 Na árvore de navegação, selecione a máquina na qual você deseja montar um ponto de recuperação.
Os pontos de recuperação aparecem no frame principal.

3 Como opção, expanda o ponto de recuperação que você deseja montar para revelar volumes de disco individuais ou bancos de dados.

4 Clique com o botão direito do mouse no ponto de recuperação que você deseja montar e selecione uma das seguintes opções:

Opção	Descrição
Montagem	Essa opção permite montar o ponto de recuperação como somente leitura.
Montagem gravável	Essa opção permite fazer alterações no ponto de recuperação montado.
Montagem de apenas leitura com gravações anteriores	Essa opção monta o ponto de recuperação como somente leitura e inclui todas as alterações feitas anteriormente.
Montagem avançada...	Essa opção abre a caixa de diálogo Montagem avançada.

5 Se você tiver selecionado **Montagem avançada**, conclua as opções descritas na tabela a seguir.

Tabela 54. Opções de Montagem avançada

Opção	Descrição
Caminho de ponto de montagem	Clique em **Procurar** para selecionar um caminho para os pontos de recuperação diferentes do caminho do ponto de montagem padrão ou insira manualmente o caminho preferido.
Tipo de montagem	Selecione uma das opções a seguir: • Montagem de apenas leitura • Montagem gravável • Montagem de apenas leitura com gravações anteriores Para obter descrições de cada opção, consulte Etapa 4.

- Clique em **Montagem**.
O LMU abre automaticamente a pasta que contém o ponto de recuperação montado.

NOTA: Se você selecionar um ponto de recuperação já montado, a caixa de diálogo Montando perguntará se é necessário desmontar o ponto de recuperação.

Usar o Local Mount Utility para explorar um ponto de recuperação montado

A exploração de um ponto de recuperação abre os dados de backup em uma janela do Windows Explorer e permite pesquisar em volumes e pastas o item ou os itens que você deseja recuperar.

Você pode recuperar itens copiando-os para o local preferido usando um gerenciador de arquivos, como o Windows Explorer (ou programaticamente usando APIs do Windows). Conclua o procedimento a seguir para explorar um ponto de recuperação montado atualmente.

NOTA: Esse procedimento não é necessário se você estiver explorando um ponto de recuperação imediatamente após a montagem dele, visto que a pasta que contém o ponto de recuperação é aberta automaticamente após a conclusão do procedimento de montagem.

1 Na interface do usuário do Utilitário de montagem local, clique em **Montagens ativas**.

A janela Montagens ativas é aberta e exibe todos os pontos de recuperação montados.

2 Expanda a árvore de navegação para revelar os pontos de recuperação montados para cada máquina e seus volumes.

3 Clique em **Explorar** próximo do volume que você deseja explorar.

Atualizar pontos de recuperação

O LMU não recebe atualizações em tempo real do Core nem das máquinas protegidas. Para atualizar uma máquina protegida e ver seus pontos de recuperação mais recentes, execute o procedimento a seguir.

Na interface de usuário do Utilitário de montagem local, clique com o botão direito na máquina protegida que você quer atualizar e, em seguida, clique em Atualizar pontos de recuperação.

Usar o Local Mount Utility para desmontar pontos de recuperação individuais

Execute o procedimento a seguir para desmontar um ponto de recuperação em um Core remoto usando o LMU.

1 Na interface do usuário do Utilitário de montagem local, clique em **Montagens ativas**.

A janela **Montagens ativas** é aberta e exibe todos os pontos de recuperação montados.

2 Na janela **Montagens ativas**, você pode clicar nos ícones de adição ou de subtração para expandir a vista de volumes em cada ponto de recuperação montado.

3 Na janela **Montagens ativas**, ao lado de cada ponto de recuperação ou volume que você deseja desmontar, clique em **Desmontar**.

Uma janela de progresso mostra quando os pontos de recuperação selecionados foram desmontados.

4 Clique no **x** no canto superior direito da janela **Montagens ativas** para fechar a janela e retornar à LMU.

Desmontar todos os pontos de recuperação de um Rapid Recovery Core único ou de uma máquina protegida

Execute o procedimento a seguir para desmontar apenas os pontos de recuperação montados a partir de um único Core ou de uma máquina protegida.

1 Na interface do usuário do Local Mount Utility, faça o seguinte:

- Clique com o botão direito no Core para o qual você quer desmontar todos os pontos de recuperação.

- Clique com o botão direito na máquina protegida para a qual você quer desmontar todos os pontos de recuperação.

2 Clique em **Desmontar todos para [nome_da_máquina]**.

3 Para confirmar o comando, clique em **Yes (Sim)** na caixa de diálogo.

NOTA: Se houver alguma tarefa ativa que usa as montagens existentes, desmontar essas montagens fará com que as tarefas falhem.

Todos os pontos de recuperação montados para a sua seleção são desmontados.

Usar o Utilitário de montagem local para desmontar todos os pontos de recuperação

Há duas formas principais que você pode usar no LMU para desmontar todos os pontos de recuperação de uma vez. Você pode desmontar todos os pontos de recuperação sem ver que pontos de recuperação estão montados no momento ou você pode ver todos os pontos de recuperação atualmente montados e, em seguida, desmontá-los. Consulte o procedimento aplicável para cada um.

Como desmontar todos os pontos de recuperação usando o botão Desmontar todas as montagens

Conclua o procedimento a seguir para desmontar todos os pontos de recuperação montados de uma só vez.

1 No menu do Local Mount Utility, clique em **Desmontar todas as montagens**.

2 Para confirmar o comando, clique em **Sim** na caixa de diálogo.

NOTA: Se houver alguma tarefa ativa que usa as montagens existentes, desmontar essas montagens fará com que as tarefas falhem.

Como desmontar todos os pontos de recuperação usando a janela Montagens ativas

Conclua o procedimento a seguir para desmontar todos os pontos de recuperação montados de uma só vez na janela Montagens ativas.

1 Na interface do usuário do Utilitário de montagem local, clique em **Montagens ativas**.

2 Na janela **Montagens ativas**, clique em **Desmontar tudo**.

3 Para confirmar o comando, na janela, clique em **Sim**.

4 Na janela **Montagens ativas**, clique em **Fechar**.

Usar o menu de bandeja do Local Mount Utility

O menu da bandeja do LMU está localizado na barra de tarefas da área de trabalho. Clique com o botão direito do mouse no ícone para revelar as opções descritas na tabela a seguir:

Tabela 55. Opções do menu de bandeja

Opção	Descrição
Buscar pontos de recuperação	Abre a janela principal do LMU.
Montagens ativas	Abre a caixa de diálogo Montagens ativas no alto da janela principal do LMU.
Opções	Abre a caixa de diálogo Opções no alto da janela principal do LMU. Na caixa de diálogo Opções, você pode alterar o diretório do ponto de montagem Padrão e as credenciais do Core padrão para a interface de usuário do LMU.
Sobre	Revela as informações de aplicação de licença do Local Mount Utility.

Opção	Descrição
Sair	Fecha o aplicativo LMU.

3

Gerenciar o dispositivo

O Core Console inclui uma guia **Appliance** (Dispositivo) que você pode usar para provisionar espaço, monitorar a integridade do dispositivo e acessar ferramentas de gerenciamento.

Tópicos:

- Como monitorar o status do Dispositivo
- Backup do Windows
- Armazenamento de provisionamento
- Apagar a alocação de espaço para um disco virtual
- Utilitário de recuperação e atualização

Como monitorar o status do Dispositivo

Você pode monitorar o status dos subsistemas do Dispositivo usando a página **Appliance** > **Health** (Saúde do dispositivo). A página **Health (Saúde)** exibes uma luz de status ao lado de cada subsistema, junto com uma descrição do status indicando a integridade do subsistema.

A página **Saúde** também fornece links para ferramentas que examinam os detalhes de cada subsistema, o qual pode ser útil para solucionar avisos ou erros. O link **Provisioning Status (Status de provisionamento)**, disponível para o subsistema Provisionamento de armazenamento , abre a tela **Provisionamento** que exibe o status de provisionamento desse subsistema. O link **Rapid Appliance Self Recovery (Recuperação automática rápida do dispositivo)** disponível para um subsistema Rapid Appliance Self Recovery abre a página **Backup**, onde você pode criar a chave USB RASR, monitorar o status de backup do Windows, e configurar a política de backup do Windows. O link Gerenciamento de VM abre a página **Virtual Standby (Espera virtual)**, onde você pode gerenciar as máquinas virtuais. O link **Server Administrator (Administrador do servidor)** disponível para o subsistema Hardware de armazenamento abre a página de integridade do seu sistema onde você pode analisar a integridade do controlador, gabinete, unidades físicas e assim por diante. O link **Controllers (Controladores)**, disponível para hardware de aparelhos abre a página **Controllers (Controladores)**, o que dá os detalhes dos controladores e das unidades físicas associadas com o controlador.

Backup do Windows

O recurso de backup do Windows está disponível em todos os modelos DL, exceto DL 1000. A guia **Backup** > **de dispositivo** permite que você configure a política de backup do Windows e exibe o status do último backup e também os itens que foram armazenados anteriormente. Para o uso deste recurso de backup do Windows, o disco virtual de backup do Windows deve existir.

- Após atualizar o seu equipamento com as versões mais recentes de RUU (3,0.x), e, se o VD do backup do Windows (criado no ambiente AppAssure) não existe, o disco virtual de backup do Windows é criado quando você terminar o Assistente de configuração de dispositivo DL.Se o VD do backup do Windows não existir, clique em **+ Create WinBackups VD (+Criar VD WinBackups** na página **Backup** sob a seção **Política de backup do Windows**. No DL 4000 e DL 4300, um disco virtual de tamanho 295 GB é criado e em DL1300, um disco virtual de tamanho 210 GB é criado.

- Após atualizar o seu equipamento com as versões mais recentes de RUU, e se o VD do backup do Windows (criado no ambiente AppAssure) existir, siga estas etapas para criar o VD de backup do Windows no ambiente RR:

  a Edite **ApplianceProvisioningConfiguration.xml** (este arquivo está localizado na raiz de cada volume, para que você possa editá-lo uma vez e, em seguida, copiar onde necessário):

  CUIDADO: Não exclua o VD de backup do Windows existente.

  1 Exclua todo o texto entre as etiquetas **<BackupVolumes>**.
  2 Apague a etiqueta **</BackupVolumes>**.
  3 Edite a etiqueta **<BackupVolumes>**, de modo que ela se torne **<Backupvolume/>**
  4 Salve e feche.

  b Vá para Core Console.

  c Clique na guia **Appliance** > **RASR (RASR de dispositivo)**.

  d Clique no botão **Create Windows Backup volume (Criar volume do backup do Windows)**.

  e O VD de backup do Windows é criado, se há espaço suficiente.

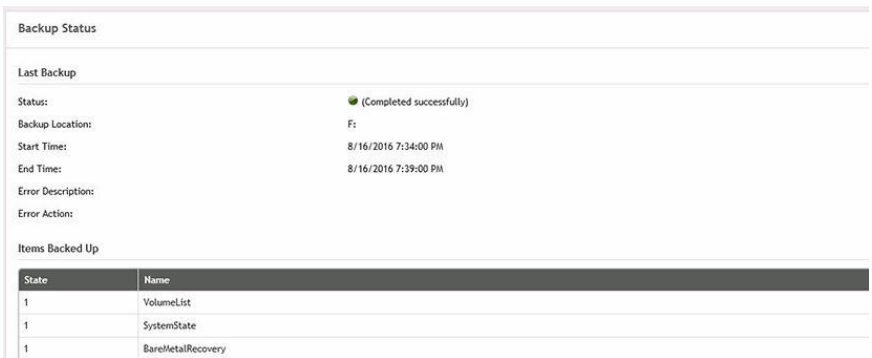
NOTA: Você pode também configurar o Backup do Windows utilizando o recurso de backup do Windows Server e armazenar backups em qualquer local, mas neste caso um erro é exibido na página RASR, porque os backups não podem ser controlados e não podem ser garantidos se eles serão consistentes para realizar restauração usando RASR.

Status do backup

O status do backup do Microsoft Windows está disponível na guia **Last Backup (Último backup)**. Se um backup estiver atualmente em execução, as informações são apresentadas na guia **Current Backup (Backup atual)**. Para ver o último backup, execute o seguinte procedimento:

1 No Core Console, navegue até a guia **Appliance (Dispositivo)** > **Backup**.
2 Clique na seta ao lado do botão **Status** para ver o status do backup.
3 O painel **Last Backup (Último backup)** mostra as informações a seguir:
   - Status
   - Estado
   - Local do backup
   - Start Time (Hora de início)
   - End Time (Hora de término)
   - Descrição do erro
   - Itens que foram incluídos no backup

NOTA: As informações acima são exibidas independente da Política de backup do Windows ser executada ou não.



Se um backup estiver em execução, as informações sobre o **Andamento atual do backup** e a **Hora de início** são exibidas.

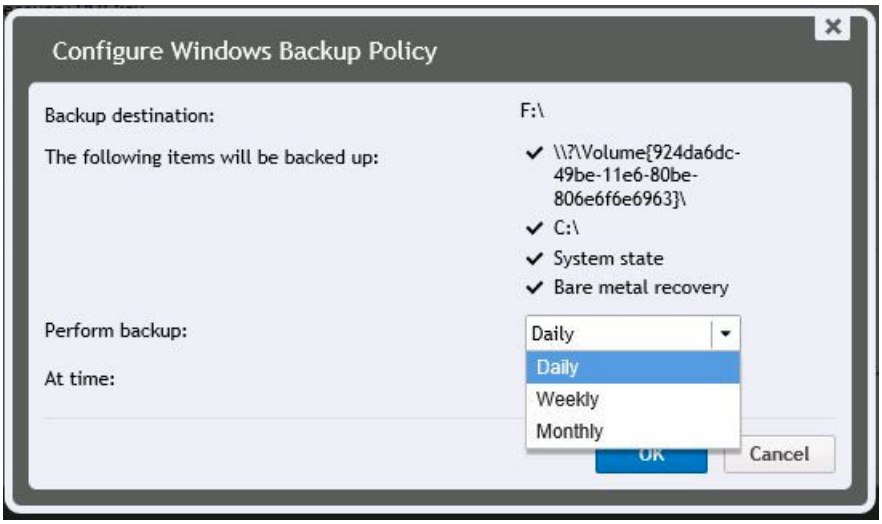
Política de backup do Windows

Para configurar uma política de backup do Windows, execute as seguintes etapas:

1 No Core Console, navegue até **Appliance (Dispositivo)** > **Backup**.

2 Clique no botão **Configure Policy (Configurar política)**.

A janela **Windows Backup Policy (Política de backup do Windows)**é mostrada.



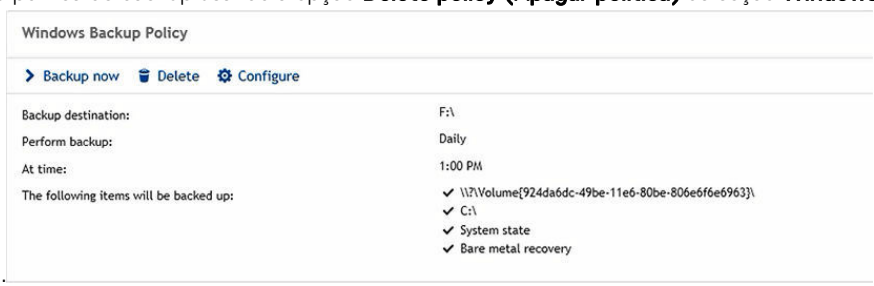
3 Digite os parâmetros, como descrito abaixo:

Caixa de texto	Descrição
O backup dos itens a seguir será feito:	• Volume do sistema operacional • Partição de recuperação • Binários de recuperação sem sistema operacional Todos os itens acima são selecionados por padrão.
Realize o backup	Selecione a frequência na qual o Winbackup deve ser executado. Você tem as seguintes opções: diário, semanal e mensal.
Selecione o horário para agendar o backup:	Digite o horário para agendar um backup.

4 Clique em **Configure (Configurar)**.

A política do Winbackup é configurada e os detalhes são mostrados na seção **Política de backup do Windows**.

Uma vez configurado, você tem a opção de fazer backup dos itens selecionados a qualquer momento usando a opção **Backup now (Fazer backup agora)** e excluir a política de backup usando a opção **Delete policy (Apagar política)** da seção **Windows Backup Policy (Política de backup do Windows)**.



Armazenamento de provisionamento

O dispositivoo configura o armazenamento interno disponível e todos os gabinetes de armazenamento externo conectados para:

- Repositórios\
- Volumes de disco para VMs em modo de espera ou qualquer outro propósito

Antes de começar a provisionar o armazenamento no disco, determine o quanto de armazenamento você quer alocar para as máquinas virtuais em espera. Você pode alocar qualquer porcentagem da capacidade disponível restante após a criação do repositório do Rapid Recovery para hospedar máquinas virtuais em espera. Por exemplo, se você estiver usando o SRM (Storage Resource Management - Gerenciamento de recursos de armazenamento), você poderá alocar até 100% da capacidade do armazenamento restante após a criação do repositório do Rapid Recovery. É possível alocar espaço para máquinas virtuais em espera apenas nos dispositivoos que são provisionados para hospedar máquinas virtuais. Usando o recurso Live Recovery (Recuperação em tempo real) do Rapid Recovery, você pode usar essas máquinas virtuais para substituir rapidamente um servidor com falha que o dispositivoo protege.

Com base em um ambiente médio que não precisa de máquinas virtuais de espera, você pode usar todo o armazenamento para fazer o backup de um número significativo de agentes. No entanto, se precisar de mais recursos para as máquinas virtuais de espera e fizer o backup de um número menor de máquinas de agente, você pode alocar mais recursos para as MVs maiores.

Quando você seleciona a guia **Appliance** > **Provisioning (Provisionamento de aparelho)**, o software Rapid Recovery Appliance localiza o espaço de armazenamento disponível de todos os controladores suportados no sistema e confirma que o hardware atende aos requisitos.

Para concluir o provisionamento de disco para todo o armazenamento disponível:

1 Clique em **Appliance** > **Provisioning (Provisionamento de aparelho)**.

A tela **Provisioning (Provisionamento)** exibe as seções **Repositories (Repositórios)** e **Storage Volumes (Volumes de armazenamento)**.

CUIDADO: Antes de continuar, confirme se as Etapas 2 a 4 foram seguidas neste procedimento.

2 Provisão disponível para criar armazenamento:
   - Repository (Repositório)
   - Volumes de disco para VMs em modo de espera ou qualquer outro propósito

3 Para criar um repositório:
   a Na página **provisioning (provisionamento)**, na seção **Repositories (Repositórios)**, clique em **Add New Repository (Adicionar novo repositório)**.

   A caixa de diálogo **Add New Repository (Adicionar novo repositório)** é mostrada.

   b Digite as informações, conforme descrito na tabela a seguir.

Tabela 56. Armazenamento de provisionamento

Caixa de texto	Description (Descrição)
Nome do repositório	Insira o nome de exibição do repositório. Por padrão, esta caixa de texto consiste em a palavra Repositório e um número que corresponde ao número de repositórios para este núcleo. Por exemplo, se este é o segundo repositório, o nome padrão é Repositório 2. Altere o nome, conforme a necessidade. Os nomes de repositório devem conter entre 1 e 40 caracteres alfanuméricos, incluindo espaços. Não use caracteres ou frases proibidas. Para obter mais informações, consulte os tópicos “caracteres proibido” ou “frases proibidas” no Guia do Usuário *Dell Proteção de dados | Rapid Recovery 6.0*.
Controlador	Selecione o controlador de armazenamento adequado dependendo se você estiver criando um repositório no armazenamento interno ou no armazenamento de conexão direta ao gabinete.

Caixa de texto	Description (Descrição)
Gabinete	Selecione o gabinete de armazenamento adequado.
Tipo de RAID	Selecione o nível de RAID. Você tem as seguintes opções para configuração de RAID: 1, 5 ou 6.
	NOTA: O seu sistema permite que você crie o repositório apenas em níveis de RAID no qual o armazenamento está configurado e como disponíveis para fora da fábrica. Para criar um repositório na configuração de RAID desejada, você precisa configurar seu armazenamento no nível desejado de RAID. Para configurar os dispositivoos de armazenamento no nível desejado de RAID, consulte a documentação Adaptadores Dell em www.dell.com/support/home.
Capacidade estimada	Exibe a capacidade disponível estimada para a criação de um repositório.
Espaço disponível no controlador	Mostra o espaço disponível no controlador.
Tamanho	Digite o tamanho do repositório.

c Clique em **Criar**.

Um novo repositório é criado.

4 Para criar volumes de disco para VM em modo de espera ou qualquer outro propósito:

a Na seção **Storage Volume (Volume de armazenamento)**, clique em **Create Volume (Criar volume)**.

b Na caixa de diálogo **Create Volume (Criar volume)**, especifique as seguintes informações sobre um novo volume de disco `Volume name (Nome do volume)`, `Controller (Controlador)`, `Enclosure (Gabinete)`, `RAID type (Tipo de RAID)`, e `Size (Tamanho)`.

O espaço disponível do Controlador é exibido por padrão. Você pode selecionar uma das seguintes configurações de RAID: 1, 5 ou 6.

c Clique em **Criar**.

Um novo volume de armazenamento é criado.

Apagar a alocação de espaço para um disco virtual

Caso precise alterar a configuração de provisionamento, entre em contato com o suporte técnico. Para obter mais informações, consulte a seção **Entrar em contato com a Dell**.

Utilitário de recuperação e atualização

O Utilitário de recuperação e atualização (RUU - Recovery and Update Utility) é um instalador do tipo "tudo em um" para recuperar e atualizar softwares de Aparelhos DL (DL1000, DL1300, DL4000 e DL4300). Ele contém o software Rapid Recovery Core e componentes específicos do aparelho.

O RUU é composto de versões atualizadas das Funções e recursos do Windows Server, .Net 4.5.2, LSI Provider, DL Applications, OpenManage Server Administrator e do software Rapid Recovery Core. Além disso, o Utilitário de recuperação e atualização também atualiza o conteúdo da Recuperação automática rápida do aparelho (RASR - Rapid Appliance Self Recovery).

NOTA: Se você estiver usando atualmente qualquer uma das versões AppAssure Core, Rapid Recovery Core versão 6.0.2.144 ou uma versão anterior, o RUU força uma atualização para a versão mais recente disponível na carga útil. Não é possível pular esta atualização e esta atualização não é reversível. Se você não quiser fazer upgrade do software Core, não execute o RUU.

Fazer upgrade do aparelho

Para fazer upgrade do aparelho:

1 Acesse o portal de licenças, na seção Downlaods, ou acesse **support.dell.com** e baixe o instalador do RUU.
2 Copie o utilitário para a área de trabalho do aparelho e extraia os arquivos.
3 Clique duas vezes no ícone **launchRUU**.
4 Quando solicitado, clique em **Yes (Sim)** para confirmar que nenhum dos processos relacionados está em andamento.
5 Quando a tela do **Utilitário de recuperação e atualização** aparecer, clique em **Start (Iniciar)**.
6 Quando for solicitado reiniciar, clique em **OK**.

   As versões atualizadas das Funções e recursos do .Net 4.5.2, LSI Provider, DL Applications, OpenManage Server Administrator e Rapid Recovery Core Software são instaladas como parte do Utilitário de recuperação e atualização. Além disso, o Utilitário de recuperação e atualização também atualiza o conteúdo RASR.

   NOTA: Se você estiver usando alguma das versões do AppAssure Core, Rapid Recovery Core versão 6.0.2.144 ou mais antiga, o RUU força uma atualização para a versão mais recente disponível no Payload. ão é possível pular a atualização e essa atualização não pode ser revertida. Se não quiser fazer o upgrade para o software do core, não execute o RUU.
7 Se solicitado, reinicie o seu sistema.
8 Depois que todos os serviços e aplicativos forem instalados, clique em **Proceed (Continuar)**.

   O Core Console será iniciado.

Reparar o dispositivo

Para reparar o dispositivo:

1 Acesse o portal de licenças, na seção Downlaods, ou acesse **support.dell.com** e baixe o instalador do RUU.
2 Copie o utilitário para a área de trabalho do aparelho e extraia os arquivos.
3 Clique duas vezes no ícone **launchRUU**.
4 Quando solicitado, clique em **Yes (Sim)** para confirmar que nenhum dos processos relacionados está em andamento.
5 Quando a tela do utilitário Recuperação e atualização for mostrada, clique em **Start (Iniciar)**.
6 Quando for solicitado reiniciar, clique em **OK**.

   As versões atualizadas das Funções e recursos do .Net 4.5.2, LSI Provider, DL Applications, OpenManage Server Administrator e Rapid Recovery Core Software são instaladas como parte do Utilitário de recuperação e atualização.
7 Se a versão agregada no utilitário for a mesma que a instalada, o Utilitário de recuperação e atualização solicita que você confirme sequer fazer uma instalação de reparo. Essa etapa pode ser ignorada se a instalação de reparo do Rapid Recovery Core não for necessária.
8 Se a versão agregada no utilitário for posterior à instalada, o utilitário Recuperação e atualização solicita que você confirme se quer fazer upgrade do software Rapid Recovery Core.

   NOTA: Não há suporte para reversão de versões de software do Rapid Recovery Core.
9 Se solicitado, reinicie o seu sistema.
10 Depois que todos os serviços e aplicativos forem instalados, clique em **Proceed (Continuar)**.

   O Assistente de configuração de dispositivo do DL será iniciados e o sistema precisar ser configurado novamente depois do reparo; caso contrário, o Core Console será iniciado.

4

Proteger estações de trabalho e servidores

Proteger as máquinas

Esta seção descreve como proteger, configurar e gerenciar as máquinas protegidas em seu ambiente do Rapid Recovery.

Sobre como proteger máquinas com Rapid Recovery

Para proteger os dados usando o Rapid Recovery, você precisa adicionar as estações de trabalho e os servidores no Rapid Recovery Core Console; por exemplo, o Exchange Server, o SQL Server, o servidor Linux etc.

Você deve instalar o software do agente Rapid Recovery em todas as máquinas virtuais ou físicas que deseja proteger no Core.

NOTA: Como uma exceção a essa regra, caso esteja protegendo máquinas virtuais em um host de VMware ou ESXi, você pode usar a proteção sem agente. Para obter mais informações, inclusive restrições da proteção sem agente, consulte Como entender o recurso Rapid Snap for virtual.

No Rapid Recovery Core Console, usando um dos assistentes de proteção de máquina, você pode identificar as máquinas que deseja proteger. Você pode fazer o seguinte:

- Você pode proteger uma máquina única usando o Assistente de proteção de máquina, que se conecta à máquina usando o nome de host ou o endereço IP da rede. Para obter mais informações sobre como proteger uma única máquina, Proteger uma máquina.
- Você pode proteger um cluster de rede usando a função Proteger cluster, que se conecta ao cluster usando o nome de host ou o endereço IP da rede.
- Você pode proteger diversas máquinas simultaneamente usando o Assistente de proteção de diversas máquinas, que se conecta às máquinas usando o Microsoft Active Directory® ou a um host ESXi ou vCenter; ou você pode especificar o nome de host de rede ou endereços IP para uma lista de máquinas inseridos manualmente.

NOTA: A Dell recomenda a limitação do número de máquinas protegidas simultaneamente a 50 ou menos para evitar restrições de recurso que possam causar uma falha na operação de proteção.

Ao identificar os requisitos de proteção para uma única máquina no assistente, você pode especificar quais volumes proteger. Quando você protege diversas máquinas, todos os volumes são protegidos por padrão. (Você pode alterar isso depois em uma máquina individual.)

O assistente também permite definir um programa personalizado para proteção (ou reutilizar um programa existente).

Usando opções avançadas, você pode adicionar medidas de segurança adicionais especificando ou aplicando uma chave de criptografia a backups das máquinas que deseja proteger.

Por fim, caso algum não exista, você pode definir um repositório usando o assistente.

Após a instalação do software do agente, cada máquina deve ser reiniciado após a instalação.

Para obter mais informações sobre como proteger estações de trabalho e servidores, consulte Proteger uma máquina.

CUIDADO: O Rapid Recovery não dá suporte a bare metal restore (BMRs) de máquinas Linux com partições de inicialização ext2. Uma BMR realizada em uma máquina com esse tipo de partição resulta em uma máquina não inicializável. Caso você queira realizar um BMR em uma máquina Linux com uma partição de inicialização ext2, você deve converter a partição de inicialização ext2 em ext3 ou ext4 para começar a proteção e o backup da máquina.

Sobre como proteger as máquinas Linux com o Rapid Recovery

O software do agente do Rapid Recovery é compatível com múltiplos sistemas operacionais Linux (para obter detalhes, consulte os requisitos de sistema contidos no *Guia de instalação e atualização do Rapid Recovery* ou nas *Notas de versão do Rapid Recovery*). O Rapid Recovery Core é compatível apenas com máquinas Windows. Embora seja possível gerenciar máquinas Linux protegidas no Rapid Recovery Core Console, vários procedimentos para máquinas Linux têm etapas que diferem dos procedimentos equivalentes no Windows. Além disso, você pode executar algumas ações diretamente em uma máquina Linux protegida usando o utilitário de linha de comando local_mount.

NOTA: O utilitário local_mount era conhecido anteriormente como aamount.

Gerenciamento de servidores Exchange e SQL no Rapid Recovery Core

As opções específicas para o Exchange Server e o SQL Server são exibidas no Console do Rapid Recovery Core quando uma instância do software e arquivos relacionados são detectados em servidores protegidos. Nesses casos, opções adicionais estão disponíveis quando você selecionar a máquina protegida do Console do Core.

Por exemplo, se você selecionar um Exchange server protegido no menu de navegação à esquerda, as opções de menu que são exibidas para a máquina protegida incluem uma opção de menu suspenso **Exchange**.

Se você selecionar um SQL Server protegido no menu de navegação à esquerda, as opções do menu que são exibidas para a máquina protegida incluem o menu suspenso **SQL**.

Enquanto essas opções funcionarem de forma diferente, haverá uniformização. As funções que você pode realizar para Exchange server e SQL server protegidos (e não para outras máquinas protegidas) incluem:

- **Forçamento do truncamento de log do server.** Tanto os SQL Servers quanto os Exchange Servers incluem logs do servidor. O processo para truncar os logs do SQL identifica o espaço disponível no servidor. Quando você truncar logs de um Exchange server, além de identificar o espaço disponível, o processo libera mais espaço no server.
- **Definição de credenciais para o respectivo server.** Os Exchange servers permitem que você defina credenciais para a máquina protegida na página Resumo para o servidor protegido. Os SQL servers permitem que você defina credenciais para uma máquina com SQL Server protegido, ou defina credenciais padrão para todos os SQL servers protegidos.
- **Exibir o estado para verificações em pontos de recuperação do Exchange Server ou SQL Server**. Os pontos de recuperação capturados de um SQL ou Exchange server protegido têm indicadores de status de cor correspondente. Essas cores indicam o sucesso ou a falha de diversas verificações relevantes para o SQL servers ou Exchange servers.

Esta seção inclui os seguintes tópicos específicos para o gerenciamento de máquinas protegidas que utilizam o Exchange Server ou o SQL Server:

- Noções básicas sobre indicadores de status de ponto de recuperação
- Definições e funções para servidores protegidos do Exchange
- Definições e funções para servidores SQL protegidos

Sobre a proteção de clusters do servidor

No Rapid Recovery, a proteção de cluster do servidor está associada às máquinas protegidas do Rapid Recovery instaladas em nós de cluster individuais (ou seja, máquinas individuais no cluster) e ao Rapid Recovery Core, que protege essas máquinas como se fossem uma única máquina composta.

É fácil configurar um Rapid Recovery Core para proteger e gerenciar um cluster. No Core Console, um cluster é organizado como entidade separada, que atua como contêiner que inclui os nós relacionados. Por exemplo, na área de navegação à esquerda, no menu **Máquinas protegidas**, os clusters protegidos são relacionados. Diretamente abaixo de cada cluster, os nós individuais associados ou máquinas agente

aparecem. Cada um desses é uma máquina protegida na qual o software do agente do Rapid Recovery é instalado. Se você clicar no cluster, a página **Resumo** do cluster aparece no Core Console.

Nos níveis de Core e cluster, é possível visualizar informações sobre o cluster, como a lista de nós relacionados e volumes compartilhados. Ao exibir as informações de um cluster no Core Console, você pode clicar em **Nós protegidos** no menu de navegação superior para ver uma tabela de resumo dos nós individuais do cluster. Dessa tabela de resumo, você pode realizar funções para cada nó, como forçar um snapshot; realizar uma exportação única ou configurar um standby virtual; montar ou visualizar pontos de recuperação; restaurar a partir de um ponto de recuperação; converter o nó do cluster para sua própria máquina protegida; ou remover a proteção do nó. Se o nó for um Exchange ou SQL Server, você também verá a opção de truncar logs.

No nível de cluster, também é possível visualizar os metadados de clusters correspondentes do Exchange e SQL para os nós do cluster. Você pode especificar as definições de todo o cluster e dos volumes compartilhados desse cluster.

Se você clicar em qualquer nó do cluster no menu de navegação à esquerda, as informações mostradas no Core Console são específicas desse nó do cluster. Aqui você pode visualizar informações específicas para esse nó ou configurar as definições apenas desse nó.

Suporte para volumes compartilhados do cluster

No Rapid Recovery versão 6.x , suporte para volumes compartilhados do cluster (CSV) é limitado a backup nativos de CSVs que executam o Windows Server 2008 R2. Você também pode restaurar volumes CSV que executam o Windows Server 2008 R2 a partir de um ponto de recuperação, ou executar uma exportação virtual para CSV Hyper-V que executam o Windows Server 2008 R2. Você não pode executar a exportação virtual de um cluster de volume compartilhado. Novo no Rapid Recovery versão 6.0.1 e posterior é a possibilidade de executar exportação virtual para um CSV Hyper-V executando o Windows Server 2012 ou o Windows Server 2012 R2.

NOTA: O recurso Hyper-V sem agente é compatível somente com o Windows Server 2012 R2 e mais recente.

Para outros sistemas operacionais, o serviço Rapid Recovery Agent pode ser executado em todos os nós em um cluster, e o cluster pode ser protegido como um cluster dentro do Rapid Recovery Core; no entanto, CSVs não são exibidos no Core Console e não estão disponíveis para proteção. Todos os discos locais (por exemplo, volume do sistema operacional) estão disponíveis para proteção.

A tabela a seguir mostra suporte atual no Rapid Recovery Core para volumes compartilhados do cluster.

Tabela 57. Suporte para volumes compartilhados do cluster Rapid Recovery

Suporte para volumes compartilhados do cluster Rapid Recovery	Proteger, Replicar, Fusão, Montar, Arquivar	Restaurar volumes CSV	Exportação virtual para CSV Hyper-V
Rapid Recovery	6,0	6,0	6.0.x
Windows Server 2008 R2	Sim	Sim	Sim
Windows Server 2012	Não	Não	Sim
Windows Server 2012 R2	Não	Não	Sim

[1] Exclui o recurso Hyper-V sem agente, o que é compatível somente com o Windows Server 2012 R2 e mais recente.

Enquanto o Rapid Recovery possa permitir que você proteja alguns outros sistemas operacionais nos volumes compartilhados do cluster, faça isso ao seu próprio risco. Apenas as configurações na tabela acima são suportadas pela Dell.

Suporte para volumes dinâmicos e básicos

O Rapid Recovery suporta a obtenção de snapshots de todos os volumes dinâmicos e básicos. O Rapid Recovery também suporta a exportação de volumes dinâmicos simples que estão em um único disco físico. Como o próprio nome indica, os volumes dinâmicos simples não são volumes distribuídos, espelhados, estendidos ou RAID.

O comportamento da exportação virtual de discos dinâmicos é diferente baseado no fato de o volume que você deseja exportar ser protegido pelo software Rapid Recovery Agent ou ele ser uma VM com proteção sem agente. Isso ocorre porque volumes dinâmicos não simples ou complexos têm geometrias de disco arbitrárias que não podem ser totalmente interpretadas pelo Rapid Recovery Agent.

Quando você tenta exportar um disco dinâmico complexo de uma máquina com o software Rapid Recovery Agent, uma notificação na interface do usuário é exibida para alertá-lo de que as exportações são limitadas e restritas aos volumes dinâmicos simples. Se você tentar exportar qualquer coisa além de um volume dinâmico simples com o Rapid Recovery Agent, o trabalho de exportação falha.

Por outro lado, volumes dinâmicos para VMs que você protege sem agente têm suporte para proteção, exportação virtual, restauração de dados, BMR e armazenamento de repositório com algumas restrições importantes. Por exemplo:

- **Proteção:** quando o volume é estendido em vários discos, você deve proteger todos os discos em conjunto para manter a integridade do volume.
- **Exportação virtual:** você pode exportar volumes dinâmicos complexos, como volumes distribuídos, espelhados, estendidos ou RAID de um host ESXi usando a proteção sem agente.

  No entanto, os volumes são exportados para o nível do disco, sem análise de volume. Por exemplo, ao exportar um volume dinâmico estendido em dois discos, a exportação incluirá dois volumes de disco distintos.

  CUIDADO: Ao exportar um volume dinâmico estendido em vários discos, você deve exportar os discos dinâmicos com o sistema original para preservar os tipos de volumes de disco.
- **Restaurar dados:** ao exportar um volume dinâmico estendido em vários discos, você deve restaurar os discos dinâmicos com o sistema original para preservar os tipos de volumes de disco. Se restaurar apenas um disco, corromperá a configuração do disco.

Armazenamento do repositório: além disso, o Rapid Recovery suporta a criação de repositórios em volumes dinâmicos complexos (distribuídos, espelhados, estendidos ou RAID). O sistema de arquivos na máquina host do repositório deve ser NTFS ou ReFS.

Noções básicas do instalador de software do agente Rapid Recovery

O Rapid Recovery permite baixar instaladores do Rapid Recovery Core. Na página **Downloads**, você pode optar por baixar o Agent Installer, o Local Mount Utility (LMU) ou um arquivo MIB SNMP. Para obter mais informações sobre o LMU, consulte O Local Mount Utility. Para obter mais informações sobre o SNMP, consulte Noções básicas das definições do SNMP.

NOTA: Para acessar o Agent Installer, consulte Como baixar o Rapid Recovery Agent Installer. Para obter mais informações sobre a implantação do Agent Installer, consulte o Guia de instalação e atualização Dell Data Protection | Rapid Recovery.

O Agent Installer é usado para instalar o aplicativo do agente Rapid Recovery em máquinas que devem ser protegidas pelo Rapid Recovery Core. Se você determinar que possui uma máquina que exige o Agent Installer, poderá baixar o instalador da Web a partir da página Downloads do Rapid Recovery Core.

NOTA: O download do Core é feito a partir do Dell Data Protection | Portal de licenças do Rapid Recovery. Para baixar o instalador do Rapid Recovery Core, acesse https://licenseportal.com. Para obter mais informações, consulte o *Guia do usuário do Dell Data Protection | Portal de licenças do Rapid Recovery*.

Como baixar o Rapid Recovery Agent Installer

Baixe o Rapid Recovery Agent Installer e o implante em qualquer máquina que você deseja proteger no Rapid Recovery Core. Execute as etapas deste procedimento para baixar o instalador da Web.

1 Para baixar o instalador da Web do agente diretamente na máquina que você deseja proteger, faça o seguinte:
   a Em um navegador web, abra o Dell Data Protection | Portal de licenças do Rapid Recovery emhttps://licenseportal.com.
   b No menu de navegação esquerdo, clique em **Downloads**.
   c No painel **Aplicativos com base em Windows**, role até a linha **Windows Agent** e clique em **Baixar** para o instalador apropriado (sistemas 32 ou 64 bits).

   O arquivo do instalador, por exemplo`Agent-X64-6.0.1.xxxx.exe`, é salvo na pasta de destino de downloads.

2 Para baixar o instalador da web no Core, na barra de ícones Core Console, clique em  Ícone **Mais** e selecione **Downloads**.

3 Na página **Downloads**, no painel **Agente**, clique em **Baixar instalador da web**.

4 Na caixa de diálogo **Abrindo Agent-Web.exe**, clique em **Salvar arquivo**.

O arquivo do instalador, por exemplo`Agent-X64-6.0.1.xxxx.exe`, é salvo na pasta de destino de downloads.

5 Mova o instalador para a máquina apropriada e instale o software do agente Rapid Recovery.

Para obter mais informações sobre a instalação do software do agente Rapid Recovery, consulte o *Guia de instalação e upgrade do Rapid Recovery*.

Implantar agente para múltiplas simultaneamente a partir do Core Console

Você pode implantar o software do Rapid Recovery Agent simultaneamente para múltiplas máquinas do Windows. As máquinas podem ser parte do domínio do Active Directory ou do host virtual vCenter ou ESX(i); ou eles podem ser máquinas já protegidas pelo Rapid Recovery Core local, como no caso de uma atualização de software do Rapid Recovery Agent. Você também tem a opção de implantar manualmente o software para as máquinas que não estão necessariamente associadas a um domínio específico ou host.

Você também pode implantar manualmente o software do Rapid Recovery Agent em uma ou mais máquinas Linux do Core Console.

CUIDADO: Se o AppAssure Agent foi instalado anteriormente em uma máquina Linux, então, antes de instalar o Rapid Recovery Agent, remova o AppAssure Agent da máquina usando um script shell. Para obter informações sobre como remover o agente de uma máquina Linux, consulte o tópico Desinstalar o software AppAssure Agent de uma máquina Linux. Para implantar com sucesso o software do agente em máquinas Linux, consulte os pré-requisitos no tópico Sobre como instalar o software de agente em máquinas Linux. Esses tópicos são encontrados no *Guia de instalação e atualização do Dell Data Protection | Rapid Recovery.*

Implantar o software do Rapid Recovery Agent não protege máquinas automaticamente. Depois de implantar, você deve selecionar a opção **Protect Multiple Machines (Proteger múltiplas máquinas)** na barra de botões do Core Console.

NOTA: O recurso no qual você implanta para múltiplas máquinas simultaneamente era anteriormente chamado de "implantação em lote". O recurso no qual você protege múltiplas máquinas simultaneamente era anteriormente chamado de "proteção em lote".

Para implantar e proteger múltiplas máquinas simultaneamente, execute as seguintes tarefas:

- Implantar o Rapid Recovery Agent para múltiplas máquinas. Consulte Implantação do software do agente Rapid Recovery em uma ou mais máquinas.
- Monitorar a implantação. Consulte Confirmar a implantação em várias máquinas.
- Proteger múltiplas máquinas. Consulte Sobre como proteger diversas máquinas.

NOTA: Se você selecionou a opção Protect Machine After Install (Proteger máquina após instalação) durante a implantação, pule essa tarefa.

- Monitore a atividade da proteção em lote. Consulte Monitorar a proteção de várias máquinas.

Implantação do software do agente Rapid Recovery em uma ou mais máquinas

Você pode simplificar a tarefa de implantação do software do agente Rapid Recovery em uma ou mais máquinas do Windows usando o Assistente de software do agente de implantação.

NOTA: No passado, esse recurso foi chamado de "implantação em massa."

Quando você usa o Assistente de software do agente de implantação, o Rapid Recovery pode detectar automaticamente as máquinas em um host e permitir que você selecione as máquinas nas quais você deseja implantar. Para máquinas em domínios ou hosts que não sejam Active Directory, vCenter ou ESX(i), você pode se conectar manualmente a máquinas individuais usando o endereço IP e as credenciais adequadas. Você também pode enviar atualizações do software para máquinas que o Rapid Recovery Core local já protege.

Do Core Console, você pode realizar qualquer uma das seguintes tarefas:

- Implantar em máquinas de um domínio Active Directory
- Implantar em máquinas de um host virtual VMware vCenter/ESX(i)
- Aplicar um upgrade do Software do agente Rapid Recovery em máquinas protegidas
- Implantar nas máquinas manualmente

NOTA: A Dell recomenda limitar o número de máquinas para as quais você implanta simultaneamente para 50 ou menos, de forma a evitar limitações de recursos que podem causar falha da operação de implantação.

NOTA: As máquinas de destino devem ter acesso à Internet para baixar e instalar bits, porque o Rapid Recovery usa a versão da Web do instalador do agente Rapid Recovery para implantar os componentes de instalação. Se o acesso à Internet estiver indisponível, use o Core Console para baixar instalador para uma mídia, como uma unidade USB, e instale fisicamente o software nas máquinas que você deseja proteger. Para obter mais informações, consulte Como baixar o Rapid Recovery Agent Installer.

Implantar em máquinas de um domínio Active Directory

Use este procedimento para implantar simultaneamente o Software do agente Rapid Recovery em uma ou mais máquinas em um domínio Active Directory.
Antes de iniciar este procedimento, tenha em mãos as informações de domínio e credenciais de login para o servidor Active Directory.

1 No Rapid Recovery Core Console, clique menu suspenso no **Proteger** e clique em **Implantar Software do agente**.

O Assistente para implantar o software do agente é aberto.

2 Na página **Conexão** do assistente, na lista suspensa **Origem**, selecione **Active Directory**.

3 Insira as informações de domínio e credenciais de login conforme descrito na tabela a seguir.

Tabela 58. Informações e credenciais do domínio

Caixa de texto	Descrição
Host	O nome de host ou endereço IP do domínio Active Directory.
Nome de usuário	O nome de usuário utilizado para se conectar ao domínio, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
Senha	A senha usada para se conectar ao domínio.

4 Clique em **Avançar**.

5 Na página **Máquinas**, selecione as máquinas em que você deseja implantar o Software do Agente Rapid Recovery.

6 Como opção, para reinicializar automaticamente as máquinas protegidas após a instalação do agente, selecione **Após a instalação, reiniciar a máquina automaticamente (recomendado)**.

7 Clique em **Concluir**.

O sistema verifica automaticamente cada máquina que você selecionou.

Se o Rapid Recovery detectar alguma preocupação durante a verificação automática, o assistente avança para uma página de Avisos em que você pode retirar as máquinas da seleção e verificar manualmente as máquinas selecionadas. Se as máquinas que você adicionou passarem na verificação automática, elas serão exibidas no painel Implantar Agente nas máquinas.

8 Se a página de Avisos for exibida e você ainda estiver satisfeito com suas seleções, clique novamente em **Concluir**.

O Software do agente Rapid Recovery é implantado nas máquinas especificadas. As máquinas ainda não estão protegidas. A proteção começa após concluir o Proteger várias máquinas em um domínio do Active Directory.

Implantar em máquinas de um host virtual VMware vCenter/ESX(i)

Use este procedimento para implantar simultaneamente o Software do agente Rapid Recovery em uma ou mais máquinas em um host virtual VMware vCenter/ESX(i).
Antes de começar este procedimento, você precisa ter as seguintes informações:

- Credenciais de login para o host virtual VMware vCenter/ESX(i).

- Local do host.
- Credenciais de login para cada máquina que você quer proteger.

NOTA: Todas as máquinas virtuais devem ter Ferramentas de VMware instaladas; caso contrário, o Rapid Recovery não consegue detectar o nome do host da máquina virtual na qual implantar. Em vez do nome do host, o Rapid Recovery usa o nome da máquina virtual, o que pode causar problemas se o nome do host for diferente do nome da máquina virtual.

1 No Rapid Recovery Core Console, clique menu suspenso no **Proteger** e clique em **Implantar Software do agente**.

O **Assistente para implantar o software do agente** é aberto.

2 Na página **Conexão** do assistente, na lista suspensa **Origem**, selecione **vCenter / ESX(i)**.

3 Insira as informações de host e credenciais de login conforme descrito na tabela a seguir.

Tabela 59. Definições de conexão do vCenter/ESX(i)

Caixa de texto	Descrição
Host	O nome ou endereço IP do host virtual VMware vCenter Server/ESX(i).
Port	A porta usada para se conectar ao host virtual. A definição padrão é 443.
Nome de usuário	O nome de usuário utilizado para se conectar ao host virtual; por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador.
Senha	A senha usada para se conectar ao host virtual.

4 Clique em **Avançar**.

5 Na página **Criar** do assistente, selecione uma das opções a seguir no menu suspenso:

- Hosts e clusters
- VMs e modelos

6 Expanda a lista de máquinas e selecione as máquinas virtuais nas quais você deseja implantar o software.

Uma notificação será exibida se o Rapid Recovery detectar que uma máquina está offline ou que as Ferramentas VMware não estão instaladas.

7 Se desejar reiniciar as máquinas automaticamente após a implantação, selecione **Após a instalação do Agente, reiniciar a máquina automaticamente (Recomendado)**.

8 Clique em **Avançar**.

O Rapid Recovery verifica automaticamente cada máquina que você selecionou.

9 Na página **Ajustes** do assistente, insira as credenciais para cada máquina no seguinte formato:`hostname::username::password`.

NOTA: Insira uma máquina em cada linha.

10 Clique em **Concluir**.

O sistema verifica automaticamente cada máquina que você selecionou.

Se o Rapid Recovery detectar alguma preocupação durante a verificação automática, o assistente avança para uma página de Avisos em que você pode retirar as máquinas da seleção e verificar manualmente as máquinas selecionadas. Se as máquinas que você adicionou passarem na verificação automática, elas serão exibidas no painel Implantar Agente nas máquinas.

11 Se a página de Avisos for exibida e você ainda estiver satisfeito com suas seleções, clique novamente em **Concluir**.

O Software do agente Rapid Recovery é implantado nas máquinas especificadas. As máquinas ainda não estão protegidas. A proteção começa após concluir o Como proteger várias máquinas em um host virtual VMware vCenter/ESX(i).

Aplicar um upgrade do Software do agente Rapid Recovery em máquinas protegidas

Você pode usar o Assistente para implementar software do agente para enviar um upgrade do Software do agente Rapid Recovery para máquinas que já estão protegidas pelo Rapid Recovery Core local.

1 No Rapid Recovery Core Console, clique menu suspenso no **Proteger** e clique em **Implantar Software do agente**.

O **Assistente para implantar o software do agente** é aberto.

2 Na página **Conexão** do assistente, na lista suspensa **Origem**, selecione **Core local**.

3 Clique em **Avançar**.

4 Na página **Máquinas** do assistente, selecione as máquinas nas quais você deseja implantar um upgrade do Software do Agente Rapid Recovery.

5 Clique em **Concluir**.

O sistema verifica automaticamente cada máquina que você selecionou.

Se o Rapid Recovery detectar alguma preocupação durante a verificação automática, o assistente avança para uma página de **Avisos** em que você pode retirar as máquinas da seleção e verificar manualmente as máquinas selecionadas. Se as máquinas que você adicionou passarem na verificação automática, elas serão exibidas no painel **Implantar Agente nas máquinas**.

6 Se a página de **Avisos** for exibida e você ainda estiver satisfeito com suas seleções, clique novamente em **Concluir**.

Implantar nas máquinas manualmente

Use o procedimento a seguir para implantar o Agente Rapid Recovery em várias máquinas de qualquer tipo de host que não seja o Core local, Active Directory ou vCenter/ESXi.

1 No Rapid Recovery Core Console, clique no menu suspenso **Proteger** e selecione **Implantar software do agente**.

O **Assistente para implantar o software do agente** é aberto.

2 Na página **Conexão** do assistente, na lista suspensa **Origem**, selecione **Manualmente**.

3 Clique em **Avançar**.

4 Na página **Máquinas** do assistente, digite o detalhes da máquina na caixa de diálogo no formato`hostname::username::password::port`. Os exemplos incluem:

```
10.255.255.255::administrator::&11@yYz90z::8006

abc-host-00-1::administrator::99!zU$o83r::168
```

5 Se desejar reiniciar as máquinas automaticamente após a implantação, selecione **Após a instalação do Agente, reiniciar a máquina automaticamente (Recomendado)**.

6 Clique em **Concluir**.

O sistema verifica automaticamente cada máquina que você selecionou.

Se o Rapid Recovery detectar alguma preocupação durante a verificação automática, o assistente avança para uma página de **Avisos** em que você pode retirar as máquinas da seleção e verificar manualmente as máquinas selecionadas. Se as máquinas que você adicionou passarem na verificação automática, elas serão exibidas no painel **Implantar Agente nas máquinas**.

7 Se a página de **Avisos** for exibida e você ainda estiver satisfeito com suas seleções, clique novamente em **Concluir**.

O Software do agente Rapid Recovery é implantado nas máquinas especificadas. As máquinas ainda não estão protegidas. A proteção começa após concluir o Como proteger diversas máquinas manualmente.

Confirmar a implantação em várias máquinas

Depois de implantar o software do agente Rapid Recovery em duas ou mais máquinas simultaneamente, você poderá verificar o sucesso visualizando cada máquina listada no menu Máquinas protegidas.

Você também pode visualizar informações em relação ao processo de implantação em massa na página Eventos. Execute as etapas deste procedimento para confirmar a implementação.

1 Navegue para Rapid Recovery Core Console, clique em  (Eventos) e clique em **Alertas**.

Aparecem eventos de alerta na lista, mostrando a hora que o evento iniciou e uma mensagem. Para cada implementação bem-sucedida do software Agent, você verá um alerta indicando que a máquina protegida foi adicionada.

2 Como opção, clique em qualquer link de uma máquina protegida.

A página **Resumo** da máquina selecionada é exibida, mostrando informações pertinentes, inclusive:

- O nome de host da máquina protegida
- O último snapshot, se aplicável
- A hora do próximo snapshot programado, com base no programa de proteção da máquina selecionada
- A chave de criptografia, caso haja alguma, usada nessa máquina protegida.
- A versão do software Agent.

Modificar definições de implantação

Execute as etapas deste procedimento para modificar as definições de implementação.

1 No Rapid Recovery Core Console, clique em  (Definições).

2 Na página **Definições**, na coluna à esquerda, clique em **Implantar** para navegar para a seção Implantar.

3 Modifique qualquer uma das opções a seguir clicando na definição que você deseja alterar para torná-la editável como uma caixa de texto ou uma lista suspensa e clique em  para salvar a definição

Tabela 60. Opções de implantação

Opção	Descrição
Agent Installer Name (Nome do instalador do agente)	Digite o nome do arquivo executável do agente. O padrão é Agent-web.exe.
Core Address (Endereço do núcleo)	Digite o endereço do Core.
Falha ao receber o tempo limite	Digite o número de minutos para aguardar sem atividade antes do tempo limite.
Máximo de instalações paralelas	Digite um número para o máximo de instalações que você deseja instalar simultaneamente. O padrão e o limite são 100.
Reinício automático após a instalação	Marque a caixa de seleção para Sim ou a desmarque para Não.
Proteger após implantação	Marque a caixa de seleção para Sim ou a desmarque para Não.

Noções básicas sobre programações de proteção

Um programa de proteção define quando os backups são transferidos de máquinas de agente protegidas para o Rapid Recovery Core.

A primeira transferência de cópia de segurança salva no Core é chamada de snapshot de imagem de base. Todos os dados em todos os volumes especificados (inclusive o sistema operacional, os aplicativos e as definições) são salvos no Core, o que pode ser muito demorado dependendo do volume de dados transferidos. Depois disso, snapshots incrementais (cópias de segurança menores, contendo apenas dados alterados na máquina protegida desde a última cópia de segurança) serão salvos no Core regularmente com base no intervalo

definido (por exemplo, a cada 60 minutos). Essa cópia de segurança contém menos dados do que uma imagem de base, e por isso a transferência demora menos.

As programações de proteção são inicialmente definidas usando o Assistente de proteção de máquina ou o Assistente de proteção de diversas máquinas. Usando um assistente, você pode personalizar os programas de proteção (escolhendo períodos ou um tempo de proteção diária) para atender às necessidades da empresa. Você pode modificar o programa existente ou criar um novo programa a qualquer momento na caixa de diálogo Programa de proteção na página de resumo de uma máquina protegida.

O Rapid Recovery fornece um programa de proteção padrão, que inclui um único período abrangendo todos os dias da semana, com um único período definido (das 0h00 às 23h59). O intervalo padrão (o período entre os snapshots) é de 60 minutos. Ao habilitar a proteção primeiro, você também ativa o programa. Assim, ao usar as definições padrão, independentemente da hora do dia atual, a primeira cópia de segurança ocorrerá a cada hora cheia (0h, 1h, 2h, e assim por diante).

Selecionar períodos permite visualizar o programa de proteção padrão e fazer os ajustes de acordo. Selecionar um tempo de proteção diária faz o Rapid Recovery Core criar uma cópia de segurança das máquinas protegidas designadas uma vez por dia na hora especificada por você.

Você pode personalizar o programa para definir horas de pico e fora do pico usando os períodos de dias da semana e fins de semana disponíveis. Por exemplo, caso as máquinas protegidas estejam em uso principalmente em dias da semana, você pode diminuir o intervalo do período de dias da semana para 20 minutos, o que resulta em três snapshots a cada hora. Ou você pode aumentar o intervalo do período de fins de semana de 60 minutos para 180 minutos, o que resulta em snapshots a cada três horas quando o tráfego está baixo.

Alternativamente, você pode alterar a programação padrão para definir horários diários de pico e fora do pico. Para isso, altere a hora final e a inicial padrão para um intervalo de tempo menor (por exemplo, das 0h00 às 16h59) e defina um intervalo apropriado (por exemplo, 20 minutos). Isso representa cópias de segurança frequentes nos períodos de pico. Você pode adicionar depois um intervalo de hora de dias da semana para o tempo restante (das 17h00 às 23h59) e definir um intervalo apropriado (presumivelmente maior) (por exemplo, 180 minutos). Essas definições configuram um período fora do pico que vai das 17h00 à meia-noite todos os dias. Essa personalização resulta em snapshots a cada três horas das 17h00 às 23h59 e em snapshots a cada 20 minutos das 0h00 às 16h59.

Quando você modifica ou cria um programa de proteção usando a caixa de diálogo Programa de proteção, o Rapid Recovery dá a opção de salvar esse programa como um modelo reutilizável que você pode aplicar a outras máquinas protegidas depois.

Entre outras opções nos assistentes de proteção estão a definição de um tempo de proteção diária. Isso resulta em uma única cópia de segurança diária no período definido (a definição padrão é 12h).

Ao proteger uma ou várias máquinas usando um assistente, você pode pausar a proteção inicialmente, o que define o programa de proteção sem proteger as máquinas. Quando você estiver pronto para começar a proteger as suas máquinas com base na programação de proteção estabelecida, você deve retomar explicitamente a proteção. Para obter mais informações sobre a retomada da proteção, consulte Pausar e retomar a proteção. Como opção, caso queira proteger uma máquina imediatamente, você pode forçar um snapshot. Para obter mais informações, consulte Forçar um snapshot.

Proteger uma máquina

Se você já tiver instalado o software do agente Rapid Recovery na máquina que você quer proteger, mas ainda não tiver realizado a reinicialização, faça isso agora.

Este tópico descreve como comece a proteger os dados em uma única máquina que você especificar usando o assistente Proteger máquina.

NOTA: Exceto caso esteja usando a proteção sem agente em um host VMware ou ESXi, a máquina que você deseja proteger deve ter o software de agente Rapid Recovery instalado para estar protegida. Você pode optar por instalar o software do agente antes desse procedimento ou pode implantar o software na máquina de destino enquanto conclui o assistente Proteger máquina.

Para obter mais informações sobre a proteção sem agente e suas restrições, consulte Como entender o recurso Rapid Snap for virtual.

Para obter mais informações sobre como instalar o software de agente, consulte "Instalar o software de agente Rapid Recovery" no *Guia de instalação e upgrade Dell Data Protection | Portal de licenças do Rapid Recovery*. Se o software de agente não estiver instalado antes de proteger uma máquina, você não poderá selecionar volumes específicos para proteção como parte desse assistente. Neste caso, por padrão, todos os volumes na máquina de destino serão incluídos para proteção. O Rapid Recovery oferece suporte para a proteção e a recuperação de máquinas configuradas com partições EISA. O suporte também é estendido para máquinas com Windows 8 e 8.1 e Windows 2012 e 2012 R2 que usam o Windows Recovery Environment (Windows RE).

Para proteger mais de uma máquina simultaneamente, consulte Sobre como proteger diversas máquinas.

Quando você adiciona uma proteção, você precisa definir as informações de conexão, como o endereço RR e a porta, e fornecer as credenciais da máquina que você quer proteger. Opcionalmente, você pode fornecer um nome de exibição para ser mostrado no Core Console em vez do endereço IP. Se você alterar isso, não verá o endereço IP da máquina protegida ao visualizar os detalhes no Core Console. Você pode também definir a programação de proteção da máquina.

O processo de proteção inclui etapas opcionais que você pode acessar se selecionar uma configuração avançada. Entre as opções avançadas, estão funções de repositório e criptografia. Por exemplo, você pode especificar um repositório existente do Rapid Recovery para salvar instantâneos ou criar um novo repositório. Você também pode especificar uma chave de criptografia existente (ou adicionar uma nova chave de criptografia) para aplicar os dados salvos ao Core para essa máquina. Para obter mais informações sobre chaves de criptografia, consulte Compreender as chaves de criptografia.

O fluxo de trabalho do assistente de proteção pode apresentar pequenas diferenças com base em seu ambiente. Por exemplo, se o software de agente Rapid Recovery estiver instalado na máquina que você deseja proteger, você não será solicitado a instalá-lo através do assistente. Da mesma maneira, se já existir um repositório no Core, você não será solicitado a criar um.

CUIDADO: O Rapid Recovery não oferece suporte para restaurações sem sistema operacional (BMRs) de máquinas Linux com partições de inicialização ext2. Qualquer BMR realizada em uma máquina com esse tipo de partição faz com que a máquina não inicie. Se quiser realizar uma BMR nesta máquina no futuro, é necessário converter quaisquer partições ext2 para ext3 ou ext4 antes de começar a proteger e fazer backups da máquina.

1 Faça um dos seguintes:
   - Se estiver começando a partir do assistente Proteger máquina, prossiga para a Etapa 2.
   - Se estiver começando do Core Console do Rapid Recovery, na barra de botões, clique em **Protect (Proteger)**.

   O assistente **Protect Machine (Proteger máquina)** é mostrado.
2 Na página **Welcome (Bem-vindo)**, selecione as opções de instalação adequadas:
   - Se você não precisa definir um repositório nem estabelecer criptografia, selecione **Typical (Típica)**.
   - Se precisar criar um repositório ou definir um repositório diferente para os backups da máquina selecionada, ou ainda se quiser estabelecer a criptografia usando o assistente, selecione **Advanced (show optional steps) (Avançado, mostrar etapas adicionais)**.
   - OpcionalOpcionalmente, se você não quiser ver a página **Welcome (Bem-vindo)** do Assistente de proteção da máquina no futuro, selecione a opção **Skip this Welcome page the next time the wizard opens (Ignorar esta página de boas-vindas na próxima vez que o assistente for aberto)**.
3 Quando estiver satisfeito com suas escolhas na página de boas-vindas, clique em **Next (Avançar)**.

   A página **Connection (Conexão)** é mostrada.
4 Na página **Connection (Conexão)**, digite as informações da máquina que você quer conectar, conforme descrito na tabela a seguir e depois clique em **Next (Avançar)**.

Tabela 61. Configurações de conexão de máquina

Caixa de texto	Descrição
Host	O nome de host ou o endereço IP da máquina que você quer proteger.
Port (Porta)	O número da porta através da qual o Rapid Recovery se comunica com o agente na máquina. O número de porta padrão é 8006.
Nome de usuário	O nome de usuário para se conectar a essa máquina; por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
Password (Senha)	A senha usada para se conectar a essa máquina.

Se a página **Install Agent (Instalar agente)** aparecer em seguida no assistente Proteger máquina, isso significa que o Rapid Recovery não detectou o agente Rapid Recovery na máquina e vai instalar a versão atual do software. Prossiga para a etapa 7.

Se a página **Upgrade Agent (Fazer upgrade de agente)** aparecer em seguida no assistente, isso significa que uma versão mais antiga do agente está instalada na máquina que você deseja proteger.

NOTA: O software de agente deve ser instalado na máquina que você deseja proteger e essa máquina deve ser iniciada antes que possa voltar ao Core. Para que o instalador reinicie a máquina protegida, selecione a opção After installation, restart the machine automatically (recommended) (Após a instalação, reiniciar a máquina automaticamente, recomendado).

5 Na página **Upgrade Agent (Fazer upgrade do agente)**, realize uma das seguintes ações:

- Para implantar a nova versão do software do agente (compatível com a versão para o Rapid Recovery Core), selecione **Upgrade the Agent to the latest version of the software (Fazer upgrade do agente para a versão mais recente de software)**.
- Para continuar a proteger a máquina sem atualizar a versão de software do agente, desmarque a opção **Upgrade the Agent to the latest version of the software (Fazer upgrade do agente para a versão mais recente de software)**.

6 Clique em **Avançar**.

7 Opcionalmente, clique na página **Protection (Proteção)** se quiser que um nome diferente do endereço IP seja mostrado no Core Console Rapid Recovery para a máquina protegida; em seguida, no campo **Display Name (Nome de exibição)**, digite um nome na caixa de diálogos.

É possível isnerir até 64 caracteres. Não use caracteres especiais descritos no tópico caracteres proibidos. Além disso, não comece o nome de exibição com nenhuma das combinações de caracteres descritas no tópico frases proibidas.

8 Selecione o cronograma de proteção adequado como descrito abaixo.

- Para definir uma programação de proteção padrão, na opção Schedule Settings (Configurações de programação), selecione **Default protection (Proteção padrão)**.

Comum cronograma de proteção padrão, o Core vai salvar instantâneos de todos os volumes da máquina protegida a cada hora. Para alterar as configurações de proteção a qualquer momento depois de fechar o assistente, incluindo selecionar quais volumes serão protegidos, acesse a página Summary (Resumo) da máquina protegida específica.

- Para definir uma programação de proteção diferente, na opção Schedule Settings (Configurações de programação), selecione **Custom protection (Proteção personalizada)**.

9 Prossiga com a configuração da seguinte forma:

- Se você tiver selecionado uma configuração típica no Assistente de proteção da máquina e especificado proteção padrão, clique em **Finish (Concluir)** para confirmar suas escolhas, feche o assistente e proteja a máquina que você especificou.

  Quando você adicionar a proteção para uma determinada máquina pela primeira vez, uma imagem base (ou seja, um instantâneo de todos os dados armazenados nos volumes protegidos) será transferida para o repositório no Rapid Recovery Core, seguindo a programação definida, a menos que você tenha especificado pausar inicialmente a proteção.
- Se você tiver selecionado uma configuração típica no Assistente de proteção da máquina e especificado proteção personalizada, clique em **Next (Avançar)** para configurar uma programação de proteção personalizada. Para obter detalhes sobre como definir uma programação de proteção personalizada, consulte Criar programações de proteção personalizadas.
- Se você tiver selecionado uma configuração avançada no Assistente de proteção da máquina e especificado proteção padrão, clique em **Next (Avançar)** e continue na Etapa 14 para ver as opções de repositório e criptografia.
- Se você tiver selecionado uma configuração avançada no Assistente de proteção da máquina e especificado proteção personalizada, clique em **Next (Avançar)** e continue na Etapa 11 para escolher os volumes que serão protegidos.

10 Na página **Protection Volumes (Volumes de proteção)**, selecione os volumes que você quer proteger. Se for mostrado algum volume que você não quer incluir na proteção, clique na coluna Check (Verificar) para desmarcar a seleção. Em seguida, clique em **Next (Avançar)**.

NOTA: Normalmente, é recomendado proteger, no mínimo, o volume reservado para o sistema e o volume com o sistema operacional (normalmente, a unidade C).

11 Na página **Protection Schedule (cronograma de proteção)**, defina um cronograma de proteção personalizado e depois clique em **Next (Avançar)**. Para obter detalhes sobre como definir um cronograma de proteção personalizado, consulte Criar programações de proteção personalizadas.

Se você já configurou as informações de repositório e selecionou a opção avançada na etapa 1, então a página Encryption (Criptografia) é mostrada. Prossiga para a etapa 13.

12 Na página **Repository (Repositório)**, faça o seguinte:

- Se você já possui um repositório e quer armazenar os dados dessa máquina para proteção no repositório existente, faça o seguinte:
  1 Selecione **Use an existing repository (Usar um repositório existente)**.
  2 Selecione um repositório existente da lista.
  3 Clique em **Avançar**.

  A página **Encryption (Criptografia)** é mostrada. Pule para a etapa 13 para definir a criptografia (opcional).
- Se quiser criar um repositório, selecione **Create a Repository (Criar um repositório)** e depois prossiga para as etapas a seguir.
  1 Na página **Repository (Repositório)**, digite as informações descritas na tabela a seguir.

Tabela 62. Configurações para adicionar novo repositório

Caixa de texto	Descrição
Nome do repositório	Insira o nome de exibição do repositório. Por padrão, essa caixa de texto é composta da palavra Repositório e um número, que corresponde ao número de repositórios deste Core. Por exemplo, se esse é o primeiro repositório, o nome padrão é Repositório 1. Altere o nome conforme necessário. Os nomes de repositório devem conter entre 1 e 40 caracteres alfanuméricos, incluindo espaços. Não use caracteres proibidos nem frases proibidas.
Operações simultâneas	Defina o número de solicitações simultâneas que você quer que o repositório suporte. Por padrão, o valor é 64.
Comentários	Opcionalmente, insira uma observação descritiva sobre esse repositório. É possível digitar até 254 caracteres. Por exemplo, digite **Repositório DMV 2**

  2 Clique em **Add Storage Location (Adicionar local de armazenamento)** para definir o local de armazenamento específico ou volume para o repositório. Esse volume deve ser um local de armazenamento primário.

CUIDADO: Defina uma pasta exclusiva dentro do diretório raiz para o local de armazenamento de seu repositório. Não especifique o diretório raiz. Por exemplo, use E:\Repository\, não E:\. Se o repositório que você estiver criando nessa etapa for removido posteriormente, todos os arquivos no local de armazenamento de seu repositório serão apagados. Se você definir seu local de armazenamento no diretório raiz, todos os outros arquivos no volume (por exemplo, E:\) são apagados, o que pode resultar em uma perda catastrófica de dados

  A caixa de diálogo **Add Storage Location (Adicionar local de armazenamento)** é mostrada.

  3 Clique em **Add Storage Location (Adicionar local de armazenamento)** para definir o local de armazenamento específico ou volume para o repositório. Esse volume deve ser um local de armazenamento primário.

  4 Na área **Storage Location (Local de armazenamento)**, especifique como adicionar o arquivo para o local de armazenamento. Você pode optar por adicionar um volume de armazenamento conectado localmente (como armazenamento conectado diretamente, uma rede de área de armazenamento ou armazenamento conectado de rede). Você também pode especificar um volume de armazenamento em um local compartilhado de sistema de arquivo de Internet comum (CIFS)

  - Selecione **Add file on local disk (Adicionar arquivo em disco local)** para especificar uma máquina local e depois insira as informações conforme descrito na tabela a seguir.

Tabela 63. Configurações de disco local

Caixa de texto	Descrição
Caminho de dados	Digite o local para armazenar os dados protegidos. Por exemplo, digite `X:\Repository\Data`. Ao especificar o caminho, use somente caracteres alfanuméricos, o hífen e o ponto final (apenas para separar os nomes de host e domínios). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Caminho de metadados	Digite o local para armazenar os metadados protegidos. Por exemplo, digite `X:\Repository\Metadata`. Ao especificar o caminho, use somente caracteres alfanuméricos, o hífen e o ponto final (apenas para separar os nomes de host e domínios). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

- Ou selecione **Add file on CIFS share (Adicionar arquivo no compartilhamento CIFS)** para especificar um local de compartilhamento de rede e depois insira as informações conforme descrito na tabela a seguir.

Tabela 64. Credenciais de compartilhamento de CIFS

Caixa de texto	Descrição
Caminho UNC	Digite o caminho para o local de compartilhamento de rede. Se esse local estiver no diretório raiz, defina um nome de pasta exclusivo (por exemplo, `Repository`). O caminho deve começar com \\. Ao especificar o caminho, use somente caracteres alfanuméricos, o hífen e o ponto final (apenas para separar os nomes de host e domínios). As letras a a z não diferenciam maiúsculas de minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Nome de usuário	Especifique um nome de usuário para acessar o local de compartilhamento da rede.
Password (Senha)	Especifique uma senha para acessar o local de compartilhamento da rede.

5 Na área **Storage Configuration (Configuração de armazenamento)**, clique em **More Details (Mais detalhes)** e insira os detalhes para o local de armazenamento como descrito na tabela a seguir.

Tabela 65. Detalhes de configuração de armazenamento

Caixa de texto	Descrição
Tamanho	Defina o tamanho ou a capacidade do local de armazenamento. O tamanho mínimo é de 1 GB. O padrão é de 250 GB. Você pode escolher entre: • GB • TB **NOTA: O tamanho que você especificar não pode exceder o tamanho do volume.** Se o local de armazenamento for um volume New Technology File System (NTFS) usando o Windows XP ou Windows 7, o limite do tamanho do arquivo é 16 TB. Se o local de armazenamento for um volume NTFS usando o Windows 8, 8.1, Windows 10, Windows Server 2012 ou 2012 R2, o limite do tamanho do arquivo é de 256 TB.

Caixa de texto	Descrição
	NOTA: Para que o Rapid Recovery valide o sistema operacional, o Windows Management Instrumentation (WMI) precisa ser instalado no local de armazenamento pretendido.
Política do cache de gravação	A política do cache de gravação controla o modo como o Windows Cache Manager é usado no repositório e ajuda a ajustar o repositório para obter o desempenho ideal em configurações diferentes. Configure o valor como uma das seguintes opções: • Ligado • Apagado • Sincronizar Se ativada, que é a configuração padrão, o Windows controla o cache. Isso é adequado para o Windows 10 e para versões do Windows Server 2012 e mais recentes. **NOTA: Ativar a política de cache de gravação pode melhorar o desempenho. Se estiver usando o Windows Server 2008 SP2 ou Windows Server 2008 R2 SP2, recomenda-se a configuração desligado.** Se desativar a configuração, o Rapid Recovery controla o cache. Se configurado como Sync (Sincronizar), o Windows controla o cache e a entrada/saída síncrona.
Bytes por setor	Especifique o número de bytes que você quer que cada setor contenha. O valor padrão é 512.
Média de bytes por registro	Especifique o número médio de bytes por registro. O valor padrão é 8192.

6 Clique em **Avançar**.

Se você selecionar a opção **Advanced (Avançado)** na etapa 1, a página **Encryption (Criptografia)** é mostrada.

13 Opcionalmente, na página **Encryption (Criptografia)**, para ativar a criptografia, selecione **Enable Encryption (Ativar criptografia)**.

Os campos Encryption key (Chave de criptografia) são mostrados na página **Encryption (Criptografia)**.

NOTA: Se você ativar a criptografia, será aplicada a todos para todos os volumes protegidos dessa máquina. É possível alterar as configurações de criptografia posteriormente no Console Core do Rapid Recovery. Para obter mais informações sobre criptografia, consulte o tópico Compreender as chaves de criptografia.

CUIDADO: O Rapid Recovery usa uma criptografia AES de 256 bits no modo CBC (Encadeamento de blocos de criptografia) com chaves de 256 bits. Apesar de o uso de criptografia ser opcional, a Dell recomenda que você estabeleça uma chave de criptografia e proteja a senha que você definir. Guarde a senha em um local seguro, pois ela é essencial para a recuperação de dados. Sem a senha, a recuperação de dados não é possível.

14 Na página **Encryption (Criptografia)**, realize uma das seguintes ações:

- Se quiser criptografar a máquina protegida usando uma chave de criptografia que já está definida neste Rapid Recovery Core, selecione **Encrypt data using an existing Encryption key (Criptografar dados usando uma chave de criptografia existente)** e depois selecione a chave adequada no menu suspenso. Prossiga para a próxima etapa.
- Se quiser adicionar uma nova chave de criptografia no Core e aplicar essa chave à máquina protegida, insira as informações como descrito na tabela a seguir.

Tabela 66. Configurações de chave de criptografia

Caixa de texto	Descrição
Nome	Digite um nome para a chave de criptografia. Os nomes de chave de criptografia devem conter entre 1 e 130 caracteres alfanuméricos. Você não pode incluir caracteres especiais como barra, barra invertida, barra vertical, dois pontos, asterisco, aspas, ponto de interrogação, parênteses iniciais ou finais, & ou traço.
Descrição	Digite um comentário para a chave de criptografia.

Caixa de texto	Descrição
	Essas informações aparecem no campo Description (Descrição) ao ver chaves de criptografia no Core Console.
Passphrase (Senha)	Digite a senha que será usada para controlar o acesso. O recomendado é evitar os caracteres especiais listados acima. Anote a senha em um local seguro. O suporte da Dell não pode recuperar uma senha. Depois de criar uma chave de criptografia e aplicá-la a uma ou mais das máquinas protegidas, você não pode recuperar os dados se perder a senha.
Confirm Passphrase (Confirmar senha)	Digite novamente a senha que você acabou de digitar.

15 Clique em **Finish (Concluir)** para salvar e aplicar as configurações.

Quando você adicionar a proteção para uma determinada máquina pela primeira vez, uma imagem base (ou seja, um instantâneo de todos os dados armazenados nos volumes protegidos) será transferida para o repositório no Rapid Recovery Core, seguindo a programação definida, a menos que você tenha especificado pausar inicialmente a proteção.

Proteger um cluster

Este tópico descreve como adicionar um cluster para proteção no Rapid Recovery. Ao adicionar um cluster para proteção, você precisa especificar o nome do host ou endereço IP do cluster, o aplicativo de cluster, ou um dos nós ou máquinas do cluster que inclua o software do agente do Rapid Recovery.

NOTA: Um repositório é usado para armazenar os snapshots de dados capturados a partir de seus nós protegidos. Antes de começar a proteger os dados em seu cluster, você deve ter definido pelo menos um repositório associado ao seu Rapid Recovery Core.

Para obter informações sobre definição de repositórios, consulte Como entender repositórios.

1 No Console do Rapid Recovery Core, clique no menu suspenso do botão **Proteger** e, em seguida, clique em **Proteger Cluster**.

2 Na caixa de diálogo Conectar-se ao cluster, digite as seguintes informações.

Tabela 67. Definições de Conectar-se ao cluster

Caixa de texto	Descrição
Host	O nome do host ou endereço IP do cluster, o aplicativo de cluster ou um dos nós do cluster.
Port	O número da porta na máquina através da qual o Rapid RecoveryCore se comunica com o agente. A porta padrão é 8006.
Nome de usuário	O nome de usuário do administrador de domínio usado para se conectar a essa máquina; por exemplo, domain_name\administrator. **NOTA: O nome de domínio é obrigatório. Não é possível conectar-se ao cluster usando o nome de usuário do administrador local.**
Senha	A senha usada para se conectar à máquina.

3 Clique em **Conectar.**

4 Na caixa de diálogo Proteger cluster, selecione um repositório para esse cluster.

5 Para proteger os pontos de recuperação desse cluster usando criptografia baseada em Core, selecione uma chave de criptografia.

6 Se não quiser que a proteção comece imediatamente após a conclusão desse procedimento, selecione **Pausar proteção inicialmente**.

7 Para proteger o cluster com base em definições padrão, selecione os nós para a proteção padrão e siga para a Etapa 10.

NOTA: As definições padrão programam um snapshot de todos os volumes a cada 60 minutos.

8 Para inserir as definições personalizadas do cluster (por exemplo, para personalizar o programa de proteção para volumes compartilhados), siga um dos passos abaixo e, em seguida, consulteCriar programações de proteção personalizadas.

- Para personalizar as definições para um nó individual, próximo ao nó que deseja personalizar, clique em **Definições**, e, em seguida, clique em **Função** próximo ao volume correspondente.
- Para personalizar as definições para o cluster, clique no botão Definições na parte inferior da caixa de diálogo e, em seguida, clique em **Função** próximo ao volume correspondente.

Para obter mais informações sobre a personalização de nós, consulte Proteger nós em um cluster.

9 Depois de fazer todas as alterações necessárias, clique em **Salvar**.

10 Na caixa de diálogo Proteger cluster, clique em **Proteger**.

Modificar configurações nó de cluster

Depois de adicionar a proteção para os nós de cluster, você pode modificar facilmente as configurações básicas para as máquinas ou nós (por exemplo, nome de exibição, nome do host e assim por diante), os parâmetros de proteção (por exemplo, alterar o agendamento da proteção para os volumes locais na máquina, adicionar ou remover volumes e pausar a proteção) e muito mais.

Para modificar as configurações do nó de cluster, execute as seguintes tarefas:

- No Rapid Recovery Core Console, navegue até o cluster que contém o nó que você deseja modificar e selecione a máquina ou nó que você deseja modificar.
- Para modificar e visualizar as definições de configuração, consulte Configurar grupos de notificação.
- Para configurar grupos de notificações de eventos do sistema, consulte Visualização e modificação das definições de máquina protegida.
- Para personalizar configurações de política de retenção, consulte Como personalizar as configurações de uma política de retenção para uma máquina protegida.
- Para modificar a programação de proteção, consulte Modificar programações de proteção.
- Para modificar configurações de transferência, consulte Sobre como modificar configurações de transferência.

Proteger nós em um cluster

Essa tarefa requer que você proteja um cluster, em primeiro lugar. Para obter informações, consulte Proteger um cluster.

Este tópico descreve como proteger os dados em um nó de cluster ou máquina que possua um agente do Rapid Recovery instalado. Este procedimento permite que você adicione nós individuais para proteção que podem ter sido omitidos quando você protegeu um cluster.

1 No Rapid Recovery Core Console, em Máquina protegida, clique no cluster com os nós que você deseja proteger.

2 Na página Resumo do cluster, clique em **Nós protegidos**.

3 Na página Nós protegidos, clique em **Proteger nó do cluster**.

4 Na caixa de diálogo Proteger nó do cluster, selecione ou insira, conforme apropriado, as seguintes informações.

Tabela 68. Definições de Proteger nó de cluster

Caixa de texto	Descrição
Host	Uma lista suspensa de nós disponíveis para proteção no cluster.
Port	Número da porta sobre a qual o Rapid Recovery Core se comunica com o agente do nó.
Nome de usuário	O nome de usuário do administrador de domínio usado para se conectar a esse nó; por exemplo, example_domain \administrator ou administrator@example_domain.com.
Senha	A senha usada para se conectar à máquina.

5 Para adicionar o nó, clique em **Conectar**.

6 Para começar a proteger esse nó com as configurações de proteção padrão, vá para a Etapa 13.

NOTA: As definições padrão garantem que todos os volumes da máquina sejam protegidos com uma programação a cada 60 minutos.

7 Na caixa de diálogo Proteger [nome do nó], se desejar utilizar um repositório diferente do repositório da configuração padrão, utilize a lista suspensa para selecionar um repositório.

8 Se desejar proteger pontos de recuperação para esse cluster utilizando a criptografia com base no Core, utilize a lista suspensa para selecionar uma chave de criptografia.

9 Se não quiser que a proteção comece imediatamente após a conclusão desse procedimento, selecione **Pausar proteção inicialmente**.

10 Para inserir as definições personalizadas (por exemplo, para personalizar o programa de proteção dos volumes compartilhados), faça o seguinte:

   a Para personalizar as configurações de um volume individual, ao lado do volume que você deseja personalizar, clique em **Função**, ao lado do volume relevante.

   b Consulte Criar programações de proteção personalizadas.

11 Clique em **Protect** (Proteger).

Criar programações de proteção personalizadas

Conclua as etapas nesse procedimento para criar programas personalizados para proteger dados em máquinas protegidas ao definir uma proteção usando um assistente.

1 Na página **Proteção** do assistente de proteção (Proteger máquina, Proteger diversas máquinas, Proteger cluster), selecione Proteção personalizada.

2 Clique em **Avançar**.

3 Na página **Volumes de proteção**, selecione os volumes que você deseja proteger e clique em **Avançar**.

4 Na página **Programa de proteção**, para alterar o programa de intervalo de qualquer período, faça o seguinte:

   a Selecione **Períodos**.

   Os períodos existentes são exibidos e podem ser modificados. Entre campos editáveis estão hora inicial, hora final e intervalo (a cada X minutos) para cada período.

   b Para cada período, clique na caixa de texto de intervalo e digite um intervalo apropriado em minutos.

   Por exemplo, destaque o intervalo padrão de 60 e o substitua pelo valor 20 para realizar snapshots a cada 20 minutos durante esse período.

5 Para criar um período de pico e fora do pico para dias da semana, altere o intervalo de tempo do período de dias da semana de maneira que não inclua um período de 24 horas, defina um intervalo ideal para o intervalo de pico, selecione **Tirar snapshots pelo restante do tempo** e defina um intervalo fora do pico fazendo o seguinte:

   a Selecione **Períodos**.

   Os períodos existentes são exibidos e podem ser modificados.

   b Clique na caixa **De** ou use o ícone de relógio para alterar a hora inicial desse período.

   c Clique na caixa **Para** ou use o ícone de relógio para alterar a hora final desse período.

   d Clique na caixa de texto do intervalo e digite um intervalo apropriado em minutos.

   Por exemplo, destaque o intervalo padrão de 60 e o substitua pelo valor 20 para realizar snapshots a cada 20 minutos durante esse o intervalo de hora selecionado para esse período.

   e Selecione **Tirar snapshots pelo restante do tempo** e insira um intervalo em minutos.

6 Para definir uma única hora do dia para uma única cópia de segurança diária, selecione **Tempo de proteção diária** e insira a hora no formato HH:MM. Por exemplo, para fazer uma cópia de segurança diária às 21h, insira 21:00.

7 Para definir a programação sem iniciar as cópias de segurança, selecione **Pausar proteção inicialmente**.

Depois que a proteção é pausada no assistente, ela permanece em pausa até que você a retome explicitamente. Depois de retomar a proteção, as cópias de segurança ocorrerão com base na programação estabelecida. Para obter mais informações sobre como retomar proteção, consulte Como pausar e retomar proteção.

8 Quando estiver satisfeito com as alterações feitas na sua programação de proteção, clique em **Concluir** ou **Avançar**, conforme o caso. Retorne ao procedimento do assistente apropriado para concluir os requisitos restantes.

Modificar programações de proteção

Um cronograma de proteção define quando backups são transferidos de máquinas agente protegidas para o Rapid Recovery Core. As programações de proteção são inicialmente definidas usando o Assistente de proteção de máquina ou o Assistente de proteção de diversas máquinas.

É possível modificar a programação de proteção existente a qualquer momento na guia Resumo de uma máquina agente específica.

NOTA: Para obter informações conceituais sobre o programa de proteção, consulte Noções básicas sobre programações de proteção. Para obter informações sobre a proteção de uma única máquina, consulte Proteger uma máquina. Para obter informações sobre proteção em massa (de várias máquinas), consulte Sobre como proteger diversas máquinas. Para obter informações sobre personalização de períodos de proteção ao proteger um agente usando um desses assistentes, consulte Criar programações de proteção personalizadas. Para obter informações sobre a modificação de um programa de proteção existente, consulte Modificar programações de proteção.

Execute as etapas deste procedimento para modificar uma programação de proteção existente para volumes de uma máquina protegida.

1 No Core Console, na lista de máquinas protegidas, clique na máquina protegida que tem o programa de proteção que você deseja alterar.

2 Na página da máquina selecionada, selecione os volumes aplicáveis e clique em **Definir um programa**.

Para selecionar todos os volumes de uma só vez, clique na caixa de seleção na linha de cabeçalho. Inicialmente, todos os volumes compartilham a mesma programação de proteção.

NOTA: Normalmente, é uma boa prática proteger, no mínimo, o volume Reservado pelo sistema e o volume em que se encontra o sistema operacional (normalmente a unidade C).

A caixa de diálogo Programação de proteção é exibida.

3 Na caixa de diálogo Programa de proteção, realize um dos procedimentos a seguir:

- Se você tiver criado um modelo de programa de proteção anteriormente e quiser aplicá-lo a essa máquina protegida, selecione o modelo na lista suspensa e depois prossiga para a Etapa 7.
- Se você quiser remover um período existente do programa, desmarque as caixas de seleção ao lado de cada opção de período e vá para a Etapa 7. Entre as opções estão:
  - Seg a sex: esse intervalo de tempo indica uma semana útil típica com cinco dias.
  - Sáb e dom: esse intervalo de tempo indica um fim de semana típico.
- Se você quiser salvar um novo programa de proteção como um modelo, continue para a Etapa 4.

4 Se a hora inicial e final do dia da semana forem 00:00 a 23:59, existe um único período. Para alterar a hora inicial e final de um período definido, faça o seguinte:

a Selecione o período adequado.

b Para alterar a hora inicial desse período, use o ícone de relógio em **Hora inicial**.

Por exemplo, use as setas para exibir o horário 08:00.

c Para alterar a hora final desse período, use o ícone de relógio em **Hora final**.

Por exemplo, use as setas para exibir o horário 18:00.

d Altere o intervalo de acordo com suas necessidades. Por exemplo, ao definir um período de pico. altere o intervalo de 60 para 20 minutos para tirar snapshots três vezes por hora.

5 Se você tiver definido um período diferente de 00:00 a 23:59 na Etapa 7 e quiser que os backups sejam realizados nos intervalos de tempo restantes, você precisa adicionar períodos adicionais para definir a proteção fazendo o seguinte:

a Na categoria adequada, clique em **Adicionar período**.

b Clique no ícone de relógio e selecione as horas inicial e final desejadas, conforme apropriado.

Por exemplo, defina a hora inicial em 0h e a hora final em 7h59.

c Altere o intervalo de acordo com suas necessidades. Por exemplo, ao definir um período fora de pico. altere o intervalo de 60 para 120 minutos para tirar snapshots a cada duas horas.

6 Se necessário, continue a criar períodos adicionais, definindo horas iniciais e finais e intervalos conforme apropriado.

NOTA: Se quiser remover um período adicionado por você, clique no ícone de lixo no canto direito do período e clique em Sim para confirmar.

7 Para criar um modelo a partir do programa definido, clique em **Salvar como modelo**.

8 Na caixa de diálogo Salvar modelo, digite um nome para o modelo e clique em **Salvar**.

9 Quando seu programa de proteção atender às suas necessidades, clique em **Aplicar**.

A caixa de diálogo Programação de proteção é fechada.

Pausar e retomar a proteção

Ao pausar a proteção, você para temporariamente todas as transferências de dados da máquina selecionada para o Rapid Recovery Core. Quando você retoma a proteção, o Rapid Recovery Core segue os requisitos no programa de proteção, fazendo regularmente o backup dos dados com base nesse programa.

Você pode pausar a proteção para qualquer máquina protegida por Rapid Recovery:

- Ao estabelecer a proteção usando o Assistente de proteção de máquina ou o Assistente de proteção de diversas máquinas.
- No menu suspenso Máquinas protegidas na área de navegação à esquerda do Rapid Recovery Core (pausando a proteção para todas as máquinas protegidas).
- Na página Máquinas protegidas (acessível ao clicar no menu Máquinas protegidas).
- Em uma máquina protegida específica no menu suspenso Máquinas protegidas.
- Na parte superior de qualquer página de uma máquina protegida específica.

Se você pausar a proteção usando o Assistente de proteção de máquina ou o Assistente de proteção de diversas máquinas, ela será pausada até ser retomada explicitamente.

Se você pausar a proteção fora de um assistente, poderá escolher se quer fazer isso até ela ser retomada ou por um período designado (especificado em qualquer combinação de dias, horas e minutos). Se você pausar por um período, quando esse tempo acabar, o sistema retomará automaticamente a proteção com base na programação de proteção.

Você pode retomar a proteção para qualquer máquina protegida por Rapid Recovery pausada:

- No menu suspenso Máquinas protegidas na área de navegação à esquerda do Rapid Recovery Core (retomando a proteção para todas as máquinas protegidas).
- Em uma máquina protegida específica no menu suspenso Máquinas protegidas.
- Na página Máquinas protegidas (acessível ao clicar no menu Máquinas protegidas).
- Na parte superior de qualquer página de uma máquina protegida específica.

Use o procedimento a seguir para pausar ou retomar a proteção, conforme o caso.

1 No Rapid Recovery Core Console, para pausar a proteção de todas as máquinas, clique no menu suspenso Máquinas protegidas na área de navegação à esquerda e faça o seguinte:
   a Selecione **Pausar proteção**.
   A caixa de diálogo Pausar proteção é exibida.
   b Selecione a definição apropriada, usando uma das opções descritas abaixo, e clique em **OK**.
      - Se quiser pausar a proteção até retomá-la explicitamente, selecione **Pausar até ser retomada**.
      - Se você quiser pausar a proteção por um período específico, selecione **Pausar por** e depois, nos controles de Dias, Horas e Minutos, digite ou selecione o período de pausa apropriado, conforme o caso.

2 Para retomar a proteção de todas as máquinas, faça o seguinte:
   a Selecione **Retomar proteção**.
   A caixa de diálogo Retomar proteção é exibida.
   b Na caixa de diálogo Retomar proteção, selecione **Sim**.
   A caixa de diálogo Retomar proteção é fechada e a proteção é retomada para todas as máquinas.

3 Para pausar a proteção de uma única máquina, na área de navegação à esquerda, clique no menu suspenso à direita da máquina que você deseja afetar e faça o seguinte:

a Selecione **Pausar proteção**.

A caixa de diálogo Pausar proteção é exibida.

b Selecione a definição apropriada, usando uma das opções descritas abaixo, e clique em **OK**.

- Se quiser pausar a proteção até retomá-la explicitamente, selecione **Pausar até ser retomada**.
- Se você quiser pausar a proteção por um período específico, selecione **Pausar por** e depois, nos controles de Dias, Horas e Minutos, digite ou selecione o período de pausa apropriado, conforme o caso.

4 Para retomar a proteção de uma única máquina, faça o seguinte:

a Selecione **Retomar proteção**.

A caixa de diálogo Retomar proteção é exibida.

b Na caixa de diálogo Retomar proteção, selecione **Sim**.

A caixa de diálogo Retomar proteção é fechada e a proteção é retomada para a máquina selecionada.

5 Para pausar a proteção de uma única máquina nas páginas de máquina, navegue até a máquina que você deseja afetar.

A página Resumo é exibida para a máquina selecionada.

a Na parte superior da página, clique em **Pausar**.

A caixa de diálogo Pausar proteção é exibida.

b Selecione a definição apropriada, usando uma das opções descritas abaixo, e clique em **OK**.

- Se quiser pausar a proteção até retomá-la explicitamente, selecione **Pausar até ser retomada**.
- Se você quiser pausar a proteção por um período específico, selecione **Pausar por** e depois, nos controles de Dias, Horas e Minutos, digite ou selecione o período de pausa apropriado, conforme o caso.

.

6 Caso queira retomar a proteção, faça o seguinte:

a Na parte superior da página, clique em **Retomar**.

b Na caixa de diálogo Retomar proteção, clique em **Sim**.

A caixa de diálogo Retomar proteção é fechada, e a proteção é retomada para a máquina selecionada.

Gerenciar máquinas protegidas

Esta seção descreve como visualizar, configurar e gerenciar as máquinas protegidas em seu ambiente do Rapid Recovery.

Sobre o gerenciamento de máquinas protegidas

As tarefas que você pode realizar para gerenciar máquinas protegidas são divididas em algumas categorias.

- Você pode visualizar as máquinas protegidas do Rapid Recovery Core usando as opções descritas no tópico Visualização de máquinas protegidas.
- Você pode configurar as definições da máquina, acessar informações do sistema ou configurar notificações de eventos referentes a uma determinada máquina. Para obter mais informações, consulte Definir as configurações da máquina.
- Você pode acessar o diagnóstico de uma máquina protegida. Para obter mais informações, consulte Download e visualização do arquivo de log de uma máquina protegida.
- Você pode remover uma máquina da proteção, cancelar as operações atuais ou visualizar informações de licença de uma máquina protegida. Para obter mais informações, consulte Gerenciar máquinas.
- Você pode visualizar e gerenciar os dados salvos no Core. Para obter mais informações, consulte Gerenciar snapshots e pontos de recuperação.

Visualização de máquinas protegidas

A partir da página **Início** do Rapid Recovery Core Console, na visualização Tabelas de resumo, você poderá ver informações de resumo de quaisquer máquinas protegidas pelo Core no painel Máquinas protegidas.

NOTA: Um agente de software atua em nome do usuário para realizar ações específicas. As máquinas protegidas também são chamadas de agentes, porque executam o software do agente do Rapid Recovery para facilitar a criação de cópias de segurança e a replicação de dados no Rapid Recovery Core.

Você pode visualizar o status, o nome de exibição de cada máquina, o repositório que ela usa, a data e hora do último snapshot, o número de pontos de recuperação que existem no repositório da máquina e a quantidade total de espaço de armazenamento que os snapshots usam no repositório.

Para começar a gerenciar aspectos de qualquer máquina protegida, navegue até a máquina que deseja visualizar, configurar ou gerenciar. Na página Início, há três maneiras de navegar até uma máquina protegida:

- Você pode clicar no endereço IP ou nome de exibição de qualquer máquina protegida do painel Máquinas protegidas. Isso leva você para a página Resumo da máquina protegida selecionada.
- Na área de navegação à esquerda, você pode clicar no título do menu **Máquinas protegidas**. A página Protected Machines (Máquinas protegidas) aparece. Na página Máquinas protegidas, você pode ver informações resumidas sobre cada máquina. Para ver uma descrição detalhada dessa página, consulte Visualização das informações de resumo de uma máquina protegida.
- Na área de navegação à esquerda, no menu Máquinas protegidas, você pode clicar no endereço IP ou nome de exibição de qualquer máquina protegida. Isso leva você para a página Resumo da máquina protegida selecionada. Para ver uma descrição detalhada dessa página, consulte Visualização das informações de resumo de uma máquina protegida

Visualizar informações de resumo de cluster

Execute as etapas deste procedimento para visualizar as informações de resumo de um cluster, incluindo informações sobre o quórum associado ao cluster.

1 No Rapid Recovery Core Console, em Máquinas protegidas, clique no cluster que você deseja visualizar.

A página Resumo da máquina é exibida.

2 Na página Resumo, você pode visualizar informações como nome do cluster, tipo de cluster, tipo de quórum (se aplicável) e caminho do quórum (se aplicável). Essa página também mostra informações de relance sobre os volumes nesse cluster, incluindo o tamanho e programação de proteção. Se aplicável, também é possível visualizar informações do SQL Server ou Exchange Server para um cluster diferente.

3 Para visualizar as informações mais recentes, clique em **Atualizar**.

Para obter informações sobre visualização de informações de resumo e status de uma máquina ou nó individual no cluster, consulte Visualização de máquinas protegidas.

Definir as configurações da máquina

Depois de adicionar máquinas para proteção no Rapid Recovery, é possível ver e modificar facilmente as configurações que controlam o comportamento da máquina protegida. Ao modificar configurações para uma máquina protegida, essas configurações substituem o comportamento definido a nível de core.

Você pode ver e definir as seguintes configurações de máquina no Rapid Recovery Core Console:

- **Geral**. Configurações gerais de máquina incluem nome de exibição, nome de host, porta, chave de criptografia e repositório. Para obter informações sobre como definir configurações gerais para uma máquina, consulte Visualização e modificação das definições de máquina protegida.
- **Trabalhos noturnos**. O subconjunto de configurações de trabalho noturno do core que aparece para uma máquina protegida específica permite que você substitua as configurações de trabalho noturno definidas a nível de core. Isso inclui implementação, que permite que você gerencie a política de retenção. Algumas configurações podem se diferir com base no tipo de máquina protegido.
- **Configurações de transferência.** Configurações específicas para gerenciar processos de transferência de dados para a máquina protegida selecionada. Para obter informações sobre os tipos de transferência de dados afetados por essas configurações, consulte Sobre como modificar configurações de transferência.
- **Gravadores excluídos**. Essas configurações permitem que você exclua gravadores e são específicas de máquina. Um gravador é uma API específica publicada pela Microsoft para permitir que outros componentes de software participem usando os serviços de sombra de volume (VSS) da Microsot. Cada um dos gravadores no Rapid Recovery que participa nos instantâneos de volume é listado nas configurações Excluded Writers (Gravadores excluídos). Caso um gravador interfira ou impeça transferências de backup, é possível desativá-los um a um. A Dell recomenda não alterar essas configurações, a não ser que você seja orientado por um representante de suporte Dell.

- **Detalhes de licença**. Esses são detalhes sobre a licença para a máquina protegida específica. Essas configurações relatam informações do core e do Dell Data Protection | Portal de licenças do Rapid Recovery. Essas configurações são somente-leitura. Para alterar essas configurações, atualize suas informações de licença entre o core e o portal de licença. Consulte seu administrador de licenças para obter detalhes. Para obter mais informações, consulte o *Guia do usuário do Dell Data Protection | Portal de licenças do Rapid Recovery*.

O procedimento para ver ou alterar configurações de nível de máquina é idêntico para tarefas gerais, gravadores excluídos e detalhes de licença. Para obter mais informações, consulte Visualização e modificação das definições de máquina protegida.

O procedimento para modificar trabalhos noturnos para uma máquina é diferente. Para obter informações sobre como definir configurações de trabalho noturno para uma máquina, consulte Como personalizar os trabalhos noturnos para uma máquina protegida.

Em alguns casos, você pode querer ajustar a taxa de transferência de dados para uma máquina protegida. Para obter mais informações, consulte Sobre como modificar configurações de transferência.

Visualização e modificação das definições de máquina protegida

As definições da máquina ajudam a determinar o comportamento de uma máquina protegida pelo Core. Quando você modifica as configurações de uma máquina específica, essas configurações substituem o comportamento definido no nível do Core.

Execute as etapas descritas neste procedimento para ver e modificar as definições gerais, de transferência, de gravadores excluídos e de licenciamento de uma máquina protegida.

NOTA: Para ver e modificar definições de trabalho noturno, consulte Como personalizar os trabalhos noturnos para uma máquina protegida.

Essa tarefa também é uma das etapas do Modificar configurações nó de cluster.

1 No Rapid Recovery Core Console, no menu Máquinas protegidas, clique no endereço IP ou no nome da máquina para a qual você quer ver ou modificar as definições de configuração.

A página **Resumo** da máquina selecionada é exibida.

2 Clique no menu **Definições**.

A página **Definições** é exibida, mostrando as definições da máquina selecionada. Opcionalmente, para mostrar categorias de definição em qualquer lugar na página, clique no hiperlink adequado no lado esquerdo da página.

Quando você clica em uma definição que deseja alterar, ela se torna editável como um campo de texto ou um menu suspenso.

Para cada configuração, quando estiver satisfeito com as alterações, clique em ✔ para salvar as alterações e sair do modo de edição, ou clique em ✖ para sair do modo de edição sem salvar.

3 Para modificar as definições gerais de uma máquina, clique na definição adequada e digite as informações de configuração, conforme descrito na tabela a seguir.

Tabela 69. Definições gerais de uma máquina protegida

Caixa de texto	Descrição
Nome de exibição	Insira um nome de exibição para a máquina. Esse é o nome da máquina protegida que será exibido no Rapid Recovery Core Console. Você pode inserir até 64 caracteres. Por padrão, esse é o nome de host da máquina. Se necessário, é possível mudá-lo para algo mais amigável. Não use caracteres proibidos ou frases proibidas.
Nome do host	Insira um nome de host para a máquina.
Port	Insira um número de porta para a máquina. A porta é usada pelo serviço Rapid Recovery Core para se comunicar com essa máquina. A porta padrão é 8006.

Caixa de texto	Descrição
Chave de criptografia	Se você quiser que a chave de criptografia definida para esse Rapid Recovery Core seja aplicada aos dados de todos os volumes nessa máquina protegida, você pode especificar a chave de criptografia aqui. A chave deve estar desbloqueada. Se não existe uma chave de criptografia, você pode adicionar uma. Para obter mais informações sobre o gerenciamento de chaves de criptografia, consulte Gerenciar chaves de criptografia. Se os volumes dessa máquina protegida estiverem criptografados, você pode alterar para uma chave de criptografia diferente. Alternativamente, você pode desassociar uma chave de criptografia selecionando **(nenhuma)** no menu suspenso **Chave de criptografia**. **NOTA: Após aplicar uma chave de criptografia, alterar uma chave ou desassociar uma chave de uma máquina protegida, o Rapid Recovery gera uma nova imagem de base no próximo snapshot programado ou forçado.**
Repositório	Selecione um repositório para os pontos de recuperação. Exibe o repositório configurado no Rapid Recovery Core no qual devem ser armazenados os dados dessa máquina. O volume do repositório pode ser local (no armazenamento conectado ao servidor do Core) ou em um volume de um local compartilhado CIFS. **NOTA: As Definições do repositório nesta página podem ser alteradas apenas se não houver pontos de recuperação ou se o repositório anterior estiver ausente.**

4 Para modificar as definições de trabalho noturno de uma máquina protegida, consulte Como personalizar os trabalhos noturnos para uma máquina protegida.

5 Para modificar as definições do Exchange de um Exchange Server, na seção Definições do Exchange Server, clique em **Habilitar a verificação de capacidade de montagem automática** e faça o seguinte:

- Para habilitar a verificação de capacidade de montagem automática, marque a caixa de seleção e clique em ✔.
- Para desabilitar a verificação de capacidade de montagem automática, desmarque a caixa de seleção e clique em ✖.

Para obter mais informações sobre a verificação de capacidade de montagem automática, consulte Sobre verificações de montabilidade do banco de dados no Exchange.

6 Para modificar as definições de transferência de uma máquina, clique na definição adequada e digite as informações de configuração, conforme descrito na tabela a seguir.

NOTA: Para obter informações conceituais sobre as definições da transferência, consulte Sobre como modificar configurações de transferência.

Tabela 70. Definições da transferência de uma máquina protegida

Caixa de texto	Descrição
Restaurar padrão	Esse comando restaura todas as definições da transferência para as definições padrão do sistema.
Prioridade	Define a prioridade de transferência entre máquinas protegidas. Permite atribuir prioridade por comparação com outras máquinas protegidas. Selecione um número de 1 a 10, sendo 1 a maior prioridade. A definição padrão estabelece uma prioridade de 5. **NOTA: A prioridade é aplicada às transferências que estão na fila.**
Máximo de fluxos simultâneos	Define o número máximo de links TCP enviados para o Core para serem processados em paralelo para cada máquina protegida em um Repositório de DVM.

Caixa de texto	Descrição
	NOTA: A Dell recomenda definir esse valor em 8. Se houver perda de pacotes, tente aumentar essa definição.
Máximo de gravações simultâneas	Define o número máximo de ações simultâneas de gravação em disco por conexão de máquina protegida. **NOTA: A Dell recomenda defini-lo com o mesmo valor selecionado para Máximo de fluxos simultâneos. Se houver perda de pacotes, defina um valor ligeiramente mais baixo; por exemplo, se Máximo de fluxos simultâneos for 8, mude este para 7.**
Usar o Número máximo de novas tentativas padrão do Core	Selecione essa opção para usar o número de tentativas padrão para cada máquina protegida, se algumas das operações não forem concluídas.
Tamanho máximo do segmento	Especifica a maior quantidade de dados, em bytes, que um computador pode receber em um único segmento TCP. A definição padrão é 4194304. Não altere essa definição padrão, a menos que tenha sido orientado por um representante do serviço de suporte da Dell.
Profundidade máxima da fila de transferência	Especifica a quantidade de comandos que podem ser enviados simultaneamente. A definição padrão é 64. É possível ajustá-la para um número maior se o seu sistema possuir um número elevado de operações simultâneas de entrada/saída.
Leituras pendentes por fluxo	Especifica quantas operações de leitura em fila serão armazenadas no back-end. Essa definição ajuda a controlar o enfileiramento de máquinas protegidas. A definição padrão é 0.
Porta do server de dados de transferência	Define a porta para transferências. A definição padrão é 8009.
Tempo limite de transferência	Especifica em minutos e segundos o tempo a permitir que um pacote permaneça estático sem transferência.
Tempo limite de snapshot	Especifica em minutos e segundos o tempo máximo a aguardar para tirar um snapshot.
Tempo limite de limpeza de snapshot	Especifica o tempo máximo do processo de exclusão de snapshots VSS em uma máquina protegida, em minutos e segundos.
Tempo limite de leitura da rede	Especifica em minutos e segundos o tempo máximo a aguardar por uma conexão de leitura. Se a leitura de rede não puder ser realizada naquele tempo, a operação será tentada novamente.
Tempo limite de gravação da rede	Especifica o tempo máximo em segundos a aguardar por uma conexão de gravação. Se a gravação de rede não puder ser realizada naquele tempo, a operação será tentada novamente.

7 Para modificar as definições de gravadores excluídos, clique na definição adequada e digite as informações de configuração, conforme descrito na tabela a seguir.

Tabela 71. Definições de gravadores excluídos de uma máquina protegida

Caixa de texto	Descrição
Gravadores excluídos	Selecione um gravador que deseja excluir. Como os gravadores que aparecem na lista são específicos para a máquina que você está configurando, você não verá todos os gravadores em sua lista. Por exemplo, alguns gravadores que você pode ver incluem: • Gravador ASR • Gravador COM+ REGDB

Caixa de texto	Descrição
	• Gravador de contadores de desempenho • Gravador de registro • Gravador Shadow Copy Optimization • SQLServerWriter • Gravador de sistema • Gravador do programador de tarefas • Gravador de armazenamento de metadados VSS • Gravador WMI

8 Os detalhes da licença de uma máquina protegida são apenas leitura. As informações de detalhes da licença são descritas na tabela a seguir.

Tabela 72. Detalhes da licença de uma máquina protegida

Caixa de texto	Descrição
Data de expiração	Indica a data de expiração da licença para a máquina protegida selecionada.
Status da licença	Indica o status atual da licença para a máquina protegida selecionada.
Tipo de licença	Indica o tipo de licença para a máquina protegida selecionada.
Tipo de agente	Indica se a máquina protegida atual é um agente físico ou virtual.

Alterar as configurações para um host Hyper-V ou nó
Este procedimento se aplica a hosts Hyper-V ou nós que usam o Rapid Recovery Rapid Snap for Virtual (proteção sem agente) para proteção de máquinas virtuais (MVs).
Um host Hyper-V que usa o Rapid Snap for Virtual (proteção sem agente) para proteção de MVs é indicado na área de navegação esquerda pelo ícone de host.  . As configurações para um host Hyper-V com MVs que são protegidas sem agente não são as mesmas de uma máquina típica protegida. Todas as mudanças feitas nas configurações para um host se aplicam às MVs nesse host.

1 No Core Console, em Protected Machines (Máquinas protegidas) na área de navegação esquerda, clique no host Hyper-V cujas configurações você deseja alterar.

A página **Summary (Resumo)** do host é mostrada.

2 Na barra de meu do host, clique em **Settings (Configurações)**.

A página **Settings (Configurações)** é mostrada.

3 Em **General (Geral)**, clique na configuração que você deseja alterar.

A configuração selecionada se torna editável, como um campo de texto ou um menu suspenso.

4 Digite as informações de configuração, conforme descrito na tabela a seguir.

Tabela 73. Informações de configurações gerais

Caixa de texto	Descrição
Display Name (Nome de exibição)	O nome que é exibido para uma máquina protegida no Rapid Recovery Core Console. Você pode inserir até 64 caracteres. Por padrão, esse é o nome da máquina. Você pode alterar o nome de exibição para algo que seja memorizado mais facilmente se necessário. Não use caracteres proibidos nem frases proibidas.
Host Name (Nome de host)	O nome da máquina protegida como mostrado nos metadados da máquina. **NOTA: Não altere essa configuração, uma vez que fazer isso pode romper a conexão entre a máquina protegida e o core.**

5 Em **Transfer Queue (Fila de transferência)**, para alterar o número de trabalhos de transferência que podem ocorrer simultaneamente em um host, clique na configuração para **Maximum concurrent transfers (Número máximo de transferências simultâneas)**.

NOTA: Para garantir o melhor desempenho, recomenda-se que o número máximo de transferências simultâneas para o host Hyper-V ou nó seja definido em 1, que é a configuração padrão.

6 Em **Nightly Jobs (Trabalhos noturnos)**, para alterar as configurações para os trabalhos noturnos disponíveis, clique em **Change**.

A janela **Nightly Jobs (Trabalhos noturnos)** é mostrada.

7 Digite as informações de configuração, conforme descrito na tabela a seguir.

Tabela 74. Informações de configurações de trabalhos noturnos

Caixa de texto	Descrição
Apagar chaves de registro órfãs em um host Hyper-V protegido	Remove os arquivos desnecessários do registro que resultam em conexão e desconexão de discos virtuais durante transferências de dados.
Verificar a integridade dos pontos de recuperação	Realiza uma verificação de integridade de cada ponto de recuperação criado para as máquinas virtuais no host Hyper-V.

8 Clique em **OK**.

9 Em **Auto Protection (Proteção automática)**, para determinar se as novas máquinas virtuais devem ser protegidas automaticamente ao serem adicionadas ao host Hyper-V, clique na configuração para **Auto protect new virtual machines (Proteger automaticamente novas máquinas virtuais)**.

Alterar as configurações para uma máquina virtual protegida Hyper-V

Este procedimento se aplica às máquinas virtuais (VMs) Hyper-V que são protegidas usando o Rapid Snap for Virtual do Rapid Recovery (proteção sem agente).

Uma VM Hyper-V que está sendo protegida pelo Rapid Snap for Virtual (proteção sem agente) é indicada na área de navegação à esquerda pelo ícone de host  . As configurações de uma VM Hyper-V sem agente são iguais a de uma máquina protegida típica, com exceção da seção Hyper-V na parte inferior da página **Configurações**. A seguinte tarefa fornece instruções para apenas as configurações da seção **Hyper-V**. Para todas as demais definições da máquina protegida, consulte Visualização e modificação das definições de máquina protegida.

1 Na área de navegação esquerda do Core Console, em **Máquinas protegidas**, clique na VM Hyper-V cujas configurações você deseja alterar.

A página **Resumo** da VM é aberta.

2 Na barra de menus do host, clique em **Configurações**.

A página **Configurações** é aberta.

3 Na lista no lado esquerdo, clique em **Hyper-V**.

A definições selecionada se tornará editável, como um campo de texto ou um menu suspenso.

4 Em **Hyper-V**, clique em **Configuração de instantâneo**.

A definição selecionada se tornará editável como um menu suspenso.

5 No menu suspenso, selecione uma das opções descritas na tabela a seguir.

Tabela 75. Informações sobre as definições do Hyper-V

Caixa de texto	Descrição
Tente criar um instantâneo VSS durante a primeira transferência; se ela falhar, crie um ponto de verificação	Se o instantâneo VSS for bem-sucedido, o ponto de recuperação estará em um estado consistente com o aplicativo. Se o instantâneo VSS falhar e um ponto de verificação for criado, o ponto de recuperação estará em um estado consistente de falha.
Não cria um instantâneo VSS durante a transferência	Gera um ponto de recuperação em um estado consistente de falha.

Caixa de texto	Descrição
Use somente instantâneos VSS durante transferências. Se a criação de um instantâneo VSS falhar, toda a transferência falhará	Gera apenas pontos de recuperação consistentes com o aplicativo. Se o instantâneo VSS falhar, nenhum ponto de recuperação é gerado.

Alterar as configurações do vSphere para uma máquina virtual protegida VMware
Este procedimento se aplica às máquinas virtuais (VMs) VMware ESXi ou Workstation que são protegidas usando o Rapid Snap for Virtual do Rapid Recovery (proteção sem agente).
As configurações de uma máquina virtual VMware que é protegida sem agente incluem as mesmas configurações que são usadas para uma máquina protegida típica, com uma exceção. A seção **vSphere** da página **Configurações** inclui as configurações que se aplicam somente a máquinas virtuais VMware protegidas sem agente. A seguinte tarefa fornece instruções para apenas a seção **vSphere** da página **Configurações**. Para todas as demais definições da máquina protegida, consulte Visualização e modificação das definições de máquina protegida.

1 No Core Console, em Máquinas protegidas na área de navegação à esquerda, clique no host Hyper-V cujas configurações você deseja alterar.

   A página **Resumo** do host é aberta.

2 Na barra de menus do host, clique em **Configurações**.

   A página **Configurações** é aberta.

3 Na lista no lado esquerdo, clique em **vSphere**.

   A definições selecionada se tornará editável, como um campo de texto ou um menu suspenso.

4 Em **vSphere**, clique na configuração que você deseja alterar.

   A definições selecionada se tornará editável, como um campo de texto ou um menu suspenso.

5 Insira as informações de configuração conforme descrito na tabela a seguir.

Tabela 76. Informações sobre as configurações do vSphere

Caixa de texto	Descrição
Permitir que o Rapid Recovery exclua VMware criado pelo usuário	A definição padrão é Não.
Permitir transferência para volumes com capacidade utilizada inválida	A definição padrão é Sim.
Permitir instantâneos fechados	A definição padrão é Sim.

Sobre como modificar configurações de transferência

No Rapid Recovery, você pode modificar as configurações para gerenciar os processos de transferência de dados de uma máquina protegida. As configurações de transferência descritas nesta seção são definidas ao nível de proteção da máquina. Para afetar transferência ao nível do Núcleo, consulte Modificar definições de fila de transferência.

O Rapid Recovery suporta o Windows 8 e Windows Server 2012 para transferências normais, ambos os da base e incremental, bem como com a restauração, restauração “bare meta”, e a exportação de máquina virtual.

Existem três tipos de transferências no Rapid Recovery:

- **Snapshot.** faz backup dos dados em sua máquina protegida. Dois tipos de snapshots são possíveis: uma imagem de base de todos os dados protegidos, um snapshot incremental para dados atualizados desde o último snapshot. Esse tipo de transferência cria pontos de recuperação, que são armazenados no repositório associado ao Núcleo. Para obter mais informações, consulte Gerenciar snapshots e pontos de recuperação.
- **Exportar Máquina Virtual**. Cria uma máquina virtual (VM) a partir de um ponto de recuperação, contendo todos os dados de backup da máquina protegida, bem como o sistema operacional e drivers e os dados associados para garantir que a VM é inicializável. Para obter mais informações, consulte Exportação de VM.
- **Restaurar**. Restaura informações de backup para uma máquina protegida. Para obter mais informações, consulte Como restaurar volumes a partir de um ponto de recuperação.

NOTA: Todo o volume é sempre regravado durante a restauração de sistemas Windows usando partições de sistema EFI.

A transferência de dados no Rapid Recovery envolve a transmissão de um volume de dados em uma rede de máquinas protegidas ao Núcleo. No caso de replicação, a transferência ocorre também do Core de origem para o Core de destino.

A transferência de dados pode ser otimizada para o seu sistema por meio de certas configurações de opção de desempenho. Essas configurações controlam o uso de largura de banda de dados durante o processo de backup de máquinas protegidas, exportação de VM ou restauração. Alguns fatores que influenciam o desempenho da transferência de dados são:

- Número de transferências simultâneas de dados do agente
- Número de fluxos de dados simultâneos
- Quantidade de mudança de dados em disco
- Largura de banda de rede disponível
- Desempenho do subsistema do disco de repositório
- Quantidade de memória disponível para buffer de dados

Você pode alterar as opções de desempenho de forma a atender melhor suas necessidades de negócios e ajustar o desempenho com base no seu ambiente. Para obter mais informações, consulte Estrangulamento da velocidade de transferência.

Estrangulamento da velocidade de transferência
Ao transferir dados de backup ou pontos de recuperação replicados entre máquinas protegidas e Cores através da rede, você pode intencionalmente reduzir a velocidade da transferência. Esse processo é conhecido como estrangulamento.

Ao estrangular a velocidade de transferência, você limita a quantidade de largura de banda de rede dedicada à transferência de arquivos do Rapid Recovery. Ao configurar a replicação, por exemplo, o estrangulamento pode reduzir a possibilidade da transferência de pontos de recuperação anteriores ao Core replicado consumir toda a largura de banda da rede.

CUIDADO: O estrangulamento da velocidade de transferência nem sempre é necessário ou recomendado. Essas informações são fornecidas para oferecer ideias para uma possível solução de problemas de desempenho em seu ambiente Rapid Recovery. Por exemplo, algumas vezes o estrangulamento resolver problemas relacionados a falhas de transferência repetidas ou lentidão da rede causados pela transferência de uma quantidade substancial de dados para seus Cores protegidos ou replicados.

Há vários fatores envolvidos na determinação da melhor abordagem para o estrangulamento. O tipo de máquina protegida é um fator-chave. Por exemplo, um Microsoft Exchange Server ocupado tem uma taxa de alteração muito mais alta que um servidor Web legado raramente usado.

As capacidades de entrada e saída dos volumes de armazenamento em suas máquinas protegidas também podem contribuir para uma eficiência maior ou menor.

A velocidade da rede é outro fator crítico, com muitas variáveis. O backbone de rede usado (como 1 GbE versus 10 GbE), a arquitetura, a configuração, o uso intencional do agrupamento de NIC e mesmo o tipo de cabo usado podem afetar a velocidade de transferência da rede. Se o ambiente tiver uma rede de longa distância mais lenta e se os trabalhos de transferência de backup ou replicação falharem, considere o estrangulamento da velocidade de transferência usando algumas dessas definições.

Em última análise, o processo de estrangulamento da rede envolve tentativa e erro. A Dell recomenda que você ajuste e teste suas definições de transferência e as reveja periodicamente para garantir que suas definições continuam a atender suas necessidades.

O ajuste da velocidade de transferência deve ser realizado nas máquinas individualmente. No Core Console, navegue até uma máquina específica, selecione Definições e ajuste a velocidade de transferência. Para obter informações específicas sobre como visualizar e alterar essas definições, consulte Visualização e modificação das definições de máquina protegida. Esse tópico também inclui uma descrição de cada definição usada para o estrangulamento da transferência. Essas descrições podem ser úteis para determinar quais definições você deve testar primeiro.

As quatro definições principais envolvidas no estrangulamento da velocidade de transferência são descritas na tabela a seguir:

Tabela 77. Definições da máquina protegida usadas para o estrangulamento da velocidade de transferência

Definição no nível da máquina	Definições padrão	Definições de estrangulamento sugeridas
Máximo de fluxos simultâneos	8	4
Máximo de gravações simultâneas	8	4
Tamanho máximo do segmento	4194304	2097152
Leituras pendentes por fluxo	0	Iniciar em 24

A Dell recomenda ajustar e testar as outras definições antes de alterar a definição padrão para leituras pendentes por fluxo, a menos que um representante de suporte da Dell tenha orientado você a fazer isso. Ao ajustar e testar esta definição, comece com um valor de 24.

Quando você especifica limitações para os parâmetros de transferência da máquina protegida, estas limitações são aplicadas por trabalho. Se dois trabalhos de transferência ocorrerem simultaneamente ou se sobrepuserem, o uso da largura de banda dobra. Se quatro trabalhos de transferência da rede se sobrepuserem, o uso da largura de banda quadruplica, e assim por diante.

Como personalizar os trabalhos noturnos para uma máquina protegida

Os trabalhos noturnos podem ser configurados no nível do núcleo e da máquina na aba Configuração adequada. Quando todas as definições do trabalho noturno são configuradas no nível do núcleo, as alterações relevantes são aplicadas a todas as máquinas protegidas por esse núcleo. As alterações efetuadas à trabalhos noturnos no nível da máquina substituem as alterações realizadas no nível do núcleo, apenas para as máquinas especificadas.

Para obter uma lista de todos os trabalhos noturnos, incluindo a descrição e o escopo disponíveis para cada, consulte o tópico Compreender trabalhos noturnos.

Conclua as etapas no procedimento a seguir para fazer alterações nos trabalhos noturnos para uma única máquina protegida.

1 No Rapid Recovery Core Console, sob o menu Máquinas protegidas, clique no endereço IP ou nome da máquina para a máquina para a qual você quer personalizar os trabalhos noturnos.

   A página **Summary (Resumo)** para a máquina selecionada é exibida.

2 Clique no menu **Settings (Configurações)**.

   A página **Configurações** é exibida, mostrando as definições de configuração para a máquina selecionada.

3 Opcionalmente, clique no link **Nightly Jobs (Trabalhos noturnos)** para rolar para baixo na página de Configurações para ver todas as configurações para trabalhos noturnos.

4 Sob o título, clique em Trabalhos noturnos, clique **Change (Alterar)**.

   A caixa de diálogo **Nightly Jobs (Tarefas noturnas)** é mostrada.

   NOTA: Para obter informações sobre como configurar a Fusão, incluindo a definição de uma política de retenção personalizada, consulte Como personalizar as configurações de uma política de retenção para uma máquina protegida.

5 Na caixa de diálogo **Trabalhos noturnos**, selecione os trabalhos que você quer incluir para executar todas as noites, ou desselecione as opções que você quer omitir para esta máquina.

   NOTA: As opções podem variar de acordo com máquina. Por exemplo, uma máquina protegida usando Exchange Server pode incluir logs de Verificação de soma de verificação de bases de dados Exchange e Truncate Exchange.

6 Clique em **OK**.

   NOTA: Os resultados deste procedimento aplicam-se apenas a máquina protegida selecionada. Para aplicar em outros lugares, repita o procedimento para cada máquina que deseja personalizar. Para alterar as definições do trabalho noturno de todas as máquinas protegidas por um núcleo, consulte Configurar trabalhos noturnos para o Core.

Visualização das informações do sistema de uma máquina protegida

O Rapid Recovery Core Console oferece acesso fácil às informações do sistema das máquinas protegidas no Core.

O painel **Geral** inclui informações gerais sobre a máquina do Core e o ambiente. O painel **Volumes** lista as informações sobre os volumes de armazenamento da máquina do Core. O painel **Conexões do mecanismo de reprodução** mostra os volumes de todas as máquinas que estão sendo protegidas.

Execute as etapas deste procedimento para visualizar as informações detalhadas do sistema de uma máquina protegida.

1 Navegue até o Rapid Recovery Core Console e, no menu Máquinas protegidas da área de navegação à esquerda, clique no nome de uma máquina protegida.

A página **Resumo** da máquina protegida selecionada é exibida.

2 Na página **Resumo**, na parte inferior do painel **Resumo**, clique em  **Informações do sistema**.

3 Na página **Informações do sistema**, você pode visualizar os seguintes detalhes sobre a máquina protegida selecionada.

- **Informações do sistema.** Isso inclui Nome de host, Versão de OS, Arquitetura de OS, Memória (Física), Nome de exibição, Nome de domínio totalmente qualificado Local de metadados de cache, Local de cache primário, Local de cache secundário e Tipo de máquina virtual (se aplicável).
- **Volumes**. Isso inclui Nome do volume, ID do dispositivo, Sistemas de arquivos, Capacidade formatada, Capacidade usada e Pontos de montagem.
- **Processadores**. Isso inclui Arquitetura e Número de cores.
- **Adaptadores de rede**. Isso inclui Tipo de adaptador e Velocidade.
- **Endereços IP**. Isso inclui Endereço IP e Família.

Gerenciar máquinas

Esta seção descreve as diferentes tarefas que você pode executar para gerenciar suas máquinas. Os tópicos são:

- Remover uma máquina
- Remover um cluster da proteção
- Visualizar informações de licença em uma máquina
- Download e visualização do arquivo de log de uma máquina protegida
- Converter um nó de cluster protegido em uma máquina protegida

Remover uma máquina

Ao remover uma máquina da proteção no Rapid Recovery Core, você tem duas opções: manter os pontos de recuperação salvos até o momento no RR Core ou removê-los. Se você mantiver os pontos de recuperação, terá o que é conhecido como máquina “apenas com pontos de recuperação". Usando esses pontos de recuperação para a máquina que foi removida da proteção atual, você pode continuar a restaurar a máquina no futuro, mas apenas até o estado capturado em um ponto de recuperação salvo.

Se você remover os pontos de recuperação, essa ação excluirá do Rapid Recovery Core todos os dados de snapshot da máquina anteriormente protegida.

CUIDADO: Se você excluir pontos de recuperação, não poderá mais restaurar os dados dessa máquina.

Execute as etapas do procedimento a seguir para remover uma máquina da proteção no seu ambiente do Rapid Recovery.

1 Do Rapid Recovery Core Console, no painel de navegação à esquerda, em Máquinas protegidas, clique na máquina que você deseja remover.

2 Na página Resumo da respectiva máquina, clique em **Remover máquina**.

3 Na caixa de diálogo, se você quiser excluir também todos os pontos de recuperação dessa máquina do repositório, selecione **Remover com pontos de recuperação**.

4 Para confirmar a sua escolha e remover a máquina, clique em **Sim**.

O Rapid Recovery remove a máquina da proteção e cancela todas as tarefas ativas da máquina.

Remover um cluster da proteção

Execute as etapas do procedimento a seguir para remover um cluster da proteção.

1 No Rapid Recovery Core Console, sob Máquinas protegidas, clique no cluster que deseja remover.
2 Na página Resumo do cluster, clique em **Remover cluster**.
3 Opcionalmente, na caixa de diálogo, para remover todos os pontos de recuperação atualmente armazenados para esse cluster a partir do repositório, selecione **Remover com pontos de recuperação**.
4 Na caixa de diálogo, clique em **Sim** para confirmar.

Remover nós de cluster da proteção

Execute as etapas dos procedimentos a seguir para remover nós de cluster da proteção.

Se quiser apenas remover um nó do cluster, consulte Converter um nó de cluster protegido em uma máquina protegida.

1 No Rapid Recovery Core Console, em Máquinas protegidas, clique no nó do cluster que você deseja remover.
2 Na página Resumo do nó, clique em **Remover máquina**.
A caixa de diálogo Remover nó é exibida.
3 Como opção, para remover do repositório todos os pontos de recuperação atualmente armazenados para este cluster, na caixa de diálogo, selecione **Remover com pontos de recuperação**.
4 Na caixa de diálogo, clique em **Sim** para confirmar.

Remover todos os nós de um cluster da proteção

Execute as etapas deste procedimento para remover todos os nós em um cluster da proteção.

CUIDADO: Se você remover todos os nós do cluster, o cluster também será removido.

1 No Console do Rapid Recovery Core, sob Máquinas protegidas, clique no cluster cujos nós você deseja remover.
2 Na página Resumo para o cluster, clique em **Nós protegidos**.
3 Na página Nós Protegidos, selecione todos os nós.
4 No menu suspenso **Remover máquinas**, selecione uma das opções descritas na tabela a seguir.

Tabela 78. Opções de Remover nós

Opção	Descrição
Remover e manter pontos de recuperação	Para manter todos os pontos de recuperação atualmente armazenados deste cluster.
Remover pontos de recuperação	Para remover do repositório todos os pontos de recuperação atualmente armazenados deste cluster.

5 Na caixa de diálogo Excluir nós, clique em **Sim** para confirmar.

Visualizar informações de licença em uma máquina

Você pode visualizar as informações de status da licença do status da licença Rapid Recovery instalado em uma máquina protegida.

1 No Rapid Recovery Core Console, em Máquinas protegidas, clique na máquina que você deseja modificar.
A página **Resumo** da máquina de seleção é exibida.
2 Clique no menu **Definições**.
A página **Definições** é exibida, mostrando definições de configuração da máquina selecionada.
3 Clique no link **Aplicação de licença** para rolar a página Definições a fim de exibir definições de aplicação de licença específicas de máquina.
Aparece a tela Status e apresenta os detalhes sobre a aplicação de licença do produto.

Download e visualização do arquivo de log de uma máquina protegida

Se você encontrar erros ou problemas com uma máquina protegida, poderá baixar os logs da máquina para visualizá-los ou compartilhá-los com seu representante de suporte da Dell.

1 Na área de navegação à esquerda do Core Console, no menu Máquinas protegidas, clique na seta para expandir o menu sensível ao contexto da máquina protegida relevante. Role para baixo até **Mais**, expanda esse menu e selecione **Log do agente**.
A página **Baixar log do agente** é mostrada.

2 Na página **Baixar log do agente**, clique em **Clique aqui para começar o download**.

3 Na caixa de diálogo **Abrindo AgentAppRecovery.log**, realize um dos procedimentos a seguir:

- Para abrir o arquivo de log, selecione **Abrir com** e um aplicativo (como Bloco de Notas) para visualizar o arquivo de log com base em texto e, por fim, clique em **OK**.
  O arquivo AgentAppRecovery.log é aberto no aplicativo selecionado.
- Para salvar o arquivo localmente, selecione **Salvar arquivo** e clique em **OK**.
  O arquivo AgentAppRecovery.log é salvo na sua pasta Downloads. Ele pode ser aberto usando-se qualquer editor de texto.

Links relacionados

Como baixar e exibir o arquivo de log do Core

Converter um nó de cluster protegido em uma máquina protegida

No Rapid Recovery, converter um nó do cluster protegido em uma máquina protegida, de modo que ela ainda seja gerenciada pelo Core, mas não faça mais parte do cluster. Isso é útil, por exemplo, se você precisar remover do cluster o nó de cluster, mas ainda mantê-lo protegido.

1 No Rapid Recovery Core Console, navegue até o cluster que contém a máquina a ser convertida e clique em **Nós protegidos**.

2 Na página **Nós protegidos**, a partir do nó específico que deseja converter, clique no menu suspenso Ações e selecione **Converter para agente**.

3 Para adicionar a máquina de volta ao cluster, selecione-a e depois, na página Resumo do menu Ações, selecione **Converter para nó do cluster** e clique em **Sim** para confirmar a ação.

Noções básicas sobre grupos personalizados

O Rapid Recovery Core mostra um menu Máquinas protegidas na área de navegação à esquerda. Ele inclui todas as máquinas ou clusters de servidores adicionados para proteção no seu Rapid Recovery Core. Outros menus poderão ser exibidos dentro deste, se você incluiu esses objetos no seu Core. Da mesma forma, você pode criar um grupo personalizado, o que exibe como o último tipo de menu na área de navegação à esquerda.

O principal benefício de um grupo personalizado é a habilidade de agrupar os objetos do Core em um contêiner lógico. Isso pode ajudá-lo a organizar e gerenciar objetos do Core para um objetivo específico (por exemplo, por organização, centro de custo, departamento, região geográfica e assim por diante).

O ato de criar um grupo sempre adiciona um membro do grupo (por exemplo, uma máquina protegida ou cluster de servidores, uma máquina replicada ou uma máquina somente de pontos de recuperação) ao novo grupo personalizado. O objeto adicionado é determinado pelo seu ponto de origem, quando você cria o grupo. O ideal é, então, adicionar mais membros ao grupo. Depois disso, você pode realizar ações de grupo que se apliquem a todos os membros semelhantes desse grupo personalizado, conforme descrito em Realizar ações de grupo.

Os grupos personalizados podem incluir máquinas protegidas, clusters de servidores, máquinas replicadas e máquinas somente de ponto de recuperação. Os clusters de servidores se comportam da mesma maneira que as máquinas protegidas, exceto que um cluster de servidores e seus nós se comportam como uma única entidade. Se você tentar adicionar um nó de um cluster de servers a um grupo, todo o cluster será adicionado.

Um grupo personalizado pode conter membros semelhantes ou diferentes. Para grupos de membros semelhantes, todas as ações do grupo se aplicam a todos os membros do grupo. Por exemplo, se você forçar um snapshot para um grupo personalizado de máquinas protegidas, será feito um backup de máquina. Para grupos com membros diferentes (por exemplo, máquinas protegidas e replicadas), se você aplicar uma ação de grupo como forçar a replicação, ela se aplicará apenas às máquinas replicadas.

É possível criar um ou mais grupos. Uma única máquina protegida ou replicada pode ser incluída em um ou mais grupos. Dessa forma, é possível agrupar máquinas em seu core da forma que você escolher e executar ações nesse grupo específico.

Cada grupo personalizado aparece na área de navegação à esquerda, com um rótulo que você atribuir. Os grupos com máquinas protegidas padrão aparecem em primeiro lugar no grupo personalizado; as máquinas replicadas serão mostradas abaixo das máquinas protegidas, se for o caso. Se houver alguma máquina somente de ponto de recuperação, ela será listada abaixo das máquinas replicadas.

Na área de navegação à esquerda, cada objeto protegido no Core aparece no seu próprio menu. Os grupos personalizados aparecem no final desses menus.

Incluir uma máquina em um grupo não a remove de seu local original. Por exemplo, se você tiver três máquinas protegidas chamadas Agente1, Agente2 e Agente3 e adicionar o Agente1 ao GrupoPersonalizado1, o Agente1 aparecerá em ambos os locais.

Para obter mais informações, consulte os seguintes tópicos:

- Modificar nomes de grupos personalizados
- Remover grupos personalizados
- Realizar ações de grupo
- Visualizar todas as máquinas de um grupo personalizado em uma página

Criar grupos personalizados

Ao rolar o cursor sobre o nome de qualquer máquina no menu Máquinas protegidas ou Máquinas replicadas, verá uma seta que abre um menu suspenso. Nesse menu, é possível criar um rótulo personalizado.

Use o procedimento abaixo para criar um grupo personalizado.

1 Navegue até o Rapid Recovery Core Console.

2 No menu Máquinas protegidas, máquinas replicadas ou máquinas apenas de pontos de recuperação, faça o seguinte:
   a Coloque o cursor sobre uma máquina no menu.
   b Clique no menu suspenso dessa máquina.
   c Role e selecione **Rotulado como** e clique em **Novo rótulo**.

   A caixa de diálogo **Criar rótulo** é exibida.

3 No campo **Nome**, digite um rótulo adequado para o seu grupo personalizado.

   Use um nome descritivo, que comunique a finalidade do grupo. Por exemplo, para agrupar máquinas protegidas, máquinas replicadas e máquinas apenas de pontos de recuperação por departamento, digite`Accounting Department`. Posteriormente, é possível renomear o grupo.

   NOTA: Os rótulos precisam ter 50 caracteres ou menos. Você pode incluir um único espaço entre as palavras. Você precisa fornecer um rótulo para o seu grupo personalizado.

4 Quando você estiver satisfeito com o nome do rótulo, clique em **OK**.

   A caixa de diálogo é fechada e o grupo personalizado é mostrado como o último elemento na área de navegação esquerda.

5 Como opção, você pode adicionar outras máquinas protegidas, máquinas replicadas ou máquinas apenas de pontos de recuperação a esse grupo. Navegue até o nome da máquina no menu apropriado, clique em seu menu suspenso, role para baixo e selecione **Rotulado como**. Depois, clique no nome do grupo personalizado.

   Agora você pode realizar ações de grupo nesse grupo. Para obter mais informações, consulte Realizar ações de grupo.

Modificar nomes de grupos personalizados

Ao modificar o nome de um grupo personalizado, apenas o rótulo é alterado. Os nomes das máquinas continuam os mesmos.

Use o procedimento abaixo para modificar o nome de um grupo personalizado.

1 Navegue até o Rapid Recovery Core Console.
2 No menu Máquinas protegidas, role o cursor sobre o grupo personalizado que deseja modificar.
3 Clique no menu suspenso desse grupo e clique em **Editar**.
A caixa de diálogo **Editar rótulo** será exibida; nessa caixa, o nome do grupo personalizado torna-se editável.
4 No campo **Nome**, atualize o texto ou exclua o texto do rótulo existente e digite um novo rótulo ou o seu grupo personalizado.
Use um nome descritivo, que comunique a finalidade do grupo. Por exemplo, para agrupar as máquinas protegidas, máquinas replicadas e máquinas apenas de ponto de recuperação por região geográfica, digite `Tokyo`. Posteriormente, é possível renomear o grupo.

NOTA: Os rótulos precisam ter 50 caracteres ou menos. Você pode incluir um único espaço entre as palavras. Você precisa fornecer um rótulo para o seu grupo personalizado.

5 Quando estiver satisfeito com o nome do rótulo, clique em **OK**.
A caixa de diálogo é fechada e o grupo personalizado modificado é exibido como o último elemento da área de navegação à esquerda.
6 Opcionalmente, você pode adicionar outras máquinas protegidas, máquinas replicadas ou máquinas apenas de ponto de recuperação a esse grupo. Opcionalmente, para adicionar outros agentes a esse grupo, navegue até o nome do agente no menu apropriado, clique no menu suspenso para abri-lo, role para baixo e selecione **Rotulado como**. Depois, clique no nome do grupo personalizado.

Remover grupos personalizados

Quando um grupo personalizado é removido, ele é excluído do menu Máquinas protegidas. As máquinas que estavam no grupo não são removidas e ainda podem ser encontradas no menu padrão apropriado.

Use o procedimento abaixo para remover um grupo personalizado.

1 Navegue até o Rapid Recovery Core Console.
2 No menu Máquinas protegidas, role o cursor sobre o grupo personalizado que deseja remover.
3 Clique no menu suspenso desse grupo e clique em **Remover rótulo**.
Aparece uma mensagem pedindo confirmação para a remoção do grupo.
4 Confirmar a remoção do grupo personalizado.
A caixa de diálogo é fechada e o grupo personalizado é removido da área de navegação.

Realizar ações de grupo

É possível realizar ações de grupo em qualquer grupo que apareça na área de navegação à esquerda do Rapid Recovery Core Console. Se o grupo contiver membros diferentes (por exemplo, máquinas replicadas e máquinas de apenas pontos de recuperação), as ações solicitadas serão realizadas apenas nos membros do grupo relevantes.

Use o procedimento abaixo para realizar ações de grupo em um grupo personalizado.

1 Navegue até o Rapid Recovery Core Console.
2 No menu Máquinas protegidas, role o cursor sobre o grupo personalizado no qual deseja realizar uma ação de grupo.
3 Clique no menu suspenso desse grupo e selecione uma ação, como a seguir:
- Para forçar um snapshot incremental ou uma imagem de base de todas as máquinas protegidas, clique em **Forçar snapshot** ou em **Forçar imagem de base**, conforme o caso. Para obter mais informações, consulte Forçar um snapshot.
- Para pausar a proteção de todas as máquinas protegidas no grupo, clique em **Pausar proteção** e especifique os parâmetros de retomada. Para obter mais informações, consulte Pausar e retomar a replicação.
- Para retomar a proteção de todas as máquinas protegidas no grupo cuja proteção tenha sido pausada, clique em **Retomar proteção** e confirme que deseja retomar. Para obter mais informações, consulte Pausar e retomar a replicação.
- Para atualizar as informações de todos os objetos no grupo, clique em **Atualizar metadados**.
- Para pausar a replicação de todas as máquinas replicadas nesse grupo, em Replicação, clique em **Pausar**. Para obter mais informações, consulte Pausar e retomar a replicação.
- Para retomar a replicação de todas as máquinas replicadas nesse grupo cuja replicação tenha sido pausada, em Replicação, clique em **Retomar**. Para obter mais informações, consulte Pausar e retomar a replicação

- Para forçar a replicação de todas as máquinas replicadas nesse grupo, em Replicação, clique em **Forçar**. Para obter mais informações, consulte Forçar a replicação.
- Para remover a replicação de todas as máquinas replicadas nesse grupo, em Replicação, clique em **Remover**. Para obter mais informações, consulte Remover replicação de entrada do Core de destino.
- Para remover as máquinas de apenas pontos de recuperação deste Core e descartar os pontos de recuperação, em Apenas pontos de recuperação, clique em **Remover pontos de recuperação**.
- Apenas para grupos personalizados, para modificar o rótulo deles, selecione **Editar**. Para obter mais informações, consulte Modificar nomes de grupos personalizados.
- Apenas para grupos personalizados, para remover o grupo personalizado do menu de navegação, selecione **Remover rótulo**. Para obter mais informações, consulte Remover grupos personalizados.

Visualizar todas as máquinas de um grupo personalizado em uma página

Clique no nome de um grupo personalizado para ver a página Máquinas que relaciona todas as máquinas nesse grupo personalizado. É possível então realizar algumas funções em todas as máquinas a partir do menu Ações ou realizar funções individualmente selecionando os comandos de cada máquina individual.

Sobre como proteger diversas máquinas

Você pode adicionar duas ou mais máquinas Windows para proteção no Rapid Recovery Core simultaneamente usando o Assistente de proteção de diversas máquinas. Para proteger os dados usando o Rapid Recovery, você precisa adicionar as estações de trabalho e os servidores no Rapid Recovery Core Console; por exemplo, o Exchange Server, o SQL Server, o servidor Linux etc.

Assim como acontece na proteção de máquinas individuais, a proteção de diversas máquinas simultaneamente requer a instalação do software do agente Rapid Recovery em cada máquina que você deseja proteger.

NOTA: Como uma exceção a essa regra, caso esteja protegendo máquinas virtuais em um host de VMware ou ESXi, você pode usar a proteção sem agente. Para obter mais informações, inclusive restrições da proteção sem agente, consulte Como entender o recurso Rapid Snap for virtual.

As máquinas protegidas devem ser configuradas com uma política de segurança que possibilite a instalação remota.

Para se conectar às máquinas, elas devem ser ligadas e estar acessíveis.

Há mais de um método de implementar o software Agent em várias máquinas simultaneamente. Por exemplo:

- Você pode instalar o software do agente Rapid Recovery em diversas máquinas usando o Assistente implantar software do agente. Para obter mais informações, consulte Implantação do software do agente Rapid Recovery em uma ou mais máquinas.
- Você pode implantar o software do agente Rapid Recovery como parte do Assistente de proteção de diversas máquinas.

O processo de proteger diversas máquinas inclui etapas opcionais que você pode acessar caso selecione uma configuração avançada. As opções avançadas incluem funções de repositório e criptografia. Por exemplo, você pode especificar um repositório do Rapid Recovery existente para salvar snapshots ou criar um novo repositório. Você também pode especificar uma chave de criptografia existente (ou adicionar uma nova chave de criptografia) para aplicar os dados salvos no Core para as máquinas protegidas.

O fluxo de trabalho do Assistente de proteção de diversas máquinas pode ser ligeiramente diferente com base no seu ambiente. Por exemplo, caso o software do agente Rapid Recovery esteja instalado nas máquinas que você deseja proteger, você não deve instalá-lo pelo assistente. Da mesma forma, caso um repositório já exista no Core, você não precisa criar um.

Ao proteger diversas máquinas, siga o procedimento apropriado, com base na configuração. Consulte as seguintes opções para proteger diversas máquinas:

- Proteger várias máquinas em um domínio do Active Directory
- Como proteger várias máquinas em um host virtual VMware vCenter/ESX(i)
- Como proteger diversas máquinas manualmente

Proteger várias máquinas em um domínio do Active Directory

Use este procedimento para proteger uma ou mais máquinas simultaneamente em um domínio do Active Directory.

1 No Rapid Recovery Core Console, clique no menu suspenso **Protect (Proteger)** e, em seguida, clique em **Protect Multiple Machines (Proteger várias máquinas)**.

O assistente Proteger várias máquinas é mostrado.

2 Na página **Welcome (Boas-vindas)** do assistente, selecione uma das opções a seguir:

- Normal
- Advanced (show optional steps) (Avançado, mostrar etapas opcionais)

3 Clique em **Avançar**.

4 Na página **Connection (Conexão)** do assistente, na lista suspensa **Source (Origem)**, selecione **Active Directory**.

5 Digite as informações de domínio e credenciais de acesso conforme descrito na tabela a seguir.

Tabela 79. Informações e credenciais de domínio

Caixa de texto	Descrição
Host	O nome do host ou o endereço IP do domínio do Active Directory.
Nome de usuário	O nome de usuário para se conectar a esse domínio; por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
Password (Senha)	A senha segura usada para conectar-se ao domínio.

6 Clique em **Avançar**.

7 Na página **Select Machines (Selecionar máquinas)** do assistente, selecione as máquinas que você deseja proteger.

O sistema verifica automaticamente cada máquina selecionada.

8 Clique em **Avançar**.

Se a página **Protection (Proteção)** aparecer ao lado do assistente Proteger múltiplas máquinas, pule para a etapa 11.

Se o software de agente ainda não estiver implementado nas máquinas que você deseja proteger, ou se qualquer uma das máquinas que você especificou não possam ser protegidas por qualquer razão, então as máquinas selecionadas aparecem na página Warnings (Avisos).

9 Opcionalmente, na página **Warnings (Avisos)** do assistente, é possível verificar qualquer máquina selecionando-a e depois clicando em **Verify (Verificar)** na barra de ferramentas.

10 Opcionalmente, na página **Warnings (Avisos)**, selecione a opção **After Agent installation, restart the machines automatically (Depois da instalação, reiniciar as máquinas automaticamente)**.

NOTA: A Dell recomenda essa opção. Você precisa reiniciar as máquinas de agente antes que possam ser protegidas.

11 Se o status indicar que a máquina pode ser contata, clique em **Next (Avanar)** para instalar o software do agente Rapid Recovery.

A página **Protection (Proteção)** é mostrada.

12 Na página **Protection (Proteção)** do assistente, selecione a programação de proteção adequada como descrito abaixo.

- Se quiser usar o cronograma de proteção padrão, selecione **Default protection (hourly snapshots of all volumes) (Proteção padrão (instantâneos de todos os volumes a cada hora))** na opção Schedule Settings (Configurações de cronograma).
- Se quiser definir outro cronograma de proteção, selecione **Custom protection (Proteção personalizada)** na opção Schedule Settings (Configurações de cronograma).

13 Prossiga com a configuração da seguinte forma:

- Se você tiver selecionado uma configuração típica no Assistente de proteção da máquina e especificado proteção padrão, clique em **Finish (Concluir)** para confirmar suas escolhas, feche o assistente e proteja a máquina que você especificou.

  Quando você adicionar a proteção para uma determinada máquina pela primeira vez, uma imagem base (ou seja, um instantâneo de todos os dados armazenados nos volumes protegidos) será transferida para o repositório no Rapid Recovery Core, seguindo a programação definida, a menos que você tenha especificado pausar inicialmente a proteção.
- Se você selecionou uma configuração típica para o assistente Proteger máquina e especificou a proteção personalizada, clique em **Next (Avançar)** e consulte Criar programações de proteção personalizadas.

- Se você tiver selecionado uma configuração avançada no Assistente de proteção da máquina e especificado proteção padrão, clique em **Next (Avançar)** e continue na Etapa 15 para ver as opções de repositório e criptografia.
- Se você tiver selecionado uma configuração avançada no Assistente de proteção da máquina e especificado proteção personalizada, clique em **Next (Avançar)** para configurar uma programação de proteção personalizada. Para obter detalhes sobre como definir uma programação de proteção personalizada, consulte Criar programações de proteção personalizadas.

14 Clique em **Avançar**.

15 Na página **Repository (Repositório)** do assistente, realize uma das opções a seguir:

- Se você já possui um repositório e quer armazenar os dados dessa máquina para proteção no repositório existente, faça o seguinte:

  1 Selecione **Use an existing repository (Usar um repositório existente)**.

  2 Selecione um repositório existente da lista.

  3 Clique em **Avançar**.

  A página **Encryption (Criptografia)** é mostrada. Pule para a etapa 19 para definir a criptografia (opcional).

- Se quiser criar um repositório, selecione **Create a Repository (Criar um repositório)** e depois prossiga para as etapas a seguir.

  1 Na página **Repository (Repositório)**, digite as informações descritas na tabela a seguir.

Tabela 80. Configurações para adicionar novo repositório

Caixa de texto	Descrição
Nome do repositório	Insira o nome de exibição do repositório. Por padrão, essa caixa de texto é composta da palavra Repositório e um número, que corresponde ao número de repositórios deste Core. Por exemplo, se esse é o primeiro repositório, o nome padrão é Repositório 1. Altere o nome conforme necessário. Os nomes de repositório devem conter entre 1 e 40 caracteres alfanuméricos, incluindo espaços. Não use caracteres proibidos nem frases proibidas.
Operações simultâneas	Defina o número de solicitações simultâneas que você quer que o repositório suporte. Por padrão, o valor é 64.
Comentários	Opcionalmente, insira uma observação descritiva sobre esse repositório. É possível digitar até 254 caracteres. Por exemplo, digite **Repositório DMV 2**

  2 Clique em **Add Storage Location (Adicionar local de armazenamento)** para definir o local de armazenamento específico ou volume para o repositório. Esse volume deve ser um local de armazenamento primário.

> △ **CUIDADO: Defina uma pasta exclusiva dentro do diretório raiz para o local de armazenamento de seu repositório. Não especifique o diretório raiz. Por exemplo, use E:\Repository\, não E:\. Se o repositório que você estiver criando nessa etapa for removido posteriormente, todos os arquivos no local de armazenamento de seu repositório serão apagados. Se você definir seu local de armazenamento no diretório raiz, todos os outros arquivos no volume (por exemplo, E:\) são apagados, o que pode resultar em uma perda catastrófica de dados**

  A caixa de diálogo **Add Storage Location (Adicionar local de armazenamento)** é mostrada.

  3 Clique em **Add Storage Location (Adicionar local de armazenamento)** para definir o local de armazenamento específico ou volume para o repositório. Esse volume deve ser um local de armazenamento primário.

  4 Na área **Storage Location (Local de armazenamento)**, especifique como adicionar o arquivo para o local de armazenamento. Você pode optar por adicionar um volume de armazenamento conectado localmente (como armazenamento conectado diretamente, uma rede de área de armazenamento ou armazenamento conectado de rede). Você também pode especificar um volume de armazenamento em um local compartilhado de sistema de arquivo de Internet comum (CIFS)

  - Selecione **Add file on local disk (Adicionar arquivo em disco local)** para especificar uma máquina local e depois insira as informações conforme descrito na tabela a seguir.

Tabela 81. Configurações de disco local

Caixa de texto	Descrição
Caminho de dados	Digite o local para armazenar os dados protegidos.

Caixa de texto	Descrição
	Por exemplo, digite `X:\Repository\Data`. Ao especificar o caminho, use somente caracteres alfanuméricos, o hífen e o ponto final (apenas para separar os nomes de host e domínios). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Caminho de metadados	Digite o local para armazenar os metadados protegidos. Por exemplo, digite `X:\Repository\Metadata`. Ao especificar o caminho, use somente caracteres alfanuméricos, o hífen e o ponto final (apenas para separar os nomes de host e domínios). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

- Ou selecione **Add file on CIFS share (Adicionar arquivo no compartilhamento CIFS)** para especificar um local de compartilhamento de rede e depois insira as informações conforme descrito na tabela a seguir.

Tabela 82. Credenciais de compartilhamento de CIFS

Caixa de texto	Descrição
Caminho UNC	Digite o caminho para o local de compartilhamento de rede. Se esse local estiver no diretório raiz, defina um nome de pasta exclusivo (por exemplo, `Repository`). O caminho deve começar com \\. Ao especificar o caminho, use somente caracteres alfanuméricos, o hífen e o ponto final (apenas para separar os nomes de host e domínios). As letras a a z não diferenciam maiúsculas de minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Nome de usuário	Especifique um nome de usuário para acessar o local de compartilhamento da rede.
Password (Senha)	Especifique uma senha para acessar o local de compartilhamento da rede.

5 Na área **Storage Configuration (Configuração de armazenamento)**, clique em **More Details (Mais detalhes)** e insira os detalhes para o local de armazenamento como descrito na tabela a seguir.

Tabela 83. Detalhes de configuração de armazenamento

Caixa de texto	Descrição
Tamanho	Defina o tamanho ou a capacidade do local de armazenamento. O tamanho mínimo é de 1 GB. O padrão é de 250 GB. Você pode escolher entre: • GB • TB **NOTA: O tamanho que você especificar não pode exceder o tamanho do volume.** Se o local de armazenamento for um volume New Technology File System (NTFS) usando o Windows XP ou Windows 7, o limite do tamanho do arquivo é 16 TB. Se o local de armazenamento for um volume NTFS usando o Windows 8, 8.1, Windows 10, Windows Server 2012 ou 2012 R2, o limite do tamanho do arquivo é de 256 TB. **NOTA: Para que o Rapid Recovery valide o sistema operacional, o Windows Management Instrumentation (WMI) precisa ser instalado no local de armazenamento pretendido.**
Política do cache de gravação	A política do cache de gravação controla o modo como o Windows Cache Manager é usado no repositório e ajuda a ajustar o repositório para obter o desempenho ideal em configurações diferentes. Configure o valor como uma das seguintes opções: • Ligado

Caixa de texto	Descrição
	• Apagado • Sincronizar Se ativada, que é a configuração padrão, o Windows controla o cache. Isso é adequado para o Windows 10 e para versões do Windows Server 2012 e mais recentes. **NOTA: Ativar a política de cache de gravação pode melhorar o desempenho. Se estiver usando o Windows Server 2008 SP2 ou Windows Server 2008 R2 SP2, recomenda-se a configuração desligado.** Se desativar a configuração, o Rapid Recovery controla o cache. Se configurado como Sync (Sincronizar), o Windows controla o cache e a entrada/saída síncrona.
Bytes por setor	Especifique o número de bytes que você quer que cada setor contenha. O valor padrão é 512.
Média de bytes por registro	Especifique o número médio de bytes por registro. O valor padrão é 8192.

6 Clique em **Avançar**.

Se você selecionar a opção **Advanced (Avançado)** na etapa 1, a página **Encryption (Criptografia)** é mostrada.

16 Opcionalmente, na página **Encryption (Criptografia)** do assistente, para ativar a criptografia, selecione **Enable Encryption (Ativar criptografia)**.

Os campos Encryption key (Chave de criptografia) são mostrados na página Encryption (Criptografia).

NOTA: Se você ativar a criptografia, será aplicada a todos para todos os volumes protegidos dessa máquina. É possível alterar as configurações posteriormente napágina Encryption Keys (Chaves de criptografia) do Console Core do Rapid Recovery. Para obter mais informações sobre criptografia, consulte o tópico Compreender as chaves de criptografia.

CUIDADO: O Rapid Recovery usa uma criptografia AES de 256 bits no modo CBC (Encadeamento de blocos de criptografia) com chaves de 256 bits. Apesar de o uso de criptografia ser opcional, a Dell recomenda que você estabeleça uma chave de criptografia e proteja a senha que você definir. Guarde a senha em um local seguro, pois ela é essencial para a recuperação de dados. Sem a senha, a recuperação de dados não é possível.

17 Se quiser criptografar essas máquinas protegidas usando uma chave de criptografia que já está definida neste Rapid Recovery Core, selecione **Encrypt data using an existing Encryption key (Criptografar dados usando uma chave de criptografia existente)** e depois selecione a chave adequada no menu suspenso. Prossiga para a próxima etapa.

Prossiga para a etapa 19.

18 Se quiser adicionar uma nova chave de criptografia no Core e aplicar essa chave às máquinas protegidas, insira as informações como descrito na tabela a seguir.

Tabela 84. Configurações de chave de criptografia

Caixa de texto	Descrição
Nome	Digite um nome para a chave de criptografia. Os nomes de chave de criptografia devem conter entre 1 e 130 caracteres alfanuméricos. Você não pode incluir caracteres especiais como barra, barra invertida, barra vertical, dois pontos, asterisco, aspas, ponto de interrogação, parênteses iniciais ou finais, & ou traço.
Descrição	Digite um comentário para a chave de criptografia. Essas informações aparecem no campo Description (Descrição) ao ver chaves de criptografia no Core Console.
Passphrase (Senha)	Digite a senha que será usada para controlar o acesso. O recomendado é evitar os caracteres especiais listados acima.

Caixa de texto	Descrição
	Anote a senha em um local seguro. O suporte da Dell não pode recuperar uma senha. Depois de criar uma chave de criptografia e aplicá-la a uma ou mais das máquinas protegidas, você não pode recuperar os dados se perder a senha.
Confirm Passphrase (Confirmar senha)	Digite novamente a senha que você acabou de digitar.

19 Clique em **Finish (Concluir)** para salvar e aplicar as configurações.

O assistente é fechado.

20 Se a página **Warning (Aviso)** foi exibida e você estiver satisfeito com as seleções, clique em **Finish (Finalizar)** novamente.

O software do agente Rapid Recovery é implantado nas máquinas especificadas, se necessário, e as máquinas são adicionadas para a proteção no Core.

Como proteger várias máquinas em um host virtual VMware vCenter/ESX(i)

Use este procedimento para proteger simultaneamente uma ou mais máquinas em um host virtual VMware vCenter/ESX(i).

CUIDADO: Se você usar proteção sem agente, a Dell recomenda que você limite a proteção para não mais de 200 máquinas virtuais em uma vez. Por exemplo, não selecione mais de 200 VMs quando usando o Assistente para proteger várias máquinas. Proteger mais de 200 máquinas virtuais resulta em desempenho lento. Não há limite para quantas máquinas virtuais um Core pode proteger sem agente com o passar do tempo. Por exemplo, você pode proteger 200 VMs hoje e outras 200 amanhã.

1 No Rapid Recovery Core Console, clique no menu suspenso **Protect (Proteger)** e, em seguida, clique em **Protect Multiple Machines (Proteger várias máquinas)**.

O Assistente para proteger várias máquinas é aberto.

2 Na página de boas-vindas, selecione uma das opções a seguir:

- Normal
- Avançado (mostrar etapas opcionais)

3 Clique em **Next (Avançar)**.

4 Na página Conexão do assistente, a partir da lista suspensa **Source (Fonte)**, selecione **vCenter / ESX(i)**.

5 Digite as informações de host e credenciais de logon como descrito na tabela a seguir.

Tabela 85. Configurações de conexão para VCenter/ESX(i)

Caixa de texto	Descrição
Host	Digite o nome ou endereço IP do host virtual VMware vCenter Server/ESX(i).
Port (Porta)	A porta usada para fazer a conexão com o host virtual. A configuração padrão é 443.
Nome de usuário	O nome do usuário usado para se conectar ao host virtual; por exemplo, Administrador ou, se a máquina estiver em um domínio, [nome de domínio]\Administrador.
Password (Senha)	Digite a senha usada para conectar-se a este host virtual.

- Para usar a proteção sem agente, selecione **Protect selected VMs Agentlessly (Proteger VMs selecionados sem agente)**, e, em seguida, consulte Como proteger máquinas virtuais vCenter/ESXi sem o agente Rapid Recovery.

6 Na página Selecionar máquinas, selecione uma das seguintes opções no menu suspenso:

- Hosts e Clusters
- VMs e Modelos

7 Expanda a lista de máquinas e selecione as VMs que você quer proteger.

Uma notificação será exibida se o Rapid Recovery detectar que uma máquina está off-line ou não tem o VMware Tools instalado.

8 Clique em **Next (Avançar)**.

9 Na página Ajustes, digite as credenciais para cada máquina no seguinte formato: `hostname::username::password`.

NOTA: Digite uma máquina em cada linha.

10 Clique em **Next (Avançar)**.

Se a página Proteção aparece próximo no Assistente para proteger várias máquinas, vá para a Etapa 14.

Se o software do agente ainda não está implementado nas máquinas que você quer proteger, ou se qualquer das máquinas que você especificou não pode ser protegida por um outro motivo, as máquinas selecionadas aparecem na página Advertências.

11 Opcionalmente, na página Advertências, você pode verificar qualquer máquina, selecionando a máquina e, em seguida, clicando em **Verifiy (Verificar)** na barra de ferramentas.

12 Opcionalmente, na página Avisos, selecione **After Agent installation, restart the machines automatically (Após instalação do agente, reinicie as máquinas automaticamente)**.

NOTA: A Dell recomenda esta opção. Você precisa reiniciar as máquinas agente antes que elas possam ser protegidas.

13 Se o status indica que a máquina pode ser acessada, clique em **Next (Avançar)** para instalar o software do agente.

A página Proteção é exibida.

14 Na página Proteção, selecione a programação de proteção adequada, conforme descrito abaixo.

- Para usar o cronograma de proteção padrão, selecione **Default protection (hourly snapshots of all volumes) (Proteção padrão (instantâneos de todos os volumes a cada hora))** na opção Schedule Settings (Configurações de cronograma).
- Se quiser definir outro cronograma de proteção, selecione **Custom protection (Proteção personalizada)** na opção Schedule Settings (Configurações de cronograma).

15 Prossiga com a configuração da seguinte forma:

- Se você tiver selecionado uma configuração típica no Assistente de proteção da máquina e especificado proteção padrão, clique em **Finish (Concluir)** para confirmar suas escolhas, feche o assistente e proteja a máquina que você especificou.

  Quando você adicionar a proteção para uma determinada máquina pela primeira vez, uma imagem base (ou seja, um instantâneo de todos os dados armazenados nos volumes protegidos) será transferida para o repositório no Rapid Recovery Core, seguindo a programação definida, a menos que você tenha especificado pausar a proteção inicialmente.
- Se você tiver selecionado uma configuração Típica para o Assistente de proteção da máquina e especificado uma proteção personalizada, clique em **Next (Avançar)** para configurar um cronograma de proteção personalizado. Para obter detalhes sobre como definir um cronograma de proteção personalizado, consulte Criar programações de proteção personalizadas.
- Se você tiver selecionado uma configuração avançada no Assistente de proteção da máquina e especificado proteção padrão, clique em **Next (Avançar)** e continue na Etapa 17 para ver as opções de repositório e criptografia.
- Se você tiver selecionado uma configuração Avançada para o Assistente de proteção da máquina e especificado uma proteção personalizada, clique em **Next (Avançar)** para configurar um cronograma de proteção personalizado. Para obter detalhes sobre como definir um cronograma de proteção personalizado, consulte Criar programações de proteção personalizadas.

16 Clique em **Next (Avançar)**.

17 Na página **Repository (Repositório)**, realize uma das seguintes ações:

- Se você já tiver um repositório e quer armazenar os dados da máquina para proteção no repositório existente, faça o seguinte:
  1 Selecione **Use an existing repository (Usar um repositório existente)**.
  2 Selecione um repositório existente na lista.
  3 Clique em **Next (Avançar)**.

  A página **Encryption (Criptografia)** é exibida. Vá para a Etapa 18 para definir a criptografia opcionalmente.
- Se você quer criar um repositório, selecione **Create a Repository (Criar um repositório)**, e, em seguida, execute o procedimento a seguir.
  1 Na página **Options (Opções)**, digite as informações descritas na tabela a seguir.

Tabela 86. Adicionar novas configurações de repositório

Caixa de texto	Descrição
Nome do repositório	Insira o nome de exibição do repositório. Por padrão, esta caixa de texto consiste em a palavra Repositório e um número que corresponde ao número de repositórios para este núcleo. Por exemplo, se este é o primeiro repositório, o nome padrão é Repositório 1. Altere o nome, conforme a necessidade.

Caixa de texto	Descrição
	Os nomes de repositório devem conter entre 1 e 40 caracteres alfanuméricos, incluindo espaços. Não use caracteres proibidos ou frases proibidas.
Operações simultâneas	Defina o número de solicitações simultâneas que você quer que o repositório suporte. Por padrão, o valor é 64.
Comentários	Opcionalmente, digite uma nota descritiva sobre esse repositório. Você pode digitar até 254 caracteres. Por exemplo, digite **DVM Repositório 2.**

2 Clique em **Add Storage Location (Adicionar armazenamento local)** para definir o local de armazenamento ou volume para o repositório específico. Este volume deve ser um local de armazenamento primário.

> **CUIDADO: Defina uma pasta na raiz dedicada para o local de armazenamento para seu repositório. Não especifique o local de raiz. Por exemplo, use E:\Repository\, não E:\. Se o repositório que você está criando em esta etapa for removido posteriormente, todos os arquivos, no local de armazenagem do seu repositório serão apagados. Se você definir o local de armazenamento na raiz, todos os outros arquivos no volume (por exemplo: E:\) são apagados, o que poderia resultar em uma perda de dados catastrófica.**

A caixa de diálogo **Add Storage Location** (Adicionar local de armazenamento) é mostrada.

3 Clique em **Add Storage Location (Adicionar local de armazenamento)** para definir o local de armazenamento ou volume para o repositório específico. Este volume deve ser um local de armazenamento primário.

4 Na área **Storage Location (Local de armazenamento)**, especifique como adicionar o arquivo para o local de armazenamento. Você pode escolher para adicionar um volume de armazenamento conectado localmente (como, por exemplo, armazenamento de conexão direta, uma rede de armazenamento de dados, ou armazenamento ligado à rede). Você pode também especificar um volume de armazenamento em um sistema de arquivos comuns de Internet (CIFS) compartilhados local.

- Selecione **Add file on local disk (Adicionar arquivo no disco local)** para especificar uma máquina local e, em seguida, insira as informações, conforme descrito na tabela a seguir.

Tabela 87. Configurações de disco local

Caixa de texto	Descrição
Caminho de dados	Digite o local para armazenar os dados protegidos. Por exemplo, digite `X:\Repository\Data`. Ao especificar o caminho, use somente caracteres alfanuméricos, o hífen e o ponto final (apenas para separar os nomes de host e domínios). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caracteres de pontuação são permitidos.
Caminho de metadados	Digite o local para armazenar os metadados protegidos. Por exemplo, digite `X:\Repository\Metadata`. Ao especificar o caminho, use somente caracteres alfanuméricos, o hífen e o ponto final (apenas para separar os nomes de host e domínios). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caracteres de pontuação são permitidos.

- Ou, selecione **Add file on CIFS share (Adicionar arquivo no compartilhamento CIFS)** para especificar um local de compartilhamento de rede e, em seguida, insira as informações, conforme descrito na tabela a seguir.

Tabela 88. Credenciais para compartilhamento CIFS

Caixa de texto	Descrição
Caminho UNC	Digite o caminho para o local de compartilhamento de rede. Se este local está na raiz, defina um nome de pasta dedicado (por exemplo, `Repository`). O caminho dever começar com \\. Ao especificar o caminho, use somente caracteres alfanuméricos, o hífen e o ponto final (apenas para separar os nomes de host e domínios). As letras

Caixa de texto	Descrição
	A a Z fazem distinção entre maiúsculas e minúsculas. Não use espaços. Nenhum caractere de símbolo ou de pontuação é permitido.
Nome de usuário	Especifique um nome de usuário para acessar o local de compartilhamento da rede.
Password (Senha)	Especifique uma senha para acessar o local de compartilhamento da rede.

5 Na área **Storage Configuration (Configuração de armazenamento)**, clique em **More Details (Mais detalhes)** e digite os detalhes para o local de armazenamento, conforme descrito na tabela a seguir.

Tabela 89. Detalhes da configuração de armazenamento

Caixa de texto	Descrição
Tamanho	Defina o tamanho ou capacidade para o local de armazenamento. O tamanho mínimo é de 1 GB. O padrão é 250 GB. Você pode escolher entre as seguintes: • GB • TB **NOTA: O tamanho que você especificar não pode exceder o tamanho do volume.** Se o local de armazenamento for um volume New Technology File System (NTFS) usando o Windows XP ou Windows 7, o limite do tamanho do arquivo é 16 TB. Se o local de armazenamento é um volume NTFS usando o Windows 8, 8,1, Windows 10, ou o Windows Server 2012, 2012 R2, o limite do tamanho do arquivo é de 256 TB. **NOTA: Para o Rapid Recovery validar o sistema operacional, o Windows Management Instrumentation (WMI) precisa ser instalado no local de armazenamento pretendido.**
Política do cache de gravação	A política do cache de gravação controla o modo como o Windows Cache Manager é usado no repositório e ajuda a ajustar o repositório para obter o desempenho ideal em configurações diferentes. Configure o valor como uma das seguintes opções: • Ligado • Apagado • Sincronizar Se essa opção estiver definida para On (Ligado), que é o padrão, o Windows controla o armazenamento em cache. Este é adequado para o Windows 10, e para as versões do Windows Server 2012 e versões posteriores. **NOTA: Configurar a política do cache de gravação para On (Ligado) pode resultar em um desempenho mais rápido. Se você estiver usando o Windows Server 2008 SP2 ou o Windows Server 2008 R2 SP2, a configuração recomendada é Off (Desligado).** Se configurado como Off (Apagado), o Rapid Recovery controla o cache. Se configurado como Sync (Sincronizar), o Windows controla o cache e a entrada/saída síncrona.
Bytes por setor	Especifique o número de bytes que você quer que cada setor contenha. O valor padrão é 512.
Média de bytes por registro	Especifique o número médio de bytes por registro. O valor padrão é 8192.

6 Clique em **Next (Avançar)**.

Se você escolher a opção **Advanced (Avançado)** na Etapa 1, a página **Encryption (Criptografia)** é exibida.

18 Opcionalmente, na página Criptografia, para ativar a criptografia, selecione **Enable Encryption (Ativar a criptografia)**.

Os campos Encryption key (Chave de criptografia) são mostrados na página Encryption (Criptografia).

NOTA: Se você ativar a criptografia, ela será aplicada aos dados para todos os volumes protegidos para essa máquina agente. Você pode alterar as configurações depois a partir da guia Configuração no Rapid Recovery Core Console. Para obter mais informações sobre criptografia, consulte o tópico Compreender as chaves de criptografia.

CUIDADO: O Rapid Recovery usa uma criptografia AES de 256 bits no modo CBC (Encadeamento de blocos de criptografia) com chaves de 256 bits. Apesar de o uso de criptografia ser opcional, a Dell recomenda que você estabeleça uma chave de criptografia e proteja a senha que você definir. Guarde a senha em um local seguro, pois ela é essencial para a recuperação de dados. Sem a senha, a recuperação de dados não é possível.

19 Se você deseja criptografar estas máquinas protegidas usando uma chave de criptografia que já está definida neste Rapid Recovery Core, selecione **Encrypt data using an existing Encryption key(Criptografar dados usando umq chave de criptografia existente)**, e selecione a chave correspondente no menu suspenso.

Vá para a Etapa 21.

20 Se você quer adicionar uma nova chave de criptografia para o Core e aplicar essa chave para estas máquinas protegidas, insira as informações, conforme descrito na tabela a seguir.

Tabela 90. Configurações para chave de Criptografia

Caixa de texto	Descrição
Nome	Digite um nome para a chave de criptografia. Os nomes de chaves de criptografia devem conter entre 1 e 130 caracteres alfanuméricos. Você pode não ter caracteres especiais, como a barra invertida, barra, tubo, dois-pontos, asterisco aspas, ponto de interrogação, abrir ou fechar suportes, e comercial ou hash.
Descrição	Digite um comentário para a chave de criptografia. Essas informações é exibida no campo Description (Descrição) ao ver chaves de criptografia do Core Console.
Passphrase (Senha)	Digite a senha que será usada para controlar o acesso. Prática recomendada é para evitar caracteres especiais listados acima. Registre a senha em um local seguro. O Suporte da Dell não pode recuperar uma senha. Uma vez que você criar uma chave de criptografia e aplicar ela em uma ou mais máquinas protegidas, não será possível recuperar os dados se você perder a senha.
Confirm Passphrase (Confirmar senha)	Digite novamente a senha que você acabou de digitar.

21 Clique em **Finish (Concluir)** para salvar e aplicar as configurações.

22 Se a página Avisos apareceu e você ainda estiver satisfeito com suas seleções, clique em **Finish (Concluir)** novamente.

O software do agente Rapid Recovery é implementado nas máquinas especificadas, se necessário, e as máquinas são adicionadas à proteção do Core.

Como proteger diversas máquinas manualmente

Use esse procedimento para inserir manualmente cada máquina que você deseja proteger. É usado, por exemplo, ao proteger máquinas Linux.

1 No Rapid Recovery Core Console, clique no menu suspenso **Proteger** e em **Proteger diversas máquinas**.

O Assistente de proteção de diversas máquinas é aberto.

2 Na página **Bem-Vindo**, selecione uma das seguintes opções:

- Normal
- Avançado (exibir etapas opcionais)

3 Clique em **Avançar**.

4 Na página **Conexão** do assistente, na lista suspensa **Origem**, selecione **Manualmente**.

5 Clique em **Avançar**.

6 Na página **Selecionar máquinas**, insira os detalhes da máquina na caixa de diálogo no formato `hostname::username::password::port`. A configuração de porta é opcional. Entre os exemplos estão:

`10.255.255.255::administrator::&11@yYz90z::8006`

`abc-host-00-1::administrator::99!zU$o83r::168`

7 Clique em **Avançar**.

Caso a página **Proteção** seja exibida depois do Assistente de proteção de diversas máquinas, passe à Etapa 11.

Se o software do agente ainda não tiver sido implementado nas máquinas que você deseja proteger ou se alguma das máquinas especificadas não puder ser protegida por outro motivo, as máquinas selecionadas aparecerão na página **Avisos**.

8 Como opção, na página **Avisos de máquinas**, você pode confirmar qualquer máquina selecionando-a e depois clicando em **Confirmar** na barra de ferramentas.

9 Como opção, na página **Avisos de máquinas**, selecione **Após a instalação do Agent, reiniciar as máquinas automaticamente**.

NOTA: A Dell recomenda esta opção. Reinicie as máquinas agente antes de protegê-las. A reinicialização garante que o serviço do agente está em execução e que o módulo de kernel adequado seja usado para proteger a máquina, se relevante.

10 Se o status indicar que a máquina está acessível, clique em **Avançar** para instalar o software Agent.

A página **Proteção** é exibida.

11 Na página **Proteção**, selecione a programação de proteção adequada, como descrito a seguir.

- Se desejar usar a programação de proteção padrão, na opção Definições de programação, selecione **Proteção padrão (snapshots horários de todos os volumes)**.
- Se desejar definir um programa de proteção diferente, na opção Definições de programa, selecione **Proteção personalizada**.

12 Prossiga com a configuração da seguinte maneira:

- Se a configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção padrão tiver sido especificada, clique em **Concluir** para confirmar suas escolhas, fechar o assistente e proteger a máquina especificada.

  Na primeira vez em que a proteção for adicionada para uma máquina, uma imagem de base (ou seja, um snapshot de todos os dados nos volumes protegidos) será transferida para o repositório no Rapid Recovery Core seguindo o programa definido por você, a menos que tenha especificado pausar proteção inicialmente.
- Caso você tenha selecionado uma configuração Típico para o Assistente de proteção de máquina e especificado uma proteção personalizada, clique em **Avançar** consulte Criar programações de proteção personalizadas.
- Se a configuração Avançado do Assistente de proteção de máquina e a proteção padrão tiverem sido selecionadas, clique em **Avançar** e vá até a Etapa 14 para ver as opções de repositório e criptografia.
- Se a configuração Avançado do Assistente de proteção de máquina e a proteção personalizada tiverem sido especificadas, clique em **Avançar** para definir um programa de proteção personalizado. Para obter detalhes sobre a definição de um programa de proteção personalizada, consulte Criar programações de proteção personalizadas.

13 Na página **Repositório**, o seguinte:

- Caso você já tenha um repositório e queira armazenar os dados dessa máquina para proteção no repositório existente, faça o seguinte:
  1 Selecione **Utilize um repositório existente**.
  2 Selecione um repositório existente na lista.
  3 Clique em **Avançar**.

  A página **Criptografia** é exibida. Passe à Etapa 19 para definir criptografia como opção.
- Caso você queira criar um repositório, selecione **Criar um repositório** e conclua as etapas a seguir.
  1 Na página **Repositório**, digite as informações descritas na tabela a seguir.

Tabela 91. Definições de Adicionar novo repositório

Caixa de texto	Descrição
Nome do repositório	Insira o nome de exibição do repositório. Por padrão, essa caixa de texto consiste na palavra Repositório e em um número, que corresponde ao número de repositórios desse Core. Por exemplo, caso esse seja o primeiro repositório, o nome padrão é Repositório 1. Altere o nome conforme necessário.

Caixa de texto	Descrição
	Os nomes de repositório devem conter entre 1 e 40 caracteres alfanuméricos, incluindo espaços. Não usecaracteres proibidos ou frases proibidas.
Operações simultâneas	Defina o número de solicitações simultâneas que você deseja que o repositório suporte. Por padrão, o valor é 64.
Comentários	Como opção, insira uma nota descritiva sobre esse repositório. Você pode inserir até 254 caracteres. Por exemplo, digite **Repositório de DVM 2.**

2 Clique em **Adicionar local de armazenamento** para definir o local de armazenamento específico ou o volume do repositório. Esse volume deve ser um local de armazenamento principal.

> **CUIDADO: Defina uma pasta dedicada na raiz para o local de armazenamento do repositório. Não especifique o local da raiz. Por exemplo, use E:\Repositorio\, e não E:\. Se o repositório que você está criando nessa etapa for removido mais tarde, todos os arquivos no local de armazenamento do seu repositório serão excluídos. Caso você defina o local de armazenamento na raiz, todos os outros arquivos no volume (por exemplo, E:\) são excluídos, o que pode resultar em perda de dados catastrófica.**

A caixa de diálogo **Adicionar local de armazenamento** é exibida.

3 Clique em **Adicionar local de armazenamento** para definir o local de armazenamento específico ou o volume do repositório. Esse volume deve ser um local de armazenamento principal.

4 Na área **Local de armazenamento**, especifique como adicionar o arquivo do local de armazenamento. Você pode escolher adicionar um volume de armazenamento conectado localmente (como um armazenamento conectado direto, uma rede de área de armazenamento ou um armazenamento conectado à rede). Você também pode especificar um volume de armazenamento em um local compartilhado Common Internet File System (CIFS).

- Selecione **Adicionar arquivo no disco local** para especificar uma máquina local e, depois, insira as informações conforme descrito na tabela a seguir.

Tabela 92. Definições de disco local

Caixa de texto	Descrição
Caminho de dados	Insira o local para armazenar os dados protegidos. Por exemplo, digite `X:\Repository\Data`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Caminho de metadados	Insira o local para armazenar os metadados protegidos. Por exemplo, digite `X:\Repository\Metadata`. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

- Ou selecione **Adicionar arquivo no compartilhamento de CIFS** para especificar um local de compartilhamento de rede e, depois, insira as informações conforme descrito na tabela a seguir.

Tabela 93. Credenciais de compartilhamento de CIFS

Caixa de texto	Descrição
Caminho de UNC	Insira o caminho para o local de compartilhamento de rede. Se esse local estiver na raiz, defina um nome de pasta dedicada (por exemplo, `Repository`). O caminho precisa começar com \\. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen e pontos (somente para separar domínios e nomes de host). As letras de A a Z

Caixa de texto	Descrição
	não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Nome de usuário	Especifique um nome de usuário para acessar o local de compartilhamento de rede.
Senha	Especifique a senha para acessar o local de compartilhamento de rede.

5 Na área **Configuração de armazenamento**, clique em **Mais detalhes** e insira os detalhes do local de armazenamento conforme descrito na tabela a seguir.

Tabela 94. Detalhes da configuração de armazenamento

Caixa de texto	Descrição
Tamanho	Defina o tamanho ou capacidade do local de armazenamento. O tamanho mínimo é 1 GB. O padrão é 250 GB. Você pode selecionar dentre os seguintes: • GB • TB **NOTA: O tamanho que você especificar não pode exceder o tamanho do volume.** Se o local de armazenamento for um volume NTFS (Sistema de arquivos de nova tecnologia) usando o Windows XP ou Windows 7, o limite de tamanho do arquivo é 16 TB. Se o local de armazenamento for um volume NTFS usando Windows 8, 8.1, Windows 10,ou Windows Server 2012, 2012 R2, o limite de tamanho do arquivo será 256 TB. **NOTA: Para o Rapid Recovery validar o sistema operacional, a Instrumentação de gerenciamento do Microsoft Windows (WMI) precisa estar instalada no local de armazenamento desejado.**
Política de cache de gravação	A política de cache de gravação controla como o Gerenciador de cache do Windows é usado no repositório e ajuda a ajustar o repositório para que o melhor desempenho seja obtido com diferentes configurações. Defina o valor para um dos seguintes: • Ligado • Desligado • Sincronizar Se definido como Ligado, que é o padrão, o Windows controla o armazenamento em cache. Isso é apropriado para o Windows 10 e para versões do Windows Server 2012 e posteriores. **NOTA: Definir a política de cache de gravação como Ligado pode resultar em desempenho mais rápido. Caso você esteja usando Windows Server 2008 SP2 ou Windows Server 2008 R2 SP2, a definição recomendada é Desligado.** Caso definido como Desligado, o Rapid Recovery controla o armazenamento em cache. Se definido como Sincronizar, o Windows controla o armazenamento em cache, além da entrada/saída síncrona.
Bytes por setor	Especifique o número de bytes que você deseja incluir em cada setor. O valor padrão é 512.
Média de bytes por registro	Especifique a média de bytes por registro. O valor padrão é 8192.

6 Clique em **Avançar**.

Caso você escolha a opção **Avançado** na Etapa 1, a página **Criptografia** é exibida.

14 Opcionalmente, para habilitar a criptografia, selecione **Habilitar criptografia** na página **Criptografia**.

O campo Chave de criptografia é exibido na página **Criptografia**.

NOTA: Se você habilitar a criptografia, ela será aplicada a dados de todos os volumes protegidos dessa máquina. Você pode alterar as definições depois na página Chaves de criptografia do Rapid Recovery Core Console. Para obter mais informações sobre criptografia, consulte o tópico Compreender as chaves de criptografia.

CUIDADO: Rapid Recovery usa criptografia AES de 256 bits em modo Cipher Block Chaining (CBC) com chaves de 256 bits. Embora o uso de criptografia seja opcional, a Dell recomenda fortemente que você estabeleça uma chave de criptografia e que proteja a frase de acesso definida. Armazene a frase de acesso em um local seguro, pois ela é essencial para a recuperação dos dados. Sem a frase de acesso, não é possível executar a recuperação dos dados.

15 Caso você queira criptografar essas máquinas protegidas usando uma chave de criptografia já definida nesse Rapid Recovery Core, selecione **Criptografar dados usando uma chave de criptografia existente** e a chave de criptografia no menu suspenso.

Vá até a Etapa 17.

16 Caso queira adicionar uma nova chave de criptografia ao Core e aplicá-la a essas máquinas protegidas, insira as informações conforme descrito na tabela a seguir.

Tabela 95. Definições de chave de criptografia

Caixa de texto	Descrição
Nome	Insira um nome para a chave de criptografia. Os nomes de chaves de criptografia devem ter entre 1 e 130 caracteres alfanuméricos. Não é possível incluir caracteres especiais, como barra, barra invertida, barra vertical, ponto e vírgula, asterisco, aspas, ponto de interrogação, colchetes, e comercial ou cerquilha.
Descrição	Insira um comentário para a chave de criptografia. Essas informações aparecem no campo Descrição ao visualizar as chaves de criptografia no Core Console.
Frase de acesso	Insira a frase de acesso usada para controlar o acesso. É uma boa prática evitar o uso dos caracteres especiais relacionados acima. Armazene a frase de acesso em um local seguro. O Suporte da Dell não consegue recuperar uma frase de acesso. Depois de criar uma chave de criptografia e aplicá-la a uma ou mais máquinas protegidas, você não poderá recuperar os dados caso perca a frase de acesso.
Confirmar frase de acesso	Insira novamente a frase de acesso que você acabou de inserir.

17 Clique em **Concluir** para salvar e aplicar suas definições.

O assistente é fechado.

18 Caso a página **Aviso** seja exibida e você continue insatisfeito com as seleções, clique em **Concluir** novamente.

O software do agente Rapid Recovery é implantado nas máquinas especificadas, caso necessário, e as máquinas são adicionadas à proteção no Core.

Monitorar a proteção de várias máquinas

É possível monitorar o progresso à medida que o Rapid Recovery aplica as programações e políticas de proteção às máquinas.

No Rapid Recovery Core Console, navegue até a página Início do Rapid Recovery e clique em  (Eventos).

A página **Eventos** é exibida, dividida em Tarefas, Alertas e Eventos. À medida que os volumes são transferidos, o status e as horas inicial e final são exibidos no painel Tarefas.

Também é possível filtrar as tarefas por status (ativa, em espera, concluída, em fila e com falha). Para obter mais informações, consulte Visualizar tarefas.

NOTA: Para ver apenas as tarefas que estão esperando para serem realizadas, certifique-se de selecionar o ícone Tarefas em espera.

À medida que cada máquina protegida é adicionada, um alerta é registrado no log, relacionando se a operação foi bem-sucedida ou se foram registrados erros no log. Para obter mais informações, consulte Visualizar alertas.

Para obter informações sobre visualização de todos os eventos, consulte Visualizar todos os eventos.

Definições e funções para servidores protegidos do Exchange

Se você estiver protegendo um servidor Microsoft Exchange no seu Core, há configurações adicionais que você pode configurar no Console do Rapid Recovery Core, e existem funções adicionais que você pode executar.

Uma configuração única, **Habilitar a verificação de capacidade de montagem automática**, está disponível no Console do Core relacionado ao Exchange Server. Se esse recurso estiver ativado, as verificações de capacidade de montagem do servidor do Exchange são conduzidas automaticamente. Esta configuração estará disponível quando o status da máquina protegida estiver verde (ativo) ou amarelo (pausado).

Para obter informações, consulteSobre verificações de montabilidade do banco de dados no Exchange.

Você também pode executar uma verificação de capacidade de montagem sob demanda, a partir do painel de Pontos de recuperação em uma máquina protegida do Exchange server. Para obter informações, consulteForçar uma verificação de capacidade de montagem de um banco de dados do Exchange.

A seguir, temos funções que você pode executar para um Exchange server protegido pelo Core.

- **Especificar credenciais do Exchange server**. ORapid Recovery Core permite que você defina credenciais de forma que o Core possa autenticar no Exchange server a fim de obter informações.

  Para obter informações sobre a definição de credenciais para os Exchange servers, consulteDefinir credenciais para uma máquina do Exchange Server.
- **Registros truncados do Exchange**. Quando você forçar truncamento de logs do Exchange server, este processo identifica o espaço disponível e retoma espaço no Exchange server protegido.

  Para obter mais informações sobre o truncamento dos logs do Exchange server em demanda, consulteForçar o truncamento de log para uma máquina Exchange. Este processo também pode ser executado como parte dos trabalhos noturnos.
- **Forçar uma verificação de capacidade de montagem de um database do Exchange**. Esta função verifica se os databases do Exchange são montáveis, a fim de detectar a corrupção e alertar os administradores para que todos os dados do Exchange server possam ser recuperados com sucesso.

  Para obter mais informações sobre forçar uma verificação de capacidade de montagem sob demanda, consulteForçar uma verificação de capacidade de montagem de um banco de dados do Exchange.

  Você também pode forçar uma verificação de capacidade de montagem para ocorrer automaticamente após cada snapshot. Para obter mais informações sobre verificação de capacidade de montagem, consulteSobre verificações de montabilidade do banco de dados no Exchange.
- **Forçar uma verificação de soma de verificação de pontos de recuperação do Exchange Server**. Esta função verifica a integridade de pontos de recuperação contendo arquivos de database do Exchange.

  Para obter mais informações sobre forçar uma verificação de soma de verificação sob demanda, consulteForçar uma verificação de soma de verificação dos arquivos do banco de dados do Exchange.

Você pode truncar logs do Exchange e forçar uma verificação de soma de verificação, como parte dos trabalhos noturnos. Para obter mais informações sobre tarefas que você pode programar como trabalhos noturnos, consulteCompreender trabalhos noturnos. Para obter informações sobre configuração de trabalhos noturnos, consulteConfigurar trabalhos noturnos para o Core.

Definir credenciais para uma máquina do Exchange Server

Para definir as credenciais de login, um Exchange Server deve estar presente em um volume protegido. Se o Rapid Recovery não detectar a presença de um Exchange Server, a função Definir credenciais não será exibida no Core Console.

Assim que você proteger os dados em um Microsoft Exchange Server, você poderá definir as credenciais de login no Rapid Recovery Core Console.

Conclua as etapas deste procedimento para definir as credenciais de cada Exchange Server.

1 Na área de navegação à esquerda do Rapid Recovery Core Console, selecione a máquina protegida do Exchange Server em relação à qual você deseja definir credenciais.

A página **Resumo** é exibida para o Exchange Server protegido.

2 Na página **Resumo**, nos links na parte superior da página clique na seta apontada para baixo ▼ à direita do menu do Exchange e, no menu suspenso resultante, selecione **Definir credenciais**.

A caixa de diálogo **Editar credenciais do Exchange** do Exchange Server protegido é exibida.

3 Na caixa de diálogo **Editar credenciais do Exchange**, insira suas credenciais como a seguir:

a No campo de texto **Nome de usuário**, insira o nome de usuário com permissões para o Exchange Server, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).

b No campo **Senha**, insira a senha associada ao nome de usuário especificado para se conectar ao Exchange Server.

c Clique em **OK** para confirmar as configurações e feche a caixa de diálogo.

Forçar o truncamento de log para uma máquina Exchange

Para forçar o truncamento de log, um banco de dados do Exchange deve estar presente em um volume protegido. Se o Rapid Recovery não detecta a presença de um banco de dados, a função de verificação de truncamento de log não é exibida no Core Console.

Quando você força o truncamento de log em um Exchange Server protegido, o tamanho dos logs é reduzido. Execute as etapas deste procedimento para forçar o truncamento de log conforme a demanda.

1 Na área de navegação esquerda do Rapid Recovery Core Console, selecione o Exchange server protegido para o qual deseja forçar o truncamento de log

A página **Resumo** da máquina protegida é exibida.

2 Na parte superior da página, clique no menu suspenso **Exchange** e selecione **Forçar truncamento de log**.

3 Na caixa de diálogo resultante, clique para confirmar que você deseja forçar truncamento de log.

A caixa de diálogo é fechada. O sistema inicia o truncamento dos logs do Exchange server. Se os alertas do sistema estiverem ativados para este tipo de evento, será exibida uma mensagem indicando que o truncamento de log foi iniciado.

Sobre verificações de montabilidade do banco de dados no Exchange

Ao usar o Rapid Recovery para fazer cópias de segurança de Microsoft Exchange Servers, poderão ser feitas verificações de montabilidade em todos os bancos de dados Exchange após cada snapshot. Esse recurso de detecção de corrupção alerta os administradores sobre possíveis falhas e garante que todos os dados nos Exchange servers sejam recuperados com êxito em caso de falha.

Para ativar ou desativar esse recurso, vá para o menu **Configurações** e defina a opção **Habilitar a verificação de capacidade de montagem automática** como Sim ou Não, respectivamente. Para obter mais informações sobre como modificar as configurações de uma máquina protegida, consulte Visualização e modificação das definições de máquina protegida.

Verificações de capacidade de montagem não são parte das configurações noturnas. No entanto, se a verificação de capacidade de montagem automática estiver ativada e se a o opção Truncar logs do Exchange estiver ativada, a verificação de capacidade de montagem é acionada depois da conclusão do truncamento de log.

Você também pode executar uma verificação de capacidade de montagem sob demanda do painel **Pontos de recuperação** em uma máquina protegida do Exchange server. Para obter informações, consulte Forçar uma verificação de capacidade de montagem de um banco de dados do Exchange.

NOTA: As verificações de montabilidade somente se aplicam ao Microsoft Exchange 2007, 2010 e 2013. Além disso, a conta de serviço do Agente Rapid Recovery deve ter a função de Administrador organizacional atribuída a ela no Exchange.

Forçar uma verificação de capacidade de montagem de um banco de dados do Exchange

Para forçar uma verificação de capacidade de montagem, um banco de dados do Exchange deve estar presente em um volume protegido. Se o Rapid Recovery não detectar a presença de um banco de dados, a função de verificação de capacidade de montagem não será exibida no Core Console.

Execute as etapas deste procedimento para forçar o sistema a realizar uma verificação de montabilidade de um ponto específico de recuperação do Exchange Server sob demanda.

1. Na área de navegação esquerda do Rapid Recovery Core Console, selecione a máquina protegida do Exchange server em relação à qual você deseja forçar a verificação de capacidade de montagem e clique no menu **Pontos de recuperação**.
2. Role para baixo até o painel **Pontos de recuperação**.
3. Navegue pelos pontos de recuperação para encontrar o pontos de recuperação desejado. Opcionalmente, clique na seta à direita de um ponto de recuperação na lista para expandir a visualização.

   Nas informações expandidas do ponto de recuperação, você pode visualizar os volumes incluídos no ponto de recuperação.
4. No painel **Pontos de recuperação**, na linha representando o ponto de recuperação correto, clique em e, no menu suspenso, selecione **Forçar verificação de capacidade de montagem**.
5. Na caixa de diálogo resultante, clique para confirmar que você deseja forçar uma verificação de capacidade de montagem.

   A caixa de diálogo é fechada. O sistema realiza a verificação de montabilidade. Se alertas do sistema estiverem ativados para esse tipo de evento, você verá uma mensagem indicando que a verificação de capacidade de montagem foi iniciada.

Para obter instruções sobre como visualizar o status da verificação de capacidade de montagem, consulte Como exibir eventos usando tarefas, alertas e registros.

Forçar uma verificação de soma de verificação dos arquivos do banco de dados do Exchange

Para forçar uma verificação de soma de verificação, um banco de dados do Exchange deve estar presente em um volume protegido. Se o Rapid Recovery não detecta a presença de um banco de dados, a função de verificação de soma de verificação não é exibida no Core Console.

Execute as etapas deste procedimento para forçar o sistema a realizar uma verificação de soma de verificação de um ponto específico de recuperação do Exchange Server.

1. Na área de navegação esquerda do Rapid Recovery Core Console, selecione o Exchange server protegido para o qual deseja forçar a verificação de soma de verificação e clique no menu **Pontos de recuperação**.

   A página **Pontos de recuperação** é exibida para o Exchange server protegido.
2. Role o painel **Pontos de recuperação** para baixo.
3. Percorra os pontos de recuperação para encontrar o ponto de recuperação desejado. Como opção, clique em na seta ao lado de um ponto de recuperação na lista para expandir a visualização.

   Nas informações expandidas do ponto de recuperação, você poderá ver os volumes incluídos no ponto de recuperação.
4. No painel **Pontos de recuperação**, na fileira que representa o ponto de recuperação correto, clique em e, no menu suspenso, selecione **Forçar verificação de soma de verificação**.
5. Na caixa de diálogo resultante, clique para confirmar que você deseja forçar uma verificação de soma de verificação.

   A caixa de diálogo é fechada. O sistema realiza a verificação de soma de verificação. Se os alertas do sistema estiverem ativados para este tipo de evento, será exibida uma mensagem indicando que a verificação de soma de verificação foi iniciada.

Para obter instruções sobre como visualizar o status da verificação de soma de verificação, consulte Como exibir eventos usando tarefas, alertas e registros.

Definições e funções para servidores SQL protegidos

Se você estiver protegendo um servidor Microsoft SQL no seu Core, há definições adicionais que você pode configurar no Console do Rapid Recovery Core, e existem funções adicionais que você pode executar.

Uma única definição, **Capacidade de anexação**, está disponível no Console do Core relacionada ao SQL Server.

O Rapid Recovery Core permite que você execute uma verificação de capacidade de anexação do SQL para verificar a integridade de pontos de recuperação contendo SQL databases. Esta ação verifica a consistência dos SQL databases e garante que todos os arquivos que suportam MDF (dados) e LDF (log) estão disponíveis no snaphot de backup.

Em versões anteriores, as verificações de capacidade de anexação do SQL solicitaram historicamente uma versão licenciada do SQL Server na máquina Core. O Rapid Recovery Core agora fornece a capacidade de executar as verificações de capacidade de anexação do SQL a partir de uma instância do SQL Server no Core ou a partir de uma versão licenciada do SQL Server na máquina protegida de um SQL Server.

As definições da capacidade de anexação permitem que você especifique qual versão licenciada do SQL Server é usada para executar esta verificação. Para obter mais informações sobre a configuração de definições da capacidade de anexação, consulteGerenciamento das definições de Capacidade de anexação SQL do Core.

Para obter mais informações sobre a capacidade de anexação do SQL, consulte Sobre a capacidade de anexação do SQL.

A seguir, temos funções que você pode executar para um SQL server protegido pelo Core.

- **Especificar as credenciais do SQL Server**. O Rapid Recovery Core permite que você defina credenciais de forma que o Core possa autenticar no SQL server a fim de obter informações. Você pode definir as credenciais para uma única máquina protegida do SQL Server, ou definir as credenciais padrão para todos os SQL Servers protegidos.

  Para obter informações sobre a definição de credenciais para SQL servers, consulte Definir credenciais para uma máquina SQL Server.
- **Truncar logs de SQL**. Quando você forçar truncamento de logs do SQL Server, este processo identifica o espaço disponível no servidor protegido. Este processo não recupera nenhum espaço.

  Para obter mais informações sobre o truncamento dos logs do SQL server sob demanda, consulteForçar truncamento de log para uma máquina SQL.
- **Forçar uma verificação de capacidade de anexação de um SQL Server**. Esta função verifica a consistência dos SQL databases e garante que todos os arquivos que suportam MDF (dados) e LDF (log) estão disponíveis no snaphot de backup.

  Para obter mais informações sobre forçar uma verificação de capacidade de anexação para SQL servers sob demanda, consulte Forçar uma verificação de capacidade de anexação do SQL Server.

Além de especificar credenciais, cada uma das funções descritas na lista anterior pode ser realizada sob demanda, e também pode ser configurada para ocorrer como parte dos trabalhos noturnos realizados para o Core. Para obter mais informações sobre tarefas que você pode programar como trabalhos noturnos, consulte Compreender trabalhos noturnos. Para obter informações sobre configuração de trabalhos noturnos, consulte Configurar trabalhos noturnos para o Core.

Definir credenciais para uma máquina SQL Server

Você deve adicionar a máquina do SQL Server para proteção no Rapid Recovery Core antes de realizar esse procedimento. Para obter mais informações sobre a proteção de máquinas, consulte Proteger uma máquina.

Assim que você proteger os dados em uma máquina do Microsoft SQL Server. você poderá definir as credenciais de login para uma instância única ou para todos os SQL Servers no Rapid Recovery Core Console.

Conclua as etapas deste procedimento para definir as credenciais de cada SQL Server.

1 Na área de navegação à esquerda do Rapid Recovery Core Console, selecione a máquina protegida do SQL Server em relação à qual você deseja definir credenciais.

A página **Resumo** é exibida para a máquina protegida do SQL Server.

2 Na página **Resumo**, nos links na parte superior da página clique na seta apontada para baixo ▼ à direita do menu SQL e, no menu suspenso resultante, siga uma das seguintes opções:

- Se desejar definir credenciais padrão para todas as instâncias do SQL Server database, clique em **Definir credenciais padrão para todas as instâncias**, e na caixa de diálogo **Editar credenciais padrão**, faça o seguinte:
  1 No campo de texto **Nome de usuário**, insira o nome de usuário com permissões para todos os SQL Servers associados, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
  2 No campo de texto **Senha**, insira a senha associada ao nome de usuário especificado para se conectar ao SQL Server.
  3 Clique em **OK** para confirmar as configurações e feche a caixa de diálogo.
- Se desejar definir credenciais para uma instância do SQL Server database, clique no nome de exibição da máquina protegida do SQL Server e, na caixa de diálogo **Editar credenciais de instância**, faça o seguinte:
  1 Selecione o tipo de credencial (Padrão, Windows ou SQL)
  2 No campo de texto **Nome de usuário**, insira o nome de usuário com permissões para o SQL Server, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
  3 No campo de texto **Senha**, insira a senha associada ao nome de usuário especificado para se conectar ao SQL Server.
  4 Clique em **OK** para confirmar as configurações e feche a caixa de diálogo.

Forçar truncamento de log para uma máquina SQL

O truncamento de log está disponível para máquinas que utilizam o SQL Server. Execute as etapas deste procedimento para forçar o truncamento de log.

NOTA: Quando realizado em uma máquina com SQL, o truncamento identifica o espaço livre em um disco, mas não reduz o tamanho dos logs.

1 Na área de navegação á esquerda do Rapid Recovery Core Console, selecione a máquina em que você deseja forçar o truncamento de log.

A página **Resumo** é exibida para a máquina protegida.

2 Na página **Resumo** (ou em qualquer página para essa máquina protegida), na parte superior da página, clique no menu suspenso **SQL** e selecione **Forçar truncamento de log**.

3 Clique em **Sim** para confirmar que deseja forçar o truncamento de log.

Sobre a capacidade de anexação do SQL

O recurso de capacidade de anexação do SQL permite que o Rapid Recovery Core conecte os arquivos mestres do banco de dados (arquivos .MDF) e arquivos de log do banco de dados (arquivos .LDF) a um snapshot de um SQL Server protegido. O snapshot é capturado usando uma instância local do Microsoft SQL Server.

Assuntos relevantes para usuários Rapid Recovery que protegem máquinas do SQL Server incluem qual instância do SQL Server executa a capacidade de anexação e o método de execução da anexação do SQL (sob demanda ou como parte dos trabalhos noturnos).

O teste da capacidade de anexação permite que o Core verifique a consistência dos bancos de dados SQL e garanta que todos os arquivos MDF e LDF estejam disponíveis no snapshot de backup.

As verificações da capacidade de anexação podem ser executadas sob demanda para pontos de recuperação específicos ou como parte de um trabalho noturno.

Para executar a Verificação de capacidade de anexação do SQL sob demanda, consulte Forçar uma verificação de capacidade de anexação do SQL Server. Para executar a capacidade de anexação do SQL uma vez por dia em uma hora especificada para as suas operações de trabalhos noturnos, ative a opção **Verificar anexação dos bancos de dados SQL** em trabalhos noturnos. Para obter mais informações sobre como configurar trabalhos noturnos no Core, consulte Configurar trabalhos noturnos para o Core. Para obter mais informações sobre como configurar trabalhos noturnos em uma máquina específica (neste caso, um SQL Server protegido), consulte Como personalizar os trabalhos noturnos para uma máquina protegida.

Em versões anteriores, a capacidade de anexação do SQL exigia que uma instância local do Microsoft SQL Server fosse instalada e configurada na máquina do Core. Agora, o Rapid Recovery Core permite que você escolha executar a verificação de capacidade de anexação em uma instância do SQL Server no Core ou em uma instância do SQL Server em uma máquina protegida do SQL Server. Essa instância precisa ser uma versão totalmente licenciada do SQL Server adquirida da Microsoft ou por meio de um revendedor licenciado. A Microsoft não permite o uso de licenças SQL passivas.

Qualquer instância do SQL Server que você especificar é usada para todas as verificações de capacidade de anexação. A capacidade de anexação é sincronizada entre as configurações do Core e os trabalhos noturnos. Por exemplo, se você especificar o uso da instância do SQL Server Core para trabalhos noturnos, as verificações de capacidade de anexação sob demanda também usarão o Core. Por outro lado, se você especificar o uso de uma instância do SQL Server em uma máquina protegida específica, todas as verificações de capacidade de anexação noturnas e sob demanda usarão a instância local da máquina protegida.

Selecione a instância do SQL Server para usar como parte das configurações do Core global. Para obter informações, consulte Gerenciamento das definições de Capacidade de anexação SQL do Core.

NOTA: Executar a verificação de capacidade de anexação de uma máquina protegida do SQL Server exige que o Software do agente Rapid Recovery esteja instalado nesse servidor. A proteção sem agente não é suportada para a capacidade de anexação do SQL.

A capacidade de anexação no Rapid Recovery suporta SQL Server 2005, 2008, 2008 R2, 2012 e 2014. À conta usada para realizar o teste deve ser concedida a função sysadmin na instância do SQL Server.

O formato de armazenamento em disco do SQL Server é o mesmo em ambientes de 64 e 32 bits, e a capacidade de anexação funciona em ambas as versões. Um banco de dados separado da instância do server que está sendo executado em um ambiente pode ser anexado em uma instância de server que é executado em outro ambiente.

NOTA: A versão do SQL Server no Core deve ser igual ou mais recente que aquela em todas as máquinas protegidas com o SQL Server instalado.

Forçar uma verificação de capacidade de anexação do SQL Server

Para forçar uma verificação de capacidade de anexação, um SQL database deve estar presente em um volume protegido. Se o Rapid Recovery não detectar a presença de um banco de dados, a função de verificação de capacidade de anexação não será exibida no Core Console.

Execute as etapas deste procedimento para forçar o sistema a realizar uma verificação de capacidade de anexação de um ponto específico de recuperação do SQL Server.

1. Na área de navegação esquerda do Rapid Recovery Core Console, selecione a máquina protegida do SQL Server em relação à qual você deseja forçar a verificação de capacidade de anexação e clique no menu **Pontos de recuperação**.
2. Role para baixo até o painel **Pontos de recuperação**.
3. Navegue pelos pontos de recuperação para encontrar o pontos de recuperação desejado. Opcionalmente, clique na seta à direita de um ponto de recuperação na lista para expandir a visualização.

   Nas informações expandidas do ponto de recuperação, você pode visualizar os volumes incluídos no ponto de recuperação.
4. No painel **Pontos de recuperação**, na linha representando o ponto de recuperação correto, clique em e, no menu suspenso, selecione **Forçar verificação de capacidade de anexação**.
5. Na caixa de diálogo resultante, clique para confirmar que você deseja forçar uma verificação de capacidade de anexação.

   A caixa de diálogo é fechada. O sistema realiza a verificação de capacidade de anexação.

Para obter instruções sobre como visualizar o status da verificação de capacidade de anexação, consulte Como exibir eventos usando tarefas, alertas e registros.

Como entender o recurso Rapid Snap for virtual

Instalando o software do agente Rapid Recovery, você pode proteger máquinas físicas ou virtuais no Rapid Recovery Core. Os sistemas operacionais suportados são indicados nos requisitos do sistema no tópico “Requisitos de software do Rapid Recovery Agent.”

Rapid Recovery oferece agora uma outra abordagem para proteger máquinas.

O recurso Rapid Snap para virtual — também conhecido como proteção sem agente - do Rapid Recovery permite proteger máquinas virtuais (VMs) em um host VMware ESXi ou Hyper-V sem instalar o Rapid Recovery Agent em cada máquina virtual.

CUIDADO: A Dell recomenda que você limite a proteção sem agente para 200 máquinas virtuais uma vez. Por exemplo, não selecione mais de 200 VMs quando usando o Assistente para proteger várias máquinas. Proteger mais de 200 máquinas virtuais resulta em desempenho lento. Não há limite para quantas máquinas virtuais um Core pode proteger sem agente com o passar do tempo. Por exemplo, você pode proteger 200 VMs hoje e 200 VMs amanhã.

Como proteger hosts vCenter/ESXi VMs

O Rapid Recovery permite proteger VMs vCenter/ESXi sem instalar o Rapid Recovery Agent na VM ou host ESXi, atingindo a proteção sem agente. Para proteger um ambiente ESXi, o Rapid Recovery Core funciona com a tecnologia de snapshot nativa ao VMware.

A proteção sem agente Rapid Recovery usa o cliente ESXi e a interface de programa aplicativo (API) existente para proteger VMs selecionadas em um único host sem instalar software do Agente Rapid Recovery. O Rapid Recovery Core, em seguida, comunica com o disco virtual da máquina (VMDK) para determinar os detalhes necessários dos volumes protegidos. Porque o Rapid Recovery cria pontos de recuperação baseado nos volumes, não VMDKs, cada volume pode ser montado, restaurado e exportado separadamente.

NOTA: O Rapid Recovery recomenda que o VMware Tools seja nstalado em máquinas virtuais (VMs) que você quer proteger em hosts vSphere ou ESXi. Quando o VMware Tools [e instalado em uma máquina virtual usando um sistema operacional Windows (SO), os backups que o Rapid Recovery Core captura usam o Microsoft Volume Shadow Services (VSS). Para obter informações sobre o comportamento de máquinas virtuais sem agente com ou VMware Tools, consulte Benefícios de instalar as Ferramentas VMware para proteção sem agente.

A proteção sem agente usa também o Rastreamento do bloco alterado VMware (CBT) para reduzir o tempo necessário para snapshots diários. CBT determina quais são os blocos alterados no arquivo de VMDK, deixando o Rapid Recovery fazer backup de apenas as partes do disco que foram alteradas desde o último snapshot. Esse método de backup frequentemente resulta em operações de backup mais curtas e consumo reduzido de recursos na rede e elementos de armazenamento.

Há múltiplos benefícios ao uso de proteção sem agente. Alguns dos mais úteis atributos incluem as seguintes características:

- Nenhum software adicional é necessário no computador host.
- A proteção sem agente permite que você opte por proteger automaticamente novas máquinas virtuais adicionadas ao host ESXi.
- Não é necessário reinicializar durante o processo de proteção.
- As credenciais não são necessárias para cada máquina virtual.
- A proteção sem agente permite proteger uma VM, mesmo se ela estiver desligada.
- A proteção sem agente permite que você faça a restauração aos discos.
- A proteção sem agente não exige espaço livre em um volume durante as transferências.
- A proteção sem agente oferece suporte a todos os sistemas operacionais convidados.
- A proteção sem agente permite que você exporte discos rígidos ou volumes dinâmicos.

NOTA: Se os volumes dinâmicos são complexos (distribuídos, espelhados, estendidos, ou RAID), eles exportam como imagens de disco e analisam em volumes depois que a operação de exportação é concluída na VM exportada.

Enquanto há muitas razões para usar proteção sem agente para VMs ESXi, opte pelo método de proteção que melhor se adapte aos seus ambientes e necessidades empresariais. Junto com os benefícios mencionados, há também as seguintes considerações para ter em mente ao escolher a proteção sem agente:

- A proteção sem agente não suporta a proteção de volumes dinâmicos (por exemplo, estendidos, particionados, espelhados, ou RAID) ao nível de volume. Ela protege ao nível do disco.
- A proteção sem agente não suporta o Live Recovery (Recuperação em tempo real). Para obter mais informações sobre este recurso, consulte Noções básicas sobre Live Recovery.
- Após cada restauração de um único volume para a VM protegida, você precisa reiniciar a máquina virtual.
- A proteção sem agente não coleta metadados Microsoft SQL ou Microsoft Exchange.
- Você não pode executar uma Verificação de anexacão SQL, log truncado ou montabilidade em pontos de recuperação capturados em máquinas protegidas sem agente.
- A proteção sem agente não recolhe ou exibe as etiquetas dos volumes, ou letras de unidade.
- A proteção sem agente não exibe a quantidade de espaço real usado em uma máquina virtual se o tipo de disco virtual é provisão grossa de zero ansioso.

Se você optar por usar a proteção sem agente para VMs ESX , o host deve atender aos seguintes requisitos mínimos para a proteção sem agente ser bem-sucedida.

- A máquina host precisa estar executando ESXi versão 5.0.0 build 623860 ou posterior.
- A máquina host precisa atender os requisitos mínimos do sistema indicado no *Guia de instalação e atualização Rapid Recovery*.
- Para proteção ao nível do volume, os VMDKs precisam incluir tabelas de partição MBR (Master Boot Record - registro mestre de inicialização) ou GUID. VMDKs sem estas tabelas de partição são protegidos como discos inteiros em vez de volumes individuais.
- Cada máquina virtual VMware precisa ter o VMware Tools instalado para assegurar consistência de instantâneos.

Como proteger os servidores e clusters Hyper-V

Para proteger um servidor Hyper-V sem agente, não é necessário instalar o Rapid Recovery Agente em qualquer VMs. Você só precisa instalá-lo na máquina host ou nó de cluster. O Agente protege o disco rígido virtual no host e converte quaisquer alterações à arquivos de disco rígido em uma imagem de volume ou imagem de disco, dependendo do sistema de arquivos. Um novo driver fornece suporte ao nível de arquivos para máquinas virtuais em hosts e em volumes de cluster compartilhado (CSVs).

NOTA: O Rapid Recovery suporta o formato de arquivo de disco VHDx. Ele não suporta o formato VHD.

Para proteger VMs em um CSV, o Rapid Recovery Agent e o driver precisa ser instalado em cada nó de cluster usando o recurso auto implementação no Assistente para proteger várias máquinas. Do nós, o agente pode proteger todas as VMs operando com CSVs , criando dois tipos de mudanças para cada arquivo. O primeiro tipo é salvo apenas antes ou depois de um snapshot ou reinicialização do sistema. O segundo tipo reside no disco, que dispõe um snapshot incremental mesmo se houver uma falha de energia ou desligamento sujo. O Agente instalado no nó mescla todas as mudanças em um antes de transferir os dados.

Quando um host ou nó está em execução, o Rapid Recovery cria um backup consistente com aplicativo. Se o host não estiver sendo executado, nenhum backup pode ser criado; no entanto, se um dos nós não está em execução, o Rapid Recovery pode continuar a tirar snapshots das VMs do cluster.

NOTA: Para obter um melhor desempenho, é recomendado que o máximo de transferências simultâneas para o host Hyper-V ou nó seja definido como 1, o que é a configuração padrão.

A proteção sem agente para Hyper-V tem muitos das mesmos recursos que a proteção tradicional onde o agente está instalado em cada máquina virtual, incluindo:

- Arquivamento
- Verificação da integridade de um ponto de recuperação
- Montagem de pontos de recuperação
- Descoberta automática de novas máquinas virtuais (exclusivo para a proteção sem agente)
- Replicação
- Restauração de VMs

- Restauração de CSVs
- Restauração em CIFS no formato VHDX
- Restauração de arquivos em um formato VHDX convidado
- Implantação
- Exportação virtual para VMs Hyper-V e outros hipervisores, incluindo ESXi, VMware Workstation e VirtualBox

Entretanto, há limitações a serem consideradas ao escolher a proteção sem agente para Hyper-V. As capacidades que não são executadas incluem:

- Verificação de integridade de montagem Exchange
- Verificação de anexacão SQL
- Recuperação em tempo real
- Restauração de VMs em CIFS no formato VHD
- Restauração de arquivos em um formato VHD convidado

NOTA: Para um snapshot consistente com aplicativo, você precisa ter o Controlador SCSI instalado em cada máquina virtual. Sem esse controlador, o resultado é sempre um snapshot com falha.

Benefícios de instalar as Ferramentas VMware para proteção sem agente

Ao proteger máquinas virtuais (VMs) sem usar o Agente Rapid Recovery, a Dell recomenda a instalação das Ferramentas VMware em máquinas virtuais protegidas em hosts vSphere ou ESXi para aproveitar as vantagens da funcionalidade do Microsoft Volume Shadow Services (VSS).

A proteção sem agente usa a tecnologia de snapshot nativa para o VMware fazer o backup dados protegidos. Quando as ferramentas VMware são instalados em uma máquina virtual com um sistema operacional (SO) Windows, os backups que o Rapid Recovery Core captura também podem usar o VSS. Sem as Ferramentas VMware instaladas, o Rapid Recovery ainda coleta snapshots, mas a ausência delas pode o estado dos dados na sua VM protegida de maneira adversa.

Existem dois estados de dados possíveis:

- **Consistentes de falhas.** O SO da VM inicializa e pode ler e compreender o sistema de arquivos.
- **Consistentes de aplicativo.** O SO da VM inicializa e pode ler e compreender o sistema de arquivos. Além disso, arquivos para aplicativos transacionais estão em um estado consistente. Por exemplo, com o SQL Server, os logs correspondem aos arquivos do banco de dados e o banco de dados abre rápida e facilmente.

Se você se recuperar um aplicativo transacional de um estado consistente de falha, o banco de dados retorna ao último estado válido. Esse estado válido mais recente pode ser da hora da falha ou anterior à ela. Se for anterior, o banco de dados deve encaminhar algum trabalho para fazer os arquivos de dados corresponderem às informações nos registros. Esse processo leva algum tempo na primeira vez em que o banco de dados é aberto, o que causa um atraso na inicialização da máquina.

As condições a seguir se aplicam se Ferramentas VMware estiverem instaladas e a VM estiver ligada:

Tabela 96. Condições de tipo de backup para máquinas virtuais

Ferramentas VMware	VM ligada	Tipo de backup
Não instalado	Sim	Consistentes de falhas
Não instalado	Não (desligamento anormal)	Consistentes de falhas
Não instalado	Não (desligamento normal)	Consistentes de aplicativo
Instalado	Sim	Consistentes de aplicativo
Instalado	Não (desligamento anormal)	Consistentes de falhas
Instalado	Não (desligamento normal)	Consistentes de aplicativo

Como proteger máquinas virtuais vCenter/ESXi sem o agente Rapid Recovery

Conclua o procedimento a seguir para proteger máquinas virtuais ESXi sem um agente.

NOTA: O Rapid Recovery recomenda que ferramentas VMware sejam instaladas em máquinas virtuais (MVs) que você deseja proteger em hosts vSphere ou ESXi. Quando as ferramentas VMware são instaladas em uma MV usando um sistema operacional (SO) Windows, os backups capturados pelo Rapid Recovery Core usam os serviços de sombra de volume (VSS) da Microsoft. Para obter informações sobre o comportamento de MVs sem agentes com ou sem ferramentas VMware, consulte Benefícios de instalar as Ferramentas VMware para proteção sem agente.

CUIDADO: A Dell recomenda que você limite a proteção sem agente para no máximo 200 MVs por vez. Por exemplo, se você não selecionar mais de 200 MVs ao usar o assistente Proteger múltiplas máquinas. Proteger mais de 200 MVs resulta em queda de desempenho. Não há limite de quantas MVs um core pode proteger sem agente por vez. Por exemplo, você pode proteger 200 MVs hoje e outras 200 MVs amanhã.

1 No Rapid Recovery Core Console, clique no menu suspenso **Protect (Proteger)** e, em seguida, clique em **Protect Multiple Machines (Proteger várias máquinas)**.

O assistente Proteger várias máquinas é mostrado.

2 Na página **Welcome (Boas-vindas)**, realize uma das seguintes ações:

- Normal
- Advanced (show optional steps) (Avançado, mostrar etapas opcionais)

3 Clique em **Avançar**.

4 Na página **Connection (Conexão)** do assistente, na lista suspensa **Source (Origem)**, selecione **vCenter/ESX(i)**.

5 Digite as informações de host e credenciais de acesso conforme descrito na tabela a seguir.

Tabela 97. Configurações de conexão de vCenter/ESX(i)

Caixa de texto	Descrição
Host	O nome ou endereço IP do host virtual VMware vCenter Server/ESX(i).
Port (Porta)	A porta usada para conectar-se ao host virtual. A configuração padrão é 443.
Nome de usuário	O nome de usuário para se conectar ao host virtual; por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
Password (Senha)	A senha usada para conectar-se a este host virtual.

6 Certifique-se de que a opção **Protect selected VMs Agentlessly (Proteger MVs selecionadas)** esteja selecionada. (Essa opção é selecionada por padrão).

7 Na página **Select Machines (Selecionar máquinas)**, selecione as MVs que você deseja proteger. Você pode usar o menu suspenso para mostrar uma lista de hosts e clusters ou uma lista de MVs e modelos.

NOTA: O rastreamento de blocos alterados (CBT) VMware deve ser ativado em cada uma das MVs que você deseja proteger. Se não estiver ativado, o Rapid Recovery ativa o CBT automaticamente a fim de garantir a proteção.

8 Se você quiser proteger automaticamente novas MVs quando forem adicionadas ao host, selecione a opção **Auto protect new machines (Proteger novas máquinas automaticamente)** e realize as etapas a seguir.

a Clique em **Avançar**.

b Na página **Auto Protection (Proteção automática)**, selecione quaisquer recipientes aos quais você espera adicionar novas máquinas.

9 Clique em **Avançar**.

10 Na página Protection (Proteção), selecione um dos cronogramas de proteção a seguir conforme adequado:

- Se quiser usar o cronograma de proteção padrão, selecione **Default protection (hourly snapshots of all volumes) (Proteção padrão (instantâneos de todos os volumes a cada hora))** na opção Schedule Settings (Configurações de cronograma).

- Se quiser definir outro cronograma de proteção, selecione **Custom protection (Proteção personalizada)** na opção Schedule Settings (Configurações de cronograma).

11 Prossiga com a configuração da seguinte forma:

- Se você tiver selecionado uma configuração típica e especificado proteção padrão, clique em **Finish (Concluir)** para confirmar suas escolhas, feche o assistente e proteja a máquina que você especificou.

  Quando você adicionar a proteção para uma máquina pela primeira vez, uma imagem base (ou seja, um instantâneo de todos os dados armazenados nos volumes protegidos) será transferida para o repositório no Rapid Recovery Core, seguindo a programação definida, a menos que você tenha especificado pausar inicialmente a proteção.
- Se você tiver selecionado uma configuração típica e especificado proteção personalizada, clique em **Next (Avançar)** para configurar uma programação de proteção personalizada. Para obter detalhes sobre como definir uma programação de proteção personalizada, consulte Criar programações de proteção personalizadas.
- Se você tiver selecionado uma configuração avançada no Assistente de proteção da máquina e especificado proteção padrão, clique em **Next (Avançar)** e continue na Etapa 13 para ver as opções de repositório e criptografia.
- Se você tiver selecionado uma configuração avançada no Assistente de proteção da máquina e especificado proteção personalizada, depois clique em **Next (Avançar)** para configurar uma programação de proteção personalizada. Para obter detalhes sobre como definir uma programação de proteção personalizada, consulte Criar programações de proteção personalizadas.

12 Clique em **Avançar**.

13 Na página **Repository (Repositório)**, faça o seguinte:

- Se você já possui um repositório e quer armazenar os dados dessa máquina para proteção no repositório existente, faça o seguinte:

  1 Selecione **Use an existing repository (Usar um repositório existente)**.

  2 Selecione um repositório existente da lista.

  3 Clique em **Avançar**.

  A página **Encryption (Criptografia)** é mostrada. Pule para a etapa 19 para definir a criptografia (opcional).
- Se quiser criar um repositório, selecione **Create a Repository (Criar um repositório)** e depois prossiga para as etapas a seguir.

  1 Na página **Repository (Repositório)**, digite as informações descritas na tabela a seguir.

Tabela 98. Configurações para adicionar novo repositório

Caixa de texto	Descrição
Nome do repositório	Insira o nome de exibição do repositório. Por padrão, essa caixa de texto é composta da palavra Repositório e um número, que corresponde ao número de repositórios deste Core. Por exemplo, se esse é o primeiro repositório, o nome padrão é Repositório 1. Altere o nome conforme necessário. Os nomes de repositório devem conter entre 1 e 40 caracteres alfanuméricos, incluindo espaços. Não use caracteres proibidos nem frases proibidas.
Operações simultâneas	Defina o número de solicitações simultâneas que você quer que o repositório suporte. Por padrão, o valor é 64.
Comentários	Opcionalmente, insira uma observação descritiva sobre esse repositório. É possível digitar até 254 caracteres. Por exemplo, digite **Repositório DMV 2**

  2 Clique em **Add Storage Location (Adicionar local de armazenamento)** para definir o local de armazenamento específico ou volume para o repositório. Esse volume deve ser um local de armazenamento primário.

> **CUIDADO: Defina uma pasta exclusiva dentro do diretório raiz para o local de armazenamento de seu repositório. Não especifique o diretório raiz. Por exemplo, use E:\Repository\, não E:\. Se o repositório que você estiver criando nessa etapa for removido posteriormente, todos os arquivos no local de armazenamento de seu repositório serão apagados. Se você definir seu local de armazenamento no diretório raiz, todos os outros arquivos no volume (por exemplo, E:\) são apagados, o que pode resultar em uma perda catastrófica de dados**

  A caixa de diálogo **Add Storage Location (Adicionar local de armazenamento)** é mostrada.

  3 Clique em **Add Storage Location (Adicionar local de armazenamento)** para definir o local de armazenamento específico ou volume para o repositório. Esse volume deve ser um local de armazenamento primário.

  4 Na área **Storage Location (Local de armazenamento)**, especifique como adicionar o arquivo para o local de armazenamento. Você pode optar por adicionar um volume de armazenamento conectado localmente (como

armazenamento conectado diretamente, uma rede de área de armazenamento ou armazenamento conectado de rede). Você também pode especificar um volume de armazenamento em um local compartilhado de sistema de arquivo de Internet comum (CIFS)

- Selecione **Add file on local disk (Adicionar arquivo em disco local)** para especificar uma máquina local e depois insira as informações conforme descrito na tabela a seguir.

Tabela 99. Configurações de disco local

Caixa de texto	Descrição
Caminho de dados	Digite o local para armazenar os dados protegidos. Por exemplo, digite `X:\Repository\Data`. Ao especificar o caminho, use somente caracteres alfanuméricos, o hífen e o ponto final (apenas para separar os nomes de host e domínios). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Caminho de metadados	Digite o local para armazenar os metadados protegidos. Por exemplo, digite `X:\Repository\Metadata`. Ao especificar o caminho, use somente caracteres alfanuméricos, o hífen e o ponto final (apenas para separar os nomes de host e domínios). Você pode usar o caractere de barra invertida apenas para definir níveis no caminho. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

- Ou selecione **Add file on CIFS share (Adicionar arquivo no compartilhamento CIFS)** para especificar um local de compartilhamento de rede e depois insira as informações conforme descrito na tabela a seguir.

Tabela 100. Credenciais de compartilhamento de CIFS

Caixa de texto	Descrição
Caminho UNC	Digite o caminho para o local de compartilhamento de rede. Se esse local estiver no diretório raiz, defina um nome de pasta exclusivo (por exemplo, `Repository`). O caminho deve começar com \\. Ao especificar o caminho, use somente caracteres alfanuméricos, o hífen e o ponto final (apenas para separar os nomes de host e domínios). As letras a a z não diferenciam maiúsculas de minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.
Nome de usuário	Especifique um nome de usuário para acessar o local de compartilhamento da rede.
Password (Senha)	Especifique uma senha para acessar o local de compartilhamento da rede.

5 Na área **Storage Configuration (Configuração de armazenamento)**, clique em **More Details (Mais detalhes)** e insira os detalhes para o local de armazenamento como descrito na tabela a seguir.

Tabela 101. Detalhes de configuração de armazenamento

Caixa de texto	Descrição
Tamanho	Defina o tamanho ou a capacidade do local de armazenamento. O tamanho mínimo é de 1 GB. O padrão é de 250 GB. Você pode escolher entre: • GB • TB **NOTA: O tamanho que você especificar não pode exceder o tamanho do volume.** Se o local de armazenamento for um volume New Technology File System (NTFS) usando o Windows XP ou Windows 7, o limite do tamanho do arquivo é 16 TB. Se o local de armazenamento for um volume NTFS usando o Windows 8, 8.1, Windows 10, Windows Server 2012 ou 2012 R2, o limite do tamanho do arquivo é de 256 TB.

Caixa de texto	Descrição
	NOTA: Para que o Rapid Recovery valide o sistema operacional, o Windows Management Instrumentation (WMI) precisa ser instalado no local de armazenamento pretendido.
Política do cache de gravação	A política do cache de gravação controla o modo como o Windows Cache Manager é usado no repositório e ajuda a ajustar o repositório para obter o desempenho ideal em configurações diferentes. Configure o valor como uma das seguintes opções: • Ligado • Apagado • Sincronizar Se ativada, que é a configuração padrão, o Windows controla o cache. Isso é adequado para o Windows 10 e para versões do Windows Server 2012 e mais recentes. **NOTA: Ativar a política de cache de gravação pode melhorar o desempenho. Se estiver usando o Windows Server 2008 SP2 ou Windows Server 2008 R2 SP2, recomenda-se a configuração desligado.** Se desativar a configuração, o Rapid Recovery controla o cache. Se configurado como Sync (Sincronizar), o Windows controla o cache e a entrada/saída síncrona.
Bytes por setor	Especifique o número de bytes que você quer que cada setor contenha. O valor padrão é 512.
Média de bytes por registro	Especifique o número médio de bytes por registro. O valor padrão é 8192.

6 Clique em **Avançar**.

Se você selecionar a opção **Advanced (Avançado)** na etapa 1, a página **Encryption (Criptografia)** é mostrada.

14 Opcionalmente, na página Encryption (Criptografia), para ativar a criptografia, selecione **Enable Encryption (Ativar criptografia)**.

Os campos Encryption key (Chave de criptografia) são mostrados na página Encryption (Criptografia).

NOTA: Se você ativar a criptografia, será aplicada a todos para todos os volumes protegidos dessa máquina de agente. É possível alterar as configurações posteriormente na guia Configuration (Configuração) do Console Core do Rapid Recovery. Para obter mais informações sobre criptografia, consulte o tópico Compreender as chaves de criptografia.

CUIDADO: O Rapid Recovery usa uma criptografia AES de 256 bits no modo CBC (Encadeamento de blocos de criptografia) com chaves de 256 bits. Apesar de o uso de criptografia ser opcional, a Dell recomenda que você estabeleça uma chave de criptografia e proteja a senha que você definir. Guarde a senha em um local seguro, pois ela é essencial para a recuperação de dados. Sem a senha, a recuperação de dados não é possível.

15 Se quiser criptografar essas máquinas protegidas usando uma chave de criptografia que já está definida neste Rapid Recovery Core, selecione **Encrypt data using an existing Encryption key (Criptografar dados usando uma chave de criptografia existente)** e depois selecione a chave adequada no menu suspenso. Prossiga para a próxima etapa.

Prossiga para a etapa 17.

16 Se quiser adicionar uma chave de criptografia no Core e aplicar essa chave às máquinas protegidas, insira as informações como descrito na tabela a seguir.

Tabela 102. Configurações de chave de criptografia

Caixa de texto	Descrição
Nome	Digite um nome para a chave de criptografia. Os nomes de chave de criptografia devem conter entre 1 e 130 caracteres alfanuméricos. Você não pode incluir caracteres especiais como barra, barra invertida, barra vertical, dois pontos, asterisco, aspas, ponto de interrogação, parênteses iniciais ou finais, & ou traço.
Descrição	Digite um comentário para a chave de criptografia.

Caixa de texto	Descrição
	Essas informações aparecem no campo Description (Descrição) ao ver chaves de criptografia no Core Console.
Passphrase (Senha)	Digite a senha que será usada para controlar o acesso. O recomendado é evitar caracteres especiais listados na descrição de nome desta tabela. Anote a senha em um local seguro. O suporte da Dell não pode recuperar uma senha. Depois de criar uma chave de criptografia e aplicá-la a uma ou mais das máquinas protegidas, você não pode recuperar os dados se perder a senha.
Confirm Passphrase (Confirmar senha)	Digite novamente a senha que você acabou de digitar.

17 Clique em **Concluir**.

O Rapid Recovery adiciona as MVs selecionadas e seu host à lista de máquinas protegidas.

Acessar o diagnóstico de máquinas protegidas

No Rapid Recovery, você pode baixar e visualizar informações de diagnóstico de máquinas protegidas individuais. Além disso, o Rapid Recovery permite baixar e visualizar dados de log do Core.

Para acessar os logs, consulte os procedimentos a seguir:

- Como baixar e exibir o arquivo de log do Core
- Download e visualização do arquivo de log de uma máquina protegida

Download e visualização do arquivo de log de uma máquina protegida

Se você encontrar erros ou problemas com uma máquina protegida, poderá baixar os logs da máquina para visualizá-los ou compartilhá-los com seu representante de suporte da Dell.

1 Na área de navegação à esquerda do Core Console, no menu Máquinas protegidas, clique na seta para expandir o menu sensível ao contexto da máquina protegida relevante. Role para baixo até **Mais**, expanda esse menu e selecione  **Log do agente**.

A página **Baixar log do agente** é mostrada.

2 Na página **Baixar log do agente**, clique em **Clique aqui para começar o download**.

3 Na caixa de diálogo **Abrindo AgentAppRecovery.log**, realize um dos procedimentos a seguir:

- Para abrir o arquivo de log, selecione **Abrir com**, selecione um aplicativo (como o Bloco de Notas) para visualizar o arquivo de log baseado em texto e, por último, clique em **OK**.

  O arquivo AgentAppRecovery.log é aberto no aplicativo selecionado.
- Para salvar o arquivo localmente, selecione **Salvar arquivo** e clique em **OK**.

  O arquivo AgentAppRecovery.log é salvo na sua pasta Downloads. Ele pode ser aberto usando qualquer editor de texto.

Download e visualização do arquivo de log de uma máquina protegida

Se você encontrar erros ou problemas com uma máquina protegida, poderá baixar os logs da máquina para visualizá-los ou compartilhá-los com seu representante de suporte da Dell.

1 Na área de navegação à esquerda do Core Console, no menu Máquinas protegidas, clique na seta para expandir o menu sensível ao contexto da máquina protegida relevante. Role para baixo até **Mais**, expanda esse menu e selecione **Log do agente**.
A página **Baixar log do agente** é mostrada.

2 Na página **Baixar log do agente**, clique em **Clique aqui para começar o download**.

3 Na caixa de diálogo **Abrindo AgentAppRecovery.log**, realize um dos procedimentos a seguir:

- Para abrir o arquivo de log, selecione **Abrir com** e um aplicativo (como Bloco de Notas) para visualizar o arquivo de log com base em texto e, por fim, clique em **OK**.
  O arquivo AgentAppRecovery.log é aberto no aplicativo selecionado.
- Para salvar o arquivo localmente, selecione **Salvar arquivo** e clique em **OK**.
  O arquivo AgentAppRecovery.log é salvo na sua pasta Downloads. Ele pode ser aberto usando-se qualquer editor de texto.

Links relacionados

Como baixar e exibir o arquivo de log do Core

Como ver o status da máquina e outros detalhes

Conclua a etapa deste procedimento para ver o status, bem como outros detalhes para uma máquina.

No Rapid Recovery Core Console, navegue até a máquina protegida que você deseja ver.
As informações sobr ea máquina são mostradas na página Summary (Resumo). Os detalhes exibios contêm o seguinte:

- Nome de host
- Último instantâneo salvo
- Próximo instantâneo agendado
- Status da criptografia
- Número da versão
  Se o Exchange Server estiver instalado na máquina, informações detalhadas sobre o servidor também são exibidas e incluem:
- Última verificação de Mountability bem-sucedida
- Última verificação de Soma de Verificação bem-sucedida
- Último truncamento de log realizado
  Informações detalhadas sobre os volumes contidos neste computador também são exibidas e incluem:
- Nome do volume
- Programação
- Cronograma atual
- Próximo instantâneo
- Tipo de sistema de arquivos
- Uso do espaço fora do tamanho total
- Se o SQL Server estiver instalado na máquina, informações detalhadas sobre o servidor também são exibidas e incluem:
  Status on-line
- Nome
- Caminho de instalação

- Versão

  Se o Exchange Server estiver instalado na máquina, as informações detalhadas sobre o servidor e os armazenamentos de e-mail também são exibidas e contêm:
- Versão
- Caminho de instalação
- Caminho de dados
- Nome do banco de dados
- Caminho dos bancos de dados Exchange
- Caminho do arquivo de log
- Prefixo de log
- Caminho do sistema
- Tipo de armazenamento de e-mail

Gerenciar máquinas

Esta seção descreve as diferentes tarefas que você pode executar para gerenciar suas máquinas. Os tópicos são:

- Remover uma máquina
- Remover um cluster da proteção
- Visualizar informações de licença em uma máquina
- Download e visualização do arquivo de log de uma máquina protegida
- Converter um nó de cluster protegido em uma máquina protegida

Remover uma máquina

Ao remover uma máquina da proteção no Rapid Recovery Core, você tem duas opções: manter os pontos de recuperação salvos até o momento no RR Core ou removê-los. Se você mantiver os pontos de recuperação, terá o que é conhecido como máquina “apenas com pontos de recuperação". Usando esses pontos de recuperação para a máquina que foi removida da proteção atual, você pode continuar a restaurar a máquina no futuro, mas apenas até o estado capturado em um ponto de recuperação salvo.

Se você remover os pontos de recuperação, essa ação excluirá do Rapid Recovery Core todos os dados de snapshot da máquina anteriormente protegida.

CUIDADO: Se você excluir pontos de recuperação, não poderá mais restaurar os dados dessa máquina.

Execute as etapas do procedimento a seguir para remover uma máquina da proteção no seu ambiente do Rapid Recovery.

1. Do Rapid Recovery Core Console, no painel de navegação à esquerda, em Máquinas protegidas, clique na máquina que você deseja remover.
2. Na página Resumo da respectiva máquina, clique em **Remover máquina**.
3. Na caixa de diálogo, se você quiser excluir também todos os pontos de recuperação dessa máquina do repositório, selecione **Remover com pontos de recuperação**.
4. Para confirmar a sua escolha e remover a máquina, clique em **Sim**.

   O Rapid Recovery remove a máquina da proteção e cancela todas as tarefas ativas da máquina.

Cancelar operações em uma máquina

É possível cancelar operações atualmente em execução em uma máquina. Você pode especificar o cancelamento de apenas um snapshot atual ou cancelar todas as operações atuais, incluindo exportações, replicações, e assim por diante.

1 No Rapid Recovery Core Console, na área de navegação à esquerda, em Máquinas protegidas, clique na máquina cujas operações você deseja cancelar.
2 Clique em **Eventos**.
3 Clique no ícone Detalhes do trabalho à direita do evento em progresso ou da operação que você deseja cancelar.
4 Na caixa de diálogo Monitorar tarefa ativa, clique em **Cancelar**.

Visualizar informações de licença em uma máquina

Você pode visualizar as informações de status da licença do status da licença Rapid Recovery instalado em uma máquina protegida.

1 No Rapid Recovery Core Console, em Máquinas protegidas, clique na máquina que você deseja modificar.
A página **Resumo** da máquina de seleção é exibida.
2 Clique no menu **Definições**.
A página **Definições** é exibida, mostrando definições de configuração da máquina selecionada.
3 Clique no link **Aplicação de licença** para rolar a página Definições a fim de exibir definições de aplicação de licença específicas de máquina.
Aparece a tela Status e apresenta os detalhes sobre a aplicação de licença do produto.

Exportação de VM

Esta seção explica como exportar um ponto de recuperação para criar uma máquina virtual.

Sobre a exportação para máquinas virtuais com o Rapid Recovery

A partir do Rapid Recovery Core, você pode exportar um ponto de recuperação de um repositório para uma máquina virtual. Esse processo — algumas vezes chamado de exportação virtual — é um processo físico para virtual (P2V) que cria uma máquina virtual a partir de um ponto de recuperação. A VM é um clone inicializável de uma máquina protegida.

NOTA: O ponto de recuperação utilizado deve fazer parte de uma cadeia completa de pontos de recuperação. Para obter mais informações sobre cadeias de pontos de recuperação, consulte o tópico Cadeias de pontos de recuperação e órfãos.

Você pode realizar uma exportação virtual a partir da página Standby virtual do Core Console ou selecionando **Exportação do VM** no menu suspenso  **Restaurar** na barra de botões.

Ao realizar uma exportação virtual no Rapid Recovery Core, você tem duas opções:

- Você pode realizar uma **exportação virtual única**, que representa um único snapshot das informações do ponto de recuperação.
- Você pode criar um **standby virtual**. Com o standby virtual, o snapshot da VM criado a partir do ponto de recuperação selecionado é atualizado continuamente pelo Core depois de cada captura de snapshot programada ou forçada da máquina de origem. Isso cria um recurso de alta disponibilidade para a recuperação de dados. Se a máquina protegida falhar, você pode inicializar a máquina virtual para substitui-la temporariamente de forma rápida, dando a você tempo para recuperar a máquina protegida original sem tempo de inatividade substancial.

O diagrama a seguir mostra uma implementação típica de exportação de dados para uma máquina virtual.

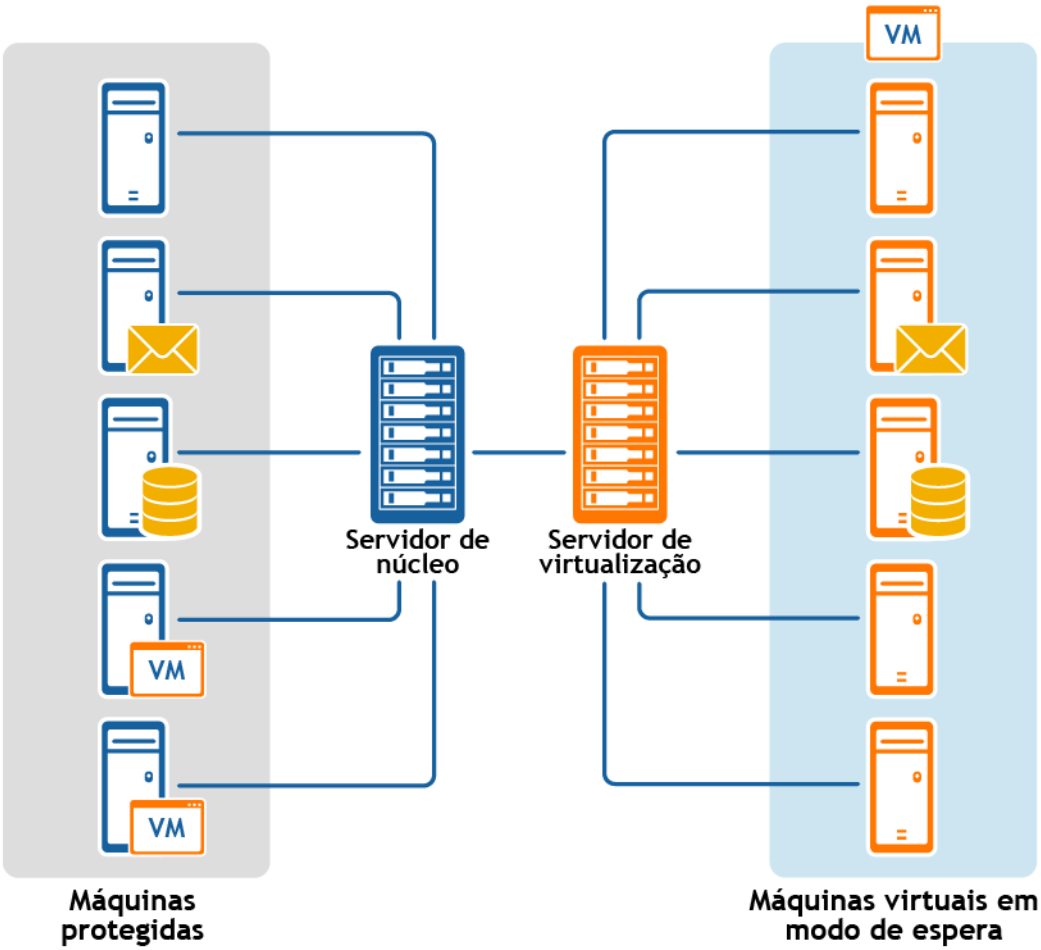


Figura 8. Implementação de standby virtual

NOTA: Em uma configuração que envolve replicação, o Core mostrado representa o Core de destino.

Ao exportar para uma máquina virtual, as informações a seguir são exportadas:

- Todos os dados de backup de um ponto de recuperação
- O sistema operacional e as definições da máquina protegida original

Você pode realizar uma exportação virtual dos pontos de recuperação de máquinas protegidas Windows ou Linux para VMware, ESXi, Hyper-V e VirtualBox.

NOTA: Para ESXi, VMware Workstation ou Hyper-V, a versão da máquina virtual deve ser uma versão licenciada dessas máquinas virtuais, não as versões gratuitas ou de teste.

Se a replicação estiver definida entre dois Cores (origem e destino), será possível exportar dados do Core de destino apenas após a replicação inicial estar concluída.

Realizar uma exportação única para ESXi

Execute as etapas deste procedimento para realizar uma exportação única para o ESXi.

1 No Rapid Recovery Core Console, na barra de botões, clique no menu suspenso **Restaurar** e em **Exportação do VM**.
2 No Assistente de exportação de máquina virtual, selecione **Exportação única**.
3 Clique em **Avançar**.
4 Na página Máquinas, selecione a máquina protegida que você deseja exportar.
5 Clique em **Avançar**.
6 Na página Pontos de recuperação, selecione o ponto de recuperação que você deseja usar na exportação.
7 Clique em **Avançar**.
8 Na página Destino do Assistente de exportação, no menu suspenso Recuperar na máquina virtual, selecione **ESX(i)**.
9 Insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir e clique em **Avançar**.

Tabela 103. Parâmetros da máquina virtual

Opções	Descrição
Nome do host	Insira um nome para a máquina de host.
Port	Insira a porta para a máquina de host. O padrão é 443.
Nome de usuário	Insira o nome de usuário de login na máquina de host.
Senha	Digite a senha de login na máquina de host.

10 Na página Opções de máquina virtual, insira as informações conforme descrito na tabela a seguir.

Tabela 104. Opções da máquina virtual

Opção	Descrição
Conjunto de recursos	Selecione um conjunto de recursos na lista suspensa.
Local da configuração de VM	Selecione um armazenamento de dados na lista suspensa.
Nome da máquina virtual	Digite um nome para a máquina virtual.
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • Usar a mesma quantidade de RAM da máquina de origem • Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.
Número de processadores	O número de processadores (CPUs) que você deseja para a máquina virtual exportada. O mínimo é 1.
Cores por processador	O número de núcleos desejado para cada processador. O mínimo é 1.
Aprovisionamento de disco	Selecione o tipo de aprovisionamento de disco nas seguintes opções: • Fino. O aprovisionamento fino cria um disco virtual com o mesmo espaço usado nos volumes originais, em vez do tamanho do volume inteiro. Por exemplo, caso o volume original seja 1 TB, mas contém apenas 2 GB de espaço usado, o Rapid Recovery cria um disco virtual de 2 GB.

Opção	Descrição
	• Grosso. O aprovisionamento grosso cria um novo disco ou volume com o mesmo volume original do servidor protegido, mesmo caso apenas uma parte do volume original esteja sendo usada. Por exemplo, caso o volume seja 1 TB, mas contém apenas 2 GB de espaço usado, o Rapid Recovery cria um disco virtual de 1 TB.
Mapeamento de disco	Especifique o tipo de mapeamento de disco nas seguintes opções: • Automático • Manual • Com VM
Versão	Selecione a versão do ESXi usado para criar a máquina virtual na lista suspensa.

11 Clique em **Avançar**.

12 Na página Volumes, selecione os volumes que deseja exportar e clique em **Avançar**.

13 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Realizar uma exportação contínua (Standby virtual) para ESXi

Execute as etapas descritas neste procedimento para realizar a exportação contínua para uma máquina virtual (VM) ESXi usando o Rapid Recovery.

1 No Rapid Recovery Core Console, escolha uma das opções a seguir:

- No Core Console, na barra de botões, clique em  menu suspenso **Restaurar** e selecione **Exportação do VM**.
  1 No Assistente de exportação de máquina virtual, selecione **Contínuo (Standby Virtual)**.
  2 Clique em **Avançar.**
- No Core Console, na barra de ícones, clique em  (Standby virtual).
  - Na página **Standby virtual**, clique em **Adicionar** para iniciar o Assistente de exportação de máquina virtual.

2 Na página **Máquinas** do Assistente de exportação de máquina virtual, selecione a máquina protegida que você deseja exportar.

3 Clique em **Avançar**.

4 Na página **Pontos de recuperação**, selecione o ponto de recuperação que você deseja usar para a exportação.

5 Clique em **Avançar**.

6 Na página **Destino** do Assistente de exportação, no menu suspenso Recuperar para uma máquina virtual, selecione **ESXi**.

7 Insira as informações para acessar a máquina virtual, conforme descrito na tabela a seguir, e clique em **Avançar**.

Tabela 105. Credenciais de ESXi

Opção	Descrição
Nome do host	Insira um nome para a máquina de host.
Port	Insira a porta para a máquina de host. O padrão é 443.
Nome de usuário	Insira as credenciais de login para a máquina de host.
Senha	Insira as credenciais de login para a máquina de host.

8 Na página **Virtual Machine Options** (Opções de máquina virtual), digite as informações conforme descrito na tabela a seguir.

Tabela 106. Opções da máquina virtual

Opção	Descrição
Conjunto de recursos	Selecione um conjunto de recursos na lista suspensa.
Armazenamento de dados	Selecione um armazenamento de dados na lista suspensa.
Nome da máquina virtual	Insira um nome para a máquina virtual.
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • Usar a mesma quantidade de RAM da máquina de origem • Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.
Número de processadores	O número de processadores (CPUs) que você deseja para a máquina virtual exportada. O valor mínimo é 1.
Cores por processador	O número de cores que você deseja ter para cada processador. O valor mínimo é 1.
Aprovisionamento de disco	Selecione o tipo de aprovisionamento de disco das seguintes opções: • Thin (Dinâmico). O aprovisionamento dinâmico cria um disco virtual do tamanho do espaço usado nos volumes originais, em vez de todo o tamanho do volume. Por exemplo, se o volume original é de 1 TB, mas contém somente 2 GB de espaço usado, o Rapid Recovery cria um disco virtual de 2 GB. • Tradicional. O aprovisionamento tradicional cria um novo disco ou volume com o mesmo tamanho do volume original do servidor protegido, mesmo que somente uma parte do volume original esteja em uso. Por exemplo, se o volume original é de 1 TB, mas contém 2 GB de espaço usado, o Rapid Recovery cria um disco virtual de 1 TB.
Mapeamento de disco	Especifique o tipo de mapeamento de disco conforme adequado (Automático, Manual ou com VM).
Versão	Selecione a versão da máquina virtual.
Realizar exportação única inicial	Selecione para realizar a exportação virtual imediatamente em vez de após o próximo snapshot programado (opcional)

9 Clique em **Avançar**.

10 Na página **Volumes**, selecione os volumes que deseja exportar e clique em **Avançar**.

11 Na página **Resumo**, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as páginas Standby virtual e Eventos.

Realizar uma exportação única para VMware Workstation

Execute as etapas deste procedimento para realizar uma exportação única para VMware Workstation.

1 No Console do Rapid Recovery Core, na barra de botões, clique no menu suspenso **Restaurar**, clique em **Exportação do VM**.

2 No Assistente de exportação de máquina virtual, selecione **Exportação única**.

3 Clique em **Avançar**.

4 Na página de Máquinas, selecione a máquina protegida que você deseja exportar.

5 Clique em **Avançar**.

6 Na página Pontos de recuperação, selecione o ponto de recuperação que você deseja exportar.

7 Clique em **Avançar**.

8 Na página Destino do Assistente de exportação, no menu suspenso Recuperar na máquina virtual, selecione **VMware Workstation** e clique em **Avançar**.

9 Na página Opções de máquina virtual, insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir.

Tabela 107. Parâmetros da máquina virtual

Opção	Descrição
Local da máquina de VM	Especifique o caminho da pasta local ou compartilhamento de rede no qual você deseja criar a máquina virtual. **NOTA: Se você especificou um caminho de compartilhamento de rede, será preciso inserir credenciais de login válidas para uma conta que está registrada na máquina de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.**
Nome de usuário	Insira as credenciais de login do local de rede para a exportação. • Se você especificou um caminho de compartilhamento de rede, será preciso inserir um nome de usuário válido para uma conta que está registrada na máquina de destino. • Se você inseriu um caminho local, um nome de usuário não é necessário.
Senha	Insira as credenciais de login do local de rede para a exportação. • Se você especificou um caminho de compartilhamento de rede, será preciso inserir uma senha válida para uma conta que está registrada na máquina de destino. • Se você inseriu um caminho local, uma senha não é necessária.
Nome de VM	Insira um nome para a máquina virtual sendo criada, por exemplo, VM-0A1B2C3D4. **NOTA: O nome padrão é o nome da máquina de origem.**
Versão	Especifique a versão do VMware Workstation da máquina virtual. Você pode selecionar dentre: • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0 • VMware Workstation 11.0 • VMware Workstation 12.0
Quantidade de RAM (MB)	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • Usar a mesma quantidade de RAM da máquina de origem • Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.
Número de processadores	O número de processadores (CPUs) que você quer para a máquina virtual exportada. O valor mínimo é 1.
Cores por processador	O número de cores que você quer ter para cada processador. O valor mínimo é 1.

10 Clique em **Avançar**.

11 Na página Volumes, selecione os volumes para exportar, por exemplo, C:\ e D:\, e clique em **Avançar**.

12 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Realizar uma exportação contínua (Standby virtual) para VMware Workstation

Execute as etapas deste procedimento para realizar a exportação contínua para uma máquina virtual (VM) de área de trabalho do VMWare usando o Rapid Recovery.

1 No Rapid Recovery Core Console, escolha uma das opções a seguir:

- No Core Console, na barra de botões, clique em  menu suspenso **Restaurar** e selecione **Exportação do VM**.
  1 No Assistente de exportação de máquina virtual, selecione **Contínuo (Standby Virtual)**.
  2 Clique em **Avançar.**
- No Core Console, na barra de ícones, clique em  (Standby virtual).
  - Na página **Standby virtual**, clique em **Adicionar** para iniciar o Assistente de exportação de máquina virtual.

2 Na página **Máquinas** do Assistente de exportação de máquina virtual, selecione a máquina protegida que você deseja exportar.

3 Clique em **Avançar**.

4 Na página **Pontos de recuperação**, selecione o ponto de recuperação que você deseja usar para a exportação.

5 Clique em **Avançar**.

6 Na página **Destino** do Assistente de exportação de máquina virtual, no menu suspenso Recuperar para uma máquina virtual, selecione **Área de trabalho do VMWare** e clique em **Avançar**.

7 Na página **Opções de máquina virtual**, insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir.

Tabela 108. Parâmetros da máquina virtual

Opção	Descrição
Caminho de destino	Especifique o caminho da pasta local ou compartilhamento de rede no qual você deseja criar a máquina virtual. **NOTA: Se você especificou um caminho de compartilhamento de rede, será preciso inserir credenciais de login válidas para uma conta que está registrada na máquina de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.**
Nome de usuário	Insira as credenciais de login do local de rede para a exportação. • Se você especificou um caminho de compartilhamento de rede, será preciso inserir um nome de usuário válido para uma conta que está registrada na máquina de destino. • Se você inseriu um caminho local, um nome de usuário não é necessário.
Senha	Insira as credenciais de login do local de rede para a exportação. • Se você especificou um caminho de compartilhamento de rede, será preciso inserir uma senha válida para uma conta que está registrada na máquina de destino. • Se você inseriu um caminho local, uma senha não é necessária.
Máquina virtual	Insira um nome para a máquina virtual sendo criada, por exemplo, VM-0A1B2C3D4. **NOTA: O nome padrão é o nome da máquina de origem.**
Versão	Especifique a versão do VMware Workstation da máquina virtual. Você pode selecionar dentre: • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0

Opção	Descrição
	• VMware Workstation 11.0 • VMware Workstation 12.0
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • Usar a mesma quantidade de RAM da máquina de origem • Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.
Número de processadores	O número de processadores (CPUs) que você deseja para a máquina virtual exportada. O valor mínimo é 1.
Cores por processador	O número de cores que você deseja ter para cada processador. O valor mínimo é 1.

8 Selecione **Realizar exportação única inicial** para realizar a exportação virtual imediatamente e não após o próximo snapshot programado.

9 Clique em **Avançar**.

10 Na página **Volumes**, selecione os volumes para exportar, por exemplo, C:\ e D:\, e clique em **Avançar**.

11 Na página **Summary** (Resumo), clique em **Finish** (Concluir) para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as páginas Standby virtual e Eventos.

Realizar uma exportação única de Hyper-V

Execute as etapas deste procedimento para realizar uma exportação única para o Hyper-V.

1 No Rapid Recovery Core Console, na barra de botões, clique no menu suspenso **Restaurar**, em **Exportação do VM**.

2 No Assistente de exportação de máquina virtual, selecione **Exportação única**.

3 Clique em **Avançar**.

4 Na página **Máquinas**, selecione a máquina protegida que você deseja exportar.

5 Clique em **Avançar**.

6 Na página **Pontos de recuperação**, selecione o ponto de recuperação que você deseja usar na exportação.

7 Clique em **Avançar**.

8 Na página **Destino**, no menu suspenso Exportar para máquina virtual, selecione **Hyper-V**.

9 Para exportar para uma máquina local com a função Hyper-V atribuída, clique em **Usar a máquina local**.

10 Para indicar que o servidor Hyper-V está localizado em uma máquina remota, clique em **Host remoto** e insira as informações do host remoto conforme descrito na tabela a seguir.

Tabela 109. Informações do host remoto

Caixa de texto	Descrição
Nome do host	Insira um endereço IP ou nome de host para o server Hyper-V. Ele representa o endereço IP ou nome de host do server Hyper-V remoto.
Port	Insira um número de porta para a máquina. Ele representa a porta através da qual o Core se comunica com esta máquina.
Nome de usuário	Insira o nome de usuário para o usuário com privilégios administrativos para a estação de trabalho com o server Hyper-V. Ele é usado para especificar as credenciais de login para a máquina virtual.

Caixa de texto	Descrição
Senha	Insira a senha da conta de usuário com privilégios administrativos na estação de trabalho com o server Hyper-V. Ele é usado para especificar as credenciais de login para a máquina virtual.

11 Clique em **Avançar**.

12 Na página **Opções de máquinas virtuais**, na caixa de texto **Local da máquina de VM**, insira o caminho da máquina virtual; por exemplo, **D:\export**. Isso é usado para identificar o local da máquina virtual.

NOTA: Você precisa especificar o local da máquina virtual para os servers Hyper-V local e remoto. O caminho precisa ser um caminho de local válido para o server Hyper-V. Diretórios não existentes são automaticamente criados. Você não deve tentar criá-los manualmente. A exportação para pastas compartilhadas (por exemplo, para \\data\share) não é permitida.

13 Na caixa de texto **Nome da máquina virtual**, insira o nome da máquina virtual.

O nome inserido será exibido na lista de máquinas virtuais no console do Hyper-V Manager.

14 Para especificar o uso da memória, clique em um dos seguintes:

- **Usar a mesma quantidade de RAM da máquina de origem**. Selecione essa opção para identificar se o uso da RAM é idêntico entre as máquinas virtuais e de origem.
- **Usar uma quantidade específica de RAM.** Selecione essa opção caso você queira especificar a quantidade de RAM em MB.

  A quantidade mínima é 1.024 MB e o máximo permitido pelo aplicativo é 65.536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

15 Para especificar o formato do disco, próximo a Formato do disco, clique em um dos seguintes:

- VHDX
- VHD

NOTA: A exportação do Hyper-V suporta formatos de disco VHDX se a máquina de destino estiver executando o Windows 8 (Windows Server 2012) ou mais recente. Se o formato VHDX não for suportado por seu ambiente, a opção será desativada.

Se desejar exportar para a geração Hyper-V 2, somente o formato de disco VHDX é suportado.

16 Para especificar a geração do Hyper-V a fim de utilizar para exportação, clique em um dos seguintes:

- Geração 1
- Geração 2

NOTA: Somente a geração 2 oferece suporte à opção de inicialização segura.

17 Especifique o adaptador de rede adequado para a VM exportada.

18 Na página **Volumes**, selecione os volumes a serem exportados; por exemplo, C:\.

NOTA: Se os volumes selecionados forem maiores do que as alocações máximas adequadas suportadas pelo aplicativo conforme indicado abaixo, ou exceder a quantidade de espaço disponível, será exibido um erro.

- Para o formato de disco VHDX, seus volumes selecionados não devem ser maiores do que 64 TB.
- Para o formato de disco VHD, seus volumes selecionados não devem ser maiores do que 2040 GB.

19 Na página **Volumes**, clique em **Concluir** para concluir e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação vendo as páginas Standby virtual ou Eventos.

Realizar uma exportação contínua (Standby virtual) para Hyper-V

Conclua as etapas nesse procedimento para realizar uma exportação contínua para uma máquina virtual (VM) Hyper-V usando Rapid Recovery.

1 No Rapid Recovery Core Console, realize um dos procedimentos a seguir:

- No Core Console, na barra de botões, clique na  Menu suspenso **Restaurar** e selecione **Exportação do VM**.

1 No Assistente de exportação de máquina virtual, selecione **Contínuo (Standby virtual)**.

2 Clique em **Avançar.**

- No Core Console, na barra de ícones, clique em  (Standby virtual).
  - Na página **Standby virtual**, clique em **Adicionar** para abrir o Assistente de exportação de máquina virtual.

2 Na página **Máquinas** do Assistente de exportação de máquina virtual, selecione a máquina protegida que você deseja exportar.

3 Clique em **Avançar**.

4 Na página **Pontos de recuperação**, selecione o ponto de recuperação que você deseja usar na exportação.

5 Clique em **Avançar**.

6 Na página **Destino**, no menu suspenso Exportar para uma máquina virtual, selecione **Hyper-V** e realize um dos seguintes procedimentos:

- Para exportar para uma máquina local com a função Hyper-V atribuída, clique em **Usar a máquina local**.
- Para indicar que o servidor Hyper-V está localizado em uma máquina remota, clique em **Host remoto** e insira os parâmetros do host remoto conforme descrito na tabela a seguir.

Tabela 110. Informações do host remoto

Caixa de texto	Descrição
Nome do host	Insira um endereço IP ou nome de host para o server Hyper-V. Ele representa o endereço IP ou nome de host do server Hyper-V remoto.
Port	Insira um número de porta para a máquina. Ele representa a porta através da qual o Core se comunica com esta máquina.
Nome de usuário	Insira o nome de usuário para o usuário com privilégios administrativos para a estação de trabalho com o server Hyper-V. Ele é usado para especificar as credenciais de login para a máquina virtual.
Senha	Insira a senha da conta de usuário com privilégios administrativos na estação de trabalho com o server Hyper-V. Ele é usado para especificar as credenciais de login para a máquina virtual.

7 Clique em **Avançar**.

8 Na página **Opções de máquinas virtuais**, na caixa de texto **Local da máquina de VM**, insira o caminho da máquina virtual; por exemplo, **D:\export**. Isso é usado para identificar o local da máquina virtual.

NOTA: Você precisa especificar o local da máquina virtual para os servers Hyper-V local e remoto. O caminho precisa ser um caminho de local válido para o server Hyper-V. Diretórios não existentes são automaticamente criados. Você não deve tentar criá-los manualmente. A exportação para pastas compartilhadas (por exemplo, para \\data\share) não é permitida.

9 Na caixa de texto **Nome da máquina virtual**, insira o nome da máquina virtual.

O nome inserido será exibido na lista de máquinas virtuais no console do Hyper-V Manager.

10 Para especificar o uso da memória, clique em um dos seguintes:

- **Usar a mesma quantidade de RAM da máquina de origem**. Selecione essa opção para identificar se o uso da RAM é idêntico entre as máquinas virtuais e de origem.
- **Usar uma quantidade específica de RAM.** Selecione essa opção caso você queira especificar a quantidade de RAM em MB.

  A quantidade mínima é 1.024 MB e o máximo permitido pelo aplicativo é 65.536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

11 Para especificar o formato do disco, próximo a Formato do disco, clique em um dos seguintes:

- VHDX
- VHD

NOTA: A exportação do Hyper-V suporta formatos de disco VHDX se a máquina de destino estiver executando o Windows 8 (Windows Server 2012) ou mais recente. Se o formato VHDX não for suportado por seu ambiente, a opção será desativada.

Se desejar exportar para a geração Hyper-V 2, somente o formato de disco VHDX é suportado.

12 Para especificar a geração do Hyper-V a fim de utilizar para exportação, clique em um dos seguintes:

- Geração 1

- Geração 2

NOTA: Somente a geração 2 oferece suporte à opção de inicialização segura.

13 Especifique o adaptador de rede adequado para a VM exportada.

14 Na página **Volumes**, selecione os volumes a serem exportados; por exemplo, C:\.

NOTA: Se os volumes selecionados forem maiores do que as alocações máximas adequadas suportadas pelo aplicativo conforme indicado abaixo, ou exceder a quantidade de espaço disponível, será exibido um erro.

- Para o formato de disco VHDX, seus volumes selecionados não devem ser maiores do que 64 TB.
- Para o formato de disco VHD, seus volumes selecionados não devem ser maiores do que 2040 GB.

15 Selecione **Realizar exportação única inicial** para realizar a exportação virtual imediatamente e não após o próximo snapshot programado.

16 Na página **Volumes**, clique em **Concluir** para concluir e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação vendo as páginas Standby virtual ou Eventos.

Realizar uma exportação única de VirtualBox

Execute as etapas deste procedimento para realizar uma exportação única para o VirtualBox.

1 No Console do Rapid Recovery Core, na barra de botões, clique no menu suspenso **Restaurar** e, em seguida, clique em **Exportação do VM**.

2 No Assistente de exportação de máquina virtual, selecione **Exportação única**.

3 Clique em **Avançar**.

4 Na página de Máquinas, selecione a máquina protegida que você deseja exportar.

5 Clique em **Avançar**.

6 Na página Pontos de recuperação, selecione o ponto de recuperação que você deseja exportar.

7 Clique em **Avançar**.

8 Na página Destino do Assistente de exportação, no menu suspenso Recuperar na máquina virtual, selecione **VirtualBox**e clique em **Avançar**.

9 Na página Opções de máquina virtual, selecione **Usar a máquina do Windows**.

10 Insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir.

Tabela 111. Parâmetros da máquina virtual

Opção	Descrição
Nome da máquina virtual	Insira um nome para a máquina virtual sendo criada. **NOTA: O nome padrão é o nome da máquina de origem.**
Caminho de destino	Especifique um caminho de destino local ou remoto para criar a máquina virtual. **NOTA: O caminho de destino não deve ser um diretório raiz.** **Se você especificou um caminho de compartilhamento de rede, será preciso inserir credenciais de login válidas (nome de usuário e senha) para uma conta que está registrada na máquina de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.**
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • Usar a mesma quantidade de RAM da máquina de origem • Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB

Opção	Descrição
	A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

11 Para especificar uma conta de usuário para a máquina virtual, selecione **Especifique a conta de usuário para a máquina virtual exportada** e insira as seguintes informações. Isso se refere a uma conta de usuário específica para a qual a máquina virtual será registrada caso existam múltiplas contas de usuários na máquina virtual. Quando essa conta de usuário estiver conectada, somente esse usuário verá essa máquina virtual no gerenciador do VirtualBox. Se uma conta não for especificada, a máquina virtual será registrada para todos os usuários existentes na máquina com Windows e VirtualBox.

- Nome de usuário - insira o nome de usuário com o qual a máquina virtual é registrada.
- Senha - insira a senha dessa conta de usuário.

12 Clique em **Avançar**.

13 Na página Volumes, selecione os volumes para exportar, por exemplo, C:\ e D:\, e clique em **Avançar**.

14 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Realizar uma exportação contínua de VirtualBox (Standby virtual)

Para realizar essa etapa, o VirtualBox deve estar instalado na máquina Core.

Conclua as etapas nesse procedimento para realizar uma exportação contínua para uma máquina virtual (VM) VirtualBox usando Rapid Recovery.

1 No Rapid Recovery Core Console, realize um dos procedimentos a seguir:

- No Core Console, na barra de botões, clique na  Menu suspenso **Restaurar** e selecione **Exportação do VM**.
  1 No Assistente de exportação de máquina virtual, selecione **Contínuo (Standby virtual)**.
  2 Clique em **Avançar.**
- No Core Console, na barra de ícones, clique em  (Standby virtual).
  - Na página **Standby virtual**, clique em **Adicionar** para abrir o Assistente de exportação de máquina virtual.

2 Na página **Máquinas** do Assistente de exportação de máquina virtual, selecione a máquina protegida que você deseja exportar.

3 Clique em **Avançar**.

4 Na página **Pontos de recuperação**, selecione o ponto de recuperação que você deseja usar na exportação.

5 Clique em **Avançar**.

6 Na página **Destino** do Assistente de exportação, no menu suspenso **Recuperar para uma máquina virtual**, selecione **VirtualBox**.

7 Na página **Virtual Machine Options** (Opções de máquina virtual), selecione **Remote Linux Machine** (Máquina Linux remota).

8 Insira as informações sobre a máquina virtual conforme descrito na tabela a seguir.

Tabela 112. Definições da máquina Linux remota

Opção	Descrição
Nome de host do VirtualBox	Insira um endereço IP ou nome de host para o server VirtualBox. Este campo representa o endereço IP ou nome de host do server VirtualBox remoto.
Port	Insira um número de porta para a máquina. Este número representa a porta através da qual o Core se comunica com esta máquina.
Nome da máquina virtual	Insira um nome para a máquina virtual sendo criada.

Opção	Descrição
	NOTA: O nome padrão é o nome da máquina de origem.
Caminho de destino	Especifique um caminho de destino para criar a máquina virtual. **NOTA: Recomenda-se criar uma pasta raiz a partir da raiz para que a máquina virtual seja executa a partir da raiz. Se você não usar a raiz, será preciso criar uma pasta de destino manualmente na máquina de destino antes de configurar a exportação. Também será preciso conectar ou carregar manualmente a máquina virtual após a exportação.**
Nome de usuário	Nome de usuário da conta na máquina de destino, por exemplo, raiz.
Senha	Senha para a conta de usuário na máquina de destino.
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • Usar a mesma quantidade de RAM da máquina de origem • Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

9 Selecione **Realizar exportação única inicial** para realizar a exportação virtual imediatamente e não após o próximo snapshot programado.

10 Clique em **Avançar**.

11 Na página **Volumes**, selecione os volumes de dados a serem exportados e clique em **Avançar**.

12 Na página **Summary** (Resumo), clique em **Finish** (Concluir) para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Gerenciar exportações

Caso o Core tenha exportação virtual estabelecida, os parâmetros de configuração de cada exportação virtual são exibidos como uma linha na página **Standby virtual**. Aqui você pode ver o status de exportações configuradas atualmente e gerenciar as máquinas de standby virtual. Você pode adicionar um standby virtual, forçar uma exportação, pausar ou retomar um standby virtual, ou remover os requisitos de exportação contínua.

Quando uma exportação única acontece, o trabalho é listado na fila de exportação da página **Standby virtual**. Durante esse tempo, você pode pausar, retomar ou cancelar a operação de exportação.

NOTA: Rapid Recovery dá suporte à exportação do Hyper-V para Windows 8, Windows 8.1, Windows Server 2012 e 2012 R2..

A exportação virtual para uma VM com standby virtual não ocorre caso a VM esteja ligada.

Conclua as etapas nesse procedimento para gerenciar exportações virtuais.

1 No Core Console, na barra de ícones, clique em  (Standby virtual).

A página **Standby virtual** é exibida. Aqui você pode ver duas tabelas de definições de exportação salvas. Elas incluem as informações descritas na tabela a seguir.

Tabela 113. Informações de standby virtual

Coluna	Descrição
Selecione um item	Para cada fila na tabela de resumo, você pode marcar a caixa de seleção para realizar ações na lista de opções do menu anterior à tabela.
Indicador de status	As esferas coloridas na coluna Status mostram o status de standby virtual. Quando você passa o cursor sobre o círculo colorido, a condição de status é exibida. • Verde. O standby virtual foi configurado com êxito, está ativo e não foi pausado. A próxima exportação é realizada logo depois da conclusão do próximo snapshot. • Amarelo. Standby virtual pausa, mas os parâmetros ainda estão definidos e salvos no Core. No entanto, depois de uma nova transferência, o trabalho de exportação não iniciará automaticamente e não haverá exportações novas para essa máquina protegida até o status mudar.
Nome da máquina	O nome da máquina de origem.
Destino	A máquina virtual e o caminho para o qual os dados estão sendo exportados.
Tipo de exportação	O tipo de plataforma de máquina virtual para a exportação, como ESXi, VMware, Hyper-V ou VirtualBox.
Última exportação	Data e hora da última exportação. Caso uma exportação tenha sido recém-adicionada, mas não tenha sido concluída, uma mensagem é exibida informando que a exportação ainda não foi realizada. Caso uma exportação tenha falhado ou tenha sido cancelada, uma mensagem correspondente também é exibida.
Definições	O menu suspenso permite realizar as seguintes funções: • **Editar**. Permite editar as definições de standby virtual. • **Forçar**. Força uma exportação virtual. • **Pausar**. Pausa a exportação virtual. Disponível apenas quando o status está ativo. • **Retomar**. Retoma a exportação virtual. Disponível apenas quando o status está pausado. • **Remover**. Remove o requisito para exportação contínua. Não remove a VM exportada atualizada mais recentemente.

Tabela 114. Informações da fila de exportação

Coluna	Descrição
Selecione um item	Para cada fila na tabela de resumo, você pode marcar a caixa de seleção para realizar ações na lista de opções do menu anterior à tabela.
Destino	A máquina virtual e o caminho para o qual os dados estão sendo exportados.
Tipo de exportação	O tipo de plataforma de máquina virtual para a exportação, como ESXi, VMware, Hyper-V ou VirtualBox.
Tipo de programação	O tipo de exportação (Única ou Contínua).
Status	O progresso da exportação, exibido como porcentagem em uma barra de progresso.

2 Para gerenciar as definições de exportação salvas, selecione uma exportação e clique em um dos seguintes:

- **Editar**. Abre o **Assistente de exportação de máquina virtual** para a página **Opções de VM**. Aqui você pode alterar o local da VM exportada, alterar a versão do tipo de VM ou especificar RAM ou processadores para a exportação. Para iniciar imediatamente a exportação do VM, selecione **Realizar a exportação única inicial**.
-
- **Forçar**. Força uma nova exportação. Essa opção pode ser útil quando o standby virtual está em pausa e é retomado, o que significa que o trabalho de exportação será reiniciado somente após uma nova transferência. Se não quiser esperar a nova transferência, poderá forçar uma exportação.

- **Pausar**. Pausa uma exportação ativa.
- **Retomar**. Retoma o requisito de continuar a exportação no próximo snapshot programado ou forçado.

3 Para remover uma exportação do sistema, selecione a exportação e clique em **Remover**.

A configuração da exportação é removida permanentemente do sistema. A remoção da configuração de standby virtual não remove qualquer máquina virtual exportada como resultado da configuração.

4 Para gerenciar o número de exportações executadas simultaneamente, faça o seguinte:

- Em Fila de exportação, clique em **Configurações**.
- Na caixa de diálogo **Máximo de exportações simultâneas**, insira o número de exportações que você deseja executar simultaneamente. O número padrão é 5.
- Clique em **Salvar**.

5 Para cancelar uma exportação única ou contínua listada no momento na Fila de exportação, selecione a exportações e clique em **Cancelar**.

6 Para adicionar uma nova exportação de standby virtual, é possível clicar em **Adicionar** para iniciar o Assistente de exportação. Para obter mais informações sobre a definição de standby virtual para uma máquina virtual específica, consulte um dos seguintes tópicos:

- Exportar dados para uma máquina virtual ESXi
- Exportar dados para uma máquina virtual VMWare Workstation
- Exportar dados para uma máquina virtual Hyper-V
- Exportar dados para uma máquina virtual VirtualBox

Exportar dados para uma máquina virtual ESXi

No Rapid Recovery, você pode exportar dados para ESXi realizando uma exportação única ou estabelecendo uma exportação contínua (para standby virtual). Execute as etapas dos procedimentos a seguir do tipo apropriado de exportação.

Realizar uma exportação única para ESXi

Execute as etapas deste procedimento para realizar uma exportação única para o ESXi.

1 No Rapid Recovery Core Console, na barra de botões, clique no menu suspenso **Restaurar** e em **Exportação do VM**.
2 No Assistente de exportação de máquina virtual, selecione **Exportação única**.
3 Clique em **Avançar**.
4 Na página Máquinas, selecione a máquina protegida que você deseja exportar.
5 Clique em **Avançar**.
6 Na página Pontos de recuperação, selecione o ponto de recuperação que você deseja usar na exportação.
7 Clique em **Avançar**.
8 Na página Destino do Assistente de exportação, no menu suspenso Recuperar na máquina virtual, selecione **ESX(i)**.
9 Insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir e clique em **Avançar**.

Tabela 115. Parâmetros da máquina virtual

Opções	Descrição
Nome do host	Insira um nome para a máquina de host.
Port	Insira a porta para a máquina de host. O padrão é 443.
Nome de usuário	Insira o nome de usuário de login na máquina de host.
Senha	Digite a senha de login na máquina de host.

10 Na página Opções de máquina virtual, insira as informações conforme descrito na tabela a seguir.

Tabela 116. Opções da máquina virtual

Opção	Descrição
Conjunto de recursos	Selecione um conjunto de recursos na lista suspensa.
Local da configuração de VM	Selecione um armazenamento de dados na lista suspensa.
Nome da máquina virtual	Digite um nome para a máquina virtual.
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • Usar a mesma quantidade de RAM da máquina de origem • Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.
Número de processadores	O número de processadores (CPUs) que você deseja para a máquina virtual exportada. O mínimo é 1.
Cores por processador	O número de núcleos desejado para cada processador. O mínimo é 1.
Aprovisionamento de disco	Selecione o tipo de aprovisionamento de disco nas seguintes opções: • Fino. O aprovisionamento fino cria um disco virtual com o mesmo espaço usado nos volumes originais, em vez do tamanho do volume inteiro. Por exemplo, caso o volume original seja 1 TB, mas contém apenas 2 GB de espaço usado, o Rapid Recovery cria um disco virtual de 2 GB. • Grosso. O aprovisionamento grosso cria um novo disco ou volume com o mesmo volume original do servidor protegido, mesmo caso apenas uma parte do volume original esteja sendo usada. Por exemplo, caso o volume seja 1 TB, mas contém apenas 2 GB de espaço usado, o Rapid Recovery cria um disco virtual de 1 TB.
Mapeamento de disco	Especifique o tipo de mapeamento de disco nas seguintes opções: • Automático • Manual • Com VM
Versão	Selecione a versão do ESXi usado para criar a máquina virtual na lista suspensa.

11 Clique em **Avançar**.

12 Na página Volumes, selecione os volumes que deseja exportar e clique em **Avançar**.

13 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Realizar uma exportação contínua (Standby virtual) para ESXi

Execute as etapas descritas neste procedimento para realizar a exportação contínua para uma máquina virtual (VM) ESXi usando o Rapid Recovery.

1 No Rapid Recovery Core Console, escolha uma das opções a seguir:

- No Core Console, na barra de botões, clique em  menu suspenso **Restaurar** e selecione **Exportação do VM**.

  1 No Assistente de exportação de máquina virtual, selecione **Contínuo (Standby Virtual)**.

  2 Clique em **Avançar.**

- No Core Console, na barra de ícones, clique em  (Standby virtual).
  - Na página **Standby virtual**, clique em **Adicionar** para iniciar o Assistente de exportação de máquina virtual.

2 Na página **Máquinas** do Assistente de exportação de máquina virtual, selecione a máquina protegida que você deseja exportar.

3 Clique em **Avançar**.

4 Na página **Pontos de recuperação**, selecione o ponto de recuperação que você deseja usar para a exportação.

5 Clique em **Avançar**.

6 Na página **Destino** do Assistente de exportação, no menu suspenso Recuperar para uma máquina virtual, selecione **ESXi**.

7 Insira as informações para acessar a máquina virtual, conforme descrito na tabela a seguir, e clique em **Avançar**.

Tabela 117. Credenciais de ESXi

Opção	Descrição
Nome do host	Insira um nome para a máquina de host.
Port	Insira a porta para a máquina de host. O padrão é 443.
Nome de usuário	Insira as credenciais de login para a máquina de host.
Senha	Insira as credenciais de login para a máquina de host.

8 Na página **Virtual Machine Options** (Opções de máquina virtual), digite as informações conforme descrito na tabela a seguir.

Tabela 118. Opções da máquina virtual

Opção	Descrição
Conjunto de recursos	Selecione um conjunto de recursos na lista suspensa.
Armazenamento de dados	Selecione um armazenamento de dados na lista suspensa.
Nome da máquina virtual	Insira um nome para a máquina virtual.
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • Usar a mesma quantidade de RAM da máquina de origem • Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.
Número de processadores	O número de processadores (CPUs) que você deseja para a máquina virtual exportada. O valor mínimo é 1.
Cores por processador	O número de cores que você deseja ter para cada processador. O valor mínimo é 1.
Aprovisionamento de disco	Selecione o tipo de aprovisionamento de disco das seguintes opções: • Thin (Dinâmico). O aprovisionamento dinâmico cria um disco virtual do tamanho do espaço usado nos volumes originais, em vez de todo o tamanho do volume. Por exemplo, se o volume original é de 1 TB, mas contém somente 2 GB de espaço usado, o Rapid Recovery cria um disco virtual de 2 GB. • Tradicional. O aprovisionamento tradicional cria um novo disco ou volume com o mesmo tamanho do volume original do servidor protegido, mesmo que somente uma parte do volume original esteja em uso. Por exemplo, se o volume original é de 1 TB, mas contém 2 GB de espaço usado, o Rapid Recovery cria um disco virtual de 1 TB.
Mapeamento de disco	Especifique o tipo de mapeamento de disco conforme adequado (Automático, Manual ou com VM).

Opção	Descrição
Versão	Selecione a versão da máquina virtual.
Realizar exportação única inicial	Selecione para realizar a exportação virtual imediatamente em vez de após o próximo snapshot programado (opcional)

9 Clique em **Avançar**.

10 Na página **Volumes**, selecione os volumes que deseja exportar e clique em **Avançar**.

11 Na página **Resumo**, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as páginas Standby virtual e Eventos.

Exportar dados para uma máquina virtual VirtualBox

No Rapid Recovery, é possível exportar dados para a Exportação do VirtualBox realizando uma exportação única ou estabelecendo uma exportação contínua (para Standby virtual).

NOTA: A exportação do VirtualBox de uma máquina protegida do Windows 10 não é suportada atualmente.

Execute as etapas dos procedimentos a seguir do tipo apropriado de exportação.

NOTA: Para realizar esse tipo de exportação, é preciso ter o VirtualBox instalado na máquina do Core. O Virtual Box Versão 4.2.18 ou superior é suportado para hosts Windows.

Realizar uma exportação única de VirtualBox

Execute as etapas deste procedimento para realizar uma exportação única para o VirtualBox.

1 No Console do Rapid Recovery Core, na barra de botões, clique no menu suspenso **Restaurar** e, em seguida, clique em **Exportação do VM**.

2 No Assistente de exportação de máquina virtual, selecione **Exportação única**.

3 Clique em **Avançar**.

4 Na página de Máquinas, selecione a máquina protegida que você deseja exportar.

5 Clique em **Avançar**.

6 Na página Pontos de recuperação, selecione o ponto de recuperação que você deseja exportar.

7 Clique em **Avançar**.

8 Na página Destino do Assistente de exportação, no menu suspenso Recuperar na máquina virtual, selecione **VirtualBox**e clique em **Avançar**.

9 Na página Opções de máquina virtual, selecione **Usar a máquina do Windows**.

10 Insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir.

Tabela 119. Parâmetros da máquina virtual

Opção	Descrição
Nome da máquina virtual	Insira um nome para a máquina virtual sendo criada. **NOTA: O nome padrão é o nome da máquina de origem.**
Caminho de destino	Especifique um caminho de destino local ou remoto para criar a máquina virtual.

Opção	Descrição
	NOTA: O caminho de destino não deve ser um diretório raiz. **Se você especificou um caminho de compartilhamento de rede, será preciso inserir credenciais de login válidas (nome de usuário e senha) para uma conta que está registrada na máquina de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.**
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • Usar a mesma quantidade de RAM da máquina de origem • Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

11 Para especificar uma conta de usuário para a máquina virtual, selecione **Especifique a conta de usuário para a máquina virtual exportada** e insira as seguintes informações. Isso se refere a uma conta de usuário específica para a qual a máquina virtual será registrada caso existam múltiplas contas de usuários na máquina virtual. Quando essa conta de usuário estiver conectada, somente esse usuário verá essa máquina virtual no gerenciador do VirtualBox. Se uma conta não for especificada, a máquina virtual será registrada para todos os usuários existentes na máquina com Windows e VirtualBox.

- Nome de usuário - insira o nome de usuário com o qual a máquina virtual é registrada.
- Senha - insira a senha dessa conta de usuário.

12 Clique em **Avançar**.

13 Na página Volumes, selecione os volumes para exportar, por exemplo, C:\ e D:\, e clique em **Avançar**.

14 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Realizar uma exportação contínua de VirtualBox (Standby virtual)

Para realizar essa etapa, o VirtualBox deve estar instalado na máquina Core.

Conclua as etapas nesse procedimento para realizar uma exportação contínua para uma máquina virtual (VM) VirtualBox usando Rapid Recovery.

1 No Rapid Recovery Core Console, realize um dos procedimentos a seguir:

- No Core Console, na barra de botões, clique na  Menu suspenso **Restaurar** e selecione **Exportação do VM**.
  1 No Assistente de exportação de máquina virtual, selecione **Contínuo (Standby virtual)**.
  2 Clique em **Avançar.**
- No Core Console, na barra de ícones, clique em  (Standby virtual).
  - Na página **Standby virtual**, clique em **Adicionar** para abrir o Assistente de exportação de máquina virtual.

2 Na página **Máquinas** do Assistente de exportação de máquina virtual, selecione a máquina protegida que você deseja exportar.

3 Clique em **Avançar**.

4 Na página **Pontos de recuperação**, selecione o ponto de recuperação que você deseja usar na exportação.

5 Clique em **Avançar**.

6 Na página **Destino** do Assistente de exportação, no menu suspenso **Recuperar para uma máquina virtual**, selecione **VirtualBox**.

7 Na página **Virtual Machine Options** (Opções de máquina virtual), selecione **Remote Linux Machine** (Máquina Linux remota).

8 Insira as informações sobre a máquina virtual conforme descrito na tabela a seguir.

Tabela 120. Definições da máquina Linux remota

Opção	Descrição
Nome de host do VirtualBox	Insira um endereço IP ou nome de host para o server VirtualBox. Este campo representa o endereço IP ou nome de host do server VirtualBox remoto.
Port	Insira um número de porta para a máquina. Este número representa a porta através da qual o Core se comunica com esta máquina.
Nome da máquina virtual	Insira um nome para a máquina virtual sendo criada. **NOTA: O nome padrão é o nome da máquina de origem.**
Caminho de destino	Especifique um caminho de destino para criar a máquina virtual. **NOTA: Recomenda-se criar uma pasta raiz a partir da raiz para que a máquina virtual seja executa a partir da raiz. Se você não usar a raiz, será preciso criar uma pasta de destino manualmente na máquina de destino antes de configurar a exportação. Também será preciso conectar ou carregar manualmente a máquina virtual após a exportação.**
Nome de usuário	Nome de usuário da conta na máquina de destino, por exemplo, raiz.
Senha	Senha para a conta de usuário na máquina de destino.
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • Usar a mesma quantidade de RAM da máquina de origem • Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

9 Selecione **Realizar exportação única inicial** para realizar a exportação virtual imediatamente e não após o próximo snapshot programado.

10 Clique em **Avançar**.

11 Na página **Volumes**, selecione os volumes de dados a serem exportados e clique em **Avançar**.

12 Na página **Summary** (Resumo), clique em **Finish** (Concluir) para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Exportar dados para uma máquina virtual VMWare Workstation

No Rapid Recovery, é possível exportar dados para o VMWare Workstation realizando uma exportação única ou estabelecendo uma exportação contínua (para Standby virtual). Execute as etapas dos procedimentos a seguir do tipo apropriado de exportação.

Realizar uma exportação única para VMware Workstation

Execute as etapas deste procedimento para realizar uma exportação única para VMware Workstation.

1 No Console do Rapid Recovery Core, na barra de botões, clique no menu suspenso **Restaurar**, clique em **Exportação do VM**.

2 No Assistente de exportação de máquina virtual, selecione **Exportação única**.

3 Clique em **Avançar**.

4 Na página de Máquinas, selecione a máquina protegida que você deseja exportar.

5 Clique em **Avançar**.

6 Na página Pontos de recuperação, selecione o ponto de recuperação que você deseja exportar.

7 Clique em **Avançar**.

8 Na página Destino do Assistente de exportação, no menu suspenso Recuperar na máquina virtual, selecione **VMware Workstation** e clique em **Avançar**.

9 Na página Opções de máquina virtual, insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir.

Tabela 121. Parâmetros da máquina virtual

Opção	Descrição
Local da máquina de VM	Especifique o caminho da pasta local ou compartilhamento de rede no qual você deseja criar a máquina virtual. **NOTA: Se você especificou um caminho de compartilhamento de rede, será preciso inserir credenciais de login válidas para uma conta que está registrada na máquina de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.**
Nome de usuário	Insira as credenciais de login do local de rede para a exportação. • Se você especificou um caminho de compartilhamento de rede, será preciso inserir um nome de usuário válido para uma conta que está registrada na máquina de destino. • Se você inseriu um caminho local, um nome de usuário não é necessário.
Senha	Insira as credenciais de login do local de rede para a exportação. • Se você especificou um caminho de compartilhamento de rede, será preciso inserir uma senha válida para uma conta que está registrada na máquina de destino. • Se você inseriu um caminho local, uma senha não é necessária.
Nome de VM	Insira um nome para a máquina virtual sendo criada, por exemplo, VM-0A1B2C3D4. **NOTA: O nome padrão é o nome da máquina de origem.**
Versão	Especifique a versão do VMware Workstation da máquina virtual. Você pode selecionar dentre: • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0 • VMware Workstation 11.0 • VMware Workstation 12.0
Quantidade de RAM (MB)	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • Usar a mesma quantidade de RAM da máquina de origem • Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.
Número de processadores	O número de processadores (CPUs) que você quer para a máquina virtual exportada. O valor mínimo é 1.
Cores por processador	O número de cores que você quer ter para cada processador. O valor mínimo é 1.

10 Clique em **Avançar**.

11 Na página Volumes, selecione os volumes para exportar, por exemplo, C:\ e D:\, e clique em **Avançar**.

12 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Realizar uma exportação contínua (Standby virtual) para VMware Workstation

Execute as etapas deste procedimento para realizar a exportação contínua para uma máquina virtual (VM) de área de trabalho do VMWare usando o Rapid Recovery.

1 No Rapid Recovery Core Console, escolha uma das opções a seguir:

- No Core Console, na barra de botões, clique em  menu suspenso **Restaurar** e selecione **Exportação do VM**.
  1 No Assistente de exportação de máquina virtual, selecione **Contínuo (Standby Virtual)**.
  2 Clique em **Avançar.**
- No Core Console, na barra de ícones, clique em  (Standby virtual).
  - Na página **Standby virtual**, clique em **Adicionar** para iniciar o Assistente de exportação de máquina virtual.

2 Na página **Máquinas** do Assistente de exportação de máquina virtual, selecione a máquina protegida que você deseja exportar.

3 Clique em **Avançar**.

4 Na página **Pontos de recuperação**, selecione o ponto de recuperação que você deseja usar para a exportação.

5 Clique em **Avançar**.

6 Na página **Destino** do Assistente de exportação de máquina virtual, no menu suspenso Recuperar para uma máquina virtual, selecione **Área de trabalho do VMWare** e clique em **Avançar**.

7 Na página **Opções de máquina virtual**, insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir.

Tabela 122. Parâmetros da máquina virtual

Opção	Descrição
Caminho de destino	Especifique o caminho da pasta local ou compartilhamento de rede no qual você deseja criar a máquina virtual. **NOTA: Se você especificou um caminho de compartilhamento de rede, será preciso inserir credenciais de login válidas para uma conta que está registrada na máquina de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.**
Nome de usuário	Insira as credenciais de login do local de rede para a exportação. • Se você especificou um caminho de compartilhamento de rede, será preciso inserir um nome de usuário válido para uma conta que está registrada na máquina de destino. • Se você inseriu um caminho local, um nome de usuário não é necessário.
Senha	Insira as credenciais de login do local de rede para a exportação. • Se você especificou um caminho de compartilhamento de rede, será preciso inserir uma senha válida para uma conta que está registrada na máquina de destino. • Se você inseriu um caminho local, uma senha não é necessária.
Máquina virtual	Insira um nome para a máquina virtual sendo criada, por exemplo, VM-0A1B2C3D4. **NOTA: O nome padrão é o nome da máquina de origem.**
Versão	Especifique a versão do VMware Workstation da máquina virtual. Você pode selecionar dentre: • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0 • VMware Workstation 11.0

Opção	Descrição
	• VMware Workstation 12.0
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • Usar a mesma quantidade de RAM da máquina de origem • Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.
Número de processadores	O número de processadores (CPUs) que você deseja para a máquina virtual exportada. O valor mínimo é 1.
Cores por processador	O número de cores que você deseja ter para cada processador. O valor mínimo é 1.

8 Selecione **Realizar exportação única inicial** para realizar a exportação virtual imediatamente e não após o próximo snapshot programado.

9 Clique em **Avançar**.

10 Na página **Volumes**, selecione os volumes para exportar, por exemplo, C:\ e D:\, e clique em **Avançar**.

11 Na página **Summary** (Resumo), clique em **Finish** (Concluir) para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as páginas Standby virtual e Eventos.

Exportar dados para uma máquina virtual Hyper-V

No Rapid Recovery, é possível exportar dados para a Exportação para Hyper-V realizando uma exportação única ou estabelecendo uma exportação contínua (para Standby virtual).

O Rapid Recovery suporta exportação de primeira geração do Hyper-V para os seguintes hosts:

- Windows 8
- Windows 8,1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

O Rapid Recovery suporta exportação de segunda geração do Hyper-V para os seguintes hosts:

- Windows 8,1
- Windows Server 2012 R2

NOTA: Nem todas as máquinas protegidas podem ser exportadas a hosts de segunda geração do Hyper-V.

Somente máquinas protegidas com os seguintes sistemas operacionais da Interface Unificada de Firmware Extensível (UEFI) suportam exportação virtual para hosts de segunda geração do Hyper-V:

- Windows 8 (UEFI)
- Windows 8.1 (UEFI)
- Windows Server 2012 (UEFI)
- Windows Server 2012 R2 (UEFI)

NOTA: A exportação do Hyper-V para VM de segunda geração poderá falhar caso o host do Hyper-V não tenha RAM suficiente alocada para realizar a exportação.

Execute as etapas dos procedimentos a seguir do tipo apropriado de exportação.

Realizar uma exportação única de Hyper-V

Execute as etapas deste procedimento para realizar uma exportação única para o Hyper-V.

1 No Rapid Recovery Core Console, na barra de botões, clique no menu suspenso **Restaurar**, em **Exportação do VM**.
2 No Assistente de exportação de máquina virtual, selecione **Exportação única**.
3 Clique em **Avançar**.
4 Na página **Máquinas**, selecione a máquina protegida que você deseja exportar.
5 Clique em **Avançar**.
6 Na página **Pontos de recuperação**, selecione o ponto de recuperação que você deseja usar na exportação.
7 Clique em **Avançar**.
8 Na página **Destino**, no menu suspenso Exportar para máquina virtual, selecione **Hyper-V**.
9 Para exportar para uma máquina local com a função Hyper-V atribuída, clique em **Usar a máquina local**.
10 Para indicar que o servidor Hyper-V está localizado em uma máquina remota, clique em **Host remoto** e insira as informações do host remoto conforme descrito na tabela a seguir.

Tabela 123. Informações do host remoto

Caixa de texto	Descrição
Nome do host	Insira um endereço IP ou nome de host para o server Hyper-V. Ele representa o endereço IP ou nome de host do server Hyper-V remoto.
Port	Insira um número de porta para a máquina. Ele representa a porta através da qual o Core se comunica com esta máquina.
Nome de usuário	Insira o nome de usuário para o usuário com privilégios administrativos para a estação de trabalho com o server Hyper-V. Ele é usado para especificar as credenciais de login para a máquina virtual.
Senha	Insira a senha da conta de usuário com privilégios administrativos na estação de trabalho com o server Hyper-V. Ele é usado para especificar as credenciais de login para a máquina virtual.

11 Clique em **Avançar**.
12 Na página **Opções de máquinas virtuais**, na caixa de texto **Local da máquina de VM**, insira o caminho da máquina virtual; por exemplo, **D:\export**. Isso é usado para identificar o local da máquina virtual.

NOTA: Você precisa especificar o local da máquina virtual para os servers Hyper-V local e remoto. O caminho precisa ser um caminho de local válido para o server Hyper-V. Diretórios não existentes são automaticamente criados. Você não deve tentar criá-los manualmente. A exportação para pastas compartilhadas (por exemplo, para \\data\share) não é permitida.

13 Na caixa de texto **Nome da máquina virtual**, insira o nome da máquina virtual.
O nome inserido será exibido na lista de máquinas virtuais no console do Hyper-V Manager.
14 Para especificar o uso da memória, clique em um dos seguintes:
- **Usar a mesma quantidade de RAM da máquina de origem**. Selecione essa opção para identificar se o uso da RAM é idêntico entre as máquinas virtuais e de origem.
- **Usar uma quantidade específica de RAM.** Selecione essa opção caso você queira especificar a quantidade de RAM em MB.
A quantidade mínima é 1.024 MB e o máximo permitido pelo aplicativo é 65.536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

15 Para especificar o formato do disco, próximo a Formato do disco, clique em um dos seguintes:
- VHDX
- VHD

NOTA: A exportação do Hyper-V suporta formatos de disco VHDX se a máquina de destino estiver executando o Windows 8 (Windows Server 2012) ou mais recente. Se o formato VHDX não for suportado por seu ambiente, a opção será desativada.

Se desejar exportar para a geração Hyper-V 2, somente o formato de disco VHDX é suportado.

16 Para especificar a geração do Hyper-V a fim de utilizar para exportação, clique em um dos seguintes:

- Geração 1
- Geração 2

NOTA: Somente a geração 2 oferece suporte à opção de inicialização segura.

17 Especifique o adaptador de rede adequado para a VM exportada.

18 Na página **Volumes**, selecione os volumes a serem exportados; por exemplo, C:\.

NOTA: Se os volumes selecionados forem maiores do que as alocações máximas adequadas suportadas pelo aplicativo conforme indicado abaixo, ou exceder a quantidade de espaço disponível, será exibido um erro.

- Para o formato de disco VHDX, seus volumes selecionados não devem ser maiores do que 64 TB.
- Para o formato de disco VHD, seus volumes selecionados não devem ser maiores do que 2040 GB.

19 Na página **Volumes**, clique em **Concluir** para concluir e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação vendo as páginas Standby virtual ou Eventos.

Realizar uma exportação contínua (Standby virtual) para Hyper-V

Conclua as etapas nesse procedimento para realizar uma exportação contínua para uma máquina virtual (VM) Hyper-V usando Rapid Recovery.

1 No Rapid Recovery Core Console, realize um dos procedimentos a seguir:

- No Core Console, na barra de botões, clique na  Menu suspenso **Restaurar** e selecione **Exportação do VM**.
  1 No Assistente de exportação de máquina virtual, selecione **Contínuo (Standby virtual)**.
  2 Clique em **Avançar.**
- No Core Console, na barra de ícones, clique em  (Standby virtual).
  - Na página **Standby virtual**, clique em **Adicionar** para abrir o Assistente de exportação de máquina virtual.

2 Na página **Máquinas** do Assistente de exportação de máquina virtual, selecione a máquina protegida que você deseja exportar.

3 Clique em **Avançar**.

4 Na página **Pontos de recuperação**, selecione o ponto de recuperação que você deseja usar na exportação.

5 Clique em **Avançar**.

6 Na página **Destino**, no menu suspenso Exportar para uma máquina virtual, selecione **Hyper-V** e realize um dos seguintes procedimentos:

- Para exportar para uma máquina local com a função Hyper-V atribuída, clique em **Usar a máquina local**.
- Para indicar que o servidor Hyper-V está localizado em uma máquina remota, clique em **Host remoto** e insira os parâmetros do host remoto conforme descrito na tabela a seguir.

Tabela 124. Informações do host remoto

Caixa de texto	Descrição
Nome do host	Insira um endereço IP ou nome de host para o server Hyper-V. Ele representa o endereço IP ou nome de host do server Hyper-V remoto.
Port	Insira um número de porta para a máquina. Ele representa a porta através da qual o Core se comunica com esta máquina.

Caixa de texto	Descrição
Nome de usuário	Insira o nome de usuário para o usuário com privilégios administrativos para a estação de trabalho com o server Hyper-V. Ele é usado para especificar as credenciais de login para a máquina virtual.
Senha	Insira a senha da conta de usuário com privilégios administrativos na estação de trabalho com o server Hyper-V. Ele é usado para especificar as credenciais de login para a máquina virtual.

7 Clique em **Avançar**.

8 Na página **Opções de máquinas virtuais**, na caixa de texto **Local da máquina de VM**, insira o caminho da máquina virtual; por exemplo, **D:\export**. Isso é usado para identificar o local da máquina virtual.

NOTA: Você precisa especificar o local da máquina virtual para os servers Hyper-V local e remoto. O caminho precisa ser um caminho de local válido para o server Hyper-V. Diretórios não existentes são automaticamente criados. Você não deve tentar criá-los manualmente. A exportação para pastas compartilhadas (por exemplo, para \\data\share) não é permitida.

9 Na caixa de texto **Nome da máquina virtual**, insira o nome da máquina virtual.

O nome inserido será exibido na lista de máquinas virtuais no console do Hyper-V Manager.

10 Para especificar o uso da memória, clique em um dos seguintes:

- **Usar a mesma quantidade de RAM da máquina de origem**. Selecione essa opção para identificar se o uso da RAM é idêntico entre as máquinas virtuais e de origem.
- **Usar uma quantidade específica de RAM.** Selecione essa opção caso você queira especificar a quantidade de RAM em MB.

  A quantidade mínima é 1.024 MB e o máximo permitido pelo aplicativo é 65.536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

11 Para especificar o formato do disco, próximo a Formato do disco, clique em um dos seguintes:

- VHDX
- VHD

NOTA: A exportação do Hyper-V suporta formatos de disco VHDX se a máquina de destino estiver executando o Windows 8 (Windows Server 2012) ou mais recente. Se o formato VHDX não for suportado por seu ambiente, a opção será desativada.

Se desejar exportar para a geração Hyper-V 2, somente o formato de disco VHDX é suportado.

12 Para especificar a geração do Hyper-V a fim de utilizar para exportação, clique em um dos seguintes:

- Geração 1
- Geração 2

NOTA: Somente a geração 2 oferece suporte à opção de inicialização segura.

13 Especifique o adaptador de rede adequado para a VM exportada.

14 Na página **Volumes**, selecione os volumes a serem exportados; por exemplo, C:\.

NOTA: Se os volumes selecionados forem maiores do que as alocações máximas adequadas suportadas pelo aplicativo conforme indicado abaixo, ou exceder a quantidade de espaço disponível, será exibido um erro.

- Para o formato de disco VHDX, seus volumes selecionados não devem ser maiores do que 64 TB.
- Para o formato de disco VHD, seus volumes selecionados não devem ser maiores do que 2040 GB.

15 Selecione **Realizar exportação única inicial** para realizar a exportação virtual imediatamente e não após o próximo snapshot programado.

16 Na página **Volumes**, clique em **Concluir** para concluir e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação vendo as páginas Standby virtual ou Eventos.

Como gerenciar dados de classificação por vencimento

Esta seção descreve como gerenciar dados de instantâneo de classificação por vencimento salvos em seu repositório. Contém informações sobre como reter pontos de recuperação em seu repositório, políticas de retenção e o processo resultante de rollup de pontos

de recuperação para economizar espaço. Descreve a nova capacidade de relocar pontos de recuperação do seu repositório para um dispositivo de backup e eliminação de duplicação DR da Dell.

Esta seção também descreve como arquivar dados para armazenamento a longo prazo não sujeitos ao rollup, e como acessar pontos de recuperação que foram arquivados.

Sobre retenção e arquivamento de dados do Rapid Recovery

Cada vez que o seu Core captura um snaphot, os dados são salvos como um ponto de recuperação em seu repositório. Os pontos de recuperação naturalmente se acumulam com o passar do tempo. O Core usa uma política de retenção para determinar quanto tempo os dados de snapshot ficarão retidos no repositório. Durante o processo de rollup no trabalho noturno, o Core reforça a política de retenção para reduzir a quantidade consumida de espaço de armazenamento. Durante o rollup, a data de cada ponto de recuperação é comparada com a data do ponto de recuperação mais recente. Em seguida, o Core combina ou "realiza o processo de rollup" dos pontos de recuperação mais antigos. Com o passar do tempo, os pontos de recuperação mais antigos são, eventualmente, substituídos por outros mais recentes, considerando que os pontos de recuperação mais antigos "envelhecem" depois do período de retenção mais antigo.

Para manter pontos de recuperação que, de outra forma seriam combinados e, finalmente excluídos, você pode criar um arquivo a partir do Console do Core. Um arquivo contém o conjunto completo de pontos de recuperação para as máquinas protegidas no seu Core, no momento em que foram criados.

Você pode armazenar um arquivo em um sistema de arquivos, ou em uma conta de armazenamento na nuvem.

Se você precisa ter acesso aos dados em um ponto de recuperação, você poderá posteriormente anexar (para Rapid Recovery 6.x e posterior) ou importar o arquivo, restaurando esses pontos de recuperação em seu repositório. Em seguida, você pode realizar as mesmas ações sobre esses dados como com quaisquer outros pontos de recuperação atualmente em seu Core.

NOTA: Desde que o Core reconheça as datas originais dos pontos de recuperação em um arquivo, os pontos de recuperação importados podem ser novamente combinados ou excluídos durante o próximo período de trabalho noturno. Se você quiser manter pontos de recuperação mais antigos, você pode desativar o rollup para as respectivas máquinas, ou você pode aumentar o período de retenção.

Como gerenciar as políticas de retenção

Uma política de retenção é um conjunto de regras que determina o período de tempo para o Núcleo manter pontos de recuperação antes de começar a fusão. As políticas de retenção podem ser definidas para fusão com base em horas, dias, semanas, meses e anos. Você pode definir até seis regras (a política padrão define cinco regras).

Sendo que você pode fazer backup com a frequência de 5 em 5 minutos, a primeira regra da política de retenção normalmente define quanto tempo reter todos os pontos de recuperação. Por exemplo, se você fizer o backup de uma máquina à cada 15 minutos, 96 pontos de recuperação são salvos no repositório para esta máquina por dia, até a fusão iniciar. Sem o gerenciamento da política de retenção, essa quantidade de dados pode rapidamente encher um repositório.

NOTA: Os administradores devem notar que backups frequentes podem ter um impacto sobre o tráfego de rede. Outros fatores que afetam o tráfego de rede incluem outras transferências (como replicação), a taxa de alteração dos seus dados, e o hardware, cabos e os comutadores de rede.

O Núcleo vem pré-ajustado com uma política de retenção padrão. A política padrão mantém:

- Todos os pontos de recuperação por três dias
- Um ponto de recuperação por hora por dois dias
- Um ponto de recuperação por dia para quatro dias
- Um ponto de recuperação por semana por três semanas
- Um ponto de recuperação por mês por dois meses
- Um ponto de recuperação por ano para X anos (desativado na política padrão).

Seguindo esta política padrão, o ponto de recuperação mais antigo é normalmente 92 dias. Dados passados desta data para uma política padrão serão apagados.

Configurar a política de retenção ao nível do núcleo aplica automaticamente a todas as máquinas que o Core protege. Você pode alterar a política padrão para atender às suas necessidades.

Para qualquer máquina, você pode também criar uma política de retenção personalizada. Configurar a política ao nível da máquina permite que você especifique uma política de retenção diferente que não seja o padrão do Core. Para obter mais informações sobre como configurar as políticas de retenção, consulte Como definir as configurações padrão da política de retenção do Núcleo e Como personalizar as configurações de uma política de retenção para uma máquina protegida.

Como definir as configurações padrão da política de retenção do Núcleo

A política de retenção para o Core especifica quanto tempo os pontos de recuperação para uma máquina protegida são armazenados no repositório.

A política de retenção do Núcleo é imposta por um processo de fusão que é executado como um dos componentes dos trabalhos noturnos em execução. Em seguida, os pontos de recuperação para além da idade especificada na política de retenção são "fusionados" (combinados) em menos pontos de recuperação que cobrem um período de tempo granular menor. Aplicar a política de retenção todas as noites resulta na fusão contínua de backups velhos. Isto eventualmente resulta em a exclusão dos pontos de recuperação mais antigos, com base nos requisitos especificados naquela política de retenção.

Diferentes definições de retenção podem ser configuradas para os Núcleos fonte e destino.

NOTA: Este tópico é específico ao personalizar as configurações da política de retenção no Rapid Recovery Core. Quando você salva essas configurações personalizadas no Core, você estabelece as configurações padrão da política de retenção que pode ser aplicada a todas as máquinas protegidas por este núcleo. Para obter mais informações sobre como personalizar as configurações da política para retenção para máquinas protegidas, consulte Como personalizar as configurações de uma política de retenção para uma máquina protegida.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Configurações), e, em seguida, faça o seguinte:

- A partir da lista de Configurações de núcleo no lado esquerdo da página de Configurações, clique em **Nightly Jobs (Trabalhos noturnos)**.
- Role a tela para baixo no lado direito da página de configurações até que você possa ver o título **Nightly Jobs (Trabalhos noturnos)**.

As configurações de núcleo dos Trabalhos noturnos são exibidas.

3 Sob **Nightly Jobs (Trabalhos noturnos)**, clique em  **Change (Alterar)**.

A caixa de diálogo **Nightly Jobs (Tarefas noturnas)** é mostrada.

4 Para especificar os intervalos de tempo para retenção dos dados de backup, conforme necessário, no painel Trabalhos Noturnos, selecione **Rollup (Fusão)**, e, em seguida, clique em **Settings (Configurações)**.

A caixa de diálogo **Configurações** para a política de retenção padrão do Núcleo é exibida.

5 Para restaurar as configurações da política de retenção do Núcleo para os valores padrão a qualquer momento, na parte inferior da caixa de diálogo Configurações, clique em **Restore Defaults (Restaurar padrões)** e, em seguida, clique em **Yes (Sim)** para confirmar.

Todas as configurações são restauradas para os valores padrão descritos na tabela na Etapa 6.

6 Para definir uma política de retenção, primeiro especifique a principal configuração que determina quanto tempo os instantâneos de backup iniciais são mantidos. Em seguida, prossiga para definir requisitos de um conjunto de fusão em cascata que determina os intervalos entre quando os pontos de recuperação devem ser acumulados.

As opções para a política de retenção são descritas na tabela a seguir.

Tabela 125. Opções de programação para política de retenção padrão

Caixa de texto	Descrição
Manter todos os pontos de recuperação para n [período de retenção]	Especifica o período de retenção para os pontos de recuperação. Digite um número que represente o período de retenção e, em seguida, selecione o período. O padrão é 3 dias. Você pode escolher entre: dias, semanas, meses, ou anos
... e, em seguida, manter um ponto de recuperação por hora para n [período de retenção]	Fornece um nível de retenção mais refinado; usado como um bloco de construção com configuração primária para definir mais detalhadamente o tempo pelo qual os pontos de recuperação serão mantidos. Digite um número que represente o período de retenção e, em seguida, selecione o período. O padrão é 2 dias. Você pode escolher entre: dias, semanas, meses, ou anos
... e, em seguida, manter um ponto de recuperação por dia para n [período de retenção]	Fornece um nível de retenção mais refinado; usado como um bloco de construção para definir mais detalhadamente o tempo pelo qual os pontos de recuperação serão mantidos. Digite um número que represente o período de retenção e, em seguida, selecione o período. O padrão é 4 dias. Você pode escolher entre: dias, semanas, meses, ou anos
... e, em seguida, manter um ponto de recuperação por semana para n [período de retenção]	Fornece um nível de retenção mais refinado; usado como um bloco de construção para definir mais detalhadamente o tempo pelo qual os pontos de recuperação serão mantidos. Digite um número que represente o período de retenção e, em seguida, selecione o período. O padrão é 3 semanas. Você pode escolher entre: semanas, meses ou anos
... e, em seguida, manter um ponto de recuperação por mês para n [período de retenção]	Fornece um nível de retenção mais refinado; usado como um bloco de construção para definir mais detalhadamente o tempo pelo qual os pontos de recuperação serão mantidos. Digite um número que represente o período de retenção e, em seguida, selecione o período. O padrão é 2 meses. Você pode escolher entre: meses ou anos
... e, em seguida, manter um ponto de recuperação por ano para n [período de retenção]	Digite um número que represente o período de retenção e, em seguida, selecione o período. Você pode escolher entre: Anos

O ponto de recuperação mais antigo é determinado pelas configurações da política de retenção.

A seguir se encontra um exemplo de como o período de retenção é calculado.

Mantenha todos os pontos de recuperação por três dias.

... e, em seguida, manter um ponto de recuperação por hora por 3 dias

... e, em seguida, manter um ponto de recuperação por dia por 4 dias

... e, em seguida, manter um ponto de recuperação por semana por 3 semanas

... e, em seguida, manter um ponto de recuperação por mês por dois meses

... e, em seguida, manter um ponto de recuperação por mês por um ano

Nesse exemplo, o ponto de recuperação mais antigo seria um ano, 4 meses e 6 dias.

7 Quando estiver satisfeito com as suas configurações da política de retenção , clique em **Save (Salvar)**.

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

8 Na caixa de diálogo **Trabalhos noturnos**, clique em **OK**.

A caixa de diálogo **Trabalhos noturnos** fecha. A política de retenção que você definiu é aplicada durante a fusão noturna.

Você pode também aplicar essas configurações ao especificar a política de retenção para qualquer máquina protegida. Para obter mais informações sobre como configurar as políticas de retenção para uma máquina protegida, consulte Como personalizar as configurações de uma política de retenção para uma máquina protegida.

Como personalizar as configurações de uma política de retenção para uma máquina protegida

A política de retenção para uma máquina protegida especifica quanto tempo os pontos de recuperação são armazenados no repositório. Tipicamente, cada máquina protegida usa a política de retenção padrão estabelecida para o Core, a menos que você especifique uma política de retenção personalizada, conforme descrito neste procedimento.

Use este procedimento para definir uma política de retenção personalizada para uma máquina protegida, incluindo uma máquina replicada.

1 A partir do menu Máquinas protegidas do Rapid Recovery Core Console, clique no nome da máquina que você quer modificar.

A página **Summary (Resumo)** para a seleção da máquina é exibida.

2 Clique no menu **Settings (Configurações)**.

A página **Configurações** é exibida, mostrando as definições de configuração para a máquina selecionada.

3 Opcionalmente, clique no link **Nightly Jobs (Trabalhos noturnos)** para rolar para baixo na página de Configurações para ver todas as configurações para trabalhos noturnos.

4 Sob o título, clique em Trabalhos noturnos, clique  **Change (Alterar)**.

A caixa de diálogo **Nightly Jobs (Tarefas noturnas)** é mostrada.

5 Para especificar os intervalos de tempo para que se possa manter os dados de backup, conforme a necessidade, selecione **Rollup (Fusão)** e, em seguida, clique em **Settings (Configurações)**.

A caixa de diálogo **Configurações** para a política de retenção é exibida.

6 Se personalizar as configurações de políticas de retenção de uma máquina replicada, e se você ver um aviso notificando para realizar uma verificação de integridade em seu repositório, prossiga com esta etapa. Caso contrário, vá para a próxima etapa.

a Se você estiver preparado para executar o trabalho, clique em **Check Integrity (Verificar a integridade)**

b Clique em **Yes (Sim)** para confirmar o trabalho de verificação de integridade.

> **NOTA: Em execução, este trabalho pode levar uma quantidade substancial de tempo, com base no tamanho do seu repositório. Durante este tempo, você pode executar nenhuma outra ações (instantâneos, replicação, exportação virtual, e assim por diante) no repositório. Para obter informações sobre este trabalho, consulte Sobre como verificar a integridade dos repositórios DVM.**

- Uma vez que trabalho de Verificação de integridade concluir todos os trabalho filho com sucesso, retorne a este procedimento e continue com a próxima etapa.

7 Na caixa de diálogo **Configuration (Configuração)**, faça o seguinte:

- Para usar a política de retenção padrão para esta máquina protegida, selecione **Use Core default retention policy (Usar política de retenção padrão do Core)**, e, em seguida, clique em **Save (Salvar)**. A política padrão é aplicada a esse agente.
- Para definir uma política de retenção personalizada para este agente, selecione **Use custom retention policy (Usar política de retenção personalizada)**, e, em seguida, continue com a próxima etapa.

A caixa de diálogo **Configuration (Configuração)** expande-se para mostrar informações da política de retenção.

8 Digite o agendamento personalizado para retenção dos pontos de recuperação, conforme descrito na tabela a seguir.

Tabela 126. Opções de programação para política de retenção personalizada

Caixa de texto	Descrição
Manter todos os pontos de recuperação para n [período de retenção]	Especifica o período de retenção para os pontos de recuperação. Digite um número que represente o período de retenção e, em seguida, selecione o período. O padrão é 3 dias. Você pode escolher entre: dias, semanas, meses, e anos
... e, em seguida, manter um ponto de recuperação por hora para n [período de retenção]	Fornece um nível de retenção mais refinado; usado como um bloco de construção com configuração primária para definir mais detalhadamente o tempo pelo qual os pontos de recuperação serão mantidos. Digite um número que represente o período de retenção e, em seguida, selecione o período. O padrão é 2 dias. Você pode escolher entre: dias, semanas, meses, e anos
... e, em seguida, manter um ponto de recuperação por dia para n [período de retenção]	Fornece um nível de retenção mais refinado; usado como um bloco de construção para definir mais detalhadamente o tempo pelo qual os pontos de recuperação serão mantidos. Digite um número que represente o período de retenção e, em seguida, selecione o período. O padrão é 4 dias. Você pode escolher entre: dias, semanas, meses, e anos
... e, em seguida, manter um ponto de recuperação por semana para n [período de retenção]	Fornece um nível de retenção mais refinado; usado como um bloco de construção para definir mais detalhadamente o tempo pelo qual os pontos de recuperação serão mantidos. Digite um número que represente o período de retenção e, em seguida, selecione o período. O padrão é 3 semanas. Você pode escolher entre: semanas, meses, e anos
... e, em seguida, manter um ponto de recuperação por mês para n [período de retenção]	Fornece um nível de retenção mais refinado; usado como um bloco de construção para definir mais detalhadamente o tempo pelo qual os pontos de recuperação serão mantidos. Digite um número que represente o período de retenção e, em seguida, selecione o período. O padrão é 2 meses. Você pode escolher entre: meses e anos
... e, em seguida, manter um ponto de recuperação por ano para n [período de retenção]	Digite um número que represente o período de retenção e, em seguida, selecione o período. Você pode escolher entre: Anos

A seguir se encontra um exemplo de como o período de retenção é calculado.

Mantenha todos os pontos de recuperação por três dias.

... e, em seguida, manter um ponto de recuperação por hora por 3 dias

... e, em seguida, manter um ponto de recuperação por dia por 4 dias

... e, em seguida, manter um ponto de recuperação por semana por 3 semanas

... e, em seguida, manter um ponto de recuperação por mês por dois meses

... e, em seguida, manter um ponto de recuperação por mês por um ano

Nesse exemplo, o ponto de recuperação mais antigo seria 1 ano, 3 meses.

9 Se você quiser manter todos os pontos de recuperação no seu repositório principal, desmarque a opção **Relocate outdated recovery points to an R3 repository (Relocar pontos de recuperação obsoletos a um repositório R3)** e pule a próxima etapa.

10 Se você quiser relocar pontos de recuperação do seu repositório principal a um repositório R3 armazenado em um dispositivo de backup Dell série DR, faça o seguinte:

   a Selecione a opção **Relocate outdated recovery points to an R3 repository (Relocar pontos de recuperação obsoletos a um repositório R3)** .

   b Especifique a idade na qual você deseja mudar pontos de recuperação do seu repositório principal para o repositório R3.

   Você pode especificar a idade por semanas, meses ou anos. O período mais curto em que você pode definir é 1 semana.

   c Do menu suspenso **Select a repository (Selecione um repositório)**, selecione o repositório R3 para o qual você quer tier os pontos de recuperação especificados.

NOTA: Independentemente do local onde os pontos de recuperação estão localizados (repositório DVM local ou em um repositório remoto R3 em um dispositivo de backup DR), eles ainda estão sujeitos à política de retenção, e ainda serão combinados. Se você precisar manter pontos de recuperação mais antigos, um método consiste em arquivamento. O outro é para desativar a fusão ou ampliar o período de retenção das máquinas protegidas.

11 Clique em **Save (Salvar)**.

Forçar rollup para uma máquina protegida

Você pode ignorar a política de retenção programada, forçando o rollup dos pontos de recuperação no nível da máquina protegida.

1 No menu Máquinas protegidas do Rapid Recovery Core Console, clique no nome de uma máquina protegida específica.

A guia **Resumo** referente à máquina selecionada é exibida.

2 Clique no menu suspenso **Mais** na parte superior da visualização da máquina protegida e selecione **Política de retenção**.

A página **Política de retenção** referente à máquina especificada é exibida.

3 Clique em **Forçar rollup**.

4 Na caixa de diálogo, clique em **Sim** para confirmar.

O Rapid Recovery inicia o rollup para esta máquina independentemente do programa da política de retenção.

Replicação

Este capítulo descreve como configurar e gerenciar a replicação de dados protegidos de um Core de origem do Rapid Recovery para um Core de destino do Rapid Recovery para recuperação após desastres.

Replicação com Rapid Recovery

Esta seção fornece informações conceituais e de procedimentos para ajudá-lo a entender e configurar a replicação no Rapid Recovery.

Replicação é um processo de copiar pontos de recuperação de um Rapid Recovery Core e transmiti-los para outro Rapid Recovery Core visando a recuperação de desastres. O processo exige uma solução com pares de origem/destino entre dois ou mais Cores.

O Core de origem copia os pontos de recuperação de máquinas protegidas selecionadas e então transmite de modo assíncrono e contínuo os dados de snapshot para o Core de destino.

A menos que você a altere o comportamento padrão, definindo um programa de reaplicação, o Core inicia um trabalho de replicação imediatamente após a conclusão de cada snapshot de backup, verificação de soma de verificação, verificação de capacidade de anexação e trabalhos noturnos. Para obter informações, consulte Programar a replicação.

Para obter melhor segurança de dados, os administradores geralmente usam um Core de destino em uma localidade remota de recuperação de desastres. É possível configurar a replicação de saída para um data center de propriedade da empresa ou para uma

localidade remota de recuperação de desastres (ou seja, um Core de destino "autogerenciado"). Ou é possível configurar a replicação de saída para um provedor de serviços gerenciados (MSP) terceirizado ou provedor de nuvem que hospede serviços de recuperação após desastres e cópia de segurança em um site externo. Ao replicar para um Core de destino de terceiros, é possível usar fluxos de trabalho incorporados que permitam solicitar conexões e receber notificações automáticas de feedback.

A replicação é gerenciada por máquina protegida. Qualquer máquina (ou todas as máquinas) protegida ou replicada em um Core de origem pode ser configurada para replicar em um Core de destino.

Os possíveis cenários de replicação incluem:

- **Replicação para uma localização local**. O Core de destino situa-se em um datacenter local ou localização no local e a replicação é sempre mantida. Nessa configuração, a perda do Core não impediria a recuperação.
- **Replicação para uma localização externa**. O Core de destino está localizado em uma instalação de recuperação após desastres externa para recuperação em caso de perda.
- **Replicação mútua**. Dois datacenters em locais diferentes, cada um contendo um Core, protegendo máquinas e atuando mutuamente como cópia de segurança externa para recuperação após desastres. Nesse cenário, cada Core replica as máquinas protegidas do Core localizado no outro datacenter.
- **Replicação hospedada e na nuvem**. Os parceiros MSP do Rapid Recovery mantêm vários Cores de destino em um datacenter ou uma nuvem pública. Em cada um desses Cores, o parceiro MSP permite que um ou mais dos seus clientes replique os pontos de recuperação a partir de um Core de origem no local do cliente para o Core de destino do MSP por uma taxa.

NOTA: Nesse cenário, os clientes têm acesso apenas aos seus próprios dados.

As possíveis configurações de replicação incluem:

- **Replicação ponto-a-ponto**. Replica uma ou mais máquinas protegidas de um único Core de origem para um único Core de destino.

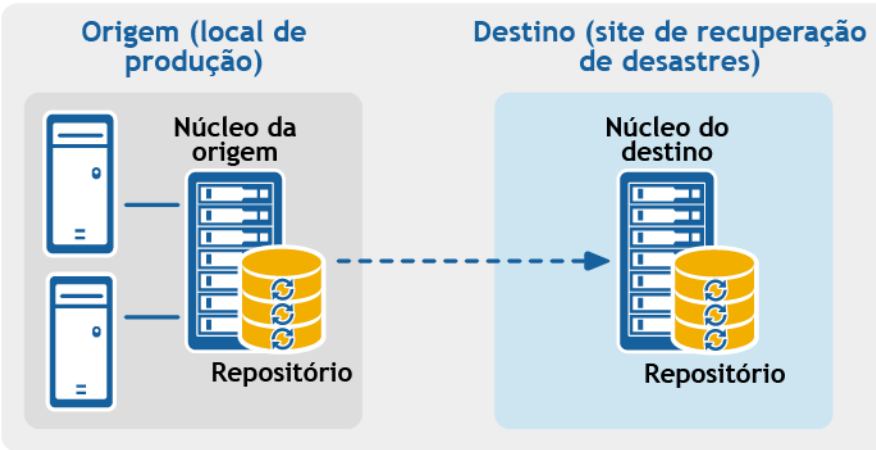


Figura 9. Configuração de replicação ponto-a-ponto

- **Replicação multiponto-a-ponto**. Replica máquinas protegidas de vários Cores de origem para um único Core de destino.

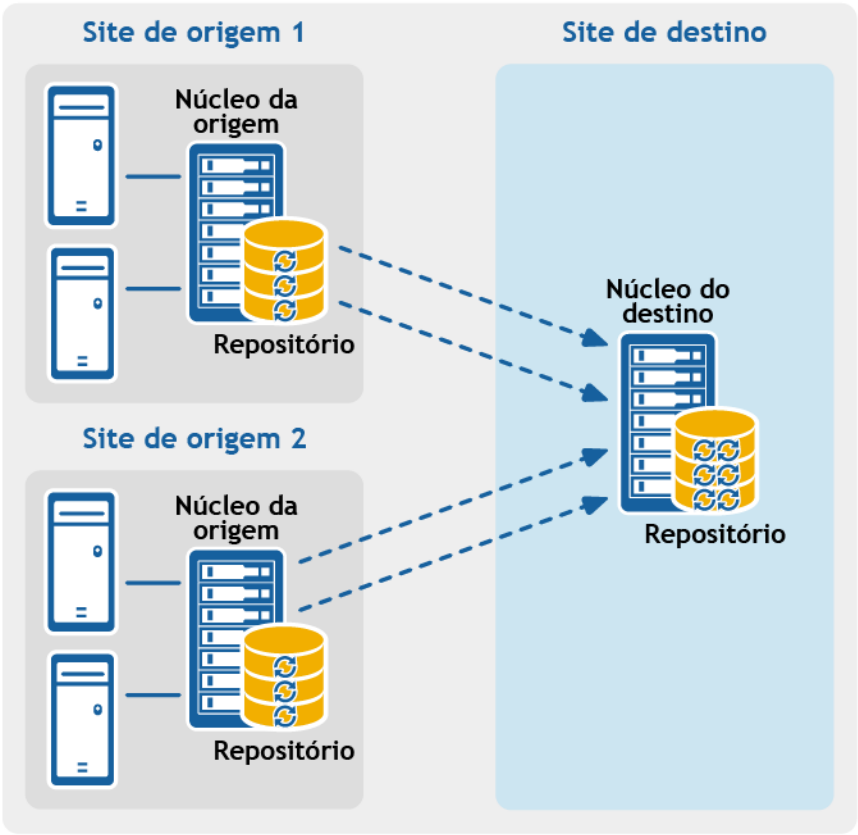


Figura 10. Configuração de replicação de multiponto-a-ponto

- **Replicação de ponto-a-multiponto**. Replica uma ou mais máquinas protegidas de um único Core de origem para mais de um Core de destino.

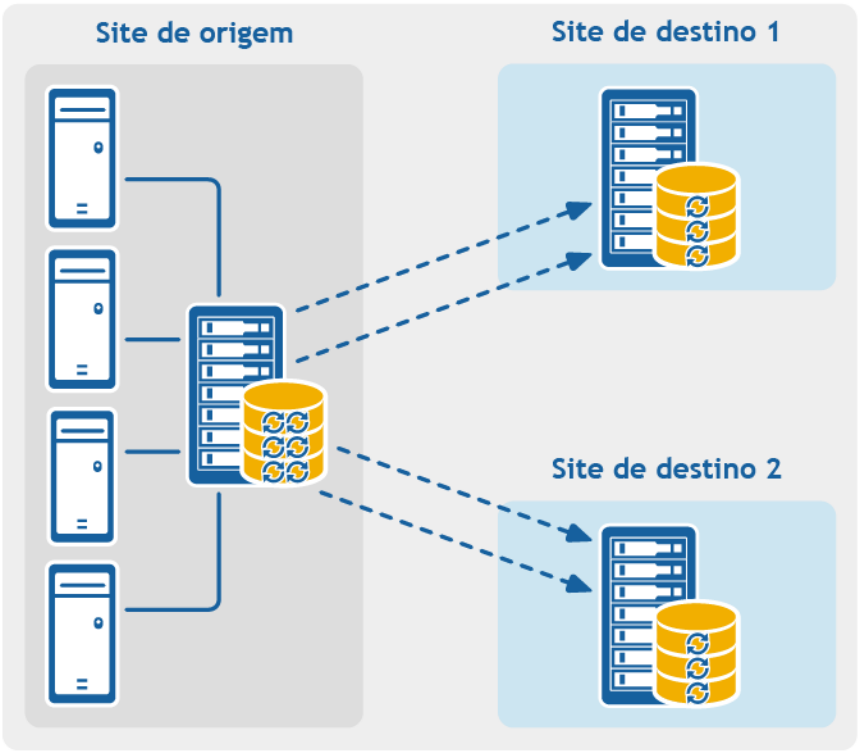


Figura 11. Configuração de replicação ponto-a-multiponto

- **Replicação de saltos múltiplos.** Replica uma ou mais máquinas protegidas de um Core de destino para outro Core de destino, produzindo opções e ativação adicional pós-falha ou recuperação no Core replicado.

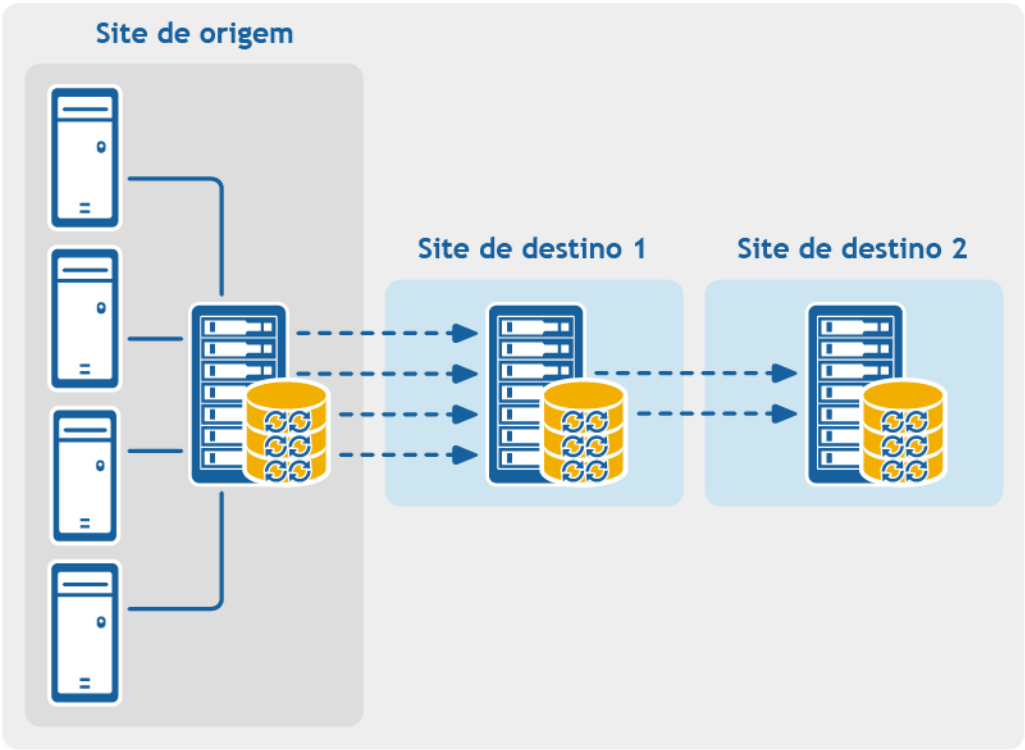


Figura 12. Configuração de replicação de saltos múltiplos

Se o uso dos appliances de backup de proteção de dados Dell como a série DL1x00 ou DL4x00, o Core de destino para o qual você replicar deve ter uma licença de software válida configurada. Esses appliances de hardware incluem uma licença de destino de replicação com a compra. Verifique a chave de licença na mensagem de e-mail de boas-vindas que você recebeu quando adquiriu o appliance. Para obter assistência, visite o site de Assistência à aplicação da licença https://support.software.dell.com/licensing-assistance ou e-mail license@software.dell.com.

Cadeias de pontos de recuperação e órfãos

O Rapid Recovery captura os snapshots de uma máquina protegida e salva os dados em um repositório como um *ponto de recuperação*. O primeiro ponto de recuperação salvo no Core é chamado de *imagem de base*. A imagem de base inclui o sistema operacional, os aplicativos e as configurações para cada volume que você seleciona para proteger, bem como todos os dados nesses volumes. Os backups sucessivos são *snapshots incrementais*, que consistem apenas em dados alterados nos volumes protegidos desde o último backup. A imagem de base e os snapshots incrementais formam uma *cadeia completa de pontos de recuperação*.

A partir de uma cadeia completa de pontos de recuperação, você pode restaurar os dados com facilidade e confiança, usando toda a faixa de opções de recuperação disponíveis para o Rapid Recovery. Essas opções incluem a restauração no nível do arquivo, no nível do volume e bare metal restore.

Uma vez que logicamente não é possível restaurar dados que não existem, no caso de uma cadeia incompleta de pontos de recuperação, você não poderá restaurar os dados no nível do volume ou realizar um bare metal restore. Nesses casos, você ainda poderá restaurar quaisquer dados existentes em um ponto de recuperação no nível do arquivo.

Se a informação que você deseja restaurar de um ponto de recuperação estiver em um backup prévio que não está disponível para o Core (um snapshot incremental ou imagem de base prévio), o ponto de recuperação será considerado *órfão*. Os pontos de recuperação órfãos são típicos em alguns cenários de replicação.

Por exemplo, quando você estabelece a replicação pela primeira vez, as suas opções para restaurar os dados dos pontos de recuperação replicados são limitadas. Até que todos os dados de backup do Core de origem sejam transmitidos ao Core de destino, criando cadeias completas de pontos de recuperação a partir dos órfãos, você pode realizar somente a restauração no nível do arquivo.

Quando a replicação começar

Por padrão, os trabalhos de transferência de replicação são automaticamente colocados em fila pelo Core, imediatamente depois da conclusão de cada transferência do backup programado regularmente. Portanto, a menos que o programa da replicação de uma máquina protegida seja personalizado, ele é baseado no programa padrão do snapshot de backup.

Quando você configurar uma replicação pela primeira vez, se houver um ou mais pontos de recuperação no Core de origem, o processo de replicação começará imediatamente, a menos que:

- Você selecione a opção para pausar a replicação inicialmente ou
- Você selecione a opção para usar uma unidade de seeding para realizar a transferência inicial.

Se você pausar a replicação inicialmente, ela começará quando você retomar a replicação explicitamente.

Se você configurar a replicação e especificar o uso de uma unidade de seeding, a replicação para o Core de destino começará com o próximo snapshot de backup regularmente programado.

NOTA: Você pode também forçar um backup da máquina protegida depois de estabelecer a replicação. Isso faz a replicação começar imediatamente depois que o snapshot da máquina protegida for concluído.

Se você especificar uma unidade de seeding ao configurar uma replicação, somente as futuras transferências de backup serão replicadas. Se você deseja que os pontos de recuperação existentes da máquina protegida original existam no Core de destino, precisará fazer o seeding dos dados da máquina protegida. Para fazer o seeding dos dados, crie uma unidade de seeding do Core de origem e, em seguida, consuma-a no Core de destino.

Você também pode personalizar o programa da replicação para uma máquina protegida. Por exemplo, se você usar o programa de proteção padrão de um backup por hora, poderá especificar que o Core de origem replique para o Core de destino em um programa diferente (por exemplo, uma vez por dia às 2AM).

Determinar suas necessidades e sua estratégia de seeding

Os tópicos a seguir discutem a restauração de dados replicados e se você precisa fazer o seeding dos dados do ponto de recuperação do Core de origem.

Quando o seeding de dados é necessário

Quando você estabelece a replicação pela primeira vez, a menos que especifique o uso de uma unidade de seeding, o Core de origem começa a transmitir todos os pontos de recuperação para as máquinas selecionadas para o Core de destino. A transmissão dos seus dados via rede pode levar um bom tempo. Os fatores envolvidos incluem a velocidade da rede, a robustez da arquitetura da rede e a quantidade de dados a serem transmitidos ao Core de destino. Por exemplo, se os dados de backup do Core de origem medirem 10GB e o link WAN transferir 24Mbps, a transferência pode demorar cerca de uma hora para ser concluída.

Com base na quantidade de informação que você deseja copiar para o Core de destino, a unidade de seeding pode adicionar até centenas ou milhares de gigabytes de dados. Muitas organizações optam por não consumir a largura de banda de rede necessária e, em vez disso, preferem definir e consumir uma unidade de seeding. Para obter mais informações, consulte Considerações sobre desempenho para transferência de dados replicados.

Se você especificar o uso de uma unidade de seeding ao definir a replicação, apenas os pontos de recuperação salvos para o Core de origem *depois* de estabelecer a replicação serão replicados para o Core de destino. Os backups salvos no Core de origem *antes* do

estabelecimento da replicação não estarão presentes no Core de destino até que você faça explicitamente o *seeding* dos dados, usando o processo a seguir.

Para evitar diminuir a velocidade da rede com uma transferência intensiva de dados históricos, faça o seeding dos dados do backup prévio para o Core de destino usando uma **unidade de seeding**. Uma unidade de seeding é um arquivo que **copia** um conjunto de imagens de base desduplicadas e snapshots incrementais do Core de origem. O arquivo da unidade de seeding contém o conjunto completo de pontos de recuperação prévios para as máquinas protegidas que você deseja replicar do Core de origem para o Core de destino.

Mova o arquivo da unidade de seeding para um volume de armazenamento, que depois você disponibiliza para o Core de destino. Em seguida, você **consome** a informação da unidade de seeding. Isso envolve anexar o volume com a imagem da unidade de seeding ao Core de destino e importar os dados para o repositório do Core Console. Esse processo repara os órfãos, unindo os snapshots incrementais replicados no Core de destino com as suas imagens de base para formar uma ou mais cadeias completas de pontos de recuperação. Esse processo é às vezes chamada de copiar-consumir.

O seeding dos dados do seu Core de origem nem sempre é necessário. Por exemplo:

- Se você estiver configurando a replicação para um novo Rapid Recovery Core, o seeding não será necessário.
- Se os dados de snapshots prévios não forem críticos para os seus dados replicados, e você precisa recuperar somente os dados salvos depois da configuração da replicação, o seeding não será necessário.

  NOTA: Nesse caso, a Dell recomenda capturar uma nova imagem de base imediatamente antes ou depois de configurar a replicação. Esta etapa garante a existência de uma cadeia completa de pontos de recuperação no Core de destino, a fim de restaurar dados no futuro.
- Se você capturou uma imagem de base imediatamente antes de configurar a replicação e precisa somente restaurar os dados capturados depois dessa data, o seeding não será necessário.
- Se você configurar a replicação sem especificar uma unidade de seeding, os dados do snapshot são transmitidos via rede do Core de origem para o Core de destino.

Se uma dessas situações aplicar-se a você, o seeding dos dados não será necessário. Nesses casos, a replicação pode ser concluída inteiramente no Core de origem.

Se você configurar a replicação para um Core com pontos de recuperação existentes e precisar restaurar no nível de volume, desejar realizar um BMR ou restaurar os dados de uma imagem de base prévia ou snapshot incremental, o seeding será necessário. Nessas situações, pense nas suas necessidades e na sua estratégia de seeding. Analise as informações sobre esse tópico e decida se fará o seeding para o Core de destino e qual abordagem usará.

Abordagens para o seeding dos dados

Se você deseja que as máquinas replicadas em um Core de destino tenham acesso aos dados salvos previamente no Core de origem, faça o seeding do Core de destino usando uma das seguintes abordagens:

1. **Faça o seeding para o Core de destino via conexão de rede.** Especifique o uso de uma unidade de seeding quando definir a replicação. Em seguida, você pode compartilhar a pasta que contém a unidade de seeding com o Core de destino e consumir o arquivo da unidade de seeding via rede. Para dados grandes ou conexões lentas, esse método de seeding pode levar uma quantidade substancial de tempo e consumir uma largura de banda substancial.

   NOTA: A Dell não recomenda o seeding de grandes quantidades de dados via conexão de rede. O seeding inicial envolve potencialmente quantidades de dados muito grandes, o que pode sobrecarregar uma conexão WAN típica.
2. **Transferir dados de backup do Core de origem usando a mídia de armazenamento físico.** Transfira o arquivo da unidade de seeding para um dispositivo de armazenamento externo removível e portátil. Normalmente, essa abordagem é útil para grandes conjuntos de dados ou sites com conexões de rede lentas. Esse método de seeding exige a realização das seguintes etapas:
   a. Crie um arquivo de seeding do Core de origem, salvando-o na mídia removível.
   b. Transporte a unidade de seeding para o local físico do Core de destino.
   c. Anexe a unidade ao Core de destino.
   d. Consuma os dados da unidade de seeding para o repositório do Core de destino.

Ao replicar para um Core de terceiros, assim que a mídia for recebida pelo MSP, um representante do datacenter normalmente anexa a mídia e avisa-o quando ela estiver pronta para você consumir (ou importar) os dados do seeding para o Core.

NOTA: Uma vez que grandes quantidades de dados precisam ser copiadas para o dispositivo de armazenamento, recomenda-se o uso de uma conexão eSATA, USB 3.0 ou outra de alta velocidade. Se o tamanho total do arquivo de dados de seeding for superior ao espaço disponível na mídia removível, o arquivo pode ocupar vários dispositivos.

3 **Para Cores de origem e de destino armazenados em máquinas virtuais, transfira os dados de backup usando um disco rígido virtual.** Se o Core de origem e de destino estiverem em uma máquina virtual, você poderá definir e consumir uma unidade de seeding na mídia de armazenamento virtual. Esse método de seeding exige a realização das seguintes etapas:

a Crie um arquivo da unidade de seeding do Core de origem, salvando-o em um volume de armazenamento virtual.

b Retire o volume do Core de origem e anexe-o ao Core de destino.

c Consuma os dados da unidade de seeding para o repositório do Core de destino.

NOTA: Embora a replicação de snapshots incrementais possa ocorrer entre os Cores de origem e destino antes do seeding terminar, os snapshots replicados transmitidos da origem para o destino permanecem órfãos até que os dados iniciais sejam consumidos e são combinados com as imagens de base replicadas.

Links relacionados

- Para obter detalhes do processo de consumo da unidade de seeding, consulte o tópico Consumo da unidade de propagação em um Core de destino.
- Para obter mais informações sobre pontos de recuperação órfãos, consulte Excluir uma cadeia de pontos de recuperação órfãos.
- Para obter informações sobre como preparar uma unidade de seeding, consulte Noções gerais sobre unidades de seeding, e Consumo da unidade de seeding em um Core de destino.

Links relacionados

Consumo da unidade de propagação em um Core de destino

Excluir uma cadeia de pontos de recuperação órfãos

Considerações sobre desempenho para transferência de dados replicados

Se a largura da banda entre os Cores de origem e de destino não pode acomodar a transferência de pontos de recuperação armazenados, configure a replicação e especifique o uso de uma unidade de seeding. Este processo propaga o Core de destino com imagens base e pontos de recuperação do servidores selecionados protegidos no Core de origem. O processo de seeding pode ser executado a qualquer momento. Ele pode ser realizado como parte da transferência inicial de dados, que funciona como fundamento para replicações programadas regularmente. Você também pode propagar dados para uma máquina anteriormente replicada se a replicação foi pausada ou apagada. Nesse caso, a opção "Criar cadeias de ponto de recuperação" permitiria copiar os pontos de recuperação ainda não replicados para uma unidade de seeding.

Ao preparar-se para a replicação, considere os seguintes fatores:

- **Taxa de alteração.** A taxa de alteração é a taxa de acumulação da quantidade de dados protegidos. A taxa depende da quantidade de dados alterados em volumes protegidos e do intervalo de proteção dos volumes. Alguns tipos de máquinas normalmente têm uma taxa maior de alteração, como, por exemplo, um e-mail do Exchange server. Uma forma de reduzir a taxa de alteração é reduzir o intervalo de proteção.
- **Largura de banda.** A largura de banda é a velocidade de transferência disponível entre o Core de origem e o de destino. É vital que a largura de banda seja superior à taxa de alteração para que a replicação acompanhe os pontos de recuperação criados pelos snapshots. Devido à quantidade de dados transmitidos de um Core para outro, vários fluxos paralelos podem ser necessários para se obter velocidades por fio de uma conexão Ethernet de 1GB.

NOTA: A largura da banda que os ISPs especificam é tipicamente a largura de banda total disponível. Todos os dispositivos na rede compartilham a largura de banda de saída. Certifique-se de que haja largura de banda livre suficiente para replicação a fim de acomodar a taxa de alteração.

- **Número de máquinas protegidas.** É importante considerar o número de máquinas protegidas pelo Core de origem e quantas você pretende replicar para o Core de destino. Você não precisa replicar cada máquina protegida no Core de origem; o Rapid Recovery permite que você replique por máquina protegida portanto, você pode optar por replicar somente certas máquinas, se quiser. Se todas as máquinas protegidas em um Core de origem precisarem ser replicadas, a taxa de alteração será normalmente mais alta. Este fator é relevante se o largura da banda entre o Core de origem e o de destino não for suficiente para a quantidade e o tamanho dos pontos de recuperação que estão sendo replicados.

A taxa de alteração máxima por tipo de conexão WAN é mostrada na tabela abaixo com exemplos da largura de banda necessária por gigabyte para obter uma taxa de alteração razoável.

Tabela 127. Exemplos de largura de banda por gigabyte

Banda larga	Largura de banda	Taxa de alteração máxima
DSL	768 Kbps ou mais	330MB por hora
Cabo	1 Mbps ou mais	429MB por hora
T1	1,5 Mbps ou mais	644MB por hora
Fibra	20 Mbps ou mais	8,38GB por hora

NOTA: Para obter resultados ideais, siga as recomendações apresentadas na lista na tabela anterior.

Se um link falhar durante a transferência de dados, a replicação é retomada a partir do ponto de falha anterior da transferência (assim que a funcionalidade do link for restaurada).

Dependendo da configuração de rede, a replicação pode ser um processo demorado. Certifique-se de que você tem largura da banda suficiente para acomodar a replicação, outras transferências do Rapid Recovery como backups, e quaisquer outros aplicativos importantes que você precisa executar.

Se você tiver problemas com a transferência de dados pela rede, particularmente para algumas máquinas protegidas ou replicadas, considere ajustar a taxa de transferência de dados para tais máquinas. Para obter mais informações, consulte Sobre como modificar configurações de transferência e Estrangulamento da velocidade de transferência.

Sobre replicação e pontos de recuperação criptografados

Embora a unidade de propagação não contenha cópias de segurança do registro e dos certificados do Core de origem, ela conterá as chaves de criptografia do Core de origem se os pontos de recuperação que estão sendo replicados da origem para o destino estiverem criptografados. Os pontos de recuperação replicados permanecem criptografados depois de transmitidos para o Core de destino. Os proprietários ou administradores do Core de destino precisam da frase de acesso para recuperar os dados criptografados.

Sobre políticas de retenção para replicação

As políticas de retenção nos Cores de origem e de destino não são sincronizadas. Rollup e exclusão sob demanda são executadas de forma independente em cada Core na ação inicial, bem como durante os trabalhos noturnos.

Para obter mais informações sobre as políticas de retenção, consulteComo gerenciar as políticas de retenção.

Replicação para um core de destino autogerenciado

Essa configuração se aplica à replicação para um local externo e para a replicação mútua. As etapas a seguir são um pré-requisito:

- O Core Rapid Recovery deve estar instalado em todas as máquinas de origem e destino.

- Se estiver configurando o Rapid Recovery para replicação de múltiplos pontos para um ponto, você precisar realizar essa tarefa em todos os cores de origem e um core de destino. Para obter descrições dessas configurações de replicação, consulte Replicação .
- Se precisar criar uma unidade de propagação e transferi-la para um volume físico de armazenamento removível para realizar a transferência inicial de pontos de recuperação existentes, você deve ter um dispositivo de armazenamento portátil e adequado preparado. Você também deve ter acesso físico à máquina do core de origem para conectar a unidade a fim de copiar o arquivo da unidade de propagação.
- Se estiver usando uma unidade de propagação em um core de destino autogerenciado, você ou um administrador de confiança devem ter acesso físico ao core de destino.

Um core de destino autogerenciado é aquele ao qual você tem acesso. Por exemplo, um core autogerenciado é muitas vezes gerenciado por sua empresa em um local externo, ou está hospedado em um local geograficamente diferente do que o core de origem. A replicação pode ser configurada totalmente no core de origem, exceto caso você opte por propagar seus dados usando uma unidade de propagação. Em tais casos, você deve criar uma unidade de propagação usando esse procedimento e conectar posteriormente a unidade de propagação ao core de destino para consumir os dados de ponto de recuperação arquivados. Para obter mais informações, consulte Determinar suas necessidades e sua estratégia de seeding.

Realize as etapas no procedimento a seguir para configurar seu core de origem para replicar um core de destino autogerenciado.

1 Navegue até o Core Console do Rapid Recovery do core de origem.

2 Na barra de botões, clique em **Replicar**.

O **assistente Replication (Replicação)** é mostrado.

3 Na página **Target Core (Core de destino)** do assistente de replicação, se estiver definindo uma replicação com um core de destino que foi emparelhado com esse core de origem anteriormente, selecione **Use an existing target Core (Usar um core de destino existente)** e depois selecione o core de destino adequado na lista suspensa. Pule para a etapa 5.

4 Na página **Target Core (Core de destino)** do assistente de replicação, se estiver definindo uma replicação com um core de destino a partir deste core de origem pela primeira vez, selecione **I have my own Target Core (Tenho meu próprio core)** e depois insira as informações como descrito na tabela a seguir.

Tabela 128. Informações de core de destino

Caixa de texto	Descrição
Host Name (Nome de host)	Digite o nome do host ou o endereço IP da máquina de núcleo à qual você está replicando.
Port (Porta)	Insira o número da porta através da qual o Rapid Recovery Core vai se comunicar com a máquina. O número de porta padrão é 8006.
User Name (Nome de usuário)	Digite o nome do usuário para acessar a máquina.
Password (Senha)	Digite a senha para acessar a máquina.

5 Clique em **Avançar**.

NOTA: Se não houver nenhum repositório no core de destino, é mostrado um aviso notificando você que é possível emparelhar o core de origem com o core de destino, mas que você não pode replicar agentes (máquinas protegidas) para esse local até um repositório ser estabelecido. Para obter informações sobre como configurar um repositório a um core, consulte Como criar um repositório DVM.

6 Na página **Request (Solicitação)**, insira um nome para essa configuração de replicação; por exemplo CoreOrigem1. Esse é o nome de exibição usado para o painel Incoming Replication (Replicação de entrada) na página Replication (Replicação) do core de destino.

7 Clique em **Avançar**.

8 Na página **Protected Machines (Máquinas protegidas)**, selecione os agentes que você deseja replicar e, em seguida, use as listas suspensas na coluna Repository (Repositório) para selecionar um repositório para cada máquina protegida.

9 Se você quiser executar o processo de propagação para a transferência de dados da base, execute as seguintes etapas:

NOTA: Devido às enormes quantidades de dados que precisam ser copiadas para o dispositivo de armazenamento portátil, a Dell recomenda uma conexão eSATA, USB 3.0 ou outra conexão de alta velocidade ao dispositivo portátil de armazenamento.

a Na página **Protected Machines (Máquinas protegidas)** do assistente de replicação, selecione **Use a seed drive to perform the initial transfer (Usar uma unidade de propagação para realizar a transferência inicial)**.
   - Se você possui atualmente uma ou mais máquinas protegidas replicando para um core de destino, é possível incluí-las na unidade de propagação selecionando a opção **Include already replicated recovery points in the seed drive (Incluir pontos de recuperação já replicados na unidade de propagação)**.

b Clique em **Avançar**.

c Na página **Seed Drive Location (Local da unidade de propagação)** do assistente de replicação, use a lista suspensa **Location type (Tipo de local)** para selecionar entre os seguintes tipos de destino:
   - Local
   - Rede
   - Cloud (Nuvem)

d Digite os detalhes do arquivo de unidade de propagação conforme descrito na tabela a seguir com base no tipo de local selecionado na Etapa c.

Tabela 129. Detalhes de arquivamento

Opção	Caixa de texto	Descrição
Local	Output location (Local de saída)	Digite o local para a saída. É usado para definir o caminho do local onde você quer salvar o arquivamento de unidade de propagação; por exemplo, D:\work\archive.
Rede	Output location (Local de saída)	Digite o local para a saída. É usado para definir o caminho do local onde você quer salvar o arquivamento de unidade de propagação; por exemplo, \\servername\sharename.
	User Name (Nome de usuário)	Digite um nome de usuário. Ele será usado para determinar as credenciais de login para o compartilhamento de rede.
	Password (Senha)	Digite uma senha para o caminho de rede. Ela será usada para determinar as credenciais de login para o compartilhamento de rede.
Cloud (Nuvem)	Account (Conta)	Selecione uma conta na lista suspensa. **NOTA: Para selecionar uma conta na nuvem, você deve adicioná-la no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.**
	Container (Contêiner)	Selecione no menu suspenso um contêiner associado à sua conta.
	Folder Name (Nome da pasta)	Digite um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é Rapid-Recovery-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

e Clique em **Avançar**.

f Na página **Seed Drive Options (Opções de unidade de propagação)** do assistente de replicação, digite as informações como descrito na tabela a seguir.

Tabela 130. Opções de unidade de propagação

Item	Descrição
Maximum Size (Tamanho máximo)	Arquivos de dados grandes podem ser divididos em múltiplos segmentos. Selecione o tamanho máximo do segmento que você deseja reservar para criar a unidade de propagação executando uma das opções a seguir:

Item	Descrição
	• Selecione **Entire Target (Todo o destino)** para reservar todo o espaço disponível no caminho fornecido na página de local de unidade de propagação para uso futuro (por exemplo, se o local for **D:\work\archive**, todo o espaço disponível na unidade D: é reservado caso seja necessário para copiar a unidade de propagação, mas não é reservado imediatamente após iniciar o processo de cópia). • Selecione a caixa de texto, digite o valor e, em seguida, selecione uma unidade de medida na lista suspensa para personalizar o espaço máximo que você deseja reservar. O padrão é de 250 MB.
Recycle action (Ação de reciclagem)	Caso o caminho já contenha uma unidade de propagação, selecione uma das opções a seguir: • **Do not reuse (Não reutilizar)**. Não substitui nem apaga os dados de propagação existentes do local. Se o local não estiver vazio, agravação da unidade de propagação vai falhar. • **Replace this Core (Substituir este núcleo)**. Substitui todos os dados arquivados de propagação pertencentes a este núcleo, mas deixa intactos os dados de outros núcleos. • **Erase completely (Apagar completamente)**. Apaga todos os dados de propagação do diretório antes de gravar na unidade de propagação.
Comment (Comentário)	Insira um comentário que descreva a unidade de propagação.
Adicionar todos os agentes à unidade de propagação	Selecione esta opção para replicar todas as máquinas protegidas no código de origem usando a unidade de propagação. Essa opção é selecionada por padrão.
Desenvolver cadeias de ponto de recuperação (corrigir pontos órfãos)	Selecione esta opção para replicar toda cadeia de ponto de recuperação para a unidade de propagação. Essa opção é selecionada por padrão. **NOTA: A propagação típica no AppAssure 5.4 replicava apenas o ponto de recuperação mais recente para a unidade de propagação, o que reduzia a quantidade de tempo e espaço necessária para criara unidade de propagação. Optar por desenvolver cadeias de ponto de recuperação (RP) para a unidade de propagação exige espaço suficiente na unidade de propagação para armazenar os pontos de recuperação mais recentes dos agentes especificados e pode levar tempo adicional para concluir a tarefa.**

g Faça um dos seguintes:

- Se você desmarcou a caixa de seleção **Add all Agents to Seed Drive (Adicionar todos os agentes à unidade de propagação)**, clique em **Next (Avançar)**.
- Se você selecionou **Add all Agents to Seed Drive (Adicionar todos os agentes à unidade de propagação)**, prossiga para a etapa 10.

h Na página **Protected Machines (Máquinas protegidas)** do assistente de replicação, selecione as máquinas protegidas que você deseja replicar no core de destino usando a unidade de propagação.

10 Clique em **Concluir**.

11 Caso você tenha criado uma unidade de propagação, envie-a para o core de destino.

O emparelhamento entre core de origem e de destino está completo.

Exceto caso você tenha selecionado a opção para pausar inicialmente a replicação, o processo de replicação começa imediatamente.

1 Se você selecionou a opção para usar uma unidade de propagação, a replicação produz pontos de recuperação órfãos no core de destino até a unidade de propagação ser consumida e fornece as imagens de base necessárias.

2 Se você especificou o uso de uma unidade, transfira o arquivo da unidade de propagação para um volume (pasta compartilhada, disco virtual ou mídia de armazenamento removível). Em seguida, consuma a unidade de propagação.

Ver a replicação de entrada e saída

Se você clicar no ícone **Replicação**  da barra de ícones, a página **Replicação** é exibida. Essa página fornece noções básicas sobre a replicação, no escopo deste Core. Ela inclui dois painéis:

- O painel **Replicação de saída** lista as máquinas protegidas neste Core que são replicadas em outro Core.
- O painel **Replicação de entrada** lista as máquinas replicadas neste Core e o Core de origem do qual essas máquinas são replicadas.

Esta seção descreve as informações mostradas nesses painéis.

As informações sobre a replicação de saída deste Rapid Recovery Core são descritas na tabela a seguir.

Tabela 131. Informações sobre a replicação de saída

Elemento de UI	Descrição
Selecione o item	Para cada linha na tabela do resumo, você pode marcar a caixa de seleção para realizar as ações da lista de opções de menu acima da tabela.
Tipo	Mostra o tipo de máquina. Você pode expandir um Core de destino para mostrar máquinas replicadas individuais.
Indicador de status	Status da replicação. Círculos coloridos na coluna Status mostram se uma máquina replicada está online ou inacessível. Quando você passa o cursor sobre o círculo colorido, a condição de status é exibida. As condições de status são verde (replicação estabelecida e online), amarelo (replicação pausada), vermelho (erro de autenticação) e cinza (offline ou inacessível).
Nome da replicação	O nome de exibição da máquina do Core para a qual as máquinas deste Core de origem serão replicadas.
Máquinas	Lista o número de máquinas replicadas no Core de destino selecionado.
Sincronizar	A data e a hora da última transferência de replicação para o Core de destino.
	Quando você clica no menu suspenso de ações nessa coluna, visualiza uma lista de ações que afetam a relação da replicação específica.

Você pode realizar ações em dois ou mais Cores de destino listados na grade de Replicação de saída. Para realizar ações em vários Cores de destino, marque a caixa de seleção de cada Core na grade e, no menu acima da grade, selecione a ação que deseja realizar. Você pode realizar as ações descritas na tabela a seguir.

Tabela 132. Ações globais disponíveis no painel Replicação de saída

Elemento de UI	Descrição
Adicionar Core de destino	Permite definir outro Core de destino para as máquinas replicadas protegidas neste Core de origem.
Atualizar	Atualiza as informações mostradas na tabela.
Force	Força a replicação.
Pause	Pausa a replicação estabelecida.
Resume	Retoma a replicação pausada.
Copy	Abre o assistente de replicação, permitindo copiar os pontos de recuperação existentes para as máquinas protegidas selecionadas para uma unidade de seeding.

Elemento de UI	Descrição
Excluir	Exclui a replicação de saída.
Unidades de seeding	Essa opção de menu aparece se os dados foram copiados para uma unidade de seeding ao configurar a replicação. Exibe informações sobre o arquivo de unidade de seeding, incluindo os dados e a hora em que a unidade foi salva. Menus minimizáveis indicam o Core de destino e as máquinas protegidas das quais os arquivos da unidade de seeding foram gerados.
	Quando você clica no menu suspenso de ações nessa coluna, visualiza uma lista de ações que afetam a relação da replicação específica.

As informações sobre a replicação de entrada de outro Core são descritas na tabela a seguir.

Tabela 133. Informações sobre a replicação de entrada

Elemento de UI	Descrição
Selecione o item	Para cada linha na tabela do resumo, você pode marcar a caixa de seleção para realizar as ações da lista de opções de menu acima da tabela.
Tipo	Mostra o tipo de máquina. Você pode expandir um Core de origem para mostrar máquinas replicadas individuais.
Indicador de status	Status da replicação. Círculos coloridos na coluna Status mostram se uma máquina replicada está online ou inacessível. Quando você passa o cursor sobre o círculo colorido, a condição de status é exibida. As condições de status são verde (replicação estabelecida e online), amarelo (replicação pausada), vermelho (erro de autenticação) e cinza (offline ou inacessível).
Nome da replicação	O nome de exibição da máquina do Core de origem que contém as máquinas protegidas que são replicadas neste Core de destino. Esse nome também pode ser especificado ao estabelecer a replicação no Core de origem usando o Assistente de replicação.
Máquinas	Lista o número de máquinas protegidas no Core de origem que são replicadas para este Core de destino.
Sincronizar	A data e a hora da última transferência de replicação do Core de origem.
	Quando você clica no menu suspenso de ações nessa coluna, visualiza uma lista de ações que afetam a relação da replicação específica.

Você pode realizar ações em dois ou mais Cores de origens listados na grade de Replicação de entrada. Para realizar ações em vários Cores de origem, marque a caixa de seleção de cada Core na grade e, no menu acima da grade, selecione a ação que deseja realizar. Você pode realizar as ações descritas na tabela a seguir.

Tabela 134. Ações globais disponíveis no painel Replicação de entrada

Elemento de UI	Descrição
Atualizar	Atualiza as informações mostradas na tabela.
Force	Força a replicação.
Pause	Pausa a replicação estabelecida.
Resume	Retoma a replicação pausada.
Excluir	Exclui a replicação de entrada.

Como configurar a replicação

Para replicar dados usando o Rapid Recovery, você precisa configurar os núcleos de origem e destino para replicação. Depois de configurar a replicação, você pode replicar os dados da máquina protegida, monitorar e gerenciar a replicação e realizar a recuperação.

A replicação no Rapid Recovery envolve as seguintes operações:

- Configurar um repositório no núcleo de destino. Para obter mais informações sobre como adicionar um repositório ao núcleo de destino, consulte Como criar um repositório DVM.
- Configurar replicação auto-gerenciada. Para obter mais informações sobre replicação para um núcleo de destino auto-gerenciado, consulte Replicação para um core de destino autogerenciado.
- Configurar replicação de terceiros. Para obter mais informações sobre replicação à um núcleo de destino de terceiro, consulte Replicar para um Core de destino de terceiros.
- Replicar uma máquina protegida existente. Para obter mais informações sobre replicação de uma máquina que já é protegida pelo núcleo de fonte, consulte Adicionar uma máquina a uma replicação existente.
- Consumir a propagação de sementes. Para obter mais informações sobre a propagação de sementes dos dados da unidade no núcleo de destino, consulte Consumo da unidade de propagação em um Core de destino.
- Defina a prioridade de replicação para uma máquina protegida. Para obter mais informações sobre como priorizar a replicação de máquinas protegidas, consulte Definir a prioridade de replicação de uma máquina protegida.
- Defina uma programação de replicação para uma máquina protegida. Para obter mais informações sobre a definição de uma programação de replicação, consulte Programar a replicação.
- Monitorar a replicação conforme necessário. Para obter mais informações sobre como monitorar a replicação, consulte Ver a replicação de entrada e saída.
- Gerenciar configurações de replicação conforme necessário. Para obter mais informações sobre como gerenciar configurações de replicação, consulte Gerenciar definições de replicação.
- Recuperar dados replicados no caso de desastre ou perda de dados.Para obter mais informações sobre como recuperar dados replicados, consulte Recuperar dados replicados.

Replicar para um Core de destino de terceiros

Um Core de terceiros é um Core de destino gerenciado e mantido por um MSP. Replicar em um Core gerenciado por terceiros não exige que o cliente tenha acesso ao Core de destino.

O processo de replicação em um Core de terceiros envolve tarefas que devem ser executadas pelo cliente, bem como por terceiros. Depois de o cliente enviar uma solicitação de replicação no(s) Core(s) de origem, o MSP deve concluir a configuração do Core de destino, revisando a solicitação.

NOTA: Essa configuração se aplica a replicação hospedada e na nuvem. O Rapid Recovery Core deve ser instalado em todas as máquinas do Core de origem. Se estiver configurando o Rapid Recovery para a replicação Multiponto a ponto, você precisará realizar essa tarefa em todos os Cores de origem.

Para replicar em um Core de destino gerenciado por terceiros, execute as seguintes tarefas:

- Enviar uma solicitação de replicação para um provedor de serviços terceirizado
- Revisar uma solicitação de replicação de um cliente
- Ignorar uma solicitação de replicação de um cliente

Enviar uma solicitação de replicação para um provedor de serviços terceirizado

Se você for um usuário final que assina um core gerenciado por terceiros, como um MSP, execute as etapas deste procedimento para enviar uma solicitação de replicação ao seu provedor de serviços de terceiros.

1 Navegue até o Rapid Recovery Core.

2 Na barra de botões do ícone, clique em **Replicar**.

O **Assistente de replicação** é exibido.

3 Na página **Core de destino** do Assistente de replicação, selecione **Eu possuo uma assinatura com um terceiro que oferece cópia de segurança em outro local e serviços de recuperação de desastres** e, em seguida, insira as informações conforme descrito na tabela a seguir.

Tabela 135. Informações sobre o Core de destino de terceiros

Caixa de texto	Descrição
Nome do host	Insira o nome de host, endereço IP ou FQDN da máquina de core de terceiros.
Port	Insira o número da porta lhe foi fornecido pelo seu provedor de serviços de terceiros. O número de porta padrão é 8006.

- Se o Core que você deseja adicionar foi emparelhado com este core de origem anteriormente, você pode fazer o seguinte:
  1 Selecione **Usar um core de destino existente**.
  2 Selecione o core de destino na lista suspensa.
  3 Clique em **Avançar**.
  4 Pule para a Etapa 7.

4 Clique em **Avançar**.

5 Na página **Solicitação** do Assistente de replicação, insira as informações conforme descrito na tabela a seguir.

Tabela 136. Detalhes do Core de destino de terceiros

Caixa de texto	Descrição
Endereço de e-mail	Insira o endereço de e-mail associado à sua assinatura de serviço de terceiros.
ID do cliente (opcional)	Como opção, insira o ID do cliente que foi atribuído a você pelo provedor de serviços.

6 Clique em **Avançar**.

7 Na página **Máquinas protegidas** do Assistente de replicação, selecione as máquinas protegidas que deseja replicar no Core de terceiros.

8 Se desejar realizar o processo de propagação para a transferência dos dados de base, execute as seguintes etapas.

NOTA: Como grandes quantidades de dados precisam ser copiadas para o dispositivo de armazenamento portátil, recomenda-se o uso de uma conexão eSATA, USB 3.0 ou outra de alta velocidade com o dispositivo.

a Na página **Máquinas protegidas** do Assistente de replicação, selecione **Usar uma unidade de seeding para realizar a transferência inicial**.

- Se já tiver uma ou mais máquinas protegidas replicando para um Core de destino, você poderá incluí-las na unidade de propagação selecionando a opção **Incluir os pontos de recuperação já replicados na unidade de seeding**.

b Clique em **Avançar**.

c Na página **Local da unidade de seeding** do Assistente de replicação, use a lista suspensa do tipo de **Local** para selecionar entre os seguintes tipos de destino:

- Local
- Rede
- Nuvem

d Digite os detalhes para o arquivamento conforme descrito na tabela a seguir com base no tipo de local selecionado na Etapa c.

Tabela 137. Detalhes do arquivo

Opção	Caixa de texto	Descrição
Local	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo da unidade de seeding resida, por exemplo, **D:\work\archive**.
Rede	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, **\\servername\sharename**.
	Nome de usuário	Insira um nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira uma senha para o caminho de rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA: Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.**
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é Rapid-Recovery-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

e Clique em **Avançar**.

f Na página **Opções da unidade de seeding** do Assistente de replicação, insira as informações conforme descrito na tabela a seguir.

Tabela 138. Opções da unidade de propagação

Item	Descrição
Tamanho máximo	Grandes arquivos de dados podem ser divididos em vários segmentos. Selecione a quantidade máxima de espaço que você deseja reservar para criar a unidade de seeding efetuando uma das seguintes ações: • Selecione **Destino inteiro** para reservar todo o espaço disponível no caminho fornecido na página Local da unidade de seeding (por exemplo, se o local for D:\work\archive, todo o espaço disponível na unidade D: será reservado). • Selecione a caixa de texto em branco, insira uma quantidade e depois selecione uma unidade de medida na lista suspensa para personalizar o espaço máximo que você deseja reservar.
Reciclar ação	Caso o caminho já tenha uma unidade de seeding, selecione uma das seguintes opções: • **Não reutilizar**. Não substituir ou apagar quaisquer dados de propagação existentes no local. Se o local não estiver vazio, a gravação da unidade de seeding falhará. • **Substituir este Core**. Substitui quaisquer dados de propagação preexistentes pertencentes a este core, porém deixando os dados de outros cores intactos. • **Apagar completamente**. Apaga todos os dados do diretório antes de gravar a unidade de seeding.
Comentários	Insira um comentário descrevendo a unidade de seeding.

Item	Descrição
Adicionar todos os agentes à unidade de seeding	Selecione essa opção para replicar todas as máquinas protegidas no Core de origem usando a unidade de propagação. Esta opção é selecionada por padrão.
Criar cadeias de pontos de recuperação (corrigir órfãos)	Selecione esta opção para replicar toda a cadeia do ponto de recuperação na unidade de seeding. Esta opção é selecionada por padrão. **NOTA: O seeding típico no AppAssure 5.4 replicava apenas o último ponto de recuperação na unidade de seeding, o que reduzia a quantidade de tempo e espaço necessária para a criação da unidade de seeding. A opção de criar cadeias de ponto de recuperação (RP) na unidade de propagação exige espaço suficiente na unidade para armazenar os últimos pontos de recuperação das máquinas protegidas especificadas e pode aumentar o tempo necessário para concluir a tarefa.**

g Realize um dos procedimentos a seguir:

- Se você tiver desmarcado a caixa de seleção **Adicionar todos os agentes à unidade de seeding**, clique em **Avançar**.
- Se você selecionou **Adicionar todos os agentes à unidade de seeding**, vá para a Etapa 9.

h Na página **Máquinas** do Assistente de replicação, selecione as máquinas protegidas que você deseja replicar no Core de destino usando a unidade de propagação.

9 Clique em **Concluir**.

10 Se tiver criado uma unidade de seeding, envie-a conforme indicado pelo seu provedor de serviços de terceiros.

Revisar uma solicitação de replicação de um cliente

Depois que um usuário final concluir o procedimento Enviar uma solicitação de replicação para um provedor de serviços terceirizado, uma solicitação de replicação será enviada do core de origem para o core de destino de terceiros. Como terceiro, você pode revisar a solicitação e aprová-la para começar a replicação para seu cliente, ou pode negá-la para impedir que a replicação ocorra.

Escolha entre as opções a seguir:

- Aprovar uma solicitação de replicação
- Negar uma solicitação de replicação

Aprovar uma solicitação de replicação

Execute o procedimento a seguir para aprovar uma solicitação de replicação em um core de destino de terceiros.

1 No Core de destino, navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Replicação).

A página **Replicação** é exibida.

3 Na página **Replicação**, clique em **Solicitar (#)**.

A seção **Pending Replication Requests** (Solicitações de replicação pendentes) é mostrada.

4 Em Solicitações de replicação pendentes, clique no menu suspenso ao lado da solicitação que deseja revisar e depois clique em **Revisar**.

A janela **Revisar solicitações de replicação** é exibida.

NOTA: As informações que aparecem na seção Identidade do core de origem dessa janela são determinadas pela solicitação executada pelo cliente.

5 Em Identidade do core de origem, realize um dos procedimentos a seguir:

- Selecione **Replace an existing replicated Core** (Substituir um núcleo replicado existente) e, em seguida, selecione um núcleo na lista suspensa.

- Selecione **Criar um novo Core de origem** e confirme se o Nome do Core, Endereço de e-mail do cliente e ID do cliente fornecidos estão corretos. Edite as informações conforme necessário.

6 Em Agentes, selecione as máquinas às quais se aplica a aprovação e use as listas suspensas na coluna Repositório para selecionar o repositório apropriado a cada máquina.

7 Como opção, na caixa de texto **Comentários** insira uma descrição ou mensagem para ser incluída na resposta ao cliente.

8 Clique em **Enviar resposta**.

A replicação é aceita.

Negar uma solicitação de replicação

Execute as etapas do procedimento a seguir para negar uma solicitação de replicação enviada a um core de terceiros a partir de um cliente.

Para negar uma solicitação sem revisá-la, consulte Ignorar uma solicitação de replicação de um cliente.

1 No Core de destino, navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Replicação).

A página **Replicação** é exibida.

3 Na página **Replicação**, clique em **Solicitar (#)**.

A seção **Pending Replication Requests** (Solicitações de replicação pendentes) é mostrada.

4 Em Solicitações de replicação pendentes, clique no menu suspenso ao lado da solicitação que deseja revisar e depois clique em **Revisar**.

A janela **Revisar solicitações de replicação** é exibida.

5 Clique em **Negar**.

A replicação é negada. A notificação de negação é exibida sob Alertas na página Eventos do Core de origem.

Ignorar uma solicitação de replicação de um cliente

Como prestador de serviço de terceiros de um core de destino, você tem a opção de ignorar uma solicitação de replicação enviada por um cliente. Essa opção pode ser usada se a solicitação tiver sido enviada por engano ou se você quiser negar uma solicitação sem revisá-la.

Para obter mais informações sobre solicitações de replicação, consulte Revisar uma solicitação de replicação de um cliente.

Execute o procedimento a seguir para ignorar uma solicitação de replicação de um cliente.

1 No Core de destino, navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Replicação).

A página **Replicação** é exibida.

3 Na página **Replicação**, clique em **Solicitar (#)**.

A seção **Pending Replication Requests** (Solicitações de replicação pendentes) é mostrada.

4 Em Solicitações de replicação pendentes, clique no menu suspenso ao lado da solicitação que deseja ignorar e depois clique em **Ignorar**.

5 Na caixa de diálogo **Ignorando solicitação**, clique em **Sim** para confirmar o comando.

Uma notificação de que a solicitação foi ignorada é enviada ao Core de origem, e a solicitação é removida da página Replicação no Core de destino.

Adicionar uma máquina a uma replicação existente

Após o estabelecimento da replicação entre um Core de origem e um de destino, é possível adicionar novas máquinas protegidas para replicação no destino. Conclua as etapas do procedimento a seguir no Core de origem para adicionar uma nova máquina protegida a um Core de destino pareado para replicação.

Para obter mais informações sobre a replicação, consulte Replicação e Replicação para um core de destino autogerenciado.

1 Navegue até o Console do Rapid Recovery Core do Core de origem.

2 Na barra de botões, clique em  **Replicar**.

O Assistente de replicação é aberto na página **Máquinas protegidas**.

3 Na página **Máquinas protegidas**, selecione as máquinas protegidas que deseja replicar e use as listas suspensas na coluna Repositório para selecionar um repositório para cada máquina protegida.

4 Se desejar realizar o processo de propagação para a transferência dos dados de base, execute as seguintes etapas:

NOTA: Como grandes quantidades de dados precisam ser copiadas para o dispositivo de armazenamento portátil, recomenda-se o uso de uma conexão eSATA, USB 3.0 ou outra de alta velocidade com o dispositivo.

a Na página **Máquinas protegidas** do Assistente de replicação, selecione **Usar uma unidade de seeding para realizar a transferência inicial**.

- Se já tiver uma ou mais máquinas protegidas replicando para um Core de destino, você poderá incluí-las na unidade de seeding selecionando a opção **Incluir os pontos de recuperação já replicados na unidade de propagação**.

b Clique em **Avançar**.

c Na página **Local da unidade de seeding** do assistente, use a lista suspensa do tipo de **Local** para selecionar entre os seguintes tipos de destino:

- Local
- Rede
- Nuvem

d Digite os detalhes para o arquivamento conforme descrito na tabela a seguir com base no tipo de local selecionado na Etapa c.

Tabela 139. Detalhes do arquivo

Opção	Caixa de texto	Descrição
Local	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, d:\work\archive.
Rede	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, \\servername \sharename.
	Nome de usuário	Insira um nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira uma senha para o caminho de rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA: Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter informações, consulte Adicionar uma conta de nuvem.**
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.

Opção	Caixa de texto	Descrição
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é Rapid-Recovery-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

e Clique em **Avançar**.

f Na página **Opções da unidade de seeding** do assistente, insira as informações conforme descrito na tabela a seguir.

Tabela 140. Opções da unidade de propagação

Item	Descrição
Tamanho máximo	Grandes arquivos de dados podem ser divididos em vários segmentos. Selecione a quantidade máxima de espaço que você deseja reservar para criar a unidade de seeding efetuando uma das seguintes ações: • Selecione **Destino inteiro** para reservar todo o espaço disponível no caminho fornecido na página Local da unidade de seeding (por exemplo, se o local for D:\work\archive, todo o espaço disponível na unidade D: será reservado). • Selecione a caixa de texto em branco, insira uma quantidade e depois selecione uma unidade de medida na lista suspensa para personalizar o espaço máximo que você deseja reservar.
Reciclar ação	Caso o caminho já tenha uma unidade de seeding, selecione uma das seguintes opções: • Não reutilizar. Não substituir ou apagar quaisquer dados de propagação existentes no local. Se o local não estiver vazio, a gravação da unidade de seeding falhará. • Substituir este Core. Substitui quaisquer dados de propagação preexistentes pertencentes a este core, porém deixando os dados de outros cores intactos. • Apagar completamente. Apaga todos os dados do diretório antes de gravar a unidade de seeding.
Comentários	Insira um comentário descrevendo a unidade de seeding.
Adicionar todos os agentes à unidade de seeding	Selecione essa opção para replicar todas as máquinas protegidas no Core de origem usando a unidade de propagação. Esta opção é selecionada por padrão.
Construir cadeias de pontos de recuperação (corrigir órfãos)	Selecione esta opção para replicar toda a cadeia do ponto de recuperação na unidade de seeding. Esta opção é selecionada por padrão. **NOTA: A propagação típica no Rapid Recovery 5.4 replica apenas o último ponto de recuperação na unidade de seeding, o que reduz a quantidade de tempo e espaço necessária para a criação da unidade de seeding. A opção de criar cadeias de ponto de recuperação (RP) na unidade de propagação exige espaço suficiente na unidade para armazenar os últimos pontos de recuperação das máquinas protegidas especificadas e pode aumentar o tempo necessário para concluir a tarefa.**

g Realize um dos procedimentos a seguir:

- Se você tiver desmarcado a caixa de seleção **Adicionar todos os agentes à unidade de seeding**, clique em **Avançar**.
- Se tiver selecionado **Adicionar todos os agentes à unidade de seeding**, vá para a Etapa 5.

h Na página **Máquinas protegidas** do assistente, selecione as máquinas protegidas que você deseja replicar no Core de destino usando a unidade de seeding.

5 Clique em **Concluir**.

Consumo da unidade de propagação em um Core de destino

Execute o procedimento a seguir para consumir os dados do arquivo da unidade de propagação no Core de destino.

NOTA: Esse procedimento será necessário apenas se um arquivo da unidade de propagação tiver sido criado como parte de Replicação para um core de destino autogerenciado ou Replicar para um Core de destino de terceiros.

1 Se a unidade de propagação tiver sido salva em um dispositivo de armazenamento portátil, como uma unidade USB, conecte a unidade ao Core de destino.

2 No Core de destino, abra o Rapid Recovery Core Console e na barra de ícones, clique em  (Replicação).

A página **Replicação** é exibida.

3 Na página **Replicação**, em Replicação de entrada, clique no menu suspenso do Core de origem correto e selecione **Consumir**.

A caixa de diálogo **Consumir** é exibida.

4 No campo **Tipo de local**, selecione uma das seguintes opções a partir da lista suspensa:

- Local
- Rede
- Nuvem

5 Insira os detalhes do arquivo para arquivamento da unidade de propagação, como descrito na tabela, com base no tipo de local selecionado na Etapa 4.

Tabela 141. Detalhes do arquivo

Opção	Caixa de texto	Descrição
Local	Local	Insira o caminho para o arquivo.
Rede	Local	Insira o caminho para o arquivo.
	Nome de usuário	Insira o nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira a senha para o caminho da rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA: Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.**
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira o nome da pasta na qual os dados arquivos estão salvos; por exemplo Rapid-Recovery-Arquivo-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

6 Clique em **Verificar arquivo**.

O Core procura o arquivo.

Depois de encontrar o arquivo, as seguintes caixas de texto serão exibidas na janela Consumir, pré-preenchidas com os dados coletados na Etapa 4, Etapa 5 e no arquivo. O Período exibe as datas dos pontos de recuperação mais antigos e mais novos contidos na unidade de seeding. Qualquer comentário inserido quando a unidade de seeding foi criada é importado automaticamente.

7 Na caixa de diálogo **Consumir**, em Agentes, selecione as máquinas em relação às quais você deseja consumir os dados.

8 Clique em **Consumir**.

9 Para monitorar o progresso do consumo de dados, clique na página  Eventos.

Abandonar uma unidade de propagação

Se você for criar uma unidade de seeding com o intuito de consumi-la no Core de destino, mas posteriormente optar por não consumi-la, você pode abandonar a unidade de seeding.

Até que você abandone a unidade de seeding ou a consuma, um link para a unidade de seeding pendente permanecerá no painel de Replicação de saída no Core de origem.

Até que você transmita informações da unidade de seeding, os pontos de recuperação órfãos (que existem na máquina original protegida, mas não no Core de destino) não podem ser usados para restaurar dados.

CUIDADO: Se você abandonar a unidade de seeding, os pontos originais de recuperação (definidos no arquivo da unidade de seeding) serão transmitidos pela rede para o Core de destino durante o próximo trabalho de replicação. A transmissão de antigos pontos de recuperação pela rede poderá reduzir consideravelmente a velocidade da rede, especialmente se houver muitos pontos de recuperação.

Execute as etapas do procedimento a seguir para abandonar uma unidade de seeding pendente.

NOTA: Abandonar a unidade de seeding no Console do Core não afeta o arquivo da unidade de seeding em seu local de armazenamento.

1. No Core de origem, abra o Console do Rapid Recovery Core, e na barra de ícones, clique em (Replicação).
   A página **Replicação** será exibida.
2. Na página **Replicação**, no painel Replicação de saída, clique em **Unidades de seeding (#)**.
   No painel Replicação de saída, uma seção será exibida contendo informações sobre as unidades de seeding pendentes.
3. Opcionalmente, clique na seta virada para baixo para expandir o menu minimizado.
   As informações sobre as unidade de seeding pendentes, incluindo o Core de destino e o período dos pontos de recuperação incluídos na unidade de seeding.
4. Clique em para abrir o menu suspenso para o arquivo da unidade de seeding que você deseja abandonar e depois selecione **Abandonar**.
5. Na janela de confirmação, confirme que você quer abandonar a unidade de seeding.
   A unidade de seeding é removida.

   Se não houver mais unidades de seeding no Core de origem, o link Unidades de seeding (#) e a seção Unidades de seeding pendentes serão removidos do painel Replicação de saída.

Gerenciar definições de replicação

O Rapid Recovery permite monitorar, programar e ajustar a replicação nos níveis global, de Core e de máquina protegida.

É possível editar as seguintes definições de replicação:

- Para programar trabalhos de replicação, consulteProgramar a replicação.
- Para criar uma unidade de propagação de uma máquina protegida que já está pareada para replicação, consulte Usar a função Copiar para criar uma unidade de propagação
- Para monitorar o progresso de um trabalho de replicação, consulteVer a replicação de entrada e saída.
- Para pausar ou retomar um trabalho de replicação em pausa, consultePausar e retomar a replicação.
- Para forçar a replicação de uma máquina protegida de entrada ou saída, consulteForçar a replicação.
- Para gerenciar as definições de todos os cores de destino e procedimentos de replicação, consulte Gerenciar definições para replicação de saída.
- Para gerenciar as definições de um core de destino individual, consulteAlterar configurações de Core de destino.
- Para gerenciar as definições de prioridade de uma máquina protegida individual que está sendo replicada para um Core de destino, consulteDefinir a prioridade de replicação de uma máquina protegida.

Programar a replicação

A menos que você altere o comportamento padrão definindo um programa de replicação, o Core iniciará um trabalho de replicação imediatamente depois da conclusão de cada snapshot de backup, verificação de soma de verificação, verificação de capacidade de anexação e dos trabalhos noturnos. Para obter mais informações, consulte Programar a replicação.

Você pode alterar o programa da replicação para reduzir a carga da rede.

Conclua as etapas do procedimento a seguir para definir um programa de replicação para qualquer máquina replicada.

1 No Core de destino, abra o Rapid Recovery Core Console e na barra de ícones, clique em (Replicação).

A página **Replicação** é mostrada.

2 No painel Replicação de saída, clique em para abrir o menu suspenso ao lado do Core para o qual deseja programar uma replicação e selecione **Programar**.

A caixa de diálogo **Programa de replicação para [NomeCore]** é aberta.

3 Selecione uma das três opções a seguir:

- **A todo o momento**. Replica após cada novo snapshot, verificação de soma de verificação e verificação de capacidade de anexação, e depois da conclusão de trabalhos noturnos.
- **Diário (Iniciar replicação somente durante o período de tempo especificado)**. Começa a replicar apenas dentro do intervalo de tempo fornecido.
  1 Na caixa de texto **De**, digite o primeiro horário em que a replicação deve começar.
  2 Na caixa de texto **A**, digite o último horário em que a replicação deve começar.

  NOTA: Se a replicação estiver em andamento quando terminar o tempo programado, o trabalho de replicação é concluído depois do período de tempo alocado.
- **Personalizado**. Começa replicar somente dentro do período fornecido, permitindo definir um período para os dias da semana e outro para os fins de semana.
  1 Ao lado de Dias da semana, na caixa de texto **De**, insira o primeiro horário em que a replicação deve ocorrer em um dia da semana. Depois, na caixa de texto **A**, insira o último horário em que a replicação deve ocorrer em um dia da semana.
  2 Ao lado de Fins de semana, na caixa de texto **De**, insira o primeiro horário em que a replicação deve ocorrer em fins de semana. Depois, na caixa de texto **A**, insira o último horário em que a replicação deve ocorrer em fins de semana.

4 Clique em **Salvar**.

O programa é aplicado a todas as replicações do Core de destino selecionado.

Usar a função Copiar para criar uma unidade de propagação

Caso tenha optado por não criar uma unidade de propagação ao configurar a replicação, você pode criar uma unidade de propagação usando a função Copiar no menu suspenso da máquina protegida.

1 No Core de origem, abra o Rapid Recovery Core Console e na barra de ícones, clique em (Replicação).

A página **Replicação** é mostrada.

2 Na página **Replicação**, no painel Replicação de saída, clique em para expandir o Core que protege a máquina para a qual você deseja criar uma unidade de seeding.

A seleção expande-se para mostrar cada máquina protegida no Core especificado.

3 Clique na primeira linha da tabela para selecionar cada máquina para a qual deseja criar uma unidade de seeding.

4 No menu sob o painel Replicação de Saída, clique em **Copiar**.

O **Assistente de replicação** é exibido.

5 Na página **Local da unidade de seeding** do assistente, use a lista suspensa **Local** para selecionar entre os seguintes tipos de destino:

- Local

- Rede
- Nuvem

6 Digite os detalhes do arquivo da unidade de seeding conforme descrito na tabela a seguir, com base no tipo de local selecionado na etapa prévia.

Tabela 142. Detalhes do arquivo

Opção	Caixa de texto	Descrição
Local	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, d:\work\archive.
Rede	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, \\servername\sharename.
	Nome de usuário	Insira um nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira uma senha para o caminho de rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA: Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta de nuvem.**
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é Rapid-Recovery-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

7 Clique em **Avançar**.

8 Na página Opções da unidade de seeding, insira as informações conforme descrito na tabela a seguir.

Tabela 143. Opções da unidade de propagação

Item	Descrição
Tamanho máximo	Grandes arquivos de dados podem ser divididos em vários segmentos. Selecione a quantidade máxima de espaço que você deseja reservar para criar a unidade de seeding efetuando uma das seguintes ações: • Selecione **Destino inteiro** para reservar todo o espaço disponível no caminho fornecido na página Local da unidade de seeding (por exemplo, se o local for D:\work\archive, todo o espaço disponível na unidade D: será reservado). • Selecione a caixa de texto em branco, insira uma quantidade e depois selecione uma unidade de medida na lista suspensa para personalizar o espaço máximo que você deseja reservar.
Reciclar ação	Caso o caminho já tenha uma unidade de seeding, selecione uma das seguintes opções: • **Não reutilizar.** Não substituir ou apagar quaisquer dados de propagação existentes no local. Se o local não estiver vazio, a gravação da unidade de seeding falhará. • **Substituir este Core**. Substitui quaisquer dados de propagação preexistentes pertencentes a este core, porém deixando os dados de outros cores intactos. • **Apagar completamente**. Apaga todos os dados do diretório antes de gravar a unidade de seeding.
Comentários	Insira um comentário descrevendo a unidade de seeding.
Adicionar todos os agentes à unidade de seeding	Selecione essa opção para replicar todas as máquinas protegidas no Core de origem usando a unidade de propagação. Esta opção é selecionada por padrão.

Item	Descrição
Criar cadeias de pontos de recuperação (corrigir órfãos)	Selecione esta opção para replicar toda a cadeia do ponto de recuperação na unidade de seeding. Esta opção é selecionada por padrão. **NOTA: O seeding típico no Rapid Recovery 5.4.x replicava somente o último ponto de recuperação para a unidade de seeding, o que reduzia o tempo e a quantidade de espaço necessários para criar a unidade de seeding. A opção de criar cadeias de ponto de recuperação na unidade de seeding exige espaço suficiente na unidade para armazenar os últimos pontos de recuperação das máquinas protegidas especificadas e pode aumentar o tempo necessário para concluir a tarefa.**

9 Realize um dos procedimentos a seguir:

- Se você tiver desmarcado a caixa de seleção **Adicionar todos os agentes à unidade de seeding**, clique em **Avançar**.
- Se você selecionou **Adicionar todos os agentes à unidade de seeding**, vá para a Etapa 10.

10 Na página **Máquinas protegidas** do assistente, selecione as máquinas protegidas para as quais deseja criar uma unidade de seeding.

11 Clique em **Concluir**.

Monitorar a replicação

Quando a replicação estiver configurada, você poderá monitorar o status das tarefas de replicação para os Cores de origem e destino. É possível atualizar as informações de status, visualizar detalhes de replicação, e muito mais.

1 No Core de origem, abra o Rapid Recovery Core Console e, na barra de ícones, clique em  (Replicação).
A página **Replicação** é exibida.

2 Nessa página, você pode ver informações e monitorar o status das tarefas de replicação conforme descrito na seguinte tabela.

Tabela 144. Tarefas de replicação

Seção	Descrição	Ações disponíveis
Unidades de propagação (#)	Depois de especificar o uso de uma unidades de propagação ao definir a replicação, um link de **Unidades de propagação (#)** será exibido no painel de Replicação de saída no Core de origem até você abandonar ou consumir a unidade. O número exibido indica quantas unidades de propagação estão pendentes. **NOTA: Esse link não será exibido a menos que uma unidade de propagação esteja pendente.** Clique nesse link para listar as unidades de propagação que foram gravadas, mas que ainda não consumidas pelo Core de destino. Ainda, expanda o menu que pode ser minimizado para exibir informações sobre unidades de propagação pendentes, incluindo o Core de destino e a faixa de data dos pontos de recuperação incluídos na unidade de propagação.	Na tarefa suspensa, clique em **Abandonar** para abandonar ou cancelar o processo de propagação. menu wn
Replicação de saída	Lista todos os Cores de destino em relação aos quais o Core de origem está replicando. Inclui um indicador de estado, o nome do Core de destino, o número de máquinas sendo replicadas e o progresso de uma transmissão de replicação.	Em um Core de origem, no menu suspenso  , você pode selecionar as seguintes opções: • **Detalhes.**Lista ID, URL, nome de exibição, estado, ID do cliente, endereço de e-mail e comentários do Core replicado.

Seção	Descrição	Ações disponíveis
		· **Alterar definições.** Lista o nome de exibição e permite editar o host e a porta do Core de destino. · **Programar.** Permite definir um programa personalizado para replicação nesse Core de destino. · **Adicionar máquinas.** Permite selecionar um host em uma lista suspensa, selecionar máquinas protegidas para replicação e criar uma unidade de propagação para a transferência inicial da nova máquina protegida. Opcionalmente, você pode incluir pontos de recuperação para máquinas já adicionada à replicação. · **Excluir.** Permite excluir a relação de replicação entre os Cores de origem e destino. Isso anulará toda a replicação nesse Core.
Replicação de entrada	Relaciona todas as máquinas de origem a partir das quais o destino recebe os dados replicados. Inclui o nome do Core remoto, estado, máquinas e progresso. Lista todos os Cores de origem partir dos quais o destino recebe os dados replicados. O nome de exibição dos Cores de origem listados é preenchido a partir do valor no Assistente de replicação ao definir a replicação. Inclui um indicador de estado, o nome do Core remoto e o progresso de uma transmissão de replicação.	Em um Core de destino, no menu suspenso  , você pode selecionar as seguintes opções: · **Detalhes.** Lista o ID, nome de host, ID do cliente, endereço de e-mail e comentário do Core replicado. · **Consumir.** Consome os dados iniciais da unidade de seeding e os salva no repositório local. · **Excluir.** Permite excluir a relação de replicação entre os Cores de origem e destino. Isso anulará toda a replicação a partir desse Core.
Solicitações de replicação pendentes	Essas informações são aplicadas somente a provedores de serviços gerenciados. Quando um cliente clica no link **Solicitações** no painel de Replicação de entrada, uma seção de tabela de resumo é exibida, listando o ID do cliente, endereço de e-mail e nome de host da solicitação.	No menu suspenso, clique em **Ignorar** para ignorar ou rejeitar a solicitação ou em **Revisar** para revisar a solicitação pendente.

Pausar e retomar a replicação

É possível pausar a replicação temporariamente para os Cores de origem (saída) ou de destino (entrada).

A opção para pausar a replicação só está disponível quando a replicação estiver ativa. A opção para retomar a replicação só está disponível se a replicação estiver pausado.

Execute as etapas do procedimento a seguir para pausar ou retomar a replicação.

1 Abra o Console do Rapid Recovery Core, e a partir da barra de ícones, clique em  (Replicação).
A página **Replicação** será exibida.

2 Para pausar a replicação para todas as máquinas replicadas, faça o seguinte:
   a Clique na caixa de seleção na parte superior da tabela de resumo para selecionar o Core de origem ou de destino.
   b Clique em **Pausar** no menu anterior ao da tabela de resumo.
   A replicação para todas as máquinas protegidas no Core selecionado será pausada.

3 Para pausar a replicação apenas para determinadas máquinas, faça o seguinte:
   a Clique em ▼ seta à direita de qualquer Core.

A vista expande-se para mostrar cada uma das máquinas protegidas do Core selecionado que estão sendo replicadas.

b Clique na primeira coluna para selecionar cada máquina para a qual você quer pausar a replicação. Clique em qualquer seleção novamente para limpar a caixa de seleção para as máquinas que você não quer pausar.

c Clique em **Pausar** no menu anterior ao da tabela de resumo.

A replicação para as máquinas protegidas selecionadas será pausada.

4 Para retomar a replicação para todas as máquinas replicadas, faça o seguinte:

a Clique na caixa de seleção na parte superior da tabela de resumo para selecionar o Core de origem ou de destino.

b Clique em **Retomar** no menu na parte superior da tabela de resumo.

A replicação para todas as máquinas protegidas no Core selecionado será retomada.

5 Para retomar a replicação apenas para determinadas máquinas, faça o seguinte:

a Clique em ▼ seta à direita de qualquer Core.

A vista expande-se para mostrar cada uma das máquinas protegidas do Core selecionado que estão sendo replicadas.

b Clique na primeira coluna para selecionar cada máquina para a qual você quer retomar a replicação. Clique em qualquer seleção novamente para limpar a caixa de seleção para as máquinas que você não quer retomar.

c Clique em **Retomar** no menu na parte superior da tabela de resumo.

A replicação para as máquinas protegidas selecionadas será retomada.

Forçar a replicação

A partir do Core de origem, você pode forçar a replicação a qualquer momento, em vez de aguardar por um trabalho de replicação na fila após um evento específico, como um backup ou verificação de capacidade de anexação.

Execute as etapas do procedimento a seguir para forçar a replicação a partir do Core de origem ou de destino.

1 No Core de origem, abra o Console do Rapid Recovery Core, e na barra de ícones, clique em (Replicação).

A página **Replicação** será exibida.

2 Realize um dos procedimentos a seguir:

- Para forçar a replicação em um Core de origem, no painel **Replicação de saída**, selecione um Core e no menu na parte superior da tabela de resumo, clique em **Forçar**.
- Para forçar a replicação em um Core de destino, no painel **Replicação de entrada**, selecione um Core e no menu na parte superior da tabela de resumo, clique em **Forçar**.

A caixa de diálogo Forçar replicação será exibida.

3 Opcionalmente, se você quiser reparar qualquer cadeia de pontos de recuperação definida como órfã, selecione **restaurar apenas cadeias de Ponto de recuperação órfãs**.

4 Para confirmar, na caixa de diálogo Forçar replicação, clique em **(Sim)**.

A caixa de diálogo é fechada e a replicação é forçada.

Gerenciar definições para replicação de saída

As alterações feitas nessas definições afetam a transferência de dados para todos os Cores de destino associados a esse Core de origem.

1 No Core de origem, abra o Rapid Recovery Core Console e, na barra de ícones, clique em (Replicação).

A página **Replicação** é exibida.

2 No painel **Replicação de saída**, na parte superior da tabela de resumo, clique em (Configurações).

A caixa de diálogo **Definições de replicação** é exibida.

3 Na caixa de diálogo **Definições de replicação**, edite as definições de replicação, como descrito na tabela a seguir.

Tabela 145. Definições de replicação

Opção	Descrição
Duração do cache (segundos)	Especificar a quantidade de tempo entre cada solicitação de status de Core de destino feita pelo Core de origem.
Tempo limite da sessão de imagem do volume (minutos)	Especificar a quantidade de tempo que o Core de origem gasta tentando transferir uma imagem de volume para o Core de destino.
Máximo de fluxos paralelos	Especificar o número de conexões de rede com uso simultâneo permitido por uma única máquina protegida para replicar os dados dessa máquina.
Velocidade máxima de transferência (MB/s)	Especificar o limite de velocidade para a transferência de dados replicados.
Tamanho máximo de transferência de dados (GB)	Especifique o tamanho máximo em GB para transferência de blocos de dados replicados.
Restore Defaults	Selecione essa opção para alterar todas as definições de replicação para o padrão do sistema. **NOTA: Tome nota de quaisquer configurações personalizadas antes de selecionar essa opção. Você não será solicitado a confirmar essa ação**

4 Quando estiver satisfeito, clique em **Salvar** para salvar as definições de replicação e fechar a caixa de diálogo.

Alterar configurações de Core de destino

Você pode alterar as configurações de host e porta para Cores de destino individuais a partir do Core de origem.

1 No Core de origem, abra o Rapid Recovery Core Console e, na barra de ícones, clique em (Replicação).
A página **Replicação** é exibida.

No painel **Replicação de saída**, a tabela de resumo inclui uma linha para cada Core de destino que foi configurado para replicar os pontos de recuperação a partir desse Core de origem.

2 Clique no menu suspenso (Configurações) do Core de destino que deseja modificar e selecione **Alterar definições**.
A caixa de diálogo **Configurações** é exibida.

3 Edite uma das opções descritas na tabela a seguir.

Tabela 146. Configurações de Core de destino

Opção	Descrição
Host	Insira o host do Core de destino.
Port	Insira uma porta para que o Core de destino use para comunicação com o Core de origem. **NOTA: A porta padrão é 8006.**

4 Clique em **Salvar**.

Definir a prioridade de replicação de uma máquina protegida

A prioridade da replicação determina quais trabalhos de replicação serão enviados para o Core em primeiro lugar. A priorização é definida ordenadamente, em uma escala de 1 a 10 na qual 1 é a primeira prioridade e 10 é a última prioridade. Quando você estabelece a replicação

pela primeira vez para qualquer máquina, a sua prioridade é definida como 5. Você pode visualizar e alterar a prioridade no nível da máquina protegida no Core de origem.

Em alguns casos, é possível que alguns trabalhos de replicação sejam abandonados. Por exemplo, os trabalhos de replicação podem ser abandonados se o seu ambiente estiver enfrentando altas taxas incomuns de alteração ou se a rede não tiver largura de banda suficiente. Essa situação é particularmente provável se você definir os programas que limitam as horas em que a replicação ocorre no seu ambiente. Para obter mais informações sobre como definir a replicação programada, consulte Programar a replicação.

Para garantir que a replicação ocorra primeiro para as máquinas importantes, defina a prioridade dos servidores críticos com um menor número (entre 1 e 5). Defina a prioridade das máquinas menos importantes com um número maior (entre 6 e 10).

A definição da prioridade da replicação como 4 para qualquer máquina protegida garante que o trabalho de replicação dessa máquina inicie antes de uma máquina com a prioridade de replicação padrão de 5. Os trabalhos de replicação das máquinas com prioridade 3 são colocados em fila antes do 4 e assim por diante. Quanto menor o número da prioridade, mais cedo os trabalhos de replicação serão enviados. É fácil lembrar que a prioridade 1 é a mais importante. As máquinas com prioridade de replicação 1 são as primeiras a entrarem na fila para a replicação.

Conclua as etapas a seguir para editar as definições que priorizam a replicação de uma máquina protegida.

1 No Core de origem, abra o Rapid Recovery Core Console e na barra de ícones, clique em  (Replicação).
A página **Replicação** é mostrada.

2 No painel **Replicação de saída**, clique na seta ▼ à direita de qualquer Core de origem.
A visualização expande para mostrar cada uma das máquinas protegidas desse Core de origem que estão sendo replicadas para o Core de destino designado.

3 Clique no menu suspenso  (Definições) da máquina protegida que deseja priorizar e depois clique em **Definições**.
Uma caixa de diálogo será exibida.

4 Clique na lista suspensa **Prioridade** e selecione uma prioridade, de **1 (Mais alta)** a **10 (Mais baixa)**, com base nos seus requisitos.

5 Clique em **Salvar**.
A caixa de diálogo é fechada e a prioridade da replicação para a máquina selecionada atualiza.

Remoção da replicação

Replicação é a duplicação intencional de pontos de recuperação para uma máquina protegida a partir de um Rapid Recovery Core (Core de origem) para um segundo Core (destino).

O objetivo da replicação é manter uma duplicação de dados de alta disponibilidade para a máquina protegida original. Para uma segurança de dados ideal, a Dell recomenda localizar o Core de destino em um local geográfico separado.

A menos que você altere o comportamento padrão ao definir um programa de replicação, o Core iniciará o trabalho de replicação imediatamente após conclusão de cada snapshot de backup, verificação de soma de verificação, verificação de capacidade de anexação e trabalhos noturnos. Para obter mais informações, consulte Programar a replicação.

Ao remover a replicação, você descontinua a cópia adicional de pontos de recuperação a partir do Core de origem para o Core de destino. A remoção da replicação nunca afeta os dados salvos no Core original (de origem).

Além disso, ao remover a replicação, você tem a opção de manter os pontos de recuperação replicados da máquina original no seu Core de destino ou excluí-los. Se você reter os pontos de recuperação para uma máquina replicada que foi removida, os pontos de recuperação dessa máquina serão representados no Core como uma máquina somente de pontos de recuperação. Você pode navegar pelos dados desses pontos de recuperação retidos ou restaurar arquivos no nível do arquivo enquanto continuam no Core de destino.

Você pode remover a replicação utilizando qualquer um dos seguintes métodos:

- Remover replicação de saída do Core de origem

• Remover replicação de entrada do Core de destino

Remover replicação de saída do Core de origem

Conclua as etapas deste procedimento para remover uma ou mais máquinas protegidas da replicação no Core de origem.

1 No Core de origem, abra o Rapid Recovery Core Console e, na barra de ícones, clique em (Replicação).
A página **Replicação** é exibida.

No painel **Replicação de saída**, a tabela de resumo inclui uma linha para cada Core de destino que foi configurado para replicar os pontos de recuperação a partir desse Core de origem.

2 Opcionalmente, clique na seta à direita de qualquer Core de destino.
A visualização é expandida para exibir cada uma das máquinas protegidas desse Core de origem que estão sendo replicadas para o Core de destino designado.

3 Selecione as máquinas protegidas que deseja remover da replicação de saída como a seguir:

- Para remover completamente a relação de replicação existente entre Core de origem e qualquer Core de destino, clique no menu suspenso (Configurações) para qualquer Core de destino e selecione **Excluir**.
- Para remover a replicação de saída para um subconjunto de máquinas no Core de destino especificado, expanda a visualização para exibir todas as máquinas sendo replicadas e marque a caixa de seleção de cada máquina replicada que deseja remover. Desmarque a caixa de seleção de qualquer máquina você deseja continuar replicando. Depois, no menu acima da tabela de resumo, clique em **Excluir**.

Uma mensagem de confirmação será exibida, perguntando se você deseja remover as relações de replicação.

4 Na caixa de diálogo resultante, clique em **Sim** para confirmar a remoção.

Remover replicação de entrada do Core de destino

Conclua as etapas deste procedimento para remover uma ou mais máquinas protegidas da replicação no Core de destino.

NOTA: Você também pode remover a replicação de máquinas protegidas do painel de Replicação de saída na página Replicação do Core de origem. Para obter mais informações, consulte Remover replicação de saída do Core de origem

1 No Core de destino, abra o Rapid Recovery Core Console e, na barra de ícones, clique em (Replicação).
A página **Replicação** é exibida. No painel de Replicação de entrada, a tabela de resumo inclui uma linha de cada Core de origem com máquinas protegidas que são replicadas por esse Core de destino.

2 Selecione as máquinas replicadas a serem removidas como a seguir:

- Para excluir **todas** as máquinas replicadas do Core de origem para seu Core de destino, no painel Replicação de entrada, marque a caixa de seleção para esse Core.
- Para excluir um subconjunto menor de máquinas do mesmo Core de origem, faça o seguinte:

  a Clique na seta à direita do Core de origem.
  A visualização é expandida para exibir cada uma das máquinas do Core de origem selecionado que são replicadas em seu Core de destino.

  b Marque a caixa de seleção de cada máquina replicada que deseja remover.

  c A partir da linha principal do Core de origem selecionado, clique no menu suspenso (Configurações) e selecione **Excluir**.
  A caixa de diálogo **Remover replicação** é exibida.

3 Na caixa de diálogo **Remover replicação**, faça o seguinte:

- Se desejar manter os pontos de recuperação replicados no Core de destino, remova a opção **Excluir pontos de recuperação existentes** .

- Se desejar excluir todos os pontos de recuperação replicados dessa máquina, bem como remover o core de origem da replicação, selecione **Excluir pontos de recuperação existentes**.

4 Clique em **Sim** para confirmar a exclusão.

ATENÇÃO: Se você selecionar essa opção, todos os pontos de recuperação nesse Core serão excluídos.

As máquinas protegidas selecionadas no Core de origem são removidas da replicação nesse Core de destino. Opcionalmente, se você tiver selecionado a opção de excluir pontos de recuperação, eles serão removidos do repositório desse Core.

Recuperar dados replicados

A funcionalidade de replicação "Dia a dia" é mantida no Core de origem, enquanto apenas o Core de destino é capaz de executar as funções necessárias para a recuperação após desastres.

Para recuperação após desastres, o Core de destino pode usar os pontos de recuperação replicados para recuperar as máquinas protegidas. Você pode executar as seguintes opções de recuperação no Core de destino:

- **Montar ponto de recuperação.** Para obter mais informações, consulte Montar um ponto de recuperação.
- **Reverter para pontos de recuperação.** Para obter mais informações, consulte Como restaurar volumes a partir de um ponto de recuperação ou Restaurar volumes em uma máquina Linux usando a linha de comando.
- **Realizar uma exportação de máquina virtual (VM).** Para obter mais informações, consulte Sobre a exportação para máquinas virtuais com o Rapid Recovery.
- **Realizar uma bare metal restore (BMR).** Para obter mais informações, consulte Como executar uma restauração "bare metal" em máquinas Windows.

5

Recuperar dados

Gerenciar a recuperação

O Rapid Recovery Core pode restaurar ou recuperar máquinas físicas ou virtuais instantaneamente a partir de pontos de recuperação. Os pontos de recuperação contêm instantâneos de volume do agente capturados a nível de bloco. Esses instantâneos possuem reconhecimento de aplicativos, o que significa que todos os logs de transação em andamento e transações em aberto são concluídos e caches são liberados do disco antes de criar o instantâneo. Usar instantâneos com reconhecimento de aplicativos em conjunto com a recuperação verificada permite que o núcleo realize diversos tipos de recuperações,incluindo:

- Recuperação de arquivos e pastas
- Recuperação de volumes de dados, usando o Live Recovery
- Recuperação de volumes de dados para o Microsoft Exchange Server e o MicrosoftSQL Server, usando a recuperação em tempo real
- Restauração bare-metal, usando o Universal Recovery
- Restauração sem sistema operacional para hardware diferente, usando a recuperação universal
- Exportação ad-hoc e contínua para máquinas virtuais

Instantâneos e pontos de recuperação

Esta seção descreve como usar e gerenciar os instantâneos e os pontos de recuperação gerados pelo Rapid Recovery. Contém informações sobre montagem, exibição e imposição, bem como migração e exclusão de pontos de recuperação.

Gerenciar snapshots e pontos de recuperação

Um ponto de recuperação é uma coleção de snapshots tirados de volumes de disco individuais e armazenados no repositório. Os snapshots capturam e armazenam o estado de um volume de disco em determinado momento, enquanto os aplicativos que geram os dados ainda estão em uso. No Rapid Recovery, é possível forçar um snapshot, pausar temporariamente os snapshots e visualizar as listas de pontos de recuperação atuais no repositório, além de excluí-los se necessário. Os pontos de recuperação são utilizados para restaurar as máquinas protegidas ou para montar um sistema de arquivos local.

Os snapshots capturados pelo Rapid Recovery são feitos no nível do bloco e reconhecem o aplicativo. Isso significa que todas as transações abertas e os logs de transação contínua são concluídos e os caches são descarregados em disco antes da criação do snapshot.

O Rapid Recovery usa um driver de filtro de volume de baixo nível, que se anexa aos volumes montados e depois rastreia todas as alterações no nível de bloco para o próximo snapshot iminente. O Microsoft Volume Shadow Services (VSS) é usado para facilitar snapshots consistentes de falhas de aplicativos.

Ver a página de pontos de recuperação de uma máquina protegida

Conclua as etapas do procedimento a seguir para ver a lista completa de ponto de recuperação de uma máquina protegida.

NOTA: Se você estiver protegendo dados a partir de um cluster de servers DAG ou CCR, os pontos de recuperação associados não aparecerão no nível de cluster. Estarão visíveis apenas no nível de nó ou máquina.

1 No Rapid Recovery Core Console, navegue até a máquina protegida da qual deseja visualizar os pontos de recuperação.

2 No menu na parte superior da página, clique em **Pontos de recuperação**.

A página Pontos de recuperação é exibida, mostrando um painel de resumo dos pontos de recuperação e um painel de pontos de recuperação.

Você pode visualizar informações resumidas sobre os pontos de recuperação da máquina conforme a descrição na tabela a seguir.

Tabela 147. Informações resumidas do ponto de recuperação

Informações	Descrição
Total de pontos de recuperação	Lista o número total de pontos de recuperação salvos no repositório para esta máquina.
Total de dados protegidos	Indica a quantidade de espaço de armazenamento usado no repositório para esses pontos de recuperação.
Repositório de DVM	Mostra o nome do repositório no qual esses pontos de recuperação estão armazenados.
Status do repositório de DVM	Exibe graficamente a quantidade de espaço consumido pelos pontos de recuperação. Mostra a porcentagem do repositório usado, a quantidade de espaço e o espaço total do repositório. Clique no gráfico para ver a quantidade de espaço restante.

Você pode visualizar informações sobre os pontos de recuperação da máquina conforme a descrição na tabela a seguir.

Tabela 148. Informações do ponto de recuperação

Informações	Descrição
Ícone	Representação gráfica de um ponto de recuperação  ou, se expandido, um volume dentro do ponto de recuperação  . Os pontos de recuperação mostram uma seta para a direita  indicando que detalhes podem ser expandidos.
Criptografado	Indica se o ponto de recuperação é criptografado.
Status	Indica o status atual do ponto de recuperação.
Conteúdo	Relaciona os volumes incluídos no ponto de recuperação. Clique em  (Informações) para ver o uso de espaço e o sistema de arquivos.
Tipo	Define um ponto de recuperação como uma imagem de base ou um snapshot (diferencial) incremental.
Data de criação	Exibe a data em que o ponto de recuperação foi criado.
Tamanho	Exibe a quantidade de espaço que o ponto de recuperação consome no repositório.
	O menu suspenso Configurações permite que você execute determinadas funções para o ponto de recuperação selecionado.

3 Opcionalmente, expanda um ponto de recuperação para ver os volumes protegidos.

Links relacionados

Como ver pontos de recuperação para uma máquina

Noções básicas sobre indicadores de status de ponto de recuperação

Após a captura de um ponto de recuperação de um SQL ou Exchange Server protegido, o aplicativo exibe um indicador de status da cor correspondente na grade Ponto de Recuperação. Essa grade é exibida no painel **Pontos de recuperação** durante a exibição dos pontos de recuperação de uma máquina específica. A cor exibida se baseia nas definições de verificação da máquina protegida e no sucesso ou na falha dessas verificações, conforme descrito nas tabelas a seguir.

NOTA: Para obter mais informações sobre como exibir pontos de recuperação, consulte Ver a página de pontos de recuperação de uma máquina protegida.

Cores de status de ponto de recuperação para bancos de dados Exchange

A tabela a seguir relaciona os indicadores de status exibidos para bancos de dados Exchange.

Tabela 149. Indicadores de status de banco de dados Exchange

Cor de status	Descrição
Branco	Indica que um banco de dados do Exchange não é detectado dentro do ponto de recuperação, do volume ou do grupos de volumes.
Amarelo	Indica que as verificações de montabilidade do banco de dados do Exchange ainda não foram executadas.
Vermelho	Indica que as verificações de montabilidade ou de soma de verificação falharam em pelo menos um banco de dados.
Verde	Indica que o ponto de recuperação contém um ou mais bancos de dados e que as verificações de capacidade de montagem estão ativadas e que a verificação de capacidade de montagem ou que a verificação de soma de verificação foi aprovada.

Cores de status de ponto de recuperação para bancos de dados SQL

A tabela a seguir relaciona os indicadores de status exibidos para bancos de dados SQL.

Tabela 150. Indicadores de status de banco de dados SQL

Cor de status	Descrição
Branco	Indica que um banco de dados SQL não é detectado dentro do ponto de recuperação, do volume ou do grupos de volumes.
Amarelo	O banco de dados SQL estava offline, indicando que as verificações de capacidade de anexação não eram possíveis e não foram realizadas.
Vermelho	Indica que a verificação de capacidade de anexação falhou ou que o banco de dados SQL está offline.
Verde	Indica que a verificação de capacidade de anexação foi aprovada.

NOTA: Pontos de recuperação que não tenham um banco de dados Exchange ou SQL associados são exibidos com um indicador de status branco. Em situações em que existe banco de dados do Exchange e do SQL para o ponto de recuperação, o indicador de status mais grave é exibido no ponto de recuperação.

Montar um ponto de recuperação

No Rapid Recovery, você pode montar um ponto de recuperação para uma máquina Windows para acessar dados armazenados através de um sistema local de arquivos.

NOTA: Para montar um ponto de recuperação do Linux com o utilitário `local_mount`, consulte Montar um volume de ponto de recuperação em máquina Linux.

NOTA: Ao montar pontos de recuperação de dados restaurados de uma máquina com deduplicação de dados ativada, será preciso ativar também a deduplicação no servidor do Core.

1. No Rapid Recovery Core Console, navegue até a máquina que deseja montar em um sistema de arquivos local.
   A página **Resumo** da máquina protegida selecionada é exibida.
2. Clique no menu **Pontos de recuperação**.
   A página **Pontos de recuperação** da máquina selecionada é exibida.
3. Opcionalmente, no painel **Pontos de recuperação**, na lista de pontos de recuperação, clique no símbolo de seta para a direita ▸ para expandir os detalhes do ponto de recuperação, mostrando os volumes incluídos no ponto de recuperação.
4. Na linha do ponto de recuperação que você deseja montar, clique em  e, no menu suspenso, selecione **Montagem**.
   O **Assistente de montagem** é exibido, mostrando a página **Volumes**.
5. Na página **Volumes**, selecione cada volume do ponto de recuperação que você deseja montar e depois clique em **Avançar**.
   A página **Opções de montagem** do Assistente de montagem é exibida.
6. Na página **Opções de montagem**, edite as definições de montagem de um ponto de recuperação, conforme descrito na tabela a seguir.

Tabela 151. Definições das Opções de montagem

Opção	Descrição
Pasta local	Especifique o caminho usado para acessar o ponto de recuperação montado. Por exemplo, selecione `C:\ProgramData\AppRecovery\MountPoints\ MountPoint1`.
Tipo de montagem	Especifique o modo de acessar os dados do ponto de recuperação montado: • Apenas leitura • Apenas leitura com gravações anteriores • Gravável
Criar um compartilhamento do Windows para essa montagem	Como opção, marque esta caixa de seleção para especificar se o ponto de recuperação montado pode ser compartilhado e defina os direitos de acesso a ele, incluindo o nome de compartilhamento e os grupos permitidos.

7. Clique em **Concluir** para montar o ponto de recuperação.

   NOTA: Se você desejar copiar diretórios ou arquivos de um ponto de recuperação montado para outra máquina com Windows, use o Windows Explorer para copiá-los com as permissões padrão ou permissões de acesso do arquivo original. Para obter mais detalhes, consulte Restaurar um diretório ou arquivo usando o Windows Explorer a Restaurar um diretório ou arquivo e preservar as permissões usando o Windows Explorer.
8. Como opção, enquanto a tarefa estiver em andamento, você poderá visualizar seu progresso no menu suspenso **Tarefas em execução** no Core Console ou visualizar informações detalhadas na página **Eventos**. Para obter mais informações sobre o monitoramento de eventos do Rapid Recovery, consulte Como exibir eventos usando tarefas, alertas e registros.

Desmontar pontos de recuperação

Conclua as etapas deste procedimento para desmontar os pontos de recuperação que estão montados no Core.

NOTA: Ao desmontar um ponto de recuperação montado remotamente, a ação é denominada *desconectar*.

1 No Rapid Recovery Core Console, na barra de ícones, clique em (Mais) e, em seguida, selecione **Montagens**.

A página **Montagens** aparece. Há um painel para Montagens locais (pontos de recuperação montados a partir do Core) e outro para Montagens remotas (pontos de recuperação montados por meio do Local Mount Utility). Em cada painel, os respectivos pontos de recuperação montados aparecem em uma lista.

2 Para desmontar montagens locais, no painel **Montagens locais**, faça o seguinte:

a Selecione o ponto ou os pontos de montagem locais que você quer desmontar.

- Para desmontar todos os pontos de recuperação, clique na caixa de verificação na barra de título da tabela Montagens locais para selecionar todos os pontos de montagem.
- Para desmontar um ou mais pontos de recuperação, clique na caixa de verificação na primeira coluna de cada linha representando o ponto de montagem que você deseja desconectar.

b Clique em **Desmontar**.

Uma caixa de diálogo de confirmação é mostrada.

c Clique para confirmar que você quer desmontar os pontos de recuperação selecionados.

Os pontos de recuperação locais são desmontados.

NOTA: Se os alertas do sistema estiverem habilitados, você pode ver um alerta de que os pontos de montagem adequados estão sendo desmontados.

3 Para desconectar pontos de recuperação montados remotamente, no painel **Montagem remota**, faça o seguinte:

a Selecione o ponto ou os pontos de montagem remota que você quer desconectar.

- Para desconectar todos os pontos de recuperação, clique na caixa de verificação na barra de título da tabela Montagem remota para selecionar todos os pontos de montagem.
- Para desconectar um ou mais pontos de recuperação, clique na caixa de verificação na primeira coluna de cada linha representando o ponto de montagem que você deseja desconectar.

b Clique em **Desconectar**.

Uma caixa de diálogo de confirmação é mostrada.

c Clique para confirmar que você quer desconectar os pontos de recuperação selecionados.

Os pontos de recuperação locais são desconectados.

NOTA: Se os alertas do sistema estiverem habilitados, você pode ver um alerta de que os pontos de montagem adequados estão sendo desconectados.

4 Confirme que os pontos de recuperação montados anteriormente não são mais exibidos na lista de Montagens remotas ou locais, conforme adequado.

Trabalhar com pontos de recuperação do Linux

O método recomendado e compatível de montar e desmontar pontos de recuperação em uma máquina Linux protegida é usar o utilitário *local_mount*.

Os procedimentos apresentados abaixo tratam especificamente do uso do local_mount para montar e desmontar pontos de recuperação do Linux.

NOTA: Para gerenciar pontos de recuperação do Linux de outras maneiras, consulte Gerenciar snapshots e pontos de recuperação, pois todas as outras atividades de gerenciamento podem ser realizadas no Core Console.

Montar um volume de ponto de recuperação em máquina Linux

Com o utilitário local_mount no Rapid Recovery, você pode montar um volume remotamente de um ponto de recuperação como um volume local em uma máquina Linux.

NOTA: Ao realizar este procedimento, não tente montar pontos de recuperação na pasta /tmp, que contém os arquivos aavdisk.

1 Crie um novo diretório para montar o ponto de recuperação (por exemplo, pode usar o comando`mkdir`).

2 Confirme se o diretório existe (por exemplo, usando o comando`ls`).

3 Execute o utilitário local_mount do Rapid Recovery como raiz ou como superusuário, por exemplo:

```
sudo local_mount
```

4 No prompt de montagem do Rapid Recovery, digite o comando a seguir para listar as máquinas protegidas.

```
lm
```

5 Quando solicitado, digite o endereço IP ou nome do host do servidor do Rapid Recovery Core.

6 Insira as credenciais de login do server do Core, ou seja, o nome de usuário e a senha.

Será exibida uma lista das máquinas que estão protegidas pelo servidor do Rapid Recovery. Cada máquina é identificada por: número de item de linha, host/endereço IP e número de ID da máquina.

Por exemplo: 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba

7 Insira o seguinte comando para relacionar os pontos de recuperação que estão disponíveis para uma máquina especificada:

```
lr <line_number_of_machine>
```

NOTA: Observe que você também pode inserir o número de ID da máquina neste comando em vez do número do item de linha.

É exibida uma lista com os pontos de recuperação de base e incrementais da máquina. Essa lista inclui o número do item de linha, o carimbo de data e hora, o local do volume, o tamanho do ponto de recuperação e número de ID do volume, que termina com um número de sequência para identificar o ponto de recuperação.

Por exemplo, 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2

8 Insira o seguinte comando para selecionar e montar o ponto de recuperação especificado no ponto/caminho de montagem especificado.

```
m <volume_recovery_point_ID_number> <volume-letter> [flag] <path>
```

O sinalizador no comando determina como montar o ponto de recuperação. Você pode usar uma das opções a seguir:

- [r] - montar apenas leitura (padrão). Este sinalizador permite montar um ponto de recuperação, mas não alterá-lo.
- [w] - montar gravável. Este sinalizador permite montar um ponto de recuperação e alterá-lo.
- [v] - montar com gravações anteriores. O sinalizador "v" permite montar o ponto de recuperação e incluir alterações que tenham sido feitas durante a montagem gravável anterior mas não estejam presentes no ponto de recuperação.
- [n] - não montar nbd em <path>. Um nbd (dispositivo de bloco de rede) estabelece uma conexão de socket entre o Core e a máquina protegida quando você realiza uma montagem local. Este sinalizador permite montar o ponto de recuperação sem montar o nbd, o que é útil caso você queira verificar manualmente o sistema de arquivos do ponto de recuperação.

NOTA: Você também pode especificar um número de linha no comando em vez do número de ID do ponto de recuperação para identificar o ponto de recuperação. Nesse caso, você usaria o número de linha da máquina (da saída de lm), seguido do número da linha do ponto de recuperação e letra de volume, seguido do caminho, como neste exemplo: m <machine_line_number> <recovery_point_line_number> <volume_letter> <path>. Por exemplo, se a saída de`lm` relacionar três máquinas protegidas e você inserir o comando`lr` para o número 2 e montar o volume b do ponto de recuperação 23 em /tmp/mount_dir, o comando será: `m 2 23 b /tmp/mount_dir`

NOTA: Se você estiver montando um volume BTRFS de um sistema operacional compatível (consulte o tópico "Matriz de compatibilidade e instalação do sistema operacional do Rapid Recovery versão 6.1" no *Guia de instalação e atualização do Dell Data Protection | Rapid Recovery*), você precisa incluir o seguinte parâmetro:

```
mount -o nodatasum,device=/dev/xxx /dev/xxx /mnt/yyy
```

9 Para confirmar se a montagem foi bem-sucedida, insira o seguinte comando, que deve listar o volume remoto anexado:

```
l
```

Desmontar um ponto de recuperação em uma máquina Linux

Complete as etapas neste procedimento para desmontar um ponto de recuperação em uma máquina Linux.

1 Execute o utilitário local_mount do Rapid Recovery como raiz ou como superusuário, por exemplo:

```
sudo local_mount
```

2 No prompt de montagem do Rapid Recovery, digite o comando a seguir para listar as máquinas protegidas.

```
lm
```

3 Quando solicitado, digite o endereço IP ou nome do host do servidor do Rapid Recovery Core.

4 Insira as credenciais de login (nome de usuário e a senha) do server do Core.

Será exibida uma lista das máquinas que estão protegidas pelo servidor do Rapid Recovery.

5 Insira o seguinte comando para relacionar os pontos de recuperação que estão disponíveis para uma máquina especificada:

```
lr <line_number_of_machine>
```

NOTA: Observe que você também pode inserir o número de ID da máquina neste comando em vez do número do item de linha.

Uma lista exibe e inclui os pontos de recuperação de base e incremental da máquina. Essa lista inclui um número de item de linha, data e carimbo de data e hora, localização do volume, tamanho de ponto de recuperação e número de ID do volume que inclui um número de sequência no fim, que identifica o ponto de recuperação.

Por exemplo: 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2

6 Execute o comando`l or list` para obter uma lista dos dispositivos Network Block Device (NBD). Se você montar um ponto de recuperação, receberá um caminho para o NBD-device depois de executar o comando`l or list .`

7 Insira o seguinte comando para desmontar um ponto de recuperação:

```
unmount <path_of_nbd-device>
```

8 Execute o comando`l or list` para garantir que a desmontagem do ponto de recuperação foi bem-sucedida.

Forçar um snapshot

Forçar um snapshot permite forçar uma transferência de dados para a máquina protegida atual. Ao forçar um snapshot, a transferência começa imediatamente ou é adicionada à fila se outros trabalhos estiverem em execução.

Você pode escolher entre dois tipos de snapshots.

Se você selecionar um snapshot incremental e não houver nenhum ponto de recuperação anterior, uma imagem de base é capturada. Forçar um snapshot não altera o horário de qualquer snapshot programado.

NOTA: O Rapid Recovery suporta Windows 8, Windows 8.1, Windows Server 2012 e Windows Server 2012 R2 para transferências de base e incrementais.

- Uma imagem de base é um snapshot de todos os dados nos volumes selecionados da máquina.
- Um snapshot incremental captura todos os dados que foram alterados desde o último snapshot.

1 No Rapid Recovery Core Console, navegue até a máquina ou cluster com o ponto de recuperação no qual deseja forçar um snapshot.

2 Na página Resumo, no painel Resumo, clique em **Forçar snapshot**.

A caixa de diálogo Forçar snapshot é mostrada.

3 Na caixa de diálogo Forçar snapshot, na caixa de seleção, clique em um ou mais volumes ou grupos de proteção.

4 Clique em **Forçar snapshot** ou Forçar imagem de base, respectivamente.

5 Se você tiver selecionado uma imagem de base, clique para confirmar que você quer capturar uma imagem de base.

Uma imagem de base pode levar uma quantidade de tempo significativa, com base na quantidade de dados dos volumes que você quer incluir no backup.

O snapshot selecionado é colocado na fila e começa assim que outros trabalhos forem concluídos.

Remover pontos de recuperação

É fácil remover do repositório os pontos de recuperação de determinada máquina. Ao excluir pontos de recuperação no Rapid Recovery, especifique uma das seguintes opções.

- **Excluir todos os pontos de recuperação**. Remove do repositório todos os pontos de recuperação da máquina protegida selecionada.
- **Excluir um intervalo de pontos de recuperação**. Remove todos os pontos de recuperação em um intervalo especificado antes do atual, até e incluindo a imagem de base, ou seja, todos os dados da máquina, além de todos os pontos de recuperação após o atual até a próxima imagem de base.

NOTA: Não é possível recuperar os pontos de recuperação excluídos. Se você precisar dos dados armazenados nos pontos de recuperação, considere arquivar os dados primeiro.

1 No Rapid Recovery Core Console, no menu **Máquinas protegidas**, clique no nome ou endereço IP da máquina para a qual você quer visualizar e remover pontos de recuperação.

A visualização Resumo da máquina protegida selecionada é exibida.

2 Ao lado do nome ou endereço IP da máquina, clique no menu **Pontos de recuperação**.

A página **Pontos de recuperação** da máquina selecionada é exibida.

3 Role para baixo até o painel **Pontos de recuperação**.

As opções aparecem sob o título painel, incluindo Atualizar, Excluir intervalo e Excluir tudo.

4 Para excluir todos os pontos de recuperação armazenados atualmente, sob o título do painel Pontos de recuperação, clique em **Excluir tudo** e, na caixa de diálogo de confirmação, clique para confirmar a exclusão.

5 Para excluir um conjunto de pontos de recuperação em um intervalo de dados específico, faça o seguinte:

a Sob o título do painel Pontos de recuperação, clique em **Excluir intervalo**.

A caixa de diálogo **Excluir pontos de recuperação dentro do intervalo** é exibida.

b Na caixa de diálogo **Excluir pontos de recuperação dentro do intervalo**, no campo **De**, selecione a data e hora a partir da qual você quer começar a excluir os pontos de recuperação.

c No campo **Até**, selecione a data e a hora que definem os últimos pontos de recuperação que você deseja excluir.

d Clique em **Excluir**.

e Na caixa de diálogo de confirmação, clique para confirmar a exclusão.

Excluir uma cadeia de pontos de recuperação órfãos

Um ponto de recuperação órfão é um snapshot incremental que não está associado a uma imagem de base. Snapshots subsequentes continuam a se acumular sobre esse ponto de recuperação. No entanto, sem a imagem de base, os pontos de recuperação resultantes são incompletos e é improvável que contenham os dados necessários para concluir uma recuperação. Esses pontos de recuperação são considerados parte da cadeia de pontos de recuperação órfãos. Se essa situação ocorrer, a melhor solução é excluir a cadeia e criar uma nova imagem de base.

Para obter mais informações sobre como forçar uma imagem de base, consulte Como forçar um snapshot.

1 No Rapid Recovery Core Console, navegue para a máquina protegida cuja corrente do ponto de recuperação você deseja excluir.
2 No menu na parte superior da página, clique em **Pontos de recuperação**.
3 No painel Pontos de recuperação, expanda o ponto de recuperação órfão.
Esse ponto de recuperação é chamado, na coluna Tipo, de “Incremental, Órfão”.
4 A seguir, em Ações, clique em **Excluir**.
Aparece a janela Excluir pontos de recuperação.
5 Na janela Excluir pontos de recuperação, clique em **Sim**.

CUIDADO: Excluir esse ponto de recuperação exclui toda a cadeia de pontos de recuperação, incluindo os pontos de recuperação incremental que ocorrem antes ou depois dela, até a próxima imagem de base. Essa operação não pode ser desfeita.

A cadeia de pontos de recuperação órfãos é excluída.

Como migrar pontos de recuperação para um repositório diferente

Caso queira remover os pontos de recuperação de uma máquina protegida de um repositório sem excluí-los, você pode migrá-los para um repositório diferente usando esse procedimento. Esse processo envolve o arquivamento de pontos de recuperação do repositório de origem e, em seguida, a importação do arquivo para o repositório de destino.

Por exemplo, você pode realizar esse procedimento caso o repositório existente esteja cheio ou caso as necessidades mudem e você queira proteger uma máquina usando um Core e um repositório diferentes.

CUIDADO: Caso o repositório tenha sido atualizado anteriormente do AppAssure 5.3 ou 5.4 e usado replicação, a Dell recomenda realizar o Trabalho de verificar o repositório em cada repositório nesse Core de destino antes da migração. A realização desse trabalho impedirá a cópia de eventuais irregularidades nos dados para o novo repositório de destino. O Trabalho de verificar o repositório só permanece disponível na UI caso seja aplicável ao Core, e pode demorar um tempo substancial para ser executado. Para obter mais informações sobre este trabalho, consulte Sobre como verificar a integridade dos repositórios DVM. Para obter mais informações sobre como executar este trabalho, consulte Executar o trabalho de verificar o repositório em um repositório de DVM.

1 No Rapid Recovery Core Console, pause a proteção da máquina protegida ou das máquinas cujos pontos de recuperação você deseja migrar. Para obter mais informações, consulte Pausar e retomar a proteção.
2 Cancele todas as operações atuais da máquina protegida ou das máquinas cujos pontos de recuperação você deseja migrar, ou aguarde a conclusão de todas elas.
3 Arquive os pontos de recuperação das máquinas que você pausou. Para obter mais informações, consulte Criar um arquivo.
4 Após o arquivamento e a verificação do arquivo, remova os pontos de recuperação existentes da máquina protegida que você deseja migrar. Para obter mais informações, consulte Remover pontos de recuperação.

NOTA: Sem remover os pontos de recuperação existentes, você não pode alterar repositórios de uma máquina protegida.

5 Crie um novo repositório para os pontos de recuperação migrados ou verifique se existe um novo repositório de destino. Para obter mais informações, consulte Como criar um repositório DVM.
   - Caso você queira utilizar um repositório existente, passe à Etapa 6.
6 Altere o repositório de cada máquina que você pausou concluindo as etapas a seguir:
   a No Core Console, clique na máquina protegida na árvore de navegação.
   b Na página **Resumo** da máquina protegida, clique em **Definições**.
   c Na página **Definições**, no painel **Geral**, clique na lista suspensa **Repositório** e selecione o nome do repositório criado na Etapa 4.
      - Se quiser usar um repositório existente, selecione o nome de um repositório.

NOTA: Ao migrar pontos de recuperação para um repositório existente, certifique-se de que o repositório possui espaço livre suficiente para conter os pontos de recuperação migrados.

d Clique em **OK**.

7 Retome a proteção das máquinas que você pausou. Para obter mais informações, consulte Pausar e retomar a proteção.

8 Gere uma nova imagem de base de cada máquina protegido que você moveu. Para obter mais informações, consulte Forçar um snapshot e use Forçar imagem de base.

9 Importe os dados arquivados das máquinas que você deseja migrar. Para obter mais informações, consulte Importar um arquivamento.

Restaurar dados

Esta seção descreve como restaurar dados armazenados em cópias de segurança.

Sobre como restaurar dados com o Rapid Recovery

O Rapid Recovery Core pode restaurar instantaneamente dados ou recuperar máquinas para máquinas físicas ou virtuais a partir dos pontos de recuperação. Os pontos de recuperação contêm snapshots de volume de agentes capturados no nível do bloco. Esses snapshots reconhecem o aplicativo, ou seja, todas as transações abertas e os registros de transações contínuas são concluídos e os caches são descarregados em disco antes da criação do snapshot. O uso de snapshots que reconhecem aplicativos em conjunto com o Verified Recovery permite que o Core realize vários tipos de recuperações, incluindo:

- Recuperação de arquivos e pastas
- Recuperação de volumes de dados usando Live Recovery
- Recuperação de volumes de dados para Microsoft Exchange Server e Microsoft SQL Server, usando Live Recovery
- Bare metal restore, usando o Universal Recovery
- Bare metal restore para hardware diferente, usando o Universal Recovery
- Exportação ad hoc e contínua para máquinas virtuais

NOTA: Ao restaurar dados ou ao executar uma exportação virtual, o ponto de recuperação utilizado deve ser parte de uma cadeia completa de pontos de recuperação. Para obter mais informações sobre cadeias de pontos de recuperação, consulte o tópico Cadeias de pontos de recuperação e órfãos.

Noções básicas sobre Live Recovery

Live Recovery é um recurso de restauração de dados no Rapid Recovery Core. Se a máquina protegida apresentar uma falha de dados de um volume do Windows sem sistema, você poderá restaurar dados a partir de um ponto de recuperação no Rapid Recovery Core. A seleção do Live Recovery no Restore Wizard permite que os usuários continuem imediatamente operações de negócios com inatividade quase zero. O Live Recovery durante a restauração dá acesso imediato aos dados, mesmo enquanto o Rapid Recovery continua restaurando dados em segundo plano. Esse recurso permite tempo de recuperação quase zero, mesmo que a restauração envolva terabytes de dados.

Rapid Recovery Core usa tecnologia de backup e recuperação com base em bloco exclusiva que permite acesso total ao usuário para servidores de destino durante o processo de recuperação. Os blocos solicitados são recuperados sob demanda para recuperação total.

O Live Recovery se aplica a máquinas físicas e virtuais protegidas pelo Rapid Recovery Core, com as seguintes exclusões:

- O Live Recovery é acessível a volumes Windows sem sistema. A unidade C:/ e a partição reservada para o sistema não podem ser restauradas usando-se o Live Recovery.
- O Live Recovery é acessível a volumes com base no Windows usando-se o Rapid Recovery Agent. Os volumes sem agente ou os volumes Linux não podem usufruir o Live Recovery.

O Live Recovery permite restaurar de maneira instantânea ou servidores virtuais diretamente do arquivo de backup. Quando um volume sem sistema está sendo restaurado, o Rapid Recovery apresenta os metadados de volume para o Sistema operacional de maneira

instantânea, o que torna esses dados disponíveis sob demanda. Por exemplo, se volume do banco de dados do Microsoft Exchange estiver corrompido, o Live Recovery poderá restaurar o volume, o banco de dados e os serviços do Exchange em questão de minutos.

Esse recurso fornece o método mais rápido de recuperar grandes quantidades de dados com o mínimo de inatividade. Os usuários podem continuar imediatamente operações de negócios.

Assim que o Live Recovery começa, o volume restaurado e o conteúdo se tornam disponíveis instantaneamente. Rapid RecoveryCore continua restaurando os dados em segundo plano, mesmo que o volume, os dados, os aplicativos e os serviços já estejam novamente em produção. Se dados específicos forem solicitados, o processo em segundo plano priorizará a restauração desses dados imediatamente. Essa funcionalidade eficiente permite que até mesmo o contrato de serviço mais rígido seja atendido.

Depois que você iniciar o Live Recovery, metadados (estrutura de diretório, descritores de segurança, atributos de arquivo NTFS, mapa de espaço livre etc.) do volume de destino serão restaurados rapidamente na máquina protegida. Assim, o volume e o conteúdo se tornam disponíveis para o sistema. O Agente do Rapid Recovery começa a restaurar blocos de dados do servidor Core do Rapid Recovery, gravando os blocos no volume de destino.

Solicitações de dados que ainda não tiverem sido restauradas serão atendidas imediatamente, com o programa solicitante ou o sistema que desconhece que os blocos acabaram de ser restaurados.

Restaurar dados de pontos de recuperação

O Rapid Recovery protege seus dados em máquinas com Windows e Linux. Os backups das máquinas de agentes protegidos são salvos no Rapid Recovery Core como pontos de recuperação. A partir desses pontos de recuperação, você pode restaurar seus dados usando um dos três métodos.

No Rapid Recovery Core Console, você pode restaurar volumes inteiros a partir de um ponto de recuperação de um volume que não seja de sistema, substituindo os volumes na máquina de destino. É possível fazer isso apenas em máquinas com Windows. Para obter mais informações, consulte Como restaurar volumes a partir de um ponto de recuperação.

Não é possível restaurar um volume que contenha o sistema operacional diretamente de um ponto de recuperação, porque a máquina para a qual você está restaurando está usando o sistema operacional e os drivers que estão incluídos no processo de restauração. Se você deseja restaurar a partir de um ponto de recuperação em agente um volume do sistema (por exemplo, a unidade C da máquina do Agent), realize uma bare metal restore (BMR). Isso envolve a criação de uma imagem inicializável a partir do ponto de recuperação, incluindo o sistema operacional e os arquivos de configuração, além dos dados, e o início da máquina de destino a partir dessa imagem inicializável para concluir a restauração. A imagem inicializável é diferente se a máquina que você deseja restaurar usa um sistema operacional Windows ou Linux. Se você deseja restaurar a partir de um ponto de recuperação em um volume do sistema em uma máquina com Windows, consulte Como executar uma restauração “bare metal” em máquinas Windows. Se você deseja restaurar a partir de um ponto de recuperação em um volume do sistema em uma máquina com Linux, consulte Como executar uma restauração “bare metal” em máquinas Windows.

Finalmente, em contraste com a restauração de volumes inteiros, é possível montar um ponto de recuperação a partir de uma máquina com Windows e navegar pelas pastas e arquivos individuais para recuperar apenas um conjunto específico de arquivos. Para obter mais informações, consulte Restaurar um diretório ou arquivo usando o Windows Explorer. Se for preciso fazer isso e preservar as permissões de arquivos originais (por exemplo, ao restaurar uma pasta de usuário em um server de arquivos), consulte Restaurar um diretório ou arquivo e preservar as permissões usando o Windows Explorer.

Os tópicos desta seção descrevem informações sobre como restaurar dados em máquinas físicas. Para obter mais informações sobre a exportação de dados protegidos de máquinas com Windows para máquinas virtuais, consulte Exportação de VM.

NOTA: Ao recuperar dados em máquinas com Windows, se o volume que você está restaurando está com a deduplicação de dados do Windows ativada, será preciso ter certeza que a deduplicação também está ativada no server do Core. O Rapid Recovery suporta o Windows 8, Windows 8.1, Windows 10, Windows Server 2012 e Windows Server 2012 R2 para transferências normais (de base e incrementais), bem como para restauração de dados, bare metal restore e exportações virtuais. Para obter mais informações sobre os tipos de volumes suportados e não suportados para cópia de segurança e recuperação, consulte Suporte para volumes dinâmicos e básicos.

Como restaurar volumes a partir de um ponto de recuperação

Você pode restaurar o volumes em uma máquina protegida a partir dos pontos de recuperação armazenados no Rapid Recovery Core.

NOTA: Em versões anteriores, este processo foi conhecido como a realização de uma reversão.

NOTA: O Rapid Recovery oferece suporte a proteção e recuperação de máquinas configuradas com partições EISA. Suporte é também estendido as Windows 8, 8,1, Windows Server 2012 e Windows Server 2012 R2 que usam máquinas em ambiente de recuperação do Windows (Windows RE).

Você pode começar uma restauração a partir de qualquer local no Rapid Recovery Core Console, clique no ícone Restaurar na barra de botões Rapid Recovery. Quando você inicia uma restauração desta forma, você precisa especificar qual das máquinas protegidas no Núcleo que você quer restaurar e, em seguida, ir para o volume que você quer restaurar.

Ou você pode ir para página Pontos de recuperação para uma máquina específica, clique no menu suspenso para um ponto específico de recuperação e, em seguida, selecione **Restore (Restaurar)**. Se você iniciar uma restauração desta forma, siga este procedimento começando com a Etapa 5.

Se você quiser restaurar a partir do ponto de recuperação para um volume do sistema, ou restaurar a partir do ponto de recuperação usando um CD de inicialização, você precisa executar uma restauração "bare metal" (BMR). Para obter informações sobre BMR, consulte Noções básicas sobre bare metal restores em máquinas Windows, e para informações de pré-requisito para Windows ou sistemas operacionais Linux, consulte Pré-requisitos para realizar uma restauração sem sistema operacional para uma máquina Windows e Pré-requisitos para realizar uma bare metal restore em máquinas Linux, respectivamente. Você pode acessar as funções do Core Console conforme descrito no mapa para cada sistema operacional. Você também pode executar uma restauração BMR usando o Assistente de restauração da máquina. Este procedimento irá orientá-lo no local apropriado no assistente para o procedimento Realizar um bare metal restore usando o Assistente de restauração de máquina.

Restaurar volumes a partir de um ponto de recuperação

A máquina protegida deve ter o software Agent instalado e deve ter pontos de recuperação a partir dos quais você realizará a operação de restauração.

Execute o procedimento a seguir para restaurar volumes em um ponto de recuperação.

1 Para restaurar um volume em uma máquina protegida no ícone Restaurar, navegue até o Core Console e clique em **Restaurar** na barra de botões do Rapid Recovery.

O Assistente de restauração de máquinas é exibido.

2 Na página Máquinas protegidas, selecione a máquina protegida da qual deseja restaurar os dados e clique em **Avançar**.

Aparece a página Pontos de recuperação.

3 Na lista de pontos de recuperação, procure o snapshot que deseja restaurar da máquina agente.

- Se necessário, use os botões na parte inferior da página para exibir páginas adicionais dos pontos de recuperação.
- Como opção, para limitar o número de pontos de recuperação que aparecem na página Pontos de recuperação do assistente, você pode filtrar por volumes (se definidos) ou por data de criação do ponto de recuperação.

4 Clique em qualquer ponto de recuperação para selecioná-lo e em **Avançar**.

Aparece a página Destino.

5 Na página Destino, escolha a máquina para a qual deseja restaurar os dados da seguinte forma:

- Para restaurar os dados a partir do ponto de recuperação selecionado para a mesma máquina, e se os volumes que deseja restaurar não incluem o volume do sistema, selecione **Recuperar em uma máquina protegida (apenas volumes que não são do sistema)**, confirme se a máquina de destino está selecionada e clique em **Avançar**.

  A página Mapeamento de volume é exibida. Vá para a Etapa 9.

- Para restaurar os dados a partir do ponto de recuperação selecionado em uma máquina protegida diferente (por exemplo, substituir o conteúdo da Machine2 pelos dados da Machine1), selecione **Recuperar em uma máquina protegida (apenas volumes que não são do sistema)**, selecione a máquina de destino na lista e clique em **Avançar**.

A página Mapeamento de volume é exibida. Vá para a Etapa 9.

- Se você deseja restaurar a partir do ponto de recuperação selecionado na mesma máquina ou em uma máquina diferente usando um CD de inicialização, esse processo é considerado uma bare metal restore (BMR). Para obter informações sobre a BMR, consulte Noções básicas sobre bare metal restores em máquinas Windows.

  NOTA: A realização de uma BMR tem requisitos específicos, com base no sistema operacional da máquina do agente que você deseja restaurar. Para entender esses pré-requisitos, consulte Pré-requisitos para realizar uma restauração sem sistema operacional para uma máquina Windows e Pré-requisitos para realizar uma bare metal restore em máquinas Linux, respectivamente.

  Se os volumes que deseja restaurar incluem o volume do sistema, selecione **Recuperar em qualquer máquina de destino usando um CD de inicialização**. Esta opção irá notificá-lo a criar um CD de inicialização.

  - Para continuar e criar o CD de inicialização com as informações do ponto de recuperação selecionado utilizando o assistente de Restauração de máquinas, clique em **Avançar** e vá para a Como executar uma restauração "bare metal" em máquinas Windows.
  - Se você já criou o CD de inicialização e a máquina de destino foi iniciada utilizando-o, vá para a Etapa 8 do tópico Como executar uma restauração "bare metal" em máquinas Windows.

- Se você deseja restaurar a partir de um ponto de recuperação em um volume do sistema (por exemplo, a unidade C da máquina agente chamada Machine1), esse processo também é considerado uma BMR. Selecione **Recuperar em qualquer máquina de destino usando um CD de inicialização**. Esta opção irá notificá-lo a criar um CD de inicialização.
  - Para continuar e criar o CD de inicialização com as informações do ponto de recuperação selecionado utilizando o assistente de Restauração de máquinas, clique em Avançar e vá para a Como executar uma restauração "bare metal" em máquinas Windows.
  - Se você já criou o CD de inicialização, vá para a Etapa 6.

6 Inicie a máquina que você deseja restaurar utilizando o CD de inicialização. Para obter mais informações para BMR em uma máquina com Windows, consulte Como carregar o CD de inicialização e iniciar o computador de destino, e para BMR em uma máquina com Linux, consulte Carregar o Live DVD e iniciar o computador de destino.

7 No server do Core, na página Destino do assistente de Restauração de máquinas, selecione **Já possuo um CD de inicialização executando na máquina de destino** e insira as informações sobre a máquina à qual deseja se conectar, conforme descrito na tabela a seguir.

Tabela 152. Informações da máquina

Caixa de texto	Descrição
Endereço IP	O endereço IP da máquina na qual deseja restaurar. É idêntico ao endereço IP exibido no URC.
Chave de autenticação	A senha específica para se conectar ao server selecionado. É idêntico à chave de autenticação exibida no URC.

8 Clique em **Avançar**.

Se as informações de conexão inseridas correspondem ao URC, e se o Core e o server de destino podem identificar um ao outro corretamente na rede, os volumes do ponto de recuperação selecionado são carregados. A página Mapeamento de disco é exibida.

Para concluir sua BMR a partir do assistente de Restauração de máquinas, vá para a Etapa 9 do tópico Como executar uma restauração "bare metal" em máquinas Windows.

NOTA: O Rapid Recovery suporta partições FAT32 e ReFS. Apenas restauração completa e BRM são suportados, pois há uma limitação de driver com ReFS. A restauração é implementada no modo de usuário, exportação de VM e assim por diante. Se um Core está protegendo pelo menos um volume agente que contém o sistema de arquivos ReFS, ele deve ser instalado em máquinas com Windows 8/2012, que fornece suporte nativo ao formato ReFS. Caso contrário, a funcionalidade ficará limitada, e operações que envolvem tarefas, como a montagem de uma imagem de volume, não funcionarão. O Rapid Recovery Core Console apresentará as mensagens de erro aplicáveis a essas ocorrências.

A bare metal restore da configuração de discos de espaços de armazenamento (um recurso do Windows 8.1) também não é suportada nesta versão. Para obter mais detalhes, consulte o Guia de instalação e atualização do Rapid Recovery.

9 Na página Mapeamento de volume, para cada volume no ponto de recuperação que você deseja restaurar, selecione o volume de destino apropriado. Se você não deseja restaurar um volume, na coluna Volumes de destino, selecione **Não restaurar**.

10 Selecione **Exibir opções avançadas** e faça o seguinte:

- Para restaurar em máquinas com Windows, se quiser usar o Live Recovery, selecione **Live Recovery**.

  Usando a tecnologia de recuperação instantânea Live Recovery no Rapid Recovery, é possível recuperar ou restaurar instantaneamente os dados em suas máquinas físicas ou virtuais a partir de pontos de recuperação armazenados de máquinas com Windows, incluindo espaços de armazenamento do Microsoft Windows. O Live Recovery não está disponível para máquinas Linux ou MVs que usam proteção sem agente.
- Se você deseja forçar a desmontagem dos volumes selecionados antes de iniciar a restauração, selecione **Forçar desmontagem**.

  CUIDADO: Se você não forçar uma desmontagem antes de restaurar os dados, a restauração pode falhar com um erro indicando que o volume está em uso.

11 Clique em **Avançar.**

12 Na página Desmontar bancos de dados, se os volumes que você quer restaurar contêm bancos de dados SQL ou Microsoft Exchange, você será solicitado a desmontá-los.

Se você quiser remontar esses bancos de dados após a restauração ser concluída, selecione **Remontar automaticamente todos os bancos de dados após o ponto de recuperação ser restaurado**.

13 Clique em **Avançar.**

A página Aviso pode ser exibida e solicitar que você feche todos os programas nos volumes que você quer restaurar. Se houver algum, clique em **Avançar** novamente.

14 Na página de resumo, selecione a opção **IMPORTANTE! Eu sei que esta operação sobrescreverá os volumes selecionados com os dados do ponto de recuperação selecionado** para confirmar que você entende as consequências de uma restauração de volume.

ATENÇÃO: Esta opção enfatiza a consequência que todos os dados salvos no volume selecionado após a data e a hora do ponto de recuperação selecionado serão perdidos devido à restauração.

15 Clique em **Concluir**.

Restaurar um diretório ou arquivo usando o Windows Explorer

É possível usar o Windows Explorer para copiar e colar os diretórios e arquivos de um ponto de recuperação montado em qualquer máquina com Windows. Isso pode ser útil quando você quiser distribuir apenas uma parte de um ponto de recuperação para seus usuários.

Ao copiar arquivos e diretórios, as permissões de acesso do usuário que está realizando a operação de cópia são utilizadas e aplicadas aos diretórios e arquivos colados. Se você quiser restaurar diretórios e arquivos para seus usuários e preservar as permissões de arquivos originais (por exemplo, ao restaurar uma pasta de usuário em um server de arquivos), consulte Restaurar um diretório ou arquivo e preservar as permissões usando o Windows Explorer.

1 Monte o ponto de recuperação que contém os dados que você deseja restaurar. Para obter detalhes, consulte Montar um ponto de recuperação.

2 No Windows Explorer, navegue até o ponto de recuperação montado e selecione os diretórios e arquivos que deseja restaurar. Clique com o botão direito do mouse e selecione **Copiar**.

3 No Windows Explorer, navegue até o local da máquina onde você deseja restaurar os dados. Clique com o botão direito do mouse e selecione **Colar**.

Restaurar um diretório ou arquivo e preservar as permissões usando o Windows Explorer

É possível usar o Windows Explorer para copiar e colar os diretórios e arquivos de um ponto de recuperação montado em qualquer máquina com Windows e, ao mesmo tempo, preservar as permissões de acesso dos arquivos.

Por exemplo, se precisar restaurar uma pasta acessada somente por usuários específicos em um server de arquivos, você pode usar os comandos Copiar e Colar com permissões para garantir que os arquivos restaurados retenham as permissões que restringem o acesso. Dessa forma, é possível evitar ter que aplicar manualmente as permissões aos diretórios e arquivos restaurados.

NOTA: O comando Colar com permissões é instalado com o Rapid Recovery Core e o software do agente. Não está disponível no Local Mount Utility.

1 Monte o ponto de recuperação que contém os dados que você deseja restaurar. Para obter detalhes, consulte Montar um ponto de recuperação.

2 No Windows Explorer, navegue até o ponto de recuperação montado e selecione os diretórios e arquivos que deseja restaurar. Clique com o botão direito do mouse e selecione **Copiar**.

3 No Windows Explorer, navegue até o local da máquina onde você deseja restaurar os dados. Clique com o botão direito do mouse e selecione **Colar com permissões**.

NOTA: Nessa etapa, se o comando Colar com permissões estiver desabilitado no menu do botão direito, o Windows Explorer não terá conhecimento dos arquivos que você deseja copiar. Repita a Etapa 2 para habilitar o comando Colar com permissões no menu acessado com o botão direito do mouse.

Como realizar uma reversão para clusters e nós de cluster

A restauração é o processo de restaurar os volumes em uma máquina a partir dos pontos de recuperação. Para um cluster de servidores, a restauração é realizada no nível do nó (isto é, da máquina). Esta seção fornece diretrizes para realizar uma restauração de volumes de cluster.

Como executar uma restauração para clusters CCR e DAG (Exchange)

Execute o procedimento descrito neste procedimento para realizar uma restauração para clusters CCR e DAG (Exchange).

1 Desligue todos os nós, exceto um.

2 Execute uma restauração usando o procedimento Rapid Recovery padrão para a máquina, conforme descrito no Como restaurar volumes a partir de um ponto de recuperação e Restaurar volumes em uma máquina Linux usando a linha de comando.

3 Quando a restauração terminar, monte todas as bases de dados para os volumes de cluster.

4 Ligue todos os outros nós.

5 No caso do Exchange, navegue até o Exchange Management Console e, para cada banco de dados, execute a operação Atualizar cópia do banco de dados.

Como realizar uma restauração para clusters SCC (Exchange, SQL)

Execute os passos descritos neste procedimento para realizar uma restauração para clusters SCC (Exchange, SQL).

1 Desligue todos os nós, exceto um.

2 Execute uma restauração usando o procedimento Rapid Recovery padrão para a máquina, conforme descrito no Como restaurar volumes a partir de um ponto de recuperação e Restaurar volumes em uma máquina Linux usando a linha de comando.

3 Quando a restauração terminar, monte todos os bancos de dados a partir dos volumes de cluster.

4 Ligue todos os outros nós, um de cada vez.

NOTA: Você não precisa reverter o disco de quórum. Ele pode ser regenerado automaticamente ou usando a funcionalidade de serviço de cluster.

Restauração a partir de um arquivo em anexo

Há duas maneiras para restaurar dados de um arquivo: você pode usar um arquivo como uma fonte para uma restauração bare-metal (BMR); ou você pode anexar um arquivo, montar um ponto de recuperação do arquivo e, em seguida, restaurar os dados arquivados.

Quando você conecta um arquivo, ele é exibido em Arquivos conectados na página do Arquivos no Core Console, enquanto o conteúdo do arquivo morto se torna acessível a partir da área de navegação à esquerda. O conteúdo aparece sob o nome do arquivamento. As máquinas que estavam arquivadas aparecem como máquinas apenas para pontos de recuperação para que você possa acessar os pontos de recuperação da mesma forma que você faria para uma máquina atualmente protegida: por montagem de um ponto de recuperação, localizarndo o item que você deseja para recuperar, e usar o Windows Explorer para copiar e colar o item para o seu destino.

Há vantagens na restauração a partir de um arquivo em anexo em vez de importar um arquivo para um repositório.

- A restauração a partir de um arquivo em anexo salva o tempo que você pode investir para importar um arquivo inteiro para um repositório.
- Além disso, quando você importa um arquivo, os pontos de recuperação arquivados são adicionados ao repositório.

  Como esses pontos de recuperação arquivados provavelmente são os itens mais antigos no repositório, eles podem ser combinadas de acordo com a política de retenção durante o próximo trabalho noturno. (Embora, esta ação não excluí-los do arquivo; você pode re-importá-los no próximo dia.)
- Por fim, o Core lembra da associação do anexo com os arquivamentos, mesmo depois que você desanexar um arquivo, tornando mais fácil e rápido para conectar o arquivamento mais tarde.

  Você pode remover a associação apagando o anexo.

Para restaurar os dados de um arquivo em anexo, complete as seguintes etapas usando os links relacionados:

NOTA: O procedimento para restauração a partir de um arquivo em anexo presume que você já tem um arquivo de pontos de recuperação fusionados.

1 Anexe o arquivamento.
2 Monte o ponto de recuperação que contém os dados que você quer recuperar.
3 Restaure os dados usando qualquer um dos seguintes métodos:
   - Restaurar dados, como arquivo ou pasta, a partir do ponto de recuperação.
   - Restaurar todo o ponto de recuperação.
   - Exportar o ponto de recuperação para uma máquina virtual.

Links relacionados

Anexar um arquivo
Montar um ponto de recuperação
Restaurar um diretório ou arquivo usando o Windows Explorer
Sobre a exportação para máquinas virtuais com o Rapid Recovery
Backup do Windows
Noções básicas sobre arquivos
Importar um arquivamento
Como realizar uma BMR com base em um arquivo

Noções básicas sobre bare metal restores em máquinas Windows

Esta seção descreve como restaurar completamente uma máquina protegida Windows a partir de hardware semelhante ou diferente.

Restauração sem sistema operacional para máquinas Windows

Os servidores, quando funcionando conforme o esperado, executam as tarefas conforme estão configurados. É apenas quando falham que as coisas mudam. Quando ocorre um evento catastrófico, deixando um server inoperante, medidas imediatas são necessárias para restaurar a funcionalidade total da máquina.

O Rapid Recovery fornece a capacidade de realizar uma bare metal restore (BMR) em suas máquinas Windows ou Linux. A BMR é um processo que restaura a configuração completa do software de um sistema específico. A operação de restauração recupera não só os

dados do server, mas também reformata o disco rígido e reinstala o sistema operacional e todos os aplicativos de software. Para realizar uma BMR, especifique um ponto de recuperação de uma máquina protegida e reverta (realize uma restauração) para a máquina física ou virtual designada. Se estiver realizando uma restauração em um volume do sistema, isso é considerado uma BMR. Se estiver realizando uma restauração e for necessário um CD de inicialização, isso também é considerado uma BMR. Outras circunstâncias em que você pode decidir realizar uma bare metal restore incluem atualização de hardware ou substituição do server. Em ambos esses casos, você realiza uma restauração a partir de um ponto de recuperação para o hardware atualizado ou substituído.

O Rapid Recovery oferece suporte aos sistemas operacionais Windows 8, 8.1 e Windows Server 2012, 2012 R2 inicializados a partir de partições FAT32 EFI disponíveis para proteção ou recuperação, bem como volumes ReFS (Resilient File System).

NOTA: A bare metal restore da configuração de discos de espaços de armazenamento (um recurso do Windows 8.1) também não é suportada nesta versão. Atualmente, apenas a restauração completa e a BMR são suportadas, visto que existe uma limitação do driver com ReFS, de modo que a restauração é implementada em modo de usuário, exportação da VM, e assim por diante. Se um Core está protegendo pelo menos um volume agente que contém o sistema de arquivos ReFS, ele deve ser instalado em um Windows 8, Windows 8.1, Windows Server 2012 ou uma máquina com Windows Server 2012 R2, desde que esses sistemas operacionais ofereçam suporte nativo ao formato ReFS. Caso contrário, a funcionalidade será limitada, e operações que envolvem tarefas, como a montagem de uma imagem de volume, não funcionarão. O Rapid Recovery Core Console apresentará as mensagens de erro aplicáveis a essas ocorrências.

Apenas os sistemas operacionais Linux suportados estão disponíveis para proteção ou recuperação. Inclui Ubuntu®, Red Hat® Enterprise Linux®, CentOS™, e SUSE® Linux Enterprise Server (SLES®). Para obter mais detalhes, consulte o *Guia de instalação e atualização doDell Data Protection | Rapid Recovery*.

É possível realizar uma BMR em máquinas físicas ou virtuais. Um benefício adicional é que o Rapid Recovery permite realizar uma BMR quer o hardware seja semelhante, quer diferente. Realizar uma BMR no Rapid Recovery separa o sistema operacional de uma plataforma específica, proporcionando portabilidade.

Exemplos de realização de uma BMR para hardwares semelhantes incluem a substituição do disco rígido do sistema existente ou troca de server com falha por uma máquina idêntica.

Exemplos de realização de uma BMR para hardwares diferentes incluem a restauração de um sistema com falha com um server produzido por um fabricante diferente ou com configuração diferente. Esse processo envolve a criação de uma imagem de CD de inicialização, gravação da imagem em disco, inicialização do server de destino a partir da imagem de inicialização, conexão com a instância do console de recuperação, mapeamento dos volumes, início da recuperação e monitoramento do processo. Depois que a bare metal restore for concluída, você poderá continuar com a tarefa de carregar o sistema operacional e os aplicativos de software no server restaurado, seguida pelo estabelecimento de definições exclusivas necessárias para sua configuração.

A bare metal restore é usada não apenas em cenários de recuperação após desastres, mas também para migração de dados ao atualizar ou substituir servers.

Como executar uma restauração “bare metal” em máquinas Windows

Para executar uma restauração “bare metal” em máquinas Windows, execute as seguintes tarefas.

- Criar uma imagem de inicialização do Windows. Este CD de inicialização de imagem ISO será usado para iniciar a unidade de destino, a partir da qual você pode acessar o Console de Recuperação Universal para se comunicar com os backups do Núcleo. Consulte Entender a criação do CD de inicialização para máquinas Windows.
  - Se você precisar de mídia física para iniciar o backup da máquina de destino, você precisa transferir o CD de inicialização de imagem ISO em mídia. Consulte Como transferir a imagem ISO do CD de inicialização para a mídia.
  - Em todos os casos, você precisa carregar a imagem de inicialização para dentro do servidor de destino e iniciar o servidor usando a imagem de inicialização. Consulte Como carregar o CD de inicialização e iniciar o computador de destino.

    NOTA: Este processo descreve como gerenciar uma imagem de CD de inicialização a partir da caixa de diálogo Criar CD de inicialização. Você também pode executar estas etapas usando o Assistente de restauração da máquina, a partir da página CD de inicialização do assistente. Você acesse isso quando você especifica Recuperar a qualquer máquina de destino usando um CD de inicialização na página Destino do assistente. Para obter instruções passo a passo para gerenciamento de uma imagem de inicialização do Windows a partir do Assistente de restauração da máquina como parte de uma uma restauração “bare metal”, consulte Sobre como realizar um bare metal restore usando o Assistente de restauração de máquina.

- Abra uma restauração “bare metal” para Windows. Após a máquina de destino for iniciada a partir do CD de inicialização, você pode abrir o BMR. Consulte Como usar o Universal Recovery Console para uma BMR. Isso envolve as seguintes tarefas:
  - Iniciar uma restauração a partir do ponto de recuperação no Núcleo. Consulte Como selecionar um ponto de recuperação e iniciar uma BMR.
  - Mapear os volumes. Consulte Sobre como mapear volumes para uma restauração sem sistema operacional.
  - Se restaurando para hardware dissimilar, e os drivers de rede e de armazenamento necessários não estão presentes no CD de inicialização, você pode precisar carregar os drivers a partir de um dispositivo de mídia portátil. Para obter mais informações, consulte Carregar drivers usando o Universal Recovery Console.
- Como executar um BMR a partir do Assistente de restauração da máquina. Opcionalmente, os processos para gerenciamento de uma imagem de inicialização do Windows e para a abertura do BMR, incluindo todas as sub-tarefas, podem ser executados a partir do Assistente de restauração da máquina. Para obter informações sobre como abrir o assistente, consulte as etapas 1 a 5 de Como restaurar volumes a partir de um ponto de recuperação e, em seguida, consulte Sobre como realizar um bare metal restore usando o Assistente de restauração de máquina.
- Como verificar uma Restauração “bare metal”. Depois de iniciar a restauração “bare metal”, você pode verificar e monitorar o andamento. Consulte Confirmar uma bare metal restore.
  - Você pode monitorar o andamento da sua restauração. Consulte Visualizar o progresso da recuperação.
  - Depois de concluído, você pode iniciar o servidor restaurado. Consulte Iniciar um servidor de destino restaurado
  - Solução de problemas do processo BMR. Consulte Como solucionar problemas de conexão com o Universal Recovery Console e Como reparar problemas de inicialização.

Pré-requisitos para realizar uma restauração sem sistema operacional para uma máquina Windows

Antes de iniciar o processo de realização de uma bare metal restore de uma máquina com Windows, é preciso garantir que as seguintes condições e critérios estejam presentes:

- Uma CPU (unidade de processamento central) de 64 bits. O CD de inicialização do Rapid Recovery contém o sistema operacional Win 5.1 PE. Os BMRs do Rapid Recovery não são compatíveis com CPUs x86. Você só pode executar um BMR em uma CPU de 64 bits.

NOTA: Esse requisito é novo a partir da versão 6.0.

- Cópias de segurança da máquina que você deseja restaurar. É preciso ter um Rapid Recovery Core funcional que contenha pontos de recuperação do server protegido que você deseja restaurar
- Hardware para restaurar (novo ou antigo, similar ou não). A máquina de destino deve atender aos requisitos de instalação de um agente; para obter detalhes, consulte o *Guia de instalação e atualização do Dell Data Protection | Rapid Recovery*.
- Software e mídia de imagem. É preciso ter um CD ou DVD virgem e um software de gravação de disco ou de criação de imagem ISO. Se gerenciar máquinas remotamente usando software de computação de rede virtual, como o UltraVNC, você precisará ter também o VNC Viewer.
- Drivers do adaptador de rede e de armazenamento compatíveis. Se a restauração for para hardware diferente, é preciso ter drivers de armazenamento compatíveis e drivers do adaptador de rede para a máquina de destino, incluindo drivers de RAID, AHCI e chipset, conforme o caso.
- Partições e espaço de armazenamento, conforme apropriado. Certifique-se que há espaço suficiente no disco rígido para criar partições de destino na máquina de destino que conterá os volumes de origem. Todas as partições de destino devem ser pelo menos do mesmo tamanho da partição de origem original.
- Partições compatíveis. Sistemas operacionais Windows 8, Windows 8.1, Windows 10, Windows Server 2012 e Windows Server 2012 R2 inicializados a partir de partições FAT32 EFI disponíveis para proteção ou recuperação, bem como volumes ReFS (Resilient File System). As partições UEFI são tratadas como simples volumes FAT32. Transferências incrementais são totalmente suportadas e protegidas. O Rapid Recovery fornece suporte de sistemas UEFI para BMR, incluindo discos GPT de particionamento automático.

Sobre como realizar um bare metal restore usando o Assistente de restauração de máquina

Gerenciar uma imagem de inicialização do Windows através do assistente inclui as seguintes ações:

- Iniciar o criação do CD de inicialização.
- Definir o caminho para a imagem na máquina Core.
- Selecionar o ambiente de recuperação adequado para o hardware que você quer restaurar.

- Opcionalmente, definir os parâmetros de conexão para o agente restaurado com o objetivo de usar a rede ou o UltraVNC.
- Opcionalmente, injetar drivers para o hardware que você quer restaurar.
- Opcionalmente, transferir a imagem de inicialização para uma mídia física.
- Inicializar a máquina com os dados que você deseja restaurar a partir do CD.
- Conectar-se ao Universal Recovery Console.
- Mapear volumes.
- Iniciar o bare metal restore do ponto de recuperação selecionado no Core.

NOTA: Esse processo descreve como gerenciar uma imagem do CD de inicialização do assistente de Restauração de máquinas como parte do processo para realizar uma BMR utilizando esse assistente. Também é possível gerenciar uma imagem de inicialização da caixa de diálogo Criar CD de inicialização. Para obter informações sobre o gerenciamento de uma imagem do CD de inicialização fora do assistente de Restauração de máquinas, consulte Entender a criação do CD de inicialização para máquinas Windows.

Realizar um bare metal restore usando o Assistente de restauração de máquina

Você pode usar o Assistente de restauração para criar um CD de inicialização, bem como executar um bare metal restore (BMR).

Antes de realizar uma BMR, consulte Pré-requisitos para realizar uma restauração sem sistema operacional para uma máquina Windows ou Pré-requisitos para realizar uma bare metal restore em máquinas Linux, conforme adequado. Se for iniciar uma BMR para uma máquina com Windows a partir do Core Console, consulte Como executar uma restauração "bare metal" em máquinas Windows.

A máquina protegida deve ter o software Agent instalado e deve ter pontos de recuperação a partir dos quais você realizará a operação de restauração.

1 Para restaurar um volume em uma máquina protegida, navegue até o Core Console e clique em **Restaurar** na barra de botões do Rapid Recovery.

O Assistente de restauração de máquinas é exibido.

2 Na página Máquinas, selecione a máquina protegida que deseja restaurar e clique em **Avançar**.

Aparece a página Pontos de recuperação.

3 Selecione o ponto de recuperação que você quer usar para restaurar a máquina.

- Como opção, se quiser limitar a quantidade de pontos de recuperação exibidos, você pode filtrar por volumes (se definidos) ou por data de criação do ponto de recuperação. Você pode também procurar por um determinado ponto de recuperação.

4 Clique em **Avançar**.

5 Na página Destino, selecione **Recuperar em qualquer máquina de destino usando um CD de inicialização**.

- Se você ainda não tiver sido carregado um CD de inicialização na máquina que você quer restaurar, clique em **Avançar** e, em seguida, continue na Etapa 6.
- Se você já tiver carregado um CD de inicialização na máquina de destino BMR, selecione **Eu já tenho um CD de inicialização em execução na máquina de destino**, clique em **Avançar** e, em seguida, vá para a Etapa 16.

6 Na página CD de inicialização, no campo de texto Caminho de saída, digite o caminho onde a imagem ISO do CD de inicialização deve ser armazenada.

NOTA: Se a unidade compartilhada na qual você deseja armazenar a imagem estiver com pouco espaço em disco, você pode criar um disco conforme necessário no caminho; por exemplo, F:\filename.iso.

NOTA: A extensão do arquivo deve ser .iso. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen, barra invertida (apenas como delimitador de caminho) e ponto (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

7 Como opção, para definir os parâmetros de rede para o computador de destino ou para adicionar recursos do UltraVNC, selecione **Exibir opções avançadas** e execute o seguinte procedimento:

- Para estabelecer uma conexão de rede com o destino BMR, selecione **Use o seguinte endereço IP** e digite as informações conforme descrito na tabela a seguir.

Tabela 153. Opções de conexão de rede

Opção	Descrição
Endereço IP	O endereço IP da máquina restaurada.
Máscara de sub-rede	A máscara de sub-rede da máquina restaurada.
Gateway padrão	Especifique o gateway padrão da máquina restaurada.
Servidor DNS	Especifique o server de nome de domínio da máquina restaurada.

- Se você já tiver uma conta do UltraVNC e gostaria de usá-la para concluir a BMR, selecione **Adicionar UltraVNC** e, em seguida, digite as informações descritas na tabela a seguir.

Tabela 154. Credenciais de conexão com o UltraVNC

Opção	Descrição
Senha	A senha da sua conta UltraVNC.
Port	A porta que você quer usar para se conectar ao destino BMR. A porta padrão é 5900.

8 Clique em **Avançar**.

9
- Para estabelecer uma conexão de rede para a máquina restaurada, selecione **Use o seguinte endereço IP**, como descrito na tabela a seguir.
- Para definir as informações de UltraVNC, selecione **Adicionar UltraVNC**, conforme descrito na tabela a seguir.

  Use essa opção se você precisar de acesso remoto ao console de recuperação. Não é possível efetuar login usando Microsoft Terminal Services enquanto o CD de inicialização é utilizado.

Tabela 155. Conexão UltraVNC

Opção	Descrição
Senha	Especifique uma senha para essa conexão UltraVNC.
Port	Especifique uma porta para essa conexão UltraVNC. A porta padrão é 5900.

10 Quando estiver satisfeito com suas seleções na página CD de inicialização, clique em **Avançar**.

11 Como opção, na página Injeção de drivers, se você pretende restaurar hardware diferente, injete o controlador de armazenamento adequado e outros drivers para o sistema de destino seguindo as etapas:

a Baixe os drivers no website do fabricante do servidor e descompacte-os.

b Compacte cada driver em um arquivo .zip, usando um utilitário de compressão adequado (por exemplo, WinZip).

c Na página Injeção de drivers do Assistente de restauração de máquina, clique em **Adicionar um arquivo de drivers**.

d Navegue pelo sistema de arquivamento para localizar o arquivo do driver compactado, selecione-o e clique em **Abrir**.

e Repita a Etapa c e a Etapa d, conforme o caso, até injetar todos os drivers necessários.

Para obter mais informações sobre como injetar drivers, consulte Entender a injeção de drivers em um CD de inicialização.

NOTA: Nem todas as versões do Windows são compatíveis com a injeção automática de drivers. Se o seu sistema operacional não for compatível, salve manualmente os drivers em C:\Program Files\AppRecovery\Core\BootCdKit\Drivers\.

O Rapid Recovery cria a imagem ISO do CD de inicialização.

12 Clique em **Avançar**.

13 Inicie a máquina de destino BMR e, em seguida, siga uma das opções:

- Se você pode inicializar a máquina de destino da imagem ISO do CD de inicialização, faça-o agora.
- Caso não seja possível, copie a imagem ISO para uma mídia física (um CD ou um DVD), carregue o disco na máquina de destino, configure a máquina para carregar a partir do CD de inicialização e reinicie a partir do CD de inicialização.

NOTA: Talvez seja necessário alterar as definições de BIOS da máquina de destino para garantir que o volume carregado primeiro seja o CD de inicialização.

A máquina de destino, quando iniciada a partir do CD de inicialização, exibe a interface do Universal Recovery Console (URC). Esse ambiente é usado para restaurar a unidade do sistema ou volumes selecionados diretamente do Rapid Recovery Core. Observe o endereço IP e as credenciais da chave de autenticação no URC, que são atualizados cada vez que é feita uma inicialização a partir do CD de inicialização.

14 Na página Conexão do Assistente de restauração de máquina no Core Console, digite as informações de autenticação da instância URC da máquina que você deseja restaurar da seguinte maneira:

Tabela 156. Opções de autenticação

Opção	Descrição
Endereço IP	O endereço IP fornecido no URC na máquina de destino.
Chave de autenticação	A chave de autenticação fornecida no URC na máquina de destino.

15 Clique em **Avançar**.

16 Na página Mapeamento de disco, se você quiser mapear os volumes manualmente, vá para a Etapa 10. Caso queira mapear os volumes automaticamente, execute as etapas a seguir:

a No menu suspenso Mapeamento de volume, selecione **Automático**.

b Na lista de volumes, certifique-se de que os volumes que você quer restaurar estão selecionados. Todos os dispositivos estão selecionados por padrão.

Se você não quiser restaurar um volume relacionado, desmarque a opção.

NOTA: Pelo menos um volume deve ser selecionado para realizar a restauração.

c No lado direito, selecione o disco de destino para a restauração.

d Clique em **Avançar**.

e Na página Visualização de mapeamento de disco, revise os parâmetros das ações de restauração selecionadas.

f Vá para a Etapa 18.

17 Para mapear volumes manualmente, na página Mapeamento de disco, execute as seguintes etapas:

a No menu suspenso Mapeamento de volume, selecione **Manual**.

b Na coluna Destino, selecione um volume de destino que você quer restaurar. Como opção, se você não deseja restaurar um volume relacionado, desmarque a opção.

NOTA: Pelo menos um volume deve ser selecionado para realizar a restauração.

18 Clique em **Concluir**.

CUIDADO: Todas as partições e dados atuais na unidade de destino serão removidos permanentemente e substituídos pelo conteúdo do ponto de recuperação selecionado, incluindo o sistema operacional e todos os dados.

19 Se os volumes que deseja restaurar contiverem bancos de dados do SQL ou Microsoft Exchange, e se você estiver realizando uma Live Restore, na página Desmontar bancos de dados, será solicitado que você os desmonte. Como opção, se você quiser remontar esses bancos de dados após a restauração ser concluída, selecione **Remontar automaticamente todos os bancos de dados após o ponto de recuperação ser restaurado**.

20 Clique em **Restaurar**.

21 Na mensagem de status, clique em **OK** para confirmar que o processo de restauração foi iniciado.

A restauração será iniciada. É possível monitorar o progresso na página Eventos. Para obter mais informações, consulte Como exibir eventos usando tarefas, alertas e registros.

Entender a criação do CD de inicialização para máquinas Windows

A restauração sem sistema operacional para Windows exige uma imagem de inicialização chamada de CD de inicialização, criada pela definição de parâmetros no Rapid Recovery Core Console. Essa imagem é adaptada às suas necessidades específicas. Use a imagem para iniciar a máquina de destino do Windows. Com base nas particularidades do seu ambiente, pode ser preciso transferir esta imagem para uma mídia física como um CD ou DVD. Você deve, então, carregar virtual ou fisicamente a imagem de inicialização e iniciar o server Windows a partir da imagem de inicialização.

A primeira etapa ao realizar uma bare metal restore (BMR) de uma máquina com Windows é criar o arquivo do CD de inicialização no Rapid Recovery Core Console. Trata-se de uma imagem ISO inicializável que contém a interface do Universal Recovery Console (URC) do Rapid Recovery, um ambiente usado para restaurar a unidade do sistema ou o server inteiro diretamente do Rapid Recovery Core.

A imagem ISO do CD de inicialização criada é adaptada à máquina que está sendo restaurada e, portanto, deve conter os drivers corretos de rede e de armazenamento em massa. Se for prevista a restauração em hardware diferente da máquina em que o ponto de recuperação se originou, inclua o controlador de armazenamento e outros drivers no CD de inicialização. Para obter informações sobre como injetar esses drivers no CD de inicialização, consulte Entender a injeção de drivers em um CD de inicialização.

Entender a injeção de drivers em um CD de inicialização

A imagem de CD de inicialização exige que os drivers de armazenamento reconheçam as unidades de server e os drivers do adaptador de rede a fim de se comunicarem com o Rapid Recovery Core pela rede.

Um conjunto genérico de drivers do controlador de armazenamento e de adaptador de rede do Windows 8.1 x64 é incluído automaticamente ao gerar um CD de inicialização para Windows. Isso atende aos requisitos de sistemas Dell mais recentes. Sistemas de outros fabricantes ou sistemas Dell mais antigos podem exigir uma injeção de drivers de controlador de armazenamento e de adaptador de rede ao criar o CD de inicialização. Se você descobrir que o CD de inicialização criado não contém os drivers necessários para executar a restauração, também poderá carregá-los na máquina de destino usando o URC. Para obter mais informações, consulte Carregar drivers usando o Universal Recovery Console.

Ao criar o CD de inicialização, a injeção de drivers é usada para facilitar a interoperabilidade entre o console de recuperação, o adaptador de rede e o armazenamento no server de destino.

Os dados restaurados a partir do ponto de recuperação incluem drivers para o hardware usado anteriormente. Se for feita uma bare metal restore para um hardware diferente, será preciso injetar também drivers do controlador de armazenamento no sistema operacional que está sendo restaurado usando o URC após os dados terem sido restaurados para a unidade. Isso permite que o sistema operacional restaurado seja inicializado usando o novo conjunto de hardware. Depois que o OS é inicializado após a restauração, é possível baixar e instalar os drivers adicionais necessários para que o OS possa interagir com seu novo hardware.

Criar uma imagem ISO do CD de inicialização

Um CD de inicialização é o termo que o Rapid Recovery usa para se referir ao local de armazenamento portátil da imagem ISO reservada para fazer uma bare metal restore (BMR). A imagem contém o Universal Recovery Console (URC) do Rapid Recovery.

Para executar uma BMR em uma máquina, você precisa iniciar a máquina do CD de inicialização, o qual iniciará o URC. O URC é o que torna possível conectar o destino da BMR ao local do ponto de recuperação que você quer usar para executar a restauração.

1. A partir do Rapid Recovery Core Console em que o servidor que você precisa restaurar é protegido, na barra de ícones, clique no menu Mais e, em seguida, clique em **CDs de inicialização**.
2. Na página CDs de inicialização, clique em **Criar CD de inicialização**.

   A caixa de diálogo Criar CD de inicialização é exibida.

3 Na caixa de diálogo Criar CD de inicialização, na caixa de texto **Caminho de saída**, insira o caminho onde deseja armazenar a imagem ISO do CD de inicialização.

NOTA: A extensão do arquivo deve ser .iso. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen, barra invertida (apenas como delimitador de caminho) e ponto (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

4 Em Opções de conexão, realize um dos procedimentos a seguir:

- Para obter o endereço IP dinamicamente usando o protocolo DHCP (Dynamic Host Configuration Protocol), selecione **Obter o endereço IP automaticamente**.
- Para especificar um endereço IP estático para o URC, selecione **Usar o seguinte endereço IP** e, em seguida, digite as seguintes informações:
  - Endereço IP
  - Máscara de sub-rede
  - Gateway padrão
  - Servidor DNS

NOTA: É preciso especificar todos esses quatro campos.

5 Se você necessita de acesso remoto para o console de recuperação e você tiver o UltraVNC instalado, nas Opções de UltraVNC, execute as seguintes etapas:

NOTA: O UltraVNC permite que você gerencie o URC remotamente enquanto ele está em uso. Não é possível efetuar login usando Microsoft Terminal Services enquanto o CD de inicialização é utilizado.

a Selecione **Adicionar UltraVNC**.
b Digite sua **Senha de UltraVNC**.
c Digite a **Porta de UltraVNC**. A porta padrão é 5900.

NOTA: As Opções de UltraVNC só estão disponíveis se você já tiver o UltraVNC instalado. Para tornar essas opções disponíveis, vá para http://www.uvnc.com/downloads/ultravnc/ para fazer o download do UltraVNC versão 1.0.9.1 ou posterior para a arquitetura x64. Instale-o e salve o arquivo winvnc.exe em C:\Program Files\AppRecovery\Core\BootCdKit\UltraVnc_x64\.

6 Se você pretende restaurar hardware diferente, injete o controlador de armazenamento adequado e outros drivers para o sistema de destino seguindo as etapas:

NOTA: Nem todas as versões do Windows são compatíveis com a injeção automática de drivers. Se o seu sistema operacional não for compatível, salve manualmente os drivers em C:\Program Files\AppRecovery\Core\BootCdKit\Drivers\.

a Baixe os drivers no website do fabricante do servidor e descompacte-os.
b Compacte cada driver em um arquivo .zip, usando um utilitário de compressão adequado (por exemplo, WinZip).
c Na caixa de diálogo Criar CD de inicialização, no painel Drivers, clique em **Adicionar um arquivo de drivers**.
d Navegue pelo sistema de arquivamento para localizar o arquivo do driver compactado, selecione-o e clique em **Abrir**.
O arquivo do driver é exibido no painel Drivers da caixa de diálogo Criar CD de inicialização.
e Repita a Etapa c e a Etapa d, conforme o caso, até adicionar todos os drivers necessários.
f No painel Drivers, selecione os drivers que você quer injetar.

Para obter mais informações sobre a injeção de drivers, consulte Entender a injeção de drivers em um CD de inicialização.

7 Clique em **Criar CD de inicialização**.

O Rapid Recovery cria e salva o CD de inicialização com o nome do arquivo fornecido.

8 Para monitorar o andamento dessa tarefa, vá até a barra de ícones e clique no ícone Eventos.

Para obter mais informações sobre o monitoramento de eventos do Rapid Recovery, consulte Como exibir eventos usando tarefas, alertas e registros.

Ao concluir a criação da imagem ISO, um registro da imagem aparece na página Cds de inicialização, a qual você pode acessar do menu Mais na barra de ícones.

Para acessar a imagem ISO, navegue até o caminho de saída especificado ou clique no link da página CDs de inicialização para salvar a imagem em um local do qual seja possível carregá-la para o novo sistema; por exemplo, uma unidade de rede.

Como transferir a imagem ISO do CD de inicialização para a mídia

Quando você cria o arquivo de CD de inicialização, ele é armazenado como imagem ISO no caminho especificado. Você deve ser capaz de montar essa imagem como unidade no server no qual está realizando uma bare metal restore.

É possível gravar a imagem ISO do CD de inicialização em mídia de CD ou DVD acessível na inicialização do sistema.

Se a máquina for iniciada do CD de inicialização, o Universal Recovery Console será iniciado automaticamente.

Caso esteja realizando uma BMR em uma máquina virtual, esta etapa não é necessária. Basta carregar a imagem ISO em uma unidade e editar as definições dessa VM para iniciar essa unidade.

Como carregar o CD de inicialização e iniciar o computador de destino

Depois de criar a imagem do CD de inicialização, é preciso inicializar o server de destino com o CD de inicialização recém-criado.

Para se conectar ao Rapid Recovery Core Console ou usar o Chromium para download de drivers adicionais, você deve primeiro carregar um controlador e um adaptador de rede Ethernet. Para obter mais informações, consulte Carregar drivers usando o Universal Recovery Console.

NOTA: Se o CD de inicialização tiver sido criado usando DHCP, será preciso capturar o endereço IP e a senha.

1 No novo servidor, carregue a imagem do CD de inicialização do local apropriado e reinicie o servidor pela imagem do CD de inicialização para carregar o software do agente Rapid Recovery e o Win PE 5.1.

   O computador de destino mostra uma tela azul da Dell com três botões de ícone na parte superior da tela.

2 Para abrir a interface do usuário do Rapid Recovery Universal Recovery Console (URC), clique no ícone da Dell na parte superior da tela.

   O endereço IP e a senha da máquina são exibidos em Autenticação.

   NOTA: Uma nova senha temporária é gerada cada vez que a máquina é iniciada com o CD de inicialização. Anote o endereço IP exibido no painel Definições de adaptadores de rede e a senha de autenticação exibida no painel Autenticação. Você precisará dessas informações durante o processo de recuperação de dados para acessar novamente o console.

   NOTA: Se não houver endereço IP fornecido, carregue o controlador e o adaptador de rede Ethernet.

3 Caso queira alterar o endereço IP, selecione-o e clique em **Alterar**.

   NOTA: Se você tiver especificado um endereço IP na caixa de diálogo Criar CD de inicialização, o Universal Recovery Console o usará e exibirá na tela Definições de adaptadores de rede.

A máquina está pronta para você se conectar ao Core, selecione um ponto de recuperação e continue o processo sem sistema operacional.

Como usar o Universal Recovery Console para uma BMR

Antes de iniciar uma bare metal restore (BMR) em uma máquina com Windows, as seguintes condições devem ser satisfeitas:

- Para restaurar um ponto de recuperação salvo no Core, é necessário ter o hardware apropriado disponível. Para obter mais informações, consulte Pré-requisitos para realizar uma restauração sem sistema operacional para uma máquina Windows.
- A máquina com Windows de destino da BMR deve ser iniciada usando a imagem do CD de inicialização. Para obter mais informações, consulte Entender a criação do CD de inicialização para máquinas Windows.

Uma BMR inicia uma máquina usando um ponto de recuperação selecionado por você. O ponto de recuperação inclui drivers do hardware anterior. Se for feita uma restauração para um hardware diferente, será preciso injetar drivers do controlador de armazenamento no sistema operacional que está sendo restaurado usando o URC após os dados terem sido restaurados na unidade. Isso permite que o sistema operacional restaurado seja inicializado usando o novo conjunto de hardware. Depois de iniciar o SO, é possível baixar e instalar os drivers adicionais necessários que o SO precisa para interagir com seu novo hardware.

Para iniciar uma BMR no Rapid Recovery Core Console, realize as seguintes tarefas.

- Como selecionar um ponto de recuperação e iniciar uma BMR
- Sobre como mapear volumes para uma restauração sem sistema operacional
- Carregar drivers usando o Universal Recovery Console

Esse processo é uma etapa do Como executar uma restauração "bare metal" em máquinas Windows.

Sobre as ferramentas do Universal Recovery Console

O Universal Recovery Console (URC) inclui acesso a ferramentas que possam auxiliar na conclusão de uma bare metal restore (BMR).

Você pode encontrar as seguintes ferramentas clicando no ícone central na parte superior da tela inicial da Dell em um destino BMR de inicialização no URC:

- **Far Manager.** Essa ferramenta é semelhante ao Windows Explorer. Ela oferece uma maneira de procurar arquivos no servidor até concluir a BMR e instalar um sistema operacional com a própria função de navegação, como Windows Explorer.
- **Chromium.** Esse navegador tem fonte aberta para o Google Chrome™ e permite navegar na Internet em um servidor com um controlador de rede carregado por meio do URC.
- **PuTTY.** Essa ferramenta é um emulador de terminal de fonte aberta. No contexto de uma BMR Rapid Recovery, isso permite se conectar a um dispositivo de armazenamento NAS que não inclui uma interface de usuário. Esse recurso poderá ser necessário se você quiser restaurar de um arquivo e o arquivo estiver em um NAS.
- **Bloco de Notas.** Como em um sistema operacional Windows, essa ferramenta permite digitar notas não formatadas e exibir arquivos de log.
- **Gerenciador de Tarefas.** Como em um sistema operacional Windows, essa ferramenta permite gerenciar processos e monitorar o desempenho do servidor enquanto a restauração estiver em progresso.
- **Editor do Registro.** Como em um sistema operacional Windows, essa ferramenta permite alterar o Registro do sistema do destino BMR.
- **Prompt de comando.** Essa ferramenta permite executar comandos no destino BMR fora do URC até você instalar uma interface de usuário.

Carregar drivers usando o Universal Recovery Console

Esse recurso permite adicionar os drivers que não foram incluídos na imagem ISO, mas são necessários para uma bare metal restore bem-sucedida.

Essa tarefa é uma das etapas do Como executar uma restauração "bare metal" em máquinas Windows. Faz parte do processo de Como usar o Universal Recovery Console para uma BMR.

Ao criar um CD de inicialização, você pode adicionar drivers necessários à imagem ISO. Depois de inicializar a máquina de destino, você também pode carregar drivers de armazenamento ou de rede de dentro do Universal Recovery Console (URC).

Se você estiver restaurando em um hardware diferente, precisará injetar os drivers de controlador de armazenamento, RAID, AHCI, chipset e outros drivers se eles não estiverem no CD de inicialização. Esses drivers permitem que o sistema operacional opere com sucesso todos os dispositivos em seu server de destino depois que o sistema for reiniciado após o processo de restauração.

Execute as etapas de um dos procedimentos a seguir para carregar drivers usando o URC:

- Carregar drivers no Universal Recovery Console usando mídia portátil
- Como carregar um driver no URC usando o Chromium

Carregar drivers no Universal Recovery Console usando mídia portátil

As seguintes tarefas são pré-requisitos para este procedimento.

- Criar uma imagem ISO do CD de inicialização
- Como transferir a imagem ISO do CD de inicialização para a mídia
- Como carregar o CD de inicialização e iniciar o computador de destino

Execute o procedimento a seguir para usar um dispositivo de mídia portátil para carregar drivers no Universal Recovery Console (URC).

1 Em uma máquina conectada à Internet, baixe os drivers do site do fabricante para o servidor e descompacte-os.
2 Compacte cada driver em um arquivo .zip, usando um utilitário de compressão adequado (por exemplo, WinZip).
3 Copie e salve o arquivo .zip dos drivers em um dispositivo de mídia portátil, como, por exemplo, uma unidade USB.
4 Remova a mídia da máquina conectada e insira-a no server de destino de inicialização.
5 No servidor de destino, carregue o CD de inicialização e inicie a máquina.
A tela inicial da Dell é exibida.
6 Para iniciar o URC, clique no **ícone da Dell**.
O URC é aberto na guia do Gerenciador de driver do CD de inicialização.
7 Expanda a lista **Outros dispositivos**.
Essa lista mostra os drivers que são necessários para o hardware, mas que não estão incluídos no CD de inicialização.
8 Clique com o botão direito em um dispositivo da lista e, em seguida, clique em **Carregar driver**.
9 Na janela Selecionar modo de carregamento do driver, selecione uma das opções a seguir:
   - Carregar pacote de driver único (o driver será carregado sem verificação de suporte do dispositivo
   - Verificar pasta dos pacotes de driver (os drivers do dispositivo selecionado serão pesquisados na pasta selecionada)
10 Expanda a unidade do dispositivo de mídia portátil, selecione o driver (com a extensão de arquivo .inf) e clique em **OK**.
O driver é carregado no sistema operacional atual.
11 Na janela Informações, clique em **OK** para confirmar que o driver foi carregado com êxito.
12 Repita este procedimento conforme necessário para cada driver que você deseja carregar.

Como carregar um driver no URC usando o Chromium

As seguintes tarefas são pré-requisitos para este procedimento.

- Criar uma imagem ISO do CD de inicialização
- Como transferir a imagem ISO do CD de inicialização para a mídia
- Como carregar o CD de inicialização e iniciar o computador de destino

Conclua o procedimento a seguir para usar o navegador Chromium que vem instalado no CD de inicialização para carregar drivers enquanto estiver no URC.

1 No servidor de destino, carregue o CD de inicialização e inicie a máquina.
A tela inicial da Dell é exibida.
2 Para iniciar o URC, clique no **ícone da Dell**.
O URC é aberto na guia do Gerenciador de driver do CD de inicialização.
3 No destino BMR, clique nas ferramentas (ícone central) na parte superior da tela e em **Chromium**.
4 No navegador Chromium, navegue até um site onde você possa baixar o driver necessário.
5 Baixe o driver ou os drivers no local escolhido, como uma pasta local ou um compartilhamento de arquivos em rede.
6 Expanda a lista **Outros dispositivos**.
Essa lista mostra os drivers que são necessários para o hardware, mas que não estão incluídos no CD de inicialização.
7 Clique com o botão direito em um dispositivo da lista e, em seguida, clique em **Carregar driver**.

8 Na janela Selecionar modo de carregamento do driver, selecione uma das opções a seguir:
   - Carregar pacote de driver único (o driver será carregado sem verificação de suporte do dispositivo)
   - Examinar pasta em busca de pacotes de driver (os drivers do dispositivo selecionado são pesquisados na pasta selecionada)
9 Navegue até o local onde você salvou o driver, selecione o driver e clique em **OK**.
   O driver é carregado no sistema operacional atual.
10 Na janela Informações, clique em **OK** para confirmar que o driver foi carregado com êxito.
11 Repita este procedimento conforme necessário para cada driver que você deseja carregar.

Como selecionar um ponto de recuperação e iniciar uma BMR

Depois que o Universal Recovery Console (URC) estiver acessível no computador de destino da bare metal restore (BMR), você deverá selecionar o ponto de recuperação que você deseja restaurar.

Navegue até o Core Console para selecionar o ponto de recuperação que você deseja carregar e designar o console de recuperação como o destino dos dados restaurados.

NOTA: Essa etapa é necessária para realizar BMR em todas as máquinas com Windows e opcional para executar BMR em máquinas com Linux.

Essa tarefa é uma das etapas do Como executar uma restauração "bare metal" em máquinas Windows. Faz parte do processo de Como usar o Universal Recovery Console para uma BMR.

Em caso de realização de uma BMR para uma máquina Linux no Core Console, essa tarefa também é uma etapa em Realizar uma bare metal restore em máquinas Linux Faz parte do processo de Realizar uma bare metal restore em uma máquina Linux usando a linha de comando.

1 No Rapid Recovery Core Console, na lista de máquinas protegidas, clique no nome da máquina protegida que você deseja restaurar.
   A página Resumo da máquina selecionada é exibida.
2 Clique em **Pontos de recuperação**.
3 Próximo do ponto de recuperação que você deseja usar na BMR, clique no menu suspenso e em **Restaurar**.
   O Assistente de restauração de máquinas é exibido.
4 Selecione **Recuperar em qualquer máquina de destino usando um CD de inicialização**.
5 Selecione **Eu já tenho um CD de inicialização em execução na máquina de destino.**
   As caixas de texto de autenticação são exibidas.
6 Insira as informações sobre a máquina que você deseja restaurar conforme descrito na tabela a seguir.

Tabela 157. Informações da máquina de destino

Caixa de texto	Descrição
Endereço IP	O endereço IP da máquina na qual deseja restaurar. É idêntico ao endereço IP exibido no URC.
Chave de autenticação	A senha específica para se conectar ao server selecionado. É idêntico à chave de autenticação exibida no URC.

7 Clique em **Avançar**.
   Se as informações de conexão inseridas correspondem ao URC, e se o Core e o server de destino podem identificar um ao outro corretamente na rede, os volumes do ponto de recuperação selecionado são carregados, e a página Mapeamento de disco é exibida. Nesse caso, a próxima etapa é mapear volumes.
8 Vá até Sobre como mapear volumes para uma restauração sem sistema operacional para saber mais sobre as opções de mapeamento de disco.

Sobre como mapear volumes para uma restauração sem sistema operacional

Depois de se conectar ao Universal Recovery Console, você precisa mapear volumes entre aqueles relacionados no ponto de recuperação e os volumes existentes no hardware de destino.

O Rapid Recovery tenta mapear os volumes automaticamente. Se você aceitar o mapeamento padrão, o disco na máquina de destino será limpo e reparticionado e quaisquer dados anteriores serão excluídos. O alinhamento é realizado na ordem em que os volumes estão relacionados no ponto de recuperação e os volumes são alocados aos discos de forma adequada de acordo com o tamanho, e assim por diante. Supondo que haja espaço suficiente na unidade de destino, nenhum particionamento será necessário ao utilizar o alinhamento automático do disco. Um disco pode ser usado em diversos volumes. Se você mapear manualmente as unidades, observe que não poderá usar o mesmo disco duas vezes.

Para o mapeamento manual, é preciso ter a nova máquina corretamente formatada antes de restaurá-la. A máquina de destino deve ter uma partição separada para cada volume no ponto de recuperação, incluindo o volume reservado do sistema. Para obter mais informações, consulte Como usar o Universal Recovery Console para uma BMR.

Execute o procedimento para uma das seguintes opções de mapeamento de disco:

- Como mapear manualmente discos para uma BMR
- Mapear manualmente discos para obter uma BMR

CUIDADO: Embora o Rapid Recovery suporte as partições FAT32 e ReFS, atualmente, apenas a restauração completa e a BMR são suportadas, visto que existe uma limitação do driver com ReFS, de modo que a restauração é implementada em modo de usuário, exportação da VM, e assim por diante. Se um Core está protegendo pelo menos um volume agente que contém o sistema de arquivos ReFS, ele deve ser instalado em máquinas com Windows 8, Windows 8.1, Windows 10, Windows Server 2012 ou Windows Server 2012 R2, quem fornece suporte nativo ao formato ReFS. Caso contrário, a funcionalidade ficará limitada, e operações que envolvem tarefas, como a montagem de uma imagem de volume, não funcionarão. O Rapid Recovery Core Console apresentará as mensagens de erro aplicáveis a essas ocorrências.

CUIDADO: A bare metal restore da configuração de discos de espaços de armazenamento (um recurso do Windows 8.1) não é suportada. Para obter mais detalhes, consulte o *Guia de instalação e atualização doDell Data Protection | Rapid Recovery*.

Essa tarefa é uma das etapas do Como executar uma restauração "bare metal" em máquinas Windows. Faz parte do processo de Como usar o Universal Recovery Console para uma BMR.

Se for feita uma BMR em uma máquina com Linux no Core Console, essa tarefa também será uma etapa do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Iniciar uma restauração sem sistema operacional para Linux.

Como mapear manualmente discos para uma BMR

Esse procedimento permite mapear automaticamente discos durante uma bare metal restore (BMR) usando o Assistente de restauração de máquina.

Conclua as etapas no procedimento a seguir para selecionar automaticamente os volumes que você deseja recuperar e o local de restauração.

1 Na página Mapeamento de disco do Assistente de restauração de máquina, ao lado do mapeamento de volume, selecione **Automático** no menu suspenso.

2 Na tabela esquerda, verifique se os volumes apropriados estão listados e selecionados.

NOTA: Em geral, em uma BMR, deve-se restaurar, no mínimo, o volume reservado do sistema e o volume do sistema (em geral, mas nem sempre, o volume C:\). Você precisa selecionar pelo menos um volume para realizar uma BMR.

3 Na tabela direita, selecione o disco ou os discos para os quais você deseja mapear volumes no computador de destino.

4 Clique em **Avançar**.

5 Na página Visualização de mapeamento de disco, revise o mapeamento dos volumes do ponto de recuperação e o volume de destino da restauração.

6 Para começar a restauração, clique em **Concluir**.

> **CUIDADO: Se você selecionar Iniciar restauração, todas as partições e os dados existentes na unidade de destino serão removidos permanentemente e substituídos pelo conteúdo do ponto de recuperação selecionado, inclusive o sistema operacional e todos os dados.**

Mapear manualmente discos para obter uma BMR

Este procedimento descreve como designar que discos devem ser armazenados e em que locais na máquina restaurada.

Para mapear os discos manualmente, você precisa primeiro usar o DiskPart na linha de comando do computador de destino de BMR para criar e formatar volumes de destino. Para obter mais informações, consulte DiskPart Command-Line Options (Standard 7 SP1) na área de trabalho do desenvolvedor da Microsoft.

Execute as etapas do procedimento a seguir para selecionar manualmente os volumes que deseja restaurar e o local de restauração.

1 Na página de mapeamento disco do assistente de restauração de máquina, ao lado do mapeamento de volume, selecione **Manual** no menu suspenso.

> **NOTA: Se não existirem volumes na unidade da máquina para os quais você esteja realizando uma restauração sem sistema operacional (BMR), não será possível ver essa opção ou mapear os volumes manualmente.**

2 Na área Mapeamento de volume, em Volume de origem, confirme se o volume de origem está selecionado e se os volumes adequados estão relacionados abaixo dele e estão selecionados.

3 Em Destino, no menu suspenso, selecione o destino correto que é o volume de destino para realizar a restauração do ponto de recuperação sem sistema operacional e depois clique em **Restaurar**.

4 Na caixa de diálogo de confirmação, revise o mapeamento da origem do ponto de recuperação e do volume de destino da restauração.

5 Para iniciar a restauração, clique em **Iniciar restauração**.

> **CUIDADO: Se você selecionar Começar a restauração, todas as partições e dados existentes na unidade de destino serão removidos permanentemente e substituídos por conteúdo do ponto de recuperação selecionado, incluindo o sistema operacional e todos os dados.**

Como realizar uma BMR com base em um arquivo

O Rapid Recovery permite restaurar uma máquina sem sistema operacional usando um ponto de recuperação arquivado.

As seguintes tarefas são pré-requisitos para este procedimento.

- Criar uma imagem ISO do CD de inicialização
- Como carregar o CD de inicialização e iniciar o computador de destino

No Universal Recovery Console (URC), você pode acessar o Rapid Recovery Core e recuperar um ponto de recuperação. Você também pode optar por restaurar a máquina sem sistema operacional em um ponto de recuperação armazenado em um arquivo. O URC permite atingir esse arquivo, independentemente de estar em uma unidade local, um compartilhamento de rede ou uma conta de nuvem.

1 No URC, clique na guia **Restaurar do arquivo**.

2 Na lista suspensa **Tipo de local**, selecione o local do arquivo. Você pode escolher dentre as opções a seguir.
   - Local
   - Rede
   - Nuvem

3 Insira as credenciais descritas na tabela a seguir de acordo com a seleção do tipo de local.

Tabela 158. Opções de credenciais do tipo de local

Tipo de local	Opção	Descrição
Local	Caminho local	O local atual do arquivo.
Rede	Caminho de rede	O local atual do arquivo.
	Usuário	O nome de usuário para acesso do compartilhamento de rede.
	Senha	A senha para acesso do compartilhamento de rede.
Nuvem	Tipo de nuvem	O fornecedor do local de armazenamento da nuvem. Selecione uma das seguintes opções: • Microsoft Azure • Amazon™ S3 • Fornecido pelo OpenStack • Arquivos do Rackspace® Cloud

4 Se você tiver selecionado um tipo de nuvem, complete as credenciais pertencentes ao fornecedor de nuvem.

- Para o Microsoft Azure, conclua as seguintes etapas:
  1 Insira as seguintes credenciais:
    - Nome da conta de armazenamento
    - Chave de acesso
  2 Para o nome Contêiner, na lista suspensa, selecione um contêiner.
  3 Para o caminho da nuvem, na lista suspensa, selecione o caminho do arquivo.
- Para o Amazon™ S3, conclua as etapas a seguir
  1 Insira as seguintes credenciais:
    - Chave de acesso
    - Chave secreta
  2 Para o nome Contêiner, na lista suspensa, selecione um contêiner.
  3 Para o caminho da nuvem, na lista suspensa, selecione o caminho do arquivo.
- Para contas Desenvolvido com o OpenStack ou Arquivos do Rackspace Cloud, conclua as seguintes etapas:
  1 Especifique as seguintes informações:
    - Região
    - Usuário
  2 Selecione uma das opções a seguir:
    - Senha
    - Chave API
  3 Na caixa de texto, insira as informações com base na seleção na Etapa c.
  4 Especifique as seguintes informações:
    - ID do locatário
    - URL de autenticação
    - Nome do contêiner
    - Caminho da nuvem

5 Clique em **Avançar**.

6 Na página **Máquinas**, selecione a máquina que deseja restaurar e clique em **Avançar**.

7 Na página **Pontos de recuperação**, selecione o ponto de recuperação que você deseja usar para restaurar a máquina e clique em **Avançar**.

8 Na página **Mapeamento**, selecione uma das seguintes opções e conclua as etapas correspondentes:

- Na lista suspensa **Mapeamento de volume**, selecione **Automático**.

1 Na tabela esquerda, verifique se os volumes apropriados estão listados e selecionados.

NOTA: Em geral, em uma BMR, deve-se restaurar, no mínimo, o volume reservado do sistema e o volume do sistema (em geral, mas nem sempre, o volume C:\). Você precisa selecionar pelo menos um volume para realizar uma BMR.

2 Na tabela direita, selecione o disco ou os discos para os quais você deseja mapear volumes no computador de destino.

- No menu suspenso **Mapeamento de volume**, selecione **Manual**.

NOTA: Para mapear os discos manualmente, você precisa primeiro usar o DiskPart na linha de comando para criar e formatar volumes de destino. Para obter mais informações, consulte DiskPart Command-Line Options (Standard 7 SP1) na área de trabalho do desenvolvedor da Microsoft.

NOTA: Se não existirem volumes na unidade da máquina para os quais você esteja realizando uma restauração sem sistema operacional (BMR), não será possível ver essa opção ou mapear os volumes manualmente.

- Em **Volumes de destino**, no menu suspenso, selecione o volume de destino adequado para cada volume no ponto de recuperação.

9 Na caixa de texto **Caminho de mapas de montagem**, digite um destino para o armazenamento temporário de mapeamento arquivos.

O local padrão é X:\ProgramData\AppRecovery\IndexEntriesMaps.

NOTA: Para garantir que o destino tenha espaço livre suficiente, divida a capacidade de volume total da montagem por 1.024. Por exemplo, usando-se a fórmula `(Mount volume total capacity) / 1024 = Free space,1 TB / 1024 = 1 GB`.

10 Clique em **Restaurar**.

O URC mapeia os volumes para os novos discos.

11 Clique em **Restaurar**.

O URC restaura os dados para o computador de destino. Você pode visualizar o progresso na guia **Progresso da restauração**.

12 Depois que a restauração estiver concluída, remova o CD de inicialização.

13 Para inicializar o computador de destino BMR no Windows, reinicie a máquina.

Carregar os drivers no sistema operacional

Este procedimento descreve como carregar drivers no sistema operacional em um destino bare metal restore (BMR).

Para injetar drivers no sistema operacional, as seguintes tarefas já precisam ter sido realizadas:

- Criado um CD de inicialização usando o Boot CD Builder do Rapid Recovery Core Console. Para obter mais informações, consulte Criar uma imagem ISO do CD de inicialização.
- Carregado o CD de inicialização no destino BMR. Para obter mais informações, consulte Como carregar o CD de inicialização e iniciar o computador de destino.
- Carregado todos os drivers ou controladores necessários para armazenamento e rede. Para obter mais informações, consulte Carregar drivers usando o Universal Recovery Console.
- Realizado uma restauração usando o Assistente de restauração de máquina no Rapid Recovery Core Console ou um arquivamento a partir do Universal Recovery Console. Para obter mais informações, consulte Realizar um bare metal restore usando o Assistente de restauração de máquina e Como realizar uma BMR com base em um arquivo.

Depois de executar uma restauração, o processo não estará completo até que você injete os drivers para o sistema operacional no destino bare metal restore (BMR). Essa tarefa é adicional ao carregamento dos drivers no URC.

1 Depois de clicar em Restauração no procedimento BMR de sua escolha (veja os pré-requisitos), clique na guia **Gerenciamento de driver do Windows existente**.

2 Na lista suspensa, selecione um sistema operacional.

O URC procura os drivers disponíveis.

3 Para carregar drivers adicionais, clique em **Forçar carregamento**.

4 Navegue pelo sistema de arquivamento para localizar o arquivo do driver compactado e selecione-o.

5 Clique em **OK**.

O URC carrega o driver no sistema operacional que você selecionou.

6 Repita a Etapa 3 até a Etapa 5 para cada driver adicional que você precisar carregar.

7 Reinicie o computador de destino BMR.

A BMR terminou. Se você tiver qualquer problema ao reinicializar, consulte Como reparar problemas de inicialização.

Realizar uma bare metal restore em máquinas Linux

No Rapid Recovery, você pode realizar uma bare metal restore (BMR) em uma máquina Linux, inclusive uma restauração do volume do sistema. Ao restaurar uma máquina com Linux, você irá reverter para o ponto de recuperação do volume de inicialização. A funcionalidade BMR tem suporte usando-se a linha de comando `local_mount` e dentro da UI do Core Console.

CUIDADO: Antes de iniciar o processo de BMR, certifique-se de que a máquina Linux que você deseja restaurar não inclui uma partição de inicialização ext2. Quando a BMR é realizada em uma máquina com o tipo de partição ext2, o processo normalmente resulta em uma máquina que não inicia. Para realizar uma BMR nesse caso, você teria que converter quaisquer partições ext2 para ext3, ext4 ou XFS antes de começar a proteger e criar cópias de segurança da máquina.

CUIDADO: Quando você inicializa uma máquina Linux restaurada pela primeira vez após uma BMR, o Rapid Recovery gera uma imagem de base da máquina restaurada. Dependendo da quantidade de dados na máquina, esse processo leva mais tempo do que a criação de um snapshot incremental. Para obter mais informações sobre imagens de base e snapshots incrementais, consulte Noções básicas sobre programações de proteção.

Para realizar uma bare metal restore em máquinas com Linux, realize as tarefas a seguir.

- Gerenciamento de uma imagem de inicialização do Linux. Essa imagem ISO do DVD de inicialização Linux Live é usada para iniciar a unidade de destino, a partir da qual é possível acessar o Universal Recovery Console para se comunicar com as cópias de segurança no Core. Consulte Gerenciar uma imagem de inicialização do Linux.
  - Para obter a imagem de inicialização da BMR, você deve primeiro determinar de qual imagem precisa e baixá-la no Portal de licenças. Consulte Sobre a imagem ISO de inicialização para Linux seguido de Baixar uma imagem ISO de inicialização para Linux.
  - Se você precisar de mídia física para iniciar a máquina Linux de destino, precisará transferir a imagem ISO para a mídia. Consulte Salvar a imagem ISO do Live DVD em mídia.
  - Em todos os casos, será preciso carregar a imagem de inicialização no server de destino e iniciar o server da imagem de inicialização. Consulte Carregar o Live DVD e iniciar o computador de destino.
  - Depois de carregar a mídia, você deverá conectar a máquina Linux ao Rapid Recovery Core. Consulte Conectar-se ao destino BMR a partir do Rapid Recovery Core.
- Gerenciamento de partições. Pode ser necessário criar ou montar as partições antes de realizar uma BMR em uma máquina com Linux. Consulte Como gerenciar partições do Linux.
  - O sistema Linux no qual você está realizando uma BMR deve ter as mesmas partições dos volumes de origem no ponto de recuperação. Talvez seja necessário criar partições adicionais no sistema de destino. Consulte Criar partições na unidade de destino.
  - Se estiver sendo feita uma BMR manual, será preciso primeiro montar partições. Consulte Montar partições a partir da linha de comando. As etapas para montar partições estão incluídas no processo de realização da BMR na linha de comando. Consulte Realizar uma bare metal restore em uma máquina Linux usando a linha de comando.

    Se você usar particionamento automático para BMR no Core Console, não precisará montar partições. O Rapid Recovery restaurará as mesmas partições incluídas nos pontos de recuperação que estão sendo restaurados.
- Iniciar uma bare metal restore para Linux. Depois que a máquina de destino é iniciada da imagem de inicialização do Live DVD, é possível iniciar a BMR. As tarefas obrigatórias dependem da realização disso na interface do usuário do Rapid Recovery ou na linha de comando usando-se o utilitário local_mount. Consulte Iniciar uma restauração sem sistema operacional para Linux.
  - Se for usado o Core Console, será preciso iniciar uma restauração em um ponto de recuperação do Core. Consulte Como selecionar um ponto de recuperação e iniciar uma BMR.
  - Se for usado o Core Console, será preciso mapear os volumes na UI. Consulte Sobre como mapear volumes para uma restauração sem sistema operacional.
  - Como opção, ao restaurar da linha de comando, você poderá usar o utilitário de tela para melhorar sua capacidade de rolar e ver os comandos no console do terminal. Esse utilitário é aberto por padrão. Se fechá-lo, você poderá iniciá-lo novamente. Para obter mais informações, consulte Iniciar o utilitário Screen.
  - Se você estiver usando local_mount, todas as tarefas serão realizadas na linha de comando. Para obter mais informações, consulte Realizar uma bare metal restore em uma máquina Linux usando a linha de comando.

- Confirmação de um bare metal restore. Após iniciar o procedimento de bare metal restore, você pode confirmar e monitorar o progresso. Consulte Confirmar a restauração sem sistema operacional na linha de comando.
  - É possível monitorar o progresso de sua restauração. Consulte Visualizar o progresso da recuperação.
  - Depois de concluída, você pode iniciar o server restaurado. Consulte Iniciar um servidor de destino restaurado.
  - Solucionar problemas do processo de BMR. Consulte Como solucionar problemas de conexão com o Universal Recovery Console e Como reparar problemas de inicialização.

Pré-requisitos para realizar uma bare metal restore em máquinas Linux

Antes de iniciar o processo de realização de uma bare metal restore em uma máquina com Linux, é preciso garantir que as seguintes condições e critérios estejam presentes:

- Cópias de segurança da máquina que você deseja restaurar. É preciso ter um Rapid Recovery Core funcional que contenha pontos de recuperação do server protegido que você deseja restaurar.
- Hardware para restaurar (novo ou antigo, similar ou não). A máquina de destino deve atender aos requisitos de instalação de um agente; para obter mais detalhes, consulte o Guia de instalação e atualização do Rapid Recovery.
- Imagem de inicialização do Live DVD. Obtenha a imagem ISO do Linux Live DVD, que inclui uma versão inicializável do Linux. Baixe do Dell Data Protection | Portal de licenças do Rapid Recovery em https://licenseportal.com. Se houver problemas para baixar o Live DVD, entre em contato com o Suporte do Rapid Recovery da Dell.
- Software e mídia de imagem. Se usar mídia física, é preciso ter um CD ou DVD virgem e um software de gravação de disco ou de criação de imagem ISO.
- Drivers do adaptador de rede e de armazenamento compatíveis. Se a restauração for para hardware diferente, é preciso ter drivers de armazenamento compatíveis e drivers do adaptador de rede para a máquina de destino, incluindo drivers de RAID, AHCI e chipset para o sistema operacional de destino, conforme o caso.
- Partições e espaço de armazenamento, conforme apropriado. Certifique-se que há espaço suficiente no disco rígido para criar partições de destino na máquina de destino que conterá os volumes de origem. Todas as partições de destino devem ser pelo menos do mesmo tamanho da partição de origem original.
- Restaurar caminho. Identifique o caminho da restauração, que é o caminho do descritor de arquivo de dispositivo. Para identificar o caminho do descritor de arquivo de dispositivo, use o comando`fdisk` de uma janela de terminal.

Gerenciar uma imagem de inicialização do Linux

Uma restauração sem sistema operacional para Linux exige uma imagem de inicialização do Live DVD, que pode ser baixada no Dell Data Protection | Portal de licenças do Rapid Recovery. Use essa imagem para iniciar a máquina de destino com Linux. Com base nas particularidades do seu ambiente, pode ser preciso transferir esta imagem para uma mídia física como um CD ou DVD. Você deve, então, carregar virtual ou fisicamente a imagem de inicialização e iniciar o server Linux a partir da imagem de inicialização.

NOTA: O Live DVD era conhecido anteriormente como Live CD.

O gerenciamento de uma imagem de inicialização do Linux é uma etapa em Realizar uma bare metal restore em máquinas Linux.

Você pode realizar as seguintes tarefas:

Sobre a imagem ISO de inicialização para Linux

A primeira etapa ao realizar uma bare metal restore (BMR) em uma máquina com Linux é baixar a imagem ISO do Live DVD para Linux do Dell Data Protection | Portal de licenças do Rapid Recovery. O Live DVD funciona com todos os sistemas de arquivo Linux suportados pelo Rapid Recovery, e inclui uma versão inicializável do Linux, um utilitário de tela e a interface do Universal Recovery Console (URC) do Rapid Recovery. O Universal Recovery Console do Rapid Recovery é um ambiente usado para restaurar a unidade do sistema ou o server inteiro diretamente do Rapid Recovery Core.

NOTA: A Organização Internacional de Padronização (ISO) é um órgão internacional de representantes de diversas organizações nacionais que define padrões para sistemas de arquivos. ISO 9660 é uma norma de sistema de arquivos usada em mídia de disco óptico para troca de dados, e ela suporta vários sistemas operacionais. Uma imagem ISO é a imagem de disco ou arquivo, que contém dados para todos os setores do disco, bem como o sistema de arquivos do disco.

Baixar uma imagem ISO de inicialização para Linux

É preciso baixar a imagem ISO do Live DVD que corresponde à sua versão do Rapid Recovery. A versão atual do Live DVD está disponível no Dell Data Protection | Portal de licenças do Rapid Recovery em https://licenseportal.com. Se você precisar de uma versão diferente, entre em contato com o Suporte do Rapid Recovery da Dell

NOTA: Para obter mais informações sobre o Dell Data Protection | Portal de licenças do Rapid Recovery, consulte o Guia do usuário do portal de licenças Dell Data Protection | Portal de licenças do Rapid Recovery.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Gerenciar uma imagem de inicialização do Linux.

Execute as etapas deste procedimento para baixar a imagem ISO do Live DVD.

1. Faça logon no Dell Data Protection | Portal de licenças do Rapid Recovery emhttps://licenseportal.com.
2. Acesse a área Downloads.
3. Role para baixo até Aplicativos com base em Linux e, na seção do Live DVD para Linux, clique em **Baixar**.
4. Salve a imagem ISO do Live DVD. Se você estiver restaurando uma máquina virtual, poderá salvá-la em um local de rede e definir a VM para iniciar da unidade de CD ou DVD associada à imagem ISO.
5. Se a restauração for de uma máquina física, grave a imagem ISO do CD de inicialização em um CD ou DVD a partir do qual a máquina de destino pode ser iniciada. Para obter mais informações, consulte Salvar a imagem ISO do Live DVD em mídia.

Salvar a imagem ISO do Live DVD em mídia

Quando você baixa o arquivo do Live DVD para Linux, ele é armazenado como imagem ISO no caminho especificado. Você deve ser capaz de inicializar a máquina Linux de destino com a imagem do Live DVD.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Gerenciar uma imagem de inicialização do Linux.

Grave a imagem ISO do CD de inicialização em mídia de CD ou DVD.

Caso esteja realizando uma BMR em uma máquina virtual, esta etapa não é necessária. Basta carregar a imagem ISO em uma unidade e editar as definições de máquina dessa VM para iniciar essa unidade. Você também pode usar a exportação virtual para restaurar uma VM Linux. Para obter mais informações, consulte Exportação de VM.

Carregar o Live DVD e iniciar o computador de destino

Depois de obter a imagem ISO do Live DVD, é preciso iniciar a máquina Linux com o Live DVD recém-criado.

Essa tarefa é uma etapa em Como realizar uma restauração sem sistema operacional de máquinas Linux. Ela faz parte do processo Como gerenciar uma imagem de inicialização Linux.

1. Navegue até o novo server e carregue a imagem do Live DVD a partir do local apropriado. Especifique se o server será iniciado da imagem do Live DVD.
2. Inicie a máquina.

   É exibida uma tela de abertura do Rapid Recovery e uma janela de terminal se abre, exibindo o endereço IP e a senha de autenticação da máquina.

   NOTA: Uma nova senha temporária é gerada cada vez que a máquina é iniciada com a imagem do Live DVD.
3. Anote o endereço IP e a senha de autenticação exibidos na tela de introdução. Você precisará dessas informações durante o processo de recuperação de dados para acessar novamente o console.

Conectar-se ao destino BMR a partir do Rapid Recovery Core

Depois de iniciar a máquina Linux de destino com o Live DVD, essa máquina ficará pronta para o usuário se conectar a ela a partir do Core e iniciar o processo de bare metal restore. É possível realizar esse processo usando um de dois métodos:

- Iniciar uma restauração a partir do Rapid Recovery Core Console. Para obter mais informações, consulte Iniciar uma restauração sem sistema operacional para Linux.
- Ativação de uma restauração a partir da linha de comando usando o utilitário aamount. Para obter mais informações, consulte Realizar uma bare metal restore em uma máquina Linux usando a linha de comando.

Como gerenciar partições do Linux

Ao realizar uma BMR, a unidade de destino na qual você restaurará os dados deve ter as mesmas partições do ponto de recuperação que está sendo restaurado. Talvez seja necessário criar partições para atender a esse requisito.

Você pode iniciar a restauração na linha de comando usando o utilitário aamount ou no Rapid Recovery Core Console. Se a restauração for feita usando a interface com o usuário, primeiro será preciso montar as partições.

O gerenciamento de partições no Linux é uma das etapas do Realizar uma bare metal restore em máquinas Linux.

Você pode realizar as seguintes tarefas:

Links relacionados

Criar partições na unidade de destino
Formatar partições na unidade de destino
Montar partições a partir da linha de comando

Criar partições na unidade de destino

Muitas vezes, ao fazer uma BMR, a unidade de destino é um novo volume que pode ser composto de uma única partição. A unidade na máquina de destino deve ter a mesma tabela de partições do ponto de recuperação, incluindo o tamanho dos volumes. Se a unidade de destino não contiver as mesmas partições, será preciso criá-las antes de realizar a bare metal restore. Use o utilitário fdisk para criar partições na unidade de destino iguais às partições na unidade de origem.

CUIDADO: O procedimento abaixo é apenas um exemplo. Ambientes de clientes são diferentes. Você deve alterar os comandos que usa de acordo com os aspectos específicos do ambiente.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Como gerenciar partições do Linux.

1 Como opção, você pode usar o utilitário Screen. Esse utilitário é iniciado por padrão e permanece ativo até você reinicializar a máquina.

NOTA: Se você fechá-lo explicitamente e quiser reabri-lo, consulte Iniciar o utilitário Screen.

2 Na linha de comando, insira o seguinte comando e pressione **Enter** para alterar os privilégios para execução como administrador e depois relacionar as partições de disco existentes:

```
sudo fdisk -l
```

Uma lista com todos os volumes é exibida.

Esse exemplo supõe que o volume que você deseja particionar é /dev/sda. Se seu volume é diferente (por exemplo, em unidades mais antigas, pode ser /dev/hda), altere os comandos adequadamente.

3 Para criar uma nova partição de inicialização, insira o seguinte comando e pressione **Enter**:

```
sudo fdisk /dev/sda
```

4 Para criar uma nova partição de inicialização, insira o seguinte comando e pressione **Enter**:

```
n
```

5 Para criar uma nova partição primária, insira o seguinte comando e pressione **Enter**:

```
p
```

6 Para especificar o número de partição, insira-o e pressione **Enter**. Por exemplo, para especificar a partição 1, digite 1 e, em seguida, pressione **Enter**.

7 Para usar o primeiro setor, 2048, pressione **Enter**.

8 Aloque uma quantidade adequada para a partição de inicialização, inserindo o sinal de mais e a quantidade de alocação e pressionando **Enter**.

Por exemplo, para alocar 500 M para a partição de inicialização, digite o seguinte e pressione **Enter**:

```
+512000K
```

9 Para alternar um sinalizador inicializável para a partição de inicialização (para tornar a partição inicializável), digite o seguinte comando e pressione **Enter**:

```
a
```

10 Para atribuir um sinalizador inicializável à partição adequada, digite o número da partição e pressione **Enter**. Por exemplo, para atribuir um sinalizador inicializável para a partição 1, digite 1 e pressione **Enter**.

11 Continue particionando o disco conforme necessário.

12 Para salvar todas as alterações no utilitário fdisk, digite o seguinte comando e pressione **Enter**:

w

Formatar partições na unidade de destino

Depois de criar partições em um novo volume na unidade de destino para realizar a restauração sem sistema operacional, se não estiver usando a partição automática, você deverá formatar as partições para elas serem montadas. Se essa situação se aplicar a você, siga este procedimento para formatar partições em formatos ext3, ext4 ou XFS.

Para todos os outros cenários, você não precisa formatar partições conforme descrito neste tópico.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Como gerenciar partições do Linux.

1 Como opção, você pode usar o utilitário Screen. Esse utilitário é iniciado por padrão e permanece ativo até você reinicializar a máquina.

NOTA: Se você fechá-lo explicitamente e quiser reabri-lo, consulte Iniciar o utilitário Screen.

2 Na linha de comando, insira o seguinte comando e pressione **Enter** para alterar os privilégios para execução como administrador e depois relacionar as partições de disco existentes:

```
sudo fdisk -l
```

Uma lista com todos os volumes é exibida.

Esse exemplo supõe que a partição que você deseja formatar é /dev/sda1. Se seu volume é diferente (por exemplo, em unidades mais antigas, pode ser /dev/hda), altere os comandos adequadamente.

3 Selecione um dos seguintes comandos dependendo do formato que você deseja utilizar a partição de destino:

- Para formatar uma partição no formato ext3, insira o seguinte comando e pressione **Enter**:

  ```
  sudo mkfs.ext3 /dev/sda1
  ```

- Para formatar uma partição no formato ext4, insira o seguinte comando e pressione **Enter**:

  ```
  sudo mkfs.ext4 /dev/sda1
  ```

- Para formatar uma partição no formato XFS, insira o seguinte comando e pressione **Enter**:

  ```
  sudo mkfs.xfs /dev/sda1
  ```

A partição selecionada é formatada de acordo.

4 De forma opcional, se você precisar formatar outras partições, repita esse procedimento.

Montar partições a partir da linha de comando

Se estiver realizando uma BMR usando o Rapid Recovery Core Console, você deverá primeiro montar as partições apropriadas na máquina de destino. Realize isso na linha de comando do Universal Recovery Console.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Como gerenciar partições do Linux.

Execute as etapas deste procedimento para montar partições na máquina com Linux antes de fazer uma restauração.

1 Na linha de comando, insira o seguinte comando e pressione **Enter** para alterar os privilégios para execução como administrador e depois relacionar as partições de disco existentes:

```
sudo fdisk -l
```

Uma lista com todos os volumes é exibida.

2 Formate todas as partições de que precisará para realizar a BMR no diretório de montagem. Elas devem corresponder aos volumes do ponto de recuperação. Por exemplo, se o volume que você deseja montar é chamado sda1 e o diretório de montagem é mnt, digite o seguinte comando e pressione **Enter**:

3 Monte todas as partições de que precisará para realizar a BMR no diretório de montagem. Elas devem corresponder aos volumes do ponto de recuperação. Por exemplo, se o volume que você deseja montar é chamado sda1 e o diretório de montagem é mnt, digite o seguinte comando e pressione **Enter**:

```
mount /dev/sda1 /mnt
```

4 Repita a Etapa 3 conforme necessário até você ter montado todos os volumes obrigatórios.

Depois de montar os volumes, você poderá realizar uma restauração na máquina Linux de destino no Rapid Recovery Core Console. Consulte Iniciar uma restauração sem sistema operacional para Linux.

Iniciar uma restauração sem sistema operacional para Linux

Antes de iniciar uma bare metal restore (BMR) para uma máquina com Linux, as seguintes condições devem ser satisfeitas:

- Para restaurar um ponto de recuperação salvo no Core, é necessário ter o hardware apropriado disponível. Para obter mais informações, consulte Pré-requisitos para realizar uma bare metal restore em máquinas Linux.
- A máquina com Linux de destino da BMR deve ser iniciada usando a imagem de inicialização do Live DVD. Para obter mais informações, consulte Gerenciar uma imagem de inicialização do Linux.
- O número de volumes na máquina com Linux a ser restaurada deve corresponder ao número de volumes no ponto de recuperação. Também é preciso decidir se deseja restaurar a partir do Rapid Recovery Core Console ou da linha de comando usando local_mount. Para obter mais informações, consulte Como gerenciar partições do Linux.
- Se a restauração for feita a partir da UI do Core Console, a primeira etapa para iniciar a BMR é selecionar o ponto de recuperação apropriado, depois iniciar a restauração no hardware especificando o endereço IP e uma senha temporária obtida a partir do Universal Recovery Console. A seguir, você precisa mapear as unidades e iniciar a restauração.

Esse processo é uma etapa do Realizar uma bare metal restore em máquinas Linux.

Para iniciar uma BMR no Rapid Recovery Core Console, realize as seguintes tarefas.

- Como selecionar um ponto de recuperação e iniciar uma BMR
- Sobre como mapear volumes para uma restauração sem sistema operacional

Se a restauração for feita da linha de comando usando o utilitário local_mount, primeiro será preciso definir os privilégios apropriados, montar volumes, executar o local_mount, obter informações sobre o Core na lista de máquinas, conectar-se ao núcleo, obter uma lista de pontos de recuperação, selecionar o ponto de recuperação do qual deseja reverter em bare metal restore e iniciar a restauração.

Como opção, você pode iniciar o utilitário Screen.

Para iniciar uma BMR na linha de comando, realize as tarefas a seguir.

- Iniciar o utilitário Screen
- Realizar uma bare metal restore em uma máquina Linux usando a linha de comando

Iniciar o utilitário Screen

O Live DVD inclui o utilitário Screen, disponível ao inicializar a partir do Live DVD no Universal Recovery Console. O Screen permite aos usuários gerenciar vários shells simultaneamente em uma única sessão Secure Shell (SSH) ou janela de console. Isso permite realizar uma tarefa em uma janela de terminal (como confirmar volumes montados) e, enquanto isso é executado, abrir ou alternar para outra instância de shell e realizar outra tarefa (como executar o utilitário local_mount).

O utilitário Screen também tem seu próprio buffer de rolagem para trás, o que permite rolar a tela para ver maiores quantidades de dados, como a lista de pontos de recuperação.

NOTA: O utilitário Screen é fornecido para sua conveniência; seu uso é opcional.

O utilitário Screen inicia na máquina inicializada com o Live DVD por padrão. Contudo, se você fechou esse aplicativo, é preciso iniciar o utilitário Screen a partir do Live DVD usando o procedimento abaixo.

Se a máquina foi inicializada a partir do Live DVD, na janela do terminal, digite screen e pressione **Enter**.

O utilitário Screen é iniciado.

Realizar uma bare metal restore em uma máquina Linux usando a linha de comando

Depois que a imagem ISO do Live DVD estiver acessível na máquina na qual você deseja realizar uma BMR e o número e tamanho dos volumes forem correspondentes entre a máquina de destino e o ponto de recuperação no qual deseja executar a bare metal restore, será possível iniciar essa restauração na linha de comando usando o utilitário local_mount.

NOTA: Esse componente era chamado de`aamount`.

Se você quiser realizar uma BMR usando a UI do Rapid Recovery Core Console, consulte Como selecionar um ponto de recuperação e iniciar uma BMR.

NOTA: Ao realizar este procedimento, não tente montar pontos de recuperação na pasta /tmp, que contém os arquivos rapidrecovery-vdisk (antigo aavdisk).

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Realizar uma bare metal restore em uma máquina Linux usando a linha de comando.

Execute as etapas deste procedimento para selecionar um ponto de recuperação no Core para reverter para a máquina de destino física ou virtual da BMR.

1 Para executar o utilitário local_mount Rapid Recovery como raiz, digite o seguinte comando e pressione **Enter**:

```
sudo local_mount
```

2 Para listar as máquinas protegidas, digite o seguinte comando e pressione **Enter**:

```
lm
```

3 Quando solicitado, especifique as informações de conexão do Rapid Recovery Core conforme descrito na seguinte tabela, pressionando Enter após cada comando obrigatório:

Tabela 159. Informações de conexão do Rapid Recovery Core

Caixa de texto	Descrição	Obrigatório
Endereço IP ou o nome de host do Rapid Recovery Core	O endereço IP ou o nome de host do Rapid Recovery Core.	Sim
Domínio	O domínio do Rapid Recovery Core. Opcional.	Não
Usuário	O nome de usuário de um usuário administrativo no Core	Sim
Senha	A senha usada para conectar o usuário administrativo ao Core.	Sim

Uma lista é exibida mostrando as máquinas protegidas pelo Rapid Recovery Core. Ela relaciona as máquinas encontradas por número de item de linha, nome de exibição do host ou endereço IP e número de ID da máquina.

4 Para relacionar os pontos de recuperação da máquina que você deseja restaurar, digite o comando Relacionar os pontos de recuperação usando a seguinte sintaxe e pressione **Enter**:

```
lr <machine_line_item_number>
```

NOTA: Você também pode inserir o número de ID da máquina nesse comando em vez do número do item de linha.

Uma lista exibe os pontos de recuperação de base e incremental da máquina. Essa lista inclui:

- Número de item de linha
- Carimbo de data e hora
- Uma lista de volumes com letras dentro do ponto de recuperação
- Localização do volume
- Tamanho do ponto de recuperação
- Um número de ID do volume que inclui um número de sequência no fim, identificando o ponto de recuperação

5 Para selecionar o ponto de recuperação de uma restauração, insira o seguinte comando e pressione **Enter**:

```
r <recovery_point_ID_number> <path>
```

CUIDADO: É preciso garantir que o volume do sistema não esteja montado.

NOTA: Se a máquina foi iniciada do Live DVD, o volume do sistema não estará montado.

Esse comando reverte a imagem do volume especificada pelo ID do Core para o caminho especificado. O caminho da restauração é o do descritor de arquivo de dispositivo e não o diretório no qual está montado.

NOTA: Você também pode especificar um número de linha no comando em vez do número de ID do ponto de recuperação para identificar o ponto de recuperação. Nesse caso, use o número de linha de agente/máquina (da saída`lm`), seguido do número da linha do ponto de recuperação e da letra de volume (da lista de volumes com letras dentro do ponto de recuperação), seguidos pelo caminho. Por exemplo:

```
r <machine_line_item_number> <base_image_recovery_point_line_number> <volume_letter> <path>
```

Por exemplo, digite:

```
r 1 24 a /dev/sda1
```

Nesse comando,`<path>` é o descritor de campo do volume real.

6 Quando solicitado a continuar, digite y para Sim e pressione **Enter**.

Depois que a restauração iniciar, uma série de mensagens será exibida para notificá-lo do status de conclusão da restauração.

NOTA: Se você receber uma mensagem de exceção, os detalhes sobre essa exceção poderão ser encontrados no arquivo local_mount.log. O arquivo local_mount.log está localizado em /var/log/apprecovery.

7 Depois de uma restauração bem-sucedida, saia de local_mount digitando`exit` e pressione **Enter**.

8 A próxima etapa é confirmar a restauração. Para obter mais informações, consulte Confirmar a restauração sem sistema operacional na linha de comando.

Restaurar volumes em uma máquina Linux usando a linha de comando

No Rapid Recovery, é possível restaurar volumes em suas máquinas Linux protegidas usando o utilitário de linha de comando `local_mount .`

NOTA: Esse processo antes era chamado de *reversão*. Ao realizar este procedimento, não tente montar pontos de recuperação na pasta /tmp, que contém os arquivos rapidrecovery-vdisk (antigo aavdisk). A restauração de volumes também é suportada nas máquinas protegidas no Rapid Recovery Core Console. Consulte Como restaurar volumes a partir de um ponto de recuperação para obter mais informações.

CUIDADO: Para restaurar a partição de sistema ou raiz (/) ou todo o sistema operacional, consulte Realizar uma bare metal restore em máquinas Linux.

1 Execute o utilitário `local_mount` do Rapid Recovery como raiz, por exemplo:

```
sudo local_mount
```

2 No prompt de montagem do Rapid Recovery, digite o comando a seguir para listar as máquinas protegidas.

```
lm
```

3 Quando solicitado, digite o endereço IP ou nome do host do servidor do Rapid Recovery Core.

4 Insira as credenciais de login desse server, ou seja, o nome de usuário e a senha.

Aparece uma lista que mostra as máquinas protegidas por esse server do Rapid Recovery. Ela mostra as máquinas protegidas encontradas por número de item de linha, host/endereço IP e um número de identificação para a máquina (por exemplo: 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2).

5 Insira o seguinte comando para relacionar os pontos de recuperação atualmente montados para a máquina especificada:

```
lr <machine_line_item_number>
```

NOTA: Observe que você também pode inserir o número de ID da máquina neste comando em vez do número do item de linha.

Uma exibição em lista exibe os pontos de recuperação de base e incremental da máquina. Essa lista inclui um número de item de linha, data/carimbo de data e hora, localização do volume, tamanho de ponto de recuperação e número de ID do volume que inclui um número de sequência no fim (por exemplo,"293cc667-44b4-48ab-91d8-44bc74252a4f:2"), que identifica o ponto de recuperação.

6 Insira o seguinte comando para selecionar um ponto de recuperação a restaurar:

```
r <volume_recovery_point_ID_number> <device path>
```

Esse comando restaura a imagem do volume especificada pelo ID do Core para o caminho especificado. O caminho da restauração é o do descritor de arquivo de dispositivo e não o diretório no qual está montado.

- Você também pode especificar um número de linha no comando em vez do número de ID do ponto de recuperação para identificar o ponto de recuperação. Nesse caso, você usaria o número de linha da máquina protegida (da saída lm), seguido do número da linha do ponto de recuperação e letra de volume, seguido pelo caminho, como, r <machine_line_item_number> <recovery_point_line_number> <volume_letter> <caminho>. Nesse comando, <caminho> é o descritor de arquivo do volume real.

  Por exemplo, se a saída `lm` lista três máquinas protegidas e você for digitar o comando `lr` para o número da máquina protegida `2` para restaurar o volume `23` do ponto de recuperação `b` para o volume que foi montado no diretório`/dev/sda5,`, o comando deve ser:

  ```
  r2 23 b /dev/sda5
  ```

  NOTA: É possível restaurar para / se necessário. Se estiver executando uma restauração sem sistema operacional usando um Live DVD, presume-se que você quer restaurar para uma máquina diferente. Para obter mais informações, consulte Iniciar uma restauração sem sistema operacional para Linux.

7 Quando solicitado para continuar, digite `y` para Sim.

Depois que a restauração continuar, uma série de mensagens será exibida para notificá-lo sobre o status.

8 Após uma restauração bem-sucedida, o utilitário `local_mount` montará e reconectará automaticamente o módulo do kernel ao volume restaurado se o destino antes estava protegido e montado. Caso contrário, será necessário montar o volume restaurado no disco local e, em seguida, confirmar se os arquivos estão restaurados (por exemplo, é possível usar o comando `sudo mount` e depois o comando `ls`.)

Confirmar uma bare metal restore

Depois de realizar uma bare metal restore (BMR), você poderá confirmar o progresso da restauração. Quando a ação for concluída com sucesso, você poderá iniciar o server restaurado. Algumas etapas de resolução de problemas são incluídas se houver dificuldades para se conectar ao Universal Recovery Console a fim de concluir a restauração e, se necessário, reparar problemas de inicialização com a máquina restaurada.

Você pode realizar as seguintes tarefas:

Links relacionados

Visualizar o progresso da recuperação
Iniciar um servidor de destino restaurado
Como solucionar problemas de conexão com o Universal Recovery Console
Como reparar problemas de inicialização

Visualizar o progresso da recuperação

Execute as etapas deste procedimento para visualizar o progresso da restauração de dados de um ponto de recuperação (incluindo bare metal restore) iniciado no Rapid Recovery Core Console.

1 Depois de iniciar o processo de restauração de dados de um ponto de recuperação, enquanto a tarefa estiver em andamento, você pode visualizar seu progresso no menu suspenso Tarefas em execução no Core Console.
2 É possível visualizar informações detalhadas na página Eventos. Para obter mais informações sobre como monitorar os eventos do Rapid Recovery, consulte Ver tarefas, alertas e eventos.

Iniciar um servidor de destino restaurado

Execute as etapas deste procedimento para iniciar o server de destino restaurado.

NOTA: Antes de iniciar o server de destino restaurado, confirme se a recuperação foi bem-sucedida. Para obter mais informações, consulte Visualizar o progresso da recuperação.

Essa tarefa é uma das etapas do Como executar uma restauração "bare metal" em máquinas Windows. Faz parte do processo de Confirmar uma bare metal restore.

1 No servidor de destino, verifique se o Universal Recovery Console do Rapid Recovery está ativo.
2 Ejete o CD de inicialização (ou desconecte a mídia física com a imagem do CD de inicialização) do server restaurado.
3 No Universal Recovery Console, clique no ícone de menu de Energia na parte superior da tela e, em seguida, clique em **Reinicialização**.
4 Especifique para iniciar o sistema operacional normalmente.
5 Efetue login na máquina. O sistema deve ser restaurado para o estado capturado no ponto de recuperação.

Como solucionar problemas de conexão com o Universal Recovery Console

Encontramos a seguir as etapas da solução de problemas de conexão com a imagem do CD de inicialização como parte do processo de Como selecionar um ponto de recuperação e iniciar uma BMR.

Se um erro for exibido indicando que o Core não pôde se conectar ao server remoto, existem várias causas possíveis.

- Confirme se o endereço IP e a senha atual exibidos no URC são idênticos às informações inseridas na caixa de diálogo Instância do console de recuperação.
- Para alcançar o server no qual irá restaurar dados, o Core deve ser capaz de identificar o server na rede. Para determinar se a identificação do servidor, você poderá abrir um prompt de comando no Core e fazer um ping do endereço IP do server de BMR de destino. Também é possível abrir um prompt de comando no server de destino e fazer um ping para o endereço IP do Rapid Recovery Core.
- Confirme se as definições do adaptador de rede são compatíveis entre o Core e o server de BMR de destino.

Como reparar problemas de inicialização

As seguintes tarefas são pré-requisitos para este procedimento.

- Criar uma imagem ISO do CD de inicialização
- Como carregar o CD de inicialização e iniciar o computador de destino
- Carregar drivers usando o Universal Recovery Console

Execute as etapas deste procedimento para reparar problemas de inicialização. Lembre-se de que, se você tiver restaurado em um hardware diferente, precisará ter injetado o driver do controlador de armazenamento, RAID, AHCI, chipset e outros drivers, se eles já não estiverem no CD de inicialização. Esses drivers permitem que o sistema operacional opere com sucesso todos os dispositivos em seu server de destino. Para obter mais informações, consulte Carregar drivers usando o Universal Recovery Console. Execute o procedimento a seguir para reparar problemas de inicialização no seu server de destino.

1 No Universal Recovery Console, clique na guia **Gerenciador de driver do Windows existente**.
2 Clique em **Reparar problemas de inicialização**.
Os parâmetros de inicialização no registro de inicialização do server de destino são reparados automaticamente.

Confirmar a restauração sem sistema operacional na linha de comando

A Dell recomenda realizar as seguintes etapas para confirmar se uma bare metal restore foi concluída na linha de comando.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux.

Links relacionados

Realizar uma verificação do sistema de arquivos no volume restaurado
Como usar a linha de comando para tornar uma máquina Linux restaurada inicializável

Realizar uma verificação do sistema de arquivos no volume restaurado

Depois de executar uma bare metal restore na linha de comando, você deve realizar uma verificação do sistema de arquivos no volume restaurado para garantir que os dados restaurados do ponto de recuperação não foram corrompidos.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Confirmar a restauração sem sistema operacional na linha de comando.

Realize a tarefa abaixo para realizar uma verificação do sistema de arquivos no volume restaurado.

1 Na linha de comando do Universal Recovery Console da máquina com Linux que você restaurou, para confirmar se as partições adequadas estão montadas, digite o seguinte comando e pressione **Enter**:

```
df
```

2 Se o volume restaurado não estiver montado, vá para Etapa 3. Se o volume restaurado estiver montado, desmonte-o digitando o seguinte comando e pressionando Enter:

```
umount <mount point>
```

3 Execute uma verificação do sistema de arquivos nos volumes restaurados digitando o seguinte comando e pressionando Enter:

```
fsck -f <volume>
```

Se o retorno do fsck for limpo, o sistema de arquivos estará confirmado.

4 Monte os volumes adequados novamente digitando o seguinte comando no formato`mount <volume> <folder>` e pressione **Enter**.

Por exemplo, se o caminho do volume for prod/sda1 e a pasta que você deseja montar for mnt, digite o seguinte e pressione **Enter**:

```
mount /dev/sda1 /mnt
```

Como usar a linha de comando para tornar uma máquina Linux restaurada inicializável

Depois de executar uma verificação limpa do sistema de arquivos no volume restaurado, crie partições inicializáveis.

O GNU Grand Unified Bootloader (GRUB) é um carregador de inicialização que permite aos administradores configurar qual sistema operacional ou configuração de kernel específica será utilizado para iniciar o sistema. Após uma BMR, o arquivo de configuração do GRUB deve ser modificado para que a máquina use o identificador universal exclusivo (UUID) apropriado para o volume raiz. Antes dessa etapa, é preciso montar os volumes raiz e de inicialização e verificar os UUIDs de cada um. Isso garante que você consiga inicializar a partir da partição.

NOTA: Este procedimento aplica-se a máquinas Linux que usam GRUB1 ou GRUB2. Ao usar este procedimento, certifique-se de que a partição de inicialização está íntegra e protegida.

GRUB ou GRUB2 costuma ser instalado com sistemas operacionais Linux. Você pode realizar esse procedimento usando a versão que acompanha a distribuição Linux. Se uma versão do GRUB não estiver instalada, você terá que reinstalar a versão padrão apropriada à sua distribuição Linux.

CUIDADO: Quando você inicializa uma máquina Linux restaurada pela primeira vez após uma BMR, o Rapid Recovery gera uma imagem de base da máquina restaurada. Dependendo da quantidade de dados na máquina, esse processo leva mais tempo do que a criação de um snapshot incremental. Para obter mais informações sobre imagens de base e snapshots incrementais, consulte Noções básicas sobre programações de proteção.

Essa tarefa é uma das etapas do Realizar uma bare metal restore em máquinas Linux. Faz parte do processo de Confirmar a restauração sem sistema operacional na linha de comando.

Realize a tarefa abaixo para criar partições inicializáveis usando a linha de comando.

1 É preciso montar o volume raiz primeiro e, depois, o volume de inicialização. Monte cada volume restaurado usando os seguintes comandos:

a Para montar o volume raiz, digite o seguinte comando e pressione **Enter**:

```
mount /<restored volume[root]> /mnt
```

Por exemplo, se /dev/sda2 for o volume raiz, digite mount /dev/sda2 /mnt and e pressione **Enter**.

b Para montar o volume de inicialização, digite o seguinte comando e pressione **Enter**:

```
mount /<restored volume[boot]> /mnt/boot
```

Por exemplo, se /dev/sda1 for o volume de inicialização, digite mount /dev/sda1 /mnt/boot e pressione **Enter**.

NOTA: Algumas configurações do sistema podem incluir o diretório de inicialização como parte do volume raiz.

2 Se o tamanho do volume estiver aumentando — ou seja, se o volume de destino na nova máquina Linux for maior do que o volume no ponto de recuperação — será preciso excluir os arquivos de dados de mapa de bits existentes.

3 Obtenha o identificador universal exclusivo (UUID) dos novos volumes usando o comando`blkid` . Digite o seguinte comando e pressione **Enter**:

```
blkid [volume]
```

NOTA: Você também pode usar o comando`ls -l /dev/disk/by-uuid .`

4 Se a BMR estiver sendo realizada em um disco novo na máquina de destino, comente a partição de swap em fstab no seu volume raiz.

5 A modificação dos caminhos fstab e mtab deve ocorrer no volume restaurado e não no Live DVD. Não há necessidade de modificar os caminhos do Live DVD. Prepare a instalação do Grand Unified Bootloader (GRUB) digitando os seguintes comandos. Depois de cada comando, pressione **Enter**:

```
mount --bind /dev /mnt/dev
mount --bind /proc /mnt/proc
mount --bind /sys /mnt/sys
```

6 Altere o diretório raiz digitando o seguinte comando e pressionando **Enter**:

```
chroot /mnt /bin/bash
```

7 Obtenha o UUID antigo da partição ou partições no arquivo`/etc/fstab` dos pontos de recuperação montados e compare-o aos UUIDs das partições raiz (para Ubuntu e CentOS), de inicialização (para CentOS e RHEL) ou de dados digitando o seguinte comando e pressionando **Enter**:

```
less /mnt/etc/fstab
```

8 Obtenha o UUID antigo das partições no arquivo `/etc/mtab` dos pontos de recuperação montados e compare-o aos UUIDs das partições raiz (para Ubuntu e CentOS), de inicialização (para CentOS e RHEL) ou de dados digitando o seguinte comando e pressionando **Enter**:

```
less /mnt/etc/mtab
```

9 Se estiver usando o SLES 11, instale o GRUB digitando os seguintes comandos, pressionando Enter depois de cada um:

```
grub-install --recheck /dev/sda
grub-install /dev/sda
```

10 Se você estiver usando Ubuntu, CentOS 6.x, RHEL 6.x ou Oracle Linux 6.x, instale GRUB digitando o seguinte comando e pressione Enter:

```
grub-install /dev/sda
```

11 Se você estiver usando SLES 12, CentOS 7, RHEL 7 ou Oracle 7, instale GRUB2 digitando o seguinte comando e pressione Enter:

```
grub2-install /dev/sda
```

12 Quando concluir a instalação, execute uma das atualizações a seguir:

- Para SLES:

```
grub-install.unsupported --recheck /dev/sda
grub-install.unsupported /dev/sda
update-grub
```

NOTA: Se o comando`update-grub` não existir na sua distribuição Linux, ignore essa opção.

- Para outras distribuições:

```
grub-install /dev/sda
update-grub
```

NOTA: Se o comando`update-grub` não existir na sua distribuição Linux, ignore essa opção.

13 Remova o disco do Live DVD da unidade de CD-ROM ou DVD e reinicie a máquina com Linux.

6

Gerar e visualizar relatórios

Esta seção fornece uma visão geral dos relatórios disponíveis no Rapid Recovery Core e no Rapid Recovery Central Management Console.

Tópicos:

- Sobre os relatórios do Rapid Recovery
- O Central Management Console

Sobre os relatórios do Rapid Recovery

Você pode gerar relatórios a partir do Rapid Recovery Core Console. Alguns desses relatórios também estão disponíveis a partir do Central Management Console.

Os relatórios disponíveis são descritos na tabela a seguir.

Tabela 160. Relatórios do Rapid Recovery

Tipo de relatório	Descrição
Relatório do trabalho	Fornece um relatório sobre o status dos trabalhos bem-sucedidos, trabalhos com falha e trabalhos com erros. Os trabalhos com falha podem ainda ser vistos com mais detalhes em um Relatório de falhas. Este tipo de trabalho pode ser executado a partir do Core Console e do Central Management Console. • Quando executado a partir do Core, este relatório pode especificar os detalhes de um ou mais Cores.Por padrão, esse conjunto de informações contém os trabalhos de todas as máquinas, ou seja, todas as máquina protegidas, replicadas e de ponto de recuperação apenas, nos Cores especificados. Nos parâmetros do relatório, você pode personalizar o relatório. Use os filtros para selecionar ou excluir algumas máquinas. Você pode também selecionar ou excluir trabalhos que são independentes de máquina; nesse caso, o relatório mostrará apenas o status dos trabalhos do Core. • Quando executado a partir da perspectiva de uma máquina protegida do Core Console, o relatório resultante exibe o status dos trabalhos dessa máquina protegida apenas. • Quando executado a partir do Central Management Console, este relatório pode especificar detalhes para qualquer combinação de Cores ou grupos de Cores configurados no Console. Os únicos parâmetros configuráveis são o tipo de relatório e o período. Para obter mais informações sobre esse tipo de relatório, consulte Noções básicas sobre o relatório do trabalho.
Relatório de falhas	Fornece informações sobre os trabalhos do Core com falha conforme os critérios especificados. Este tipo de trabalho pode ser executado a partir do Core Console e do Central Management Console. • Quando executado a partir do Core, este relatório pode incluir ou não detalhes da máquina protegida. Assim como o Relatório do trabalho, este relatório pode também ser executado apenas a partir de uma máquina protegida selecionada no Core. O relatório resultante mostra detalhes sobre trabalhos com falha somente para a máquina protegida selecionada. • Quando executado a partir do Central Management Console, este relatório pode especificar eventos de falha para qualquer combinação de Cores ou grupos de Cores configurados no Console. Os únicos parâmetros configuráveis são o tipo de relatório e o período. Para obter mais informações sobre esse tipo de relatório, consulte Noções básicas sobre o relatório de falhas.

Tipo de relatório	Descrição
Relatório resumido	Fornece informações de resumo.Por padrão, esse conjunto de informações contém os trabalhos de todas as máquinas, ou seja, todas as máquina protegidas, replicadas e de ponto de recuperação apenas, nos Cores especificados. Nos parâmetros do relatório, você pode personalizar o relatório. Use os filtros para selecionar ou excluir algumas máquinas. Você pode também selecionar ou excluir trabalhos que são independentes de máquina; nesse caso, o relatório mostrará apenas o status dos trabalhos do Core. Este relatório não está disponível da perspectiva de uma única máquina protegida. Este tipo de trabalho pode ser executado a partir do Core Console e do Central Management Console. • Quando executado a partir do Core Console, as categorias de informações deste relatório são Core, licença e repositório. As informações são apresentadas na forma de listas, gráficos e tabelas. • Quando executado a partir do Central Management Console, este relatório pode especificar informações de resumo para qualquer combinação de Cores ou grupos de Cores configurados no Console. Os únicos parâmetros configuráveis são o tipo de relatório e o período. As categorias de informações deste relatório são Core, licença e repositório. O relatório resumido também contém um relatório sobre as máquinas protegidas e a taxa de trabalhos bem-sucedidos para todos os trabalhos. As informações são apresentadas na forma de listas, gráficos e tabelas. Para obter mais informações sobre esse tipo de relatório, consulte Noções básicas sobre o relatório resumido.
Relatório do repositório	Este tipo de relatório fornece um relatório de todos os repositórios no Core ou Cores selecionados. Você pode também selecionar qualquer repositório único disponível para o Core. Este relatório está disponível a partir do Core Console somente e apenas do ponto de vista do Core. Para obter mais informações sobre esse tipo de relatório, consulte Noções básicas sobre o relatório do Repositório.
Relatório programado	Você pode também programar um desses relatórios no Core Console. A programação de um relatório faz com que o relatório que você especificar seja gerado repetidamente conforme a programação definida. Como opção, você pode estabelecer notificações de e-mail cada vez que um relatório for gerado. Para obter mais informações sobre como programar, modificar, pausar ou apagar relatórios, consulte Gerenciar relatórios programados do Core Console.

Baseado no tipo de relatório e nos parâmetros selecionados, você pode gerar um relatório em um ou mais Rapid Recovery Cores ou para uma ou mais máquinas protegidas.

A partir do Central Management Console, você pode gerar um relatório para qualquer combinação de Cores ou grupos de Cores configurados nesse Console.

Gerar um relatório no Core Console

Você pode gerar relatórios sob demanda a partir do Core Console. As seguintes regras se aplicam:

- Todos os relatórios podem ser gerados a partir do ponto de vista do Core.
- Além disso, dois tipos de trabalho (o Relatório do trabalho e o Relatório de falhas) podem ser gerados do ponto de vista de uma máquina protegida. Para tais relatórios, os dados gerados são relativos apenas à máquina selecionada.
- Os Relatório de falhas conterão dados apenas se os trabalhos nos Cores selecionados (ou máquinas protegidas) falharam.

O método de geração de relatórios sob demanda é similar se o relatório for gerado a partir do foco do Core ou se ele for gerado do ponto de vista de uma máquina protegida. No entanto, a navegação é ligeiramente diferente.

Você pode também agendar relatórios para que eles sejam gerados regularmente. Para obter mais informações sobre como programar, modificar, pausar ou apagar relatórios, consulte Gerenciar relatórios programados do Core Console.

Gerar um relatório de Core sob demanda

Conforme descrito no tópico Sobre os relatórios do Rapid Recovery, é possível gerar a faixa completa de relatórios disponíveis do Core Console.

Execute as etapas do procedimento a seguir para gerar um relatório do ponto de vista do Rapid Recovery Core.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Mais) e, em seguida, selecione **Relatórios**.

A página **Relatório do trabalho** é mostrada. À direita do nome do relatório no título da página, uma seta voltada para baixo é mostrada, a partir da qual você pode selecionar outro tipo de relatório.

Se você quiser gerar um relatório de trabalho, vá para a Etapa 6 para começar a especificação dos seu critérios de relatório.

3 Para escolher outro tipo de relatório, clique na seta à direita do nome do relatório para ver um menu de relatórios disponíveis.

4 Para definir relatórios programados, consulte Programar um relatório.

5 Para gerar um relatório do repositório apenas, vá para a Etapa 11.

6 Para um relatório resumido, de trabalho, de resumo do trabalho ou de falha, selecione um período no menu suspenso **Período**.

Se você não escolher um período, a opção padrão (Últimos 31 dias) será usada. Você pode escolher uma das opções da tabela a seguir.

Opção	Descrição
Últimas 24 horas	Reporta a atividade do último dia, relativo ao horário em que o relatório for gerado.
Últimos 7 dias	Reporta a atividade da semana anterior, relativo ao horário em que o relatório for gerado.
Últimos 31 dias	Reporta a atividade dos últimos 31 dias, relativo ao horário em que o relatório for gerado.
Últimos 90 dias	Reporta a atividade dos últimos 90 dias, relativo ao horário em que o relatório for gerado.
Últimos 365 dias	Reporta a atividade do ano anterior, relativo ao horário em que o relatório for gerado.
Desde o começo	Esse período abrange toda a vida útil do Core.
Personalizada	Esse período exige que você ainda especifique as datas de início e de fim.
Mês até a data	Reporta a atividade do primeiro dia do mês atual até a data em que o relatório for gerado.
Ano até a data	Reporta a atividade do primeiro dia do ano atual até a data em que o relatório for gerado.

NOTA: Em todos os casos, não existem dados de relatório disponíveis anteriores a implantação do Core, ou de antes de as máquinas serem protegidas no Core.

7 Para um relatório de falhas ou de trabalho, no menu suspenso **Cores de destino**, selecione um ou mais Cores para os quais você quer gerar um relatório.

A seleção padrão contém todos os Cores disponíveis.

8 No menu suspenso **Máquinas protegidas**, selecione a máquina ou as máquinas para as quais você quer gerar o relatório.

Por padrão, esse conjunto de informações contém os trabalhos de todas as máquinas, ou seja, todas as máquina protegidas, replicadas e de ponto de recuperação apenas, nos Cores especificados. Nos parâmetros do relatório, você pode personalizar o relatório. Use os filtros para selecionar ou excluir algumas máquinas. Você pode também selecionar ou excluir trabalhos que são independentes de máquina; nesse caso, o relatório mostrará apenas o status dos trabalhos do Core.

Você pode selecionar dentre:

Opção	Descrição
Selecionar tudo	Esta opção seleciona todas as máquinas protegidas neste Core. **NOTA: Você pode selecionar todas as máquinas e, em seguida, apagar algumas seleções para especificar um subconjunto de todas as máquinas.**
Independente de máquina	Selecione esta opção para gerar um relatório que contenha os trabalhos da perspectiva de um Core. Tipos de trabalho como criar ou apagar um repositório ou criar um CD de inicialização não estão associados a uma

Opção	Descrição
	máquina específica. Se estiver implantando o software do agente em uma máquina ainda não protegida, esse tipo de trabalho também é considerado como independente de máquina. Esses trabalhos não mostram uma máquina protegida na coluna Máquina protegida do relatório resultante. Em contraste, se você implantar o software do agente em uma máquina já protegida no Core, o nome da máquina protegida será incluída no relatório. Ela não é considerada independente de máquina.
Máquinas protegidas	Esta opção mostra as máquinas protegidas por este Core. Você pode selecionar todas ou um subconjunto de máquinas protegidas.
Apenas pontos de recuperação	Esta opção mostra as máquinas que já foram protegidas uma vez, mas que ainda têm pontos de recuperação salvos no repositório.
[Cores de origem]	Se o seu Core for um Core de destino e replica pontos de recuperação para quaisquer máquinas protegidas em um Core de origem, o nome do Core de origem é mostrado (com todas as letras maiúsculas). Esta opção mostra uma lista de todas as máquinas protegidas nesse Core de origem. Você pode selecionar todas as máquinas replicadas nesse Core de destino ou você pode selecionar um subconjunto.
[Grupos personalizados]	Se você tiver grupos personalizados criados nesse Core, o nome de cada grupo personalizado aparecerá como uma opção. Será exibido todos os objetos nesse grupo personalizado. Você pode selecionar todos os objetos no grupo ou um subconjunto deles.

9 Se for gerar um relatório resumido, vá para a Etapa 12.

10 Para um relatório de falhas, de trabalho ou de resumo do trabalho, no menu suspenso **Tipos de trabalho**, selecione os tipos de trabalho adequados.

Por padrão, esse conjunto de informações inclui todos os trabalhos para as máquinas protegidas selecionadas. Nos parâmetros do relatório, você pode personalizar o relatório. Use os filtros para selecionar ou excluir todos os trabalhos na categoria Principais trabalhos e todos os trabalhos na categoria Outros trabalhos. Ou você pode expandir cada uma dessas categorias ao definir parâmetros do trabalho e selecionar apenas os tipos de trabalho de cada categoria que você deseja que apareça no relatório. Clique na caixa de seleção de qualquer tipo de trabalho para marcá-lo ou desmarcá-lo. Você pode selecionar alguns ou todos os trabalhos de cada categoria.

Você pode escolher um dos seguintes tipos de trabalho **outros**:

11 Para um relatório do repositório, no menu Repositórios, selecione o repositório ou os repositórios que você deseja incluir no relatório.

A seleção padrão contém todos os repositórios disponíveis.

12 Clique em **Pré-visualizar** para gerar o relatório com os critérios especificados.

Se os critérios de relatório selecionados não forem encontrados, o relatório ainda assim será gerado, mas com uma linha vazia. Por exemplo, se não houver erros, o conteúdo da coluna Erro será null no relatório.

13 Realize um dos procedimentos a seguir:

- Visualize o relatório gerado on-line.
- Atualize o relatório dinamicamente alterando um dos critérios e, em seguida, clique em **Pré-visualizar** novamente.
- Use o **menu Relatórios** para selecionar um formato de exportação (incluindo o formato padrão, PDF) e clique em  para exportar o relatório. Para obter mais informações sobre o menu Relatórios, consulte Como usar o menu Relatórios.
- Use a **barra de ferramentas Relatórios** para ver, manipular ou imprimir o relatório. Para obter mais informações sobre a barra de ferramentas Relatórios, consulte Usar a barra de ferramentas Relatórios.

Gerar um relatório de máquina protegida sob demanda

Você pode gerar um Relatório do trabalho ou um Relatório de falhas para qualquer máquina protegida.

Execute as etapas do procedimento a seguir para gerar um relatório para uma máquina protegida.

1 Navegue até o Rapid Recovery Core Console.

2 No menu Máquinas protegidas, selecione a máquina protegida da qual você quer ver um relatório.

A página de resumo da máquina protegida selecionada é exibida.

3 Na parte superior da página, nas opções de menu ao lado do nome da máquina protegida, clique na seta virada para baixo próxima a Relatórios e selecione um tipo de relatório.

- Se você quiser gerar um relatório de todos os trabalhos relacionados a essa máquina protegida, incluindo os trabalhos com falha, clique em **Relatório do trabalho** e comece a especificar os critérios do relatório.
- Se você quiser gerar apenas uma lista de trabalhos com falhas relacionados a essa máquina protegida, clique em **Relatório de falhas** e comece a especificar os critérios do relatório.

4 Para um Relatório do trabalho ou de falhas, selecione um período no menu suspenso **Período**.

Se você não escolher um período, a opção padrão (Últimos 31 dias) será usada. Você pode escolher uma das opções da tabela a seguir.

Opção	Descrição
Últimas 24 horas	Reporta a atividade do último dia, relativo ao horário em que o relatório for gerado.
Últimos 7 dias	Reporta a atividade da semana anterior, relativo ao horário em que o relatório for gerado.
Últimos 31 dias	Reporta a atividade dos últimos 31 dias, relativo ao horário em que o relatório for gerado.
Últimos 90 dias	Reporta a atividade dos últimos 90 dias, relativo ao horário em que o relatório for gerado.
Últimos 365 dias	Reporta a atividade do ano anterior, relativo ao horário em que o relatório for gerado.
Desde o começo	Esse período abrange toda a vida útil do Core.
Personalizada	Esse período exige que você ainda especifique as datas de início e de fim.
Mês até a data	Reporta a atividade do primeiro dia do mês atual até a data em que o relatório for gerado.
Ano até a data	Reporta a atividade do primeiro dia do ano atual até a data em que o relatório for gerado.

NOTA: Em todos os casos, não existem dados de relatório disponíveis anteriores a implantação do Core, ou de antes de as máquinas serem protegidas no Core.

5 No menu suspenso **Tipos de trabalho**, selecione os tipos de trabalho adequados.

Por padrão, esse conjunto de informações inclui todos os trabalhos para as máquinas protegidas selecionadas. Nos parâmetros do relatório, você pode personalizar o relatório. Use os filtros para selecionar ou excluir todos os trabalhos na categoria Principais trabalhos e todos os trabalhos na categoria Outros trabalhos. Ou você pode expandir cada uma dessas categorias ao definir parâmetros do trabalho e selecionar apenas os tipos de trabalho de cada categoria que você deseja que apareça no relatório. Clique na caixa de seleção de qualquer tipo de trabalho para marcá-lo ou desmarcá-lo. Você pode selecionar alguns ou todos os trabalhos de cada categoria.

6 Clique em **Pré-visualizar** para gerar o relatório com os critérios especificados.

Se os critérios de relatório selecionados não forem encontrados, o relatório ainda assim será gerado, mas com uma linha vazia. Por exemplo, se não houver erros, o conteúdo da coluna Erro será null no relatório.

7 Realize um dos procedimentos a seguir:

- Visualize o relatório gerado on-line.
- Atualize o relatório dinamicamente alterando um dos critérios e, em seguida, clique em **Pré-visualizar** novamente.
- Use o menu **Relatórios** para selecionar um formato de exportação e exportar o relatório. Para obter mais informações sobre o menu Relatórios, consulte Como usar o menu Relatórios.
- Use a **barra de ferramentas Relatórios** para ver, manipular ou imprimir o relatório. Para obter mais informações sobre a barra de ferramentas Relatórios, consulte Usar a barra de ferramentas Relatórios.

Gerenciar relatórios programados do Core Console

Você pode programar qualquer um dos relatórios disponíveis a partir do Core Console. A programação de um relatório fará com que ele seja gerado repetidamente no futuro. A programação define se o relatório deve ser gerado diariamente, semanalmente ou mensalmente.

Como opção, o Rapid Recovery permite que você envie uma notificação de e-mail a um ou mais destinatários quando cada relatório for gerado. O e-mail especifica o tipo de relatório, o formato do relatório e o período, e inclui o relatório como um anexo.

NOTA: Antes de enviar os relatórios por e-mail, você precisa configurar um servidor SMTP para o Core. Para obter mais informações, consulte Configurar um servidor de e-mail.

Independentemente de optar pelo envio de notificações de e-mail, você pode salvar os relatórios gerados localmente ou em um local de rede acessível ao servidor Core.

Você precisa especificar uma notificação de e-mail e entrega, ou que você precisa especificar um local onde os relatórios serão salvos. Você pode também escolher as duas opções.

Esta seção inclui os seguintes tópicos:

Links relacionados

Programar um relatório
Modificar uma programação de relatório
Pausar, retomar ou excluir um relatório programado

Programar um relatório

Você pode programar um relatório disponível a partir do Core Console. Em seguida, o relatório é gerado de acordo com a programação definida até que você pause ou apague o relatório.

Você precisa especificar uma notificação de e-mail e entrega, ou que você precisa especificar um local onde os relatórios serão salvos. Você pode também escolher as duas opções.

Execute as etapas deste procedimento para programar um relatório.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em (Mais) e, em seguida, selecione **Relatórios**.
A página **Relatório do trabalho** é mostrada. Um seta virada para baixo aparece à direita do atual nome do relatório.

3 Clique na seta à direita do nome do relatório e selecione **Relatórios programados** no menu suspenso.
A página **Relatórios programados** é exibida.

4 Para programar um relatório a ser gerado regularmente, clique em **Adicionar**.
O **Assistente de definição do programa de relatório** é exibido.

5 Na página **Configuração** do assistente, digite os detalhes para o relatório que você deseja programar e, em seguida, clique em **Avançar**. As opções de configuração são descritas na tabela a seguir.

Tabela 161. Opções de configuração de relatório programado

Máquina	Relatórios disponíveis
Nome	Digite o nome de exibição que você quer atribuir a essa programação específica. O nome padrão é Agendar relatório 1. Limite o nome em 64 caracteres ou menos. Não use caracteres proibidos ou frases proibidas.
Formato do relatório	Selecione um formato de saída para o relatório. Se você não selecionar um valor, o formato padrão (pdf) será usado.
Tipo de relatório	Selecione o tipo de relatório que você quer gerar de forma regular.
Rótulos	Selecione os rótulos que você quer que apareça no seu relatório programado. É preciso selecionar pelo menos um rótulo. O recurso Grupos personalizados permite que você agrupe objetos do Core em um contêiner lógico, para o qual você define um rótulo. Ao usar o parâmetro Rótulos no Assistente de definição do programa de relatório, você pode selecionar um grupo personalizado para o qual relatórios programados serão executados. Se não houver nenhum rótulo personalizado, as opções disponíveis no menu suspenso Rótulos são Selecionar todos e Máquinas protegidas. Se forem mostrados grupos personalizados, cada grupo aparece como uma opção.

Máquina	Relatórios disponíveis
	Você pode selecionar ou desmarcar qualquer uma das opções para incluir ou excluir esses objetos no relatório programado.
Máquina protegida	Selecione uma ou mais máquinas protegidas a serem incluídas no relatório. Esta opção não está disponível para o relatório do repositório.
Tipos de trabalho	Selecione os tipos de trabalho que você quer que apareça no relatório. Por padrão, esse conjunto de informações contém os trabalhos de todas as máquinas, ou seja, todas as máquina protegidas, replicadas e de ponto de recuperação apenas, nos Cores especificados. Nos parâmetros do relatório, você pode personalizar o relatório. Use os filtros para selecionar ou excluir algumas máquinas. Você pode também selecionar ou excluir trabalhos que são independentes de máquina; nesse caso, o relatório mostrará apenas o status dos trabalhos do Core. O parâmetro Tipos de trabalho não está disponível para os tipos de relatórios programados Resumo do Core e Repositório.

6 Na página **Destino** do assistente, selecione um destino para os relatórios que você deseja programar. Você precisa escolher uma ou ambas as opções a seguir. Quando estiver satisfeito, clique em **Avançar**.

- No campo **Enviar para endereços de e-mail**, digite um ou mais endereços de e-mail válidos para notificar os usuários por mensagem de e-mail quando um relatório programado for gerado.

  NOTA: Se você não especificar as notificações de e-mail e a entrega, você precisará especificar um local de armazenamento.

- Selecione **Salvar como arquivo** para salvar os arquivos do relatório gerado em um local que você especificar, e no menu suspenso **Tipo de local**, selecione uma opção de local, rede ou armazenamento na nuvem. Em seguida, no campo **Local**, especifique as informações adicionais de local conforme descrito na tabela a seguir.

Tabela 162. Opções de Local para relatórios programados

Tipo de local	Descrição do tipo de local	Local
Local	Selecione o tipo de local Local para salvar os relatórios gerados em um caminho local que o Core pode acessar.	Especifique o caminho no campo Local. Digite um local acessível ao Core localmente. Por exemplo, para armazenar relatórios na pasta Relatórios da unidade D, digite **D:\Relatórios**.
Rede	Selecione o tipo de local Rede para salvar os relatórios gerados em um caminho que o Core pode acessar na rede. Especifique o caminho no campo Local.	Especifique o caminho no campo Local. Digite um local acessível ao Core na rede. Use o formato \\servername\sharename. Por exemplo, para armazenar relatórios sobre o servidor de dados na pasta compartilhada chamada Relatórios, digite **\\Data\Relatórios**. Especifique as credenciais de rede nos campos Nome de usuário e Senha.
Nuvem	Selecione o tipo de local Nuvem para salvar os relatórios gerados em uma conta de armazenamento na nuvem configurada no Core. A conta de armazenamento já deve estar definida antes de executar esta etapa. Para obter informações sobre como configurar uma conta de	No campo Conta, selecione a conta de armazenamento na nuvem para usá-la para armazenar os relatórios gerados. No campo Contêiner, especifique um contêiner adequado na conta de armazenamento. No campo Nome da pasta, especifique a pasta onde os relatórios gerados futuros devem ser armazenados.

Tipo de local	Descrição do tipo de local	Local
	armazenamento na nuvem para funcionar com o Core, consulte Gerenciar contas de nuvem.	

7 Quando estiver satisfeito com as opções de destino, clique em **Avançar**.

8 Na página **Programa** do assistente, no menu **Enviar dados**, selecione uma opção para determinar com que frequência o relatório especificado deve ser gerado. Você pode gerar relatórios diariamente, semanalmente ou mensalmente. Cada opção tem seus próprios parâmetros, conforme descrito na tabela a seguir.

Tabela 163. Opções de frequência para a geração dos relatórios programados

Frequência	Detalhes de frequência	Parâmetros de frequência
Diariamente	Gera e salva ou envia o relatório especificado uma vez por dia no horário definido. O horário padrão para esta ação é 12:00 (com base na hora do servidor do Core).	Para alterar o horário padrão que o relatório é gerado, no campo de texto de hora, digite um novo valor ou use os controles para alterar a hora, os minutos e AM ou PM.
Semanalmente	Gera e salva ou envia o relatório especificado uma vez por semana no horário e dia definidos. O horário padrão para esta ação é domingo às 12:00 (com base na hora do servidor do Core).	Para alterar o dia padrão que o relatório é gerado, no menu do dia da semana, selecione um dia da semana. Para alterar o horário padrão que o relatório é gerado, no campo de texto de hora, digite um novo valor ou use os controles para alterar a hora, os minutos e AM ou PM.
Mensalmente	Gera e salva ou envia o relatório especificado uma vez por mês na data e horário definidos. A data padrão para esta ação é o primeiro dia de cada mês às 12:00 (com base na hora do servidor do Core).	Para alterar a data padrão que o relatório é gerado, no menu do dia do mês, selecione uma data. Para alterar o horário padrão que o relatório é gerado, no campo de texto de hora, digite um novo valor ou use os controles para alterar a hora, os minutos e AM ou PM.

9 Opcionalmente, na página **Programa** do assistente, se você quiser impedir que o relatório programado seja gerado até que você retome os relatórios pausados, selecione **Pausar geração de relatórios inicialmente**.

Se você quiser que este relatório seja gerado conforme programado, desmarque essa opção.

10 Quando estiver satisfeito com o programa, clique em **Concluir** para sair do assistente e salve o trabalho.

O novo programa de relatório é mostrado na tabela de resumo Relatórios resumidos.

Modificar uma programação de relatório

Depois que um relatório está programado, você pode modificar qualquer um de seus parâmetros ou detalhes. Você pode editar as informações de configuração do relatório (nome do relatório, formato de saída, tipo de relatório, repositórios incluídos. Você pode também alterar as opções de notificação por e-mail e o destino em que o relatório gerado será salvo. Por fim, você pode também alterar a programação do relatório.

Execute este procedimento para modificar os parâmetros de um relatório programado.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em (Mais), e, em seguida, selecione **Relatórios**.

A página **Relatório do trabalho** é mostrada. Um seta virada para baixo aparece à direita do atual nome do relatório.

3 Clique na seta à direita do nome do relatório e selecione **Relatórios programados** no menu suspenso.

A página **Relatórios programados** é exibida.

4 Na tabela de resumo Relatórios programados, na linha do relatório que você quer modificar, clique no ícone Configurações e, em seguida, selecione **Editar**.

O **Assistente de definição do programa de relatório** é exibido.

5 Navegue pelas páginas desse assistente, alterando todos os parâmetros necessários. Para obter informações sobre algum parâmetro deste assistente, consulte o tópico Programar um relatório.

6 Na página **Programa** do assistente, clique em **Concluir** para fechar o assistente e salvar as alterações.

O assistente irá fechar e a programação do relatório estará modificado.

Pausar, retomar ou excluir um relatório programado

Depois de programar um relatório, ele será gerado conforme a programação definida. Se você quiser interromper temporariamente a geração de um relatório programado, você pode pausar a programação.

Se um relatório programado estiver pausado e você desejar retomar a geração do relatório, você pode retomar o relatório conforme descrito neste procedimento.

Se um relatório programado estiver sendo gerado e você já não precisa dele, você pode apagá-lo.

Para determinar se um relatório programado está pausado, verifique a coluna status da tabela de resumo de relatórios programados. Uma esfera verde indica um relatório programado ativo; uma esfera amarela indica uma programação pausada; e uma esfera vermelha indica um erro.

Execute as etapas deste procedimento para pausar, retomar ou excluir uma programação de um relatório.

1 Navegue até o Rapid Recovery Core Console.

2 Na barra de ícones, clique em  (Mais), e, em seguida, selecione **Relatórios**.

A página **Relatório do trabalho** é mostrada. Um seta virada para baixo aparece à direita do atual nome do relatório.

3 Clique na seta à direita do nome do relatório e selecione **Relatórios programados** no menu suspenso.

A página **Relatórios programados** é exibida.

4 Na tabela de resumo Relatórios programados, veja o status de todos os relatórios programados por meio dos indicadores coloridos.

5 Para cada relatório que você quiser pausar ou retomar, selecione a caixa de verificação na primeira coluna.

6 A partir das opções dos Relatórios programados acima da tabela de resumo, você pode fazer o seguinte:

- Para pausar a geração dos relatórios selecionados, clique em **Pausar**.
- Para retomar a geração de relatórios programados anteriormente pausados, clique em **Retomar**.
- Para apagar as programações selecionadas de relatórios programados existentes, clique em **Excluir**.

  Apagar um relatório programado apenas impede a geração de futuros relatórios. Relatórios programados salvos anteriormente não são removidos.

Como usar o menu Relatórios

O menu Relatórios aparece na parte superior da página ao exibir os relatórios. Este menu inclui o título do relatório, o qual também é um menu suspenso que permite que você veja quais tipos de relatório estão disponíveis. Abaixo deste menu há um ou mais filtros que ajudam você a definir seus critérios de relatório.

Os filtros específicos disponíveis dependem do tipo de relatório. Para obter informações sobre os parâmetros que se aplicam a cada tipo de relatório, consulte o respectivo tópico para entender esse tipo de relatório.

No lado direito do menu de relatórios, são exibidos alguns controles. Estes controles, descritos na tabela a seguir, ajudam você a gerar e exportar o relatório.

Tabela 164. Controles do menu de relatórios

Elemento de UI	Descrição
Botão de pré-visualização	Clique no botão de pré-visualização para gerar um relatório com base no tipo de relatório selecionado e nos parâmetros de relatório especificados nos filtros.
Menu suspenso para o formato de exportação	O menu suspenso Exportar permite que você selecione um formato de saída para o relatório. Se você não selecionar um valor, o formato padrão (pdf) será usado.
Botão/ícone de download	O botão de download exporta o relatório gerado no tipo de formato selecionado no menu Exportar.

Os relatórios incluem as unidades de medida, o que torna mais fácil determinar se uma coluna é representada em GB, TB ou segundos.

Se você não estiver satisfeito com a aparência de um relatório gerado ou exportado, você pode alterar a fonte usada nos relatórios. Para obter mais informações, consulte Gerenciamento de definições de relatórios.

Depois que um relatório é gerado, você pode usar a barra de ferramentas dos relatórios.

Links relacionados

Noções básicas sobre o relatório do trabalho
Noções básicas sobre o relatório de falhas
Noções básicas sobre o relatório resumido
Como entender relatórios de núcleo do Console de Gerenciamento central

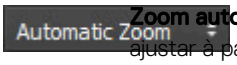
Usar a barra de ferramentas Relatórios

Depois de gerá-lo a partir do menu Relatórios, o relatório é mostrado abaixo da barra de ferramentas Relatórios. A barra de ferramentas pode ajudar a manipular a saída do relatório, incluindo salvar e imprimir os relatórios.

No lado esquerdo da barra de ferramentas, há uma opção de barra lateral Alternar. Essa ferramenta expande ou encolhe a barra lateral, dando acesso a mais algumas opções de vídeo. À direita da barra de ferramentas, a opção Ferramentas expande um menu suspenso fornecendo os controles de navegação do relatório. Os elementos da barra de ferramentas Relatórios são descritos na tabela a seguir.

Tabela 165. Ícones da barra de ferramentas de relatórios

Ícone	Descrição
	**Barra lateral Alternar**. Todas as páginas do relatório são exibidas como miniaturas. Outras opções na barra lateral não são suportadas.
	**Barra lateral: Mostrar miniaturas**. Esta é a exibição padrão para todas as páginas de um relatório gerado.
	**Barra lateral: Mostrar contorno do documento**. Esse recurso não é suportado.
	**Barra lateral: Mostrar anexos**. Não há anexos para relatórios. Esse recurso não é suportado.
	**Procurar**. Permite que você pesquise um texto dentro do relatório gerado. Inclui opções para destacar todos os textos que correspondem aos critérios inseridos, e também coincidir ou não maiúsculas e minúsculas.

Ícone	Descrição
	**Página anterior**. Move a visualização do relatório para a página anterior.
	**Próxima página**. Segue para a próxima página na visualização do relatório.
	**Inserir o número da página**. Clique no campo de texto do número da página, digite um número de página válido e, em seguida, pressione Enter para ir até essa página na visualização do relatório.
	**Diminuir o zoom**. Permite que você diminua o zoom da visualização do relatório gerado. Cada clique sucessivo afasta ainda mais o zoom, até um mínimo de 25%.
	**Aumentar o zoom**. Permite que você aumente o zoom da visualização do relatório gerado. Cada clique sucessivo aproxima ainda mais o zoom, até um máximo de 1000%.
	**Zoom automático**. Permite que você controle a exibição do zoom do relatório gerado, incluindo visualizar no tamanho real, ajustar à página, largura total ou por porcentagem, incluindo 50%, 75%, 100%, 125%, 150%, 200%, 300% ou 400%.
	**Abrir arquivo**. Permite que você navegue no sistema de arquivos para localizar e abrir um relatório salvo.
	**Imprimir**. Permite imprimir o relatório gerado.
	**Ferramentas**. O menu suspenso Ferramentas expande ou retrai ao clicar neste ícone. As opções de Ferramentas estão descritas abaixo.
	**Ferramentas: Ir para a primeira página**. Leva você para a primeira página do relatório gerado.
	**Ferramentas: Ir para a última página**. Leva você para a última página do relatório gerado.
	**Ferramentas: Girar no sentido horário**. Esta opção gira a tela do relatório gerado no sentido horário.
	**Ferramentas: Girar no sentido anti-horário**. Esta opção gira a tela do relatório gerado no sentido anti-horário.
	**Ferramentas: Ferramenta de mão**. Ao selecionar esta ferramenta, permite que você mova o relatório ao clicar e arrastar ele pela tela.
	**Ferramentas: Propriedades do documento**. Fornece informações sobre as propriedades do documento do relatório gerado. Clique em **Fechar** para fechar esta janela.

Para obter informações sobre como gerar um relatório, consulte Gerar um relatório no Core Console. Para obter informações sobre como gerar um relatório para vários cores no Central Management Console, consulte Gerar um relatório no Central Management Console.

Noções básicas sobre o relatório do trabalho

O Relatório do trabalho está disponível para o Rapid Recovery Core e para as máquinas protegidas no Core. Ele fornece uma maneira de visualizar o status dos trabalhos realizados por um Core ou uma máquina protegida selecionado. Linhas ou colunas de dados no relatório sem dados indicam que o parâmetro testado estava null. Por exemplo, se uma coluna (por exemplo, Erros) aparece sem qualquer informação, então não ocorreram erros para o registro selecionado. Se o relatório gera uma linha em branco, o trabalho para o registro selecionado reflete a atividade independente da máquina.

Para obter informações sobre como gerar um relatório do trabalho a partir do Core, consulte Gerar um relatório de Core sob demanda. Para obter informações sobre como gerar um relatório do trabalho para uma máquina protegida, consulte Gerar um relatório de máquina protegida sob demanda.

Ao gerar um relatório do trabalho, os detalhes do relatório são os seguintes:

- Critérios de seleção do relatório
- Uma tabela de resumo que mostra uma linha para cada trabalho no período especificado. Além de apresentar o Core, a máquina protegida e o tipo de trabalho adequados, cada linha contém:
  - Um resumo do trabalho
  - O status do trabalho
  - Todos os erros relacionados com o trabalho
  - As datas de início e término do trabalho
  - A duração do trabalho em segundos
  - O trabalho total em MB

Se as informações não forem relevantes para uma determinada categoria, essa célula será mostrada no relatório sem informações. Por exemplo, se o Core de uma determinada máquina protegida não contiver erros, a coluna Erro ficará em branco para essa linha do relatório.

Noções básicas sobre o relatório de resumo dos trabalhos

O relatório de resumo dos trabalhos está disponível ao reportar da perspectiva do Core apenas; este relatório não está disponível a partir dos relatórios de uma máquina protegida. Este relatório tem um resumo único, mostrando informações resumidas sobre todos os trabalhos executados no Core, incluindo uma contagem de trabalhos com falha, concluídos e cancelados. Ele mostra mais detalhes do que o relatório do trabalho, pois especifica cada trabalho como uma linha separada no relatório.

Para obter informações sobre como gerar um relatório de resumo dos trabalhos, consulte Gerar um relatório no Core Console.

Os parâmetros do relatório para esse tipo de relatório são:

- Intervalo de datas
- Máquinas protegidas
- Tipos de trabalho

Ao gerar um relatório de resumo dos trabalhos, os detalhes do relatório contêm os critérios de seleção para o relatório, bem como informações sobre máquinas protegidas, volumes e tipos de trabalho.

Informações do Core

A parte do Relatório resumido referente ao Core contém dados em relação ao Rapid Recovery Core sendo reportado. Essas informações incluem:

- O número de máquinas protegidas no Rapid Recovery Core

- O número de máquinas com trabalhos com falha

Resumo das máquinas protegidas

A parte do Relatório resumido referente às máquinas protegidas contém dados de todas as máquinas protegidas por um ou mais Rapid Recovery Cores selecionados e os volumes nessas máquinas.

A tabela mostra uma linha para cada tipo de trabalho de cada máquina, e contém a proporção de trabalhos bem-sucedidos (de qualquer tipo), o número de trabalhos concluídos, o número de trabalhos com falha e o número de trabalhos cancelados. (Os trabalhos cancelados não são considerados nessas estatísticas.)

Noções básicas sobre o relatório de falhas

O Relatório de falhas é um subconjunto do Relatório do trabalho e está disponível para o Rapid Recovery Core e para as máquinas protegidas no Core. O Relatório de falhas contém apenas os trabalhos cancelados e com falha relacionados no Relatório do trabalho e os compila em um único relatório que pode ser impresso e exportado. Se o relatório for gerado com uma linha em branco, não houve erros no período especificado nos critérios de relatório.

NOTA: Os resultados para os parâmetros de máquinas protegidas e Cores de destino aparecem apenas no relatório do nível do Core.

Para obter informações sobre como gerar um relatório do trabalho a partir do Core, consulte Gerar um relatório de Core sob demanda. Para obter informações sobre como gerar um relatório do trabalho para uma máquina protegida, consulte Gerar um relatório de máquina protegida sob demanda.

Ao gerar um Relatório de falhas, uma tabela de resumo que mostra uma linha para cada trabalho no período especificado. Além de apresentar o Core, a máquina protegida e o tipo de trabalho adequados, cada linha contém:

- Um resumo do trabalho
- O status do trabalho
- Todos os erros relacionados com o trabalho
- As datas de início e término do trabalho
- A duração do trabalho em segundos
- O trabalho total em MB

Noções básicas sobre o relatório resumido

O Relatório resumido está disponível para um ou mais Cores. Este relatório não está disponível entre relatórios de uma máquina protegida. O relatório resumido inclui informações sobre os repositórios no Rapid Recovery Core selecionado e as máquinas protegidas por esse Core. As informações aparecem como dois resumos dentro de um relatório.

Para obter informações sobre como gerar um Relatório resumido, consulte Gerar um relatório no Core Console.

Os parâmetros do relatório para esse tipo de relatório são:

- Intervalo de datas
- Máquinas protegidas

Ao gerar um Relatório resumido, os detalhes do relatório contêm os critérios de seleção para o relatório, bem como informações sobre repositórios e máquinas protegidas.

Informações do Core

A parte do Relatório resumido referente ao Core contém dados em relação ao Rapid Recovery Core sendo reportado. Essas informações incluem:

- A chave de licença (identificador)
- A versão atual do software Rapid Recovery Core

Resumo de repositórios

A parte do Relatório resumido referente aos Repositórios contém dados dos repositórios localizados no Rapid Recovery Core selecionado. Essas informações incluem:

- O número de repositórios no Rapid Recovery Core
- Um resumo dos repositórios no Core.

Resumo das máquinas protegidas

A parte do Relatório resumido referente às máquinas protegidas contém dados de todas as máquinas protegidas por um ou mais Rapid Recovery Cores selecionados. Inclui um gráfico e uma tabela de resumo.

A tabela mostra as máquinas protegidas na proporção de trabalhos bem-sucedidos (de qualquer tipo), em comparação aos trabalhos com falha. (Os trabalhos cancelados não são considerados nessas estatísticas.)

O X ou eixo horizontal mostra o número de máquinas protegidas. O Y ou eixo vertical mostra as camadas de sucesso. Especificamente, o eixo Y mostra, por máquina protegida, as quantidades:

- Não foram realizados trabalhos
- Menos de 50% bem-sucedidos
- 50% ou mais bem-sucedidos
- 100% bem-sucedidos

Abaixo do gráfico, são mostradas informações sobre as máquinas protegidas. Essas informações incluem:

- A quantidade de máquinas protegidas
- O número de máquinas protegidas com trabalhos com falha
- Uma tabela de resumo por máquina protegida, que mostra:
  - Nome da máquina protegida
  - Os volumes protegidos pela máquina
  - Espaço protegido, em GB (total e atual)
  - Taxa de alteração diária (média e mediana)
  - Estatísticas do trabalho (bem-sucedidos, concluídos, com falha, cancelados)
  - Se a criptografia foi aplicada
- A versão do Core

Noções básicas sobre o relatório do Repositório

O relatório do Repositório inclui informações sobre os repositórios no Rapid Recovery Core selecionado e as máquinas protegidas por esse Core. As informações aparecem como dois resumos dentro de um relatório.

Para obter informações sobre como gerar um relatório do Repositório do Core, consulte Gerar um relatório de Core sob demanda.

Os parâmetros para esse tipo de relatório incluem somente repositórios.

Ao gerar um relatório de repositório, os detalhes do relatório para cada repositório contêm uma lista de resumo dos repositórios no Core.

O Central Management Console

O Central Management Console do Rapid Recovery é um componente opcional que se destina a ambientes com dois ou mais Rapid Recovery Cores. Esse componente é um portal Web que fornece uma interface central onde você pode agrupar, gerenciar e gerar relatórios para vários Cores.

Os requisitos do sistema operacional do Console de Gerenciamento Central são idênticos aos requisitos do Rapid Recovery Core. Esses componentes podem ser instalados na mesma máquina ou em máquinas diferentes, conforme as necessidades determinam.

Após a instalação, você deverá configurar o Console de Gerenciamento Central adicionando Cores que deseja gerenciar, individualmente ou como parte dos grupos do Core.

NOTA: Você precisa executar o instalador com privilégios de administrador local.

Os sistemas operacionais Windows 8, 8.1 e 10, além dos sistemas operacionais Windows Server 2012 e 2012 R2, deve ter o recurso ASP.NET 4.5 instalado no servidor para que haja carregamento apropriado da GUI. Essa configuração está incluída como parte do instalador do Rapid Recovery.

Para obter mais informações sobre como instalar esse componente, consulte o tópico "Como instalar o Rapid Recovery Central Management Console" no Guia de instalação e upgrade do *Dell Data Protection | Rapid Recovery*.

Para obter mais informações sobre como configurar esse componente, consulte o tópico Como configurar o Rapid Recovery Central Management Console no Guia do usuário do *Dell Data Protection | Rapid Recovery*.

Para obter mais informações sobre noções básicas da UI desse componente, consulte o tópico Noções básicas sobre o Console de gerenciamento central do Rapid Recovery no Guia do usuário do *Dell Data Protection | Rapid Recovery*.

Noções básicas sobre o Console de gerenciamento central do Rapid Recovery

Quando você abre o Console de gerenciamento central, as informações são exibidas na vista Console. A página **Bem-vindo** é exibida, e você pode ver o seguinte:

Tabela 166. Elementos da UI no Console de gerenciamento central do Rapid Recovery

Elemento de UI	Descrição
Área de imagem corporativa	Para ambientes típicos, o lado superior esquerdo do Console de gerenciamento central tem o nome do produto pai completo, Dell Data Protection | Rapid Recovery. O clique em qualquer lugar na área da marca resulta na direção do usuário do navegador Web para a documentação do produto no site do Suporte da Dell.
Área de navegação esquerda	A área de navegação esquerda aparece abaixo da área de imagem corporativa, no lado esquerdo da interface de usuário. As funções de área de navegação diferem com base no modo selecionado no canto superior direito do Central Management Console **Modo Console.** Na área de navegação, quando no modo Console, clicar em qualquer Core ou Grupo de Cores abre o Núcleos ou os Grupos de Core selecionado no Rapid Recovery Core Console. **Modo Relatórios.** Na área de navegação, quando no modo Relatórios, selecionar Núcleos ou grupos de Core determina o conjunto de informações que aparecerá ao gerar relatórios.

Elemento de UI	Descrição
	Modo Gerenciar. Na área de navegação, quando no modo Gerenciar, você pode navegar pelas configurações para Núcleos e Grupos de Core. Você pode também adicionar e remover Núcleos e Grupos de Core no modo Gerenciar. O clique nas setas expande e minimiza o menu. Estão incluídos os seguintes níveis de hierarquia: Organização, Grupos de Core e Núcleos. Se você clicar na seta para a esquerda, a área de navegação é recolhida. Para expandir a área de navegação, clique na seta para a direita.
Menu Links	**Entre em contato com o Suporte da Dell.** Links para o site do Suporte da Dell em uma nova janela do navegador, dando acesso ao Live Chat, aos tutoriais em vídeo, aos artigos da base de conhecimento do Rapid Recovery, às perguntas frequentes e muito mais.
Menu Links	**Documentação.** Links para o site do Suporte da Dell em uma nova janela do navegador, dando acesso ao Live Chat, aos tutoriais em vídeo, aos artigos da base de conhecimento do Rapid Recovery, às perguntas frequentes e muito mais.
Menu Links	**Versão.** Lista a versão atual do Central Management Console. O clique neste link abre a caixa de diálogo Sobre.
Menu Links	**Seletor de modo.** No canto superior direito do menu de links, o nome do usuário do Windows conectado no momento é exibido em um menu suspenso. Nesse menu, você pode alterar a vista do Console de Gerenciamento Central. Você pode escolher dentre as seguintes vistas: **Console.** Esse é o modo padrão, que permite visualizar os Núcleos e os grupos de Core no ambiente de um local. **Relatórios.** Nesse modo, você pode gerar, ver e exportar relatórios dos Núcleos configurados nesse console. **Gerenciar.** No modo Gerenciar, você pode remover ou adicionar núcleos adicionais ao Console de Gerenciamento Central, isoladamente ou em grupos. **Idioma.** Nas versões que suportam localização, a opção Idioma é mostrada. A seleção desta opção abre a caixa de diálogo Trocar idioma, a partir da qual você pode selecionar um idioma de exibição para o Central Management Console. . **Limpar cache da conta.** Selecione essa opção para limpar informações existentes da conta do usuário conectado.

Você pode alterar a vista do Console de Gerenciamento Central selecionando uma opção no seletor de modo (o menu suspenso no canto superior direito da página). Por exemplo:

- Para gerenciar Cores ou grupos de núcleos já configurados, use a vista Console.
- Para configurar o Console de Gerenciamento Central, alterne para a vista Gerenciar.
- Para gerar relatórios, alterne para a vista Relatórios.

Os Cores que você pode ver e gerenciar são exibidos no menu de navegação à esquerda. Você pode configurar Cores individuais ou organizá-los por grupo. Você pode restringir o acesso a Cores em grupos específicos usando nomes de usuário ou grupos do Windows.

Como configurar o Rapid Recovery Central Management Console

Como configurar o Rapid Recovery Central Management Console envolve adicionar Cores e grupos de núcleos, estabelecer as configurações e especificar configurações de acesso para grupos, se necessário.

Após concluir a configuração, será possível gerenciar as definições e todas as Cores de um local central.

Para configurar o Central Management Console, você pode executar todas as tarefas apresentadas nos links relacionados abaixo.

Links relacionados

Como adicionar um Core ao Console de Gerenciamento Central
Como configurar definições do Core no Console de Gerenciamento Central
Como adicionar um grupo de Core ao Console de Gerenciamento Central
Configuração das definições do grupo de Cores
Configuração do acesso ao grupo de Cores

Como adicionar um Core ao Console de Gerenciamento Central

Se você quiser adicionar um núcleo a um grupo de Cores, o grupo precisará ser criado primeiro. Para obter mais informações, consulte Como adicionar um grupo de Core ao Console de Gerenciamento Central. Você também pode editar os detalhes do núcleo depois para especificar um grupo.

Adicione um ou mais Cores ao Console de Gerenciamento Central para gerenciá-los ou gerar relatórios de uma única interface.

Conclua as etapas no procedimento a seguir para adicionar um Core ao Console de Gerenciamento Central.

1 No Console de Gerenciamento Central do Rapid Recovery, clique no menu suspenso do seletor de modo e selecione **Gerenciar**.
A página é atualizada, mostrando os ícones de Adicionar Core, Adicionar Grupo e Excluir.
2 Na parte superior do menu de navegação à esquerda, clique em **Adicionar Core**.
A página **Adicionar Core** é exibida.
3 Especifique as informações obrigatórias de conexão ao Core, conforme descrito na tabela a seguir.

Tabela 167. Adicionar detalhes do núcleo

Caixa de texto	Descrição
Grupo principal	Como opção, se você quiser que o Core ingresse em um grupo de Cores existente, selecione o grupo pai na organização apropriada.
Nome de exibição	Insira um nome de exibição para o Core. O nome de exibição deve ser limitado a 150 caracteres ou menos. A melhor prática é manter esse nome com menos de 33 caracteres. Não use caracteres proibidos ou frases proibidas. Para obter mais informações sobre caracteres ou frases proibidos, consulte o Guia do usuário do *Dell Data Protection | Rapid Recovery*.
Nome do host	Insira um endereço IP para acessar o Core. Se o Core que você estiver adicionando for o servidor atual, você poderá usar o host local.
Port	Insira um número de porta para a conexão. O valor padrão é 8006.
Nome de usuário	Insira um nome de usuário para acessar o serviço de Core do Core recém-adicionado.
Senha	Insira uma senha para acessar o serviço de Core para o Core recém-adicionado.

4 Clique em **Testar conexão** para testar a configuração.
Se o teste for bem-sucedido, uma mensagem bem-sucedida será exibida. Clique em **OK** para fechar a mensagem de confirmação.
5 Clique em **Salvar**.
As alterações são salvas, e o Core agora é adicionado ao grupo principal.

Links relacionados

Como adicionar um grupo de Core ao Console de Gerenciamento Central

Como configurar definições do Core no Console de Gerenciamento Central

Conclua as etapas no procedimento a seguir para configurar definições do Core no Console de Gerenciamento Central.

1 No Console de Gerenciamento Central do Rapid Recovery, clique no menu suspenso do seletor de modo e selecione **Gerenciar**.
A página é atualizada, mostrando os ícones de Adicionar Core, Adicionar Grupo e Excluir.

2 No menu de navegação à esquerda, clique no nome do Core apropriado.
A página **Definições** é exibida para o Core selecionado.

3 Na guia Definições, modifique as informações do Core conforme descrito na tabela a seguir.

Tabela 168. Definições do Core

Caixa de texto	Descrição
Grupo principal	Selecione o grupo principal dos Cores para as novas definições do Core que você deseja adicionar.
Nome de exibição	Insira um nome de exibição para o Core.
Nome de usuário	Insira o nome de usuário do Core.
Senha	Insira a senha do Core.
Como o portal de gerenciamento deve se conectar ao [nome do Core]?	Selecione a opção que especifica a conexão. Você pode selecionar: • Usar o último endereço IP (xxx.xxx.xxx.xxx) conhecido do [nome do Core] ou • Usar o nome do host ou o endereço IP [nome do host ou endereço IP]. Se você optar por especificar a conexão através do uso de um nome de host ou endereço IP, é necessário inserir as informações apropriadas no campo do endereço IP ou do nome do host.
Em qual porta o [nome do Core] está escutando?	Selecione uma das opções de porta. Você pode selecionar: • Porta padrão (8006) ou • Porta personalizada [porta] Se você optar por especificar uma porta, insira o número da porta no campo Porta personalizada.

4 Clique em **Testar conexão**.
Se o teste for bem sucedido, uma mensagem será exibida para indicar que a conexão foi bem sucedida.

5 Clique em **Salvar**.

Como adicionar um grupo de Core ao Console de Gerenciamento Central

Conclua as etapas no procedimento a seguir para adicionar um grupo de Cores ao Rapid Recovery Central Management Console.

1 No Console de Gerenciamento Central do Rapid Recovery, clique no menu suspenso do seletor de modo e selecione **Gerenciar**.
A página é atualizada, mostrando os ícones de Adicionar Core, Adicionar Grupo de Cores e Excluir.

2 Na parte superior do menu de navegação à esquerda, clique em **Adicionar grupo**.
A página **Adicionar grupo** é exibida.

3 Selecione o grupo principal e o nome de exibição conforme a descrição da tabela a seguir.

Tabela 169. Adição de um grupo de Cores

Caixa de texto	Descrição
Grupo principal	Selecione o grupo principal dos Cores para o novo grupo de Cores que você deseja adicionar.
Nome de exibição	Insira um nome de exibição do grupo de Cores. O nome de exibição deve ser limitado a 150 caracteres ou menos. A melhor prática é manter esse nome com menos de 33 caracteres. Não use caracteres proibidos ou frases proibidas. Para obter mais informações sobre caracteres ou frases proibidos, consulte o Guia do usuário do *Dell Data Protection | Rapid Recovery*.

4 Clique em **Salvar**.

Links relacionados

Como adicionar um grupo de Core ao Console de Gerenciamento Central

Configuração das definições do grupo de Cores

Antes de poder configurar as definições ou o acesso ao grupo de Cores, o grupo precisa ser criado. Para obter mais informações, consulte Como adicionar um grupo de Core ao Console de Gerenciamento Central.

Execute as etapas do procedimento a seguir para configurar as definições do grupo de Cores.

1 No Console de Gerenciamento Central do Rapid Recovery, clique no menu suspenso do seletor de modo e selecione **Gerenciar**.
A página é atualizada, mostrando os ícones de Adicionar Core, Adicionar Grupo de Cores e Excluir.
2 No menu de navegação à esquerda, clique no nome do grupo de Cores que você deseja configurar.
A página Definições é exibida para o grupo de Cores selecionado.
3 Modifique as informações do grupo de Cores conforme descrito na tabela a seguir.

Tabela 170. Definições do grupo de Cores

Caixa de texto	Descrição
Grupo principal	Selecione o grupo principal dos Cores para as definições do novo grupo de Cores que você deseja adicionar.
Nome de exibição	Insira um nome de exibição do grupo de Cores. O nome de exibição deve ser limitado a 150 caracteres ou menos. A melhor prática é manter esse nome com menos de 33 caracteres. Não use caracteres proibidos ou frases proibidas. Para obter mais informações sobre caracteres ou frases proibidos, consulte o Guia do usuário do Dell Data Protection | Rapid Recovery.

4 Clique em **Salvar**.

Configuração do acesso ao grupo de Cores

Antes de poder configurar as definições ou o acesso ao grupo de Cores, o grupo precisa ser criado. Para obter mais informações, consulte Como adicionar um grupo de Core ao Console de Gerenciamento Central.

Para adicionar ou visualizar cores no Console de Gerenciamento Central, a conta de usuário atual deve ser um membro do grupo de administradores de domínio Active Directory. Como alternativa, você pode dar acesso a usuários ou grupos individuais usando esse procedimento.

Conclua as etapas no procedimento a seguir para configurar o acesso ao grupo de Cores.

1 No Console de Gerenciamento Central do Rapid Recovery, clique no menu suspenso do seletor de modo e selecione **Gerenciar**.

A página é atualizada, mostrando os ícones de Adicionar Core, Adicionar Grupo e Excluir.

2 No menu de navegação à esquerda, clique no nome do grupo de Cores que você deseja configurar.

A página **Definições** é exibida para o grupo de Cores selecionado.

3 Clique na guia **Acesso**.

As definições de acesso do grupo Core são exibidas.

4 Clique em **Adicionar**.

A caixa de diálogo **Permitir acesso** é exibida. Você pode dar acesso a um indivíduo ou a um grupo.

5 Realize um dos procedimentos a seguir:

- Se você quiser dar acesso a um indivíduo, no campo de texto **Nome**, digite o nome do indivíduo e clique em **Usuário**. Essa é a opção padrão.

  Por exemplo, digite Administrador (ou, se a máquina estiver em um domínio, [nome do domínio] \Administrador).

- Se você quiser dar acesso a um grupo, no campo de texto **Nome**, digite o nome do grupo e clique em **Grupo**.

  Por exemplo, digite AdminGroup (ou, se a máquina estiver em um domínio, [nome do domínio] \AdminGroup).

6 Clique em **Verificar Nome** para validar se o nome de usuário ou o nome do grupo que você especificou é acessível.

Se o nome digitado for válido, uma mensagem Conta verificada será exibida.

7 Depois que você tiver digitado e validado um nome, clique em **Salvar**.

A caixa de diálogo **Permitir acesso** é fechada, e as configurações são salvas. O nome de acesso é exibido na guia Acesso do grupo Core.

Como entender relatórios de núcleo do Console de Gerenciamento central

O Rapid Recovery permite a você gerar e visualizar relatórios de tarefa, relatórios de falha e informações de resumo para múltiplos núcleos Rapid Recovery. Mais detalhes sobre os Núcleos são apresentados em tabelas de resumo com as mesmas categorias descritas nas seções Noções básicas sobre o relatório do trabalho, Noções básicas sobre o relatório de falhas, e Noções básicas sobre o relatório resumido.

Para obter informações sobre como gerar um relatório para múltiplos núcleos, consulte Gerar um relatório no Central Management Console.

Gerar um relatório no Central Management Console

Conclua o procedimento a seguir para gerar um relatório para vários Rapid Recovery Cores no Central Management Console.

1 No Rapid Recovery Central Management Console, clique no menu suspenso do seletor de modo no canto superior direito e selecione **Relatórios**.

A página de seleção de idioma é mostrada. O CoreJobReport é selecionado por padrão. À direita do nome do relatório, é exibida uma seta para baixo na qual você pode selecionar outro tipo de relatório.

2 No menu de navegação à esquerda, selecione qualquer combinação de Rapid Recovery Cores individuais ou grupos de Cores que deseja incluir no relatório.

3 No menu suspenso do tipo de relatório, selecione o tipo de relatório que deseja gerar. Você pode escolher entre as seguintes opções:

- Relatório do trabalho
- Relatório de falhas
- Relatório resumido
- Relatório de resumo do trabalho

Para obter mais informações sobre esses tipos de relatório, consulte Sobre os relatórios do Rapid Recovery.

4 No menu suspenso do período, selecione um período.

Você pode escolher entre as opções da tabela a seguir.

Opção	Descrição
Dia	Relata a atividade do último dia, referente à hora em que você gera o relatório.
Semana	Relata a atividade da última semana, referente à hora em que você gera o relatório.
Mês	Relata a atividade dos últimos 31 dias, referente à hora em que você gera o relatório.
Ano	Relata a atividade do último ano, referente à hora em que você gera o relatório.
A todo o momento	Esse período abrange a vida útil do Core.
Personalizada	Esse período requer que você especifique adicionalmente as datas inicial e final.

NOTA: Em todos os casos, nenhum dado de relatório está disponível antes da implantação do software Core ou antes de as máquinas serem protegidas no Core.

5 Realize um dos procedimentos a seguir:

- Clique em **Pré-visualizar** para gerar e visualizar o relatório gerado online.
- Atualize o relatório dinamicamente, alterando os critérios do relatório; em seguida, clique em **Pré-visualizar** novamente.
- Escolha um formato de exportação (incluindo o formato padrão, XLSX) e clique em **Fazer download**.
- Use a **barra de ferramentas Relatórios** para visualizar, manipular ou imprimir o relatório. Para obter mais informações sobre a barra de ferramentas Relatórios, consulte Usar a barra de ferramentas Relatórios.

7

Noções básicas do utilitário Command Line Management do Rapid Recovery

O Dell Data Protection | Rapid Recovery consiste em vários componentes de software. Os principais componentes relevantes para esse tópico incluem o seguinte:

- O Rapid Recovery Core gerencia a autenticação para as máquinas protegidas, os programas para transferir dados para fazer o backup e a replicação, a exportação para máquinas virtuais, a criação de relatórios e a bare metal restore (BMR) para hardware similar ou dissimilar.
- O Rapid Recovery Agent é responsável pelos snapshots de volume e pela rápida transferência dos dados para o repositório gerenciado pelo Core.
- O utilitário Command Line Management do Rapid Recovery, cmdutil.exe, fornece acesso a terceiros para gerenciar a funcionalidade do sistema. Essa ferramenta permite a geração de script das funções de gerenciamento do Rapid Recovery Core.

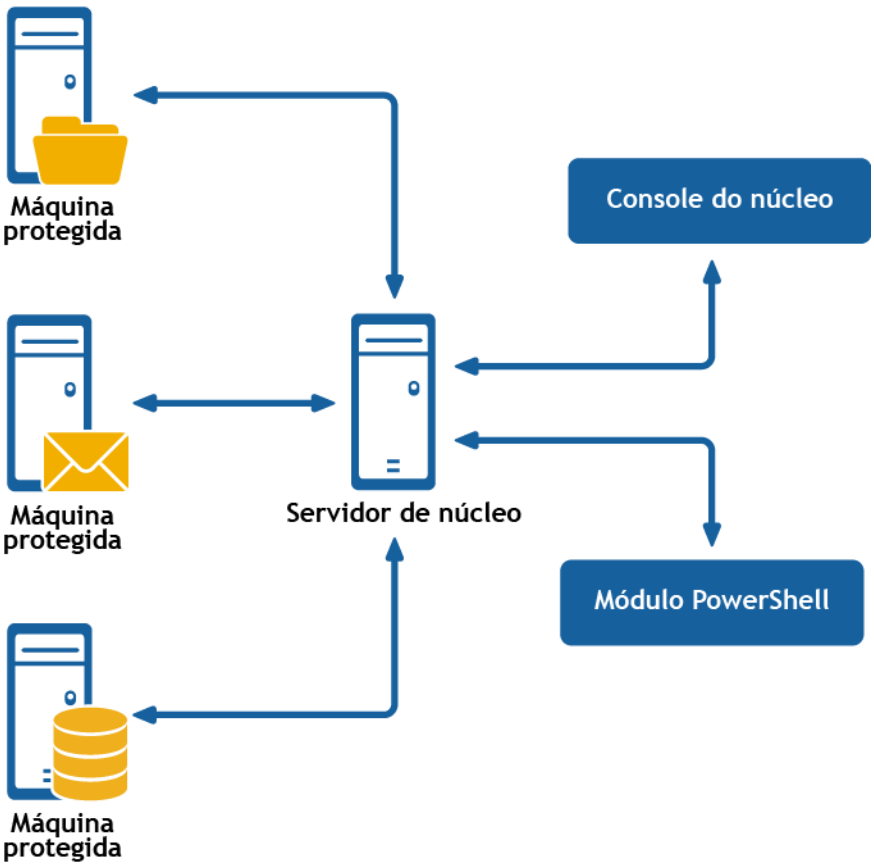


Figura 13. O Command Line Management do Rapid Recovery fornece funções de gerenciamento da linha de comando

O Command Line Management do Rapid Recovery é um utilitário de linha de comando do Windows que permite aos usuários interagirem com o servidor do Rapid Recovery Core. Ele oferece algumas das mesmas funções da interface gráfica de usuário do Rapid Recovery Core Console. Por exemplo, o utilitário Command Line Management do Rapid Recovery pode montar pontos de recuperação ou forçar um snapshot.

O utilitário Command Line Management do Rapid Recovery está incorporado a cada instalação do Rapid Recovery Core. Para abrir o utilitário Command Line Management para uma instalação padrão, navegue para o caminho **C:\Program Files\AppRecovery\Core \CoreService** e clique duas vezes no arquivo `cmdutil.exe` .

No Modo de linha de comando, os sinalizadores de ação podem ser passados para o utilitário Command Line Management do Rapid Recovery com a seleção de opções do comando e qualificadores para realizar funções limitadas de gerenciamento.

Tópicos:

- Comandos
- Localização

Comandos

Esta seção descreve os comandos e as opções disponíveis para a ferramenta Command Line Management do Rapid Recovery. Os seguintes comandos estão disponíveis para uso:

- Arquivo
- CancelActiveJobs
- CheckRepository
- CreateArchiveRepository
- CreateBootCD
- CreateRepository
- DeleteRepository
- Dismount
- DismountArchiveRepository
- EditEsxServer
- Force
- ForceAttach
- ForceChecksum
- ForceLogTruncation
- ForceMount
- ForceReplication
- ForceRollup
- ForceVirtualStandby
- Ajuda
- List
- Montagem
- MountArchiveRepository
- NewCloudAccount
- OpenDvmRepository
- Pause
- Protect
- ProtectCluster
- ProtectEsxServer
- RemoveAgent
- RemoveArchiveRepository
- RemovePoints

- RemoveScheduledArchive
- RemoveVirtualStandby
- Replicate
- Replicação
- RestoreAgent
- RestoreArchive
- RestoreUrc
- Resume
- SeedDrive
- StartExport
- UpdateRepository
- Versão
- VirtualStandby

Arquivo

As empresas frequentemente usam o armazenamento de longo prazo para arquivar dados compatíveis e não compatíveis. O recurso de arquivo do Rapid Recovery suporta retenção estendida para dados compatíveis e não compatíveis. O administrador pode salvar um arquivo no armazenamento local ou no local de rede especificando o parâmetro `-path` e as credenciais.

Forma de uso

A forma de uso do comando é a seguinte:

```
/archive -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address] -path [location] -startdate [time string] -enddate [time string] -archiveusername [name] -archivepassword [password] -comment [text]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`archive`:

Tabela 171. Opções do comando Archive

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-all`	Arquivar todos os pontos de recuperação para todas as máquinas protegidas no Core.

Opção	Descrição
-protectedserver	Máquina protegida com pontos de recuperação a serem arquivados. Você pode especificar vários nomes de máquinas entre aspas duplas e separados por espaços.
-path	O caminho é colocado onde estão os dados arquivados; por exemplo: d:\work\archive ou caminho de rede \\NomedoServidor\Compartilhamento.
-startdate	Iniciar a data selecionando pontos de recuperação pela data de criação. O valor deve ser informado entre aspas duplas; por exemplo,"04/30/2012 02:55 PM".
-enddate	Opcional. Data final para selecionar os pontos de recuperação pela data de criação. O valor deve ser informado entre aspas duplas; por exemplo,"05/31/2012 11:00 AM". O sistema de tempo atual é usado por padrão.
-archiveusername	Opcional. Nome de usuário da máquina remota. Necessário para caminho de rede apenas.
-archivepassword	Opcional. Senha para a máquina remota. Necessário para caminho de rede apenas.
-comment	Opcional. O texto de comentário deve ser informado entre aspas duplas; por exemplo:-comment "comment goes here...".

Exemplos:

Arquivar todos os pontos de recuperação com datas de criação de 04/30/2012 14h55min para todas as máquinas no Core:

```
>cmdutil /archive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -path d:\work
\archive -startdate "04/30/2012 02:55 PM" -all
```

Arquivar pontos de recuperação que entram num intervalo de datas para duas máquinas protegidas:

```
>cmdutil /archive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver
"10.20.30.40" "20.20.10.1" -path d:\work\archive -startdate "04/30/2012 02:55 PM" -enddate
"05/31/2012 11:00 AM"
```

CancelActiveJobs

Use o comando cancelactivejobs para cancelar a execução de todos os trabalhos em andamento de um tipo específico, como transferência e replicação.

Forma de uso

A forma de uso do comando é a seguinte:

```
/cancelactivejobs -core [host name] -user [user name] -password [password] -jobtype [job type
filter]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando cancelactivejobs:

Tabela 172. Opções do comando CancelActiveJobs

Opção	Descrição
`-?`	Exibir ajuda sobre o comando.
`-core`	Opcional. Endereço IP da máquina de host do core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, são usadas as credenciais para o usuário registrado.
`-protectedserver`	Determinar a máquina protegida na qual os trabalhos serão cancelados.
`-all`	Selecionar e cancelar eventos de tipo específico em todos os servidores protegidos.
`-jobtype`	Opcional. Especifica o filtro do tipo de trabalho. Os valores disponíveis são: • 'transfer' (transferência de dados) • 'repository' (manutenção de repositório) • 'replication' (replicações locais e remotas) • 'backup' (cópia de segurança e restaurar) • 'bootcdbuilder' (criar CDs de inicialização) • 'diagnostics' (logs para fazer upload) • 'exchange' (verificação de arquivos do Exchange Server) • 'export' (exportação do ponto de recuperação) • 'pushinstall' (implementar agentes) • "restaurar" (restauração do ponto de recuperação) • 'rollup' (rollups de ponto de recuperação) • 'sqlattach' (verificações da capacidade de anexação do agente) • 'mount' (montar repositório) Como padrão, todos os trabalhos do tipo especificado são cancelados.

Exemplo:

Cancelar todos os trabalhos de transferência no Core 10.10.10.10:

```
>cmdutil /cancelactivejobs -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -
jobtype transfer
```

CheckRepository

Você pode usar o comando CheckRepository para verificar a integridade de um repositório de DVM existente criado no AppAssure Core ou no Rapid Recovery Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
/checkrepository -repository [repository name] | -all [check all repositories] -core [host
name] -user [user name] -password [password] name] -force
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`CheckRepository`:

Tabela 173. Opções do comando CheckRepository

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. O nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. A senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-all`	Opcional. Essa opção verifica todos os repositórios de DVM associados ao Core.
`-repository`	O nome do repositório de DVM.
`-force`	Opcional. Esta opção executa a verificação sem sua confirmação.

Exemplo:

Inicie a verificação do repositório de DVM:

```
>cmdutil /checkrepository -repository "Repository1" -core 10.10.10.10 -user administrator -
password 23WE@#$sdd
```

CreateArchiveRepository

Ao criar um repositório de arquivamento, você cria um destino para o conteúdo de um arquivamento programado. Esse recurso permite que você monte uma ponto de recuperação arquivado e restaure uma máquina sem importar o arquivamento.

Forma de uso

A forma de uso do comando é a seguinte:

```
/createarchiverepository -core [host name] -user [user name] -password [password] name] -name
[archive repository name] -path [path to the archive] -archiveusernamme [network user name] -
```

```
archivepassword [network password] -cloudaccountname [name of the cloud account] -
cloudcontainer [name of the cloud container]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`CreateArchiveRepository`:

Tabela 174. Opções do comando CreateArchiveRepository

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. O nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. A senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-name`	Obrigatório. O nome do repositório de arquivo.
`-path`	O caminho para o arquivo existente. Pode ser local, na rede ou na nuvem. Por exemplo: d:\work\archive ou \ \servername\sharename.
`-archiveusername`	Opcional. Esta opção é o login para a máquina remota. É necessário para caminho de rede apenas.
`-archivepassword`	Opcional. Esta opção é a senha da máquina remota. Só é necessário para um caminho de rede apenas.
`-cloudaccountname`	Opcional. Esta opção é o nome de exibição de uma conta de nuvem existente. É necessário somente para um caminho da nuvem.
`-cloudcontainer`	Opcional. O contêiner de nuvem é onde o arquivo está localizado. É necessário somente para um caminho da nuvem.

Exemplos:

Criar um repositório de arquivamento com o nome "NewArchive:"

```
>cmdutil /createarchiverepository -name NewArchive -core 10.10.10.10 -user administrator -
password 23WE@#$sdd -path d:\work\archive
```

Além disso, se um arquivo contém mais de um local, o comando deverá incluir os caminhos para todos os segmentos ordenados de 1 a N, onde N é igual ao número de segmentos.

Criar um repositório de arquivamento com o nome "NewSegmentArchive:"

```
>cmdutil /createarchiverepository -name NewSegmentArchive -path1 \\RemmoteServer1\Share\Archive
\Segment1 - archiveusername1 Administrator -archivepassword1 23WE@#$sdd -path2 Archives
\NewSegment -cloudcontainer2 ArchiveContainer -cloudaccountname AmazonS3Local - path3 d:\work
\archive\Third
```

CreateBootCD

Este comando permite que você crie um CD de inicialização bare metal restore (BMR) sem usar o Rapid Recovery Core Console.

Forma de uso

A forma de uso do comando é a seguinte:

```
/createbootcd -ip [IP address] -mask -defaultgateway -dnsserver -vncpassword -vncport -
isofilepath [destination for the boot image]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`CreateBootCD`:

Tabela 175. Opções do comando CreateBootCD

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-ip`	Opcional. Esta opção especifica o endereço IP da máquina BMR de destino. Por padrão, ela é gerada automaticamente.
`-mask`	Opcional. Esta opção especifica a máscara de sub-rede da máquina BMR de destino. Por padrão, ela é gerada automaticamente.
`-defaultgateway`	Opcional. Esta opção especifica o gateway padrão da máquina BMR de destino. Por padrão, ela é gerada automaticamente.
`-dnsserver`	Opcional. Esta opção especifica o servidor DNS da máquina BMR de destino. Por padrão, ela é gerada automaticamente.
`-vncpassword`	Opcional. Esta opção especifica a senha do usuário para uma conta UltraVNC existente. Por padrão, esta opção está vazia.
`-vncport`	Opcional. Esta opção especifica a porta a ser usada para UltraVNC. Você pode alterá-la apenas se você usou a opção`-vncpassword`. Por padrão, a porta é 5900.
`-isofilepath`	Opcional. Esta opção especifica o caminho para o arquivo do CD de inicialização. O caminho padrão é C:\ProgramData\AppRecovery\Boot CDs.

Exemplo:

Crie um CD de inicialização:

```
>cmdutil /createbootcd -ip 192.168.20.188 -mask 255.255.255.0 -defaultgateway 192.168.20.2 -
dnsserver 192.168.20.2 -isofilepath D:\bcd\newbcd3.iso
```

CreateRepository

Use o comando`createrepository` para criar um novo repositório de DVM em uma máquina local ou em um local de compartilhamento de CIFS.

Forma de uso

A forma de uso do comando, enquanto cria um repositório num espaço local, é a seguinte:

```
/createrepository -name [repository name] -size [size allocated for repository] -datapath [data path of repository] -metadatapath [metadata path of repository] -core [host name] -user [user name] -password [password]
```

A forma de uso do comando, enquanto cria um repositório de DVM em um local partilhado, é a seguinte:

```
/createrepository -name [repository name] -size [size allocated for repository] -uncpath [path for data and metadata] -shareusername [user name for share location] -sharepassword [password for share user name] -concurrentoperations [number of operations to occur at one time] -core [host name] -user [user name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`createrepository`:

Tabela 176. Opções do comando CreateRepository

Opção	Descrição
`-?`	Exibir ajuda sobre o comando.
`-core`	Opcional. Endereço IP da máquina de host do core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-name`	Nome do repositório.
`-size`	Tamanho do local de armazenamento do repositório. As unidades disponíveis são b, Kb, Mb, Gb, Tb, e Pb.
`-datapath`	Para espaço local, somente. Determinar o caminho de dados do local de armazenamento do repositório.
`-metadatapath`	Para espaço local, somente. Determinar o caminho de metadados do local de armazenamento do repositório.
`-uncpath`	Para local partilhado, somente. Determinar os caminhos de dados e metadados do local de armazenamento do repositório.
`-shareusername`	Para local partilhado, somente. Determina o nome de usuário para o local de compartilhamento.
`-sharepassword`	Para local partilhado, somente. Determinar senha para local partilhado.

Opção	Descrição
`-comment`	Opcional. Descrição do repositório.
`-concurrentoperations`	Opcional. O número máximo de operações pode estar pendente de uma só vez. Valor por padrão: 64.

Exemplos:

Criar um repositório de DVM em um espaço local:

```
>cmdutil /createrepository -name "Repository 1" -size 200 Gb -datapath d:\repository -
metadatapath d:\repository -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
```

Criar um repositório de DVM em um local compartilhado:

```
>cmdutil /createrepository -name "Repository 1" -size 200 Gb -uncpath \\share\repository -
shareusername login -sharepassword pass123 -comment "First repository." -concurrentoperations 8
-core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
```

DeleteRepository

Você pode usar o comando DeleteRepository para remover um repositório de DVM inteiro criado no AppAssure Core ou no Rapid Recovery Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
/deleterepository -core [host name] -user [user name] -password [password] name] -name
[repository name] | -a [all repositories]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`DeleteRepository`:

Tabela 177. Opções do comando DeleteRepository

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. O nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. A senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-a`	Opcional. Esta opção apaga todos os repositórios DVM associados ao Core.

Opção	Descrição
-name	O nome do repositório de DVM que você quer apagar.

Exemplo:

Apagar todos os repositórios DVM:

```
>cmdutil /deleterepository -a
```

Apagar o repositório com o nome "RepositoryName":

```
>cmdutil /deleterepository -name RepositoryName
```

Dismount

Use o comando para`dismount` desmontar um ponto de recuperação montado especificado pela opção`-path`. desmontar pontos para o agente selecionado pelo parâmetro `-protectedserver` ou desmontar todos os pontos de recuperação montados `-all`.

Forma de uso

A forma de uso do comando é a seguinte:

```
/dis[mount] -core [host name] -user [user name] -password [password] [-all | -
protectedserver [name | IP address] | -path [location]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `dismount`:

Tabela 178. Opções do comando Dismount

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
-all	Desmontar todos os pontos de recuperação montados.
-protectedserver	Desmontar todos os pontos de recuperação montados para o agente atual.
-path	Desmontar ponto de montagem selecionado.

Exemplo:

Desmontar um ponto de recuperação que foi montado na pasta c:\mountedrecoverypoint:

```
>cmdutil /dismount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -path c:
\mountedRecoveryPoint
```

DismountArchiveRepository

Depois de obter as informações que você desejar de um arquivo montado, você deve desmontar o arquivo para evitar possíveis problemas.

Forma de uso

A forma de uso do comando é a seguinte:

```
/dismountarchiverepository -core [host name] -user [user name] -password [password] name] -name
[archive repository name]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`DismountArchiveRepository`:

Tabela 179. Opções do comando DismountArchiveRepository

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. O nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. A senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-name`	Obrigatório. O nome do repositório de arquivo.

Exemplos:

Desmontar o repositório com o nome "NewArchive":

```
>cmdutil /dismountarchiverepository -name NewArchive -core 10.10.10.10 -user administrator -
password 23WE@#$sdd -path d:\work\archive
```

EditEsxServer

Você pode usar o comando`editesxserver` sempre que quiser fazer alterações no número de máquinas virtuais VMware ESX(i) que você quer proteger sem agente.

Forma de uso

A forma de uso do comando é a seguinte:

```
/editEsxServer -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -add | -remove -virtualMachines [virtual machines collection | all] -autoProtect [object ID or name collection]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`editesxserver`:

Tabela 180. Opções do comando EditEsxServer

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. O nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. A senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-repository`	Obrigatório. O nome do repositório que está associado ao Core que você quer usar para proteger a máquina virtual. **NOTA: Você precisa colocar o nome entre aspas duplas.**
`-protectedserver`	Use esta opção para editar os objetos do vCenter e ESX(i) de uma máquina protegida específica.
`-add`	Use esta opção para adicionar um objeto do vCenter ou ESXi específico.
`-remove`	Use esta opção para remover um objeto do vCenter ou ESXi expecífico.
`-virtualmachines`	Opcional. Esta opção permite listar as máquinas virtuais que você quer proteger.
`-autoprotect`	Opcional. Esta opção permite listar as novas máquinas virtuais que você quer proteger automaticamente.

Exemplos:

Proteger automaticamente os objetos do vCenter ou ESXi específicos de um servidor vCenter ou ESXi com o Core:

```
>cmdutil /editEsxServer -protectedserver 10.10.8.150 -add -autoprotect "Folder1" "Folder2"
```

Force

O comando`force` força um snapshot do servidor protegido especificado. Forçar um snapshot permite forçar uma transferência de dados para a máquina protegida atual. Ao forçar um snapshot, a transferência iniciará imediatamente ou será adicionada à fila. Somente os dados que foram alterados em relação a um ponto de recuperação anterior serão transferidos. Caso não existir um ponto de recuperação anterior, todos os dados nos volumes protegidos serão transferidos.

Forma de uso

A forma de uso do comando é a seguinte:

```
/force [snapshot] default | [base] [-all | -protectedserver [name | IP address]] -core [host name] -user [user name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`force`:

Tabela 181. Opções do comando Force

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-force`	Opcional. Tipo de snapshot para criar. Valores disponíveis: 'snapshot' (snapshot incremental) e 'base' (snapshot de imagem de base). Por padrão, um snapshot incremental é realizado.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-all`	Forçar snapshots para todas as máquinas no Core.
`-protectedserver`	Forçar um snapshot numa máquina protegida específica.

Exemplo:

Forçar snapshots para todas as máquinas no Core:

```
>cmdutil /force snapshot -core 10.10.10.10 -user administrator -password 23WE@#$sdd -all
```

ForceAttach

O comando`forceattach` permite que você force uma verificação de capacidade de anexação do banco de dados SQL. Quando você força uma verificação de capacidade de anexação, o comando inicia imediatamente.

Forma de uso

A forma de uso do comando é a seguinte:

```
/forceattach -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -rpn [number | numbers] | -time [time string]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`forceattach`:

Tabela 182. Opções do comando ForceAttach

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-protectedserver`	Máquina protegida na qual a verificação de capacidade de anexação será realizada.
`-rpn`	O número sequencial de pontos de recuperação nos quais realizar verificações (executar comando /list rps para obter os números). Para realizar verificações em muitos pontos de recuperação com um único comando, você pode especificar os vários números separados por espaços.
`-time`	Selecionar um ponto de recuperação para o tempo de criação. Você deve especificar o tempo exato no formato “mm/dd/aaaa hh:mm tt” (por exemplo, “2/24/2012 09:00 AM”). Lembrar de especificar os valores de data e de tempo do fuso horário definidos no seu PC.

Exemplo:

Executar verificações de capacidade de anexação para pontos de recuperação com números 5 e 7:

```
>cmdutil /forceattach -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -rpn 5 7
```

ForceChecksum

O comando`forcechecksum` permite forçar uma verificação de integridade de bancos de dados de mensagem do Exchange (MDBs) presentes no ponto ou pontos de recuperação especificados. Quando você força uma verificação de soma de verificação, o comando inicia imediatamente.

Forma de uso

A forma de uso do comando é a seguinte:

```
/forcechecksum -core [host name] -user [user name] -password [password] -protectedserver [name
| IP address] -rpn [number | numbers] -time [time string]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`forcechecksum`:

Tabela 183. Opções do comando ForceChecksum

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-protectedserver`	Máquina protegida na qual a verificação de soma de verificação será realizada.
`-rpn`	O número sequencial de pontos de recuperação nos quais realizar verificações (executar comando /list rps para obter os números). Para realizar verificações em muitos pontos de recuperação com um único comando, você pode especificar os vários números separados por espaços.
`-time`	Selecionar um ponto de recuperação para o tempo de criação. Você deve especificar o tempo exato no formato “mm/dd/aaaa hh:mm tt” (por exemplo, “2/24/2012 09:00 AM”). Lembrar de especificar os valores de data e de tempo do fuso horário definidos no seu PC.

Exemplo:

Executar uma verificação de soma de verificação nos pontos de recuperação com números 5 e 7:

```
>cmdutil /forcechecksum -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -rpn 5 7
```

ForceLogTruncation

Forçar truncamento de log permite que você execute este trabalho de uma vez, sob demanda. Ele imediatamente trunca os logs para o agente SQL Server da máquina especificada.

Forma de uso

A forma de uso do comando é a seguinte:

```
/[forcelogtruncation | flt] -core [host name] -user [user name] -password [password] -
protectedserver [name | IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`forcelogtruncation`:

Tabela 184. Opções do comando ForceLogTruncation

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-protectedserver`	Máquina protegida na qual o truncamento de arquivo log será realizado.

Exemplo:

Forçar truncamento de log para um servidor protegido:

```
>cmdutil /forcelogtruncation -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.20.20
```

ForceMount

Usar o comando`forcemount` para conduzir uma verificação única de capacidade de montagem do ponto de recuperação. Isso determina se o ponto de recuperação especificado ou os pontos de recuperação podem ou não ser montados e usados para restaurar dados da cópia de segurança. Você deve listar um ou mais pontos de recuperação específicos sobre os quais conduzir a verificação ou um intervalo de tempo durante o qual foram criados os pontos de recuperação.

Forma de uso

A forma de uso do comando é a seguinte:

```
/forcemount -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -rpn [number | numbers] | -time [time string]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`forcemount`:

Tabela 185. Opções do comando ForceMount

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-protectedserver`	Máquina protegida na qual a verificação de capacidade de montagem será realizada.
`-rpn`	O número sequencial de pontos de recuperação nos quais realizar verificações (executar comando /list rps para obter os números). Para realizar verificações em muitos pontos de recuperação com um único comando, você pode especificar os vários números separados por espaços.
`-time`	Selecionar um ponto de recuperação para o tempo de criação. Você deve especificar o tempo exato no formato “mm/dd/aaaa hh:mm tt” (por exemplo, “2/24/2012 09:00 AM”). Lembrar de especificar os valores de data e de tempo do fuso horário definidos no seu PC.

Exemplo:

Executar verificações de montabilidade para pontos de recuperação com números 5 e 7:

```
>cmdutil /forcemount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.20.20 -rpn 5 7
```

ForceReplication

Usar o comando`forcereplication` para forçar uma transferência única de dados replicados do core de origem para o core de destino. Você pode replicar um servidores protegido específico ou replicar todos os servidores protegidos. Os servidores protegidos devem ser imediatamente configurados para replicação.

Forma de uso

A forma de uso do comando é a seguinte:

```
/[forcereplication |frep] -core [host name] -user [user name] -password [password] -targetcore
[host name] -all | -protectedserver [name | IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`forcereplication`:

Tabela 186. Opções do comando ForceReplication

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então serão usadas as credenciais para o usuário conectado
`-targetcore`	O nome do host do core de destino no qual a replicação deverá ser forçada.
`-protectedserver`	A máquina protegida que você quer replicar.
`-all`	Forçar replicação para todas as máquinas sendo replicadas no core de destino.

Exemplo:

Forçar replicação para um servidor protegido num core de destino específico:

```
>cmdutil /forcereplication -target core 10.10.10.10 -protectedserver 10.20.30.40
```

ForceRollup

Use o comando `forcerollup` para forçar o rollup dos pontos de recuperação em uma máquina protegida.

Forma de uso

A forma de uso do comando é a seguinte:

```
/[forcerollup | fro] -core [host name] -user [user name] -password [password] -protectedserver
[name | IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `forcerollup`:

Tabela 187. Opções do comando ForceRollup

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então serão usadas as credenciais para o usuário conectado
`-protectedserver`	Opcional. Máquina protegida na qual o rollup será realizado.

Exemplo:

Forçar rollup para o agente 10.10.10.1 no Core:

```
>cmdutil /forcerollup -core 10.10.10.10 - user administrator -password 23WE@#$sdd -
protectedserver 10.10.10.1
```

ForceVirtualStandby

A exportação dos dados de uma máquina protegida para uma máquina virtual cria uma máquina de standby virtual. Se tiver uma configuração da exportação virtual contínua, você poderá usar esse comando para forçar o Rapid Recovery para exportar dados sob demanda, independentemente do programa predeterminado.

Forma de uso

A forma de uso do comando é a seguinte:

```
/forcevirtualstandby -core [host name] -user [user name] -password [password login] -
protectedserver [name] | -all
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`ForceVirtualStandby`:

Tabela 188. Opções do comando ForceVirtualStandby

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-protectedserver`	O nome ou nomes separados por espaço das máquinas virtualizadas.
`-all`	Esse comando especifica se é necessário forçar todas as exportações virtuais programadas.

Exemplos:

Force todas as exportações de standby virtual:

```
>cmdutil /forcevirtualstandby -all
```

Force standby virtual para duas máquinas:

```
>cmdutil /forcevirtualstandby -protectedserver 10.10.35.48 10.10.35.69
```

Ajuda

O comando`help` exibe uma lista dos comandos disponíveis e suas definições. Também fornece detalhes dos direitos autorais e da versão.

Forma de uso

A forma de uso do comando é a seguinte:

```
/help
```

Exemplo:

Solicitar o comando linha de ajuda:

```
>cmdutil /help
```

List

O comando `list` retorna informações sobre todos os pontos de recuperação, trabalhos ativos, trabalhos concluídos, trabalhos com falha, pontos de recuperação inválidos (com falha), pontos de recuperação válidos (aprovados), montagens, servidores protegidos, volumes, servidores virtualizados, volumes desprotegidos, clusters, grupos de proteção, bancos de dados SQL, bancos de dados do Exchange, servidores replicados e repositórios para o agente especificado ou lista de servidores atualmente protegidos pelo Núcleo. Os registros mais recentes retornados por padrão: Você pode listar todos os registros ou quantos registros serão exibidos usando um parâmetro numérico. Esse parâmetro deve conter a letra "l" para os pontos de recuperação mais recentes e "f" para o primeiro ponto de recuperação. Cada ponto de recuperação tem seu próprio número, que o administrador pode usar para a montagem.

Forma de uso

A forma de uso do comando é a seguinte:

```
/list [rps | passed | failed | mounts | volumes | protectedservers | activejobs | completed
jobs | failedjobs | virtualizedservers | unprotectedvolumes | clusters | protectiongroups |
sqldatabases | exchangemailstores | replicatedservers | repositories] -protectedserver [name |
IP address] -core [host name] -user [user name] -password [password] -number [all | l<number> |
f<number> | <number>] -jobtype
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `list`:

Tabela 189. Opções do comando List

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-list`	Selecione uma das opções a seguir: • todos os pontos de recuperação (‘rps’) • pontos de recuperação válidos (‘passed’) • pontos de recuperação inválidos (‘failed’) • montagens (‘mounts’) • volumes protegidos ('volumes') • volumes desprotegidos ('unprotectedvolumes') • máquinas protegidas ('protectedservers') • trabalhos ativos ('activejobs') • trabalhos com falha ('failedjobs') • trabalhos concluídos ('completedjobs') • servidores virtualizados ('virtualizedservers') • clusters ('clusters') • grupos de proteção ('protectiongroups') • Bancos de dados do SQL Server ('sqldatabases') • Bancos de dados do MS Exchange ('exchangemailstores') • servidores replicados ('replicatedservers') • repositórios (‘repositories’)

Opção	Descrição
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
-all	Para exibição de trabalhos, somente. Exibir todos os eventos de um tipo específico (ativo/com falha/concluído) no servidor do core.
-protectedserver	Máquina protegida com pontos de recuperação para exibir.
-number	Opcional. Número de itens de dados para exibir. Use somente com os seguintes especificadores: "rps", "activejobs", "completedjobs", "failedjobs". Os valores disponíveis são: • all (buscar todos os itens de dados) • l[number] ou [number] (busca os ## itens de dados do topo) • f[number] (busca os primeiros ## itens de dados) Somente tem efeito quando exibir pontos de recuperação e trabalhos.
-jobtype	Opcional. Filtrar saída pelo tipo de trabalho. Valores disponíveis incluem: • 'transfer' (transferência de dados) • 'repository' (manutenção de repositório) • 'replication' (replicações locais e remotas) • 'backup' (cópia de segurança e restaurar) • 'bootcdbuilder' (criar CDs de inicialização) • 'diagnostics' (logs para fazer upload) • 'exchange' (verificação de arquivos do Exchange Server) • 'export' (exportar o ponto de recuperação) • 'pushinstall' (implementar agentes) • "restaurar" (restaurações do ponto de recuperação) • 'rollup' (rollups de máquina protegida) • 'sqlattach' (verificações da capacidade de anexação do agente) • 'mount' (montar repositório)

Exemplos:

Listar os 30 mais recentes pontos de recuperação:

```
>cmdutil /list rps -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver
10.10.5.22 -number 130
```

Ver todos os trabalhos com falha de transferência de dados realizados por uma máquina protegida:

```
>cmdutil /list failed jobs -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -number all -jobtype transfer
```

Montagem

O comando`mount` monta um snapshot de uma ou mais unidades. Você pode especificar se a montagem deve ler, escrever ou ser apenas leitura com gravações anteriores. A seleção padrão é apenas leitura.

Forma de uso

A forma de uso do comando é a seguinte:

```
/mount -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -mounttype [read | write | readOnlyWithPreviousWrites] -drives [drive names] -volumes [volume names] -path [location] -rpn [number | numbers] | -time [time string]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`mount`:

Tabela 190. Opções do comando Mount

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-protectedserver`	Máquina protegida com ponto ou pontos de recuperação a serem montados.
`-mounttype`	Opcional. Especifica um modo de montagem. Os valores disponíveis são`'read' (read-only)``'readOnlyWithPreviousWrites'` (apenas leitura com gravações anteriores) e `'write'` (gravável). O modo padrão é`read-only`.
`-volumes`	Opcional. Lista de nomes de volumes a serem montados. Se não especificado, todos os volumes serão montados. Os valores devem ser informados entre aspas duplas e separados por um espaço; por exemplo: "c:" "d:". Não use barras nos nomes dos volumes.
`-path`	Caminho para uma pasta no core servidor na qual o ponto de recuperação deve ser montado. Se esse não existir, uma pasta será automaticamente criada.
`-rpn`	Opcional. O número sequencial de um ponto de recuperação para montar (use o comando`/list rps` para obter os números). Para especificar muitos pontos de recuperação com um único comando, usar vários números separados por espaços. Neste caso, os dados de cada ponto de recuperação serão armazenados em uma pasta child separada. Nota: se nenhuma opção -time ou -rpn for especificada, então o ponto de recuperação mais recente que passou com êxito na verificação de integridade será montado.

Opção	Descrição
-time	Opcional. Determinar ponto ou pontos de recuperação a serem selecionados para montagem. Os valores disponíveis são: 'último', 'aprovado', hora exata no formato "mm/dd/aaaa hh:mm tt" (por exemplo, "2/24/2012 09:00 AM"). Lembrar de especificar os valores de data e de tempo do fuso horário definidos no seu PC. Se nenhuma opção -time ou -rpn for especificada, então, o ponto de recuperação mais recente que passou com êxito na verificação de integridade será montado.
-localdrive	Opcional. Realizar montagem no disco de usuário no PC local.

Exemplos:

Montar os mais recentes pontos de recuperação contendo volumes “c:\” e “d:\” no modo apenas leitura:

```
>cmdutil /mount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver
10.10.5.22 -path c:\mountedrecoverypoint -mounttype read -volumes "c:" "d:"
```

Montar pontos de recuperação com números 2 e 7:

```
>cmdutil /mount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver
10.10.5.22 -path c:\mountedrecoverypoint -rpn 2 7
```

MountArchiveRepository

Para restaurar dados de um arquivo no Rapid Recovery, você precisa primeiro montá-lo.

Forma de uso

A forma de uso do comando é a seguinte:

```
/mountarchiverepository -core [host name] -user [user name] -password [password] -name [archive
repository name]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`mountarchiverepository`:

Tabela 191. Opções do comando MountArchiveRepository

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. O nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
-password	Opcional. A senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.

Opção	Descrição
-name	Obrigatório. O nome do repositório de arquivo.

Exemplos:

Montar o repositório com o nome "NewArchive:"

```
>cmdutil /mountarchiverepository -name NewArchive
```

NewCloudAccount

Use o comando NewCloudAccount para adicionar uma conta de um provedor de nuvem ao Rapid Recovery Core. Você pode usar a conta para armazenar arquivos de retenção ou replicação.

Forma de uso

A forma de uso do comando é a seguinte:

```
/newcloudaccount -core [host name] -user [user name] -password [password] -displayname [name
for the account] -type [cloud account provider] -useername [user name for the account] -key
[secret key] -region [region for account] tenanatid [tenant ID] -authurl [authorization URL]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`NewCloudAccount`:

Tabela 192. Opções do comando NewCloudAccount

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. O nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
-password	Opcional. A senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
-displayname	O nome que você deseja usar na conta de nuvem.
-type	O tipo de conta de nuvem. Os valores suportados incluem: • amazon • openstack • rackspace • windowsazure • "windows azure"

Opção	Descrição
	• azure
`-username`	O nome de usuário da conta de nuvem que você deseja adicionar. Essa é a credencial que você usa no processo de autenticação. A propriedade tem as seguintes variações com base no tipo de nuvem: • Amazon - Chave de acesso • OpenStack - Nome de usuário • Rackspace - Nome de usuário • Windows Azure - Nome da conta de armazenamento
`-key`	A chave de autenticação da conta de nuvem que você deseja adicionar. Essa é a credencial que você usa no processo de autenticação. A propriedade tem as seguintes variações com base no tipo de nuvem: • Amazon - Chave secreta • OpenStack - Chave de API • Rackspace - Chave de API • Windows Azure - Chave de acesso
`-region`	A região da conta de nuvem que você deseja adicionar. Essa opção só é obrigatória para contas de OpenStack e Rackspace.
`-tenantid`	O ID que você usa para autenticar uma conta de nuvem de OpenStack. Essa opção só é obrigatória para contas de OpenStack.
`-authurl`	O URL que você usa para autenticar uma conta de nuvem de OpenStack. Essa opção só é obrigatória para contas de OpenStack.

Exemplos:

Adicione uma nova conta de nuvem com o nome "Amazon S3 Conta" com a chave de acesso "akey" e a chave secreta "skey:"

```
>cmdutil /newcloudaccount -displayname "Amazon S3 Account" -type amazon -useername akey -key
skey
```

OpenDvmRepository

Use esse comando para abrir um repositório DVM existente criado em AppAssure Core ou Rapid Recovery Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
/opendvmrepository -localpath [local path] -sharepath [network share path] -shareusername [user
name for network share] -sharepassword [network share password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`OpenDvmRepository`:

Tabela 193. Opções do comando OpenDvmRepository

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-localpath`	O caminho para a pasta com um repositório de DVM no Core local.
`-sharepath`	O caminho para a pasta com o repositório de DVM em um compartilhamento de CIFS.
`-shareusername`	O nome de usuário que você usa para fazer logon na pasta compartilhada.
`-sharepassword`	A senha que você usa para fazer logon na pasta compartilhada.

Exemplo:

Abra um repositório DVM existente na máquina local:

```
>cmdutil /opendvmrepository -localpath E:\Repository
```

Pause

Um administrador pode pausar snapshots, exportar para máquinas virtuais ou replicar para um Core. O comando`pause` aceita três parâmetros:`snapshot`,`vmexport` e`replication`. Somente um parâmetro pode ser especificado. Um snapshot pode ser pausado até um determinado momento, caso um parâmetro de tempo seja especificado.

Um usuário pode pausar uma replicação de três maneiras:

- Em um Core de origem de todas as máquinas protegidas.(`-[outgoing]`).
  O administrador precisa especificar o nome da máquina remota com o emparelhamento de replicação de saída para pausar a replicação de saída no core de origem:

  ```
  >cmdutil /pause replication /o 10.10.12.10
  ```
- No Core de origem de uma única máquina protegida.(`-protectedserver`):
  ```
  >cmdutil /pause replication /protectedserver 10.10.12.97
  ```
- No Core de destino (`-incoming`).
  Se o Core local é um Core de destino, o administrador pode pausar a replicação especificando o core de origem usando o parâmetro incoming:

  ```
  >cmdutil /pause replication /i 10.10.12.25
  ```

Forma de uso

A forma de uso do comando é a seguinte:

```
/pause [snapshot | vmexport | replication] -core [host name] -user [user name] -password
[password] -all | -protectedserver [name | IP address] -incoming [host name] | outgoing [host
name] -time [time string]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`pause`:

Tabela 194. Opções do comando Pause

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-pause`	`[snapshots]`, `[replication]` ou `[vmexport]`.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-all`	Opcional. Pausar todos os agentes do Core selecionado.
`-protectedserver`	Opcional. Pausar o servidor protegido atual.
`-incoming`	Opcional. Nome do host do core remoto que replica para o core da máquina.
`-outgoing`	Opcional. Nome do host do core de destino remoto no qual os dados são replicados.
`-time`	Opcional. O horário no formato “Dia-Horas-Minutos” em que os snapshots serão retomados (somente para pausas de snapshots).

Exemplos:

Pausar a criação de snapshots para um servidor protegido específico:

```
>cmdutil /pause snapshot -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.10.4
```

Pausar a criação de snapshots para uma máquina protegida e retomar depois de três dias, 20 horas e 50 minutos:

```
>cmdutil /pause snapshot -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.10.4 -time 3-20-50
```

Pausar exportação para máquina virtual para cada máquina protegida no core:

```
>cmdutil /pause vmexport -core 10.10.10.10 /user administrator -password 23WE@#$sdd –all
```

Pausar replicação de saída no core de uma máquina protegida específica:

```
>cmdutil /pause replication –core 10.10.10.10 -user administrator -password 23WE@#$sdd –
protectedserver 10.10.1.76
```

Pausar replicação de saída para todas as máquinas protegidas no core de destino:

```
>cmdutil /pause replication -core 10.10.10.10 -user administrator -password -23WE@#$sdd -
outgoing 10.10.1.63
```

Pausar replicação de entrada para todas as máquinas do core de destino:

```
>cmdutil /pause replication -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
incoming 10.10.1.82
```

Protect

O comando`protect` adiciona um servidor sob proteção de um Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
/protect -core [host name] -user [user name] -password [password] -repository [name] -agentname
[name | IP address] -agentusername [user name] -agentpassword [password] -agentport [port] -
volumes [volume names]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`protect`:

Tabela 195. Opções do comando Protect

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-repository`	Nome do repositório do Core onde os dados da máquina protegida deverão ser armazenados. O nome deve ser informado entre aspas duplas.
`-agentname`	O nome ou endereço IP do servidor que deseja proteger.
`-agentusername`	Nome de usuário do servidor a ser protegido.
`-agentpassword`	Senha do servidor a ser protegido.
`-agentport`	Número da porta do servidor protegido.
`-volumes`	Lista de volumes a serem protegidos. Os valores devem ser informados entre aspas duplas e separados por um espaço. Não use barras à direita em nomes de volumes; por exemplo: "c:" "d".

Exemplo:

Proteger volumes específicos de um servidor com o Core:

```
>cmdutil /protect -core 10.10.10.10 -username administrator -password 23WE@#$sdd -repository
"Repository 1" -agentname 10.10.9.120 -agentport 5002 -agentusername administrator
agentpassword 12345 -volumes "c:" "d:"
```

ProtectCluster

O comando`protectcluster` adiciona um cluster sob proteção de um core.

Forma de uso

A forma de uso do comando é a seguinte:

```
/protectcluster -core [host name] -user [user name] -password [password] -repository [name] -
clustername [name | IP address] -clusterusername [user name] -clusterpassword [password] -
clusterport [port] -clustervolumes [volume names] -clusternodes [cluster nodes collection]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`protectcluster`:

Tabela 196. Opções do comando ProtectCluster

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-repository`	Nome do repositório do Core onde os dados da máquina protegida deverão ser armazenados. O nome deve ser informado entre aspas duplas.
`-clustername`	O nome ou endereço IP do cluster que deseja proteger.
`-clusterusername`	Nome de usuário para o cluster a ser protegido.
`-clusterpassword`	Senha do cluster a ser protegido.
`-clusterport`	Número da porta do cluster do servidor protegido.

Opção	Descrição
`-clustervolumes`	Lista de volumes a serem protegidos. Os valores devem ser informados entre aspas duplas e separados por um espaço. Não use barras à direita em nomes de volumes; por exemplo: "c:" "d".
`-clusternodes`	Lista dos nós de cluster e os volumes que você deseja proteger em cada nó.

Exemplo:

Proteger volumes específicos de um cluster do servidor com o Core:

```
>cmdutil /protectcluster -core 10.10.10.10 -username administrator -password 23WE@#$sdd -
repository "Repository 1" -clustername 10.10.8.150 -clusterport 8006 -clusterusername
clusterAdmin clusterpassword password -volumes "C:\ClusterStorage\Volume1" -clusternodes
nodeName 10.10.8.150 volumes "c:" nodeName 10.10.8.151 volumes "c:"
```

ProtectEsxServer

Você pode usar o comando`protectesxserver` sempre que quiser adicionar uma máquina virtual VMware ESX(i) para proteção.

Forma de uso

A forma de uso do comando é a seguinte:

```
/protectesxserver -core [host name] -user [user name] -password [password] -repository
[repository name] -server [name | IP address] -serverusername [user name] -serverpassword
[password for server login] -serverport [port] -virtualMachines [virtual machines collection |
all] -autoProtect [object ID or name collection]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`protectesxserver`:

Tabela 197. Opções do comando ProtectEsxServer

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. O nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. A senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-repository`	Obrigatório. O nome do repositório que está associado ao Core que você quer usar para proteger a máquina virtual. **NOTA: Você precisa colocar o nome entre aspas duplas.**

Opção	Descrição
-server	O nome ou o endereço IP do servidor vCenter ou ESXi que deseja proteger.
-serverusername	O nome de usuário para fazer login no servidor vCenter ou ESXi que deseja proteger.
-serverpassword	A senha para fazer login no servidor vCenter ou ESXi que deseja proteger.
-serverport	Opcional. O número da porta do servidor vCenter ou ESXi que deseja proteger.
-virtualmachines	Opcional. Esta opção permite listar as máquinas virtuais que você quer proteger.
-autoprotect	Opcional. Esta opção permite que você liste novas máquinas virtuais que você quer proteger automaticamente.

Exemplos:

Proteger máquinas virtuais específicas a partir de um servidor vCenter ou ESXi com o Core:

```
>cmdutil /protectesxserver -core 10.10.10.10 -user admin -password password -repository
"Repository 1" -server 10.10.8.150 -serverport 443 -serverusername root -serverpassword
password -virtualmachines "VM1" "VM2" -autoprotect "Folder1"
```

RemoveAgent

O comando`RemoveAgent` permite remover uma máquina protegida da proteção de um Core e, como opção, excluir os pontos de recuperação da máquina removida. Se você não excluir os pontos de recuperação, o Rapid Recovery irá retê-los e rotulá-los como uma máquina apenas de pontos de recuperação.

Forma de uso

A forma de uso do comando é a seguinte:

```
/removeagent -core [host name] -user [user name] -password [password] -protectedserver [name |
IP address] -deleterecoverypoints
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`RemoveAgent` :

Tabela 198. Opções do comando RemoveAgent

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.

Opção	Descrição
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-protectedserver`	O nome ou endereço IP do servidor a ser removido da proteção.
`-deleterecoverypoints`	Opcional. Exclui todos os pontos de recuperação da máquina a ser removida.

Exemplo:

Remover uma máquina da proteção e excluir os pontos de recuperação associados:

```
>cmdutil /removeagent -protectedserver 10.10.1.1 -deleterecoverypoints
```

RemoveArchiveRepository

Você pode usar o comando`removearchiverepository` para excluir um repositório do Rapid Recovery Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
/removearchiverepository -core [host name] -user [user name] -password [password] name] -name
[archive repository name]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`removearchiverepository`:

Tabela 199. Opções do comando RemoveArchiveRepository

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. O nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. A senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-name`	Obrigatório. O nome do repositório de arquivo.

Exemplos:

Remover o repositório com o nome "NewArchive" do Core local:

```
>cmdutil /removearchiverepository -name NewArchive
```

RemovePoints

O comando`removepoints` permite excluir pontos de recuperação específicos de uma máquina protegida.

Forma de uso

A forma de uso do comando é a seguinte:

```
/removepoints -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -rpn [number | numbers] | -time [time string]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`removepoints`:

Tabela 200. Opções do comando RemovePoints

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-protectedserver`	O nome ou endereço IP do servidor cujos pontos de recuperação você deseja excluir
`-rpn`	Opcional. O número sequencial de um ponto de recuperação a ser excluído (use o comando`/list rps` para obter os números). Especifique vários números separados por espaço para excluir múltiplos pontos de recuperação com um único comando.
`-time`	Opcional. Determina quais pontos de recuperação serão excluídos até o momento da criação. Especifique o tempo exato no formato "mm/dd/aaaa hh:mm tt" (por exemplo, "2/24/2012 09:00 AM"). Lembre-se de especificar os valores de data e hora do fuso horário definido no seu PC.

Exemplo:

Excluir os pontos de recuperação com números 5 e 7:

```
>cmdutil /removepoints -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -rpn 5 7
```

RemoveScheduledArchive

Use esse comando para descontinuar um arquivo contínuo programado Rapid Recovery existente.

Forma de uso

A forma de uso do comando é a seguinte:

```
/removescheduledarchive -core [host name] -user [user name] -password [password] name] -all -
ids [id | id1 id2]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`removescheduledarchive`:

Tabela 201. Opções do comando RemoveScheduledArchive

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. O nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. A senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-all`	Essa opção especifica se é necessário remover todos os arquivos programados associados a esse Core.
`-ids`	Use essa opção para listar o ID ou os IDs para cada arquivamento programado que você deseja remover. Separe vários IDs com espaços.

Exemplos:

Remova todos os arquivos programados:

```
>cmdutil /removescheduledarchive -all
```

Remova um arquivo programado:

```
>cmdutil /removescheduledarchive -ids 6c123c39-5058-4586-bd0c-7c375e72017b
```

RemoveVirtualStandby

Use esse comando para descontinuar a exportação contínua de dados em uma máquina virtual no utilitário de comando do Rapid Recovery.

Forma de uso

A forma de uso do comando é a seguinte:

```
/removevirtualstandby -core [host name] -user [user name] -password [password login] -
protectedserver [name] | -all
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`removevirtualstandby`:

Tabela 202. Opções do comando RemoveVirtualStandby

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-protectedserver`	O nome ou nomes separados por espaço das máquinas virtualizadas.
`-all`	Esse comando especifica se é necessário remover todas as exportações virtuais programadas.

Exemplos:

Remova todas as exportações de standby virtual:

```
>cmdutil /removevirtualstandby -all
```

Remova exportação de standby virtual para duas máquinas:

```
>cmdutil /removevirtualstandby -protectedserver 10.10.35.48 10.10.35.69
```

Replicate

Utilize o comando`Replicate` para configurar uma replicação entre dois Rapid Recovery Cores.

Forma de uso

A forma de uso do comando é a seguinte:

```
/replicate -request [email | email customer ID] -targetserver [host name | hostname port | hostname user name password | hostname port user name password] -replicationname [name] -seeddrive [localpath | network path username password] [comment] -protectedserver [name | name repository]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Replicate`:

Tabela 203. Opções do comando Replicate

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então serão usadas as credenciais para o usuário conectado
`-request`	Opcional. Especifique esta opção se você deseja usar uma assinatura com um terceiro que oferece cópia de segurança em outro local e serviços de recuperação de desastres.
`-targetserver`	O nome do servidor ao qual você quer estabelecer a replicação. Inclui os seguintes parâmetros: • port • user name • password O parâmetro de porta é opcional, com um padrão de 8006. Se você usou a opção`request`, você deve também usar o nome de usuário e uma senha para o servidor de destino.
`-replicationname`	Opcional. Use o nome do trabalho de replicação se você não usar a opção`request`.
`-seeddrive`	Opcional. Use esta opção para especificar uma unidade de seeding para a transferência inicial de dados. O parâmetro do comentário é opcional.
`-protectedserver`	A lista de máquinas protegidas que você quer replicar. Se você usar a opção`request`, liste apenas os nomes ou os endereços IP das máquinas protegidas. Caso contrário, liste as máquinas protegidas e o nome do repositório remoto correspondente.

Exemplo:

Replicar duas máquinas protegidas para o Core remoto usando uma unidade de seeding de um compartilhamento de rede:

```
>cmdutil /replicate -targetserver 10.10.1.100 Administrator 123Q -replicationname
ReplicationName -seeddrive Network \\10.10.1.100\seeddrive Administrator 123Q -protectedserver
10.10.1.1 Repository1 10.10.1.2 Repository2
```

Replicação

Utilize o comando`replication` para controlar a replicação existente entre dois Rapid Recovery Cores e gerenciar solicitações de replicação pendentes.

NOTA: Este comando substitui o comando`Replicate`, que estabelece a conexão, chamada de emparelhamento, entre os Cores e usa uma unidade de seeding para o transferência inicial dos dados. Para obter mais informações sobre esse comando, consulte Replicate.

Forma de uso

A forma de uso do comando é a seguinte:

```
/replication [-list [incoming | outgoing | pending] -accept | -deny | -ignore | -delete | -
edit] -id [replication ID] -protectedserver [name | name repository] -responsecomment [comment]
-deleterecoverypoints -scheduletype [type] -dailystarttime [time] -dailyendtime [time] -
weekdaystarttime [time] -weekdayendtime [time] -weekendstarttime [time] -weekendendtime [time]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`replication`:

Tabela 204. Opções do comando Replication

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então serão usadas as credenciais para o usuário conectado
`-list`	A lista de trabalhos de replicação de entrada ou de saída ou de solicitações de replicação pendentes.
`-accept`	Aceita a solicitação de replicação.
`-deny`	Nega a solicitação de replicação.

Opção	Descrição
`-ignore`	Ignora a solicitação de replicação.
`-delete`	Use esta opção para apagar um trabalho de replicação existente ou uma máquina do trabalho de replicação. Especifique apenas o parâmetro `-id` para apagar uma relação de replicação inteira ou para especificar os parâmetros `-id` e `-protectedserver` para apagar apenas máquinas específicas da replicação.
`-edit`	Edita os trabalhos do programa de uma replicação existente.
`-id`	O identificador para o trabalho de replicação ou para a solicitação de replicação pendente. Pode ser um ID de Core remoto, um nome de host, um ID do cliente, um endereço de e-mail, ou um ID de solicitação de replicação pendente.
`-protectedserver`	Ao responder a uma solicitação de replicação, use esta opção para aplicar sua resposta à lista de servidores protegidos com um nome de repositório ou um ID. Use o parâmetro "all" (todos) para aplicar uma resposta a todas as máquinas solicitadas.
`-responsecomment`	O comentário que você fornecer com uma resposta para uma solicitação de replicação pendente.
`-deleterecoverypoints`	Use esta opção se determinados pontos de recuperação de uma máquina replicada excluída devem também ser removidos.
`-scheduletype`	Se você usar a opção `-edit`, esta opção especifica o tipo de programação de replicação. Inclui um dos quatro valores a seguir: • atalltimes - replica automaticamente a qualquer momento. • daily - replica diariamente. Especifique os parâmetros `-dailystarttime` e `-dailyendtime`. • custom - ao usar a replicação diariamente, use este valor para programar a replicação em dias da semana ou nos final de semana. Especifique os parâmetros `-weekdaystarttime`, `-weekdayendtime`, `-weekendstarttime` e `-weekendendtime`.
`-dailystarttime`	Use apenas para o valor diário da opção `-scheduletype`. É usada para estabelecer uma janela de tempo para quando a replicação deve ocorrer. Use esta opção para especificar o horário mais cedo do dia em que você quer que a replicação comece.
`-dailyendtime`	Use apenas para o valor diário da opção `-scheduletype`. É usada para estabelecer uma janela de tempo para quando a replicação deve ocorrer. Use esta opção para especificar o horário mais tarde do dia em que você quer que a replicação comece.
`-weekdaystarttime`	Use apenas para o valor personalizado da opção `-scheduletype`. É usada para estabelecer uma janela de tempo para quando a replicação deve ocorrer. Use esta opção para especificar o horário mais cedo de um dia da semana em que você quer que a replicação comece.
`-weekdayendtime`	Use apenas para o valor personalizado da opção `-scheduletype`. É usada para estabelecer uma janela de tempo para quando a replicação deve ocorrer. Use esta opção para especificar o horário mais tarde de um dia da semana em que você quer que a replicação comece.
`-weekendstarttime`	Use apenas para o valor personalizado da opção `-scheduletype`. É usada para estabelecer uma janela de tempo para quando a replicação deve ocorrer. Use esta opção para especificar o horário mais cedo do fim de semana em que você quer que a replicação comece.
`-weekendendtime`	Use apenas para o valor personalizado da opção `-scheduletype`. É usada para estabelecer uma janela de tempo para quando a replicação deve ocorrer. Use esta opção para especificar o horário mais tarde do fim de semana em que você quer que a replicação comece.

Exemplo:

Mostrar uma lista de todas as replicações de entrada:

```
>cmdutil /replication -list incoming
```

Aceitar solicitações de replicação pendentes para duas máquinas protegidas:

```
>cmdutil /replication -accept -id customer@email.address -protectedserver 10.10.1.1 Repository1
10.10.1.2 Repository2 -responsecomment A response comment
```

Negar uma solicitação de replicação pendente:

```
>cmdutil /replication -deny -id customer@email.address
```

Excluir replicação existente com os pontos de recuperação replicados:

```
>cmdutil /replication -delete -id RemoteServerHostname -deleterecoverypoints
```

Remover duas máquinas da replicação existente:

```
>cmdutil /replication -delete -id "156d7a46-8e44-43f4-9ed8-60d998e582bf" -protectedserver
10.10.1.1 10.10.1.2
```

Editar a programação de replicação com os horários especificados dos dias da semana e do fim de semana:

```
>cmdutil /replication -edit -id RemoteServerHostName -scheduletype custom -weekdaystarttime
"9:00 AM" -weekdayendtime "6:00 PM" -weekendstarttime "9:00 AM" -weekendendtime "6:00 PM"
```

RestoreAgent

O comando`restoreagent` permite restaurar uma máquina protegida ou um volume em um ponto de recuperação do Rapid Recovery específico.

Forma de uso

A forma de uso do comando é a seguinte:

```
/restoreagent -protectedserver [name | IP address] -rpn [recovery point number] -volumes [IDs |
names | all] -targetmachine [name] -targetvolume [volume name] -forcedismount -autorestart
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`restoreagent`:

Tabela 205. Opções do comando RestoreAgent

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.

Opção	Descrição
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-protectedserver`	O nome ou o endereço IP do servidor que você deseja restaurar.
`-rpn`	O número de identificação do ponto de recuperação que você quer usar para restaurar a máquina. Para encontrar o número correto, use o comando `/list rps`.
`-volumes`	Os IDs ou os nomes dos volumes que você quer restaurar. Para restaurar todos os volumes protegidos, utilize `–volumes all`.
`-targetmacchine`	O nome da máquina para a qual você quer restaurar a máquina protegida.
`-targetvolume`	O nome ou o ID do volume para a qual você deseja restaurar a máquina.
`-forcedismount`	Opcional. Use essa opção para forçar a desmontagem do banco de dados sob demanda.
`-autorestart`	Opcional. Use esse comando se você a reinicialização de uma máquina Exchange Server for necessária.

Exemplo:

Restaure uma máquina para uma máquina protegida com o endereço IP 192.168.20.130, inclusive a opção forçar desmontagem do banco de dados:

```
>cmdutil /restoreagent -protectedserver 192.168.20.130 -rpn 259 -volumes "F:" "E:" "C:" -
targetmachine 192.168.20.174 -targetvolume "E:" "G:" "F:" -forcedismount
```

RestoreArchive

Este comando restaura um arquivo a partir de um arquivo local ou partes e coloca os dados restaurados em um repositório específico.

Forma de uso

A forma de uso do comando é a seguinte:

```
/restorearchive -core [host name] -user [user name] -password [password] -all | -
protectedserver [name | IP address] -repository [name] -archiveusername [name] -archivepassword
[password] -path [location]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`restorearchive`:

Tabela 206. Opções do comando RestoreArchive

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-all`	Restaurar dados para todas as máquinas protegidas dos arquivos compactados.
`-protectedserver`	Máquina protegida com pontos de recuperação para restauro. Você pode especificar vários nomes de máquinas entre aspas duplas e separados por espaços.
`-repository`	Nome do repositório do Core onde os pontos de recuperação restaurados deverão ser colocados. O nome deve ser informado entre aspas duplas.
`-archiveusername`	Opcional. Nome de usuário da máquina remota. Necessário para caminho de rede apenas.
`-archivepassword`	Opcional. Senha para a máquina remota. Necessário para caminho de rede apenas.
`-path`	Local dos dados arquivados a serem restaurados; por exemplo: d:\work\archive ou network path \\servidor \compartilhamento.

Exemplos:

Restaurar dados arquivados para todos os servidores protegidos:

```
>cmdutil /restorearchive -core 10.10.10.10 -username administrator -password 23WE@#$sdd -all -
repository repository1 -path d:\work\archive
```

Restaurar dados arquivados para os servidores protegidos específicos:

```
>cmdutil /restorearchive -core 10.10.10.10 -username administrator -password 23WE@#$sdd -
protectedserver "10.10.20.30" "20.10.10.5" -repository repository1 -path d:\work\archive
```

RestoreUrc

O comando`restoreurc` permite que você restaure uma máquina protegida ou um volume a partir de um ponto de recuperação específico do Rapid Recovery em uma máquina sem sistema operacional usando o Universal Recovery Console (URC).

Forma de uso

A forma de uso do comando é a seguinte:

```
/restoreurc -protectedserver [name | IP address] -rpn [recovery point number] -volumes [IDs | names | all] -targetmachine [IP address] -urcpassword [password from the URC] -targetdisk [disk number | all]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`restoreurc`:

Tabela 207. Opções do comando RestoreUrc

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-protectedserver`	O nome ou o endereço IP do servidor para o qual você quer restaurar o URC.
`-rpn`	O número de identificação do ponto de recuperação que você quer usar para restaurar a máquina. Para encontrar o número correto, use o comando`/list rps`.
`-volumes`	Os IDs ou os nomes dos volumes que você quer restaurar. Para restaurar todos os volumes protegidos, utilize `–volumes all`.
`-targetmacchine`	O nome da máquina para a qual você quer restaurar a máquina protegida.
`-urcpassword`	A chave de autenticação do URC.
`-targetdisk`	Os números dos discos nos quais você quer restaurar a máquina. Para selecionar todos os discos da máquina usando o URC, utilize `-targetdisk all`.

Exemplo:

Restaurar uma máquina nos discos 0 e 1 da máquina usando o URC, quando o endereço IP do máquina do URC é 192.168.20.175:

```
>cmdutil /restoreurc -protectedserver 192.168.20.130 -rpn 259 -volumes "C:" "E:" -targetmachine 192.168.20.175 -urcpassword ******** -targetdisk 0 1
```

Resume

O administrador pode usar esse comando para retomar snapshots, exportar para uma máquina virtual e replicar. Você precisa especificar sua necessidade de retomar com um parâmetro. Os seguintes parâmetros são válidos: `snapshot`,`vmexport` e `replication`. Consulte Pause para obter mais detalhes.

Forma de uso

A forma de uso do comando é a seguinte:

```
/resume [snapshot | vmexport | replication] -core [host name] -user [user name] -password
[password] -all | -protectedserver [name | IP address] -incoming [host name] | outgoing [host
name] -time [time string]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`resume`:

Tabela 208. Opções do comando Resume

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-restore`	[`snapshots`], [`replication`] ou [`vmexport`].
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-all`	Retomar todos os agentes do Core selecionado.
`-protectedserver`	Retomar o servidor protegido atual.
`-incoming`	Nome do host do core remoto que replica para o core da máquina.
`-outgoing`	Nome do host do core de destino remoto no qual os dados são replicados.

Exemplos:

Retomar snapshots para os servidores protegidos específicos:

```
>cmdutil /resume snapshot -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.10.4
```

Retomar exportação para máquina virtual para todas as máquinas protegidas no core:

```
>cmdutil /resume vmexport -core 10.10.10.10 -user administrator -password 23WE@#$sdd -all
```

Retomar replicação de saída no core de uma máquina protegida específica:

```
>cmdutil /resume replication -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.1.76
```

Retomar replicação de saída para todas as máquinas protegidas no core de destino:

```
>cmdutil /resume replication -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
outgoing 10.10.1.63
```

Retomar replicação de entrada para todas as máquinas do core de destino:

```
>cmdutil /resume replication -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
incoming 10.10.1.82
```

SeedDrive

Você pode usar uma unidade de seeding para a transferência de dados inicial ao estabelecer a replicação do Rapid Recovery.

Forma de uso

A forma de uso do comando é a seguinte:

```
/seeddrive [-list | -startcopy | -startconsume | -abandon] -path [local | network path] -
seeddriveusername [user name] -seeddrivepassword [password] -remotecore [name] [-targetcore
[name or IP] | -protectedserver [name] | -all] -usecompatibleformat
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`seeddrive`:

Tabela 209. Opções do comando SeedDrive

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. O nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. A senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-list`	A lista de unidades de seeding pendentes com informações estendidas.
`-startcopy`	Iniciar cópia de dados para a unidade de propagação.
`-startconsume`	Iniciar consumo da unidade de propagação.

Opção	Descrição
`-abandon`	Abandonar a solicitação pendente da unidade de propagação.
`-path`	O caminho local ou de rede da unidade de seeding.
`-seeddriveusername`	Opcional. O nome de usuário para o local de rede da unidade de seeding.
`-seeddrivepassword`	Opcional. A senha para o local de rede da unidade de seeding.
`-targetcore`	Opcional. Use somente com a opção `-copy`. É o nome ou o endereço IP do Core remoto. Todas as máquinas protegidas sendo replicadas nesse Core recebem pontos de recuperação da unidade de seeding.
`-remotecore`	Use somente com a opção `-consume`. É o nome do Core remoto a partir do qual os pontos de recuperação da unidade de seeding são criados ou consumidos.
`-protectedserver`	O nome ou o endereço IP da máquina protegida que você está usando para criar ou consumir a unidade de seeding de pontos de recuperação. Por exemplo: -protectedserver "10.10.60.48" "10.10.12.101."
`-all`	Esta opção especifica o consumo ou a cópia de todas as máquinas protegidas disponíveis.
`-usecompatibleformat`	O novo formato de arquivamento oferece melhor desempenho, contudo, não é compatível com os Cores mais antigos. Use esta opção ao trabalhar com um AppAssure Core antigo.

Exemplos:

Listar unidades de seeding pendentes:

```
>cmdutil /seeddrive -list
```

Copiar duas máquinas protegidas para a unidade de seeding no compartilhamento de rede:

```
>cmdutil /seeddrive -startcopy -remotecore TargetCoreName -path \\10.10.1.1\Share\Seed\ -
seeddriveusername Administrator -seeddrivepassword 12345 -usecompatibleformat
```

Iniciar o consumo da unidade de seeding:

```
>cmdutil /seeddrive -startconsume -path \\10.10.1.1\Share\Seed\ -seeddriveusername
Adminsitrator -seeddrivepassword 12345 -remotecore RemoteCoreName
```

Abandonar uma solicitação de unidade de seeding pendente:

```
>cmdutil /seeddrive -abandon RemoteCoreHostName
```

StartExport

O comando`startexport` força uma exportação única de dados de sua máquina protegida para um servidor virtual. Você pode exportar para ESXi, VMware Workstation, Hyper-V ou VirtualBox da máquina virtual. Se exportar ESXi, você deve especificar se o disco de aprovisionamento é thick ou thin.

Forma de uso

A forma de uso do comando é a seguinte:

```
/startexport -exporttype [esxi | vm | hyperv | vb] -core [host name] -user [user name] -
password [password] -protectedserver [name | IP address] -volumes [volume names] -rpn [recovery
point number | numbers] | -time [time string] -vmname [virtual machine name] -hostname [virtual
host name] -hostport [virtual hostport number] -hostusername [virtual host user name] -
hostpassword [virtual host password] [-ram [total megabytes] | -usesourceram] -diskprovisioning
[thin | thick] -diskmapping [automatic | manual | withvm] -targetpath [location] -pathusername
[user name] -pathpassword [password] [-uselocalmachine]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`startexport`:

Tabela 210. Opções do comando StartExport

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-exporttype`	Realizar exportação de dados do servidor protegido para um servidor ESXi ('esxi'), servidor VMware Workstation ('vm'), servidor Hyper-V ('hyperv') ou servidor VirtualBox ('vb').
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-protectedserver`	Máquina protegida com pontos de recuperação a serem exportados.
`-volumes`	Opcional. Lista de nomes de volumes a serem exportados. Se não especificado, todos os volumes serão exportados. Os valores devem ser informados entre aspas duplas e separados por espaços; por exemplo: “c:” “d:”. Não use barras nos nomes dos volumes.
`-rpn`	Opcional. O número sequencial de um ponto de recuperação para exportar (use o comando Get-RecoveryPoints para obter os números). Se nenhuma opção ‘time’ ou ‘rpn’ for especificada, então, o ponto de recuperação mais recente é exportado.
`-time`	Opcional. Determinar ponto ou pontos de recuperação a serem selecionados para exportação. Você deve especificar o tempo exato no formato “mm/dd/aaaa hh:mm tt” (por exemplo, “2/24/2012 09:00 AM”). Lembrar de especificar os valores de data e de tempo definidos no seu PC. Nota: se nenhuma opção ‘time’ ou ‘rpn’ for especificada, então, o ponto de recuperação mais recente é exportado.
`-vmname`	O nome do Windows da máquina virtual.
`-hostname`	Para exportações virtuais do ESXi e Hyper-V apenas. O nome do host do servidor virtual.
`-linuxhostname`	Para exportação do VirtualBox apenas. O nome do host do servidor virtual.

Opção	Descrição
`-hostport`	Para exportações virtuais do ESXi e Hyper-V apenas. O número da porta do servidor virtual.
`-hostusername`	Para exportações virtuais do ESXi e Hyper-V apenas. O nome de usuário para o host do servidor virtual.
`-hostpassword`	Para exportações virtuais do ESXi e Hyper-V apenas. A senha para o host do servidor virtual.
`-ram`	Use esta opção para alocar uma quantidade específica de RAM no servidor virtual.
`-usesourceram`	Opcional. Use esta opção para alocar a mesma quantidade de RAM no servidor virtual que a máquina de origem contém.
`-diskprovisioning`	Use esta opção para exportações do ESXi apenas. Opcional. A quantidade de espaço em disco que você quer alocar na máquina virtual. Use uma das duas especificações a seguir: • Grosso - Esta especificação torna o disco virtual tão grande quanto a unidade original na máquina protegida. • Fino - Esta especificação aloca a quantidade de espaço em disco ocupada no momento na unidade original com mais alguns megabytes. A especificação padrão é "fino".
`-diskmapping`	Use esta opção para exportações do ESXi apenas. Opcional. Esta opção determina como mapear os discos da máquina protegida para a máquina virtual. Use um dos seguintes valores: • auto - Este valor mapeia os discos automaticamente. • manual - Este valor permite que você mapeie os discos manualmente. • withvm - Este valor armazena os discos virtuais no armazenamento de dados que você selecionar. O valor padrão é "auto".
`-targetpath`	Para exportações do VMware Workstation ou do VirtualBox apenas. Esta opção especifica o caminho de rede ou local (ou o caminho do Linux, para VirtualBox apenas) até a pasta onde você quer armazenar os arquivos da máquina virtual
`-pathusername`	Para exportações do VMware Workstation apenas. É o nome de usuário para a máquina da rede. É necessário apenas quando você especifica o caminho de rede na opção `-targetpath`.
`-pathpassword`	Para exportações do VMware Workstation apenas. É a senha para a máquina da rede. É necessário apenas quando você especifica o caminho de rede na opção `-targetpath`.
`-uselocalmachine`	Para exportações do Hyper-V apenas. Opcional. Use este comando para conectar-se ao servidor Hyper-V local. Esta opção ignora as opções `-hostname`, , ,`-hostport` `-hostusername`e `-hostpassword`.

Exemplos:

Exportar dados para uma máquina virtual ESXi com um nome específico e a mesma quantidade de RAM e tamanho do disco como o server de origem protegido:

```
>cmdutil     /startexport -exporttype esxi -core 10.10.10.10 -user administrator -password
23WE@#$sdd -protectedserver 10.10.5.22 -vmname Win2008-Smith -hostname 10.10.10.23 -hostport
443 -hostusername root -hostpassword 12QWsdxc@# -usesourceram -diskprovisioning thick
```

Criar um arquivo de máquina VMware Workstation na unidade local com dados protegidos do ponto de recuperação #4:

```
>cmdutil /startexport -exporttype vmstation -core 10.10.10.10 -user administrator -password
23WE@#$sdd -protectedserver 10.10.5.22 -rpn 4 -vmname Win2008-Smith -targetpath c:
\virtualmachines -ram 4096
```

Criar arquivos de máquina Hyper-V a serem arquivados numa máquina remota:

```
>cmdutil /startexport -exporttype hyperv -core 10.10.10.10 -user administrator -password 23WE@#
$sdd -protectedserver 10.10.5.22 -vmlocation \\WIN7-Bobby\virtualmachines -hostname 10.10.10.23
-hostport 443 -hostusername root -hostpassword 12QWsdxc@# -ram 4096
```

UpdateRepository

O comando`updaterepository` adiciona um local de armazenamento novo a um repositório existente.

Forma de uso

A forma de uso do comando é a seguinte:

```
/updaterepository -name [repository name] -size [size of the repository] [-datapath [data path]
-metadatapath [metadata path] | [-uncpath [UNC path] -shareusername [share user name] -
sharepassword [share password] -core [host name] -user [user name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`updaterepository` :

Tabela 211. Opções do comando UpdateRepository

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-name`	Nome do repositório.
`-size`	Tamanho do local de armazenamento do repositório. As unidades disponíveis são b, Kb, Mb, Gb, Tb, e Pb.
`-datapath`	Para espaço local, somente. Determinar o caminho de dados do local de armazenamento do repositório.
`-metadatapath`	Para espaço local, somente. Determinar o caminho de metadados do local de armazenamento do repositório.
`-uncpath`	Para local partilhado, somente. Determinar os caminhos de dados e metadados do local de armazenamento do repositório.
`-shareusername`	Para local partilhado, somente. Determina o nome de usuário para o local de compartilhamento.
`-sharepassword`	Para local partilhado, somente. Determinar senha para local partilhado.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.

Exemplos:

Criar um novo local de armazenamento no repositório de DVM local:

```
>cmdutil /updaterepository -name "Repository 1" -size 200Gb -datapath d:\repository -
metadatapath d:\repository -core 10.10.10.10:8006 -username administrator -password 23WE@#$sdd
```

Criar um local de armazenamento para um repositório de DVM no local partilhado:

```
>cmdutil /updaterepository -name "Repository 1" -size 200Gb -uncpath \\share\repository -
shareusername login -sharepassword 23WE@#$sdd -core 10.10.10.10:8006 -username administrator -
password 23WE@#$sdd
```

Versão

O comando`version` exibe informações sobre a versão do software Rapid Recovery instalado no servidor especificado. Se você não especificar um Core ou server protegido, serão retornadas informações relacionadas ao Core no qual você está trabalhando no momento.

Forma de uso

A forma de uso do comando é a seguinte:

```
/[version | ver] -protectedserver [name | IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`version`:

Tabela 212. Opções do comando Version

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-protectedserver`	Opcional. A máquina protegida cujas informações de versão você deseja visualizar. Se você não especificar uma máquina protegida, serão retornadas informações sobre a máquina Core na qual você está trabalhando no momento.

Exemplo:

Exibir informações sobre a versão do Rapid Recovery instalado no Rapid Recovery Core atual:

```
>cmdutil /version
```

VirtualStandby

Você pode usar o comando`virtualstandby` para exportar os dados de uma máquina protegida Rapid Recovery para uma máquina virtual compatível.

Forma de uso

A forma de uso do comando é a seguinte:

```
/virtualstandby -edit -exporttype [esxi | vm | hyperv | vb] -core [host name] -user [user name]
-password [password] -protectedserver [name | IP address] -volumes [volume names] -vmname
[virtual machine name] -gen2 -hostname [virtual host name] -hostport [virtual host port number]
-hostusername [virtual host user name] -hostpassword [virtual host password] [-ram [total
megabytes] | -usesourceram] -diskprovisioning [thin | thick] -diskmapping [automatic | manual |
withvm] -targetpath [location] -pathusername [user name] -pathpassword [password] [-uselocal
machine] -initialexport
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`virtualstandby`:

Tabela 213. Opções do comando VirtualStandby

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-exporttype`	Esta opção exporta os dados de uma máquina protegida para um dos seguintes servidores virtuais especificados: • esxi (ESXi) • vm (VMware Workstation) • hyperv (Hyper-V) • vb (VirtualBox)
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. O nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-password`	Opcional. A senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nenhum for fornecido, então, serão usadas as credenciais para o usuário conectado.
`-protectedserver`	Use esta opção para especificar a máquina protegida cujos pontos de recuperação você quer exportar.

Opção	Descrição
`-volumes`	Opcional. Use esta opção para listar os nomes dos volumes que você quer exportar. Se você não especificar nenhum volume, todos os volumes no ponto de recuperação serão exportados. Coloque os valores entre aspas duplas e separe-os com um espaço; por exemplo: "c:" "d: ". Não use barras nos nomes dos volumes.
`-ram`	Use esta opção para alocar uma quantidade específica de RAM no servidor virtual.
`-usesourceram`	Opcional. Use esta opção para alocar a mesma quantidade de RAM no servidor virtual que a máquina de origem contém.
`-vmname`	O nome do Windows da máquina virtual.

`-gen2`	Opcional. Esta opção especifica a Geração 2 do servidor VM. Se você não especificar a geração, o comando usa a Geração 1. Os seguintes sistemas operacionais suportam a Geração 2:
	• Windows
	  • Windows Server 2012 R2
	  • Windows 8,1
	• Ubuntu Linux
	  • CentOs
	  • RHEL
	  • Oracle Linux 7

`-hostname`	Para exportações virtuais do ESXi e Hyper-V apenas. O nome do host do servidor virtual.
`-linuxhostname`	Para exportação do VirtualBox apenas. O nome do host do servidor virtual.
`-hostport`	Para exportações virtuais do ESXi e Hyper-V apenas. O número da porta do servidor virtual.
`-hostusername`	Para exportações virtuais do ESXi e Hyper-V apenas. O nome de usuário para o host do servidor virtual.
`-hostpassword`	Para exportações virtuais do ESXi e Hyper-V apenas. A senha para o host do servidor virtual.
`-diskprovisioning`	Para exportações do ESXi apenas. Opcional. A quantidade de espaço em disco que você quer alocar na máquina virtual. Use uma das duas especificações a seguir: • Grosso - Esta especificação torna o disco virtual tão grande quanto a unidade original na máquina protegida. • Fino - Esta especificação aloca a quantidade de espaço em disco ocupada no momento na unidade original com mais alguns megabytes. A especificação padrão é "fino".
`-diskmapping`	Para exportações do ESXi apenas. Opcional. Esta opção determina como mapear os discos da máquina protegida para a máquina virtual. Use um dos seguintes valores: • auto - Este valor mapeia os discos automaticamente. • manual - Este valor permite que você mapeie os discos manualmente. • withvm - Este valor armazena os discos virtuais no armazenamento de dados que você selecionar. O valor padrão é "auto".
`-targetpath`	Para exportações do VMware Workstation ou do VirtualBox apenas. Esta opção especifica o caminho de rede ou local (ou o caminho do Linux, para VirtualBox apenas) até a pasta onde você quer armazenar os arquivos da máquina virtual.
`-pathusername`	Para exportações do VMware Workstation apenas. É o nome de usuário para a máquina da rede. É necessário apenas quando você especifica o caminho de rede na opção `-targetpath`.

Opção	Descrição
`-pathpassword`	Para exportações do VMware Workstation apenas. É a senha para a máquina da rede. É necessário apenas quando você especifica o caminho de rede na opção `-targetpath`.
`-uselocalmachine`	Para exportações do Hyper-V apenas. Opcional. Use este comando para conectar-se ao servidor Hyper-V local. Esta opção ignora as opções `-hostname, , ,-hostport -hostusernamee-hostpassword`.
`-edit`	Opcional. Esta opção permite que você edite as máquinas virtuais existentes. Ela ignora as opções `-exporttypee-initialexport`.
`-initialexport`	Opcional. Esta opção especifica se uma exportação inicial de máquina virtual sob demanda deve ser iniciada depois de configurar um standby virtual contínuo.

Exemplos:

Configurar uma exportação de standby virtual para uma máquina virtual ESXi com o nome, quantidade de RAM e o tamanho do disco do servidor protegido de origem:

```
>cmdutil /virtualstandby -exporttype esxi -core 10.10.10.10 -user administrator -password 23WE@#
$sdd -protectedserver 10.10.5.22 -vmname Win2008-Smith -hostname 10.10.10.23 -hostport 443 -
hostusername root -hostpassword 12QWsdxc@# -usesourceram -diskprovisioning thick
```

Configurar uma exportação de standby virtual para um arquivo de máquina VMWare Workstation na unidade local:

```
>cmdutil /virtualstandby -exporttype vm -core 10.10.10.10 -user administrator -password 23WE@#
$sdd -protectedserver 10.10.5.22 -vmname Win2008-Smith -targetpath c:\virtualmachines -ram 4096
```

Configurar uma exportação de standby virtual para arquivos de máquina Hyper-V e armazená-los em uma máquina remota:

```
>cmdutil /virtualstandby -exporttype hyperv -core 10.10.10.10 -user adminstrator -password
23WE@#$sdd -protectedserver 10.10.5.22 -vmname Win20008-Smith -vmlocation \\WIN7-Bobby
\virtualmachines -hostname 10.10.10.23 -hostport 443 -hostusername root -hostpassword
12QWsdxc@# -ram 4096
```

Localização

Quando é executado na mesma máquina em que o Rapid Recovery Core está instalado, o utilitário Rapid Recovery Command Line Management usa como idioma de exibição o idioma configurado para o Rapid Recovery Core. Nesta versão, os idiomas compatíveis são inglês, chinês (simplificado), francês, coreano, alemão, japonês, português (Brasil) e espanhol.

Se o Rapid Recovery Command Line Management estiver instalado em uma máquina separada, inglês é o único idioma compatível.

A

Referências do Core Console

Este apêndice contém as tabelas de referência que descrevem muitas das funções e ícones disponíveis no Rapid Recovery Core Console. Ele funciona como um complemento para o capítulo Noções básicas do Rapid Recovery Core Console do Guia do Usuário do *Dell Data Protection | Rapid Recovery.*

Tópicos:

- Como ver a interface do usuário do Core Console
- Como ver o painel Máquinas protegidas

Como ver a interface do usuário do Core Console

Core Console é a interface do usuário por meio da qual os usuários interagem com o Rapid Recovery. Ao efetuar login no Rapid Recovery Core Console, você vê os elementos a seguir.

Tabela 214. Elementos de UI incluídos no Core Console

Elemento de UI	Descrição
Área de imagem corporativa	Para ambientes típicos, o lado superior esquerdo do Core Console tem o nome do produto completo, inclusive o logotipo Dell. Clicar em qualquer lugar na área da marca resulta na abertura de uma nova guia do navegador da Web, exibindo a documentação no site de suporte do produto.
Barra de botões	A barra de botões, exibida à direita da área da marca, contém botões acessíveis de qualquer lugar do Core Console. Esses botões abrem assistentes para realizar tarefas comuns, como proteger uma máquina, realizar uma restauração do ponto de recuperação; criar, conectar ou importar um arquivo; ou replicar desse Core de origem para um Core de destino. Cada botão da barra de botões é descrito mais detalhadamente na tabela Tabela 215. Botões e menus da barra de botões.
Contagem de tarefas em execução	Mostra quantos trabalhos estão em execução no momento. Esse valor é dinâmico, com base no estado do sistema. Ao clicar no menu suspenso, você vê um resumo do status de todos os trabalhos em execução. Clicando no **X** de qualquer trabalho, você pode escolher cancelar esse trabalho.
Menu suspenso de Ajuda	O menu **Ajuda** inclui as seguintes opções: • **Ajuda**. Links para ajuda dentro do produto, que se abre em uma janela do navegador à parte. • **Documentação**. Links para a documentação técnica do Rapid Recovery no site do Suporte Dell. • **Suporte**. Links para o site do Suporte Dell, fornecendo acesso ao Live Chat, aos tutoriais em vídeo, aos artigos da base de conhecimento do Rapid Recovery, às perguntas frequentes e muito mais. • **Guia de início rápido**. O Guia de início rápido é um fluxo guiado de tarefas sugeridas para configurar e usar o Rapid Recovery. O guia é aberto automaticamente cada vez que você efetua login no Core Console, a menos que você desabilite essa função. Também é possível abrir o Guia de início rápido no menu Ajuda. Para obter mais informações sobre o Guia de início rápido, consulte Noções básicas sobre o Guia de início rápido. • **Sobre**. Abre a caixa de diálogo Sobre o Dell Data Protection | Rapid Recovery, que inclui informações da versão e uma descrição do software.

Elemento de UI	Descrição
Data e hora do servidor	A hora atual da máquina que executa o serviço Rapid Recovery Core é exibida no canto superior direito do Core Console. Quando você passa o mouse sobre a hora, a data do servidor também é exibida. Essa é a data e hora gravada pelo sistema para eventos como registro em log, programação e geração de relatórios. Por exemplo, ao aplicar as programações de proteção, o horário exibido no Core Console é usado. Isso é verdadeiro mesmo que o fuso horário seja diferente no server de banco de dados ou na máquina cliente onde o navegador está sendo executado.
Barra de ícones	A barra de ícones inclui uma representação gráfica das principais funções acessíveis no Core Console. Ela é exibida no lado esquerdo da interface do usuário (UI), logo abaixo da área da marca. O clique no item apropriado da barra de ícones leva você até a seção correspondente da UI, onde você pode gerenciar essa função. Cada um dos ícones da barra é descrito mais detalhadamente na tabela Tabela 216. Barra de ícones.
Área de navegação esquerda	A área de navegação esquerda é exibida no lado esquerdo da interface do usuário, abaixo da barra de ícones. • A área de navegação esquerda contém o filtro de texto e o menu Máquinas protegidas. • Se você adicionou replicação a esse Core, esta área contém um menu Máquinas replicadas. • Se há máquinas que foram removidas da proteção, mas cujos pontos de recuperação foram salvos, esta área contém um menu Apenas pontos de recuperação. • Se você adicionou grupos personalizados, esta área contém um menu Grupo personalizado. • Caso você tenha anexado um arquivo, essa área contém um menu de arquivos anexados. Você pode ativar ou desativar a exibição da área de navegação esquerda. Isso é útil quando é preciso ver mais conteúdo na área de navegação principal da UI. Para ocultar esta seção, clique na borda cinza entre as áreas de navegação esquerda e de navegação principal. Para mostrar este elemento de UI novamente, clique na borda cinza outra vez. Cada um dos elementos na área de navegação esquerda é descrito mais detalhadamente na tabela Tabela 218. Área de navegação à esquerda e menus.
Ajuda sensível ao contexto	 No Rapid Recovery Core Console, sempre que você clica no ícone Ajuda (um ponto de interrogação azul), uma janela de navegador redimensionável é aberta com dois frames. O frame esquerdo contém uma árvore de navegação que mostra os tópicos do Guia do usuário do Dell Rapid Recovery. O frame direito exibe o conteúdo para o tópico de ajuda selecionado. A qualquer momento, a árvore de navegação de ajuda se expande para exibir a localização do tópico selecionado em sua hierarquia. É possível procurar em todos os tópicos do Guia do usuário utilizando esse recurso de ajuda sensível ao contexto. Feche o navegador quando você terminar de pesquisar tópicos. Você pode também abrir a ajuda pela opção **Ajuda** do menu **Ajuda**.

Barra de botões

Os detalhes sobre a barra de botões são exibidos na tabela a seguir.

Tabela 215. Botões e menus da barra de botões

Elemento de UI	Descrição
Barra de botões: botão e menu Proteger	 O botão **Proteger** abre o Assistente de proteção de máquina, no qual você pode proteger uma única máquina no Rapid Recovery Core. Além disso, para outras opções de proteção, você pode acessar o menu suspenso próximo a esse botão, que inclui as opções a seguir. • A opção **Proteger máquina** é outro método para iniciar o assistente de proteção de máquina para proteger uma única máquina. • A opção **Proteger cluster** permite que você se conecte a um cluster de servidor.

Elemento de UI	Descrição
	• A opção **Proteger diversas máquinas** abre o Assistente de proteção de diversas máquinas a fim de permitir que você proteja duas ou mais máquinas simultaneamente. • A opção **Implantar software do agente** permite instalar o software do agente Rapid Recovery em uma ou mais máquinas simultaneamente. Essa função usa o Assistente de implantação do software do agente.
Barra de botões: botão e menu Restaurar 	O botão **Restaurar** abre o assistente Restaurar máquina, que permite restaurar dados a partir de pontos de recuperação salvos de uma máquina protegida. Além disso, para outras opções de restauração ou exportação, você pode acessar o menu suspenso próximo a esse botão, que inclui as opções a seguir. • A opção **Restaurar máquina** é outro método para abrir o Assistente de restauração de máquina a fim de restaurar dados. • A opção **Montar ponto de recuperação** abre o Assistente de montagem, que permite montar ponto de recuperação em uma máquina protegida. • O botão **Exportação do VM** abre o Assistente de exportação. Nesse assistente você pode criar uma máquina virtual usando pontos de recuperação salvos no Rapid Recovery Core. Você pode criar uma exportação única ou definir parâmetros para uma VM que é continuamente atualizada após cada snapshot de uma máquina protegida.
Barra de botões: botão e menu Arquivar 	O botão **Arquivar** abre o Assistente de arquivo. Nesse assistente você pode criar um arquivo único usando pontos de recuperação ou criar um arquivo e salvar continuamente nesse arquivo com base em um programa definido por você. Além disso, para outras opções de arquivamento, você pode acessar o menu suspenso próximo a esse botão, que inclui as opções a seguir. • A opção **Criar arquivo** é outro método para abrir o Assistente de criação de arquivo para criar um arquivo único ou arquivar continuamente. • A opção **Importar arquivo** abre o Assistente de importação de arquivo, que permite importar arquivo. • A opção **Anexar arquivo** monta um arquivo para você poder ler o conteúdo como um sistema de arquivos.
Barra de botões: botão Replicação 	O botão **Replicação** abre o Assistente de replicação. Nesse assistente você pode especificar um Core de destino, selecionar máquinas protegidas no Core de origem e replicar pontos de recuperação de máquinas protegidas para o Core de destino especificados por você. Você pausar a replicação ao defini-la, ou a replicação pode começar imediatamente. Além disso, você pode especificar se uma unidade de seeding será usada para copiar dados para pontos de recuperação existentes para o Core de destino.

Barra de ícones

Os detalhes sobre a barra de ícone são exibidos na tabela a seguir.

Tabela 216. Barra de ícones

Elemento de UI	Descrição
Barra de ícones	A barra de ícones inclui uma representação gráfica das principais funções acessíveis no Core Console. Quando você clica em um item, é conduzido para a seção correspondente da interface de usuário, onde pode gerenciar aquela função. Os ícones da barra de ícones são:
Barra de ícones: ícone Inicial	**Inicial**. Clique no ícone Inicial para navegar até a página Inicial do Core.
Barra de ícones: ícone Replicação	**Replicação**. Clique no ícone Replicação para visualizar ou gerenciar a replicação de entrada ou de saída.
Barra de ícones: ícone Standby virtual	**Standby virtual**. Clique no ícone Standby virtual para exportar informações de um ponto de recuperação para uma máquina virtual inicializável.
Barra de ícones: ícone Eventos	**Eventos**. Clique no ícone Eventos para visualizar um registro de todos os eventos relacionados ao Rapid Recovery Core.
Barra de ícones: ícone Definições	**Definições**. Clique no ícone Definições para visualizar ou gerenciar definições do Rapid Recovery Core. Você pode fazer cópia de segurança ou restaurar definições da configuração da restauração do núcleo. Você pode fazer definições gerais para controlar portas ou exibir aspectos. Além disso, você pode configurar definições nas seguintes categorias: atualizações automáticas; trabalhos noturnos; definições da fila de transferência; definições de tempo limite do cliente; definições de cache de deduplicação DVM; definições do Replay Engine e definições de implantação. Você pode visualizar ou alterar conexões do banco de dados; definições do servidor de SMTP; contas de armazenamento em nuvem e alterar definições de fonte para relatórios. Você pode determinar definições de capacidade de anexação SQL; definições de trabalho do núcleo; definições de licença; definições SNMP e definições vSphere.
Barra de ícones: ícone Mais	**Mais**. Clique no ícone Mais para acessar outros recursos importantes. Cada um tem o próprio ícone, listado abaixo.
Barra de ícones: ícone Mais	Informações do sistema	**Informações do sistema**. Clique em Informações do sistema para exibir dados sobre o servidor do Rapid Recovery Core. Você pode ver o nome de host, OS, arquitetura e memória do Core. Você pode ver o nome exibido no Core Console. Também pode visualizar o nome de domínio totalmente qualificado do Core na rede e o caminho para os metadados de cache e para o cache de deduplicação. Para obter mais informações sobre como alterar o nome de exibição, consulte Noções básicas sobre as informações do sistema do Core. Para obter mais informações sobre cache de deduplicação, consulte Noções básicas sobre o cache de deduplicação e locais de armazenamento. Para obter informações sobre como ajustar as definições, consulte Configuração das definições de cache de deduplicação DVM.
Barra de ícones: ícone Mais	Arquivos	**Arquivos**. Rapid Recovery permite gerenciar arquivos de informações no Core. Você pode visualizar informações sobre arquivos anexados ou programados e adicionar, verificar ou importar arquivos.
Barra de ícones: ícone Mais	Montagens	**Montagens**. Permite mostrar e desmontar montagens locais e mostrar e desconectar montagens remotas.

Elemento de UI	Descrição		
Barra de ícones: ícone Mais	CDs de inicialização		**CDs de inicialização**. Permite gerenciar CDs de inicialização, normalmente usados em uma bare metal restore (BMR). Você pode criar a imagem ISO de um CD de inicialização, excluir uma imagem existente ou clicar no caminho da imagem para abrir ou salvá-la.
Barra de ícones: ícone Mais	Repositórios		**Repositórios**. Permite mostrar e gerenciar repositórios associados ao Core.
Barra de ícones: ícone Mais	Chaves de criptografia		**Chaves de criptografia**. Permite mostrar, gerenciar, importar ou adicionar chaves de criptografia que você pode aplicar a máquinas protegidas. Caso não estejam sendo usadas, você pode excluir as chaves de criptografia.
Barra de ícones: ícone Mais	Contas de nuvem		**Contas de nuvem**. Permite mostrar e gerenciar conexões entre o seu Core e as contas de armazenamento em nuvem.
Barra de ícones: ícone Mais	Política de retenção		**Política de retenção**. Permite mostrar e modificar a política de retenção de núcleo, inclusive por quanto tempo manter pontos de recuperação antes de avançar e finalmente excluí-los.
Barra de ícones: ícone Mais	Notificações		**Notificações**. Permite configurar notificações sobre eventos do Core, determinar definições do servidor de SMTP para notificações de e-mail e configurar redução de repetição para suprimir notificações repetidas sobre o mesmo evento.
Barra de ícones: ícone Mais	Downloads		Downloads. Você pode baixar instalador da web do software do agente, o utilitário de montagem local ou os arquivos MIB que contêm informações do evento a serem usadas em um navegador SNMP.
Barra de ícones: ícone Mais	Relatórios		Relatórios. Permite acessar relatórios do Core ou agendar relatórios para serem gerados continuamente.
Barra de ícones: ícone Mais	Log do Core		Log do Core. Permite baixar o arquivo de log do Core para fins de diagnóstico.

Menu de navegação à esquerda

O conjunto completo de menus que podem aparecer na área de navegação esquerda está descrito na tabela a seguir:

Tabela 217. Opções do menu de navegação à esquerda

Elemento de UI	Descrição
Menu Máquinas protegidas	O menu de máquinas protegidas aparece como primeiro menu na área de navegação esquerda, se uma ou mais máquinas estiverem protegidas em seu Core. Quando você clica em uma máquina específica exibida nesse painel, uma página Resumo será exibida, mostrando informações resumidas sobre essa máquina selecionada. Para obter mais informações sobre o que você pode realizar na página Resumo, consulte Visualização das informações de resumo de uma máquina protegida.
Menu de máquinas replicadas	Se você visualizar o nome de um outro Rapid Recovery Core como um menu de navegação de nível superior, o Core no qual você esta visualizando o Console do Core é um Core de destino. O menu recebe o nome do Core de origem e cada máquina listada sob ele representa uma máquina do Core de origem que está replicada neste destino. Se este Core de destino replica os pontos de recuperação de mais de um Core de origem, cada Core de origem será exibido como seu próprio menu navegável na área de navegação à esquerda.

Elemento de UI	Descrição
	Quando você clica em uma máquina específica exibida em um menu de máquinas replicadas, uma página Resumo será exibida, mostrando informações resumidas sobre a máquina selecionada replicada. Para obter mais informações sobre replicação, consulte Replicação.
Menu Apenas pontos de recuperação	Se você visualizar um menu APENAS PONTOS DE RECUPERAÇÃO, o seu Core manterá os pontos de recuperação para uma máquina que esteja protegida ou replicada. Considerando que aquela máquina não continuará a capturar novos snapshots, os pontos de recuperação anteriormente capturados em seu Core permanecerão. Esses pontos de recuperação podem ser usados para recuperação em nível de arquivo, mas não podem ser usados para realizar um bare metal restore, restaurar volumes inteiros ou adicionar dados de snapshot.
Menu de grupos personalizados	Se você criou quaisquer grupos personalizados, um menu de grupos personalizados será exibido no menu de navegação. Os grupos personalizados são contêineres lógicos usados para agrupar máquinas (por exemplo, por função ou organização ou por localização geográfica). Os grupos personalizados podem conter objetos heterogêneos (máquinas protegidas, máquinas replicadas e assim por diante). Você pode definir o rótulo para um grupo personalizado; como outros menus, o nome é exibido no menu com todas as letras maiúsculas. Você pode executar ações para, por exemplo, itens em um grupo personalizado, clicando na seta à direita do título do grupo personalizado. Por exemplo, você pode forçar um snapshot para cada máquina protegida em um grupo personalizado. Para obter mais informações sobre como criar e gerenciar grupos personalizados, consulte Noções básicas sobre grupos personalizados.
Menu de arquivos anexados	Se você anexar qualquer arquivo em seu Core, cada arquivo será listada no menu de navegação à esquerda. Seu rótulo é o nome do arquivo. Cada máquina incluída no arquivo está contida nesta lista.

Os detalhes sobre os elementos na área de navegação à esquerda são exibidos na tabela a seguir.

Tabela 218. Área de navegação à esquerda e menus

Elemento de UI	Descrição	
Filtro de texto de menus das máquinas		Filtro de texto é um campo de texto que permite filtrar os itens exibidos nos menus Máquinas protegidas, Máquinas replicadas e Máquinas "apenas pontos de recuperação". Caso você digite os critérios neste filtro, apenas as máquinas que atendam aos critérios são exibidas nos menus apropriados.
Detalhes de Expandir e contrair		Clique na seta à direita do filtro de texto para expandir e contrair detalhes dos menus Máquinas protegidas, Máquinas replicadas e Máquinas "apenas pontos de recuperação".
Menu Máquinas protegidas	  	O menu Máquinas protegidas aparece na área de navegação esquerda da UI. Neste menu, você pode ver as máquinas protegidas, clusters protegidos ou máquinas replicadas configurados no Core. Se houver grupos protegidos ou máquinas apenas com pontos de recuperação, eles também serão exibidos como parte desse menu. Você pode minimizar ou expandir a visualização de qualquer uma das máquinas protegidas no Core clicando na seta no lado esquerdo do rótulo desse menu. O ícone exibido retrata o tipo de máquina: · Um ícone de máquina simples retrata uma máquina física ou uma VM protegida com software do agente Rapid Recovery instalado. · Um ícone de várias máquinas retrata um cluster protegido. · Um ícone de máquina dupla oco retrata uma VM VMware usando proteção sem agente. · Um ícone de máquina tripla oco retrata um host vCenter VMware.

Elemento de UI	Descrição
	Caso você clique no menu Máquinas protegidas, a página Máquinas protegidas é exibida, mostrando todas as máquinas protegidas neste Core no painel Máquinas protegidas. Para obter mais informações, consulte Visualização do menu Máquinas protegidas.
Menu Máquinas replicadas	Caso você esteja replicando máquinas de outro Rapid Recovery Core, o nome desse Core é exibido como um menu à parte no menu Máquinas protegidas. Cada máquina replicada nesse core de destino pelo núcleo de origem listado é exibida nesse menu. Para cada máquina replicada, o ícone indica o tipo de máquina replicada. Por exemplo, em caso de replicação de uma máquina única, o ícone mostra uma máquina. Em caso de replicação de um cluster de servidor, o ícone representa um cluster. Você pode minimizar ou expandir a visualização de qualquer uma dessas máquinas replicadas clicando na seta no lado esquerdo do rótulo desse menu. No menu Máquinas replicadas, você pode executar ações em todas as máquinas replicadas. Se você clicar no menu Máquinas replicadas, a página Máquinas é exibida. Essa página mostra todas as máquinas protegidas em outro Core (de origem) que são replicadas para este Core de destino. Para obter mais informações, consulte Ver máquinas replicadas no menu de navegação.
Menu Apenas pontos de recuperação	Se alguma máquina que estava protegida anteriormente no Core tiver sido removida da proteção sem que seus pontos de recuperação tenham sido excluídos, o menu Apenas pontos de recuperação aparecerá. Cada uma das máquinas protegidas anteriormente com pontos de recuperação retidos é exibida nessa lista. Você pode minimizar ou expandir a visualização de qualquer uma das máquinas "apenas pontos de recuperação" clicando na seta no lado esquerdo do rótulo desse menu. No menu Apenas pontos de recuperação, você pode remover os pontos de recuperação de todas as máquinas que têm apenas pontos de recuperação neste Core. Quando você clica no menu Apenas pontos de recuperação, a página Máquinas aparece, mostrando as máquinas cujos pontos de recuperação foram salvos. Para obter mais informações, consulte Visualizar o menu Apenas pontos de recuperação.
Menu Grupos personalizados	Se o Core inclui algum grupo personalizado, a área de navegação esquerda inclui um menu Grupo personalizado. Cada um dos objetos nesse grupo personalizado é exibido nessa lista. Você pode minimizar ou expandir a visualização de qualquer um dos grupos personalizados no Core clicando na seta no lado esquerdo do rótulo desse menu. No menu Grupos personalizados, você pode executar ações com itens semelhantes no grupo. Caso você clique no menu Grupos personalizados, a página Máquinas é exibida, mostrando um painel para cada um dos objetos Rapid Recovery exibidos no grupo: máquinas protegidas, máquinas replicadas e máquinas "apenas pontos de recuperação". Para obter mais informações, consulte Visualizar o menu Grupos personalizados.
Menu Arquivos anexados 	Caso você tenha anexado qualquer arquivo ao Core, a área de navegação à esquerda inclui um menu para cada arquivo anexado. Cada uma das máquinas protegidas incluídas no arquivo é exibida nessa lista. O rótulo do menu usa o nome especificado quando o arquivo foi salvo. Você pode minimizar ou expandir a visualização de qualquer um dos arquivos anexados no Core clicando na seta no lado esquerdo do rótulo desse menu. No menu de arquivos anexados, você pode realizar ações para itens semelhantes no grupo. Caso você clique no menu de arquivos anexados, a página Máquinas é exibida, mostrando um painel para cada um dos objetos Rapid Recovery exibidos no grupo: máquinas protegidas, máquinas replicadas e máquinas "apenas pontos de recuperação". Para obter mais informações, consulte Visualizar o menu Grupos personalizados.

Como ver o painel Máquinas protegidas

O painel Máquinas protegidas contém informações sobre todas as máquinas protegidas nesse Rapid Recovery Core. Para cada máquina protegida (se houver algumas ainda não protegidas), você verá listados na grade as informações descritas na tabela a seguir.

Tabela 219. Informações sobre cada máquina protegida

Elemento INTERFACE	Descrição
Selecionar item	Para cada fila na tabela de resumo, você pode selecionar a caixa de seleção para executar ações da lista de opções de menu acima da tabela.
Tipo	Mostra o tipo de máquina.
Indicador de status	Círculos coloridos na coluna Status mostram se uma máquina está on-line ou não encontrada. Se você passar o cursor sobre o círculo colorido, a condição de status é exibida. As Condições de status incluem verde (on-line e protegido), amarelo (proteção pausada), vermelho (erro de autenticação), e cinza (offline ou não encontrada).
Status da criptografia	O ícone de cadeado indica o status da criptografia para a máquina protegida selecionada. Um cadeado aberto indica que não há criptografia; um cadeado fechado indica que as chaves de criptografia estão estabelecidas. Para obter mais informações sobre criptografia, consulte Compreender as chaves de criptografia.
Nome da tela	O nome de exibição da máquina protegida.
Último snapshot	Lista a data e a hora dz últimz transferência de backup desta máquina.
Nome do repositório	Lista o repositório no qual os dados para esta máquina são armazenados.
Pontos de recuperação	Lista o número de pontos de recuperação e como eles consumem espaço no repositório.
Versão	A versão do software de agente Rapid Recovery carregado na máquina.
Ações	Quando você clica em Configurações do menu suspenso nessa coluna, você verá uma lista de ações para executar especificamente na máquina protegida selecionada.

Se todas as máquinas protegidas neste Core são configurados para espera virtual, em seguida, você verá informações adicionais, conforme descrito na tabela a seguir.

Tabela 220. Informações sobre máquinas protegidas configuradas para espera virtual

Elemento INTERFACE	Descrição
Última exportação	A data e a hora da última exportação virtual.
Destination (Destination)	O destino para salvar máquinas protegidas como uma máquina virtual. Por exemplo, ESXi, VMware Workstation, Hyper-V, ou VirtualBox.
Status	Status da máquina configurado para espera virtual. Condições de Status incluem “Em sincronia,” “Pausada,” e “Não ativada."

A partir do menu suspenso de Ações do painel Máquinas protegidas, você pode executar as ações descritas na tabela a seguir. Algumas opções só serão exibidas para um servidor Exchange ou o SQL, conforme indicado

Tabela 221. Ações disponíveis no painel Máquinas protegidas

Elemento INTERFACE	Descrição
Forçar snapshot	Permite que você forçar um snapshot ou um imagem de base incremental para todos os volumes protegidos em máquinas protegidas selecionadas. Para obter mais informações, consulte Forçar um snapshot.
Exportar uma única vez	Abre o Assistente de exportação de máquina virtual. Este Assistente permite que você execute uma única exportação de dados de um ponto de recuperação de uma máquina protegida à uma máquina virtual em qualquer formato VM suportado. Para obter mais informações, consulte Exportação de VM.
Virtual Standby (Espera virtual)	Abre o Assistente de exportação de máquina virtual. Este Assistente permite que você execute uma espera virtual para exportação de dados de um ponto de recuperação de uma máquina protegida à uma máquina virtual em qualquer formato VM suportado. Para obter mais informações, consulte Exportação de VM.
Mount (Montar)	Abre o Assistente para montagem. Este Assistente permite que você monte pontos de recuperação da máquina protegida selecionada.
Pontos de recuperação	Abre a página Resumo de Pontos de recuperação.
Restaurar	Abre o Assistente de restauração da máquina. Este processo permite restaurar dados a partir de um ponto de recuperação no núcleo à uma máquina protegida. Para obter mais informações, consulte Como restaurar volumes a partir de um ponto de recuperação.
Remover máquina	Remove a máquina selecionada da proteção no Rapid Recovery Core, deixando você escolher entre apagar ou reter os pontos de recuperação já no Rapid Recovery Core. Para obter mais informações, consulte Remover uma máquina.

Você pode executar ações em duas ou mais das máquinas listadas na grade de máquinas protegidas. Para executar ações em várias máquinas, selecione a caixa de seleção para cada máquina protegida. Em seguida, no menu acima da tabela de resumo, você pode executar qualquer uma das ações descritas na tabela a seguir.

Tabela 222. Ações adicionais estão disponíveis no painel Máquinas protegidas quando as máquinas são selecionadas

Elemento INTERFACE	Descrição
Forçar snapshot	Permite que você forçar um snapshot incremental para todos os volumes protegidos em máquinas protegidas selecionadas. Para obter mais informações, consulte Forçar um snapshot.
Forçar imagem de base	Permite forçar uma imagem de base para todos os volumes protegidos em máquinas protegidas selecionadas. Para obter mais informações, consulte Forçar um snapshot.
Proteção > Pausa ou Retomar	Permite pausar a proteção das máquinas selecionadas (se estiver ativada), ou permite que retome a proteção das máquinas selecionadas (se a proteção é pausada). Para obter mais informações, consulte Pausar e retomar a proteção.
Replicação	Permite que você ative, force, copie, pause ou retome a replicação. Você também pode copiar pontos de recuperação existentes para uma propagação de sementes. Para obter mais informações, consulte Gerenciar definições de replicação.
Cancelar	Permite que você cancele todas as operações ativas para as máquinas selecionadas, ou permite cancelar instantâneos apenas que já estão em curso para as máquinas selecionadas. Isso não afeta operações programadas para o futuro.
Remover máquinas	Remove a máquina selecionada da proteção no Rapid Recovery Core, deixando você escolher entre apagar ou reter os pontos de recuperação já no Rapid Recovery Core. Para obter mais informações, consulte Remover uma máquina.

A partir do menu suspenso Configuração para cada máquinas protegida, você pode executar as ações descritas na tabela a seguir. Algumas opções só serão exibidas para um servidor Exchange ou o SQL, conforme indicado.

Tabela 223. Ações disponíveis no painel Máquinas protegidas

Elemento INTERFACE	Descrição
Forçar snapshot	Permite que você forçar um snapshot ou um imagem de base incremental para um ou mais volumes em máquinas selecionadas. Para obter mais informações, consulte Forçar um snapshot.
Forçar log truncado para o Exchange	Para uma máquina Exchange Server protegida, força truncamento dos logs do Exchange, que identifica espaço livre no Exchange server. Para obter mais informações, consulte Forçar truncamento de log para uma máquina SQL.
Forçar log truncado para o SQL	Para uma máquina SQL Server protegida, força truncamento dos logs do SQL Server, que identifica espaço livre no SQL server. Para obter mais informações, consulte Forçar truncamento de log para uma máquina SQL.
Exportar	Abre o Assistente de exportação. Este Assistente permite exportar os dados de um ponto de recuperação de uma máquina protegida à uma máquina virtual em qualquer formato VM suportado. Você pode exportar uma única vez ou configurar uma espera virtual para exportação contínua. Para obter mais informações, consulte Exportação de VM.
Mount (Montar)	Abre a caixa de diálogo Montar ponto de recuperação, o que permite navegar pelos dados de snapshot salvos no Rapid Recovery Core para montar em um ponto de recuperação específico. Para obter mais informações, consulte Montar um ponto de recuperação ou Montar um volume de ponto de recuperação em máquina Linux, respectivamente.
Pontos de recuperação	Abre a aba Pontos de recuperação para a máquina agente selecionada. Para obter mais informações, consulte Gerenciar snapshots e pontos de recuperação.
Restaurar	Abre o Assistente de restauração da máquina. Este processo permite restaurar dados a partir de um ponto de recuperação no núcleo à uma máquina protegida. Para obter mais informações, consulte Como restaurar volumes a partir de um ponto de recuperação.
Remover máquina	Remove a máquina selecionada da proteção no Rapid Recovery Core, deixando você escolher entre apagar ou reter os pontos de recuperação já no Rapid Recovery Core. Para obter mais informações, consulte Remover uma máquina.

Visualizar eventos de uma máquina protegida

Na página **Eventos**, você pode visualizar os trabalhos que ocorreram ou estão em progresso na máquina protegida selecionada. Os botões na parte superior da página permitem navegar para listas de trabalhos em cada uma das três categorias de atividades:

- **Tarefas.** Um trabalho que deve ser realizado pelo Rapid Recovery para que funcione corretamente.
- **Alertas.**Ama notificação relacionada a uma tarefa ou evento que inclui erros e aviso.
- **Registro.**Uma combinação de todas as tarefas e alertas de máquinas protegidas.

A tabela a seguir contém descrições de cada elemento da página **Eventos**.

Tabela 224. Elementos da página Eventos

Elemento de UI	Descrição
Pesquisar palavra-chave	Permite pesquisar um item específico dentro de cada categoria. Disponível somente para tarefas.
De	Para restringir os resultados, você pode inserir uma data de início da pesquisa. Disponível somente para tarefas.
Para	Para restringir os resultados, você pode inserir uma data de término da pesquisa. Disponível somente para tarefas.
Ícones de status	Cada ícone representa um status diferente do trabalho. Para alertas e tarefas, clicar em um dos ícones permite filtrar a lista por esse status, gerando, essencialmente, um relatório. Quando você clica no ícone uma segunda vez, o filtro desse status é removido. Você pode filtrar por mais de um status. Os status são: • **Ativo.**Um trabalho em progresso. • **Enfileirado.** Um trabalho que está aguardando a conclusão de outro trabalho para poder começar. • **Aguardando.**Um trabalho que está aguardando sua aprovação ou conclusão, como uma unidade de propagação. (Para obter mais informações sobre unidades de propagação, consulte Replicação.) • **Concluído.**Um trabalho que foi concluído com êxito. • **Com falha.** Um trabalho que teve uma falha e não foi concluído.
Ícone de serviço	Este botão adiciona trabalhos de serviços à lista de trabalhos. Quando você clica nesse ícone, um ícone de serviço menor aparece em cada ícone de status, permitindo filtrar por trabalhos de serviço que possuam esses status (se houver). Exemplos de trabalhos de serviços são a exclusão de arquivos de índice ou a remoção de uma máquina da proteção.
Lista suspensa Tipo de exportação	A lista suspensa inclui os formatos para os quais você pode exportar o relatório de eventos. Disponível somente para tarefas. Ela inclui os seguintes formatos: • PDF • HTML • CSV • XLS • XLSX
Ícone (Exportar)	Converte o relatório de eventos para o formato selecionado. Disponível somente para tarefas.
Seleção de página	Os relatórios de eventos podem incluir vários trabalhos em múltiplas páginas. Os números e as setas na parte inferior da página **Eventos** permitem navegar pelas páginas adicionais do relatório.

O página **Eventos** exibe todos os eventos em uma tabela. A seguinte tabela lista as informações exibidas para cada item.

Tabela 225. Informações detalhadas da tabela de resumo de eventos

Elemento de UI	Descrição
Status	Exibe o status da tarefa, alerta ou item de registro. Disponível para alertas ou itens de registro, clique no cabeçalho para filtrar os resultados por status.
Nome	Nome está disponível somente para tarefas. Esse campo de texto lista o tipo de tarefa que foi concluída nessa máquina protegida. Os exemplos incluem transferência de volumes, manutenção de repositório, execução, realização de verificação de capacidade de montagem, realização de verificação de soma de verificação e assim por diante.
Hora inicial	Disponível para tarefas, alertas e itens de registro. Exibe a data e a hora de início do trabalho ou da tarefa.

Elemento de UI	Descrição
Hora final	Disponível somente para tarefas. Exibe a data e a hora de conclusão do trabalho ou da tarefa.
Detalhes do trabalho	Disponível somente para tarefas. Abra a caixa de diálogo **Monitorar tarefa ativa** de maneira que você possa visualizar os detalhes do trabalho ou da tarefa específico(a). Esses detalhes incluem um ID do trabalho, taxa de transferência de dados do core (se relevante), tempo decorrido para conclusão do trabalho, trabalho total em quantidade de gigabytes e tarefas subordinadas associadas ao trabalho.
Mensagem	Disponível para alertas e itens de registro. Esse campo de texto fornece uma mensagem descritiva do alerta ou do item de registro.

Como ver o menu Mais para obter uma máquina protegida

O menu **More (Mais)** oferece opções adicionais para ajudar a gerenciar a seleção de uma máquina protegida. Para acessar estas ferramentas, clique no menu suspenso More (Mais) e selecione uma das seguintes opções descritas na tabela a seguir.

Tabela 226. Ferramentas acessíveis a partir da opção Mais para uma máquina protegida

Elemento INTERFACE	Descrição
System Information (Informações do sistema)	Exibe as informações sobre a máquina protegida, informações do sistema, volumes, processadores, adaptadores de rede e endereços IP para esta máquina. Para obter mais informações, consulte Visualização das informações do sistema de uma máquina protegida.
Montagens	A partir do painel Montagens local, você pode ver ou desmontar volumes montados localmente. Do painel Remote Mounts (Montagens remotas) , você pode ver ou desmontar volumes montados usando o utilitário Montagem local. Para obter informações sobre como desmontar volumes, consulte Desmontar pontos de recuperação. Para obter informações sobre a montagem de um ponto de recuperação localmente, consulte Montar um ponto de recuperação ou Montar um volume de ponto de recuperação em máquina Linux, respectivamente.
Política de retenção	Permite que você especifique uma política de retenção para a máquina selecionada. Você pode optar por usar a política padrão do Núcleo, ou você pode diferenciar a política de retenção para esta máquina. Para obter mais informações, consulte Como personalizar as configurações de uma política de retenção para uma máquina protegida.
Notificações	Permite que você especifique um grupo de notificação personalizado para eventos relacionados à máquina selecionada. Esta não altera as notificações já definidas no Núcleo. Para obter mais informações, consulte Configurar grupos de notificação.
Log do agente	Permite que você faça o download e veja o arquivo de log para uma máquina protegida usando o software Rapid Recovery Agent. Para obter mais informações, consulte Download e visualização do arquivo de log de uma máquina protegida.

B

Compreender o módulo Rapid Recovery PowerShell

O Dell Data Protection | Rapid Recovery consiste de vários componentes de software. Os principais componentes relevantes a este tópico incluem o seguinte:

- O Rapid Recovery Core gerencia autenticações para máquinas protegidas, programações para transferir dados para backup e replicação, exportação para máquinas virtuais, criação de relatórios e restauração sem sistema operacional (BMC) para hardware similar ou diferente.
- O Agente Rapid Recovery é responsável por capturar snapshots de volume e pela rápida transferência de dados para o repositório gerenciado pelo Core.
- O módulo Rapid Recovery PowerShell é um utilitário do Windows que permite que os usuários interajam com o servidor do Core usando scripts Windows PowerShell®. Este módulo oferece algumas das mesmas funcionalidades fornecidas pela interface gráfica de usuário (GUI) do Rapid Recovery Console Core. Por exemplo, o módulo Rapid Recovery PowerShell pode montar pontos de recuperação do Rapid Recovery ou forçar um snapshot de uma máquina protegida.

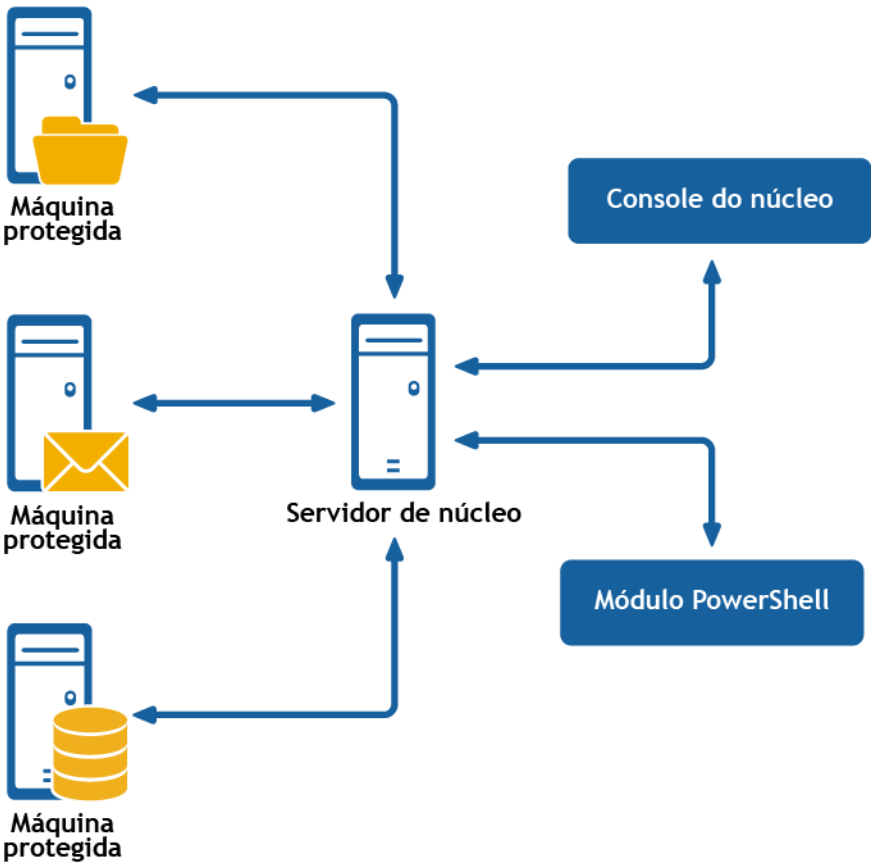


Figura 14. O módulo PowerShell interage com o Rapid RecoveryCore

O PowerShell é um ambiente conectado ao Microsoft .NET Framework projetado visando a automação administrativa. Esta seção descreve o módulo Rapid Recovery PowerShell e os cmdlets que os administradores podem usar para mapear certas funções sem a interação com a interface gráfica de usuário (GUI) do Rapid Recovery Core.

NOTA: Você também pode executar scripts PowerShell como pré-scripts e pós-scripts. Para obter mais informações e exemplos de scripts, consulte Prolongamento dos trabalhos do Rapid Recovery usando scripts.

Tópicos:

- Pré-requisitos para usar o PowerShell
- Trabalhar com comandos e cmdlets
- Cmdlets do módulo PowerShell do Rapid Recovery
- Localização
- Qualificadores

Pré-requisitos para usar o PowerShell

Para usar o módulo PowerShell do Rapid Recovery, é preciso instalar o Windows PowerShell 2.0 ou posterior. Devido a novos recursos introduzidos no PowerShell 3.0, incluindo acesso mais fácil a propriedades de objeto, acesso a PowerShell Web e suporte a chamadas REST, a Dell recomenda usar o PowerShell 3.0 ou posterior.

NOTA: Certifique-se de colocar o arquivo powershell.exe.config no diretório base do PowerShell. Por exemplo, C:\WindowsPowerShell\powershell.exe.config

powershell.exe.config

```
<?xml version="1.0"?>
<configuration>
    <startup useLegacyV2RuntimeActivationPolicy="true">
        <supportedRuntime version="v4.0.30319"/>
        <supportedRuntime version="v2.0.50727"/>
    </startup>
</configuration>
```

Iniciar o PowerShell e importar o módulo

Diferentemente dos módulos de outros sistemas, o módulo Rapid Recovery PowerShell não é carregado por padrão. Em cada sessão, você pode abrir o Windows PowerShell com privilégios administrativos e importar o módulo. Siga as instruções descritas neste procedimento para iniciar o PowerShell e importar o módulo Rapid Recovery PowerShell.

1 Abra um prompt de comando elevado do Windows PowerShell. Por exemplo, digite Windows PowerShell no menu Iniciar e, no aplicativo Windows PowerShell resultante, clique com o botão direito e selecione **Executar como administrador**.

O Windows PowerShell é aberto em uma nova janela de comando.

2 Digite o seguinte comando e pressione Enter:

```
Import-Module "RapidRecoveryPowerShellModule"
```

O módulo Rapid Recovery PowerShell é importado para sua sessão atual. Você pode começar a executar cmdlets na janela de comando atual.

Trabalhar com comandos e cmdlets

Cmdlets são comandos especializados em um script Windows PowerShell que realizam uma única função. Um cmdlet geralmente é representado por um par verbo-substantivo. O resultado retornado por um cmdlet é um objeto.

Você pode usar pipelines com comandos PowerShell, o que permite que a saída de um cmdlet seja usada como entrada de outro cmdlet. Um exemplo simples é solicitar a lista de comandos no módulo Rapid Recovery PowerShell e classificar a lista por nome. O script de exemplo para isso seria:

```
Get-Command -module rapidrecoverypowershellmodule | sort-object name
```

Obter ajuda e exemplos de cmdlet

Depois de abrir o PowerShell e importar o módulo Rapid Recovery PowerShell, você pode solicitar mais informações a qualquer momento usando o cmdlet Get-Help <command_name>. Por exemplo, para obter informações sobre o cmdlet de exportação de máquina virtual, digite o cmdlet a seguir e pressione Enter:

```
Get-Help Start-VMExport
```

O objeto retornado inclui o nome do comando, a sinopse, a sintaxe e as opções que podem ser usadas.

Outro método para obter ajuda sobre um cmdlet específico é digitar o nome do comando seguido de`-?`. Por exemplo:

```
Start-VMExport -?
```

Para solicitar exemplos de um cmdlet, execute o comando a seguir:

```
>Get-Help Start-VMExport -examples
```

Cmdlets do módulo PowerShell do Rapid Recovery

Esta seção descreve os cmdlets e as opções disponíveis no módulo PowerShell do Rapid Recovery. Todos os cmdlets no Módulo PowerShell do Rapid Recoverysuportam os seguintes parâmetros comuns:

- Verbose
- Debug
- ErrorAction
- ErrorVariable
- WarningAction
- WarningVariable
- OutBuffer
- OutVariable

Para obter mais informações, utilize`Get-Help about_commonparameters`.

Os cmdlets disponíveis são listados na tabela a seguir.

Tabela 227. Cmdlets no Módulo PowerShell Rapid Recovery

Nome do cmdlet	Descrição
Edit-Esxi VirtualStandby	Editar uma configuração existente standby virtual ESXi.
Edit-Hyper VVirtualStandby	Editar uma configuração existente standby virtual Hyper-V.
Editar-VBVirtualStandby	Editar uma configuração existente standby virtual VirtualBox.
Editar-VMVirtualStandby	Editar uma configuração existente standby virtual da Área de trabalho do VMWare.
Edit-ScheduledArchive	Editar uma configuração existente do arquivamento programado.

Nome do cmdlet	Descrição
Get-ActiveJobs	Recuperar uma coleção de trabalhos ativos.
Get-CloudAccounts	Obter informações sobre as contas de nuvem salvas no Core.
Get-Clusters	Recuperar uma coleção de clusters protegidos.
Get-CompletedJobs	Recuperar uma coleção de trabalhos concluídos.
Get-ExchangeMailStores	Recuperar uma coleção de armazenamentos de e-mail do Exchange.
Get-Failed	Obter informações sobre pontos de recuperação com falha.
Get-FailedJobs	Recuperar uma coleção de trabalhos com falha.
Get-Mounts	Exibir todos os pontos de recuperação montados.
Get-Passed	Obter informações sobre pontos de recuperação aprovados.
Get-ProtectedServers	Obter informações sobre servidores protegidos.
Get-ProtectionGroups	Recuperar uma coleção de grupos de proteção.
Get-QueuedJobs	Recuperar uma coleção de trabalhos aguardando na fila.
Get-RecoveryPoints	Obter informações sobre pontos de recuperação.
Get-ReplicatedServers	Obter informações sobre servidores replicados.
Get-Repositories	Obter informações sobre repositórios.
Get-ScheduledArchive	Obter informações sobre trabalhos de arquivo recorrente.
Get-SqlDatabases	Recuperar uma coleção de SQL databases.
Get-UnprotectedVolumes	Recuperar uma coleção de volumes não protegidos.
Get-VirtualizedServers	Obter informações sobre servidores virtualizados.
Get-Volumes	Obter informações sobre volumes.
New-Base	Forçar snapshot de imagem de base.
New-CloudAccount	Adicione uma nova conta de nuvem ao Core.
New-EncryptionKey	Criar uma nova chave de criptografia.
New-EsxiVirtualStandby	Criar uma nova máquina virtual de standby virtual ESXi.
New-HyperVVirtualStandby	Criar uma nova máquina virtual de standby virtual Hyper-V.
New-Mount	Montar pontos de recuperação.
New-Replication	Definir e forçar replicação.
New-Repository	Criar novo repositório DVM.
New-ScheduledArchive	Programar um novo arquivo recorrente.
New-Snapshot	Forçar snapshot.
New-VBVirtualStandby	Criar uma nova máquina virtual de standby virtual VirtualBox.
New-VMVirtualStandby	Criar uma nova máquina virtual de standby virtual da Área de trabalho do VMWare.
Push-Replication	Forçar replicação.

Nome do cmdlet	Descrição
Push-Rollup	Forçar rollup.
Remove-Agent	Remover uma máquina da proteção.
Remove-Mount	Desmontar pontos de recuperação.
Remove-Mounts	Desmontar todos os pontos de recuperação montados.
Remove-RecoveryPoints	Excluir pontos de recuperação para uma máquina protegida.
Remove-Repository	Apagar um repositório DVM existente.
Remove-ScheduledArchive	Descontinuar um arquivamento programado.
Remove-VirtualStandby	Remover uma máquina virtual de standby virtual do Core.
Resume-Replication	Retomar replicação.
Resume-RepositoryActivity	Retomar a atividade do repositório.
Resume-ScheduledArchive	Retomar um arquivamento programado.
Resume-Snapshot	Retomar snapshot.
Resume-VirtualStandby	Retomar dados de exportação para uma máquina virtual de standby virtual.
Start-Archive	Arquivar pontos de recuperação.
Start-AttachabilityCheck	Forçar verificação de capacidade de anexação em SQL databases de MS protegidos.
Start-ChecksumCheck	Forçar verificação de soma de verificação para armazenamentos de e-mail do Exchange.
Start-EsxiExport	Forçar exportação para um servidor ESXi.
Start-HypervExport	Forçar exportação para um servidor Hyper-V.
Start-LogTruncation	Forçar truncamento de log.
Start-MountabilityCheck	Forçar verificação de capacidade de montagem para armazenamentos de e-mail do Exchange protegidos.
Start-Protect	Colocar um servidor sob proteção.
Start-ProtectCluster	Colocar um cluster sob proteção.
Start-RepositoryCheck	Forçar uma verificação do repositório DVM.
Start-RestoreArchive	Restaurar arquivo com pontos de recuperação.
Start-ScheduledArchive	Forçar a transferência de dados para um arquivamento programado.
Start-VBExport	Forçar exportação para um servidor VirtualBox.
Start-VirtualStandby	Force a transferência de dados para uma máquina virtual existente de standby virtual.
Start-VMExport	Forçar exportação para um servidor da Área de trabalho do VMWare.
Stop-ActiveJobs	Cancelar trabalhos ativos.
Suspend-Replication	Pausar replicação.
Suspend-RepositoryActivity	Pausar atividade para um repositório.

Nome do cmdlet	Descrição
Suspend-ScheduledArchive	Pausar as transferências de dados para um arquivamento programado.
Suspend-Snapshot	Pausar snapshot.
Suspend-VirtualStandby	Pausar transferências de dados para uma máquina virtual de standby virtual.
Update-Repository	Adicionar extensão ao repositório DVM.

Edit-EsxiVirtualStandby

O comando`Edit-EsxiVirtualStandby` permite utilizar o PowerShell para fazer alterações em uma exportação virtual existente para uma máquina virtual ESXi (VM).

Forma de uso

A forma de uso do comando é a seguinte:

```
Edit-EsxiVirtualStandby [-HostName <String>] [-HostPort <String>] [-HostUserName <String>] [-
HostPassword <String>] [-DiskProvisioning <String>] [-DiskMapping <String>] [-ProtectedServer
<String>] [-Volumes <String[]>] [-VMName <String>] [-UseSourceRam] [-Ram <String>] [-User
<String>] [-Core <String>] [-Password <String>] [-Verbose] [-Debug] [-
ErroAction<ActionPreference>] [-WarningAction<ActionPreference>] [-ErrorVariable String>] [-
WarningVariable <String> [-OutVariable <String>] [-OutBuffer <Int32>]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Edit-EsxiVirtualStandby`:

Tabela 228. Opções do comando Edit-EsxiVirtualStandby

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.
`-all`	Mostrar todos os trabalhos, incluindo aqueles realizados pelo Core e todos os servidores protegidos.
`-number`	Opcional. Determinar quantos registros são exibidos. os valores disponíveis são:

Opção	Descrição
	all (exibir todos os trabalhos); l[number] ou [number] (recupera os XX trabalhos mais recentes classificados por execução e hora); f[number] (exibe os XX primeiros trabalhos de recuperação classificados por execução e hora). Por padrão, os 20 trabalhos mais recentes são exibidos.
`-jobtype`	Opcional. Especifica o filtro do tipo de tarefa. Os valores disponíveis são:`'transfer'` (transferência de dados),`'repository'` (manutenção de repositório),`'replication'` (replicações locais e remotas),`'backup'` (backup e recuperação),`'bootcdbuilder'` (criar CDs de inicialização),`'diagnostics'` (carregar logs),`'exchange'` (verificação de aruqivos do Exchange Server),`'export'` (exportação de pnto de recuperação),`'pushinstall'` (agentes de implementação),`'rollback'` (restauração a partir de um ponto de recuperação),`'rollup'` (rollups de ponto de recuperação),`'sqlattach'` (verificações de de agente) e`'mount'` (mount repository). Como padrão, todas as tarefas do tipo especificado são retornadas.
`-time`	Opcional. Filtrar a saída por data e hora do trabalho iniciado. Os tipos disponíveis de entrada incluem: #d ou DD (em que # é um número relativo ao período de tempo em dias até agora) #h ou #H (em que # é um número relativo ao período de tempo em horas antes até agora) "time date 1", "time date 2" (para exibir um intervalo personalizado de tempo, de uma data específica antes da vírgula até uma data específica após a vírgula).

Exemplo:

Listar todas as tarefas ativas no Core local:

```
>Get-activejobs -all
```

Edit-HyperVVirtualStandby

O comando `Edit-HyperVVirtualStandby` permite usar o PowerShell para alterar uma exportação virtual existente para uma máquina virtual (VM) Hyper-V.

Forma de uso

A forma de uso do comando é a seguinte:

```
Edit-HyperVVirtualStandby [-HostName <String>] [-HostPort <String>] [-HostUserName <String>] [-
HostPassword <String>] [-VMLocation <String>] [-UseLocalMachine] [-gen2] [-UseVhdx] [-
ProtectedServer <String>] [-Volumes <String[]>] [-VMName <String>] [-UseSourceRam] [-Ram
<String>] [-User <String>] [-Core <String>] [-Password <String>] [-Verbose] [-Debug] [-
ErrorAction <ActionPreference>] [-WarningAction <ActionPreference>] [-ErrorVariable <String>] [-
WarningVariable <String>] [-OutVariable <String>] [-OutBuffer <Int32>]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Edit-HyperVVirtualStandby`:

Tabela 229. Opções do comando Edit-HyperVVirtualStandby

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.
`-all`	Mostrar todos os trabalhos, incluindo aqueles realizados pelo Core e todos os servidores protegidos.
`-number`	Opcional. Determine quantos registros serão exibidos. os valores disponíveis são: all (exibir todos os trabalhos); l[number] ou [number] (recupera os XX trabalhos mais recentes classificados por execução e hora); f[number] (exibe os XX primeiros trabalhos de recuperação classificados por execução e hora). Por padrão, os 20 trabalhos mais recentes são exibidos.
`-jobtype`	Opcional. Especifica o filtro do tipo de tarefa. Os valores disponíveis são: `'transfer'` (transferência de dados), `'repository'` (manutenção do repositório), `'replication'` (replicações locais e remotas), `'backup'` (backup e restauração), `'bootcdbuilder'` (criar CDs de inicialização), `'diagnostics'` (carregar logs), `'exchange'` (verificação de arquivos do Exchange Server), `'export'` (exportação do ponto de recuperação), `'pushinstall'` (agentes de implantação), `'rollback'` (restaurar de um ponto de recuperação), `'rollup'` (rollups de ponto de recuperação), `'sqlattach'` (verificações de capacidade de anexação de agente) e `'mount'` (montar repositório). Como padrão, todas as tarefas do tipo especificado são retornadas.
`-time`	Opcional. Filtrar a saída por data e hora do trabalho iniciado. Os tipos disponíveis de entrada incluem: #d ou DD (em que # é um número relativo ao período de tempo em dias até agora) #h ou #H (em que # é um número relativo ao período de tempo em horas antes até agora) "time date 1", "time date 2" (para exibir um intervalo personalizado de tempo, de uma data específica antes da vírgula até uma data específica após a vírgula).

Exemplo:

Listar todas as tarefas ativas no Core local:

```
>Get-activejobs -all
```

Edit-ScheduledArchive

O comando `Edit-ScheduledArchive` permite usar o PowerShell para alterar um arquivamento programado existente.

Forma de uso

A forma de uso do comando é a seguinte:

```
Edit-ScheduledArchive -core [host name] -user [login] -password [password] -all | -
protectedserver [name | IP address | "[name1 | IP address1]" "[name2 | IP address2]"] -path
[location] -cloudaccountname [name] -cloudcontainer [name] -recycleaction [type] -scheduletype
[type] -dayofweek [name] -dayofmonth [number] -time [time] -initialpause -id [id]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Edit-ScheduledArchive`:

Tabela 230. Opções do comando Edit-ScheduledArchive

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	A máquina protegida com pontos de recuperação que você deseja arquivar. Você pode especificar vários nomes de máquinas entre aspas duplas e separados por vírgulas.
`-all`	Arquive os pontos de recuperação para todas as máquinas protegidas.
`-path`	O caminho para salvar os dados arquivados. Por exemplo: • Máquina local: "d:\work\archive" • Caminho da rede: "\\servername\sharename" • Pasta em uma conta de nuvem: "Nome da pasta" **NOTA: O número de símbolos não deve ser maior que 100 para locais e locais de rede nem maior que 150 para um local de nuvem.**
`-cloudaccountname`	Opcional. Use somente para arquivo na nuvem. O nome da conta de nuvem em que você deseja salvar o arquivamento.
`-cloudcontainer`	Opcional. Use somente para arquivo na nuvem. O nome do contêiner da nuvem, na conta de nuvem escolhida, onde o arquivo será salvo. Quando você usar essa opção, também deve especificar o parâmetro "-cloudaccountname".
`-recycleaction`	O tipo de ação de reciclagem. Especificado usando um dos quatro valores a seguir: • "replacethiscore" - Substitui qualquer dado arquivado pré-existente pertencente a esse Core, mas deixa os dados de outros Cores intactos.

Opção	Descrição
	• "erasecompletely" - Limpa todos os dados arquivados do diretório antes de gravar o novo arquivo. • "incremental" - Permite adicionar pontos de recuperação a um arquivo existente. Compara pontos de recuperação para evitar duplicação de dados que já existem no arquivo.
`-scheduletype`	Tipo de intervalo do programa. Opção especificada com um dos quatro valores a seguir: • "diário" - Para um arquivo criado automaticamente, diariamente. • "semanalmente" - Para um arquivo criado automaticamente, semanalmente. Especifique o parâmetro "-dayofweek". • "mensalmente" - Para um arquivo criado automaticamente, mensalmente. Especifique o parâmetro "-dayofmonth". Se um mês não tiver o dia especificado – por exemplo, "31" – o arquivamento não ocorrerá para esse mês. • "lastdayofmonth" - Para criar um arquivo automaticamente no último dia de cada mês.
`-dayofweek`	Use somente para a opção "semanalmente" do parâmetro "-scheduletype". O dia da semana no qual deseja criar automaticamente o arquivo (por exemplo, "Segunda-feira").
`-dayofmonth`	Use somente para a opção "mensalmente" do parâmetro "-scheduletype". O dia (número) do mês no qual deseja criar automaticamente o arquivo (por exemplo, "15").
`-time`	A hora do dia em que você deseja criar um arquivo.
`-initialpause`	Opcional. Especifique essa opção se deseja pausar o arquivo inicialmente depois de configurar o programa de arquivo
`-id`	O identificador do arquivamento programado que você deseja editar.

Exemplo:

Edite um arquivamento programado no Core local:

```
>Edit-ScheduledArchive -protectedserver protectedserver1 -path d:\work\archive -
cloudaccountname cloud1 -cloudcontainer cloudarchives -recycleaction incremental -scheduletype
daily -time 12:00 AM -initialpause -i
    d archiveid
```

Edit-VBVirtualStandby

O comando `Edit-VBVirtualStandby` permite usar o PowerShell para alterar uma exportação virtual existente para uma máquina virtual (VM) VirtualBox.

Forma de uso

A forma de uso do comando é a seguinte:

```
Edit-VBVirtualStandby [-TargetPath <String>] [-PathUserName <String>] [-PathPassword <String>]
[-LinuxHostName <String>] [-HostPort <UInt32>] [-AccountUserName <String>] [-AccountPassword
<String>] [-ProtectedServer <String>] [-Volumes <String[]>] [-VMName <String>] [-UseSourceRam]
[-Ram <String>] [-User <String>] [-Core <String>] [-Password <String>] [-Verbose] [-Debug] [-
ErrorAction <ActionPreference>] [-WarningAction <ActionPreference>] [-ErrorVariable <String>] [-
WarningVariable <String>] [-OutVariable <String>] [-OutBuffer <Int32>]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Edit-VBVirtualStandby`:

Tabela 231. Opções do comando Edit-VBVirtualStandby

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.
`-all`	Mostrar todos os trabalhos, incluindo aqueles realizados pelo Core e todos os servidores protegidos.
`-number`	Opcional. Determine quantos registros serão exibidos. os valores disponíveis são: all (exibir todos os trabalhos); l[number] ou [number] (recupera os XX trabalhos mais recentes classificados por execução e hora); f[number] (exibe os XX primeiros trabalhos de recuperação classificados por execução e hora). Por padrão, os 20 trabalhos mais recentes são exibidos.
`-jobtype`	Opcional. Especifica o filtro do tipo de tarefa. Os valores disponíveis são: `'transfer'` (transferência de dados), `'repository'` (manutenção do repositório), `'replication'` (replicações locais e remotas), `'backup'` (backup e restauração), `'bootcdbuilder'` (criar CDs de inicialização), `'diagnostics'` (carregar logs), `'exchange'` (verificação de arquivos do Exchange Server), `'export'` (exportação do ponto de recuperação), `'pushinstall'` (agentes de implantação), `'rollback'` (restaurar de um ponto de recuperação), `'rollup'` (rollups de ponto de recuperação), `'sqlattach'` (verificações de capacidade de anexação de agente) e `'mount'` (montar repositório). Como padrão, todas as tarefas do tipo especificado são retornadas.
`-time`	Opcional. Filtrar a saída por data e hora do trabalho iniciado. Os tipos disponíveis de entrada incluem: #d ou DD (em que # é um número relativo ao período de tempo em dias até agora) #h ou #H (em que # é um número relativo ao período de tempo em horas antes até agora) "time date 1", "time date 2" (para exibir um intervalo personalizado de tempo, de uma data específica antes da vírgula até uma data específica após a vírgula).

Exemplo:

Listar todas as tarefas ativas no Core local:

```
>Get-activejobs -all
```

Edit-VMVirtualStandby

O comando `Edit-VMVirtualStandby` permite usar o PowerShell para alterar uma exportação virtual existente para uma máquina virtual (VM) VMware Workstation.

Forma de uso

A forma de uso do comando é a seguinte:

```
 Edit-VMVirtualStandby [-TargetPath <String>] [-PathUserName <String>] [-PathPassword <String>]
[-ProtectedServer <S
    tring>] [-Volumes <String[]>] [-VMName <String>] [-UseSourceRam] [-Ram <String>] [-User
<String>] [-Core <String>]
    [-Password <String>] [-Verbose] [-Debug] [-ErrorAction <ActionPreference>] [-WarningAction
<ActionPreference>] [-Er
    rorVariable <String>] [-WarningVariable <String>] [-OutVariable <String>] [-OutBuffer
<Int32>]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Edit-VMVirtualStandby`:

Tabela 232. Opções do comando Edit-VMVirtualStandby

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.
`-all`	Mostrar todos os trabalhos, incluindo aqueles realizados pelo Core e todos os servidores protegidos.
`-number`	Opcional. Determine quantos registros serão exibidos. os valores disponíveis são: all (exibir todos os trabalhos); l[number] ou [number] (recupera os XX trabalhos mais recentes classificados por execução e hora); f[number] (exibe os XX primeiros trabalhos de recuperação classificados por execução e hora). Por padrão, os 20 trabalhos mais recentes são exibidos.
`-jobtype`	Opcional. Especifica o filtro do tipo de tarefa. Os valores disponíveis são: `'transfer'` (transferência de dados), `'repository'` (manutenção do repositório), `'replication'` (replicações locais e remotas), `'backup'` (backup e restauração), `'bootcdbuilder'` (criar CDs de inicialização), `'diagnostics'` (carregar logs), `'exchange'` (verificação de arquivos do Exchange Server), `'export'` (exportação do ponto de recuperação),

Opção	Descrição
	'pushinstall' (agentes de implantação), 'rollback' (restaurar de um ponto de recuperação), 'rollup' (rollups de ponto de recuperação), 'sqlattach' (verificações de capacidade de anexação de agente) e 'mount' (montar repositório). Como padrão, todas as tarefas do tipo especificado são retornadas.
-time	Opcional. Filtrar a saída por data e hora do trabalho iniciado. Os tipos disponíveis de entrada incluem: #d ou DD (em que # é um número relativo ao período de tempo em dias até agora) #h ou #H (em que # é um número relativo ao período de tempo em horas antes até agora) "time date 1", "time date 2" (para exibir um intervalo personalizado de tempo, de uma data específica antes da vírgula até uma data específica após a vírgula).

Exemplo:

Listar todas as tarefas ativas no Core local:

```
>Get-activejobs –all
```

Get-ActiveJobs

O comandoGet-ActiveJobs retorna todos os trabalhos ativos do Core. O parâmetro-jobtype pode ser usado para observar tarefas específicas.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-ActiveJobs -core [host name] -user [user name] -password [password] -all |
-protectedserver [server name or IP address] -number [all | f[number] |l[number] | number] -
jobtype [type] -time [time]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comandoGet-ActiveJobs :

Tabela 233. Opções do comando Get-ActiveJobs

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon.

Opção	Descrição
	Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.
`-all`	Mostrar todos os trabalhos, incluindo aqueles realizados pelo Core e todos os servidores protegidos.
`-number`	Opcional. Determinar quantos registros serão exibidos. os valores disponíveis são: all (exibir todos os trabalhos); l[number] ou [number] (recupera os XX trabalhos mais recentes classificados por execução e hora); f[number] (exibe os XX primeiros trabalhos de recuperação classificados por execução e hora). Por padrão, os 20 trabalhos mais recentes são exibidos.
`-jobtype`	Opcional. Especifica o filtro do tipo de tarefa. Os valores disponíveis são: `'transfer'` (transferência de dados), `'repository'` (manutenção do repositório), `'replication'` (replicações locais e remotas), `'backup'` (cópia de segurança e restauração), `'bootcdbuilder'` (criar CDs de inicialização), `'diagnostics'` (carregar logs), `'exchange'` (verificação de arquivos do Exchange Server), `'export'` (exportação de pontos de recuperação), `'pushinstall'` (implantar agentes), `'rollback'` (restaurar de um ponto de recuperação), `'rollup'` (rollups de ponto de recuperação), `'sqlattach'` (verificações de capacidade de anexação de agente) e `'mount'` (montar repositório). Como padrão, todas as tarefas do tipo especificado são retornadas.
`-time`	Opcional. Filtrar a saída por data e hora do trabalho iniciado. Os tipos disponíveis de entrada incluem: #d ou DD (em que # é um número relativo ao período de tempo em dias até agora) #h ou #H (em que # é um número relativo ao período de tempo em horas antes até agora) "time date 1", "time date 2" (para exibir um intervalo personalizado de tempo, de uma data específica antes da vírgula até uma data específica após a vírgula).

Exemplo:

Listar todas as tarefas ativas no Core local:

```
>Get-activejobs -all
```

Get-Clusters

O comando `Get-Clusters` retorna informações sobre os clusters do servidor protegidos no Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-Clusters -core [host name] -user [user name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Get-Clusters`:

Tabela 234. Opções do comando Get-Clusters

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Mostrar uma lista de clusters do servidor protegidos no Core local:

```
>Get-Clusters
```

Get-CompletedJobs

O comando`Get-CompletedJobs` retorna uma lista de trabalhos concluídos no Core. O parâmetro`-jobtype` pode ser usado para observar tarefas específicas.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-CompletedJobs -core [host name] -user [user name] -password [password] -all |
-protectedserver [server name or IP address] -number [all | f[number] |l[number] | number] -
jobtype [type] -time [time]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Get-CompletedJobs`:

Tabela 235. Opções do comando Get-CompletedJobs

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha.

Opção	Descrição
	Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.
`-all`	Mostrar todos os trabalhos, incluindo aqueles realizados pelo Core e todos os servidores protegidos.
`-number`	Opcional. Determinar quantos registros serão exibidos. os valores disponíveis são: all (exibir todos os trabalhos); l[number] ou [number] (recupera os XX trabalhos mais recentes classificados por execução e hora); f[number] (exibe os XX primeiros trabalhos de recuperação classificados por execução e hora). Por padrão, os 20 trabalhos mais recentes são exibidos.
`-jobtype`	Opcional. Especifica o filtro do tipo de tarefa. Os valores disponíveis são: `'transfer'` (transferência de dados), `'repository'` (manutenção do repositório), `'replication'` (replicações locais e remotas), `'backup'` (cópia de segurança e restauração), `'bootcdbuilder'` (criar CDs de inicialização), `'diagnostics'` (carregar logs), `'exchange'` (verificação de arquivos do Exchange Server), `'export'` (exportação de pontos de recuperação), `'pushinstall'` (implantar agentes), `'rollback'` (restaurar de um ponto de recuperação), `'rollup'` (rollups de ponto de recuperação), `'sqlattach'` (verificações de capacidade de anexação de agente) e `'mount'` (montar repositório). Como padrão, todas as tarefas do tipo especificado são retornadas.
`-time`	Opcional. Filtrar a saída por data e hora do trabalho iniciado. Os tipos disponíveis de entrada incluem: #d ou DD (em que # é um número relativo ao período de tempo em dias até agora) #h ou #H (em que # é um número relativo ao período de tempo em horas antes até agora) "time date 1", "time date 2" (para exibir um intervalo personalizado de tempo, de uma data específica antes da vírgula até uma data específica após a vírgula).

Exemplo:

Listar todas as tarefas ativas no Core local:

```
>Get-CompletedJobs -all
```

Listar todas as tarefas de criação de repositório concluídas no Core local:

```
>Get-CompletedJobs -jobtype repository
```

Get-ExchangeMailStores

O comando`Get-ExchangeMailStores` retorna informações sobre armazenamentos de e-mail em Exchange servers protegidos pelo Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-ExchangeMailStores -core [host name] -user [user name] -password [password]
-protectedserver [server name or IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Get-ExchangeMailStores`:

Tabela 236. Opções do comando Get-ExchangeMailStores

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.

Exemplo:

Mostra a lista de armazenamentos de e-mail do servidor Exchange do Core local:

```
>Get-ExchangeMailStores -protectedserver 10.10.10.10
```

Get-Failed

O comando`Get-Failed` retorna informações sobre pontos de recuperação com falha no Core local.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-Failed -core [host name] -user [user name] -password [password] -all |
-protectedserver [server name or IP address] -number [all | f[number] |l[number] | number]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Get-Failed` :

Tabela 237. Opções do comando Get-Failed

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.
`-number`	Opcional. Determinar quantos registros serão exibidos. Os valores disponíveis são: all (exibir todos os trabalhos); l[number] ou [number] (recupera os XX trabalhos mais recentes classificados por execução e hora); f[number] (exibe os XX primeiros trabalhos de recuperação classificados por execução e hora). Por padrão, os 20 trabalhos mais recentes são exibidos.

Exemplo:

Mostra uma lista de todos os pontos de recuperação com falha:

```
>Get-failed -protectedserver 10.10.10.10
```

Get-FailedJobs

O comando`Get-FailedJobs` retorna todos os trabalhos com falha do Core local.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-FailedJobs -core [host name] -user [user name] -password [password] -all |
-protectedserver [server name or IP address] -number [all | f[number] |l[number] | number] -
jobtype [type] -time [time]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Get-FailedJobs`:

Tabela 238. Opções do comando Get-FailedJobs

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.
`-all`	Mostrar todos os trabalhos, incluindo aqueles realizados pelo Core e todos os servidores protegidos.
`-number`	Opcional. Determinar quantos registros serão exibidos. Os valores disponíveis são: all (exibir todos os trabalhos); l[number] ou [number] (recupera os XX trabalhos mais recentes classificados por execução e hora); f[number] (exibe os XX primeiros trabalhos de recuperação classificados por execução e hora). Por padrão, os 20 trabalhos mais recentes são exibidos.
`-jobtype`	Opcional. Especifica o filtro do tipo de tarefa. Os valores disponíveis são: `'transfer'` (transferência de dados), `'repository'` (manutenção do repositório), `'replication'` (replicações locais e remotas), `'backup'` (cópia de segurança e restauração), `'bootcdbuilder'` (criar CDs de inicialização), `'diagnostics'` (carregar logs), `'exchange'` (verificação de arquivos do Exchange Server), `'export'` (exportação de pontos de recuperação), `'pushinstall'` (implantar agentes), `'rollback'` (restaurar de um ponto de recuperação), `'rollup'` (rollups de ponto de recuperação), `'sqlattach'` (verificações de capacidade de anexação de agente) e `'mount'` (montar repositório). Como padrão, todas as tarefas do tipo especificado são retornadas.
`-time`	Opcional. Filtrar a saída por data e hora do trabalho iniciado. Os tipos disponíveis de entrada incluem: #d ou DD (em que # é um número relativo ao período de tempo em dias até agora) #h ou #H (em que # é um número relativo ao período de tempo em horas antes até agora) "time date 1", "time date 2" (para exibir um intervalo personalizado de tempo, de uma data específica antes da vírgula até uma data específica após a vírgula).

Exemplo:

Mostra uma lista de todos os trabalhos com falha no Core local:

```
>Get-FailedJobs -all
```

Listar todas as tarefas de criação de cópia de segurança que falharam no local Core:

```
>Get-FailedJobs -type backup
```

Get-Mounts

O comando`Get-Mounts` retorna todos os pontos de recuperação montados no Core local.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-Mounts -core [host name] -user [user name] -password [password] -protectedserver [server name or IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Get-Mounts` :

Tabela 239. Opções do comando Get-Mounts

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.

Exemplo:

Exibir todos os pontos de recuperação montados:

```
>Get-Mounts -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22
```

Get-Passed

O comando`Get-Passed` retorna informações sobre pontos de recuperação que foram aprovados em verificações no Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-Passed -core [host name] -user [user name] -password [password] -protectedserver [server name or IP address] -number [all | f[number] |l[number] | number]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Get-Passed` :

Tabela 240. Opções do comando Get-Passed

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Lista todos os pontos de recuperação no Core local que foram aprovados em verificações:

```
>Get-Passed -protectedserver 10.10.10.10
```

Get-ProtectedServers

O comando`Get-ProtectedServers` retorna informações sobre máquinas protegidas no Core local.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-ProtectedServers -core [host name] -user [user name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Get-ProtectedServers` :

Tabela 241. Opções do comando Get-ProtectedServers

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Lista todas as máquinas protegidas atualmente no Core local:

```
>Get-ProtectedServers
```

Get-ProtectionGroups

O comando`Get-ProtectionGroups` retorna informações sobre grupos de proteção no Core local.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-ProtectionGroups -core [host name] -user [user name] -password [password] -all |
-protectedserver [server name or IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Get-ProtectionGroups`:

Tabela 242. Opções do comando Get-ProtectionGroups

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Opção	Descrição
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-protectedserver	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.

Exemplo:

Lista grupos de proteção no Core local:

```
>Get-ProtectionGroups -protectedserver 10.10.10.10
```

Get-QueuedJobs

O comando `Get-QueuedJobs` retorna todos os trabalhos aguardando para iniciar no Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-QueuedJobs -core [host name] -user [login] -password [password] -all | -protectedserver
[name | IP address] -nu
    mber [all | f[number] | l[number] | number] -jobtype [type] -time [time]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Get-ActiveJobs`:

Tabela 243. Opções do comando Get-ActiveJobs

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-protectedserver	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.
-all	Mostrar todos os trabalhos, incluindo aqueles realizados pelo Core e todos os servidores protegidos.

Opção	Descrição
`-number`	Opcional. Determine quantos registros serão exibidos. os valores disponíveis são: all (exibir todos os trabalhos); l[number] ou [number] (recupera os XX trabalhos mais recentes classificados por execução e hora); f[number] (exibe os XX primeiros trabalhos de recuperação classificados por execução e hora). Por padrão, os 20 trabalhos mais recentes são exibidos.
`-jobtype`	Opcional. Especifica o filtro do tipo de tarefa. Os valores disponíveis são: `'transfer'` (transferência de dados), `'repository'` (manutenção do repositório), `'replication'` (replicações locais e remotas), `'backup'` (backup e restauração), `'bootcdbuilder'` (criar CDs de inicialização), `'diagnostics'` (carregar logs), `'exchange'` (verificação de arquivos do Exchange Server), `'export'` (exportação do ponto de recuperação), `'pushinstall'` (agentes de implantação), `'rollback'` (restaurar de um ponto de recuperação), `'rollup'` (rollups de ponto de recuperação), `'sqlattach'` (verificações de capacidade de anexação de agente) e `'mount'` (montar repositório). Como padrão, todas as tarefas do tipo especificado são retornadas.
`-time`	Opcional. Filtrar a saída por data e hora do trabalho iniciado. Os tipos disponíveis de entrada incluem: #d ou DD (em que # é um número relativo ao período de tempo em dias até agora) #h ou #H (em que # é um número relativo ao período de tempo em horas antes até agora) "time date 1", "time date 2" (para exibir um intervalo personalizado de tempo, de uma data específica antes da vírgula até uma data específica após a vírgula).

Exemplo:

Lista todos os trabalhos em fila no Core local:

```
>Get-QueuedJobs -all
```

Get-RecoveryPoints

O comando`Get-RecoveryPoints` retorna informações sobre pontos de recuperação de máquinas protegidas no Core local.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-RecoveryPoints -core [host name] -user [user name] -password [password]
-protectedserver [server name or IP address] -number [all | f[number] |l[number] | number]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Get-RecoveryPoints`:

Tabela 244. Opções do comando Get-RecoveryPoints

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.

Opção	Descrição
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.
`-number`	Opcional. Determinar quantos registros serão exibidos. Os valores disponíveis são: all (exibir todos os trabalhos); l[number] ou [number] (recupera os XX trabalhos mais recentes classificados por execução e hora); f[number] (exibe os XX primeiros trabalhos de recuperação classificados por execução e hora). Por padrão, os 20 trabalhos mais recentes são exibidos.

Exemplo:

Lista pontos de recuperação de máquinas protegidas no Core local:

```
>Get-RecoveryPoints -protectedserver 10.10.10.10
```

Get-ReplicatedServers

O comando`Get-ReplicatedServers` retorna informações sobre máquinas replicadas no Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-ReplicatedServers -core [host name] -user [user name] -password [password]
```

A Dell recomenda que você considere a segurança quando usar comandos para retornar os valores. Por exemplo, este comando retorna a senha de administrador para cada servidor replicado. Se for usada em um ambiente MSP do Core de destino, isso pode potencialmente expor a senha de login do usuário administrador. Para ambientes com dados de repositório criptografados, isso não representa problemas substanciais de segurança.

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Get-ReplicatedServers`:

Tabela 245. Opções do comando Get-ReplicatedServers

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.

Opção	Descrição
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Lista todos os servidores replicados no Core local:

```
>Get-ReplicatedServers
```

Get-Repositories

O comando`Get-Repositories` retorna informações sobre repositórios no Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-Repositories -core [host name] -user [user name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Get-Repositories`:

Tabela 246. Opções do comando Get-Repositories

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Lista repositórios no Core local:

```
>Get-Repositories
```

Get-ScheduledArchives

O comando `Get-ScheduledArchives` permite usar o PowerShell para ver informações sobre os arquivos programados existentes do Rapid Recovery associados a este Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-ScheduledArchives -core [host name] -user [login] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Get-ScheduledArchives`:

Tabela 247. Opções do comando Get-ScheduledArchives

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Obtenha informações sobre os arquivos programados neste Core:

```
>Get-ScheduledArchives -core 10.10.10.10 -user administrator -password password
```

Get-SqlDatabases

O comando`Get-SqlDatabases` retorna uma lista de SQL databases da máquina protegida especificada.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-SqlDatabases -core [host name] -user [user name] -password [password]
-protectedserver [server name or IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Get-SqlDatabases`:

Tabela 248. Opções do comando Get-SqlDatabases

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.

Exemplo:

Lista todos os trabalhos de bancos de dados SQL no Core local:

```
>Get-SqlDatabases -protectedserver 10.10.10.10
```

Get-UnprotectedVolumes

O comando`Get-UnprotectedVolumes` retorna informações sobre volumes que estão disponíveis para proteção, mas não estão protegidos atualmente no Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-UnprotectedVolumes
-core [host name] -user [user name] -password [password] -protectedserver [server name or IP
address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Get-UnprotectedVolumes`:

Tabela 249. Opções do comando Get-UnprotectedVolumes

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.

Exemplo:

Lista todos os volumes disponíveis para proteção (mas que não estão protegidos) na máquina de agente especificada:

```
>Get-UnprotectedVolumes -protectedserver 10.10.10.10
```

Get-VirtualizedServers

O comando`Get-VirtualizedServers` retorna informações sobre servidores virtualizados.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-VirtualizedServers -core [host name] -user [user name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Get-VirtualizedServers` :

Tabela 250. Opções do comando Get-VirtualizedServers

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Lista todos os servidores virtualizados no Core local:

```
>Get-VirtualizedServers
```

Get-Volumes

O comando`Get-Volumes` retorna informações sobre volumes em uma máquina especificada que é protegida pelo Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
Get-Volumes -core [host name] -user [user name] -password [password]
-protectedserver [server name or IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Get-Volumes`:

Tabela 251. Opções do comando Get-Volumes

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Opção	Descrição
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-protectedserver	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.

Exemplo:

Lista todos os volumes na máquina especificada:

```
>Get-Volumes -protectedserver 10.10.10.10
```

New-Base

O comando`New-Base` força uma nova imagem de base resultando em uma transferência de dados da máquina atualmente protegida. Ao forçar uma imagem de base, a transferência iniciará imediatamente ou será adicionada à fila. Somente os dados que foram alterados em relação a um ponto de recuperação anterior serão transferidos. Caso não existir um ponto de recuperação anterior, todos os dados nos volumes protegidos serão transferidos.

Forma de uso

A forma de uso do comando é a seguinte:

```
New-Base [[-all] | -protectedserver [machine name]] -core [host name] -user [user name] -
password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`New-Base`:

Tabela 252. Opções do comando New-Base

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-all	Imagem de base para todos os agentes.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-protectedserver	Forçar para o nome da máquina protegida atual.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Forçar imagem de base para todas as máquinas protegidas:

```
>New-Base -all
```

New-CloudAccount

O comando`New-CloudAccount` permite adicionar uma nova conta de nuvem ao Rapid Recovery Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
New-CloudAccount -core [host name] -user [login] -password [password] -displayname [display
name] -type [cloud acco
    unt type] -username [user name] - key [secret key] -region [region] - tenantid [tenant Id] -
authurl [authorization
    url]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`New-CloudAccount`:

Tabela 253. Opções do comando New-CloudAccount

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-displayname`	O nome da conta de nuvem a ser exibida.
`-type`	O tipo de conta de nuvem que deseja adicionar. Os valores suportados incluem: • amazon • openstack • rackspace • windowsazure • "windows azure" • azure

Opção	Descrição
-username	O nome de usuário da conta de nuvem que você deseja adicionar. É utilizado no processo de autenticação. Essa propriedade é determinada como "Chave de acesso" para a nuvem Amazon™, “Nome de usuário” para Rackspace e OpenStack e “Nome da conta de armazenamento" para contas de nuvem do Windows Azure.
-key	A chave da conta de nuvem que deseja adicionar. É utilizado no processo de autenticação. Essa propriedade é determinada como "Chave secreta" para a nuvem Amazon™, "Chave de Api" para Rackspace e OpenStack e "Chave de acesso" para conta de nuvem do Windows Azure.
-region	A região da conta de nuvem que você deseja adicionar. Essa propriedade é necessária somente para contas de nuvem RackSpace e OpenStack.
-tenantid	O identificados que é utilizado no processo de autenticação de uma conta de nuvem OpenStack. Esta opção é necessária somente para a criação de conta da nuvem OpenStack.
-authurl	A URL que é utilizada no processo de autenticação de uma conta de nuvem OpenStack. Esta opção é necessária somente para a criação de conta da nuvem OpenStack.

Exemplo:

Crie uma nova conta de nuvem Amazon™ S3 com o nome "Conta Amazon S3” com a chave de acesso "akey" e a chave secreta "skey."

```
>New-CloudAccount -displayname "Amazon S3 Account" -type Amazon -username akey -key skey
```

New-EncryptionKey

O comando `New-EncryptionKey` permite criar uma nova chave de criptografia para proteger os seus dados com backup do Rapid Recovery .

Forma de uso

A forma de uso do comando é a seguinte:

```
New-EncryptionKey -core [host name] -user [login] -password [password] -name [encryption key
name] -passphrase [pas
    sphrase] -comment [comment]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `New-EncryptionKey`:

Tabela 254. Opções do comando New-EncryptionKey

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha.

Opção	Descrição
	Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-name`	O nome da chave de criptografia que você deseja criar.
`-passphrase`	A frase de acesso para a chave de criptografia que você deseja criar.
`-comment`	Opcional. A descrição da chave de criptografia.

Exemplo:

Crie uma chave de criptografia no Core local:

```
>New-EncryptionKey -name EncryptionKey1 -passphrase 123456
```

New-EsxiVirtualStandby

O comando PowerShell `New-EsxiVirtualStandby` permite criar uma nova máquina em standby virtual do ESXi usando o Rapid Recovery.

Forma de uso

A forma de uso do comando é a seguinte:

```
New-EsxiVirtualStandby -core [host name] -user [login] -password [password] -protectedserver
[name | IP address] -volumes [volumes names] -vmname [virtual machine name] -hostname [virtual
host name] -hostport [virtual host port number] -hostusername [virtual host login] -
hostpassword [virtual host password] [-ram [total megabytes] | -usesourceram] -diskprovisioning
[thin | thick] -diskmapping [automatic | manual | withvm] -initialexport
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `New-EsxiVirtualStandby`:

Tabela 255. Opções do comando New-EsxiVirtualStandby

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Opção	Descrição
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-protectedserver	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.
-volumes	Opcional. Liste os nomes de volume que deseja exportar. Se não for especificado, todos os volumes no(s) ponto(s) de recuperação serão exportados. Os valores devem ser informados entre aspas duplas e separados por um espaço; por exemplo, "c:", "d:". **NOTA: Não use barras nos nomes dos volumes.**
-vmname	O nome do Microsoft Windows da máquina virtual.
-hostname	O nome do host do servidor virtual.
-hostport	O número de porta a ser usado para a comunicação com o servidor virtual.
-hostusername	O nome de usuário para o login no host do servidor virtual.
-hostpassword	A senha para o login no host do servidor virtual.
-ram	Alocar uma quantidade específica de RAM no servidor virtual.
-usesourceram	Opcional. Aloque no servidor virtual a mesma quantidade de RAM que a máquina de origem protegida possui.
-diskprovisioning	Opcional. A quantidade de espaço em disco a ser alocada na máquina virtual. Valores disponíveis incluem: • Grosso – Especifique "grosso" para tornar o disco virtual tão grande quanto a unidade original no servidor protegido. • Fino – Especifique "fino" para alocar a quantidade de espaço em disco real ocupada na unidade original e alguns megabytes adicionais. O aprovisionamento de disco padrão é "fino".
-diskmappinjg	Opcional. Determina como mapear os discos do ponto de recuperação para a máquina virtual. Valores disponíveis incluem: • "automático" • "manual" • "withvm" A definição padrão é "automático".
-initialexport	Opcional. Especifique essa opção se precisar iniciar uma exportação de máquina virtual sob demanda depois de configurar o standby virtual.

Exemplo:

Crie um novo standby virtual do ESXi:

```
>New-EsxiVirtualStandby -protectedserver 10.10.10.4 -vmname ExportedMachine -hostname
10.10.10.127 -hostport 443 -hostusername root -hostpassword pass123 -usesourceram -
diskprovisioning thin -diskmapping auto
```

New-HyperVVirtualStandby

O comando PowerShell `New-HyperVVirtualStandby` permite criar uma nova máquina virtual (VM) Hyper-V usando o Rapid Recovery.

Forma de uso

A forma de uso do comando é a seguinte:

```
New-HyperVVirtualStandby -core [host name] -user [login] -password [password] -protectedserver
[name | IP address]
    -volumes [volumes names] -vmname [virtual machine name] [-gen2] -useVhdx [-uselocalmachine]
| -hostname [virtual ho
    st name] -hostport [virtual host port number] -hostusername [virtual host login] -
hostpassword [virtual host passwo
    rd]] -vmlocation [location] [-ram [total megabytes] | -usesourceram] -initialexport
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `New-HyperVVirtualStandby`:

Tabela 256. Opções do comando New-HyperVVirtualStandby

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.
`-volumes`	Opcional. Liste os nomes de volume que deseja exportar. Se não for especificado, todos os volumes no(s) ponto(s) de recuperação serão exportados. Os valores devem ser informados entre aspas duplas e separados por um espaço; por exemplo, "c:", "d:". **NOTA: Não use barras nos nomes dos volumes.**
`-vmname`	O nome do Microsoft Windows da máquina virtual.
`-gen2`	Opcional. Especifique para usar a segunda geração de VM. Se não for especificado, a geração 1 será usada. O Rapid Recovery suporta a geração 2 desde o Windows Server 2012 R2 até o Windows 8.1.
`-usevhdx`	Opcional. Se você especificar essa opção, o Rapid Recovery usará o formato do disco VHDX para criar a VM. Do contrário, ele usará o formato de disco VHD. A geração 2 usa somente o formato VHDX.

Opção	Descrição
-uselocalmachine	Opcional. Conectar ao server Hyper-V local. Quando você especifica esse valor, o Rapid Recovery ignora as seguintes opções: • hostname • hostport • hostusername • hostpassword
-hostname	O nome do host do servidor virtual.
-hostport	O número de porta a ser usado para a comunicação com o servidor virtual.
-hostusername	O nome de usuário para o login no host do servidor virtual.
-hostpassword	A senha para o login no host do servidor virtual.
-vmlocation	Caminho local ou de rede para a pasta em que você quer armazenar os arquivos da máquina virtual.
-ram	Alocar uma quantidade específica de RAM no servidor virtual.
-usesourceram	Opcional. Aloque no servidor virtual a mesma quantidade de RAM que a máquina de origem protegida possui.
-initialexport	Opcional. Especifique essa opção se precisar iniciar uma exportação de máquina virtual sob demanda depois de configurar o standby virtual.

Exemplo:

Crie uma nova máquina de standby virtual do Hyper-V:

```
>New-HyperVVirtualStandby -core [host name] -user [login] -password [password] -protectedserver
[name | IP address]
    -volumes [volumes names] -vmname [virtual machine name] [-gen2] -useVhdx [-uselocalmachine]
| -hostname [virtual ho
    st name] -hostport [virtual host port number] -hostusername [virtual host login] -
hostpassword [virtual host passwo
    rd]] -vmlocation [location] [-ram [total megabytes] | -usesourceram] -initialexport
```

New-Mount

O comando `New-Mount` monta um snapshot de uma ou mais unidades.

Forma de uso

A forma de uso do comando é a seguinte:

```
New-Mount -core [host name] -user [user name] -password [password] -protectedserver [machine
name] -mounttype [read | write | readonlywithpreviouswrites] -drives [drive names] -path
[location] -time [MM/DD/YYYY hh:mm:ss tt | passed | latest] -rpn [number]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `New-Mount`:

Tabela 257. Opções do comando New-Mount

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-protectedserver`	O nome da máquina ou endereço IP do servidor protegido (depende de como a máquina específica foi protegida).
`-time`	Opcional. O timestamp do ponto de recuperação a ser montado. Ele deve estar no formato especificado pelo OS do computador em questão. O administrador é capaz de obter o ponto de recuperação mais recente especificando o último ponto de recuperação ou o mais recentemente verificado pelo valor de parâmetro aprovado. Como padrão, a opção de último horário é escolhida.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-path`	Caminho na máquina Core para a qual os pontos de recuperação serão montados.
`-mounttype`	Opcional. Especifica um modo de montagem. As opções disponíveis são `'read'`,`'readOnlyWithPreviousWrites'` (somente leitura com gravações anteriores),`'write'` (gravável). O modo padrão é `read-only`.
`-volumes`	Opcional. Lista separada por espaços dos nomes de volumes a serem montados. Se o nome do volume contém espaços ou caracteres especiais, ele precisa ser especificado usando aspas duplas. Se não especificado, todos os volumes serão montados.
`-drivers`	Opcional. Lista separada por vírgulas dos nomes de volumes a serem montados. Se não especificado, todos os volumes serão montados. **NOTA: Essa opção é obsoleta, use `'-volumes'` em vez disso.**
`-rpn`	Opcional. Número do ponto de recuperação para a montagem. Você pode conseguir isso usando o comando `get-mounts`. Especifique diversos números para o parâmetro `rpn` para montar diferentes pontos com um único comando. **NOTA: Se você definir uma matriz de pontos para montar, cada ponto estará localizado em um diretório subordinado separado. O nome descreve o horário em que o ponto de recuperação foi criado. Quando você chamar a função de desmontar, todos os diretórios subordinados serão removidos. Você deve remover o diretório principal manualmente.**

Exemplo:

```
>New-Mount -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -protectedserver
10.10.5.22 -path C:\MountedRecoveryPoint -mounttype read -volumes c “d, ko”
```

Montar uma matriz de pontos de recuperação:

```
>New-Mount –rpn 10 52 41 -protectedserver localhost –path “D:/Folder for mount”
```

Montar um ponto de recuperação com certo horário de criação:

```
>New-Mount -protectedserver 10.10.5.56 -path "D:/Folder for mount" -time "8/24/2012 11:46 AM"
```

Resume-Replication

O comando `New-Replication` permite configurar e forçar a replicação para um ou mais servidores protegidos.

Forma de uso

A forma de uso do comando é a seguinte:

```
New-Replication -core [host name] -user [login] -password [password] -targetserver [host name] -protectedserver [name | IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `New-Replication`:

Tabela 258. Opções do comando New-Replication

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-replicationname`	Nome da configuração da replicação no Core de destino.
`-targetserver`	O nome do host, nome de usuário e senha do Core de destino.
`-protectedserver`	O nome da máquina protegida e do repositório no Core de destino para configurar uma replicação.

Exemplo:

Crie uma nova replicação para a máquina protegida com o IP 10.10.10.4:

```
>New-Replication -targetserver 10.10.10.128 -protectedserver 10.10.10.4
```

New-Repository

O comando `New-Repository` cria um novo repositório de DVM no Rapid Recovery Core. O tamanho especificado deve estar entre 250MB e 16TB.

Forma de uso

A forma de uso do comando é a seguinte:

```
New-Repository | -name [name] -size [size] -datapath [location] -metadatapath [location]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `New-Repository` :

Tabela 259. Opções do comando New-Repository

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-name`	Nome do repositório.
`-size`	Tamanho da extensão do repositório. As unidades disponíveis são: b, Kb, MB, GB, TB, PB.
`-datapath`	Para espaço local, somente. Determina o caminho de dados da extensão de repositório.
`-metadatapath`	Para espaço local, somente. Determina o caminho de metadados da extensão de repositório.
`-uncpath`	Para local partilhado, somente. Determina os caminhos de dados e metadados da extensão de repositório.
`-shareusername`	Para local partilhado, somente. Determinar login para local partilhado.
`-sharepassword`	Para local partilhado, somente. Determinar senha para local partilhado.
`-comment`	Opcional. Descrição do repositório.
`-concurrent Operations`	Opcional. O número máximo de operações pode estar pendente de uma só vez. Valor por padrão: 64.

Exemplo:

Crie um novo repositório de DVM do tamanho mínimo na unidade local E:

```
>New-Repository -name Repository2 -size 250Mb -datapath e:\Repository\Data -metadatapath e:
\Repository\Metadata
```

New-ScheduledArchive

O comando `New-ScheduledArchive` permite usar o PowerShell para alterar um arquivamento programado existente.

Forma de uso

A forma de uso do comando é a seguinte:

```
New-ScheduledArchive -core [host name] -user [login] -password [password] -all | -
protectedserver [name | IP address] -path [location] -archiveusername [name] -archivepassword
[password] -cloudaccountname [name] -cloudcontainer [name] -recycleaction [type] -schdeuletype
[type] -dayofweek [name] -dayofmonth [number] -time [time]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `New-ScheduledArchive`:

Tabela 260. Opções do comando New-ScheduledArchive

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	A máquina protegida com pontos de recuperação que você deseja arquivar. Você pode especificar vários nomes de máquinas entre aspas duplas e separados por vírgulas.
`-all`	Arquive os pontos de recuperação para todas as máquinas protegidas.
`-path`	O caminho para salvar os dados arquivados. Por exemplo: • Máquina local: "d:\work\archive" • Caminho da rede: "\\servername\sharename" • Pasta em uma conta de nuvem: "Nome da pasta" **NOTA: O número de símbolos não deve ser maior que 100 para locais e locais de rede nem maior que 150 para um local de nuvem.**
`-archiveusername`	Opcional. O nome de usuário para o login na máquina remota. Necessário para um caminho de rede apenas.
`-archivepassword`	Opcional. A senha para fazer login na máquina remota. Necessário para um caminho de rede apenas.

Opção	Descrição
-cloudaccountname	Opcional. Use somente para arquivo na nuvem. O nome da conta de nuvem em que você deseja salvar o arquivamento.
-cloudcontainer	Opcional. Use somente para arquivo na nuvem. O nome do contêiner da nuvem, na conta de nuvem escolhida, onde o arquivo será salvo. Quando você usar essa opção, também deve especificar o parâmetro "-cloudaccountname".
-recycleaction	O tipo de ação de reciclagem. Especificado usando um dos quatro valores a seguir: • "replacethiscore" - Substitui qualquer dado arquivado pré-existente pertencente a esse Core, mas deixa os dados de outros Cores intactos. • "erasecompletely" - Limpa todos os dados arquivados do diretório antes de gravar o novo arquivo. • "incremental" - Permite adicionar pontos de recuperação a um arquivo existente. Compara pontos de recuperação para evitar duplicação de dados que já existem no arquivo.
-scheduletype	Tipo de intervalo do programa. Opção especificada com um dos quatro valores a seguir: • "diário" - Para um arquivo criado automaticamente, diariamente. • "semanalmente" - Para um arquivo criado automaticamente, semanalmente. Especifique o parâmetro "-dayofweek". • "mensalmente" - Para um arquivo criado automaticamente, mensalmente. Especifique o parâmetro "-dayofmonth". Se um mês não tiver o dia especificado – por exemplo, "31" – o arquivamento não ocorrerá para esse mês. • "lastdayofmonth" - Para criar um arquivo automaticamente no último dia de cada mês.
-dayofweek	Use somente para a opção "semanalmente" do parâmetro "-scheduletype". O dia da semana no qual deseja criar automaticamente o arquivo (por exemplo, "Segunda-feira").
-dayofmonth	Use somente para a opção "mensalmente" do parâmetro "-scheduletype". O dia (número) do mês no qual deseja criar automaticamente o arquivo (por exemplo, "15").
-time	A hora do dia em que você deseja criar um arquivo.
-initialpause	Opcional. Especifique essa opção se deseja pausar o arquivo inicialmente depois de configurar o programa de arquivo

Exemplos:

Arquive todos os pontos de recuperação com datas de criação a partir de 04/30/2012 02:55 PM para todas as máquinas no Core e recoloque os dados arquivados pré-existentes pertinentes a este Core:

```
>New-ScheduledArchive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -path "d:\work
\archive" -s
    tartdate "04/30/2012 02:55 PM" -all -recycleaction replacethiscore
```

Arquive os pontos de recuperação que estiverem dentro de um período para duas máquinas protegidas e limpe todos os dados arquivados do diretório antes de gravar o novo arquivo:

```
>New-ScheduledArchive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver "10.20.30.40" "20.20.10.1" -path "d:\work\archive" -startdate "04/30/2012 02:55
PM" -enddate "05/31/2012 11:00 AM" -recycleaction erasecompletely
```

Crie um arquivo incremental para todos os pontos de recuperação com datas de criação a partir de 04/30/2012 02:55 PM para todas as máquinas no Core para a conta de nuvem com o nome "Amazon S3" e um contêiner chamado "Contêiner":

```
>New-ScheduledArchive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -path
"ArchiveOnCloud" -cloudaccountname "Amazon S3" -cloudcontainer "Container" -startdate
"04/30/2012 02:55 PM" -all -recycleaction incremental
```

New-Snapshot

O comando `New-Snapshot` força um snapshot que resulta em uma transferência de dados da máquina atualmente protegida. Ao forçar um snapshot, a transferência iniciará imediatamente ou será adicionada à fila. Somente os dados que foram alterados em relação a um ponto de recuperação anterior serão transferidos. Caso não existir um ponto de recuperação anterior, todos os dados nos volumes protegidos serão transferidos.

Forma de uso

A forma de uso do comando é a seguinte:

```
New-Snapshot [-all] | -protectedserver [machine name]] -core [host name] -user [user name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `New-Snapshot`:

Tabela 261. Opções do comando New-Snapshot

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-all`	Forçar todas as máquinas protegidas.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Forçar para o nome da máquina protegida atual.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Forçar um snapshot de todas as máquinas protegidas:

```
>New-Snapshot -all
```

New-VBVirtualStandby

O comando `New-VBVirtualStandby` permite usar o PowerShell para criar uma nova exportação virtual para uma máquina virtual (VM) VirtualBox.

Forma de uso

A forma de uso do comando é a seguinte:

```
New-VBVirtualStandby -core [host name] -user [login] -password [password] -protectedserver
[name | IP address] -volumes [volumes names] -vmname [virtual machine name] [-ram [total
megabytes] | -usesourceram]  -linuxhostname [linux hostname] -hostport [linux port] -targetpath
[location] -pathusername [login] -pathpassword [password] -initialexport
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `New-VBVirtualStandby`:

Tabela 262. Opções do comando New-VBVirtualStandby

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.
`-volumes`	Opcional. Liste os nomes de volume que deseja exportar. Se não for especificado, todos os volumes no(s) ponto(s) de recuperação serão exportados. Os valores devem ser informados entre aspas duplas e separados por um espaço; por exemplo, "c:", "d:". **NOTA: Não use barras nos nomes dos volumes.**
`-vmname`	O nome do Microsoft Windows da máquina virtual.
`-ram`	Alocar uma quantidade específica de RAM no servidor virtual.
`-usesourceram`	Opcional. Aloque no servidor virtual a mesma quantidade de RAM que a máquina de origem protegida possui.
`-linuxhostname`	O nome do host do servidor Linux VirtualBox.
`-hostport`	A porta do servidor Linux VirtualBox.
`-targetpath`	O caminho do local, de rede ou do Linux para a pasta em que você deseja armazenar os arquivos da máquina virtual.
`-pathusername`	O nome de usuário para o login na máquina da rede. Necessário somente ao especificar um local de rede para o caminho de destino.

Opção	Descrição
-pathpassword	A senha para fazer login na máquina da rede. Necessário somente ao especificar um local de rede para o caminho de destino.
-accountusername	Opcional. Você pode especificar uma conta de usuário para registrar a máquina virtual exportada. O nome de usuário para o login na conta de usuário. Use essa opção apenas para uma máquina local ou de rede.
-accountpassword	Opcional. Você pode especificar uma conta de usuário para registrar a máquina virtual exportada. Senha para fazer login na conta de usuário. Use essa opção apenas para uma máquina local ou de rede.
-initialexport	Opcional. Especifique essa opção se precisar iniciar uma exportação de máquina virtual sob demanda depois de configurar o standby virtual.

Exemplo:

Crie uma máquina de standby virtual do VirtualBox com o nome ExportedMachine1 em um local especificado:

```
>New-VBVirtualStandby -protectedserver 10.10.10.4 -volumes C:\ -vmname ExportedMachine1 -
usesourceram -targetpath I:\VMExport
```

New-VMVirtualStandby

O comando PowerShell `New-VMVirtualStandby` permite criar uma nova máquina em standby virtual do VMWare Workstation usando o Rapid Recovery.

Forma de uso

A forma de uso do comando é a seguinte:

```
New-VMVirtualStandby -core [host name] -user [login] -password [password] -protectedserver
[name | IP address] -volumes [volumes names] -vmname [virtual machine name] [-ram [total
megabytes] | -usesourceram] -targetpath [location] -pathusername [login] -pathpassword
[password] -initialexport
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `New-VMVirtualStandby`:

Tabela 263. Opções do comando New-VMVirtualStandby

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon.

Opção	Descrição
	Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Mostrar trabalhos de uma máquina protegida específica, indicada por endereço IP.
`-volumes`	Opcional. Liste os nomes de volume que deseja exportar. Se não for especificado, todos os volumes no(s) ponto(s) de recuperação serão exportados. Os valores devem ser informados entre aspas duplas e separados por um espaço; por exemplo, "c:", "d:". **NOTA: Não use barras nos nomes dos volumes.**
`-vmname`	O nome do Microsoft Windows da máquina virtual.
`-ram`	Alocar uma quantidade específica de RAM no servidor virtual.
`-usesourceram`	Opcional. Aloque no servidor virtual a mesma quantidade de RAM que a máquina de origem protegida possui.
`-pathusername`	O nome de usuário para o login na máquina da rede. Necessário somente ao especificar um local de rede para o caminho de destino.
`-pathpassword`	A senha para fazer login na máquina da rede. Necessário somente ao especificar um local de rede para o caminho de destino.
`-initialexport`	Opcional. Especifique essa opção se precisar iniciar uma exportação de máquina virtual sob demanda depois de configurar o standby virtual.

Exemplo:

Crie um novo standby virtual do VMWare Workstation:

```
>New-VMVirtualStandby -protectedserver 10.10.10.4 -volumes C:\ -vmname ExportedMachine1 -
usesourceram -targetpath I:\VMExport
```

O script faz uma pausa, exigindo que o usuário especifique um número de índice remissivo para a estação de trabalho adequada. Digite o número de índice remissivo para o script concluir (nesse caso, 2). O exemplo continua:

```
2
Verify location ...
Virtual Standby successfully configured
PS C:\Users\Administrator>
```

Push-Replication

O comando `Push-Replication` força a replicação de uma ou mais máquinas protegidas.

Forma de uso

A forma de uso do comando é a seguinte:

```
Push-Replication -core [host name] -user [user name] -password [password] -targetcore [host
name] -all | -protectedserver [machine name | IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Push-Replication` :

Tabela 264. Opções do comando Push-Replication

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-all`	Forçar replicação para todas as máquinas sendo replicadas no Core de destino.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Nome da máquina protegida no Core de destino contra a qual a replicação será forçada.
`-user`	Opcional. Login para a máquina de host do Core remoto. Se você especificar um login, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Enviar replicação para uma única máquina protegida:

```
>Push-Replication -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
-targetcore 10.10.10.20:8006 -protectedserver 10.10.5.22
```

Enviar replicação para todas as máquinas protegidas:

```
>Push-Replication -all
```

Push-Rollup

O comando `Push-Rollup` força o rollup de uma máquina protegida.

Forma de uso

A forma de uso do comando é a seguinte:

```
Push-Rollup -core [host name] -user [user name] -password [password] -protectedserver [machine
name | IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Push-Rollup` :

Tabela 265. Opções do comando Push-Rollup

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-all`	Forçar todas as máquinas protegidas.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Forçar para o nome da máquina protegida atual.
`-user`	Opcional. Login para a máquina de host do Core remoto. Se você especificar um login, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Enviar rollup para uma única máquina protegida:

```
>Push-Rollup -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22
```

Enviar rollup para todas as máquinas protegidas:

```
>Push-Rollup -all
```

Remove-Agent

O comando`Remove-Agent` PowerShell permite remover uma máquina da proteção do Rapid Recovery Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
Remove-Agent -core [host name] -user [login] -password [password] -protectedserver [name | IP address] -deleterecoverypoints -all
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Remove-MountAgent`:

Tabela 266. Opções do comando Remove-Agent

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.

Opção	Descrição
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-protectedserver	Desmontar todos os pontos de recuperação montados para a máquina protegida atual.
-deleterecoverypoints	Opcional. Excluir todos os pontos de recuperação dessa máquina protegida.
-all	Opcional. Excluir todas as máquinas protegidas do Core.

Exemplo:

Desmontar todas as máquinas protegidas e seus pontos de recuperação:

```
>Remove-Agent -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -
deleterecoverypoints -all
```

Remove-Mount

O comando `Remove-Mount` desmonta um ponto de recuperação montado especificado pelo `/Path`. Desmonta pontos para a máquina selecionada usando o parâmetro `-protectedserver` ou desmonta pontos para todos os pontos de recuperação montados usando o parâmetro `-all`.

Forma de uso

A forma de uso do comando é a seguinte:

```
Remove-Mount -core [host name] -user [user name] -password [password] [-
protectedserver [machine name] | -path [mount path]]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Remove-Mount`:

Tabela 267. Opções do comando Remove-Mount

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-all	Desmontar todos os pontos de recuperação montados.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.

Opção	Descrição
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-path	Desmontar ponto de montagem selecionado.
-protectedserver	Desmontar todos os pontos de recuperação montados para a máquina protegida atual.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Desmontar o ponto de recuperação especificado pelo caminho:

```
>Remove-Mount -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -path C:
\mountedRecoveryPoint
```

Remove-Mounts

O comando `Remove-Mounts` desmonta todos os pontos de recuperação montados.

Forma de uso

A forma de uso do comando é a seguinte:

```
Remove-Mounts -core [host name] -user [user name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Remove-Mounts`:

Tabela 268. Opções do comando Remove-Mounts

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Exemplo:

Desmontar todos os pontos de recuperação no Core especificado:

```
>Remove-Mounts -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
```

Remove-RecoveryPoints

O comando`Remove-RecoveryPoints` do PowerShell permite excluir pontos de recuperação de uma determinada máquina.

Forma de uso

A forma de uso do comando é a seguinte:

```
Remove-RecoveryPoints -core [host name] -user [login] -password [password] -[range | chain |
all] -protectedserver
    [name | IP address] -rpn [number | numbers] | -time [time string | time interval specified
by two time strings]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Remove-RecoveryPoints`:

Tabela 269. Opções do comando Remove-RecoveryPoints

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Desmontar todos os pontos de recuperação montados para a máquina protegida atual.
`-rpn`	Opcional. Somente para exclusão de cadeia (imagem base com cadeia de pontos incrementais ou órfãos). O número sequencial de um ponto de recuperação a ser excluído (use o comando Get-RecoveryPoints para obter os números). É possível especificar diversos números separados por espaço para excluir vários pontos de recuperação com um único comando.
`-time`	Use esta opção para apagar uma cadeia de pontos de recuperação. Opcional. Para apagar um único ponto de recuperação, selecione o ponto de recuperação pela sua hora de criação. Especifique o tempo exato no formato "mm/dd/aaaa hh:mm tt" (por exemplo, "2/24/2012 09:00 AM"). Lembre-se de especificar os valores de data e hora do fuso horário definido no computador.

Opção	Descrição
	Obrigatório. Para um período, especifique um intervalo de tempo utilizando duas strings de tempo separadas por vírgula e espaço para selecionar a faixa de pontos de recuperação que devem ser apagados.
`-range`	Opcional. A faixa de pontos de recuperação a serem apagados por intervalo de tempo.
`-chain`	Opcional. Uma imagem de base com incrementos sequenciais ou um conjunto sequencial de pontos definidos como órfão para apagar os selecionados por número do ponto de recuperação ou pela hora de criação do ponto de recuperação.
`-all`	Opcional. Excluir todas as máquinas protegidas do Core.

Exemplo:

Excluir o ponto de recuperação especificado pela data:

```
>Remove-RecoveryPoints -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -time
"2/24/2012 09:00 AM"
```

Remove-Repository

O comando PowerShell `Remove-Repository` exclui o repositório do Rapid Recovery e seu conteúdo do Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
Remove-Repository -core [host name] -user [login] -password [password] -name [repository name] -
all
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Remove-Repository`:

Tabela 270. Opções do comando Remove-Repository

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Opção	Descrição
-name	O nome do repositório que você deseja excluir.
-all	Exclua todos os repositórios associados a esse Core.

Exemplo:

Remova todos os repositórios no Core local:

```
>Remove-repository -all
```

Remove-ScheduledArchive

Se você programou o Rapid Recovery para arquivar regularmente pontos de recuperação de uma máquina específica, você pode usar o comando`Remove-ScheduledArchive` do PowerShell para remover esses arquivos programados do Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
Remove-ScheduledArchive -core [host name] -user [login] -password [password] -all -ids [id | id1 id2]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Remove-ScheduledArchive`:

Tabela 271. Opções do comando Remove-ScheduledArchive

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-all	Remova todos os arquivos associados a esse Core.
-id	O identificador do arquivo que você deseja remover. Para listar mais de um arquivo, separe cada ID com um espaço.

Exemplo:

Remover vários arquivos programados do Core local:

```
>Remove-ScheduledArchive -ids 799138c8-3dfc-4398-9711-1823733c2a31, 26c29bb7-b320-47f5-b5a8-
dffc49f50e25
```

Remove-VirtualStandby

Se você programou o Rapid Recovery para exportar continuamente dados para uma máquina virtual, você pode usar o comando`Remove-VirtualStandby` do PowerShell para cancelar e apagar esse trabalho programado.

Forma de uso

A forma de uso do comando é a seguinte:

```
Remove-VirtualStandby -core [host name] -user [login] -password [password] -all | -
protectedserver [name(s) | IP ad
    dress]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Remove-VirtualStandby`:

Tabela 272. Opções do comando Remove-VirtualStandby

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-all`	Remova todos os trabalhos de standby virtual associados a esse Core.
`-protectedserver`	O nome ou o endereço IP da máquina protegida da qual você deseja remover o standby virtual.

Exemplo:

Remover todos os trabalhos de standby virtual associados a esse Core:

```
>Remove-VirtualStandby -all
```

Resume-Replication

O comando`Resume-Replication` permite que você retome uma replicação. Consulte Suspend-Replication para obter mais detalhes.

Forma de uso

A forma de uso do comando é a seguinte:

```
Resume-Replication -core [host name] -user [user name] -password [password] -all | -
protectedserver [machine name | IP address] -incoming [host name] | -outgoing [host name]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Resume-Replication`:

Tabela 273. Opções do comando Resume-Replication

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-all`	Todos os servidores protegidos.
`-protectedserver`	Retomar a replicação da máquina especificada.
`-incoming`	Nome do host do Core remoto que replica para a máquina Core. A replicação de todas as máquinas protegidas no Core remoto é retomada.
`-outgoing`	Nome de host do Core de destino remoto no qual os dados são replicados. A replicação de todas as máquinas protegidas no Core remoto é retomada.

Exemplo:

Retomar replicação da máquina protegida com o IP 10.10.10.128 para o Core local, especificando o repositório sendo usado:

```
>Resume-Replication replicationname Replication1 -targetserver 10.10.10.128,Administrator,
123asdQ -protectedserver 10.10.10.4

# Repository
- ----------

1 Repository A
2 Repository B
Please, input number of Repository from the list above or type 'exit' to exit:
```

O script é pausado, o que exige que o usuário especifique um número de índice para o repositório adequado. Digite o número de índice para o script para concluir (neste caso, 2). O exemplo continua:

```
2
Replication job was started.
True
PS C:\Users\Administrator>
```

Resume-Snapshot

Um administrador é capaz de retomar snapshots, exportar para máquinas virtuais e realizar replicações. Consulte Start-VMExport para obter mais detalhes.

Forma de uso

A forma de uso do comando é a seguinte:

```
Resume-Snapshot -core [host name] -user [user name] -password [password] -all | -
protectedserver [name | IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Resume-Snapshot`:

Tabela 274. Opções do comando Resume-Snapshot

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-all`	Todos os servidores protegidos.
`-protectedserver`	Retoma o snapshot da máquina especificada.

Exemplo:

Retomar snapshots da máquina protegida com o IP 10.10.10.4 para o Core local:

```
>Resume-Snapshot -protectedserver 10.10.10.4
```

Resume-VirtualStandby

O comando PowerShell `Resume-VirtualStandby` permite retomar a exportação suspensa dos dados para uma máquina de standby virtual do Rapid Recovery.

Forma de uso

A forma de uso do comando é a seguinte:

```
Resume-VirtualStandby -core [host name] -user [login] -password [password] -all | -
protectedserver [name(s) | IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Resume-VirtualStandby`:

Tabela 275. Opções do comando Resume-VirtualStandby

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-all`	Retoma as exportações para todas as máquinas de standby virtual.
`-protectedserver`	O nome ou nomes – separados por vírgula e espaço – das máquinas protegidas com as máquinas de standby virtual que você deseja retomar.

Exemplo:

Retoma as exportações de standby virtual para uma máquina protegida:

```
>Resume-VirtualStandby -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22
```

Resume-VMExport

O comando `Resume-VMExport` permite que um administrador exporte para máquinas virtuais. Consulte Suspend-VMExport para obter mais detalhes.

Forma de uso

A forma de uso do comando é a seguinte:

```
Resume-VMExport -core [host name] -user [user name] -password [password] -all | -
protectedserver [name | IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Resume-VMExport`:

Tabela 276. Opções do comando Resume-VMExport

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-all`	Todos os servidores protegidos.
`-protectedserver`	Retoma o snapshot da máquina especificada.

Exemplo:

Retomar a exportação para uma máquina virtual em cada máquina protegida no Core local:

```
>Resume-VMExport -all
```

Start-Archive

As empresas frequentemente usam o armazenamento de longo prazo para arquivar dados compatíveis e não compatíveis. O recurso de arquivo do Rapid Recovery é usado para suportar a retenção estendida para dados compatíveis e não compatíveis. O administrador pode salvar um arquivo no armazenamento local ou local de rede especificando o comando `/Path` e as credenciais.

Forma de uso

A forma de uso do comando é a seguinte:

```
Start-Archive -path -startdate -enddate [-all] | -protectedserver [machine name] or [IP]] -core
[host name] -user [user name] -password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Start-Archive`:

Tabela 277. Opções do comando Start-Archive

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-path`	Caminho até o local. Exemplo de caminho: 'D:\work\archive' or network path: '\\servername\sharename'.
`-all`	Arquivar os pontos de recuperação para todas as máquinas no Core.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-startdate`	Data inicial dos pontos de recuperação criados no período. Ela deve estar no formato especificado pelo OS do computador em questão.
`-enddate`	Data final do período. O padrão é a data atual.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Arquiva pontos de recuperação para a máquina especificada.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-archiveusername`	Opcional. Necessário para caminho de rede apenas.
`-archivepassword`	Opcional. Necessário para caminho de rede apenas.
`-comment`	Opcional. Exemplo:`-comment 'Before install new application'`.

Exemplo:

Arquivar todos os pontos de recuperação para todas as máquinas no Core:

```
>Start-Archive -path D:\work\archive -startdate 'Example 04/30/2012' -all
```

Start-AttachabilityCheck

O comando`Start-AttachabilityCheck` força uma verificação de capacidade de anexação em todos os SQL Server databases protegidos pelo Core.

Forma de uso

A forma de uso do comando é a seguinte:

```
Start-AttachabilityCheck -core [host name] -user [username] - password [password]
- protectedserver [machine name | IP address] -rpn [number | numbers] | -time [time string]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Start-AttachabilityCheck`:

Tabela 278. Opções do comando Start-AttachabilityCheck

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	A máquina protegida na qual será realizada a verificação de capacidade de anexação do SQL.
`-rpn`	Opcional. O número sequencial de um ponto de recuperação no qual deverá ser realizada a verificação de capacidade de anexação do SQL. Use o comando`-GetRecoveryPoints` para obter números de pontos de recuperação. Você pode especificar vários números separados por espaços para realizar verificações em vários pontos de recuperação com um único comando. **NOTA: Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será usado para a verificação de capacidade de anexação.**
`-time`	Opcional. Determina o ponto de recuperação a ser selecionado para a verificação de capacidade de anexação do SQL. Você deve especificar o tempo exato no formato "MM/DD/AAAA hh:mm tt" (por exemplo: "04/24/2015 09:00 AM"). Especificar os valores de data e hora do fuso horário definido na sua máquina local. **NOTA: Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será exportado.**

Exemplo:

Realizar uma verificação de capacidade de anexação do SQL no ponto de recuperação mais recente para o servidor SQL protegido especificado:

```
>Start-AttachabilityCheck - protectedserver 10.10.9.120
```

Start-ChecksumCheck

O comando PowerShell `Start-ChecksumCheck` permite forçar uma verificação de soma de verificação dos pontos de recuperação do Exchange Server.

Forma de uso

A forma de uso do comando é a seguinte:

```
Start-ChecksumCheck -core [host name] -user [login] -password [password] -protectedserver [name | IP address] -rpn [number | numbers] | -time [time string]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Start-ChecksumCheck`:

Tabela 279. Opções do comando Start-ChecksumCheck

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Nome da máquina protegida.
`-rpn`	Opcional. Somente para exclusão de cadeia (imagem base com cadeia de pontos incrementais ou órfãos). O número sequencial de um ponto de recuperação para verificar (use o comando Get-RecoveryPoints para obter os números). É possível especificar diversos números separados por espaço para excluir vários pontos de recuperação com um único comando.
`-time`	Opcional. Selecione o ponto de recuperação para a verificação pela hora da criação, não pelo número sequencial. Especifique o tempo exato no formato "mm/dd/aaaa hh:mm tt" (por exemplo, "2/24/2012 09:00 AM"). Lembre-se de especificar os valores de data e hora do fuso horário definido no seu computador.

Exemplo:

Inicie uma verificação de soma de verificação em dois pontos de recuperação:

```
> Start-ChecksumCheck -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver 10.10.5.22 -rpn 5 7
```

Start-EsxiExport

O comando PowerShell `Start-EsxiExport` inicia uma exportação virtual do ponto de recuperação Rapid Recovery selecionado para uma máquina virtual de servidor ESX(i).

Os parâmetros necessários incluem o nome da máquina protegida que contém os pontos de recuperação a serem exportados; o nome da máquina virtual para a qual a exportação está sendo feita; a quantidade de RAM a ser alocada na máquina virtual; o nome de host e porta do host de servidor Linux; e o caminho para a pasta local, de rede ou de Linux na qual os arquivos de máquina virtual resultantes serão armazenados.

Forma de uso

A forma de uso do comando é a seguinte:

```
Start-EsxiExport -core [host name] -user [user name] -password [password] -protectedserver
[machine name | IP address] -volumes [volume names] -rpn [number | numbers] | -time [time
string] -vmname [virtual machine name] -hostname [virtual host name] -hostport [virtual host
port number] -hostusername [virtual host user name] hostpassword [virtual host password] [-ram
[total megabytes] | -usesourceram] -diskprovisioning [thin | thick] -diskmapping [automatic |
manual | withvm]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Start-EsxiExport`:

Tabela 280. Opções do comando Start-EsxiExport

Opção	Descrição
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Máquina protegida com pontos de recuperação a serem exportados.
`-volumes`	Opcional. Lista de nomes de volumes a serem exportados. Se não for especificado, todos os volumes nos pontos de recuperação especificados serão exportados. Os valores devem ser informados entre aspas duplas e cada um separado por um espaço. não use barras nos nomes dos volumes. Por exemplo, especifique "C:" e não "C:/"
`-rpn`	Opcional. O número sequencial de um ponto de recuperação a ser exportado. (Use o comando `Get-RecoveryPoints` para obter números de pontos de recuperação. **NOTA: Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será exportado.**
`-time`	Opcional. Determina o ponto de recuperação a ser selecionado para exportação. Você precisa especificar a hora exata no formato "MM/DD/AAAA hh:mm tt" (por exemplo: "04/24/2015 09:00 AM"). Especifique valores de data e hora do fuso horário definido em sua máquina local.

Opção	Descrição
	NOTA: Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será exportado.
`-vmname`	Nome do Windows da máquina virtual.
`-hostname`	O nome do host do servidor virtual.
`-hostport`	O número da porta do servidor virtual.
`-hostusername`	O nome de usuário para o host do servidor virtual.
`-hostpassword`	A senha para o host do servidor virtual.
`-ram`	Alocar uma quantidade específica de RAM no servidor virtual.
`-usesourceram`	Opcional. Alocar a mesma quantidade de RAM no servidor virtual quanto na máquina de origem protegida.
`-diskprovisioning`	Opcional. A quantidade de espaço em disco que será alocada na máquina virtual. Especifique "thick" para fazer o disco virtual ter o mesmo tamanho da unidade original no server protegido, ou "thin" para alocar a quantidade de espaço em disco efetivamente ocupada na unidade original mais algum espaço extra em megabytes. Por padrão, o provisionamento "thin" é selecionado.
`-diskmapping`	Opcional. Selecione "auto", "manual" ou "withvm". O automapeamento está ativado por padrão.
`-resetup`	Opcional. Recria a máquina virtual automaticamente se ela já estiver apresentada no local especificado.
`-datacenter`	Opcional. Especifica o datacenter que será usado.
`-resourcepool`	Opcional. Especifica o conjunto de recursos que será usado.
`-datastore`	Opcional. Especifica os dados que serão usados.
`-computeresource`	Opcional. Especifica o recurso de computação que será usado.
`-version`	Opcional. Especifica a versão do ESXi que será usada.

Start-HypervExport

O comando PowerShell `Start-HypervExport` inicia uma exportação virtual do ponto de recuperação Rapid Recovery selecionado para uma máquina virtual de servidor Hyper-V.

Forma de uso

A forma de uso do comando é a seguinte:

```
Start-HypervExport -core [host name] -user [user name] -password [password] -protectedserver
[[machine name] or [IP address]] -volumes [volume names] -rpn [number | numbers] | -time [time
string] [-vmname [uselocalmachine] | -hostname [virtual host name] -hostport [virtual host port
number] -hostusername [virtual host user name] -hostpassword [virtual host password] -
vmlocation [location]] [-ram [total megabytes] | -usesourceram] -diskformat [VHD | VHDX]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Start-HypervExport`:

Tabela 281. Opções do comando Start-HypervExport

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Máquina protegida com pontos de recuperação a serem exportados.
`-volumes`	Opcional. Lista de nomes de volumes a serem exportados. Se não for especificado, todos os volumes nos pontos de recuperação especificados serão exportados. Os valores devem ser informados entre aspas duplas e cada um separado por um espaço. não use barras nos nomes dos volumes. Por exemplo, especifique "C:" e não "C:/"
`-rpn`	Opcional. O número sequencial de um ponto de recuperação a ser exportado. (Use o comando `Get-RecoveryPoints` para obter números de pontos de recuperação. **NOTA: Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será exportado.**
`-time`	Opcional. Determina o ponto de recuperação a ser selecionado para exportação. Você precisa especificar a hora exata no formato "MM/DD/AAAA hh:mm tt" (por exemplo: "04/24/2015 09:00 AM"). Especifique valores de data e hora do fuso horário definido em sua máquina local. **NOTA: Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será exportado.**
`-vmname`	Nome do Windows da máquina virtual.
`-gen2`	Opcional. Especifique para usar a segunda geração de VM. Se não for especificado, a geração 1 será usada. O Rapid Recovery suporta a geração 2 desde o Windows Server 2012 R2 até o Windows 8.1.
`-usevhdx`	Opcional. Se você especificar essa opção, o Rapid Recovery usará o formato do disco VHDX para criar a VM. Do contrário, ele usará o formato de disco VHD. A geração 2 usa somente o formato VHDX.
`-uselocalmachine`	Opcional. Conectar ao servidor Hyper-V local. Quando este parâmetro é usado, as seguintes opções são ignoradas: hostname, host port, host username, host password.
`-hostname`	O nome do host do servidor virtual.
`-hostport`	O número da porta do servidor virtual.
`-hostusername`	O nome de usuário para o host do servidor virtual.
`-hostpassword`	A senha para o host do servidor virtual.

Opção	Descrição
-vmlocation	Caminho local ou de rede para a pasta em que você quer armazenar os arquivos da máquina virtual.
-ram	Alocar uma quantidade específica de RAM no servidor virtual.
-usesourceram	Opcional. Alocar a mesma quantidade de RAM no servidor virtual quanto na máquina de origem protegida.

Start-LogTruncation

O comando `Start-LogTruncation` força o truncamento de log para o SQL Server ou servidor Microsoft Exchange protegido especificado.

Forma de uso

A forma de uso do comando é a seguinte:

```
Start-LogTruncation -core [host name] -user [user name] -password [password] -protectedserver
[[machine name] or [IP address]] -target [sql | exchange]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Start-LogTruncation`:

Tabela 282. Opções do comando Start-LogTruncation

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-protectedserver	Arquivo de pontos de recuperação para a máquina especificada.
-target	Especificar o tipo de truncamento de log ("sql" ou "exchange"). Se não for especificado, os logs de todos os bancos de dados serão truncados.

Exemplo:

Truncar logs de SQL:

```
>Start-LogTruncation -protectedserver SQL1 -target sql
```

Truncar logs de servidor Exchange: todos os pontos de recuperação de todas as máquinas no Core:

```
> start-LogTruncation -protectedserver ExServer2 -target exchange
```

Start-MountabilityCheck

O comando`Start-MountabilityCheck` força uma verificação de capacidade de montagem em armazenamentos de e-mail do Microsoft Exchange protegidos.

Forma de uso

A forma de uso do comando é a seguinte:

```
Start-MountabilityCheck -core [host name] -user [user name] -password [password] -
protectedserver [[machine name] or [IP address]] -rpn [number | numbers] |
-time [time string]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Start-MountabilityCheck`:

Tabela 283. Opções do comando Start-MountabilityCheck

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Arquivo de pontos de recuperação para a máquina especificada.
`-rpn`	Opcional. O número sequencial de um ponto de recuperação a ser exportado. Use o comando`-GetRecoveryPoints` para obter números de pontos de recuperação. **NOTA: Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será exportado.**
`-time`	Opcional. Determina o ponto de recuperação a ser selecionado para exportação. Você deve especificar o tempo exato no formato "MM/DD/AAAA hh:mm tt" (por exemplo: "04/24/2015 09:00 AM"). Especificar os valores de data e hora do fuso horário definido na sua máquina local. **NOTA: Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será exportado.**

Exemplo:

Iniciar uma verificação de capacidade de montagem em todos os pontos de recuperação para todas as máquinas no Core:

```
> Start-MountabilityCheck -protected EX01
```

Start-Protect

O comando`Start-Protect` permite que um administrador adicione um servidor sob proteção de um Core.

Forma de uso

```
Start-Protect -core [host name] -user [user name] -password [password] -repository [repository name] -agent [name | IP address] -agentusername [user name]
-agentpassword [password] -agentport [port] -volumes [volume names]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Start-Protect`:

Tabela 284. Opções do comando Start-Protect

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-repository`	Nome do repositório do Core onde os dados da máquina protegida estão armazenados.
`-agentname`	Nome da máquina protegida ou endereço IP.
`-agentusername`	Login do servidor a ser protegido.
`-agentpassword`	Senha do servidor a ser protegido.
`-agentport`	Número da porta do servidor protegido.
`-volumes`	Lista de volumes a serem protegidos. Os valores devem ser informados entre aspas duplas e separados por um espaço. Não use barras nos nomes dos volumes. Por exemplo, "c:" ou "d:".

Exemplo:

Colocar os volumes de um servidor sob proteção:

```
>Start-Protect -repository "Repository 1" -agentname 10.10.9.120 -agentusername administrator -agentpassword 12345 -agentport 5002 -volumes "c:" "d:"
```

Start-ProtectCluster

O comando`Start-ProtectCluster` permite que um administrador adicione um cluster do servidor sob a proteção de um Core.

Forma de uso

O uso do comando é o seguinte:

```
Start-ProtectCluster -core [host name] -user [user name] -password [password] -repository [repository name] -clustername [name | IP address] -clusterusername [user name for cluster] -clusterpassword [password for cluster] -clusterport [port] -clustervolumes [volume names] -clusternodes [cluster nodes names and volumes]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Start-ProtectCluster`:

Tabela 285. Opções do comando Start-ProtectCluster

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-repository`	Nome do repositório do Core onde os dados da máquina protegida estão armazenados. O nome deve ser informado entre aspas duplas.
`-clustername`	O nome do cluster a ser protegido.
`-clusterusername`	Nome de usuário para o cluster a ser protegido.
`-clusterpassword`	Senha do cluster a ser protegido.
`-clusterport`	Número de porta do cluster a ser protegido.
`-clustervolumes`	Lista de volumes a serem protegidos. Os valores devem ser informados entre aspas duplas e separados por um espaço. Não use barras nos nomes dos volumes. Por exemplo, "c:", "d".
`-clusternodes`	Lista de nós de cluster com volumes a serem protegidos. Primeiro especifique o rótulo "nodename" e, em seguida, digite o nome do nó. Em seguida, especifique o rótulo "volumes" e digite uma lista de volumes para o nó. Por exemplo:`"nodename", "10.10.10.10", "volumes", "c:", "e:", "nodename", "10.10.10.11," "volumes", "c:"`

Exemplo:

Colocar os volumes de um servidor sob proteção:

```
>Start-ProtectCluster -repository "Repository 1" -clustername 10.10.9.120 -clusterusername
administrator -clusterpassword 12345 -clusterport 5002 -clustervolumes "c:" "d:" -clusternodes
nodename 10.10.10.10 volumes “c:” “e:”
```

Start-RepositoryCheck

O comando`Start-RepositoryCheck` do PowerShell permite verificar a integridade de um repositório.

Forma de uso

A forma de uso do comando é a seguinte:

```
Start-RepositoryCheck -name [repository name] | -all [check all repositories] -password
[password] -force
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Start-RepositoryCheck`:

Tabela 286. Opções do comando Start-RepositoryCheck

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-repository`	Obrigatório. O nome do repositório que você quer verificar.
`-all`	Opcional. Verifique todos os repositórios associados a esse Core.
`-force`	Opcional. Execute a verificação do repositório sem confirmação.

Exemplo:

Iniciar a verificação de um repositório:

```
>Start-RepositoryCheck -repository newRepository1 -core 10.10.10.10:8006 -user administrator -
password 23WE@#$sdd
```

Start-RestoreArchive

As empresas frequentemente usam o armazenamento de longo prazo para arquivar dados compatíveis e não compatíveis. O recurso de arquivo do Rapid Recovery é usado para suportar a retenção estendida para dados compatíveis e não compatíveis. O administrador pode salvar um arquivo no armazenamento local ou no local de rede especificando o comando `-Path` e as credenciais.

Forma de uso

A forma de uso do comando é a seguinte:

```
Start-RestoreArchive -core [host name] -user [login] -password [password] -all | -
protectedserver [name | IP address | "[name1 | IP address1]" "[name2 | IP address2]"] -
repository [name] -archiveusername [name] -archivepassword [password] -path [location]  -
cloudaccountname [name] -cloudcontainer [name]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Start-RestoreArchive`:

Tabela 287. Opções do comando Start-RestoreArchive

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-all`	Arquiva pontos de recuperação para todas as máquinas protegidas.
`-protectedserver`	A máquina protegida com os pontos de recuperação que você quer arquivar. Você pode especificar vários nomes de máquinas entre aspas duplas e separados por vírgulas.
`-repository`	O nome do repositório onde você quer colocar os pontos de recuperação restaurados. Você precisa colocar o nome entre aspas duplas; por exemplo, "Repository1".
`-archiveusername`	Opcional. O nome de usuário para fazer login na máquina remota. É necessário para caminho de rede apenas.
`-archivepassword`	Opcional. A senha para fazer login na máquina remota. É necessário para caminho de rede apenas.
`-path`	O caminho para o local onde os dados arquivados serão salvos. Por exemplo: • Máquina local: "d:\work\archive" • Caminho de rede: "\\servername\sharename"

Opção	Descrição
	• Pasta em uma conta de nuvem: "Nome da pasta" **NOTA: O número de símbolos não deve ser maior que 100 para local e local da rede, e não deve ser maior do que 150 para um local da nuvem.**
`-cloudaccountname`	Opcional. Use somente para arquivo na nuvem. O nome da conta de nuvem em que você quer salvar o arquivo.
`-cloudcontainer`	Opcional. Use somente para arquivo na nuvem. O nome do contêiner da nuvem, na conta de nuvem escolhida, onde o arquivo será salvo. Ao usar esta opção, você deve também especificar o parâmetro "-cloudaccountname".
`-manifestcore`	Opcional. Especifique o Core que você deseja usar do manifesto do arquivo restaurado.

Exemplo:

Arquivar todos os pontos de recuperação de todas as máquinas no Core e armazená-los na máquina local:

```
>Start-RestoreArchive -path D:\work\archive -startdate 'Example 04/30/2012' -all
```

Start-ScheduledArchive

O comando`Start-ScheduledArchive` do PowerShell permite forçar o início sob demanda de um arquivamento programado do Rapid Recovery, independentemente do plano pré-estabelecido.

Forma de uso

A forma de uso do comando é a seguinte:

```
Start-ScheduledArchive -core [host name] -user [login] -password [password] -all -ids [id | id1 id2]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Start-ScheduledArchive`:

Tabela 288. Opções do comando Start-ScheduledArchive

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon.

Opção	Descrição
	Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-all`	Forçar todos os arquivos programados.
`-id`	O número de identificação ou os identificadores separados por espaço dos arquivos programados que você quer forçar.

Exemplo:

Iniciar vários trabalhos de arquivamento programado:

```
>Start-ScheduledArchive -ids 799138c8-3dfc-4398-9711-1823733c2a31, 26c29bb7-b320-47f5-b5a8-dffc49f50e25
```

Start-VBExport

O comando `start-VBExport` inicia uma exportação virtual do ponto de recuperação selecionado para uma máquina virtual de servidor Oracle VirtualBox.

Os parâmetros necessários incluem o nome da máquina protegida que contém os pontos de recuperação a serem exportados; o nome da máquina virtual para a qual a exportação está sendo feita; a quantidade de RAM a ser alocada na máquina virtual; o nome de host e porta do host de servidor Linux; e o caminho para a pasta local, de rede ou de Linux na qual os arquivos de máquina virtual resultantes serão armazenados.

Forma de uso

A forma de uso do comando é a seguinte:

```
Start-VBExport -core -user [user name] -password [password] -protectedserver [machine name] or
[IP address]] -volumes [volume names] -rpn [number | numbers] |
-time [time string] -vmname [virtual machine name] [-ram [total megabytes] |
-usesourceram] -linuxhostname [linux hostname] -hostport [linux port] -targetpath [location]
pathusername [user name] - pathpassword [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Start-VBExport`:

Tabela 289. Opções do comando Start-VBExport

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.

Opção	Descrição
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Máquina protegida com pontos de recuperação a serem exportados.
`-volumes`	Opcional. Lista de nomes de volumes a serem exportados. Se não for especificado, todos os volumes nos pontos de recuperação especificados serão exportados. Os valores devem ser informados entre aspas duplas e cada um separado por um espaço. não use barras nos nomes dos volumes. Por exemplo, especifique "C:" e não "C:/"
`-rpn`	Opcional. O número sequencial de um ponto de recuperação a ser exportado. (Use o comando `Get-RecoveryPoints` para obter números de pontos de recuperação.) **NOTA: Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será exportado.**
`-time`	Opcional. Determina o ponto de recuperação a ser selecionado para exportação. Você precisa especificar a hora exata no formato "MM/DD/AAAA hh:mm tt" (por exemplo: "04/24/2015 09:00 AM"). Especifique valores de data e hora do fuso horário definido em sua máquina local. **NOTA: Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será exportado.**
`-vmname`	Nome do Windows da máquina virtual.
`-ram`	Alocar uma quantidade específica de RAM no servidor virtual.
`-usesourceram`	Opcional. Alocar a mesma quantidade de RAM no servidor virtual quanto na máquina de origem protegida.
`-linuxhostname`	Nome de host do servidor Linux VirtualBox.
`-hostport`	Porta do servidor Linux VirtualBox.
`-targetpath`	Caminho local, de rede ou de Linux para a pasta em que os arquivos da máquina virtual devem ser armazenados.
`-pathusername`	Nome de usuário da máquina de rede. Necessário apenas quando você especifica o caminho de rede no parâmetro `-targetpath`.
`-pathpassword`	Senha para a máquina da rede. Necessário apenas quando você especifica o caminho de rede no parâmetro `-targetpath`.
`-accountusername`	Opcional. Use caso possa especificar uma conta de usuário para registrar a máquina virtual exportada. Apenas para máquina local ou de rede.
`-accountpassword`	Opcional. Use apenas quando você especificar uma conta de usuário para registrar a máquina virtual exportada usando o parâmetro `-accountusername.` . Apenas para máquina local ou de rede.

Exemplo:

Exportar todos os volumes do último ponto de recuperação na máquina 10.10.12.97 para uma VM chamada NewVirtualBoxVM:

```
>Start-VBExport -protectedserver 10.10.12.97 -vmname NewVirtualBoxVM -ram usesourceram -
targetpath D:/exports
```

Start-VirtualStandby

O comando`Start-VirtualStandby` do PowerShell permite que você force uma exportação de dados para uma máquina de standby virtual através do Rapid Recovery. Essa exportação sob demanda poderá ocorrer fora das exportações de standby virtual programadas regularmente.

Forma de uso

A forma de uso do comando é a seguinte:

```
Start-VirtualStandby -core [host name] -user [login] -password [password] -all | -
protectedserver [name(s) | IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Start-VirtualStandby`:

Tabela 290. Opções do comando Start-VirtualStandby

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-all`	Force uma exportação para todas as máquinas de standby virtual.
`-protectedserver`	O nome ou os nomes, separados por vírgula e espaço, das máquinas protegidas cuja exportação você quer forçar.

Exemplo:

Forçar uma exportação de standby virtual para uma máquina protegida:

```
>Start-VirtualStandby -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22
```

Start-VMExport

O comando`Start-VMExport` inicia uma exportação virtual do ponto de recuperação selecionado para uma máquina virtual de servidor VMware Workstation.

Os parâmetros necessários incluem o nome da máquina protegida que contém os pontos de recuperação a serem exportados; o nome da máquina virtual para a qual a exportação está sendo feita; a quantidade de RAM a ser alocada na máquina virtual; e o caminho para a pasta local ou de rede na qual os arquivos de máquina virtual resultantes serão armazenados.

Forma de uso

A forma de uso do comando é a seguinte:

```
Start-VMExport -core -user [user name] -password [password] -protectedserver [machine name] or
[IP address]] -volumes [volume names] -rpn [number | numbers] |
-time [time string] -vmname [virtual machine name] [-ram [total megabytes] |
-usesourceram] -linuxhostnme [linux hostname] -hostport [linux port] -targetpath [location]
pathusername [user name] - pathpassword [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Start-VMExport`:

Tabela 291. Opções do comando Start-VMExport

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Máquina protegida com pontos de recuperação a serem exportados.
`-volumes`	Opcional. Lista de nomes de volumes a serem exportados. Se não for especificado, todos os volumes nos pontos de recuperação especificados serão exportados. Os valores devem ser informados entre aspas duplas e separados por um espaço. Não use barras nos nomes dos volumes. Por exemplo, especifique "C:" e não "C:/"
`-rpn`	Opcional. O número sequencial de um ponto de recuperação a ser exportado. Use o comando`Get-RecoveryPoints` para obter números de pontos de recuperação. **NOTA: Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será exportado.**
`-time`	Opcional. Determina o ponto de recuperação a ser selecionado para exportação. Você deve especificar o tempo exato no formato "MM/DD/AAAA hh:mm tt" (por exemplo: "04/24/2015 09:00 AM"). Especificar os valores de data e hora do fuso horário definido na sua máquina local.

Opção	Descrição
	NOTA: Se nenhuma opção "time" ou "rpn" for especificada neste comando, o ponto de recuperação mais recente será exportado.
`-vmname`	Nome do Windows da máquina virtual.
`-ram`	Alocar uma quantidade específica de RAM no servidor virtual.
`-usesourceram`	Opcional. Alocar a mesma quantidade de RAM no servidor virtual quanto na máquina de origem protegida.
`-targetpath`	Caminho local, de rede ou de Linux para a pasta em que os arquivos da máquina virtual devem ser armazenados.
`-pathusername`	Nome de usuário da máquina de rede. Necessário apenas quando você especifica o caminho de rede no parâmetro `-targetpath`.
`-pathpassword`	Senha para a máquina da rede. Necessário apenas quando você especifica o caminho de rede no parâmetro `-targetpath`.
`-version`	Versão do VMware Tools a ser usada. As versões válidas são: 7, 8, 9 e 10.

Exemplo:

Exportar todos os volumes do último ponto de recuperação na máquina 10.10.12.97 para uma VM chamada NewVMwareVM:

```
>Start-VBExport -protectedserver 10.10.12.97 -vmname NewVMWareVM -ram usesourceram -targetpath
D:/exports
```

Stop-ActiveJobs

O comando `Stop-ActiveJobs` cancela os trabalhos ativos de uma máquina protegida especificada.

Forma de uso

A forma de uso do comando é a seguinte:

```
Stop-ActiveJobs [-protectedserver [machine name | IP address] | -core [host name]] -user [user
name] -password [password] -jobtype [jobtype]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Stop-ActiveJobs`:

Tabela 292. Opções do comando Stop-ActiveJobs

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-all`	Selecionar e cancelar eventos do tipo especificado em todas as máquinas protegidas.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.

Opção	Descrição
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-protectedserver	Determina a máquina protegida na qual os trabalhos serão cancelados.
-jobtype	Opcional. Especifica o filtro do tipo de trabalho. Os valores disponíveis são: "transfer" (transferência de dados), "repository" (manutenção do repositório), "replication" (replicações locais e remotas), "backup" (cópia de segurança e restauração), "bootcdbuilder" (criar CDs de inicialização), "diagnostics" (carregar logs), "exchange" (verificação de arquivos do Exchange Server), "export" (exportação de ponto de recuperação), "pushinstall" (implementar software Agent em máquinas protegidas), “rollback" (restaurar dados de um ponto de recuperação), "rollup" (rollups de ponto de recuperação), "sqlattach" (verificações de capacidade de anexação de agente), "mount" (não repositório). Como padrão, todos os trabalhos do tipo especificado são cancelados.

Exemplo:

Interromper o trabalho de transferência na máquina protegida:

```
>Stop-ActiveJobs -protectedserver 10.10.1.76 -jobtype transfer
```

Interromper todos os trabalhos para uma máquina protegida específica:

```
>Stop-ActiveJobs -protectedserver 10.10.1.76 -all
```

Suspend-Replication

O comando`Suspend-Replication` permite que um administrador pause a replicação.

Um usuário pode pausar uma replicação de três maneiras:

- Pausar a replicação no Core mestre de todas as máquinas protegidas (`-outgoing parameter`)

  O administrador precisa especificar o nome da máquina remota com o emparelhamento de replicação de saída para pausar a replicação de saída no Core mestre.

  ```
  >Suspend-replication -outgoing 10.10.12.10
  ```
- Pausar a replicação no Core mestre de uma única máquina protegida (parâmetro `-protectedserver`)

  ```
  >Suspend-replication -protectedserver 10.10.12.97
  ```
- Pausar a replicação no Core de destino (`-incoming parameter`)

  Se o Core local é um Core de destino, o administrador pode pausar a replicação especificando o Core mestre usando o parâmetro –incoming.

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Suspend-Replication`:

Tabela 293. Opções do comando Suspend-Replication

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-all`	Pausa todas as máquinas protegidas no Core selecionado.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-pause`	`[snapshots],[replication]` ou `[vmexport]`.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-protectedserver`	Pausar o servidor protegido atual.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-incoming`	Nome do host do Core remoto que replica para a máquina Core. A replicação de todas as máquinas protegidas no Core remoto é suspensa.
`-outgoing`	Nome de host do Core de destino remoto no qual os dados são replicados. A replicação de todas as máquinas protegidas no Core remoto é suspensa.

Exemplo:

Pausar uma replicação de saída no Core remota com o endereço IP: 10.10.1.15 para a única máquina protegida com o endereço IP: 10.10.1.76:

```
>Suspend-replication -core 10.10.1.15 -protectedserver 10.10.1.76
```

Pausar a replicação de saída no Core local para o destino remoto com o endereço IP: 10.10.1.63 para todas as máquinas protegidas:

```
>Suspend-replication -outgoing 10.10.1.63
```

Pausar uma replicação de entrada do 10.10.1.82 no Core remoto com o endereço IP: 10.10.1.15 (o administrador pode pausar a replicação de entrada somente para toda a máquina):

```
>Suspend-replication -core 10.10.1.15 -incoming 10.10.1.82
```

Suspend-RepositoryActivity

O comando`Suspend-RepositoryActivity` do PowerShell permite que você pause as atividades de um repositório do Rapid Recovery. Suspender as atividades coloca uma trava no repositório, impedindo a entrada e a saída de dados.

Forma de uso

A forma de uso do comando é a seguinte:

```
Suspend-RepositoryActivity -core [host name] -user [login] -password [password] -all | -
repository ["name" | "name1 " "name2"]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Suspend-RepositoryActivity`:

Tabela 294. Opções do comando Suspend-RepositoryActivity

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-all`	Suspende as atividades de todos os repositórios associados a esse Core.
`-repository`	O nome do repositório que você deseja bloquear. O nome deve ser informado entre aspas duplas. Você pode especificar vários repositórios separados por espaço.

Exemplos:

Suspender as atividades de vários repositórios:

```
>Suspend-RepositoryActivity -repository "repository1" "repository2"
```

Suspender as atividades em todos os repositórios:

```
>Suspend-RepositoryActivity -all
```

Suspend-ScheduledArchive

O comando`Suspend-ScheduledArchive` do PowerShell permite que você pause um arquivamento programado do Rapid Recovery. Este comando impede que o arquivamento ocorra conforme programado até você reativá-lo..

Forma de uso

A forma de uso do comando é a seguinte:

```
Suspend-ScheduledArchive -core [host name] -user [login] -password [password] -all -ids [id |
id1 id2]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Suspend-ScheduledArchive`:

Tabela 295. Opções do comando Suspend-ScheduledArchive

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-all`	Pausa todos os arquivos programados.
`-id`	O número de identificação ou os números separados por espaço dos arquivos programados a serem suspensos.

Exemplo:

Suspender múltiplos arquivos programados:

```
>Suspend-ScheduledArchive -ids 799138c8-3dfc-4398-9711-1823733c2a31, 26c29bb7-b320-47f5-b5a8-dffc49f50e25
```

Suspend-Snapshot

O comando`Suspend-Snapshot` permite que um administrador pause snapshot.

Forma de uso

A forma de uso do comando é a seguinte:

```
Suspend-Snapshot -core [host name] -user [user name] -password [password] -all |
-protectedserver [name | IP address] -time [time string]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Suspend-Snapshot`:

Tabela 296. Opções do comando Suspend-Snapshot

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-all`	Pausa todas as máquinas protegidas no Core selecionado.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-time`	O horário no formato `'Day-Hours-Minutes'` em que os snapshots serão retomados (somente para pausas de snapshots).

Exemplo:

Pausar snapshots da máquina protegida com o IP 10.10.10.4 para o Core local, com retomada em um determinado horário:

```
>Suspend-Snapshot -protectedserver 10.10.10.4 -time 3-20-50
```

Suspend-VirtualStandby

O comando`Suspend-VirtualStandby` do PowerShell permite pausar a exportação de dados para uma máquina de standby virtual do Rapid Recovery.

Forma de uso

A forma de uso do comando é a seguinte:

```
Suspend-VirtualStandby -core [host name] -user [login] -password [password] -all | -
protectedserver [name(s) | IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Suspend-VirtualStandby`:

Tabela 297. Opções do comando Suspend-VirtualStandby

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.

Opção	Descrição
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um logon. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-all`	Pausar as exportações para todas as máquinas de standby virtual.
`-protectedserver`	O nome ou os nomes, separados por vírgula e espaço, das máquinas protegidas com as máquinas de standby virtual que você quer suspender.

Exemplo:

Suspender exportações de standby virtual para uma máquina protegida:

```
>Suspend-VirtualStandby -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22
```

Suspend-VMExport

O comando `Suspend-VMExport` permite que um administrador pause as exportações para máquinas virtuais.

Forma de uso

```
Suspend-VMExport -core [host name] -user [user name] -password [password] -all | -
protectedserver [name | IP address]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando `Suspend-VMExport`:

Tabela 298. Opções do comando Suspend-VMExport

Opção	Descrição
`-?`	Exibir esta mensagem de ajuda.
`-core`	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
`-user`	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-password`	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
`-all`	Pausa todas as máquinas protegidas no Core selecionado.

Opção	Descrição
-protectedserver	Pausar o servidor protegido atual.

Exemplo:

Suspender a exportação de VM da máquina protegida com IP 10.10.10.4 para o Core local:

```
>Suspend-VMExport -protectedserver 10.10.12.25
```

Update-Repository

O comando`Update-Repository` adiciona uma extensão a um repositório de DVM existente. O tamanho especificado deve estar entre 250 MB e 16 TB.

Forma de uso

```
Update-Repository -name [repository name] -size [size] [[[-datapath [datapath]
-metadatapath [metadata path]] | [-uncpath [UNC path] -shareusername [share user name] -
sharepassword [share password]]] -core [host name] -user [user name]
-password [password]
```

Opções do comando

A tabela a seguir descreve as opções disponíveis para o comando`Update-Repository`:

Tabela 299. Opções do comando Update-Repository

Opção	Descrição
-?	Exibir esta mensagem de ajuda.
-core	Opcional. Endereço IP da máquina de host do Core remoto (com um número de porta opcional). Por padrão, a conexão é feita com o Core instalado na máquina local.
-user	Opcional. Nome de usuário para a máquina host do Core remoto. Se você especificar um nome de usuário, também deverá fornecer uma senha. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-password	Opcional. Senha para a máquina de host de Core remoto. Se você especificar uma senha, também deverá fornecer um nome de usuário. Se nada for fornecido, então as credenciais do usuário conectado serão usadas.
-name	Nome do repositório de DVM.
-size	Tamanho da extensão do repositório de DVM. As unidades disponíveis são: b, Kb, MB, GB, TB, PB.
-datapath	Para espaço local, somente. Determina o caminho dos dados da extensão do repositório de DVM.
-metadatapath	Para espaço local, somente. Determina o caminho dos metadados da extensão do repositório de DVM.
-uncpath	Para local partilhado, somente. Determina o caminho dos dados e metadados da extensão do repositório de DVM.
-shareusername	Para local partilhado, somente. Determinar login para local partilhado.

Opção	Descrição
`-sharepassword`	Para local partilhado, somente. Determinar senha para local partilhado.

Exemplo:

Adicionar ao repositório de DVM uma extensão do tamanho mínimo:

```
>Update-Repository -name Repository1 -size 250Mb -datapath C:\Repository\Data -metadatapath C:
\repository\Metadata
```

Localização

Quando é executado na mesma máquina em que o Rapid Recovery Core está instalado, o módulo Rapid Recovery PowerShell usa como idioma de exibição o idioma definido para o Core. As versões localizadas do Rapid Recovery como esta suportam inglês, chinês (simplificado), francês, coreano, alemão, japonês, português (Brasil) e espanhol.

Se o módulo Rapid Recovery PowerShell estiver instalado em uma máquina separada, o idioma inglês é o único compatível.

Qualificadores

A tabela a seguir descreve os qualificadores disponíveis para o Módulo Rapid Recovery PowerShell.

Tabela 300. Qualificadores de módulo Rapid Recovery PowerShell

Qualificador	Forma de uso
`-core <Rapid Recovery Core Name>`	Nome do host do Core. Padrão:`Localhost`
`-ProtectedServer <Protected Server Name>`	Nome do host/endereço IP do agente Rapid Recovery. Padrão:`Localhost` se vários servidores estiverem protegidos; caso contrário, o único servidor protegido.
`-Mode <READ, READWRITE, WRITE>`	Modo de montagem do ponto de recuperação. Padrão:`Read`.
`-Volumes <Snapshot Volume Letter>`	Letra do volume do snapshot do agente Rapid Recovery. Padrão:`All`.
`-User <User Name>`	Nome de usuário usado para se conectar ao Rapid Recovery Core. Normalmente é o usuário de serviço.
`-Domain <Domain Name>`	Domínio ao qual pertence o usuário definido em /User.
`-Password <Password>`	Senha do usuário definida em`/User`.
`-Path <Target path to mount, dismount recovery points or archive location>`	Por exemplo:`C:\RapidRecoveryMount`.

C

Prolongamento dos trabalhos do Rapid Recovery usando scripts

O Rapid Recovery permite aos administradores automatizar a administração e o gerenciamento de recursos em determinadas ocorrências pela execução de comandos e scripts. O software Rapid Recovery suporta o uso de script de PowerShell para Windows e script de Bourne Shell para Linux.

Os trabalhos do Core são criados automaticamente quando você inicia operações no Rapid Recovery Core, como replicação, exportação virtual ou snapshot de cópia de segurança. Você pode estender esses trabalhos executando um script antes ou depois deles. Esses scripts são chamados de pré-script e pós-script.

Esta seção descreve os scripts que podem ser usados por administradores em ocorrências designadas no Rapid Recovery para Windows e Linux.

CUIDADO: Os exemplos de script PowerShell e Bourne oferecidos neste documento funcionarão quando forem executados conforme projetado por administradores qualificados. Tome cuidado ao modificar scripts de funcionamento para manter versões de trabalho. Qualquer modificação nos exemplos de script incluídos aqui ou qualquer script que você criar são considerados como uma personalização, que normalmente não é coberta pelo suporte da Dell.

Tópicos:

- Usar scripts PowerShell no Rapid Recovery
- Parâmetros de entrada do PowerShell Scripting
- Exemplos de scripts PowerShell
- Usar scripts do Bourne Shell no Rapid Recovery
- Parâmetros de entrada para scripts do Bourne Shell
- Exemplos de scripts do Bourne Shell

Usar scripts PowerShell no Rapid Recovery

O Windows PowerShell é um ambiente conectado ao Microsoft .NET Framework projetado visando a automação administrativa. O Rapid Recovery inclui kits abrangentes de desenvolvimento de software cliente (SDKs) para PowerShell Scripting que permitem aos usuários administrativos executar scripts PowerShell fornecidos pelo usuário em ocorrências designadas; por exemplo, antes ou depois de um snapshot, de verificações de capacidade de anexação e montabilidade e assim por diante. Os administradores podem executar scripts a partir do Rapid Recovery Core e da máquina protegida. Os scripts podem aceitar parâmetros e a saída de um script é gravada nos arquivos de log do Core e da máquina protegida.

NOTA: Para trabalhos noturnos, preserve um arquivo de script e o parâmetro de entrada JobType para distinguir entre trabalhos noturnos.

Os arquivos de script estão localizados na pasta **%ALLUSERSPROFILE%\AppRecovery\Scripts**.

- No Windows 7, o caminho para localizar a pasta %ALLUSERSPROFILE% é: **C:\ProgramData**.
- No Windows 2003, o caminho para localizar a pasta é: **Documents and Settings\All Users\Application Data**.

NOTA: É necessário que o Windows PowerShell esteja instalado e configurado antes de executar scripts do Rapid Recovery.

Para obter mais informações sobre como usar os scripts do PowerShell consulte Exemplos de scripts PowerShell, Parâmetros de entrada do PowerShell Scripting, Parâmetros de entrada para scripts do Bourne Shell e Exemplos de scripts do Bourne Shell.

Pré-requisitos para PowerShell Scripting

Antes de executar scripts do PowerShell no Rapid Recovery é necessário instalar o Windows PowerShell 2.0 ou posterior. Devido a novos recursos introduzidos no PowerShell 3.0, incluindo acesso mais fácil a propriedades de objeto, acesso a PowerShell Web e suporte a chamadas REST, a Dell recomenda usar o PowerShell 3.0 ou posterior.

NOTA: Coloque o arquivo powershell.exe.config no diretório base do PowerShell. Por exemplo, C:\WindowsPowerShell \powershell.exe.config.

powershell.exe.config

```
<?xml version="1.0"?>
<configuration>
    <startup useLegacyV2RuntimeActivationPolicy="true">
        <supportedRuntime version="v4.0.30319"/>
        <supportedRuntime version="v2.0.50727"/>
    </startup>
</configuration>
```

Teste dos scripts do PowerShell

Se desejar testar os scripts que pretende executar, poderá fazê-lo usando o editor gráfico do PowerShell, o powershell_is. Também é preciso adicionar o arquivo de configuração, powershell_ise.exe.config na mesma pasta do arquivo de configuração, powershell.exe.config.

NOTA: O arquivo de configuração, powershell_ise.exe.config, deve ter o mesmo conteúdo do arquivo powershell.exe.config.

CUIDADO: Se o script pré-PowerShell ou pós-PowerShell falhar, o trabalho também falhará.

Localização

Quando é executado na mesma máquina em que o Rapid Recovery Core está instalado, o módulo Rapid Recovery PowerShell usa como idioma de exibição o idioma definido para o Core. Versões localizadas do Rapid Recovery como esta têm suporte para inglês, chinês (simplificado), francês, coreano, alemão, japonês, português (brasileiro) e espanhol.

Se o módulo Rapid Recovery PowerShell estiver instalado em uma máquina separada, o idioma inglês é o único suportado.

Qualificadores

A tabela a seguir descreve os qualificadores disponíveis para o Módulo Rapid Recovery PowerShell.

Tabela 301. Qualificadores de módulo Rapid Recovery PowerShell

Qualificador	Forma de uso
`-core <Rapid Recovery Core Name>`	Nome do host do Core.

Qualificador	Forma de uso
	Padrão:`Localhost`
`-ProtectedServer <Protected Server Name>`	Nome do host/endereço IP do agente Rapid Recovery. Padrão:`Localhost` se vários servidores estiverem protegidos; caso contrário, o único servidor protegido.
`-Mode <READ, READWRITE, WRITE>`	Modo de montagem do ponto de recuperação. Padrão:`Read`.
`-Volumes <Snapshot Volume Letter>`	Letra do volume do snapshot do agente Rapid Recovery. Padrão:`All`.
`-User <User Name>`	Nome de usuário usado para se conectar ao Rapid Recovery Core. Normalmente é o usuário de serviço.
`-Domain <Domain Name>`	Domínio ao qual pertence o usuário definido em /User.
`-Password <Password>`	Senha do usuário definida em`/User`.
`-Path <Target path to mount, dismount recovery points or archive location>`	Por exemplo:`C:\RapidRecoveryMount`.

Parâmetros de entrada do PowerShell Scripting

Todos os parâmetros de entrada disponíveis são usados em scripts de exemplo. Os parâmetros estão descritos nas tabelas a seguir.

NOTA: Os arquivos de script devem possuir o mesmo nome dos arquivos de script de exemplo.

AgentProtectionStorageConfiguration (espaço de nomes Replay.Common.Contracts.Agents)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro AgentProtectionStorageConfiguration.

Tabela 302. Objetos para o parâmetro AgentProtectionStorageConfiguration

Método	Descrição
public Guid RepositoryId { get; set; }	Obtém ou define o ID do repositório onde os pontos de recuperação do Agent estão armazenados.
public string EncryptionKeyId { get; set; }	Obtém ou define o ID da chave de criptografia dos pontos de recuperação do Agent. Uma cadeia de caracteres vazia significa nenhuma criptografia.

AgentTransferConfiguration (espaço de nomes Replay.Common.Contracts.Transfer)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro AgentTransferConfiguration.

Tabela 303. Objetos para o parâmetro AgentTransferConfiguration

Método	Descrição
public uint MaxConcurrentStreams { get; set; }	Obtém ou define o número máximo de conexões TCP simultâneas que o Core estabelece com o Agent para transferência de dados.
public uint MaxTransferQueueDepth { get; set; }	Obtém ou define o número máximo de extensões de bloco que podem ser colocadas em fila para gravação. Quando um intervalo de blocos é lido de um fluxo de transferência, esse intervalo é colocado em uma fila de produtor ou consumidor, onde um thread de consumidor o lê e grava no objeto epoch. Se o repositório grava mais lentamente do que a rede lê, essa fila fica cheia. O ponto em que a fila está cheia e a leitura é interrompida é a extensão máxima da fila de transferência.
public uint MaxConcurrentWrites { get; set; }	Obtém ou define o número máximo de operações de gravação de blocos pendentes em um epoch em qualquer momento. Se blocos adicionais forem recebidos além do número máximo de operações de gravação especificado nesse parâmetro, esses blocos adicionais serão ignorados até uma das gravações pendentes ser concluída.
public ulong MaxSegmentSize { get; set; }	Obtém ou define o número máximo de blocos contíguos que serão transferidos em uma única solicitação. Dependendo do teste, valores mais altos ou mais baixos podem ser ideais.
public Priority Priority { get; set; }	Obtém ou define a prioridade da solicitação de transferência.
public uint GetChangedBlocksRetries { get; set; }	Obtém ou define a contagem de novas tentativas caso haja falha na recuperação inicial de blocos alterados no agente.
public int MaxRetries { get; set; }	Obtém ou define o número máximo de vezes que uma transferência com falha deve ser tentada novamente antes de ser considerada como falha.
public bool UseDefaultMaxRetries { get; set; }	Se for incluído, o número máximo de novas tentativas padrão (especificado na configuração da transferência) será usado.
public Guid ProviderId{ get; set; }	Obtém ou define o GUID do provedor de VSS que será usado para snapshots neste host. Os administradores em geral aceitam o padrão.
public Collection<ExcludedWriter> ExcludedWriterIds { get; set; }	Obtém ou define o conjunto de IDs de gravação do VSS que devem ser excluídos desse snapshot. O ID do gravador é determinado pelo nome do gravador. Esse nome se destina apenas a fins de documentação e não necessariamente fornece uma correspondência exata do nome de gravação.
public ushort TransferDataServerPort { get; set; }	Obtém ou define um valor que contém a porta TCP na qual as conexões são aceitas pelo Core para a transferência real de dados da máquina protegida para o Core. O Agent tenta escutar essa porta, mas caso ela esteja em uso, ele pode usar uma porta diferente. O Core deve usar o número de porta especificado nas propriedades BlockHashesUri e BlockDataUri do objeto VolumeSnapshotInfo para cada volume expandido.
public TimeSpan CleanSnapshotTimeout { get; set; }	Obtém ou define o tempo de espera de limpeza do snapshot após a conclusão da transferência.
public TimeSpan SnapshotTimeout { get; set; }	Obtém ou define o tempo de espera para que uma operação de snapshot do VSS seja concluída antes que ela seja abandonada e expire.

Método	Descrição
public TimeSpan TransferTimeout { get; set; }	Obtém ou define o tempo de espera para contatos adicionais do Core antes de abandonar o snapshot.
public TimeSpan NetworkReadTimeout { get; set; }	Obtém ou define o tempo limite para operações de leitura de rede relacionadas a essa transferência.
public TimeSpan NetworkWriteTimeout { get; set; }	Obtém ou define o tempo limite para operações de gravação de rede relacionadas a essa transferência.
public uint InitialQueueSize { get; set; }	Obtém ou define um tamanho de fila ou solicitações iniciais.
public uint MinVolumeFreeSpacePercents { get; set; }	Obtém ou define um valor mínimo de espaço livre em um volume, medido por porcentagem. Caso o espaço livre seja menor que o valor especificado nesse parâmetro, todos os logs de alteração são excluídos e uma imagem de base é forçada.
public uint MaxChangeLogsSizePercents { get; set; }	Obtém ou define um tamanho máximo de logs de alteração do driver como parte da capacidade de volume, medido por porcentagem. Caso parte dos logs de alteração seja maior do que esse valor, todos os logs de alteração são excluídos e uma imagem de base é forçada.
public bool EnableVerification { get; set; }	Obtém ou define um valor indicando se a verificação de diagnóstico de cada bloco enviado para o Core deve ser realizada.

BackgroundJobRequest (espaço de nomes Replay.Core.Contracts.BackgroundJobs)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro BackgroundJobRequest.

Tabela 304. Objetos para o parâmetro BackgroundJobRequest

Método	Descrição
public AgentIdsCollection AgentIds { get; set; }	Obtém ou define os IDs das máquinas protegidas.
public bool IsNightlyJob { get; set; }	Obtém ou define o valor que indica se o trabalho em segundo plano é um trabalho noturno.
public Guid NightlyJobTransactionId { get; set; }	Obtém ou define o ID da transação de trabalho noturno.
public Guid JobId { get; set; }	Obtém ou define o ID do trabalho em segundo plano.
public bool Force { get; set; }	Obtém ou define o valor que indica se um trabalho foi forçado.
public uint JobStartsCount { get; set; }	Obtém ou define o número de tentativas para iniciar um trabalho.
public virtual bool InvolvesAgentId(Guid agentId)	Determina o valor que indica se o Agent concreto está envolvido no trabalho.

ChecksumCheckJobRequest (espaço de nomes Replay.Core.Contracts.Exchange.ChecksumChecks)

Herda seus valores do parâmetro DatabaseCheckJobRequestBase.

DatabaseCheckJobRequestBase (espaço de nomes Replay.Core.Contracts.Exchange)

Herda seus valores do parâmetro, BackgroundJobRequest.

Tabela 305. Objetos para o parâmetro DatabaseCheckJobRequestBase

Método	Descrição
public string RecoveryPointId { get; set; }	Obtém ou define o ID do ponto de recuperação para o qual os bancos de dados serão verificados.

ExportJobRequest (espaço de nomes Replay.Core.Contracts.Export)

Herda seus valores do parâmetro, BackgroundJobRequest.

A tabela a seguir apresenta os objetos disponíveis para o parâmetro ExportJobRequest.

Tabela 306. Objetos para o parâmetro ExportJobRequest

Método	Descrição
public uint RamInMegabytes { get; set; }	Obtém ou define o tamanho da memória para a VM exportada. Defina como zero (0) para usar o tamanho da memória da máquina de origem.
public ushort CpuCount { get; set; }	Obtém ou define a contagem de CPUs para a VM exportada. Defina como 0 para usar a contagem de CPUs da máquina de origem.
public ushort CoresPerCpu { get; set; }	Obtém ou define a contagem de cores por CPU para a VM exportada. Defina como 0 para usar a contagem de cores por CPU da máquina de origem.
public VirtualMachineLocation Location { get; set; }	Obtém ou define o local de destino dessa exportação. Trata-se de uma classe de base abstrata.
public VolumeImageIdsCollection VolumeImageIds { get; private set; }	Obtém ou define as imagens de volume a incluir na exportação da VM.
public ExportJobPriority Priority { get; set; }	Obtém ou define a prioridade da solicitação de exportação.

NightlyAttachabilityJobRequest (espaço de nomes Replay.Core.Contracts.Sql)

Herda seus valores do parâmetro, BackgroundJobRequest.

Tabela 307. Objetos para o parâmetro NightlyAttachabilityJobRequest

Método	Descrição
public int SimultaneousJobsCount { get; set; }	Obtém ou define a contagem de trabalhos que podem ser executados simultaneamente.

RollupJobRequest (espaço de nomes Replay.Core.Contracts.Rollup)

Herda seus valores do parâmetro, BackgroundJobRequest.

TakeSnapshotResponse (espaço de nomes Replay.Agent.Contracts.Transfer)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro TakeSnapshotResponse.

Tabela 308. Objetos para o parâmetro TakeSnapshotResponse

Método	Descrição
public Guid SnapshotSetId { get; set; }	Obtém ou define o GUID atribuído pelo VSS a este snapshot.
public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }	Obtém ou define o conjunto de informações do snapshot para cada volume incluído no snapshot.

TransferJobRequest (espaço de nomes Replay.Core.Contracts.Transfer)

Herda seus valores do parâmetro, BackgroundJobRequest.

A tabela a seguir apresenta os objetos disponíveis para o parâmetro TransferJobRequest.

Tabela 309. Objetos para o parâmetro TransferJobRequest

Método	Descrição
public VolumeNameCollection VolumeNames { get; set; }	Obtém ou define o conjunto de nomes para transferência. VolumeNames é uma estrutura de dados que contém os seguintes dados: • GuidName. O GUID associado ao volume, usado como o nome caso DisplayName não tenha sido definido. • DisplayName. O nome de exibição do volume.
public VolumeNameCollection TransferredVolumes { get; set; }	Obtém ou define o conjunto de volumes transferidos.
public VolumeNameCollection DependentVolumeNames { get; set; }	Obtém ou define o conjunto de volumes dependentes.

Método	Descrição
public QuotaSettingsCollection EnabledDiskQuotas { get; set; }	Obtém ou define cotas ativadas em um volume.
public ShadowCopyType ShadowCopyType { get }	Obtém o tipo de cópia da transferência. Os valores disponíveis são: • Copy • Full

public AgentTransferConfiguration TransferConfiguration { get; set; }	Obtém ou define a configuração da transferência.
	AgentTransferConfiguration é um objeto que terá os seguintes dados:
	• MaxConcurrentStreams. O número máximo de conexões TCP simultâneas que o Core estabelecerá com o agente para transferir dados
	• MaxTransferQueueDepth. O número máximo de extensões de bloco que podem ser enfileiradas para gravação
	• MaxConcurrentWrites. O número máximo de operações de gravação de bloco pendentes em uma época a qualquer momento. Se blocos adicionais forem recebidos quando essa quantidade de gravações de blocos estiver pendente, esses blocos adicionais serão ignorados até que um dos blocos pendentes seja gravado.
	• MaxSegmentSize. O número máximo de blocos contíguos que serão transferidos em uma única solicitação
	• Priority. Um objeto que terá os seguintes dados:
	  • Undefined
	  • One
	  • Two
	  • Three
	  • Four
	  • Five
	  • Six
	  • Seven
	  • Eight
	  • Nine
	  • Ten
	  • Highest (which is equal to One)
	  • Lowest (which is equal to Ten)
	  • Default (which is equal to Five)
	• MaxRetries. O número máximo de vezes que uma transferência deve ser tentada novamente antes de ser considerada como falha
	• UseDefaultMaxRetries. Um valor indicando que o número máximo de tentativas é o valor padrão
	• ProviderId. O GUID do provedor de VSS que será usado para snapshots nesse host. Os usuários geralmente usam a definição padrão.

public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }	Obtém ou define a configuração do armazenamento.
public string Key { get; set; }	Gera uma chave pseudoaleatória (mas não criptograficamente segura), que pode ser usada como senha única para autenticar solicitações de transferência.
public bool IsBaseImage { get; set; }	Obtém ou define o valor que indica se a imagem de base será feita.
public bool IsForced { get; set; }	Obtém ou define o valor que indica se a transferência foi forçada.
public Guid ProtectionGroupId { get; set; }	Obtém ou define o ID do grupo de proteção.
public TargetComponentTypes LogTruncationTargets { get; set; }	Obtém ou define o valor que indica para quais bancos de dados o truncamento de log será realizado (SQL ou Exchange).

Método	Descrição
public bool ForceBaseImage { get }	Obtém o valor que indica se a imagem de base foi forçada ou não.
public bool IsLogTruncation { get }	Obtém o valor que indica se o trabalho de truncamento de log está sendo realizado ou não.

TransferPrescriptParameter (espaço de nomes Replay.Common.Contracts.PowerShellExecution)

Herda seus valores do parâmetro TransferScriptParameterBase.

TransferPostscriptParameter (espaço de nomes Replay.Common.Contracts.PowerShellExecution)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro TransferPostscript. Herda seu valor do parâmetro TransferScriptParameterBase.

Tabela 310. Objetos para o parâmetro TransferPostscript

Método	Descrição
public VolumeNameCollection VolumeNames (get; set;)	Obtém ou define o conjunto de nomes de volume para transferência. VolumeNames é uma estrutura de dados que contém os seguintes dados: • GuidName. O GUID associado ao volume, usado como o nome caso DisplayName não tenha sido definido. • DisplayName. O nome de exibição do volume.
public ShadowCopyType ShadowCopyType { get; set; }	Obtém ou define o tipo de cópia da transferência. ShadowCopyType é uma enumeração com valores. Os valores disponíveis são: • Unknown • Copy • Full
public AgentProtectionStorageConfigurationCommon StorageConfiguration { get; set; }	Obtém ou define a configuração do armazenamento.
public AgentTransferConfiguration TransferConfiguration { get; set; }	Obtém ou define a configuração da transferência. AgentTransferConfiguration é um objeto que terá os seguintes dados: • MaxConcurrentStreams. O número máximo de conexões TCP simultâneas que o Core estabelecerá com o agente para transferir dados • MaxTransferQueueDepth. O número máximo de extensões de bloco que podem ser enfileiradas para gravação • MaxConcurrentWrites. O número máximo de operações de gravação de bloco pendentes em uma época a qualquer momento. Se blocos adicionais forem recebidos quando essa quantidade de gravações de blocos estiver pendente, esses blocos adicionais serão ignorados até que um dos blocos pendentes seja gravado. • MaxSegmentSize. O número máximo de blocos contíguos que serão transferidos em uma única solicitação • Priority. Um objeto que tem os seguintes dados:

Método	Descrição
	• “Indefinido • “Um • “Dois • “Três • “Quatro • “Cinco • “Seis • “Sete • “Oito • “Nove • “Dez • “Mais alto (é igual a Um) • “Mais baixo (igual a Dez) • “Padrão (igual a Cinco) • MaxRetries. O número máximo de vezes que uma transferência deve ser tentada novamente antes de ser considerada como falha • UseDefaultMaxRetries. Um valor indicando que o número máximo de tentativas é o valor padrão • ProviderId. O GUID do provedor de VSS que será usado para snapshots nesse host. Os administradores em geral aceitam o padrão.
public AgentTransferConfiguration TransferConfiguration { get; set; } (cont.)	• ExcludedWriterIds. Conjunto de IDs de gravador de VSS que devem ser excluídos desse snapshot. O ID do gravador é determinado pelo nome do gravador. Esse nome é apenas para fins de documentação e não precisa corresponder exatamente ao nome real do gravador. • TransferDataServerPort. Um valor contendo a porta TCP em que serão aceitas conexões do Core para a transferência efetiva de dados do agente para o Core. • SnapshotTimeout. Tempo de espera para que uma operação de snapshot de VSS seja concluída antes que ela seja abandonada e expire. • TransferTimeout. Tempo de espera por contatos adicionais do Core antes de abandonar o snapshot. • NetworkReadTimeout. O tempo limite para operações de leitura de rede relacionadas a essa transferência. • NetworkWriteTimeout. O tempo limite para operações de gravação de rede relacionadas a essa transferência. • InitialQueueSize. O tamanho da fila inicial de solicitações. • MinVolumeFreeSpacePercents. Quantidade mínima de espaço livre em um volume, expressa como uma porcentagem. • MaxChangeLogsSizePercents. Tamanho máximo dos registros de alterações de driver como parte da capacidade do volume, expresso como uma porcentagem. • EnableVerification. Um valor que indica se a verificação de diagnóstico de cada bloco enviado ao Core deve ser realizada.
public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }	Obtém ou define a configuração do armazenamento O objeto AgentProtectionStorageConfiguration contém os seguintes dados: • RepositoryId. Nome do repositório onde os pontos de recuperação desse agente serão armazenados • EncryptionKeyId. O ID da chave de criptografia para os pontos de recuperação desse agente. Uma cadeia de caracteres vazia significa nenhuma criptografia
public string Key { get; set; }	O método Key gera uma chave pseudoaleatória (mas não criptograficamente segura), que pode ser usada como senha única para autenticar solicitações de transferência.

Método	Descrição
public bool ForceBaseImage { get; set; }	Obtém ou define o valor que indica se a transferência foi uma captura de imagem de base forçada.
public bool IsLogTruncation { get; set; }	Obtém ou define o valor que indica se o registro está sendo truncado.
public uint LatestEpochSeenByCore { get; set; }	Obtém ou define o valor de epoch mais recente. O método LatestEpochSeenByCore é o número original do snapshot mais recentemente capturado pelo Core. Esse é o "número de epoch" atribuído pelo driver do filtro a este snapshot específico no momento em que ele foi capturado com o VSS.
public Guid SnapshotSetId { get; set; }	Obtém ou define o GUID atribuído pelo VSS a este snapshot.
public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }	Obtém ou define o conjunto de informações do snapshot para cada volume incluído no snapshot.

TransferScriptParameterBase (espaço de nomes Replay.Common.Contracts.PowerShellExecution)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro TransferScriptParameterBase.

Tabela 311. Objetos para o parâmetro TransferScriptParameterBase

Método	Descrição
public AgentTransferConfiguration TransferConfiguration { get; set; }	Obtém ou define a configuração da transferência.
public AgentProtectionStorageConfigurationCommon StorageConfiguration { get; set; }	Obtém ou define a configuração do armazenamento.

VirtualMachineLocation (espaço de nomes Replay.Common.Contracts.Virtualization)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro VirtualMachineLocation.

Tabela 312. Objetos para o parâmetro VirtualMachineLocation

Método	Descrição
public string Description { get; set;}	Obtém ou define uma descrição desse local legível para humanos.
public string Name { get; set;}	Obtém ou define o nome da VM.

VolumeImageIdsCollection (espaço de nomes Replay.Core.Contracts.RecoveryPoints)

Herda seus valores do parâmetro System.Collections.ObjectModel.Collection<string>.

VolumeName (espaço de nomes Replay.Common.Contracts.Metadata.Storage)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro VolumeName.

Tabela 313. Objetos para o parâmetro VolumeName

Método	Descrição
public string GuidName { get; set;}	Obtém ou define o ID do volume.
public string DisplayName { get; set;}	Obtém ou define o nome do volume.
public string UrlEncode()	Obtém uma versão do nome codificada como URL que pode ser passada adequadamente em uma URL. **NOTA: Existe um problema conhecido no .NET 4.0 WCF (https://connect.microsoft.com/VisualStudio/feedback/ViewFeedback.aspx?FeedbackID=413312), que impede os caracteres de escape de caminho de funcionar corretamente em um modelo de URI. Visto que o nome do volume contém '\' e '?', substitua os caracteres especiais '\' e '?' por outros caracteres especiais.**
public string GetMountName()	Retorna um nome para esse volume que é válido para a imagem do volume de montagem em alguma pasta.

VolumeNameCollection (espaço de nomes eplay.Common.Contracts.Metadata.Storage)

Herda seus valores do parâmetro System.Collections.ObjectModel.Collection<VolumeName>.

A tabela a seguir apresenta os objetos disponíveis para o parâmetro VolumeNameCollection.

Tabela 314. Objetos para o parâmetro VolumeNameCollection

Método	Descrição
public override bool Equals(object obj)	Determina se essa instância e um objeto especificado, que também deve ser um objeto VolumeNameCollection, têm o mesmo valor. (Substitui Object.Equals(Object).)
public override int GetHashCode()	Retorna o código hash de VolumeNameCollection. (Substitui Object.GetHashCode().)

VolumeSnapshotInfo (espaço de nomes Replay.Common.Contracts.Transfer)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro VolumeSnapshotInfo.

Tabela 315. Objetos para o parâmetro VolumeSnapshotInfo

Método	Descrição
public Uri BlockHashesUri { get; set;}	Obtém ou define o URI em que os hashes MD5 dos blocos de volume podem ser lidos.
public Uri BlockDataUri { get; set;}	Obtém ou define o URI em que os blocos de dados de volume podem ser lidos.

VolumeSnapshotInfoDictionary (espaço de nomes Replay.Common.Contracts.Transfer)

Herda seus valores do parâmetro System.Collections.Generic.Dictionary<VolumeName, VolumeSnapshotInfo>.

Exemplos de scripts PowerShell

Os exemplos de scripts a seguir são fornecidos para auxiliar os usuários administrativos na execução de scripts PowerShell.

Links relacionados

PreTransferScript.sh
PostTransferScript.ps1
PreExportScript.ps1
PostExportScript.ps1
PreNightlyJobScript.ps1
PostNightlyJobScript.ps1

PreTransferScript.ps1

O PreTransferScript é executado na máquina protegida antes da transferência de um snapshot.

Amostra de PreTransferScript

```
# receiving parameter from transfer job
param([object]$TransferPrescriptParameter)
# building path to Agent's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null
# Converting input parameter into specific object
$TransferPrescriptParameterObject = $TransferPrescriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPrescriptParameter];
# Working with input object. All echo's are logged
if($TransferPrescriptParameterObject -eq $null) {
        echo 'TransferPrescriptParameterObject parameter is null'
}
else {
        echo 'TransferConfiguration:'$TransferPrescriptParameterObject.TransferConfiguration
        echo 'StorageConfiguration:' $TransferPrescriptParameterObject.StorageConfiguration
}
```

PostTransferScript.ps1

O PostTransferScript é executado na máquina protegida após a transferência de um snapshot.

Amostra de PostTransferScript

```
# receiving parameter from transfer job
param([object] $TransferPostscriptParameter)
# building path to Agent's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null
# Converting input parameter into specific object
$TransferPostscriptParameterObject = $TransferPostscriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPostscriptParameter];
# Working with input object. All echo's are logged
if($TransferPostscriptParameterObject -eq $null) {
            echo 'TransferPostscriptParameterObject parameter is null'
}
else {
echo 'VolumeNames:' $TransferPostscriptParameterObject.VolumeNames
            echo 'ShadowCopyType:' $TransferPostscriptParameterObject.ShadowCopyType
        echo 'ForceBaseImage:' $TransferPostscriptParameterObject.ForceBaseImage
        echo 'IsLogTruncation:' $TransferPostscriptParameterObject.IsLogTruncation
}
```

PreExportScript.ps1

O PreExportScript é executado no Core antes de qualquer trabalho de exportação.

Amostra de PreExportScript

```
# receiving parameter from export job
param([object]$ExportJobRequest)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null
# Converting input parameter into specific object
$ExportJobRequestObject = $ExportJobRequest -as [Replay.Core.Contracts.Export.ExportJobRequest]
# Working with input object. All echo's are logged
if($ExportJobRequestObject -eq $null) {
        echo 'ExportJobRequestObject parameter is null'
}
else {
        echo 'Location:' $ExportJobRequestObject.Location
        echo 'Priority:' $ExportJobRequestObject.Priority
}
```

PostExportScript.ps1

O PostExportScript é executado no Core após qualquer trabalho de exportação.

NOTA: Não há parâmetros de entrada para o PostExportScript quando usado para executar uma vez na máquina protegida exportada após a inicialização inicial. A máquina protegida regular deve conter esse script na pasta de scripts PowerShell como PostExportScript.ps1.

Amostra de PostExportScript

```
# receiving parameter from export job
param([object]$ExportJobRequest)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2 = $regVal2 + 'CoreService\Common.Contracts.dll'
# Converting input parameter into specific object
$ExportJobRequestObject = $ExportJobRequest -as [Replay.Core.Contracts.Export.ExportJobRequest]
# Working with input object. All echo's are logged
if($ExportJobRequestObject -eq $null) {
        echo 'ExportJobRequestObject parameter is null'
}
else {
        echo 'VolumeImageIds:' $ExportJobRequestObject.VolumeImageIds
        echo 'RamInMegabytes:' $ExportJobRequestObject.RamInMegabytes
}
```

PreNightlyJobScript.ps1

O PreNightlyJobScript é executado antes de cada trabalho noturno no lado do Core. Ele contém o parâmetro $JobClassName, que ajuda a lidar com os trabalhos subordinados separadamente.

Amostra de PreNightlyJobScript

```
# receiving parameters from Nightlyjob
param([System.String]$JobClassMethod , [object]$NightlyAttachabilityJobRequest, [object]
$RollupJobRequest, [object]$Agents, [object]$ChecksumCheckJobRequest, [object]
$TransferJobRequest, [int]$LatestEpochSeenByCore)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null
# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job, Checksum Check Job and
Log Truncation Job. All of them are triggering the script, and $JobClassMethod (contain job
name that calls the script) helps to handle those child jobs separately
switch ($JobClassMethod) {
# working with NightlyAttachability Job
    NightlyAttachabilityJob {
        $NightlyAttachabilityJobRequestObject = $NightlyAttachabilityJobRequest -as
```

```
[Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];
        echo 'Nightly Attachability job results:';
            if($NightlyAttachabilityJobRequestObject -eq $null) {
                echo 'NightlyAttachabilityJobRequestObject parameter is null';
            }
            else {
                echo 'AgentIds:' $NightlyAttachabilityJobRequestObject.AgentIds;
                echo 'IsNightlyJob:' $NightlyAttachabilityJobRequestObject.IsNightlyJob;
            }
            break;
        }
# working with Rollup Job
    RollupJob {
        $RollupJobRequestObject = $RollupJobRequest -as
[Replay.Core.Contracts.Rollup.RollupJobRequest];
        echo 'Rollup job results:';
            if($RollupJobRequestObject -eq $null) {
                    echo 'RollupJobRequestObject parameter is null';
            }
            else {
                echo 'SimultaneousJobsCount:' $RollupJobRequestObject.SimultaneousJobsCount;
                    echo 'AgentIds:' $RollupJobRequestObject.AgentIds;
                    echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;
            }
            $AgentsCollection = $Agents -as "System.Collections.Generic.List``1[System.Guid]"
            if($AgentsCollection -eq $null) {
                echo 'AgentsCollection parameter is null';
            }
            else {
                echo 'Agents GUIDs:'
                foreach ($a in $AgentsCollection) {
                    echo $a
            }
        }
        break;
    }
# working with Checksum Check Job
        ChecksumCheckJob {
            $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as
[Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
            echo 'Exchange checksumcheck job results:';
            if($ChecksumCheckJobRequestObject -eq $null) {
                echo 'ChecksumCheckJobRequestObject parameter is null';
        }
        else {
                echo 'RecoveryPointId:' $ChecksumCheckJobRequestObject.RecoveryPointId;
                echo 'AgentIds:' $ChecksumCheckJobRequestObject.AgentIds;
                echo 'IsNightlyJob:' $ChecksumCheckJobRequestObject.IsNightlyJob;
            }
            break;
        }
# working with Log Truncation Job
    TransferJob {
        $TransferJobRequestObject = $TransferJobRequest -as
[Replay.Core.Contracts.Transfer.TransferJobRequest];
        echo 'Transfer job results:';
        if($TransferJobRequestObject -eq $null) {
                echo 'TransferJobRequestObject parameter is null';
        }
        else {
                echo 'TransferConfiguration:' $TransferJobRequestObject.TransferConfiguration;
                echo 'StorageConfiguration:' $TransferJobRequestObject.StorageConfiguration;
            }
            echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
            break;
        }
}
```

PostNightlyJobScript.ps1

O PostNightlyJobScript é executado após cada trabalho noturno no Core. Ele contém o parâmetro $JobClassName, que ajuda a lidar com os trabalhos subordinados separadamente.

Amostra de PostNightlyJobScript

```
# receiving parameters from Nightlyjob
param([System.String]$JobClassMethod , [object]$NightlyAttachabilityJobRequest, [object]
$RollupJobRequest, [object]$Agents, [object]$ChecksumCheckJobRequest, [object]
$TransferJobRequest, [int]$LatestEpochSeenByCore, [object]$TakeSnapshotResponse)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2= $regVal2 + 'CoreService\Core.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal2) | out-null
# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job, Checksum Check Job and
Log Truncation Job. All of them are triggering the script, and $JobClassMethod (contain job
name that calls the script) helps to handle those child jobs separately
switch ($JobClassMethod) {
# working with NightlyAttachability Job
    NightlyAttachabilityJob {
        $NightlyAttachabilityJobRequestObject = $NightlyAttachabilityJobRequest -as
[Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];
        echo 'Nightly Attachability job results:';
        if($NightlyAttachabilityJobRequestObject -eq $null) {
            echo 'NightlyAttachabilityJobRequestObject parameter is null';
        }
        else {
            echo 'AgentIds:' $NightlyAttachabilityJobRequestObject.AgentIds;
            echo 'IsNightlyJob:' $NightlyAttachabilityJobRequestObject.IsNightlyJob;
        }
        break;
    }
# working with Rollup Job
    RollupJob {
        $RollupJobRequestObject = $RollupJobRequest -as
[Replay.Core.Contracts.Rollup.RollupJobRequest];
        echo 'Rollup job results:';
        if($RollupJobRequestObject -eq $null) {
            echo 'RollupJobRequestObject parameter is null';
        }
        else {
            echo 'AgentIds:' $RollupJobRequestObject.AgentIds;
            echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;
        }
        $AgentsCollection = $Agents -as "System.Collections.Generic.List``1[System.Guid]"
        if($AgentsCollection -eq $null) {
            echo 'AgentsCollection parameter is null';
        }
        else {
        echo 'Agents GUIDs:'
            foreach ($a in $AgentsCollection) {
                echo $a
                }
            }
            break;
        }
```

```
# working with Checksum Check Job
    ChecksumCheckJob {
        $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as
[Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
        echo 'Exchange checksumcheck job results:';
        if($ChecksumCheckJobRequestObject -eq $null) {
            echo 'ChecksumCheckJobRequestObject parameter is null';
        }
        else {
            echo 'RecoveryPointId:' $ChecksumCheckJobRequestObject.RecoveryPointId;
            echo 'AgentIds:' $ChecksumCheckJobRequestObject.AgentIds;
            echo 'IsNightlyJob:' $ChecksumCheckJobRequestObject.IsNightlyJob;
        }
        break;
    }
# working with Log Truncation Job
    TransferJob {
        $TransferJobRequestObject = $TransferJobRequest -as
[Replay.Core.Contracts.Transfer.TransferJobRequest];
        echo 'Transfer job results:';
        if($TransferJobRequestObject -eq $null) {
            echo 'TransferJobRequestObject parameter is null';
        }
        else {
             echo 'TransferConfiguration:' $TransferJobRequestObject.TransferConfiguration;
            echo 'StorageConfiguration:' $TransferJobRequestObject.StorageConfiguration;
        }
        echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
        $TakeSnapshotResponseObject = $TakeSnapshotResponse -as
[Replay.Agent.Contracts.Transfer.TakeSnapshotResponse];
        if($TakeSnapshotResponseObject -eq $null) {
            echo 'TakeSnapshotResponseObject parameter is null';
        }
        else {
            echo 'ID of this transfer session:' $TakeSnapshotResponseObject.SnapshotSetId;
            echo 'Volumes:' $TakeSnapshotResponseObject.VolumeSnapshots;
        }
        break;
    }
}
```

Usar scripts do Bourne Shell no Rapid Recovery

Bourne shell (sh) é uma linguagem de shell ou intérprete de linha de comando para sistemas operacionais baseados em Unix. Bourne Shell é usado no Rapid Recovery com Linux para personalizar ambientes e especificar que certas operações ocorram em uma sequência predeterminada. .sh é a extensão de arquivo e convenção de nomenclatura para arquivos Bourne shell.

Bourne Again Shell (BASH) é uma linguagem de shell semelhante que implementa a mesma gramática, parâmetro e expansão de variável, redireção e citação. BASH também usa a extensão de arquivo .sh. As informações fornecidas aqui também se aplicam ao BASH.

Usando os ganchos de script pré e pós-transferência e de exportação, é possível executar operações do sistema antes e depois de uma transferência ou exportação. Por exemplo, você talvez queira desativar certo cronjob enquanto a transferência está ocorrendo e ativá-lo assim que ela for concluída. Em outro exemplo, pode ser necessário executar comandos para liberar dados específicos do aplicativo para o disco. O conteúdo é gravado em um arquivo temporário e executado usando exec. O script é executado usando o intérprete definido na sua primeira linha, como por exemplo, `(#!/usr/bin/env bash)`. Se o intérprete especificado não estiver disponível, o script usará o shell padrão definido na variável de ambiente $SHELL.

Você pode substituir e usar qualquer intérprete. Por exemplo, na `#!` linha do script, você pode substituir “bash” por “zsh” (Z shell), “tcsh” (tee shell) e assim por diante, segundo sua preferência.

É possível adicionar objetos disponíveis do parâmetro TransferPrescript ou adicionar seus próprios comandos aos scripts PreTransferScript.sh e PostTransfer.sh para personalizá-los.

Esta seção descreve os scripts que podem ser usados por administradores em ocorrências designadas no Rapid Recovery para Windows e Linux. Os seguintes tópicos estão incluídos:

- Parâmetros de entrada para scripts do Bourne Shell
- Exemplos de scripts do Bourne Shell

Pré-requisitos para scripts do Bourne Shell

O Rapid Recovery fornece a capacidade de executar scripts do Bourne Shell na máquina com o Agente para Linux antes e depois de uma transferência. Os seguintes scripts são suportados para máquinas Linux protegidas com o Software do agente do Rapid Recovery.

NOTA: Observe que se um script não for executável, a tarefa de transferência falhará.

- PreTransferScript.sh
- PostTransferScript.sh
- PostExportScript.sh

Para usar estes scripts, certifique-se de que residem no diretório `/opt/apprecovery/scripts/`.

Parâmetros suportados para scripts de transferência e pós-transferência

Os seguintes parâmetros são suportados no Linux para scripts de transferência. Para obter informações, consulteExemplos de scripts do Bourne Shell.

- TransferPrescriptParameter_VolumeNames=$TransferPrescriptParameter_VolumeNames
- TransferPrescriptParameter_ShadowCopyType=$TransferPrescriptParameter_ShadowCopyType
- TransferPrescriptParameter_TransferConfiguration=$TransferPrescriptParameter_TransferConfiguration
- TransferPrescriptParameter_StorageConfiguration=$TransferPrescriptParameter_StorageConfiguration
- TransferPrescriptParameter_Key=$TransferPrescriptParameter_Key
- TransferPrescriptParameter_ForceBaseImage=$TransferPrescriptParameter_ForceBaseImage
- TransferPrescriptParameter_IsLogTruncation=$TransferPrescriptParameter_IsLogTruncation
- TransferPrescriptParameter_LatestEpochSeenByCore=$TransferPrescriptParameter_LatestEpochSeenByCore

Os seguintes parâmetros são suportados no Linux para scripts de pós-transferência.

- TransferPostscriptParameter_VolumeNames=$TransferPostscriptParameter_VolumeNames
- TransferPostscriptParameter_ShadowCopyType=$TransferPostscriptParameter_ShadowCopyType
- TransferPostscriptParameter_TransferConfiguration=$TransferPostscriptParameter_TransferConfiguration
- TransferPostscriptParameter_StorageConfiguration=$TransferPostscriptParameter_StorageConfiguration
- TransferPostscriptParameter_Key=$TransferPostscriptParameter_Key
- TransferPostscriptParameter_ForceBaseImage=$TransferPostscriptParameter_ForceBaseImage
- TransferPostscriptParameter_IsLogTruncation=$TransferPostscriptParameter_IsLogTruncation
- TransferPostscriptParameter_LatestEpochSeenByCore=$TransferPostscriptParameter_LatestEpochSeenByCore

Testar os scripts do Bourne Shell

É possível testar os scripts que deseja executar usando o editor de arquivos de script (.sh).

NOTA: Se os scripts pré-Bourne Shell ou pós-Bourne Shell falharem, o trabalho também falhará. Há informações sobre o trabalho disponível no arquivo /var/log/apprecovery/apprecovery.log.
Os scripts bem-sucedidos retornam o código de saída 0.

Parâmetros de entrada para scripts do Bourne Shell

Os parâmetros dos scripts do Bourne Shell no Rapid Recovery são descritos nas tabelas a seguir.

TransferPrescriptParameters_VolumeNames

A tabela a seguir apresenta os objetos disponíveis para o parâmetro TransferPrescript.

Tabela 316. Objetos de TransferPrescript

Método	Descrição
public VolumeNameCollection VolumeNames (get; set;)	Obtém ou define o conjunto de nomes de volume para transferência. VolumeNames é uma estrutura de dados que contém os seguintes dados: • GuidName. O GUID associado ao volume, usado como o nome caso DisplayName não tenha sido definido. • DisplayName. O nome de exibição do volume.
public ShadowCopyType ShadowCopyType { get; set; }	Obtém ou define o tipo de cópia da transferência. ShadowCopyType é uma enumeração com valores. Os valores disponíveis são: • Unknown • Copy • Full
public string Key { get; set; }	O método Key gera uma chave pseudoaleatória (mas não criptograficamente segura), que pode ser usada como senha única para autenticar solicitações de transferência.
public bool ForceBaseImage { get; set; }	Obtém ou define o valor que indica se a transferência foi uma captura de imagem de base forçada.
public bool IsLogTruncation { get; set; }	Obtém ou define o valor que indica se o registro está sendo truncado.
public uint LatestEpochSeenByCore { get; set; }	Obtém ou define o valor de epoch mais recente. O método LatestEpochSeenByCore é o número original do snapshot mais recentemente capturado pelo Core. Esse é o "número de epoch" atribuído pelo driver do filtro a este snapshot específico no momento em que ele foi capturado com o VSS.

TransferPostscriptParameter

A tabela a seguir apresenta os objetos disponíveis para o parâmetro TransferPostscript.

Tabela 317. Objetos de TransferPostscript

Método	Descrição
public VolumeNameCollection VolumeNames (get; set;)	Obtém ou define o conjunto de nomes de volume para transferência.

Método	Descrição
	VolumeNames é uma estrutura de dados que contém os seguintes dados: • GuidName. O GUID associado ao volume, usado como o nome caso DisplayName não tenha sido definido. • DisplayName. O nome de exibição do volume.
public ShadowCopyType ShadowCopyType { get; set; }	Obtém ou define o tipo de cópia da transferência. ShadowCopyType é uma enumeração com valores. Os valores disponíveis são: • Unknown • Copy • Full
public string Key { get; set; }	O método Key gera uma chave pseudoaleatória (mas não criptograficamente segura), que pode ser usada como senha única para autenticar solicitações de transferência.
public bool ForceBaseImage { get; set; }	Obtém ou define o valor que indica se a transferência foi uma captura de imagem de base forçada.
public bool IsLogTruncation { get; set; }	Obtém ou define o valor que indica se o registro está sendo truncado.
public uint LatestEpochSeenByCore { get; set; }	Obtém ou define o valor de epoch mais recente. O método LatestEpochSeenByCore é o número original do snapshot mais recentemente capturado pelo Core. Esse é o "número de epoch" atribuído pelo driver do filtro a este snapshot específico no momento em que ele foi capturado com o VSS.

Exemplos de scripts do Bourne Shell

Esta seção descreve os exemplos de scripts de Bourne Shell disponíveis para execução por usuários administrativos em máquinas protegidas.

CUIDADO: Os exemplos de script Bourne fornecidos neste documento funcionarão quando forem executados conforme projetado por administradores qualificados. Tome cuidado ao modificar scripts de funcionamento para manter versões de trabalho. Qualquer modificação nos exemplos de script incluídos aqui ou qualquer script que você criar são considerados como uma personalização, que normalmente não é coberta pelo Suporte Dell.

NOTA: Máquinas protegidas usam o comando de shell "exec" para iniciar o script. Para indicar qual intérprete deve executar o script, defina essa informação na primeira linha do script. Se você não especificar o intérprete, o shell padrão interpretará o script. Se você optar por algo diferente do shell padrão, precisará garantir que o intérprete especificado esteja disponível em todas as máquinas protegidas.

Os exemplos de scripts para máquinas protegidas incluem:

PreTransferScript.sh

O PreTransferScript é executado na máquina protegida antes da transferência de um snapshot.

O seguinte script armazena os valores de parâmetros de entrada no arquivo Pre(Post)TransferScriptResult.txt, localizado e armazenado no diretório base raiz.

Amostra de PreTransferScript

```
#!/bin/bash
echo "TransferPrescriptParameter_VolumeNames=$TransferPrescriptParameter_VolumeNames
TransferPrescriptParameter_ShadowCopyType=$TransferPrescriptParameter_ShadowCopyType
```

```
TransferPrescriptParameter_Key=$TransferPrescriptParameter_Key
TransferPrescriptParameter_ForceBaseImage=$TransferPrescriptParameter_ForceBaseImage
TransferPrescriptParameter_IsLogTruncation=$TransferPrescriptParameter_IsLogTruncation
TransferPrescriptParameter_LatestEpochSeenByCore=
$TransferPrescriptParameter_LatestEpochSeenByCore" > ~/PreTransferScriptResult.txt
exit 0
```

PostTransferScript.sh

O PostTransferScript é executado na máquina protegida após a transferência de um snapshot.

O seguinte script armazena os valores de parâmetros de entrada no arquivo Pre(Post)TransferScriptResult.txt, localizado e armazenado no diretório base raiz.

Amostra de PostTransferScript

```
#!/bin/bash
echo "TransferPostscriptParameter_VolumeNames=$TransferPostscriptParameter_VolumeNames
TransferPostscriptParameter_ShadowCopyType=$TransferPostscriptParameter_ShadowCopyType
TransferPostscriptParameter_Key=$TransferPostscriptParameter_Key
TransferPostscriptParameter_ForceBaseImage=$TransferPostscriptParameter_ForceBaseImage
TransferPostscriptParameter_IsLogTruncation=$TransferPostscriptParameter_IsLogTruncation
TransferPostscriptParameter_LatestEpochSeenByCore=
$TransferPostscriptParameter_LatestEpochSeenByCore" > ~/PostTransferScriptResult.txt
exit 0
```

PostExportScript.sh

O PostExportScript é executado na máquina protegida após a transferência.

O seguinte script armazena os valores de parâmetros de entrada no arquivo Pre(Post)ExportScriptResult.txt, localizado e armazenado no diretório base raiz.

Amostra de PostExportScript

```
#!/bin/bash
echo
"$curr_name-exported" > /etc/hostname
exit 0
```

D

APIs do Rapid Recovery

O objetivo desta seção é fornecer uma introdução e uma visão geral das APIs (Application Program Interfaces) de REST (Representational State Transfer) do Rapid Recovery, seu uso e sua função.

As APIs de serviço da Web do Rapid Recovery são RESTful e permitem automatizar e personalizar certas funções e tarefas na solução de software Rapid Recovery para ajudá-lo a atingir os seus objetivos comerciais.

Essas APIs podem ser obtidas da página **Downloads** do Dell Data Protection | Portal de licenças do Rapid Recovery.

Tópicos:

- Público-alvo
- Trabalhar com as APIs REST do Rapid Recovery
- Fazer download e visualizar as APIs de Core e Agente
- Leitura adicional recomendada

Público-alvo

As APIs do Rapid Recovery são destinadas a desenvolvedores de aplicativos que desejem integrar e estender o Rapid Recovery em seus aplicativos e a administradores que desejem criar scripts de interações com o Rapid Recovery Core Server.

Trabalhar com as APIs REST do Rapid Recovery

As APIs do Rapid Recovery são APIs em estilo REST, o que significa que usam solicitações HTTP para fornecer acesso a recursos (entidades de dados) por meio de caminhos de URI. As APIs do Rapid Recovery usam métodos HTTP padrão, como GET, PUT, POST e DELETE. Como as APIs REST são baseadas em padrões abertos, você pode usar qualquer idioma ou ferramenta com suporte a chamadas HTTP.

Há duas maneiras para desenvolvedores e administradores de aplicativos trabalharem com as APIs do Rapid Recovery. São elas:

- Empregar C# ou outra linguagem .DLL para usar diretamente os arquivos DLL de cliente .NET do Rapid Recovery.
- Comunicar-se diretamente com o terminal HTTP para gerar seu próprio XML.

Recomendamos a primeira abordagem. Os DLLs de cliente estão incluídos no SDK do Rapid Recovery. O método para chamar as APIs do Rapid Recovery é consistente com a maneira de consumir qualquer serviço WCF (Windows Communication Foundation) do .NET 4.5X.

Fazer download e visualizar as APIs de Core e Agente

O *SDK (Software Developer Kit) do Dell Data Protection | Rapid Recovery* inclui as APIs de REST para os componentes Rapid Recovery Core e Rapid Recovery Agent, e arquivos de exemplos e de suporte. Esse conteúdo é incluído nas seguintes pastas e, em seguida, comprimidos como um arquivo que inclui os seguintes componentes:

Tabela 318. Componentes incluídos no arquivo do SDK

Nome da pasta	Conteúdo	Descrição
Core.Contracts	APIs do Rapid Recovery Core	Contém as APIs que ajudam os programadores ou administradores a criar scripts de funções no Rapid Recovery Core. Há 2 conjuntos de contratos de serviço. 1 Abra o arquivo HTML CoreWeb.Client em um navegador da Web para exibir as informações dos padrões gerais de REST. Os contratos de serviço são apresentados. Ao clicar em um URI (Uniform Resource Identifier) vinculado correspondente, o navegador abrirá as informações presentes no diretório Core.Contracts/docWeb/. A página resultante mostra as informações sobre operações de serviço REST gerais, incluindo os métodos e as descrições. 2 Abra o arquivo HTML Core.Client em um navegador da Web para ver informações de C# detalhadas. Ao clicar em um contrato de serviço vinculado (classe), o navegador abrirá as informações presentes no diretório Core.Contracts/doc/. A página resultante mostra informações detalhadas para todos os métodos C# na classe selecionada.
Agent.Contracts	APIs do Rapid Recovery Agent (substituído)	Contém as APIs que os programadores ou os administradores podem usar para manipular o Rapid Recovery Agent nas máquinas protegidas. **CUIDADO: As APIs do Agent foram substituídas e serão removidas em uma versão futura do SDK. O uso direto das APIs do Agent não é recomendado. O uso desses APIs é considerado personalização e não será suportado. As informações são fornecidas na documentação para fins de histórico.** 1 Abra o arquivo HTML AgentWeb.Client em um navegador da Web para exibir as informações dos padrões gerais de REST. 2 Abra o arquivo HTML Agent.Client em um navegador da Web para ver informações de C# detalhadas.
AppRecoveryAPI Samples	Exemplos de código e bibliotecas de link dinâmico	AppRecoveryAPISamples contém exemplos de código escritos na linguagem de programação C#. Esses arquivos representam um bom ponto de partida para ver detalhes do código se estiver usando as APIs para personalizar sua interface gráfica, os sistemas de gerenciamento, e assim por diante. AppRecoveryAPISamples\Dependencies contém os arquivos DLL (Dynamic Link Library) que o Rapid Recovery Core usa. Os DLLs contêm os contratos de dados (os tipos com os quais o Core está familiarizado) e os contratos de serviço (métodos e operações de gerenciamento que podem ser usados para forçar o Core a fazer alguma coisa). Se você quiser personalizar sua própria interface gráfica de usuário ou usar um sistema de gerenciamento para funcionar com o Rapid Recovery Core, esses DLLs serão necessários. **NOTA: A versão do DLL utilizada deve coincidir com a versão do Core.**

Você pode fazer o download do SDK como arquivo (API-Reference-x.x.x-xxxx). Cada x representa um dígito no número do build para a versão relevante.

Execute o procedimento aqui descrito para obter o SDK, para baixá-lo para o seu destino específico e para descompactar os arquivos em preparação para o uso das APIs do Core e do Agent.

1 Faça login no Dell Data Protection | Portal de licenças do Rapid Recovery em https://licenseportal.com.

2 No menu de navegação esquerdo do portal de licenças, clique em **Downloads**.

A página **Downloads** do portal de licenças é exibida.

3 Na página **Downloads**, na seção de aplicativos com base em Windows, role para baixo até a descrição para o SDK e clique em **Download**.

4 Salve o arquivo baixado no local de sua preferência.

5 Descompacte o arquivo.

Na nova pasta API-Reference-x.x.x-xxxx, você verá os diferentes conjuntos de arquivos descritos na tabela anterior.

6 Abra os arquivos HTML chaves descritos na tabela anterior em um navegador da Web para ver as orientações sobre as APIs.

Leitura adicional recomendada

O *Guia de instalação e atualização do Dell Data Protection | Rapid Recovery* fornece uma visão geral da arquitetura do Rapid Recovery, e descreve as etapas necessárias para a instalação dos componentes do Rapid Recovery e para o upgrade dos componentes do Core e agente de versões anteriores.

O guia está disponível para download em https://support.software.dell.com/rapid-recovery/release-notes-guides/.

Sobre a Dell

A Dell escuta os clientes e fornece tecnologia inovadora, soluções empresariais e serviços globais de confiança e valor. Para obter mais informações, visite http://software.dell.com.

Como entrar em contato com a Dell

Para vendas ou outras questões, visite http://software.dell.com/company/contact-us.aspx ou ligue para +1-949 -754-8000.

Recursos do suporte técnico

O suporte técnico está disponível para clientes que compraram produtos de software da Dell com um contrato de manutenção válido e clientes que estão usando versões de teste. Para acessar o Portal de suporte, visite https://support.software.dell.com.

O Portal de suporte fornece ferramentas de autoajuda, que você pode usar para resolver problemas de forma rápida e independente, 24 horas por dia, 365 dias por ano. Além disso, o Portal de suporte fornece acesso direto a engenheiros de suporte de produtos por meio de um sistema online de Solicitação de serviço.

O Portal de suporte permite que você:

- Crie, atualize e gerencie as Solicitações (casos) de serviço.
- Visualize artigos da Base de conhecimento.
- Obtenha notificações de produtos.
- Baixe o software. Para software de teste, acesse http://software.dell.com/trials.
- Participe de discussões da comunidade.

Glossário

Agente

O Rapid Recovery Agent é um software instalado em uma máquina física ou virtual que permite adicionar essa máquina à proteção no Rapid Recovery Core.

APIs REST

REST (Representational State Transfer) é uma arquitetura de software simples sem estado projetado para escalabilidade. O Rapid Recovery usa essa arquitetura para suas APIs (Applications Programming Interface, Interface de programação de aplicações) com o objetivo de automatizar e personalizar determinadas funções e tarefas. Há um conjunto separado de APIs REST para a funcionalidade do Core e para a funcionalidade da máquina protegida (agente).

atribuição de marca branca

O Rapid Recovery fornece a capacidade de os provedores de serviços de cópia de segurança e de recuperação após desastres colocarem um rótulo branco ou uma nova marca no Rapid Recovery com sua própria identidade e, depois, vendê-lo ou distribuí-lo como seu próprio produto ou serviço.

capacidade de anexação do SQL

A capacidade de anexação do SQL é uma execução de teste dentro do Rapid Recovery Core para garantir que todos os pontos de recuperação do SQL estejam isentos de erro e disponíveis para backup em caso de falha.

capacidade de montagem

A montabilidade do Exchange é um recurso de detecção de corrupção que alerta os administradores sobre possíveis falhas e garante que todos os dados nos servidores do Exchange sejam recuperados com êxito em caso de falha.

caracteres proibidos

Caracteres proibidos são aqueles que não devem ser usados ao definir o nome de um objeto no Rapid Recovery Core Console. Por exemplo, ao definir um nome de exibição para uma máquina protegida, não use os caracteres especiais a seguir:

Tabela 319. Caracteres proibidos

Caractere	Nome do caractere	Proibida em
?	ponto de interrogação	nome de exibição de máquina, chave de criptografia, repositório, descrição de caminho
|	barra vertical	nome de exibição de máquina, chave de criptografia, repositório, descrição de caminho
:	dois pontos	nome de exibição de máquina, chave de criptografia, repositório O uso desse símbolo é permitido ao especificar um caminho, como **c:\data**.
/	barra	nome de exibição de máquina, chave de criptografia, repositório, descrição de caminho
\	barra invertida	nome de exibição de máquina, chave de criptografia, repositório O uso desse símbolo é permitido ao especificar um caminho local ou de rede, como **c:\data** ou **\\ \\ComputerName\SharedFolder**
*	asterisco	nome de exibição de máquina, chave de criptografia, repositório, descrição de caminho
"	aspas	nome de exibição de máquina, chave de criptografia, repositório, descrição de caminho
<	menor que	nome de exibição de máquina, chave de criptografia, repositório, descrição de caminho

Caractere	Nome do caractere	Proibida em
>	maior que	nome de exibição de máquina, chave de criptografia, repositório, descrição de caminho

Central Management Console

O Central Management Console do Rapid Recovery é um componente opcional que se destina a ambientes com dois ou mais Rapid Recovery Cores. Este componente é um portal Web que fornece uma interface central onde você pode agrupar, gerenciar e gerar relatórios para múltiplos Cores usando uma única interface baseada na Web.

chave de licença

Uma chave de licença é um método usado para registrar seu software ou appliance Rapid Recovery. (Você também pode usar um arquivo de licença.) Você pode obter chaves ou arquivos de licença ao abrir uma conta no Dell Data Protection | Portal de licenças do Rapid Recovery. Para obter mais informações, consulte Portal de licenças.

cluster

Consulte Cluster de ativação pós-falha do Windows.

cluster Continuous Replication (CCR)

Uma solução não compartilhada de cluster de ativação pós-falha de armazenamento que usa a tecnologia integrada de envio de log assíncrono para criar e manter uma cópia de cada grupo de armazenamento em um segundo server de um cluster de ativação pós-falha. A CCR foi projetada para ser uma solução de um ou dois data centers, para fornecer alta disponibilidade e resiliência local. É um dos dois tipos de implementação de server de caixa de correio em cluster (CMS) disponíveis no Exchange 2007.

cluster de ativação pós-falha do Windows

Um grupo de computadores independentes que funcionam juntos para aumentar a disponibilidade de aplicativos e serviços. Os servers em cluster (chamados de nós) são conectados por cabos físicos e por software. Se um dos nós do cluster falhar, outro nó começará a prestar o serviço (um processo conhecido como ativação pós-falha). Os usuários têm interrupções mínimas no serviço. O Rapid Recovery oferece suporte à proteção de vários tipos de cluster de SQL Server e Exchange Server.

cluster do servidor

Consulte Cluster de ativação pós-falha do Windows.

compressão

A Storage Networking Industry Association (SNIA) define a compressão como o processo de codificação de dados que visa reduzir seu tamanho.

cópia de segurança de SQL

Uma cópia de segurança de SQL é uma cópia de dados que é usada para restaurar e recuperar esses dados em um SQL Server após uma falha do sistema. Com a cópia de segurança de SQL, você pode realizar a recuperação de todo o banco de dados SQL ou de um ou mais componentes do banco de dados.

cópia de segurança diferencial de SQL

Uma cópia de segurança diferencial do banco de dados é uma cópia cumulativa de todas as alterações nos dados desde a última cópia de segurança completa do banco de dados SQL. A criação de cópias de segurança diferenciais geralmente é mais rápida do que a de cópias completas do banco de dados, reduzindo também o número de logs de transações necessários para recuperar o banco de dados.

cópia de segurança do SharePoint

Uma cópia de segurança do SharePoint é uma cópia de dados que é usada para restaurar e recuperar esses dados em um servidor SharePoint após uma falha do sistema. Com a cópia de segurança do SharePoint, você pode realizar a recuperação de todo o farm do SharePoint ou de um ou mais componentes do farm.

Core

O Rapid Recovery Core é o componente central da arquitetura do Rapid Recovery. O Core fornece os serviços essenciais para cópia de segurança, recuperação, retenção, replicação, arquivamento e gerenciamento. No contexto da replicação, o Core também é

chamado de core de origem. O core de origem é o núcleo originador, enquanto o core de destino é o núcleo de destino (outro Rapid Recovery Core em seu próprio servidor dedicado, em que máquinas ou clusters protegidos são replicados).

Core Console

O Rapid Recovery Core Console é uma interface baseada na Web que permite gerenciar totalmente o Rapid Recovery Core.

Core de destino

Também chamado de Core de réplica, é o Rapid Recovery Core que recebe os dados replicados (pontos de recuperação) do Core de origem.

Core remoto

Um Core remoto representa um Rapid Recovery Core acessado por uma máquina não Core usando o Local Mount Utility ou o Central Management Console.

criptografia

Os dados são criptografados com a intenção de que estejam acessíveis apenas aos usuários autorizados que têm a chave de descriptografia apropriada. Os dados são criptografados usando AES de 256 bits no modo Cipher Block Chaining (CBC). No CBC, XOR é aplicado a cada bloco de dados com o bloco de texto cifrado anterior, antes de ser criptografado. Dessa forma, cada novo bloco de texto cifrado depende de todos os blocos anteriores de texto simples. Uma frase de acesso é usada como vetor de inicialização.

deduplicação global

A Storage Networking Industry Association (SNIA) define a deduplicação de dados como a substituição de várias cópias dos dados, com níveis variados de granularidade, por referências a uma cópia compartilhada, para economizar espaço de armazenamento ou largura de banda. O Rapid Recovery Volume Manager realiza a deduplicação global de dados dentro de um volume lógico. O nível de granularidade da deduplicação é 8 KB. O escopo da deduplicação no Rapid Recovery é limitado às máquinas protegidas que usam o mesmo repositório e a mesma chave de criptografia.

evento

Um evento é um processo registrado pelo Core. Os eventos podem ser vistos no Core Console, clicando no ícone  (Eventos) da barra de ícones. A exibição padrão ao clicar no ícone  (Eventos) mostra a página **Tarefas**. Essa exibição mostra os eventos relacionados a um trabalho. Os eventos de prioridade sobre os quais você será notificado podem ser vistos na página **Alertas**. Um registro de todos os eventos aparece na página **Diário**. Através da configuração ou da modificação de grupos de notificação existentes, você pode personalizar a notificação para qualquer evento. Essa ação aumenta a prioridade do evento exibindo-o na página **Alertas**. Os membros de um grupo de notificação serão notificados dos eventos usando os métodos de notificação definidos nas opções de notificação do grupo.

frase de acesso

A frase de acesso é uma chave usada na criptografia de dados. Se a frase de acesso for perdida, os dados não poderão ser recuperados.

frases proibidas

Frases proibidas são frases (ou conjuntos de caracteres) que não devem ser usadas como nome de algum objeto no Rapid Recovery Core Console, pois estão reservadas para uso pelos sistemas operacionais. É uma boa prática evitar o uso dessas frases sempre que possível. Por exemplo, ao definir um nome de exibição para uma máquina protegida, não use as frases a seguir:

Tabela 320. Frases proibidas

Frase	Uso geral	Proibida em
con	console	nome de exibição de máquina, chave de criptografia, repositório, descrição de caminho
prn	porta da impressora	nome de exibição de máquina, chave de criptografia
aux	porta auxiliar	nome de exibição de máquina, chave de criptografia
nul	valor nulo	nome de exibição de máquina, chave de criptografia
com1, com2... *até* com9	porta de comunicação	nome de exibição de máquina, chave de criptografia
lpt1, lpt2... *até* lpt9	porta do terminal de impressão em linha	nome de exibição de máquina, chave de criptografia, repositório, descrição de caminho

funções de gerenciamento

O Central Management Console do Rapid Recovery introduz um novo conceito de funções de gerenciamento que permite dividir a responsabilidade administrativa entre administradores confiáveis de dados e serviços, além de acessar o controle de forma a oferecer suporte à delegação segura e eficiente da administração.

grupo de disponibilidade de banco de dados (DAG)

Um conjunto de até 16 servers de caixa de correio do Microsoft Exchange Server 2010 que fornece recuperação automática em nível de banco de dados após uma falha de banco de dados, server ou rede. Os DAGs usam a replicação contínua e um subconjunto de tecnologias de cluster de ativação pós-falha do Windows para fornecer alta disponibilidade e resiliência local. Os servers de caixa de correio em um DAG monitoram uns aos outros em busca de falhas. Quando um server de caixa de correio é adicionado a um DAG, ele funciona com os outros servers no DAG para fornecer recuperação automática ao nível de banco de dados após falhas de banco de dados.

imagem de base

A primeira transferência de cópia de segurança salva no Core é chamada de snapshot de imagem de base. Todos os dados em todos os volumes especificados (incluindo o sistema operacional, aplicativos e definições) são salvos no Core. Para obter mais informações, consulte snapshot.

Live Recovery

O Rapid Recovery Live Recovery é uma tecnologia de recuperação instantânea para VMs e servers. Fornece um acesso quase contínuo a volumes de dados em um servidor virtual ou físico, que permite recuperar um volume inteiro com RTO próximo de zero e RPO de minutos.

Local Mount Utility

O Local Mount Utility (LMU) é um aplicativo que pode ser adquirido via download, que permite a montagem de um ponto de recuperação em um Rapid Recovery Core remoto a partir de qualquer máquina.

máquina apenas com pontos de recuperação

Uma máquina apenas com pontos de recuperação é a representação no Core de pontos de recuperação de uma máquina que estava anteriormente protegida no Core e então removida. Se você remover a replicação, mas manter os pontos de recuperação, isso também resulta em uma máquina apenas com pontos de recuperação. As informações podem ser vistas e recuperadas no nível de arquivo. Você não pode usar uma máquina apenas com pontos de recuperação para executar uma BMR ou para restaurar volumes inteiros, nem pode adicionar mais dados a uma máquina apenas com pontos de recuperação.

máquina protegida

Uma máquina protegida, às vezes chamada de "agente", é um computador físico ou uma máquina virtual que é protegido pelo Rapid Recovery Core. Os dados salvos em backup são transmitidos da máquina protegida para o repositório especificado no Core usando

um intervalo de proteção predefinido. A imagem de base transmite todos os dados para um ponto de recuperação (incluindo o sistema operacional, os aplicativos e as configurações). Cada snapshot incremental posterior apenas vincula os blocos alterados nos volumes de disco especificados da máquina protegida. As máquinas com proteção baseada em software têm o software do agente do Rapid Recovery instalado. Algumas máquinas virtuais podem também ser protegidas sem agente, com algumas limitações.

nó de cluster

Máquina individual que faz parte de um cluster de ativação pós-falha do Windows.

pontos de recuperação

Os pontos de recuperação são uma coleção de snapshots de vários volumes de disco. Por exemplo, C:, D: e E:.

Portal de licenças

O Dell Data Protection | Portal de licenças do Rapid Recovery é uma interface Web onde os usuários e parceiros podem fazer download de software, registrar os dispositivos do Rapid Recovery e gerenciar assinaturas de licença. Os usuários do Portal de licenças podem registrar uma conta, baixar software Rapid Recovery Core e Agent, gerenciar grupos, monitorar a atividade de grupos, registrar máquinas, registrar appliances, convidar usuários e gerar relatórios. Para obter mais informações, consulte o documento *Dell Data Protection | Portal de licenças do Rapid Recovery User Guide* (Guia do usuário do portal de licenças do Dell Data Protection | Recuperação rápida).

PowerShell scripting

O Windows PowerShell é um ambiente conectado ao Microsoft .NET Framework projetado visando a automação administrativa. O Rapid Recovery inclui SDKs de cliente abrangentes para PowerShell scripting que permitem aos administradores automatizar a administração e o gerenciamento dos recursos do Rapid Recovery pela execução de comandos diretos ou por meio de scripts.

propagação

Na replicação, a transferência inicial de imagens de base de deduplicação e snapshots incrementais dos agentes protegidos, que pode acrescentar centenas ou milhares de gigabytes de dados. A replicação inicial pode ser propagada para o core de destino usando mídias externas, o que é útil para grandes conjuntos de dados ou locais com links lentos.

quórum

Para um cluster de ativação pós-falha, o número de elementos que devem estar on-line para determinado cluster continuar em execução. Os elementos relevantes nesse contexto são os nós do cluster. Esse termo também pode se referir ao recurso com capacidade de quórum selecionado para manter os dados de configuração necessários para a recuperação do cluster. Esses dados contém detalhes de todas as alterações aplicadas ao banco de dados de cluster. O recurso de quórum geralmente é acessível a outros recursos de cluster de modo que qualquer nó de cluster tem acesso às mais recentes alterações do banco de dados. Por padrão há apenas um recurso de quórum por cluster de server. A configuração de quórum especial (definições de cluster de ativação pós-falha) determina o ponto em que muitas falhas interrompem a execução do cluster.

Rapid Recovery

O Rapid Recovery estabelece um novo padrão de proteção de dados unificada, combinando cópia de segurança, replicação e recuperação em uma única solução, projetada para ser a cópia de segurança mais rápida e confiável para a proteção de máquinas virtuais (VM), bem como ambientes físicos e de nuvem.

replicação

Replicação é o processo de cópia de pontos de recuperação de um Rapid Recovery Core e de transmissão deles para outro Rapid Recovery Core para fins de recuperação de desastres. O processo exige uma solução com pares de origem/destino entre dois ou mais Cores. A replicação é gerenciada por máquina protegida. Qualquer máquina (ou todas as máquinas) protegida ou replicada em um Core de origem pode ser configurada para replicar em um Core de destino. Ele é os pontos de recuperação copiados para o Core de destino.

repository

Um repositório é uma coleção de imagens de base e snapshots incrementais capturados das máquinas protegido em um Rapid Recovery Core. Os repositórios precisam ser criados em dispositivos de armazenamento primários rápidos. O local de armazenamento de um repositório de DVM pode ser local para a máquina Core (neste caso, é hospedado em um OS Windows suportado apenas).

Pode-se usar um armazenamento de conexão direta, uma rede de área de armazenamento ou um servidor conectado à rede classificado adequadamente.

restore

O processo de restaurar um ou mais volumes de armazenamento em uma máquina a partir de pontos de recuperação salvos no Rapid Recovery Core é chamado de restauração. Anteriormente era chamado de reversão.

retenção

A retenção define o período pelo qual os snapshots de cópia de segurança de máquinas protegidas são armazenados no Rapid Recovery Core. A política de retenção é aplicada aos pontos de recuperação por meio do processo de rollup.

rollup

Trata-se de um procedimento de manutenção noturna interna que reforça a política de retenção por meio de colapso e eliminação de pontos de recuperação datados. O Rapid Recovery reduz o rollup apenas a operações de metadados.

single copy cluster

Uma solução compartilhada de cluster de ativação pós-falha de armazenamento, que usa uma única cópia de um grupo de armazenamento no armazenamento que é compartilhado entre os nós do cluster. É um dos dois tipos de implementação de server de caixa de correio em cluster disponíveis no Exchange 2007.

Sistema de arquivos de objeto

O Armazenamento do Objeto Escalável do Rapid Recovery é um componente de sistema de arquivos de objeto. Ele trata todos os blocos de dados, dos quais os snapshots são derivados, como objetos. Ele armazena, recupera, mantém e replica esses objetos. Foi projetado para oferecer desempenho de entrada e saída (I/O) escalável em conjunto com deduplicação global de dados, criptografia e gerenciamento de retenção. O sistema de arquivos de objeto faz interface direta com tecnologias de armazenamento padrão do setor.

Smart Agent

O Rapid Recovery Smart Agent é instalado nas máquinas protegidas pelo Rapid Recovery Core. O Smart Agent rastreia os blocos alterados no volume de disco e cria um snapshot dos blocos alterados em um intervalo de proteção predefinido.

snapshot

Snapshot é um termo comum do setor que define a capacidade de capturar e armazenar o estado de um volume de disco em um determinado ponto, enquanto os aplicativos estão executando. O snapshot é crítico em caso de necessidade de recuperação do sistema devido a uma interrupção ou falha do sistema. Os snapshots do Rapid Recovery reconhecem o aplicativo, ou seja, todas as transações abertas e os logs de transação contínua são concluídos e os caches são alinhados antes da criação do snapshot. O Rapid Recovery usa o Microsoft Volume Shadow Services (VSS) para facilitar snapshots consistentes de falhas de aplicativos.

snapshot incremental

Snapshots incrementais são cópias de segurança compostas apenas de dados alterados na máquina protegida desde a última cópia de segurança. São salvos regularmente no Core, com base no intervalo definido (por exemplo, a cada 60 minutos). Para obter mais informações, consulte snapshot.

soma de verificação

A soma de verificação é uma função que cria blocos de dados que são usados para detectar erros acidentais ocorridos durante a transmissão ou o armazenamento.

standby virtual

O Standby virtual é um processo que cria uma máquina virtual clone de uma máquina protegida. A máquina de origem pode ser física ou virtual, mas o produto é sempre virtual. Você pode criar um standby virtual único sob demanda ou definir requisitos para criar a VM inicializável e atualizá-la continuamente depois que cada snapshot é capturado na máquina original protegida.

Transport Layer Security

Transport Layer Security (TLS) é um protocolo moderno de rede de criptografia projetado para garantir a segurança da comunicação pela Internet. Esse protocolo, definido pela Força-Tarefa de Engenharia de Internet, é o sucessor do Secure Sockets Layer (SSL). O termo SSL ainda é geralmente usado, e os protocolos são interoperáveis (um cliente TLS pode fazer o downgrade para se comunicar com um server SSL).

True Scale

True Scale é a arquitetura escalável do Rapid Recovery.

truncamento de log

O truncamento de log é uma função que remove registros de log do log de transações. Para uma máquina do SQL Server, quando você forçar o truncamento dos registros do SQL Server, esse processo identifica espaço livre no server do SQL. Para uma máquina do Exchange Server, você força o truncamento dos logs do Exchange Server. Essa ação libera espaço no server do Exchange.

Universal Recovery

A tecnologia Universal Recovery do Rapid Recovery oferece uma flexibilidade ilimitada de restauração de máquinas. Permite realizar uma recuperação monolítica de/para qualquer plataforma física ou virtual de sua escolha, bem como atualizações de recuperação incremental para máquinas virtuais a partir de qualquer origem física ou virtual. Também permite realizar a recuperação de arquivos individuais, pastas, e-mail, itens de calendário, bancos de dados e aplicativos no nível de aplicativo, de item e de objeto.

Verified Recovery

A tecnologia Verified Recovery é usada para realizar testes de recuperação e confirmação de cópias de segurança de forma automatizada. Suporta vários sistemas de arquivo e servidores.

Volume Manager

O Rapid Recovery Volume Manager gerencia objetos e, depois, os armazena e apresenta como um volume lógico. Ele aproveita a arquitetura de pipeline dinâmico para fornecer escalabilidade TruScale, paralelismo e modelo assíncrono de entrada e saída (I/O) para alta taxa de transferência com latência mínima de I/O.