Dispositivo Dell DL4300
Guia do usuário

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.

2015 - 12

Rev. A01

Índice

1

Introdução ao dispositivo Dell DL4300

Este capítulo fornece uma introdução e visão geral do DL4300. Ele descreve os recursos, a funcionalidade e a arquitetura e consiste nos seguintes tópicos:

- Tecnologias do Core
- Arquitetura de dimensionamento verdadeiro
- Arquitetura de implementação
- Recursos do produto

O dispositivo define um novo padrão para proteção de dados unificada, combinando backup, replicação e recuperação em uma única solução que foi projetada para ser o backup mais rápido e mais confiável para proteger máquinas virtuais (VMs), máquinas físicas e ambientes em nuvem.

O dispositivo é capaz de lidar com até petabytes de dados com desduplicação global incorporada, compressão, criptografia e replicação para qualquer infraestrutura de nuvem privada ou pública. Os aplicativos e dados do servidor podem ser recuperados em minutos para fins de retenção de dados (DR) e conformidade.

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

O dispositivo combina as seguintes tecnologias:

- Recuperação em tempo real
- Recuperação verificada
- Recuperação universal
- Desduplicação global verdadeira

Essas tecnologias foram projetadas com a integração segura para recuperação de desastres em nuvem, a entrega rápida e a recuperação confiável. Com o armazenamento de objeto escalonável, o dispositivo é exclusivamente capaz de lidar com até petabytes de dados rapidamente, com desduplicação global incorporada, compressão, criptografia e replicação para qualquer infraestrutura de nuvem privada ou pública.

O AppAssure resolve a complexidade e as ineficiências das ferramentas de legado com a tecnologia central e o suporte a ambientes multi-hipervisor, incluindo os que funcionam no VMware vSphere e Microsoft Hyper-V, que incluem nuvens privadas e públicas. O AppAssure oferece esses avanços tecnológicos ao mesmo tempo em que reduz drasticamente os custos de armazenamento e gerenciamento de TI.

Tecnologias do Core

Mais detalhes sobre as principais tecnologias do AppAssure são descritos nos tópicos a seguir.

Recuperação em tempo real

A Live Recovery (Recuperação em tempo real) é a tecnologia de recuperação instantânea para MVs ou servidores. Ela permite um acesso quase contínuo aos volumes de dados em servidores virtuais ou físicos. Você pode recuperar um volume inteiro com RTO quase zero e um RPO de minutos.

A tecnologia de backup e replicação registra instantâneos simultâneos de várias máquinas virtuais ou servidores, fornecendo proteção quase instantânea dos dados e do sistema. Você pode retomar o uso do servidor diretamente a partir do arquivo de backup, sem esperar uma restauração completa do armazenamento da produção. Os usuários continuam trabalhando e os departamentos de TI reduzem as janelas de recuperação para atender ao RTO (objetivo de tempo de recuperação) e aos acordos de nível de serviço do RPO (objetivo do ponto de recuperação) atuais, cada vez mais rigorosos.

Recuperação verificada

A recuperação verificada permite realizar testes automatizados da recuperação e a verificação de backups. Isso inclui, mas não está limitado, aos sistemas de arquivos:- Microsoft Exchange 2007, 2010 e 2013, e diferentes versões do Microsoft SQL Server 2005, 2008, 2008 R2, 2012 e 2014. A recuperação verificada fornece a recuperação de aplicativos e backups em ambientes virtuais e físicos . Ela contém um algoritmo abrangente de verificação da integridade, baseado nas chaves SHA de 256 bits para verificar a exatidão de cada bloco do disco no backup durante o processo de arquivamento, replicação e operações de propagação de dados. Isso garante que a corrupção dos dados seja identificada precocemente e evita que os blocos de dados corrompidos sejam mantidos ou transferidos durante o processo de backup.

Recuperação universal

A tecnologia Universal Recovery (Recuperação universal) permite flexibilidade ilimitada na restauração da máquina. Você pode restaurar seus backups de sistemas físicos para máquinas virtuais, de máquinas virtuais para máquinas virtuais, de máquinas virtuais para sistemas físicos ou de sistemas físicos para sistemas físicos e realizar a restauração sem sistema operacional para hardwares diferentes. Por exemplo, P2V, V2V, V2P, P 2P, P2C, V2C, C2P e C2V.

A tecnologia de recuperação universal também acelera a movimentação de plataforma cruzada entre máquinas virtuais. Por exemplo, mover do VMware para o Hyper-V ou do Hyper-V para o VMware. Ela é baseada na recuperação no nível do aplicativo, do item e do objeto (arquivos individuais, pastas, e-mails, itens de calendário, bancos de dados e aplicativos). Com o AppAssure, você pode recuperar ou exportar do físico para a nuvem ou do virtual para a nuvem.

Desduplicação global real

O dispositivo fornece a desduplicação global real, que reduz os requisitos de capacidade de armazenamento do disco físico e oferece razões de redução do espaço superiores a 50:1, enquanto cumpre os requisitos de armazenamento de dados. A desduplicação e a compressão no nível de bloco em linha AppAssure True Scale com desempenho de velocidade de linha, combinadas à verificação integrada de integridade, impedem que a corrupção de dados afete a qualidade dos processos de backup e arquivamento .

Arquitetura True Scale

O dispositivo é baseado na arquitetura AppAssure True Scale. Ele aproveita a arquitetura de pipeline dinâmica e de múltiplos núcleos que é otimizada para fornecer consistentemente um desempenho sólido para os ambientes empresariais. O True Scale foi projetado do zero para fazer um dimensionamento linear, armazenar e gerenciar big data com eficiência e entregar RTOs e RPOs de minutos sem comprometer o desempenho. Ele é composto por um objeto voltado a objetivos e um gerenciador de volume com desduplicação global, compressão, criptografia, replicação e retenção integradas. O diagrama a seguir descreve a arquitetura AppAssure True Scale.

Figura 1. Arquitetura AppAssure True Scale

O AppAssure Volume Manager and Scalable Object Store serve como base para a arquitetura AppAssure True Scale. O armazenamento do objeto escalável armazena os instantâneos no nível de bloco que são capturados dos servidores virtuais e físicos. O gerenciador de volume gerencia numerosos armazenamentos de objetos, fornecendo um repositório comum ou armazenamento imediato apenas para o que é necessário. O armazenamentos de objetos suporta tudo simultaneamente, com a E/S assíncrona que fornece uma alta produtividade com mínima latência e maximiza a utilização do sistema. O repositório reside em diferentes tecnologias de armazenamento, como Storage Area Network (SAN), Direct Attached Storage (DAS) ou Network Attached Storage (NAS).

A função do AppAssure Volume Manager é similar à função do gerenciador de volume em um sistema operacional. Ele captura vários dispositivos de armazenamento, que podem ser de diferentes tipos e tamanhos, e os combina em volumes lógicos usando políticas segmentadas ou de alocação sequencial. O armazenamento de objetos salva, recupera, mantém e, em seguida, replica os objetos que são derivados de instantâneos com reconhecimento do aplicativo. O gerenciador de volume fornece um desempenho escalonável de E/S, em conjunto com desduplicação global de dados , criptografia, gerenciamento e retenção.

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.

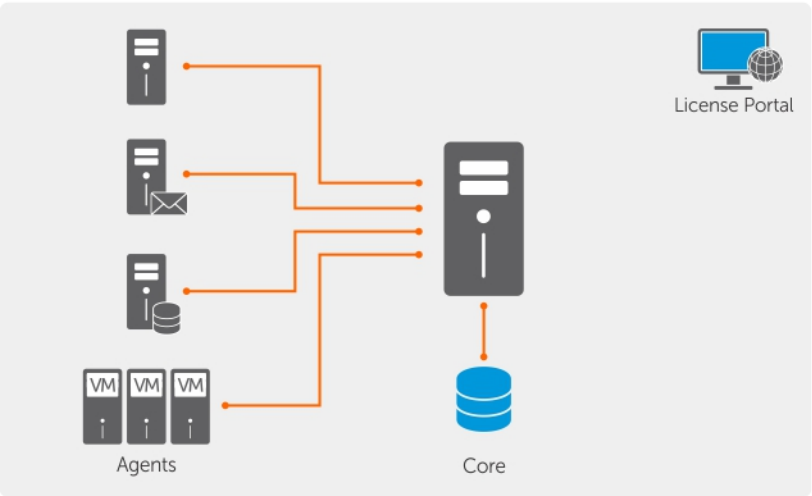


Figura 2. Arquitetura de implantação básica

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

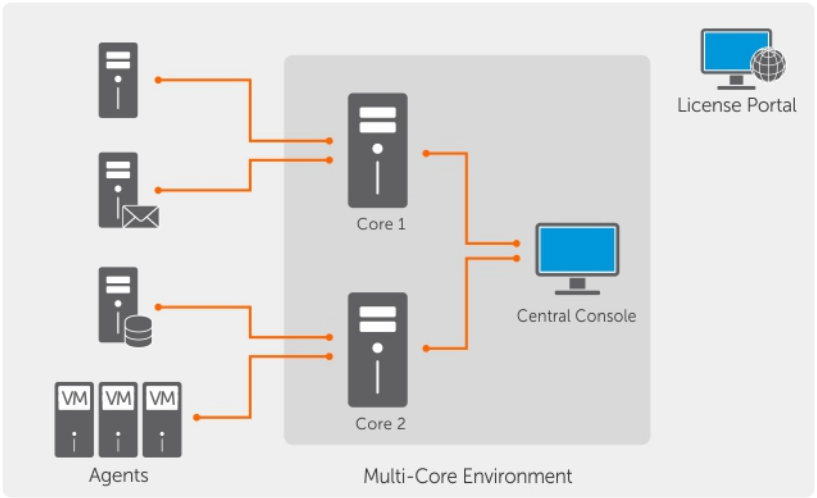


Figura 3. Arquitetura de implantação de múltiplos núcleos

Smart Agent

O Smart Agent rastreia os blocos alterados no volume do disco e, em seguida, encaixa uma imagem dos blocos alterados em um intervalo de proteção predefinido. A abordagem de instantâneos incrementais no nível do bloco para sempre impede a cópia dos mesmos dados da máquina protegida para o Core. O Smart Agent é instalada nas máquinas protegidas pelo Core.

O Smart Agent reconhece o aplicativo e fica inativo quando não estiver em uso , com praticamente 0% de utilização da CPU e menos de 20 MB de sobrecarga da memória. Quando o Smart Agent está ativo, ele usa até 2 a 4% do processador e menos de 150 MB de memória, incluindo a transferência de instantâneos para o Core.

O Smart Agent 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 AppAssure 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 Core usando 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 desduplica os dados na origem e as máquinas protegidas são emparelhadas com um Core para a proteção.

Core DL4300

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 versão de 64 bits do sistema operacional Microsoft Windows. O dispositivo realiza a compressão in-line baseada no destino, criptografia e desduplicação 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 Attached Storage).

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 APIs REST. 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 instantâneo

Um instantâneo é quando uma imagem básica é transferida de uma máquina protegida para o Core. Essa é a única vez em que uma cópia completa da máquina é transportada via rede na operação normal, seguida pelos instantâneos incrementais. O software AppAssure Agent para Windows usa o serviço de cópia Microsoft Volume Shadow (VSS) para congelar e desativar os dados do aplicativo para o disco, para capturar um backup consistente com o sistema de arquivos e o aplicativo. Quando um instantâneo é criado, o VSS e o gravador no servidor de destino impedem que o conteúdo seja gravado no disco. Quando a gravação do conteúdo no disco é interrompida, todas as operações de E/S do disco entram na fila e são retomadas apenas depois da conclusão do instantâneo, enquanto as operações que estão em andamento são concluídas e todos os arquivos abertos são fechados. O processo de criação de uma cópia de sombra não afeta significativamente o desempenho do sistema de produção.

O AppAssure usa o Microsoft VSS porque tem um suporte integrado para todas as tecnologias internas do Windows como NTFS, Registry e Active Directory para nivelar os dados no disco antes do instantâneo. Além disso, outros aplicativos corporativos, como o Microsoft Exchange e o SQL, usam os plug-ins de VSS Writer para serem notificados quando um instantâneo estiver sendo preparado e quando tiverem que nivelar as páginas usadas do banco de dados no disco, para deixar o banco de dados em um estado transacional consistente. É importante observar que o VSS é usado para desativar os dados de sistema e dos aplicativos no disco; ele não é usado para criar o instantâneo. Os dados capturados são transferidos imediatamente e armazenados no Core. O uso do VSS para o backup não coloca o servidor de aplicativos no modo de backup por um longo período, pois o tempo necessário para criar o instantâneo é de segundos, não horas. Outra vantagem de utilizar o VSS para os backups é que ele permite que o software AppAssure Agent crie um instantâneo de grandes quantidades de dados de uma vez, pois o instantâneo funciona no nível do volume.

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)
- True Global Deduplication (Features) [Desduplicação global real (recursos)]
- Criptografia
- Replicação
- Recovery-as-a-Service (RaaS) (Recuperação como um serviço)
- Retenção e arquivamento
- Virtualização e nuvem
- Gerenciamento de alertas e eventos
- Portal de licenças
- Console web
- APIs de gerenciamento de serviço

Repositório

O repositório usa o Deduplication Volume Manager (DVM) para implementar um gerenciador de volume que fornece suporte para múltiplos volumes, cada um dos quais podendo residir em diferentes tecnologias de armazenamento como Storage Area Network (SAN), Direct Attached Storage (DAS), Network Attached Storage (NAS) ou armazenamento em nuvem. Cada volume consiste em um armazenamento de objeto escalável com a desduplicação. Esse armazenamento comporta-se como um sistema de arquivos baseado em registros, no qual a unidade de alocação do armazenamento é um bloco de dados de tamanho fixo chamado de registro. Essa arquitetura permite configurar o suporte com o tamanho do bloco para a compactação e a desduplicação. As operações de implantação são reduzidas aos metadados para as operações de uso intenso do disco , porque a implantação não move mais os dados, apenas os registros.

O DVM pode combinar um conjunto de armazenamentos de objeto em um volume e eles podem ser expandidos criando sistemas de arquivos adicionais. Os arquivos do armazenamento de objeto são pré-alocados e podem ser adicionados sob demanda, conforme os requisitos de armazenamento mudarem. É possível criar até 255 repositórios independentes em um único Core e aumentar o tamanho de um repositório adicionando novas extensões de arquivo. Um repositório estendido pode conter até 4.096 extensões, que se distribuem entre diferentes tecnologias de armazenamento. O tamanho máximo de um repositório é 32 exabytes. Múltiplos repositórios podem existir em um único núcleo.

Desduplicação global real

Desduplicação global real é um método eficaz para reduzir as necessidades de armazenamento de backup , eliminando dados redundantes ou duplicados. A desduplicação é eficaz porque apenas uma instância dos dados, em múltiplos backups, é armazenada no repositório. Os dados redundantes são

armazenados, mas não fisicamente ; eles são simplesmente substituídos por um ponteiro para a única instância de dados no repositório.

Os aplicativos de backup convencionais realizavam backups completos e repetitivos uma vez por semana, mas o seu dispositivo faz backups da máquina incrementais e no nível do bloco. A abordagem sempre incremental, combinada com a desduplicação de dados, ajuda a reduzir drasticamente a quantidade total dos dados gravados no disco.

O layout de um disco típico consiste em um servidor sistema operacional, aplicativo e dados. Na maioria dos ambientes, os administradores frequentemente usam uma variação comum do servidor e do sistema operacional da área de trabalho em múltiplos sistemas, para a eficácia na implementação e no gerenciamento. Quando o backup é feito no nível do bloco em múltiplas máquinas ao mesmo tempo, ele proporciona uma visão mais granular do que está ou não no backup, independentemente da origem. Esses dados incluem o sistema operacional, os aplicativos e os dados de aplicativos em todo o ambiente.

Figura 4. Diagrama da desduplicação

O dispositivo realiza a desduplicação inline de dados baseada no destino, na qual os dados do instantâneo são transmitidos para o Core antes de serem desduplicados. A desduplicação inline de dados significa simplesmente que os dados são desduplicados antes que sejam comprometidos no disco. Isso é diferente da desduplicação na origem ou pós-processo , em que os dados são desduplicados na origem antes de serem transmitidos para o destino para o armazenamento. No pós-processo, os dados brutos são enviados ao destino, onde são analisados e desduplicados depois de serem gravados no disco. A desduplicação na origem consome recursos preciosos do sistema, enquanto a abordagem pós-processo exige todos os dados necessários no disco (uma sobrecarga maior da capacidade inicial) antes de iniciar o processo de desduplicação . Por outro lado, a desduplicação inline dos dados não precisa de capacidade adicional do disco e de ciclos de CPU na origem ou no Core para o processo de desduplicação. Por fim, os aplicativos convencionais de backup realizam backups completos e repetitivos uma vez por semana, enquanto o seu dispositivo realiza backups das máquinas incrementais e no nível de bloco para sempre. Essa abordagem sempre incremental, em combinação com a desduplicação dos dados, ajuda a reduzir drasticamente a quantidade total de dados gravados no disco com uma relação de redução de até 50:1.

Criptografia

O dispositivo fornece criptografia integrada para proteger os backups e os dados em repouso contra o acesso e o uso não autorizados, garantindo a privacidade dos dados. Apenas um usuário com a chave de criptografia pode acessar e descriptografar os dados. Não há limite para o número de chaves de criptografia que podem ser criadas e armazenadas em um sistema. O DVM usa a criptografia AES de 256 bits no modo Encadeamento de Blocos de Cifras (CBC) com chaves de 256 bits. A criptografia é feita in-line com os dados do instantâneo, nas velocidades da linha e sem afetar o desempenho. Isso ocorre porque a implementação do DVM tem múltiplos threads e usa a aceleração de hardware específica do processador em que ele é implementado.

A criptografia está pronta para múltiplos locatários. A desduplicação foi especificamente limitada aos registros criptografados com a mesma chave; dois registros idênticos que foram criptografados com chaves diferentes não são desduplicados um em relação ao outro. Esse design garante que a desduplicação não seja usada para vazamento de dados entre diferentes domínios de criptografia. Isso é um benefício para os provedores de serviços gerenciados, pois os backups replicados para múltiplos locatários (clientes) podem ser armazenados em um único núcleo sem que um locatário possa ver ou acessar os dados do outro. Cada chave de criptografia do locatário ativo cria um domínio de criptografia dentro do repositório , em que apenas o proprietário das chaves pode ver, acessar ou usar os dados. Em um cenário de múltiplos locatários, os dados são particionados e desduplicados dentro dos domínios de criptografia.

Nos cenários de replicação, o dispositivo usa o SSL 3.0 para proteger as conexões entre os dois núcleos em uma topologia de replicação, a fim de evitar escutas clandestinas e adulteração.

Replicação

Replicação é o processo de copiar pontos de recuperação de um AppAssure Core e transmiti-los para outro AppAssure Core em um local separado, para fins de recuperação de desastres. O processo exige uma relação de origem e destino emparelhados entre dois ou mais núcleos.

O núcleo de origem copia os pontos de recuperação das máquinas protegidas e, em seguida, transmite os dados dos instantâneos incrementais de maneira assíncrona e contínua para o núcleo de destino em um local remoto de recuperação de desastres. Você pode configurar a replicação de saída para um datacenter da empresa ou um local remoto de recuperação de desastres (isto é, um núcleo de destino autogerenciado). Ou então, pode configurá-la para um fornecedor de serviço gerenciado por terceiros (MSP) ou a nuvem que hospeda os serviços externos de backup e recuperação de desastres. Ao replicar para um núcleo de destino de terceiros, você pode usar fluxos de trabalho que permitam solicitar conexões e receber notificações de feedback automático.

A replicação é gerenciada com base na máquina protegida. Quaisquer (ou todas as) máquinas protegidas ou replicadas em um núcleo de origem podem ser configuradas para a replicação para um núcleo de destino.

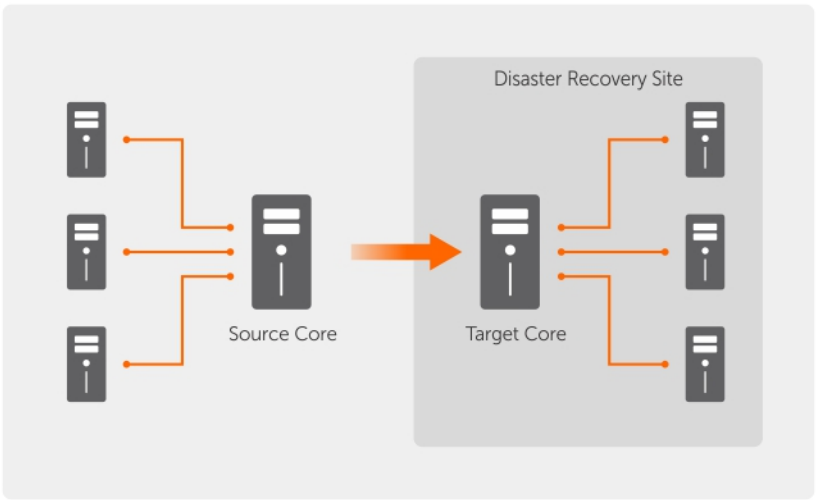


Figura 5. Arquitetura de replicação básica

A replicação é auto-otimizada com um exclusivo algoritmo de Leitura-Correspondência-Gravação (RMW) estreitamente combinado com a desduplicação. Com a replicação RMW, o serviço de replicação de origem e destino corresponde as chaves antes de transferir os dados e, em seguida, replica apenas os dados comprimidos, criptografados e desduplicados via WAN, resultando em uma redução no 10x nos requisitos de largura de banda.

A replicação começa com a propagação. Propagação é a transferência inicial das imagens básicas desduplicadas e instantâneos incrementais das máquinas protegidas. Os dados podem somar até centenas ou milhares de gigabytes. A replicação inicial ser propagada no núcleo de destino usando a mídia externa. Isso é útil para grandes conjuntos de dados ou sites com links lentos. Os dados no arquivamento da propagação são compactados , criptografados e desduplicados. Se o tamanho total do arquivamento for maior que o espaço disponível na mídia externa, o arquivamento pode se distribuir por múltiplos dispositivos. Durante o processo de propagação, os pontos de recuperação incrementais são replicados para o local de destino. Depois que os dados forem transferidos para o núcleo de destino, os pontos de recuperação recém-replicados sincronizam automaticamente.

Recuperação como um serviço (RaaS)

Os provedores de serviços gerenciados (MSPs - Managed Service Providers) podem utilizar o dispositivo como uma plataforma para oferecer a recuperação como um serviço (RaaS). O RaaS facilita a recuperação completa na nuvem replicando os servidores físicos e virtuais do cliente , junto com seus dados, para a nuvem do fornecedor de serviço como máquinas virtuais para dar suporte ao teste da recuperação ou às operações reais de recuperação. Os clientes que quiserem realizar a recuperação em nuvem podem configurar a replicação em suas máquinas protegidas nos núcleos locais para um fornecedor de serviço do AppAssure. Em caso de desastre, os MSPs podem acelerar as máquinas virtuais instantaneamente para o cliente.

Os MSPs podem implementar a infraestrutura de RaaS de múltiplos locatários do AppAssure, que pode hospedar organizações ou unidades de negócios múltiplas e diferentes (os locatários) que normalmente não compartilham a segurança ou os dados em um único servidor ou em um grupo de servidores. Os dados de cada locatário são isolados e protegidos dos demais locatários e do fornecedor de serviço.

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.

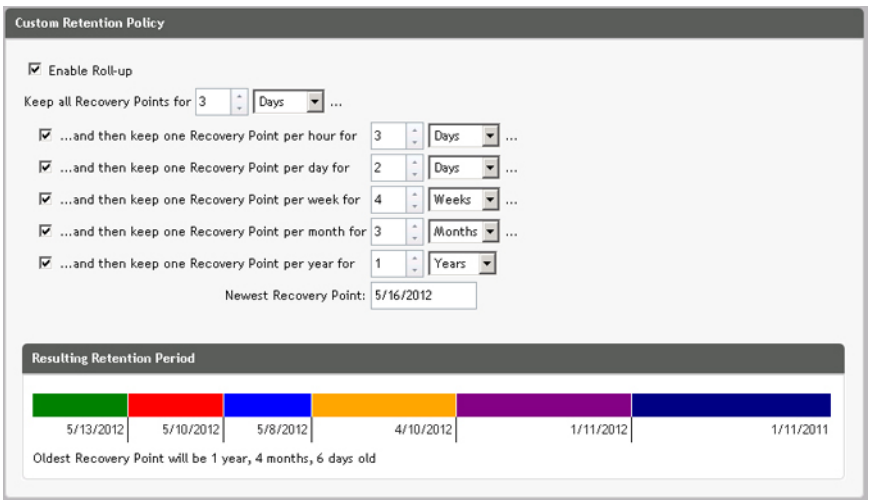


Figura 6. Política de retenção personalizada

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 Core DL4300

Acessar o Core Console DL4300

Para acessar o Core Console:

1. Atualize os sites confiáveis em seu navegador. Consulte Atualizar sites confiáveis no Internet Explorer.
2. Configure o seu navegador para acesso remoto ao Core Console. Consulte Configurar os navegadores para acesso remoto ao Core Console.
3. Execute um dos seguintes procedimentos para acessar o Core Console:
   - Faça login localmente no Core Server do DL4300 e, em seguida, clique duas vezes no ícone do **Core Console**.
   - Digite um dos seguintes URLs em seu navegador da Web:
     - **https://<NomeDoCoreServer>:8006/apprecovery/admin/core**
     - **https://<EndereçoIPDoCoreServer>:8006/apprecovery/admin/core**

Atualizar sites confiáveis no Internet Explorer

Para atualizar sites confiáveis no Microsoft Internet Explorer:

1. Abra o Internet Explorer.
2. Se os menus **Arquivo**, **Editar, Exibir** e outros menus não aparecerem, pressione <F10>.
3. Clique no menu **Ferramentas** e selecione **Opções da Internet**.
4. Na janela **Opções da Internet**, clique na guia **Segurança**.
5. Clique em **Sites confiáveis** e, em seguida, clique em **Sites**.
6. Em **Adicionar este site à zona**, digite **https://[Nome de exibição]**, usando o novo nome que você forneceu para o Nome de exibição.
7. Clique em **Adicionar**.
8. Em **Adicionar este site à zona**, digite **about:blank**.
9. Clique em **Adicionar**.
10. Clique em **Fechar** e, em seguida, em **OK**.

Configurar os navegadores para o acesso remoto ao Core Console

Para acessar o Core Console a partir de uma máquina remota, você precisará modificar as configurações do seu navegador.

NOTA: Para modificar as configurações do navegador, faça login no sistema como administrador.

NOTA: O Google Chrome usa as configurações do Microsoft Internet Explorer; altere as configurações do Chrome usando o Internet Explorer.

NOTA: Confirme se a **Internet Explorer Enhanced Security Configuration** (Configuração de segurança avançada do Internet Explorer) está ativada ao acessar o Core Web Console local ou remotamente. Para ativar a **Internet Explorer Enhanced Security Configuration** (Configuração de segurança avançada do Internet Explorer):

1. Abra o **Server Manager**.
2. Selecione **Local Server IE Enhanced Security Configuration** (Configuração de segurança avançada do IE do servidor local) mostrada no lado direito. Confirme se a opção está **On** (Ativada).

Configurar o navegador Internet Explorer e Chrome

Para modificar as configurações do navegador no Internet Explorer e Chrome:

1. Abra o Internet Explorer.
2. No menu **Ferramentas**, selecione **Opções da Internet**, guia **Segurança**.
3. Clique em **Sites confiáveis** e, em seguida, clique em **Sites**.
4. Desmarque a opção **Exigir verificação de servidor (https:) para todos os sites desta zona** e depois adicione http://*<nome do host ou endereço IP do servidor que hospeda o dispositivo AppAssure Core>* a **Sites confiáveis**.
5. Clique em **Fechar**, selecione **Sites confiáveis** e, em seguida, clique em **Nível personalizado**.
6. Role para baixo até **Miscelânea** → **Exibir conteúdo misto** e selecione **Habilitar**.
7. Role para baixo até a parte inferior da tela para **Autenticação de usuário** → **Logon** e, em seguida, selecione **Logon automático com o nome de usuário e a senha atuais**.
8. Clique em **OK** e, em seguida, selecione a guia **Avançadas**.
9. Role para baixo até **Multimídia** e selecione **Reproduzir animações em páginas da Web**.
10. Role para baixo até **Segurança**, marque a opção **Habilitar a autenticação integrada do Windows** e, em seguida, clique em **OK**.

Configurar o navegador Mozilla Firefox

NOTA: Para modificar as configurações do navegador Mozilla Firefox nas versões mais recentes, desative a proteção. Clique com o botão direito no botão Identificação do site (localizado à esquerda do URL), acesse **Opções** e clique em **Desativar proteção por enquanto**.

Para modificar as configurações do navegador Mozilla Firefox:

1. Na barra de endereços do Firefox, digite **about:config** e clique em **Serei cuidadoso, prometo!** se solicitado.
2. Procure o termo **ntlm**.

   A pesquisa deve retornar pelo menos três resultados.
3. Clique duas vezes em **network.automatic-ntlm-auth.trusted-uris** e digite a seguinte configuração, conforme apropriado para a sua máquina:
   - Para máquinas locais, digite o nome do host .
   - Para máquinas remotas, digite o nome do host ou o endereço IP , separados por uma vírgula, do dispositivo que hospeda o sistema AppAssure Core; por exemplo, *IPAddress*, *nome de host*.
4. Reinicie o Firefox.

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

NOTA: Se você estiver usando este Dispositivo, é recomendável usar a guia **Appliance** (Dispositivo) para configurar o Core. Para obter mais informações sobre como configurar o Core após a instalação inicial, consulte o *Guia de Implementação do Dispositivo Dell DL4300* em **dell.com/support/home**.

Gerenciar licenças

Você pode gerenciar as licenças diretamente no Core Console. No console, você pode alterar a chave de licença e entrar em contato com o servidor de licenças. Você pode também acessar o Portal de licenças na página Licensing (Licenciamento) do Core Console.

A página Licensing (Licenciamento) contém as seguintes informações:

- Tipo de licença
- Status da licença
- Restrições da licença
- Número de máquinas protegidas
- Status da última resposta do servidor de licenciamento
- Hora do último contato com o servidor de licenciamento
- Próxima tentativa agendada de contato com o servidor de licenciamento

Alterar uma chave de licença

Para alterar uma chave de licença:

1. Navegue até o Core Console.
2. Selecione **Configuration (Configuração)** → **Licensing (Licenciamento)**.
   A página **Licensing** (Licenciamento) aparece.
3. Na seção **License Details** (Detalhes da licença), clique em **Change License** (Alterar licença).
   A caixa de diálogo **Change License** (Alterar licença) aparece.
4. Na caixa de diálogo **Change License** (Alterar licença), digite a nova chave de licença e, em seguida, clique em **Continue** (Continuar).

Entrar em contato com o servidor do Portal de licenças

O Core Console contata frequentemente o servidor do portal para permanecer atualizado com todas as alterações efetuadas no portal de licenças. Tipicamente, a comunicação com o servidor do portal ocorre automaticamente em intervalos designados; no entanto, você pode iniciar uma comunicação sob demanda.

Para entrar em contato com o servidor do portal:

1. Navegue até o Core Console.
2. Clique em **Configuration (Configuração)** → **Licensing (Licenciamento)**.
3. Na opção **License Server** (Servidor de licença) , clique em **Contact Now** (Entrar em contato agora).

Alterar o idioma do AppAssure manualmente

O AppAssure permite que você altere o idioma que você selecionou ao executar o assistente Configuração de dispositivo AppAssure para qualquer um dos idiomas compatíveis.
Para alterar o idioma do AppAssure para aquele desejado:

1. Abra o editor de registro usando o comando `regdit`.
2. Navegue até **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **AppRecovery** → **Core** → **Localization** (Localização).
3. Abra **Lcid**.
4. Selecione **decimal**.
5. Digite o valor do idioma necessário na caixa `Value data` (Dados de valor), os valores de idiomas compatíveis são:
   a. Inglês: 1033
   b. Português brasileiro: 1046
   c. Espanhol: 1034
   d. Francês: 1036
   e. Alemão: 1031
   f. Chinês simplificado: 2052
   g. Japonês: 1041
   h. Coreano: 1042
6. Clique com o botão direito e reinicie os serviços na ordem apresentada:
   a. Windows Management Instrumentation
   b. SRM Web Service
   c. AppAssure Core
7. Limpe o cache do navegador.
8. Feche o navegador e reinicie o console do núcleo pelo ícone na área de trabalho.

Alterar o idioma do sistema operacional durante a instalação

Em uma instalação com Windows em execução, você pode usar o painel de controle para selecionar os pacotes de idiomas e definir configurações internacionais adicionais.
Para alterar o idioma do sistema operacional:

NOTA: É recomendado definir o mesmo idioma para o sistema operacional e o AppAssure; do contrário, algumas mensagens podem ser mostradas em idiomas diferentes.

NOTA: É recomendado alterar o idioma do sistema operacional antes de alterar o idioma do AppAssure.

1. Na página **Start** (Iniciar), digite `language` (idioma) e certifique-se de que o escopo de busca esteja definido para Settings (Configurações).
2. No painel **Results** (Resultados), selecione **Language** (Idioma).
3. No painel **Change your language preferences** (Alterar suas preferências de idioma), selecione **Add a language** (Adicionar um idioma).
4. Procure ou pesquise pelo idioma que você deseja instalar.

   Por exemplo, selecione Catalan (Catalão) e, em seguida, selecione Add (Adicionar). O idioma catalão é agora adicionado como um dos idiomas.
5. No painel Change your language preferences (Alterar suas preferências de idioma), selecione **Options** (Opções) ao lado do idioma que você adicionou.
6. Se um pacote de idioma estiver disponível para o seu idioma, selecione `Download and install language pack` (Fazer download e instalar pacote de idiomas).
7. Quando o pacote de idiomas é instalado, o idioma é mostrado como disponível para uso como idioma de exibição do Windows.
8. Para tornar este o idioma de exibição, mova-o para o topo de sua lista de idiomas.
9. Faça logout e depois faça o login novamente no Windows para que a alteração seja aplicada.

Gerenciar as configurações do Core

As configurações do Core são usadas para definir vários parâmetros de configuração e desempenho. A maior parte delas é configurada para uso otimizado, mas você pode alterar as configurações a seguir conforme necessário:

- General (Gerais)
- Tarefas noturnas
- Fila de transferência
- Configurações do tempo limite do cliente
- Configuração do cache de desduplicação
- Configurações da conexão com o banco de dados

Alterar o nome de exibição do Core

NOTA: É recomendável que você selecione um nome de exibição permanente durante a configuração inicial do dispositivo. Se você alterá-lo mais tarde, precisará realizar várias etapas manualmente para garantir que o novo nome do host tenha efeito e o dispositivo funcione corretamente. Para obter mais informações, consulte Alterar o nome do host manualmente.

Para alterar o nome de exibição do Core:

1. Navegue até o Core Console.
2. Clique em **Configuration (Configuração)** → **Settings (Parâmetros)**.
3. No painel **General** (Geral), clique em **Change** (Alterar).

   A caixa de diálogo **General Settings** (Configurações gerais) é exibida.
4. No caixa de texto **Display Name** (Nome de exibição), digite um novo nome de exibição para o Core.

   Esse é o nome que aparecerá no Core Console. Você pode digitar até 64 caracteres.
5. Na caixa de texto **Web Server Port** (Porta do servidor web), digite um número de porta para o servidor web. O padrão é 8006.

6. Na caixa de texto **Service Port** (Porta de serviço), digite um número de porta para o serviço. O padrão é 8006.
7. Clique em **OK**.

Ajustar o horário da tarefa noturna

Para ajustar o horário da tarefa noturna:

1. Navegue até o Core Console.
2. Clique em **Configuration (Configuração)** → **Settings (Parâmetros)**.
3. Na área **Nightly Jobs** (Tarefas noturnas), clique em **Change** (Alterar).

   A caixa de diálogo **Nightly Jobs** (Tarefas noturnas) é mostrada.
4. Na caixa de texto **Nightly Jobs Time** (Horário das tarefas noturnas), digite um novo horário para realizar as tarefas noturnas.
5. Clique em **OK**.

Modificar as configurações da fila de transferência

As configurações da fila de transferência ocorrem no nível do núcleo e estabelecem o número máximo de transferências simultâneas e o número máximo de novas tentativas de transferência de dados.

Para modificar as configurações da fila de transferência:

1. Navegue até o Core Console.
2. Clique em **Configuration (Configuração)** → **Settings (Parâmetros)**.
3. No painel **Transfer Queue** (Fila de transferência), clique em **Change** (Alterar).

   A caixa de diálogo **Transfer Queue** (Fila de transferência) aparece.
4. Na caixa de texto **Maximum Concurrent Transfers** (Máximo de transferências simultâneas), digite um valor para atualizar o número de transferências simultâneas.

   Configure um número de 1 a 60. Quanto menor o número, menor a carga imposta à rede e a outros recursos do sistema. Conforme a capacidade processada aumenta, a carga para o sistema também aumenta.
5. Na caixa de texto **Maximum Retries** (Máximo de novas tentativas), digite um valor para atualizar o número máximo de novas tentativas.
6. Clique em **OK**.

Ajustar as configurações do tempo limite do cliente

Para ajustar as configurações do tempo limite do cliente:

1. Navegue até o Core Console.
2. Clique em **Configuration (Configuração)** → **Settings (Parâmetros)**.
3. Na área **Client Timeout Settings Configuration** (Configurações do tempo limite do cliente), clique em **Change** (Alterar).

   A caixa de diálogo **Client Timeout Settings** (Configurações do tempo limite do cliente) aparece.
4. Na caixa de texto **Connection Timeout** (Tempo limite da conexão), digite o número de minutos e segundos antes que o tempo limite da conexão seja atingido.
5. Na caixa de texto **Connection UI Timeout** (Tempo limite da UI da conexão), digite o número de minutos e segundos antes que o tempo limite da UI da conexão seja atingido.

6. Na caixa de texto **Read/Write Timeout** (Tempo limite da leitura/gravação), digite o número de minutos e segundos antes que um tempo limite seja atingido, durante um evento de leitura/gravação.
7. Na caixa de texto **Read/Write UI Timeout** (Tempo limite da UI da leitura/gravação), digite o número de minutos e segundos antes que um tempo limite da UI de leitura/gravação seja atingido.
8. Clique em **OK**.

Configurar o cache de desduplicação

Para configurar o cache de desduplicação:

1. Navegue até o Core Console.
2. Clique em **Configuration (Configuração) → Settings (Parâmetros)**
3. Na área **Deduplication Cache Configuration** (Configuração do cache de desduplicação), clique em **Change** (Alterar).

   A caixa de diálogo **Deduplication Cache Configuration** (Configuração do cache de desduplicação) aparece.
4. Na caixa de texto **Primary Cache Location** (Local do cache primário) , digite um valor atualizado para alterar o local do cache primário.
5. Na caixa de texto **Secondary Cache Location** (Local do cache secundário) , digite um valor atualizado para alterar o local do cache secundário.
6. Na caixa de texto **Metadata Cache Location** (Local do cache de metadados) , digite um valor atualizado para alterar o local do cache de metadados.
7. Na caixa de texto **Dedupe Cache Size** (Tamanho do cache de desduplicação), insira um valor correspondente à quantidade de espaço que você quer atribuir ao cache de desduplicação.

   No campo suspenso do tamanho da unidade, selecione GB (gigabytes) ou TB (terabytes) para especificar a unidade de medida para o valor na caixa de texto Dedupe Cache Size (Tamanho do cache de desduplicação).
8. Clique em **OK**.

   NOTA: Você precisa reiniciar o serviço do Core para que as alterações tenham efeito.

Modificar as configurações do mecanismo

Para modificar as configurações do mecanismo:

1. Navegue até o Core Console.
2. Clique em **Configuration (Configuração) → Settings (Parâmetros)**
3. Na área **Replay Engine Configuration** (Configuração do mecanismo de reprodução), clique em **Change** (Alterar).

   A caixa de diálogo **Replay Engine Configuration** (Configuração do mecanismo de reprodução) aparece.
4. Digite as informações de configuração descritas da seguinte forma:

Caixa de texto	Descrição
Endereço IP	• Para usar o endereço IP preferencial do seu TCP/IP, clique em **Automatically Determined** (Determinado automaticamente)

Caixa de texto	Descrição
	• Para digitar um endereço IP, clique em **Use a specific address** (Usar um endereço específico).
Porta preferível	Digite um número de porta ou aceite a configuração padrão (8007 é a porta padrão). A porta é usada para especificar o canal de comunicação com o mecanismo.
Porta em uso	Representa a porta que está em uso para a configuração do mecanismo de reprodução.
Permitir atribuição automática da porta	Clique para permitir o uso da atribuição automática da porta de TCP.
Grupo Admin	Digite um novo nome para o grupo da administração. O nome padrão é BUILTIN\Administrators.
Comprimento mínimo da E/S assíncrona	Digite um valor ou escolha a configuração padrão. Descreve o comprimento mínimo da entrada/saída assíncrona. A configuração padrão é 65536.
Tamanho do buffer de recebimento	Digite o tamanho do buffer de entrada ou aceite a configuração padrão, que é 8192.
Tamanho do buffer de envio	Digite o tamanho do buffer de envio ou aceite a configuração padrão, que é 8192.
Tempo limite da leitura	Digite um valor do tempo limite da leitura ou escolha a configuração padrão, que é 00:00:30.
Tempo limite da gravação	Digite um valor do tempo limite da gravação ou escolha a configuração padrão, que é 00:00:30.
Sem atraso	É recomendável deixar essa caixa de seleção desmarcada, caso contrário a eficiência da rede será afetada. Se você determinar que precisa modificar essa configuração, entre em contato com o serviço de suporte da Dell para obter orientação.

5. Clique em **OK**.

Modificar as configurações de conexão ao banco de dados

Para modificar as configurações de conexão ao banco de dados:

1. Navegue até o Core Console.
2. Clique em **Configuration** → **Settings** (Configuração > Parâmetros).
3. Na área **Database Connection Settings** (Configurações da conexão ao banco de dados), escolha uma das seguintes opções:
   - Clique em **Apply Default** (Aplicar padrão).
   - Clique em **Change** (Alterar).

   A caixa de diálogo **Database Connection Settings** (Configurações da conexão ao banco de dados) é exibida.

4. Digite as configurações para modificar a conexão ao banco de dados, descritas a seguir:

Caixa de texto	Descrição
Host Name (Nome do host)	Digite um nome de host para a conexão ao banco de dados.
Port (Porta)	Digite um número de porta para a conexão ao banco de dados.
User Name (Nome de usuário) (opcional)	Digite um nome de usuário para acessar e gerenciar as configurações da conexão ao banco de dados. Isso é usado para especificar as credenciais de login para acessar a conexão ao banco de dados.
Password (Senha) (opcional)	Digite uma senha para acessar e gerenciar as configurações de conexão ao banco de dados.
Retain event and job history for, days (Reter o histórico de eventos e tarefas por dias)	Digite o número de dias para reter o histórico de eventos e tarefas para a conexão ao banco de dados.
Max connection pool size (Tamanho máx. do pool da conexão)	Configure o número máximo de conexões ao banco de dados no cache para permitir a reutilização dinâmica. A configuração padrão é 100.
Min connection pool size (Tamanho mín. do pool da conexão)	Configure o número mínimo de conexões ao banco de dados no cache para permitir a reutilização dinâmica. A configuração padrão é 0.

5. Clique em **Test Connection** (Testar conexão) para verificar as configurações.
6. Clique em **Save** (Salvar).

Sobre repositórios

Um repositório armazena os instantâneos que são capturados de estações de trabalho e servidores protegidos. O repositório pode residir em diferentes tecnologias de armazenamento como SAN (Storage Area Network), DAS (Direct Attached Storage) ou NAS (Network Attached Storage).

Quando você cria um repositório, o Core pré-aloca o espaço de armazenamento exigido para os dados e metadados no local especificado. Você pode criar até 255 repositórios independentes em um único núcleo, que serão distribuídos por diferentes tecnologias de armazenamento. Além disso, você ainda pode aumentar o tamanho de um repositório adicionando novas extensões de arquivo ou especificações. Um repositório estendido pode conter até 4096 extensões, que serão distribuídas por diferentes tecnologias de armazenamento.

Os principais conceitos e considerações do repositório são:

- O repositório é baseado no Sistema de arquivos de objeto escalonável do AppAssure.
- Todos os dados armazenados dentro de um repositório são globalmente desduplicados.
- O Sistema de arquivos de objeto escaonlável pode fornecer desempenho de E/S escalonável em conjunto com a desduplicação global de dados, criptografia e gerenciamento de retenção.

NOTA: Os repositórios DL4300 são armazenados em dispositivos de armazenamento primários. Os dispositivos de armazenamento de arquivamento como Data Domain não são suportados devido a limitações de desempenho. Da mesma forma, os repositórios não precisam ser armazenados nos arquivistas NAS em camada com a nuvem, pois esses dispositivos tendem a ter limitações de desempenho quando usados como armazenamento primário.

Roteiro para gerenciar um repositório

O roteiro para o gerenciamento de um repositório descreve tarefas como criar, configurar e ver um repositório e inclui os seguintes tópicos:

- Acessar o Core Console
- Criar um repositório
- Ver detalhes do repositório
- Modificar configurações do repositório
- Adicionar um local de armazenamento a um repositório existente
- Verificar um repositório
- Apagar um repositório
- Recuperar um repositório

NOTA: É recomendável usar a guia **Appliance** (Dispositivo) para configurar os repositórios.

Antes de começar a usar o dispositivo, você precisa configurar um ou mais repositórios no Core Server. Um repositório armazena os seus dados protegidos. Mais especificamente, ele armazena os instantâneos capturados dos servidores protegidos no seu ambiente.

Ao configurar um repositório, você pode realizar várias tarefas como especificar o local do armazenamento dos dados no Core Server, quantos locais podem ser adicionados a cada repositório, o nome do repositório e quantas operações os repositórios suportam.

Quando você cria um repositório, o Core pré-aloca o espaço necessário para armazenar os dados e metadados no local especificado. Você pode criar até 255 repositórios independentes em um único núcleo. Para aumentar ainda mais o tamanho de um único repositório, você pode adicionar novos locais de armazenamento ou volumes.

Você pode adicionar ou modificar repositórios no Core Console.

Criar um repositório

NOTA: Se você estiver usando este dispositivo como um SAN, é recomendável usar a guia **Appliance** (Dispositivo) para criar repositórios, consulte Provisionar armazenamento selecionado.

Faça o seguinte para criar manualmente um repositório:

1. Navegue até o Core Console.
2. Clique em **Configuration (Configuração)** → **Repositories (Repositórios)**.
3. Clique em **Add new** (Adicionar novo).
   A caixa de diálogo **Add New Repository** (Adicionar novo repositório) é mostrada.
4. Digite as informações, conforme descrito na tabela a seguir.

Caixa de texto	Descrição
Nome do repositório	Digite o nome de tela do repositório. Por padrão, essa caixa de texto consiste na palavra Repository (Repositório) e um número de índice que adiciona sequencialmente um número ao novo repositório, começando com 1. Você pode alterar o nome conforme a necessidade e digitar até 150 caracteres.
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 este repositório.

5. Para definir o local de armazenamento específico ou volume para o repositório, clique em **Add Storage Location** (Adicionar local de armazenamento).

   CUIDADO: Se o repositório do AppAssure que você está criando nesta etapa for removido mais tarde, todos os arquivos no local de armazenamento do repositório serão apagados. Se você não definir uma pasta dedicada para armazenar os arquivos do repositório, eles serão armazenados na raiz; o apagamento do repositório também apagará todo o conteúdo da raiz, resultando em uma catastrófica perda de dados.

   NOTA: Os repositórios são armazenados em dispositivos de armazenamento primários. Os dispositivos de armazenamento de arquivamento como Data Domain não são suportados devido a limitações de desempenho. Da mesma forma, os repositórios não precisam ser armazenados nos arquivistas NAS em camada com a nuvem, pois esses dispositivos tendem a ter limitações de desempenho quando usados como armazenamento primário.

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

6. Especifique como você quer adicionar o arquivo ao local de armazenamento. Você pode optar por adicionar o arquivo no disco local ou em compartilhamento CIFS.

   - Para especificar uma máquina local, clique em **Add file on local disk** (Adicionar arquivo no disco local) e digite as informações da seguinte forma:

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). As letras a a z não diferenciam maiúsculas de minúsculas. 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). As letras a a z não diferenciam maiúsculas de minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

   - Ou, para especificar um local de compartilhamento de rede, clique em **Add file on CIFS share** (Adicionar arquivo no compartilhamento CIFS) e digite as informações da seguinte forma:

Caixa de texto	Descrição
Caminho UNC	Digite o caminho para o local de compartilhamento de rede. Se esse local estiver na raiz, defina um nome da pasta dedicado (por exemplo, Repositório). O caminho precisa 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.
User Name (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.

7. No painel **Details** (Detalhes), clique em **Show/Hide Details** (Mostrar/ocultar detalhes) e digite os detalhes do local de armazenamento descritos da seguinte forma:

Caixa de texto	Descrição
Size (Tamanho)	Configure o tamanho ou capacidade do local de armazenamento. O padrão é 250 MB. Você pode escolher entre as seguintes opções: • MB • GB • TB **NOTA:** O tamanho que você especificar não pode exceder o tamanho do volume. **NOTA:** 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 ou Windows Server 2012, o limite do tamanho do arquivo é de 256 TB. **NOTA:** Para 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 o valor for configurado como On (Ligado), que é o padrão, o Windows controla o cache.

Caixa de texto	Descrição
	NOTA: A configuração da política de cache de gravação como On (Ligado) pode resultar em um desempenho mais rápido. Se você estiver usando uma versão do Windows Server anterior ao Server 2012,a configuração recomendada é **Off** (Apagado). Se configurado como **Off** (Apagado), o AppAssure 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.

8. Clique em **Save** (Salvar).
   A tela **Repositories** (Repositórios) aparece, para incluir o local de armazenamento adicionado recentemente.
9. Repita as Etapas 4 a 7 para adicionar mais locais de armazenamento ao repositório.
10. Clique em **Create** (Criar) para criar o repositório.
    As informações do **Repository** (Repositório) aparecem na guia **Configuration** (Configuração).

Ver os detalhes do repositório

Para ver os detalhes do repositório:

1. Navegue até o Core Console.
2. Clique em **Configuration (Configuração)** → **Repositories (Repositórios)**.
3. Clique em **>** ao lado da coluna **Status** do repositório cujos detalhes você quer ver.
4. Na vista expandida, você pode executar as seguintes ações:
   - Modify Settings (Modificar configurações)
   - Add a Storage Location (Adicionar um local de armazenamento)
   - Check a Repository (Verificar um repositório)
   - Delete a Repository (Apagar um repositório)

   Também são mostrados os detalhes do repositório, incluindo os locais de armazenamento e as estatísticas. Os detalhes do local de armazenamento incluem o caminho dos metadados , o caminho dos dados e o tamanho. As informações estatísticas incluem:
   - Deduplication (Desduplicação) – relatada como o número de acessos de desduplicação no bloco, desduplicações de bloco perdidas e taxa de compressão do bloco.
   - Record I/O (E/S do registro) – Consiste na taxa (MB/s), taxa de leitura (MB/s) e taxa de gravação (MB/s).
   - Storage Engine (Mecanismo de armazenamento) – Inclui a taxa (MB/s), taxa de leitura (MB/s) e taxa de gravação (MB/s).

Modificar as configurações do repositório

Depois de adicionar um repositório, você pode modificar suas configurações, como a descrição ou o máximo de operações simultâneas. Você também pode criar um novo local de armazenamento para o repositório.

Para modificar as configurações do repositório:

1. Navegue até o Core Console.
2. Clique em **Configuration (Configuração)** → **Repositories (Repositórios)**.
3. Clique no ícone Settings (Configurações) ao lado da coluna Compression Ratio (Taxa de compressão) abaixo do botão **Actions** (Ações) e, em seguida, em **Settings** (Configurações).

   A caixa de diálogo **Repository Settings** (Configurações do repositório) aparece.
4. Edite as informações do repositório descritas da seguinte forma:

Campo	Descrição
Nome do repositório	Representa o nome de tela do repositório. Por padrão, essa caixa de texto consiste na palavra Repository (Repositório) e um número de índice que corresponde ao número de repositório. NOTA: Você não pode editar o nome do repositório.
Descrição	Opcionalmente, digite uma nota descritiva sobre o repositório.
Máximo de operações simultâneas	Defina o número de solicitações simultâneas que você quer que o repositório suporte.
Ativar desduplicação	Para desativar a desduplicação, desmarque a caixa de seleção. Para ativá-la, selecione a caixa. NOTA: A alteração dessa configuração aplica-se somente para backups feitos após a configuração. Os dados existentes , replicados de outro núcleo ou importados de um arquivamento, mantêm os valores da desduplicação na data e hora em que foram capturados da máquina protegida.
Ativar compressão	Para desativar a compressão, desmarque a caixa de seleção. Para ativá-la, selecione a caixa. NOTA: Essa configuração aplica-se somente para backups feitos após a configuração. Os dados existentes , replicados de outro núcleo ou importados de um arquivamento, mantêm os valores da compressão na data e hora em que foram capturados da máquina protegida.

5. Clique em **Save** (Salvar).

Expandir um repositório existente

Se você adicionar outro DAS MD1400 ao dispositivo, pode usar o armazenamento disponível para expandir um repositório existente.

Para expandir um repositório existente:

1. Depois de instalar o DAS MD1400, abra o Core Console e selecione a guia **Appliance** (Dispositivo), clique em **Tasks** (Tarefas).
2. Na tela **Tasks** (Tarefas), ao lado do novo armazenamento, clique em **Provision** (Provisionar).
3. Na tela **Provisioning Storage** (Armazenamento de provisionamento), selecione **Expand the existing repository** (Expandir o repositório existente) e selecione o repositório que você quer expandir.
4. Clique em **Provision** (Provisionar).

   A tela **Tarefas** mostra a **Status Description** (Descrição do status) ao lado do dispositivo de armazenamento como **Provisioned** (Provisionado).

Adicionar um local de armazenamento a um repositório existente

A adição de um local de armazenamento permite definir onde você quer armazenar o repositório ou volume.

Para adicionar um local de armazenamento a um repositório existente:

1. Clique em **>** ao lado da coluna **Status** do repositório ao qual você quer adicionar um local de armazenamento.
2. Clique em **Add Storage Location** (Adicionar local de armazenamento).

   A caixa de diálogo **Add Storage Location** (Adicionar local de armazenamento) aparece.
3. Especifique como você quer adicionar o arquivo ao local de armazenamento. Você pode optar por adicionar o arquivo no disco local ou em um compartilhamento CIFS.
   - Para especificar uma máquina local, clique em **Add file on local disk** (Adicionar arquivo no disco local) e digite as informações da seguinte forma:

Caixa de texto	Descrição
Caminho dos metadados	Digite o local para armazenar os metadados protegidos.
Caminho de dados	Digite o local para armazenar os dados protegidos.

   - Para especificar um local de compartilhamento de rede, clique em **Add file on CIFS share** (Adicionar arquivo no compartilhamento CIFS) e digite as informações da seguinte forma:

Caixa de texto	Descrição
Caminho UNC	Digite o caminho para o local de compartilhamento de rede.
Nome de usuário	Especifique um nome de usuário para acessar o local de compartilhamento da rede.
Senha	Especifique uma senha para acessar o local de compartilhamento da rede.

4. Na seção **Details** (Detalhes), clique em **Show/Hide Details** (Mostrar/ocultar detalhes) e digite os detalhes do local de armazenamento descritos da seguinte forma:

Caixa de texto	Descrição
Tamanho	Configure o tamanho ou capacidade do local de armazenamento. O tamanho padrão é 250 MB. Você pode escolher entre as seguintes opções: • MB • GB • TB

Caixa de texto	Descrição
	NOTA: O tamanho que você especificar não pode exceder o tamanho do volume. **NOTA:** Se o local de armazenamento for um volume 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 ou Windows Server 2012, o limite do tamanho do arquivo é de 256 TB. **NOTA:** Para validar o sistema operacional, o 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 configurado como **On** (Ligado), que é o padrão, o Windows controla o cache. **NOTA:** A configuração da política de cache de gravação como **On** (Ligado) pode resultar em um desempenho mais rápido; no entanto a configuração recomendada é **Off** (Apagado). Se configurado como **Off** (Apagado), o AppAssure 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.

5. Clique em **Save** (Salvar).
   A tela **Repositories** (Repositórios) aparece, para incluir o local de armazenamento adicionado recentemente.
6. Repita as Etapas 4 a 7 para adicionar mais locais de armazenamento ao repositório.
7. Clique em **OK**.

Verificar um repositório

O dispositivo pode realizar uma verificação de diagnóstico de um volume do repositório quando erros ocorrerem. Os erros do Core podem ser consequências de um desligamento incorreto ou uma falha de hardware, entre outros motivos.

NOTA: Esse procedimento deve ser realizado somente para fins de diagnóstico.

Para verificar um repositório:

1. Na guia **Configuration** (Configuração), clique em **Repositories** (Repositórios) e selecione **>** ao lado do repositório que você quer verificar.
2. No painel **Actions** (Ações), clique em **Check** (Verificar).

   A caixa de diálogo **Check Repository** (Verificar repositório) é mostrada.
3. Na caixa de diálogo **Check Repository** (Verificar repositório) , clique em **Check** (Verificar).

   NOTA: Se a verificação falhar, restaure o repositório a partir de um arquivamento.

Apagar um repositório

Para apagar um repositório:

1. Na guia **Configuration** (Configuração), clique em **Repositories** (Repositórios) e selecione **>** ao lado do repositório que você quer apagar.
2. No painel **Actions** (Ações), clique em **Delete** (Apagar).
3. Na caixa de diálogo **Delete Repository** (Apagar repositório) , clique em **Delete** (Apagar).

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

   Ao apagar um repositório, você precisa consultar o Open Manage System Administrator e apagar os discos virtuais que abrigavam o repositório. Depois de apagar os discos virtuais, você pode reprovisionar os discos e recriar o repositório.

Remontar volumes

Para remontar volumes:

1. Navegue até o Core Console.
2. **Appliance (Dispositivo)** → **Tasks (Tarefas)**.
3. Clique em **Remount Volumes** (Remontar volumes).

   Os volumes são remontados.

Resolver volumes estranhos

Se um MD1400 provisionado for desligado ou desconectado e depois religado, aparece um evento no Core Console relatando que o MD1400 está conectado. No entanto, nenhuma tarefa aparece na guia **Appliance** (Dispositivo) da tela **Tasks** (Tarefas) que permita recuperá-lo. A tela **Enclosures** (Gabinetes) relata que o MD1400 está em um estado estranho e os repositórios nos discos virtuais externos estão off-line.

Para resolver volumes estranhos:

1. No Core Console, selecione a guia **Appliance** (Dispositivo) e, em seguida, clique em **Remount Volumes** (Remontar volumes).

   Os volumes são remontados.
2. Clique na guia **Configuration** (Configuração) e, em seguida, clique em **Repositories** (Repositórios).
3. Expanda o repositório com o indicador de status vermelho, clicando em **>** ao lado de **Status**.
4. Para verificar a integridade do repositório, em **Actions** (Ações), clique em **Check** (Verificar).

Recuperar um repositório

Quando o dispositivo falha ao importar um repositório, ele relata a falha na tela **Tasks** (Tarefas) com o status da tarefa indicado por um círculo vermelho e a descrição do status relatando **Error, Completed—Exception** (Erro, concluído – exceção). Para ver os detalhes do erro na tela **Tasks** (Tarefas), expanda os detalhes da tarefa clicando em **>** ao lado da coluna **Status**. **Status Details** (Detalhes do status) relata que o status da tarefa de recuperação é exceção e a coluna **Error Message** (Mensagem de erro) fornece detalhes adicionais sobre a condição de erro.

Para recuperar um repositório de um estado de importação com falha:

1. Navegue até o Core Console.

   A tela **Repositories** (Repositórios) mostra o repositório com falha com um indicador de status vermelho.
2. Clique em **Configuration (Configuração)** → **Repositories (Repositórios)**.
3. Expanda o repositório com falha clicando em **>** ao lado de **Status**.
4. Na seção **Actions** (Ações), clique em **Check** (Verificar) e, em seguida, clique em **Yes (Sim)** para confirmar que você quer realizar a verificação.

   O dispositivo recupera o 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.

Adicionar uma chave de criptografia

Para adicionar uma chave de criptografia:

1. Navegue até o Core Console.
2. Clique em **Configuration (Configuração)** → **Security (Segurança)**.

   A página **Encryption Keys** (Chaves de criptografia) aparece.
3. Clique em **Actions** (Ações) e, em seguida, clique em **Add Encryption Key** (Adicionar chave de criptografia).

   A caixa de diálogo **Create Encryption Key** (Criar chave de criptografia) é mostrada.

4. Na caixa de diálogo **Create Encryption Key** (Criar chave de criptografia) , digite os detalhes da chave da seguinte forma.

Caixa de texto	Descrição
Nome	Digite um nome para a chave de criptografia.
Descrição	Digite uma descrição da chave de criptografia, usada para fornecer mais detalhes da chave de criptografia.
Senha	Digite uma senha, usada para controlar o acesso.
Confirmar senha	Digite novamente a senha; usado para confirmar a senha digitada.

5. Clique em **OK**.

CUIDADO: É recomendável você proteger a senha. Se você perder a senha, não poderá acessar os dados.

Editar uma chave de criptografia

Para editar uma chave de criptografia:

1. Navegue até o Core Console.
2. Clique em **Configuration (Configuração)** → **Security (Segurança)**

   A tela **Encryption Keys** (Chaves de criptografia) aparece.
3. Selecione a chave de criptografia que você quer modificar e clique em **Edit** (Editar).

   A caixa de diálogo **Edit Encryption Key** (Editar chave de criptografia) aparece.
4. Na caixa de diálogo **Edit Encryption Key** (Editar chave de criptografia), edite o nome ou modifique a descrição da chave de criptografia.
5. Clique em **OK**.

Alterar uma senha da chave de criptografia

Para alterar uma senha da chave de criptografia:

1. Navegue até o Core Console.
2. Clique em **Configuration (Configuração)** → **Security (Segurança)**.

   A página Encryption Keys (Chaves de criptografia) aparece.
3. Selecione a chave de criptografia que você quer modificar e clique em **Change Passphrase** (Alterar senha).

   A caixa de diálogo **Change Passphrase** (Alterar senha) aparece.
4. Na caixa de diálogo **Change Passphrase** (Alterar senha), digite a nova senha para a criptografia e, em seguida, digite-a novamente para confirmar.
5. Clique em **OK**.

CUIDADO: É recomendável você proteger a senha. Se você perder a senha, não poderá acessar os dados no sistema.

Importar uma chave de criptografia

Para importar uma chave de criptografia:

1. Navegue até o Core Console.
2. Clique em **Configuration (Configuração)** → **Security (Segurança)**.
3. Selecione o menu suspenso **Actions** (Ações) e, em seguida, clique em **Import** (Importar).

   A caixa de diálogo **Import Key** (Importar chave) é mostrada.
4. Na caixa de diálogo **Import Key** (Importar chave), clique em **Browse** (Procurar) para localizar a chave de criptografia que você quer importar e , em seguida, clique em **Open** (Abrir).
5. Clique em **OK**.

Exportar uma chave de criptografia

Para exportar uma chave de criptografia:

1. Navegue até o Core Console.
2. Clique em **Configuration (Configuração)** → **Security (Segurança)**.
3. Clique em **>** ao lado do nome da chave de criptografia que você quer exportar e, em seguida, clique em **Export** (Exportar).

   A caixa de diálogo **Export Key** (Exportar chave) é exibida.
4. Na caixa de diálogo **Export Key** (Exportar chave), clique em **Download Key** (Fazer download da chave) para salvar e armazenar as chaves de criptografia em um local seguro.
5. Clique em **OK**.

Remover uma chave de criptografia

Para remover uma chave de criptografia:

1. Navegue até o Core Console.
2. Clique em **Configuration (Configuração)** → **Security (Segurança)**.
3. Clique em **>** ao lado do nome da chave de criptografia que você quer remover e, em seguida, clique em **Remove** (Remover).

   A caixa de diálogo **Remove Key** (Remover chave) aparece.
4. Na caixa de diálogo **Remove Key** (Remover chave), clique em **OK** para remover a chave de criptografia.

   NOTA: A remoção de uma chave de criptografia não descriptografa os dados.

Gerenciar contas na nuvem

O dispositivo DL permite que você crie backups de seus dados ao criar um arquivamento de backup de pontos de recuperação em uma nuvem. Com o dispositivo DL, você pode criar, editar e gerenciar sua conta na nuvem através de um provedor de armazenamento na nuvem. Você pode arquivar dados na nuvem usando o Azure, Amazon S3, Rackspace Cloud Block Storage ou outros serviços na nuvem baseados em OpenStack. Consulte os tópicos a seguir para gerenciar contas na nuvem:

- Adicionar uma conta na nuvem
- Editar uma conta na nuvem
- Definir configurações de conta na nuvem

- Remover uma conta na nuvem

Adicionar uma conta na nuvem

Antes que você possa exportar os dados arquivados para uma nuvem, adicione a conta ao seu provedor de serviços na nuvem no Core Console.

Para adicionar uma conta na nuvem:

1. No Core Console, clique na guia **Tools** (Ferramentas).
2. No menu à esquerda, clique em **Clouds** (Nuvens).
3. Na página **Clouds** (Nuvens), clique em **Add New Account** (Adicionar nova conta).

   A caixa de diálogo **Add New Account** (Adicionar nova conta) é mostrada.
4. Selecione um provedor de serviços na nuvem na lista suspensa **Cloud Type** (Tipo de nuvem).
5. Digite os detalhes conforme descrito na tabela a seguir com base no tipo de nuvem selecionado na etapa 4.

   Tabela 1. Adicionar uma conta na nuvem

Tipo de nuvem	Caixa de texto	Descrição
Microsoft Azure	Storage Account Name (Nome da conta de armazenamento)	Digite o nome da conta de armazenamento do Microsoft Azure.
	Access Key (Chave de acesso)	Digite a chave de acesso para sua conta.
	Display Name (Nome de exibição)	Crie um nome de exibição para essa conta no AppAssure; por exemplo, Windows Azure 1.
Amazon S3	Access Key (Chave de acesso)	Digite a chave de acesso para sua conta na nuvem da Amazon.
	Secret Key (Chave secreta)	Digite a chave secreta para essa conta.
	Display Name (Nome de exibição)	Crie um nome de exibição para essa conta no AppAssure; por exemplo, Amazon 1.
Desenvolvida pela OpenStack	User Name (Nome de usuário)	Digite o nome de usuário de sua conta na nuvem baseada em OpenStack.
	API Key (Chave de API)	Digite a chave de API para a conta.
	Display Name (Nome de exibição)	Crie um nome de exibição para essa conta no AppAssure; por exemplo, OpenStack 1.
	Tenant ID (ID de locatário)	Digite a ID de locatário dessa conta.

Tipo de nuvem	Caixa de texto	Descrição
	Authentication URL (URL de autenticação)	Digite o URL de autenticação para essa conta.
Rackspace Cloud Block Storage	User Name (Nome de usuário)	Digite o nome de usuário da sua conta na nuvem Rackspace.
	API Key (Chave de API)	Digite a chave de API para a conta.
	Display Name (Nome de exibição)	Crie um nome de exibição para essa conta no AppAssure; por exemplo, Rackspace 1.

6. Clique em **Adicionar**.
   A caixa de diálogo é fechada e a conta é mostrada na página **Clouds** (Nuvens) do Core Console.

Editar uma conta na nuvem

Execute as etapas a seguir para editar uma conta na nuvem:

1. No Core Console, clique na guia **Tools** (Ferramentas).
2. No menu à esquerda, clique em **Clouds** (Nuvens).
3. Ao lado da conta na nuvem que você deseja editar, clique no menu suspenso e depois clique em **Edit** (Editar).
   A janela **Edit Account** (Editar conta) é mostrada.
4. Digite os detalhes conforme for necessário e depois clique em **Save** (Salvar).

   NOTA: Você não pode editar o tipo de nuvem.

Definir configurações de conta na nuvem

As definições de configuração da nuvem permitem que você determine o número de vezes que o AppAssure deve tentar se conectar à conta da nuvem e a quantidade de tempo gasto em uma tentativa antes que o tempo expire.
Para definir as configurações de conexão de conta na nuvem:

1. No Core Console, clique na guia **Configuration** (Configuração).
2. No menu à esquerda, clique em **Settings** (Configurações).
3. Na página **Settings** (Configurações), navegue até **Cloud Configuration** (Configuração da nuvem).
4. Clique no menu suspenso ao lado da conta na nuvem que você deseja configurar e depois siga uma das opções:
   - Clique em **Edit** (Editar).
     A caixa de diálogo **Cloud Configuration** (Configuração de nuvem) é mostrada.

     1. Use as setas subir e descer para editar um das opções a seguir:

        – **Request Timeout** (Tempo limite de solicitação): mostrado em minutos e segundos, determina a quantidade de tempo que o AppAssure deve gastar em uma tentativa única para se conectar à conta na nuvem quando houver um atraso. As tentativas de conexão vão terminar após a quantidade de tempo informada.

- **Retry Count** (Contagem de novas tentativas): determina o número de tentativas que o AppAssure deve realizar antes de determinar que não é possível se comunicar com a nuvem.
- **Write Buffer Size** (Tamanho do buffer de gravação): determina o tamanho de buffer reservado para gravação de dados arquivados na nuvem.
- **Read Buffer Size** (Tamanho do buffer de leitura): determina o tamanho de buffer reservado para leitura de dados arquivados na nuvem.

2. Clique em **Next** (Avançar).

- Clique em **Reset** (Redefinir). Isso retorna a configuração para as seguintes definições padrão:
  - **Tempo limite de solicitação:** 01:30 (minutos e segundos)
  - **Contagem de novas tentativas:** 3 (tentativas)

Remover uma conta na nuvem

Você pode remover uma conta na nuvem, interromper o serviço na nuvem ou deixar de utilizá-lo ou para um determinado núcleo.
Para remover uma conta na nuvem:

1. No Core Console, clique na guia **Tools** (Ferramentas).
2. No menu à esquerda, clique em **Clouds** (Nuvens).
3. Ao lado da conta na nuvem que você deseja editar, clique no menu suspenso e depois clique em **Remove** (Remover).
4. Na janela **Delete Account** (Apagar conta), clique em **Yes** (Sim) para confirmar que você deseja remover a conta.
5. Se a conta na nuvem estiver em uso no momento, uma segunda janela perguntará se você ainda deseja removê-la. Clique em **Yes** (Sim) para confirmar.

   NOTA: Remover uma conta que está em uso no momento faz com que todos os trabalhos de arquivo agendados para essa conta falhem.

Informações gerais sobre replicação

Sobre a proteção de estações de trabalho e servidores

Para proteger seus dados, adicione as estações de trabalho e os servidores que deseja proteger no Core Console; por exemplo, seu servidor Exchange, SQL Server ou servidor Linux.

NOTA: Nesta seção, geralmente a palavra *máquina* também se refere ao software AppAssure Agent instalado em sua máquina.

No Core Console, você pode identificar a máquina na qual um software AppAssure Agent está instalado e especificar quais volumes quer proteger, definir agendamentos para a proteção, adicionar medidas extras de segurança como criptografia e muito mais. Para obter mais informações sobre como acessar o Core Console para proteger estações de trabalho e servidores, consulte Proteger uma máquina.

Sobre a replicação

Replicação é o processo de copiar pontos de recuperação e transmiti-los para um local secundário, para a recuperação de desastres. O processo exige uma relação emparelhada de origem-destino 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 local remoto de recuperação de desastres. O local externo pode ser um datacenter 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. Os cenários possíveis para a replicação são:

- **Replicação local**. O núcleo de destino está localizado em um datacenter local ou no local e a replicação é mantida o tempo todo. Nessa configuração, a perda do núcleo não impede a recuperação.
- **Replicação para locais externos**. O núcleo de destino está em um local externo de recuperação de desastres, para recuperação em caso de perda.
- **Replicação mútua**. Existem dois datacenters em dois locais diferentes; cada um deles contém um núcleo e protege os agentes e serve como backup externo de recuperação de desastres do outro. Nesse cenário, cada núcleo replica os máquinas protegidas para o núcleo que está localizado no outro datacenter.
- **Replicação hospedada e em nuvem**.Os parceiros do AppAssure MSP mantêm vários núcleos de destino em um datacenter ou uma nuvem pública. Em cada um desses núcleos, os parceiros do MSP permitem que um ou mais de seus clientes repliquem os pontos de recuperação de um núcleo de origem no local do cliente para o núcleo de destino do MSP, mediante uma taxa.

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

As possíveis configurações da replicação são:

- **Ponto a ponto**. Replica uma única máquina protegida a partir de um único núcleo de origem para um único núcleo de destino.

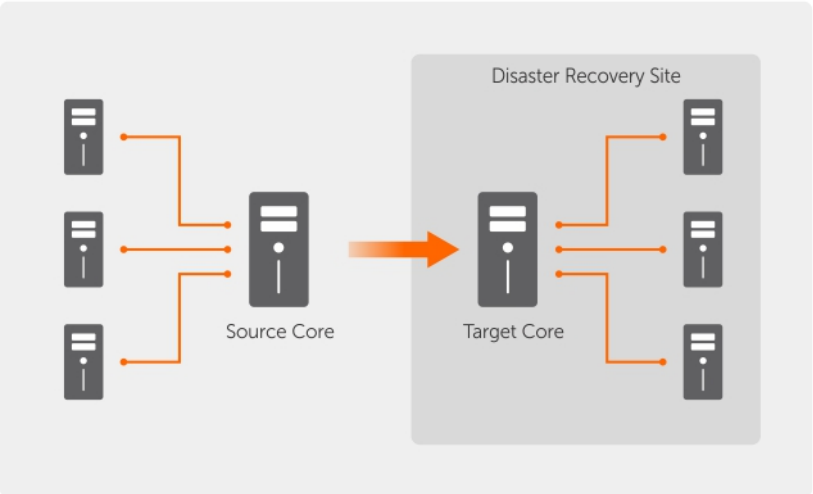


Figura 7. Diagrama da arquitetura de replicação básica

- **Múltiplos pontos para ponto**. Replicados múltiplos núcleos de origem para um único núcleo de destino.

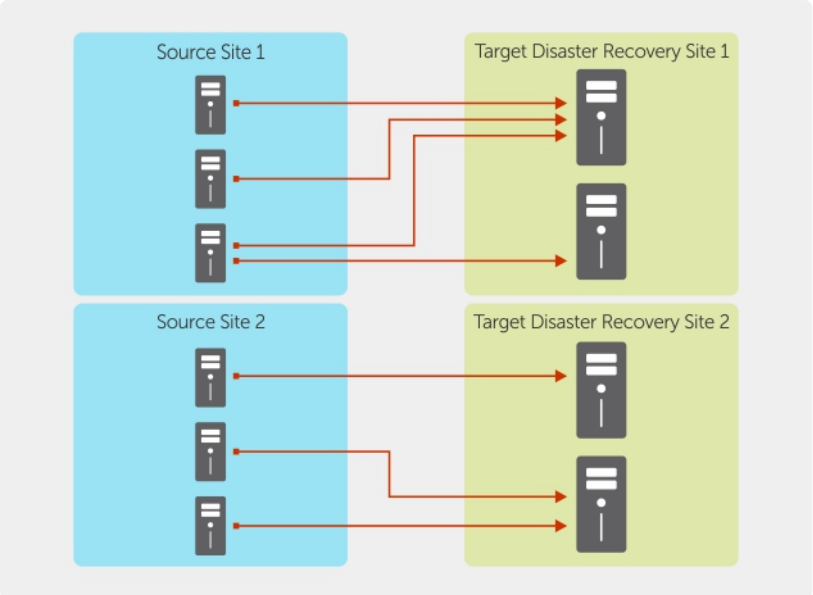


Figura 8. Diagrama da arquitetura de replicação de múltiplos pontos

Sobre a propagação

A replicação começa com a propagação: a transferência inicial de imagens básicas desduplicadas e instantâneos incrementais das máquinas protegidas, o que pode adicionar até centenas ou milhares de gigabytes de dados. A replicação inicial pode ser propagada no núcleo de destino usando a mídia externa. Isso é útil para grandes conjuntos de dados ou sites com links lentos.

NOTA: Embora seja possível fazer a propagação dos dados básicos através de uma conexão de rede, isso não é recomendado. A propagação inicial envolve quantidades potencialmente muito grandes de dados, o que poderia esgotar uma conexão típica de rede WAN. Por exemplo, se os dados da propagação totalizarem 10 GB e o link da WAN transferir 24 Mbps, a transferência pode demorar mais de 40 dias para terminar.

Os dados no arquivamento de propagação são compactados, criptografados e desduplicados. Se o tamanho total do arquivamento for maior que o espaço disponível na mídia externa, o arquivamento pode se distribuir por múltiplos dispositivos. Durante o processo de propagação, os pontos de recuperação incrementais são replicados para o local de destino. Depois que os dados forem transferidos para o núcleo de destino, os pontos de recuperação recém-replicados sincronizam automaticamente.

A propagação é um processo de duas partes (também conhecido como copiar-consumir):

- A primeira parte envolve a cópia, isto é, gravar os dados replicados iniciais em uma mídia removível. A cópia duplica todos os pontos de recuperação existentes do núcleo de origem para um dispositivo de armazenamento removível local, como uma unidade USB. Quando a cópia terminar, você precisa transportar a unidade do núcleo de origem local para o local do núcleo de destino remoto.
- A segunda parte é o consumo, que ocorre quando um núcleo de destino recebe a unidade transportada e copia os dados replicados para o repositório . Então, o núcleo de destino consome os pontos de recuperação e usa -os para formar as máquinas protegidas replicadas.

NOTA: Embora a replicação de instantâneos incrementais possa ocorrer entre os núcleos de origem e destino antes da propagação terminar, os instantâneos replicados transmitidos da origem para o destino permanece "órfãos" até que os dados iniciais sejam consumidos e são combinados com as imagens básicas replicadas.

Uma vez que grandes quantidades de dados precisam ser copiadas para o dispositivo de armazenamento portátil, é recomendada uma conexão eSATA, USB 3.0 ou outra de alta velocidade nesse dispositivo.

Sobre failover e failback

No caso de uma suspensão temporária grave, na qual as máquinas protegida e núcleo de origem falham, seu dispositivo DL suporta failover e failback nos ambientes replicados. Failover refere-se à alternação para um Core de destino redundante ou em espera quando ocorre uma falha no sistema ou a finalização anormal de um núcleo de origem e máquinas protegidas associadas. O principal objetivo do failover é iniciar um novo agente idêntico ao agente com falha que era protegido pelo núcleo de origem com falha. O objetivo secundário é alternar o núcleo de destino para um novo modo, de forma que o núcleo de destino proteja o agente de failover da mesma forma que o núcleo de origem protegia o agente inicial antes da falha. O núcleo de destino pode recuperar instâncias dos agentes replicados e iniciar a proteção imediatamente nas máquinas com failover.

Failback é o processo de restaurar uma máquina protegida e o núcleo de volta a seus estados originais (antes da falha). O objetivo primário do failback é restaurar a máquina protegida (na maioria dos casos, essa é uma nova máquina que substitui um agente com falha) para um estado idêntico ao último estado do novo agente temporário. Quando a restauração é feita, ela é protegida por um núcleo de origem restaurado. A replicação também é restaurada e o núcleo de destino atua novamente como um destino da replicação.

Sobre a replicação e os pontos de recuperação criptografados

Embora a unidade de propagação não contenha backups do registro e dos certificados do núcleo de origem, a unidade de propagação contém as chaves de criptografia do núcleo 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 serem transmitidos para o núcleo de destino. Os proprietários ou os administradores do núcleo de destino precisam da senha para recuperar os dados criptografados.

Sobre as políticas de retenção para replicação

A política de retenção no núcleo de origem determina a política de retenção para os dados replicados no núcleo de destino, pois a tarefa de replicação transmite os pontos de recuperação mesclados que resultam de uma implantação ou um apagamento ad-hoc.

NOTA: O núcleo de destino não tem a capacidade de acúmulo ou exclusão ad-hoc dos pontos de recuperação. Essas ações só podem ser feitas pelo núcleo de origem.

Considerações sobre o desempenho na transferência de dados replicados

Se a largura de banda entre o núcleo de origem e de destino não puder acomodar a transferência de pontos de recuperação armazenados, a replicação começa com a propagação do núcleo de destino com as imagens básicas e pontos de recuperação dos servidores selecionados protegidos no núcleo de origem. O processo de propagação precisa ser realizado apenas uma vez, pois funciona como a base necessária para a replicação regularmente agendada.

Ao preparar-se para a replicação, você precisa considerar os seguintes fatores:

Taxa de alteração A taxa de alteração é a taxa na qual a quantidade de dados protegidos são acumulados. Ela depende da quantidade de dados que mudam nos volumes

protegidos e do intervalo de proteção dos volumes. Se um conjunto de blocos alterar no volume, a redução no intervalo de proteção reduz a taxa de alteração.

Largura de Banda A largura de banda é a velocidade de transferência disponível entre o núcleo de origem e de destino. É fundamental que a largura de banda seja maior que a taxa de alteração, para que a replicação mantenha-se atualizada com os pontos de recuperação criados pelos instantâneos. Devido à quantidade de dados transmitidos de um núcleo para outro, pode ser necessário realizar múltiplos fluxos paralelos em velocidades de transferências de até 1 GB de conexão Ethernet.

NOTA: A largura de banda especificada pelo provedor de internet é a largura de banda total disponível. A largura de banda de saída é compartilhada por todos os dispositivos na rede. Certifique-se de que exista largura de banda livre suficiente para replicação de maneira que seja possível acomodar a taxa de alteração.

Número de máquinas protegidas É importante considerar o número de máquinas protegidas por núcleo de origem e quantas você planeja replicar para o destino.O AppAssure permite realizar a replicação com base em cada servidor protegido, para que você possa optar por replicar certos servidores. Se todos os servidores protegidos precisarem ser replicados, isso afeta drasticamente a taxa de alteração, particularmente se a largura de banda entre os núcleos de origem e destino for insuficiente para a quantidade e o tamanho dos pontos de recuperação que estão sendo replicados.

Dependendo da sua configuração de rede, a replicação pode ser um processo que demande tempo.

A tabela a seguir mostra exemplos da largura de banda necessária por Gigabyte, para obter uma taxa de alteração razoável

NOTA: Para obter resultados ideais, siga as recomendações apresentadas na lista na tabela a seguir.

Taxa de alteração máxima para tipos de conexão WAN

Tabela 2. Taxa de alteração máxima para tipos de conexão WAN

Banda larga	Largura de Banda	Taxa de alteração máx.
DSL	Até 768 Kbps	330 MB por hora
Cabo	Até 1 Mbps	429 MB por hora
T1	Até 1,5 Mbps	644 MB por hora
Fibra	Até 20 Mbps	838 GB por hora

Se um link falhar durante a transferência de dados, a replicação é retomada desde o ponto de falha anterior da transferência, depois que a funcionalidade do link for restaurada.

Roteiro para executar a replicação

Para replicar dados usando o AppAssure, 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 AppAssure envolve as seguintes operações:

- Configurar a replicação autogerenciada. Para obter mais informações sobre como replicar em um núcleo de destino autogerenciado, consulte Replicar em um núcleo autogerenciado.
- Configurar a replicação terceirizada. Para obter mais informações sobre como replicar em um núcleo de destino terceirizado, consulte Replicar em um núcleo gerenciado por um terceiro.
- Replicar em uma nova máquina protegida anexada ao núcleo de origem. Para obter mais informações sobre como replicar uma máquina protegida, consulte Replicar uma nova máquina protegida.
- Replicar em uma máquina protegida atual. Para obter mais informações sobre como configurar um agente para replicação, consulte Replicar dados de agente em uma máquina.
- Definir a prioridade de replicação para um agente. Para obter mais informações sobre como priorizar a replicação dos agentes, consulte Definir a prioridade de replicação para um agente.
- Monitorar a replicação conforme for necessário. Para obter mais informações sobre como monitorar a replicação, consulte Monitorar a replicação.
- Gerenciar configurações de replicação conforme necessário. Para obter mais informações sobre como gerenciar configurações de replicação, consulte Gerenciar configurações 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.

Replicação para um núcleo autogerenciado

Um núcleo autogerenciado core é um núcleo ao qual você tem acesso, normalmente porque ele é gerenciado por sua empresa um local externo. A replicação pode ser concluída totalmente no núcleo de origem, a menos que você opte por propagar os dados. A propagação exige que você consuma a unidade de propagação no núcleo de destino depois de configurar a replicação no núcleo de origem.

NOTA: Esta configuração aplica-se à replicação para um local externo e à replicação mútua. O núcleo precisa estar instalado em todas as máquinas de origem e de destino. Se você estiver configurando o sistema para replicação de multiponto para ponto, você precisa executar essa tarefa em todos os núcleos de origem e no núcleo de destino.

Configurar o núcleo de origem para replicar para um núcleo de destino autogerenciado

Para configurar o núcleo de origem para replicar para um núcleo de destino autogerenciado:

1. No núcleo, clique na guia **Replication** (Replicação).
2. Clique em **Add Target Core** (Adicionar núcleo de destino).
   O assistente **Replication** (Replicação) é mostrado.
3. Selecione **I have my own Target Core** (Tenho meu próprio núcleo de destino) e, em seguida, digite as informações conforme descrito na tabela a seguir.

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)	Digite o número da porta na qual o AppAssure Core se comunica com a máquina. O número de porta padrão é 8006.
User Name (Nome de usuário)	Digite o nome do usuário para acessar a máquina. Por exemplo, **Administrador**.
Password (Senha)	Digite a senha para acessar a máquina.

Se o núcleo que você deseja adicionar tiver sido emparelhado com esse núcleo de origem anteriormente, faça o seguinte:

a. Selecione **Use an existing target core** (Usar um núcleo de destino existente).
b. Selecione o núcleo de destino na lista suspensa.
c. Clique em **Next** (Avançar).
d. Pule para a etapa 7.

4. Clique em **Next** (Avançar).
5. Na página **Details** (Detalhes), digite um nome para essa configuração de replicação; por exemplo, NucleoOrigem1. Se você estiver reiniciando ou reparando uma configuração de replicação anterior, selecione a replicação **My Core has been migrated and I would like to repair** (Meu núcleo foi migrado e eu gostaria de reparar)
6. Clique em **Next** (Avançar).
7. Na página **Agents** (Agentes), selecione os agentes que você deseja replicar e, em seguida, use as listas suspensas na coluna **Repository** (Repositório) para selecionar um repositório para cada agente.
8. Se você planeja 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,é recomendado uma conexão eSATA, USB 3.0 ou outra conexão de alta velocidade ao dispositivo portátil de armazenamento.

   a. Na página **Agents** (Agentes), selecione **Use a seed drive to perform initial transfer** (Usar uma unidade de propagação para realizar a transferência inicial). Se você tem atualmente uma ou mais máquinas replicando em um núcleo de destino, você pode incluir essas máquinas protegidas na unidade de propagação selecionando a opção **With already replicated** (Com máquinas já replicadas).
   b. Clique em **Next** (Avançar).
   c. Na página **Seed Drive Location** (Local da unidade de propagação), use a lista suspensa **Location Type** (Tipo de local) para selecionar uma das opções a seguir:
      - Local: Na caixa de texto **Location** (Local), digite onde você deseja salvar a unidade de propagação; por exemplo, D:\trabalho\arquivo.
      - Rede: Na caixa de texto **Location** (Local), digite onde você deseja salvar a unidade de propagação e, em seguida, digite as credenciais para o compartilhamento de rede nas caixas de texto **User name** (Nome de usuário) e **Password** (Senha).
      - Nuvem: Na caixa de texto **Account** (Conta), selecione a conta. Para selecionar uma conta na nuvem, você precisa primeiro ter adicionado-a no Core Console. Para obter mais informações, consulte Como adicionar uma conta na nuvem. Selecione o **Container** (Contêiner) associado à sua conta. Selecione o **Folder Name** (Nome da pasta) na qual os dados arquivados devem ser salvos.
   d. Clique em **Next** (Avançar).
9. Na caixa de diálogo **Seed Drive Option** (Opção de unidade de propagação), digite as informações descritas abaixo:

Caixa de texto	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: • 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:\trabalho \arquivo, 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).

Caixa de texto	Descrição
	• Selecione a caixa de texto em branco, digite o valor e, em seguida, selecione uma unidade de medida na lista suspensa para personalizar o espaço máximo que você deseja reservar.
Customer ID (ID de cliente) (opcional)	Opcionalmente, digite a ID de cliente que foi atribuída a você pelo prestador de serviços.
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 existentes do local. Se o local não estiver vazio, agravação da unidade de propagação falha. • **Replace this core** (Substituir esse núcleo) - Substitui quaisquer dados pré-existentes que pertençam a esse núcleo, mas deixa os dados de outros núcleos intactos. • **Erase completely** (Apagar completamente) - Apaga todos os dados do diretório antes de gravar na unidade de propagação.
Comment (Comentário)	Digite um comentário ou descrição do arquivo.
Adicionar todos os agentes à unidade de propagação	Selecione os agentes que você deseja replicar usando a unidade de propagação.
Build RP chains (fix orphans) (Construir cadeias de ponto de recuperação (corrigir órfãos))	Selecione esta opção para replicar toda cadeia de ponto de recuperação para a unidade de propagação. Essa opção é selecionada por padrão. A propagação típica no AppAssure replica apenas o ponto de recuperação mais recente para a unidade de propagação, reduzindo 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.
Use compatible format (Usar formato compatível)	Selecione esta opção para criar a unidade de propagação em um formato que é compatível com as versões novas e mais antigas do AppAssure Core.

10. Na página **Agents** (Agentes), selecione os agentes que você deseja que sejam replicados para o núcleo de destino usando a unidade de propagação.
11. Clique em **Finish** (Concluir).
12. Caso você tenha criado uma unidade de propagação, envie-a para o núcleo de destino.

    O emparelhamento do núcleo de origem com o núcleo de destino está concluído. A replicação começa, mas produz pontos de recuperação órfãos no núcleo de destino até que a unidade de propagação seja consumida e forneça as imagens de base necessárias.

Consumir a unidade de propagação em um núcleo de destino

Esse procedimento só é necessário se você criou uma unidade de propagação enquanto configurava a replicação para um núcleo autogerenciado.
Para consumir a unidade de propagação em um núcleo de destino:

1. Se a unidade de propagação foi salva em um dispositivo de armazenamento portátil, como uma unidade USB, conecte a unidade ao núcleo de destino.
2. No Core Console no núcleo de destino, selecione a guia **Replication** (Replicação).
3. Em **Incoming Replication** (Replicação de entrada), selecione o núcleo de origem correto usando o menu suspenso e depois clique em **Consume** (Consumir).

   A janela Consume (Consumir) é mostrada.
4. Em **Location type** (Tipo de local), selecione uma das opções a seguir na lista suspensa:
   - Local
   - Network (Rede)
   - Cloud (Nuvem)
5. Insira as seguintes informações conforme necessário:

Caixa de texto	Descrição
Local	Digite um caminho onde a unidade de propagação está situada, como uma unidade USB ou um compartilhamento de rede (por exemplo, D:\).
User Name (Nome de usuário)	Digite o nome do usuário da pasta ou unidade compartilhada. O nome de usuário só é necessário para um caminho de rede.
Password (Senha)	Digite a senha da pasta ou unidade compartilhada. A senha só é necessária para um caminho de rede.
Account (Conta)	Selecione uma conta na lista suspensa. Para selecionar uma conta na nuvem, você precisa primeiro ter adicionado a conta ao Core Console.
Container (Contêiner)	Selecione um contêiner associado à conta no menu suspenso.
Folder Name (Nome da pasta)	Digite o nome da pasta na qual os dados arquivados estão salvos; por exemplo, -Arquivo-[DATA DE CRIAÇÃO]- [HORÁRIO DE CRIAÇÃO]

6. Clique em **Check File** (Verificar arquivo).

   Depois de o núcleo verificar o arquivo, ele preenche automaticamente a opção **Date Range** (Intervalo de datas) com as datas dos pontos de recuperação mais antigos e mais recentes contidos na unidade de propagação. Ele também importa quaisquer comentários inseridos ao configurar a replicação para um núcleo autogerenciado.
7. Em **Agent Names** (Nomes de agente) na janela **Consume** (Consumir), selecione as máquinas para as quais você deseja consumir dados e depois clique em **Consume** (Consumir).

   NOTA: Para monitorar o andamento do consumo de dados, selecione a guia **Events** (Eventos).

Abandonar uma unidade de propagação pendente

Se você criar uma unidade de propagação com o objetivo de consumi-la no núcleo de destino mas optar por não enviá-la para o local remoto, uma conexão para a unidade de propagação pendente permanece na guia **Replication** (Replicação) do núcleo de origem. Você pode querer abandonar a unidade de propagação e optar por dados de propagação mais atuais ou diferentes.

NOTA: Esse procedimento remove a conexão com a unidade de propagação pendente do Core Console no núcleo de origem. Ele não remove a unidade do local de armazenamento no qual ela está salva.

Para abandonar uma unidade de propagação pendente:

1. No Core Console no núcleo de origem, selecione a guia **Replication** (Replicação).
2. Clique em **Outstanding Seed Drive (#)** (Unidade de propagação pendente (número)).

   A seção **Outstanding seed drives** (Unidades de propagação pendentes) é mostrada. Ela inclui o nome do núcleo de destino remoto, os dados e o horário no qual a unidade de propagação foi criada e o intervalo de dados dos pontos de recuperação incluídos na unidade de propagação.
3. Clique no menu suspenso da unidade que você deseja abandonar e depois selecione **Abandon** (Abandonar).

   A janela **Outstanding Seed Drive** (Unidade de propagação pendente) é mostrada.
4. Clique em **Yes** (Sim) para confirmar a ação.

   A unidade de propagação é removida. Se não houver mais unidades de propagação no núcleo de origem, na próxima vez que você abrir a guia **Replication** (Replicação), o link **Outstanding Seed Drive (#)** (Unidade de propagação pendente (número)) e a seção **Outstanding seed drives** (Unidades de propagação pendentes) não serão mostrados.

Replicar para um núcleo gerenciado por terceiros

Um núcleo de terceiros core é um núcleo de destino que é gerenciado e mantido por um provedor de serviços gerenciados (MSP). A replicação para um núcleo gerenciado por terceiros não exige que você tenha acesso ao núcleo de destino. Depois que um cliente configura a replicação em um ou mais núcleos de origem, o MSP conclui a configuração no núcleo de destino.

NOTA: Esta configuração aplica-se à replicação em nuvem e hospedada. O AppAssure Core precisa estar instalado em todas as máquinas de núcleo origem.

Configurar a replicação para um núcleo de destino gerenciado por terceiros

NOTA: Essa configuração aplica-se à replicação hospedada e em nuvem. Se você estiver configurando o AppAssure de multiponto para a replicação do ponto, precisa realizar essa tarefa em todos os núcleos de origem.

Para configurar a replicação para um núcleo gerenciado por terceiros:

1. Navegue até o Core Console e, em seguida, clique na guia **Replication** (Replicação).
2. No menu suspenso **Actions** (Ações), clique em **Add Remote Core** (Adicionar núcleo remoto).
3. Na caixa de diálogo **Select Replication Type** (Selecionar tipo de replicação), selecione a opção **I have a subscription to a third-party providing off-site backup and disaster recovery services, and wish to replicate my backups to that service** (Tenho uma assinatura de um terceiro que fornece serviços externos de backup e recuperação de desastres e quero replicar meus backups para esse serviço) e, em seguida, digite as informações descritas da seguinte forma:

Caixa de texto	Descrição
Nome do host	Digite o nome do host, o endereço IP ou FQDN da máquina do núcleo remoto.
Porta	Digite o número da porta indicado pelo seu provedor de serviços terceirizados.

Caixa de texto	Descrição
	O número de porta padrão é 8006.

4. Clique em **Continue** (Continuar).
5. Na caixa de diálogo **Add Remote Core** (Adicionar núcleo remoto), faça o seguinte:
   a. Selecione as máquinas protegidas que serão replicadas.
   b. Selecione um repositório para cada máquina protegida.
   c. Digite o endereço de e-mail da assinatura e o ID de cliente que foi atribuído a você pelo provedor de serviço.
6. Se você planeja realizar o processo de propagação para a transferência de dados básicos, selecione **Use a seed drive to perform initial transfer** (Usar uma unidade de propagação para realizar a transferência inicial).
7. Clique em **Submit Request** (Enviar solicitação).

   NOTA: Se você selecionar **Use a seed drive to perform initial transfer** (Usar uma unidade de propagação para realizar a transferência inicial), a caixa de diálogo **Copy to Seed Drive** (Copiar para unidade de propagação) é mostrada.
8. Na caixa de diálogo **Copy to Seed Drive** (Copiar para unidade de propagação), digite as informações da unidade, conforme descrito na tabela a seguir.

Caixa de texto	Descrição
Local	Digite o caminho da unidade em que você quer salvar os dados iniciais , como um USB local.
Nome de usuário	Digite o nome do usuário para conectar-se com a unidade. NOTA: Isso é necessário se a unidade de propagação estiver localizada em um compartilhamento de rede.
Senha	Digite a senha para conectar-se com a unidade. NOTA: Isso é necessário se a unidade de propagação estiver localizada em um compartilhamento de rede.
Tamanho máximo	Selecione uma das seguintes opções: • Todo o destino. • Uma parte do espaço disponível da unidade. Para designar uma parte da unidade: a. Digite a quantidade desejada de espaço na caixa de texto. b. Selecione a medição.
Reciclar ação	Caso o caminho já contenha uma unidade de propagação, selecione uma das opções a seguir: • **Do not reuse** (Não reutilizar) - Não sobrescreve nem limpa os dados existentes em um local. Se o local não estiver vazio, a gravação da unidade de propagação falhará. • **Replace this core** (Substituir esse núcleo) - Substitui quaisquer dados preexistentes pertinentes a este núcleo, mas deixa os dados de outros núcleos intactos.

Caixa de texto	Descrição
	• **Erase completely** (Apagar completamente) - Limpa todos os dados do diretório antes de gravar a unidade de propagação.
Comentário	Digite um comentário ou descrição do arquivamento.
Agentes	Selecione os agentes que quer replicar usando a unidade de propagação.

NOTA: Uma vez que grandes quantidades de dados precisam ser copiadas para o dispositivo de armazenamento portátil, é recomendada uma conexão eSATA, USB 3.0 ou outra de alta velocidade nesse dispositivo.

9. Clique em **Start** (Iniciar) para gravar a unidade de propagação no caminho que você indicou.
10. Envie a unidade de propagação conforme instruído pelo provedor de serviços terceirizados.

Analisar uma solicitação de replicação

Uma solicitação replicação é enviada do núcleo de origem para o núcleo de destino de terceiros. Como terceiro, você pode analisar a solicitação e depois aprová-la para começar a replicação para o seu cliente ou recusá-la para evitar que a replicação ocorra.

Para analisar uma solicitação em uma replicação de núcleo de destino de terceiros:

1. Navegue até o Core Console no núcleo de destino e, em seguida, selecione a guia **Replication** (Replicação).
2. Clique em **Pending Requests (#)** (Solicitações pendentes [número]).

   A seção **Pending Replication Requests** (Solicitações de replicação pendentes) aparece.
3. Ao lado da solicitação que você quer analisar, selecione **Review** (Analisar) no menu suspenso.

   A janela **Review Replication Request** (Analisar solicitação de replicação) aparece.

   NOTA: A solicitação concluída pelo cliente determina as informações que aparecem na seção **Source Core Identity** (Identidade do núcleo de origem).
4. Na janela Review Replication Request (Analisar solicitação de replicação), escolha uma destas opções:
   - Para recusar o solicitação, clique em **Deny** (Negar).
   - Para aprovar a solicitação:

     1. – Selecione **Replace an existing replicated Core** (Substituir um núcleo replicado existente) e, em seguida, selecione um núcleo na lista suspensa.
        – Selecione **Create a new source Core** (Criar um novo núcleo de origem). Verifique o **Core Name** (Nome do núcleo), **Email Address** (Endereço de e-mail) do cliente e **Customer ID** (ID do cliente), editando as informações conforme necessário.
     2. Em **Agents** (Agentes), selecione as máquinas para aplicar a aprovação e, em seguida, selecione o repositório adequado para cada máquina, usando a lista suspensa.
     3. Opcionalmente, digite as notas que você quer mostrar na caixa **Comment** (Comentário).
     4. Clique em **Send Response** (Enviar resposta).

        A replicação é aceita.

Ignorar uma solicitação de replicação

Como prestador de serviços terceirizado de um núcleo de destino, você tem a opção de ignorar uma solicitação de replicação enviada por um cliente. Essa opção pode ser usada se um cliente enviou uma solicitação por engano ou se você quiser recusar uma solicitação sem analisá-la.

Para ignorar uma replicação de solicitação:

1. No Core Console no núcleo de destino, selecione a guia **Replication** (Replicação).
2. Na guia Replication (Replicação), clique em **Pending Requests (#)** (Solicitações pendentes [no.]).
   A seção **Pending Replication Requests** (Solicitações de replicação pendentes) é mostrada.
3. Ao lado da solicitação que você quer ignorar, selecione **Ignore** (Ignorar) no menu suspenso.
   O núcleo de destino envia uma notificação para o núcleo de origem de que a solicitação foi ignorada.

Monitorar a replicação

Quando a replicação estiver configurada, você pode monitorar o status das tarefas de replicação para os núcleos de origem e destino. Você pode atualizar informações de status, ver detalhes de replicação e muito mais.

Para monitorar a replicação:

1. No Core Console, clique na guia **Replication** (Replicação).
2. Nessa guia, você pode ver informações e monitorar o status das tarefas de replicação conforme descrito a seguir:

Tabela 3. Monitorar a replicação

Section (Seção)	Descrição	Ações disponíveis
Pending Replication Requests (Solicitações de replicação pendentes)	Lista sua ID de cliente, endereço de e-mail e nome de host quando uma solicitação de replicação é enviada para um prestador de serviços terceirizado.As informações são listadas aqui até o MSP aceitar a solicitação.	No menu suspenso, clique em **Ignore** (Ignorar) para ignorar ou rejeitar a solicitação.
Outstanding Seed Drives (Unidades de propagação faltantes)	Lista as unidades de propagação que foram gravadas, mas ainda não foram consumidas pelo núcleo de destino. Inclui o nome do núcleo remoto, a data na qual ele foi criado e o intervalo de datas.	No menu suspenso, clique em **Abandon** (Abandonar) para abandonar ou cancelar o processo de propagação.
Outgoing Replication (Replicação de saída)	Lista todos os núcleos para os quais o núcleo de origem está replicando. Inclui o nome do núcleo remoto, o estado de existência, o número de máquinas protegidas sendo replicadas e o andamento de uma transmissão de replicação.	Em um núcleo de origem, no menu suspenso, você pode selecionar as seguintes opções: • **Details** (Detalhes) — Lista a ID, URI, nome de exibição, estado, ID de cliente, endereço de e-mail e comentários do núcleo replicado. • **Change Settings** (Alterar configurações) - Lista o

Section (Seção)	Descrição	Ações disponíveis
		nome de exibição e permite que você edite o host e a porta do núcleo de destino. • **Add Agents** (Adicionar agentes) — Permite que você selecione um host em uma lista suspensa, selecione as máquinas protegidas para replicação e crie uma unidade de propagação para a transferência inicial da nova máquina protegida.
Incoming Replication (Replicação de entrada)	Lista todas as máquinas de origem a partir das quais o destino recebe os dados replicados. Inclui o nome do núcleo remoto, estado, máquinas e andamento.	Em um núcleo de destino, no menu suspenso, você pode selecionar as seguintes opções: • **Details** (Detalhes) — Lista a ID, nome de host, ID de cliente, endereço de e-mail e comentários para o núcleo replicado. • **Consume** (Consumir) — Consome os dados iniciais da unidade de propagação e os salva no repositório local.

3. Clique no botão **Refresh** (Atualizar) para atualizar as seções dessa guia com as informações mais recentes.

Gerenciar configurações de replicação

Você pode ajustar diversos parâmetros de como a replicação é executada nos núcleos de origem e de destino.

Para gerenciar as configurações de replicação:

1. No Core Console, clique na guia **Replication** (Replicação).
2. No menu suspenso **Actions** (Ações), clique em **Settings** (Configurações).
3. Na janela **Replication Settings** (Configurações de replicação), edite as configurações de replicação descritas da seguinte forma:

Opção	Descrição
Cache lifetime (Vida útil do cache)	Especifique a quantidade de tempo entre cada solicitação de status de núcleo de destino feita pelo núcleo de origem.
Volume image session timeout (Tempo limite de imagem de volume)	Especifique a quantidade de tempo que o núcleo de origem gasta tentando transferir uma imagem de volume para o núcleo de destino.

Opção	Descrição
Max. concurrent replication jobs (Número máximo de trabalhos de replicação simultâneos)	Especifique o número permitido de máquinas protegidas para replicar para o núcleo de destino por vez.
Max. parallel streams (Número máximo de fluxos paralelos)	Especifique o número permitido de conexões de rede a serem usadas por uma única máquina protegida para replicar os dados da máquina por vez.

4. Clique em **Save** (Salvar).

Remover a replicação

Você pode descontinuar a replicação e remover máquinas protegidas da replicação de várias formas. Entre as opções, estão:

- Remover um agente de replicação no núcleo de origem
- Remover um agente do núcleo de destino
- Remover um núcleo de destino da replicação
- Remover um núcleo de origem da replicação

NOTA: Remover um núcleo de destino resulta na remoção de todas as máquinas replicadas que estão protegidas por esse núcleo.

Remover uma máquina protegida de replicação do núcleo de origem

Para remover uma máquina protegida de replicação do núcleo de origem:

1. No núcleo de destino, abra o Core Console e clique na guia **Replication** (Replicação).
2. Amplie a seção **Outgoing Replication** (Replicação de saída).
3. No menu suspenso da máquina protegida que você deseja remover a replicação, clique em **Delete** (Apagar).
4. Na caixa de diálogo **Outgoing Replication** (Replicação de saída), clique em **Yes** (Sim) para confirmar a exclusão.

Remover uma máquina protegida no núcleo de destino

Para remover uma máquina protegida no núcleo de destino:

1. No núcleo de origem, abra o Core Console e clique na guia **Replication** (Replicação).
2. Amplie a seção **Incoming Replication** (Replicação de entrada).
3. No menu suspenso da máquina protegida que você deseja remover a replicação, clique em **Delete** (Apagar) e selecione uma das opções a seguir.

Opção	Descrição
Relationship Only (Apenas relação)	Remove a máquina protegida da replicação mas mantém os pontos de recuperação replicados.
With Recovery Point (Com ponto de recuperação)	Remove a máquina protegida da replicação e apaga todos os pontos de recuperação replicados recebidos da máquina.

Remover um núcleo de destino da replicação

Para remover um núcleo de destino da replicação:

1. No núcleo de destino, abra o Core Console e clique na guia **Replication** (Replicação).
2. Em **Outgoing Replication** (Replicação de saída), clique no menu suspenso ao lado do núcleo remoto que você deseja apagar e clique em **Delete** (Apagar).
3. Na caixa de diálogo **Outgoing Replication** (Replicação de saída), clique em **Yes** (Sim) para confirmar a exclusão.

Remover um núcleo de origem da replicação

NOTA: Remover um núcleo de destino resulta na remoção de todos os agentes replicados que estão protegidos por esse núcleo.

Para remover um núcleo de origem da replicação:

1. No núcleo de origem, abra o Core Console e clique na guia **Replication** (Replicação).
2. Em **Incoming Replication** (Replicação de entrada), no menu suspenso, clique em **Delete** (Apagar) e selecione uma das opções a seguir.

Opção	Descrição
Relationship Only (Apenas relação)	Remove o núcleo de origem da replicação mas mantém os pontos de recuperação replicados.
With Recovery Points (Com pontos de recuperação)	Remove o núcleo de origem da replicação e apaga todos os pontos de recuperação replicados recebidos da máquina.

3. Na caixa de diálogo **Incoming Replication** (Replicação de entrada), clique em **Yes** (Sim) para confirmar a exclusão.

Recuperar dados replicados

O recurso de replicação diária é mantido no núcleo de origem, enquanto só o núcleo de destino é capaz de concluir as funções necessárias para a recuperação de desastres.

Para a recuperação de desastres, o núcleo de destino pode usar os pontos de recuperação replicados para a recuperação dos agentes e núcleo protegidos.

Você pode executar as seguintes opções de recuperação no núcleo de destino:

- Montar pontos de recuperação.
- Reverter para pontos de recuperação.
- Realizar uma exportação de máquina virtual (MV).

- Executar uma restauração sem sistema operacional (BMR).
- Executar o failback (caso você tenha um ambiente de failover/failback de replicação configurado).

Roteiro para failover e failback

Quando houver uma situação de desastre em que o núcleo de origem e a respectiva máquina protegida falharam, você pode ativar a failover no AppAssure para alternar a proteção ao núcleo idêntico de failover (destino) e iniciar um novo agente (replicado), idêntico ao agente que falhou. Depois do reparo do núcleo de origem e dos agentes, você pode realizar o failback para restaurar os dados a partir do núcleo e do agente com failover para o núcleo de origem e o agente. No AppAssure, a failover e o failback envolvem os procedimentos a seguir.

- Configurar um ambiente para failover.
- Realize o failover para o núcleo de destino e o agente associado.
- Restaure o núcleo de origem realizando o failback.

Configurar um ambiente para failover

A configuração do ambiente para failover exige que você tenha um núcleo de origem e destino e o agente associado configurado para a replicação. Execute o procedimento descrito para configurar uma replicação para failover.

Para configurar um ambiente para failover:

1. Instale um Core para a origem e um Core para o destino.
2. Instale um AppAssure Agent que será protegido pelo núcleo de origem.
3. Crie um repositório no núcleo de origem e outro no de destino.

   Para obter mais informações, consulte Criar um repositório.
4. Adicione o agente para proteção sob o núcleo de origem.

   Para obter mais informações, consulte Proteger uma máquina.
5. Configure uma replicação do núcleo de origem para o de destino e replique o agente protegido com todos os pontos de recuperação.

   Siga o procedimento Replicar para um núcleo autogerenciado para adicionar o núcleo de destino da replicação.

Realizar o failover no núcleo de destino

Quando você encontrar uma situação de desastre em que o núcleo de origem e as máquinas protegidas associadas falharam, você pode ativar o failover para alternar a proteção para o núcleo de ativação pós-falha (destino) idêntico. O núcleo de destino torna-se o único núcleo que protege os dados em seu ambiente e então você inicia um novo agente para substituir temporariamente o agente que falhou.

Para realizar o failover no núcleo de destino:

1. Navegue até o Core Console no núcleo de destino e, em seguida, clique na guia **Replication** (Replicação).
2. Em **Incoming Replication** (Replicação de entrada), selecione o núcleo de origem e expanda os detalhes sob o agente individual.
3. No menu **Actions** (Ações) do respectivo núcleo, clique em **Failover** (Failover).

   O status dessa máquina na tabela muda para **Failover** (Failover).
4. Clique na guia **Machines** (Máquinas) e, em seguida, selecione a máquina que tem o agente AppAssure associado com os pontos de recuperação.

5. Exporte as informações do ponto de recuperação de backup nesse agente para uma máquina virtual.
6. Desligue a máquina que tem o agente do AppAssure.
7. Inicie a máquina virtual que agora inclui as informações do backup exportado.

   Aguarde enquanto o software do driver de dispositivo é instalado.
8. Reinicialize a máquina virtual e aguarde o serviço do agente iniciar.
9. Volte ao Core Console para o núcleo de destino e verifique se o novo agente é mostrado na guia **Machines** (Máquinas) sob **Protected Machines** (Máquinas protegidas) e na guia **Replication** (Replicação) sob **Incoming Replication** (Replicação de entrada).
10. Force múltiplos instantâneos e verifique se são concluídos corretamente.

    Para obter mais informações, consulte Forçar um instantâneo.
11. Agora, você pode prosseguir com a realização do failback.

    Para obter mais informações, consulte Realizar failback.

Realizar o failback

Depois de você reparar ou substituir o núcleo de origem com falha e as máquinas protegidas, precisará mover os dados das máquinas com ativação pós-falha para restaurar as máquinas de origem.

Para realizar o failback:

1. Navegue até o Core Console no núcleo de destino e, em seguida, clique na guia **Replication** (Replicação).
2. Em **Incoming Replication** (Replicação de entrada), selecione o agente com ativação pós-falha e expanda os detalhes.
3. No menu **Actions** (Ações), clique em **Failback**.

   A caixa de diálogo **Failback Warnings** (Advertências de failback) é aberta para descrever as etapas que você precisará seguir antes de clicar no botão **Start Failback** (Iniciar failback).
4. Clique em **Cancel** (Cancelar).
5. Se a máquina com ativação pós-falha estiver executando o Microsoft SQL Server ou o Microsoft Exchange Server, pare esses serviços.
6. No Core Console no núcleo de destino, clique na guia **Tools** (Ferramentas).
7. Crie um arquivamento do agente com ativação pós-falha e faça sua saída para o disco ou um local de compartilhamento de rede.
8. Depois de criar o arquivamento, navegue até o Core Console no núcleo de origem recém-reparado e, em seguida, clique na guia **Tools** (Ferramentas).
9. Importe o arquivamento que você acabou de criar na Etapa 7.
10. Volte para o Core Console no núcleo de destino e, em seguida, clique na guia **Replication** (Replicação).
11. Em **Incoming Replication** (Replicação de entrada), selecione o agente com ativação pós-falha e expanda os detalhes.
12. No menu **Actions** (Ações), clique em **Failback**.
13. Na caixa de diálogo **Failback Warnings** (Advertências de failback), clique em **Start Failback** (Iniciar failback).
14. Desligue a máquina que contém o agente exportado que foi criado durante a ativação pós-falha.
15. Execute uma restauração sem sistema operacional (BMR) para o núcleo de origem e o agente.

    NOTA: Quando você iniciar a restauração, precisará usar os pontos de recuperação que foram importados do núcleo de destino para o agente na máquina virtual.

16. Aguarde até o BMR e o serviço do agente reiniciarem e, em seguida, veja e anote os detalhes da conexão de rede da máquina.
17. Navegue até o Core Console no núcleo de origem e, na guia **Machines** (Máquinas), modifique as configurações de proteção da máquina para adicionar os novos detalhes da conexão de rede.
18. Navegue até o Core Console no núcleo de destino e apague o agente da guia **Replication** (Replicação).
19. No Core Console do núcleo de origem, configure novamente uma replicação entre a origem e o destino, clicando na guia **Replication** (Replicação) e, em seguida, adicione o núcleo de destino para a replicação.

Gerenciar os eventos

O gerenciamento dos eventos do núcleo ajuda no monitoramento da integridade e do uso do Core. O núcleo inclui conjuntos predefinidos de eventos, que podem ser usados para notificar os administradores de problemas críticos no Core ou nas tarefas de backup .

Na guia **Events** (Eventos), você pode gerenciar os grupos de notificações, as configurações de SMTP de e-mail, a redução da repetição e a retenção de eventos. A opção Notification Groups (Grupos de notificações) permite gerenciar esses grupos, nos quais você pode:

- Especificar um evento para gerar um alerta para o seguinte:
  - Clusters (Agrupamentos)
  - Attachability (Capacidade de conexão)
  - Jobs (Tarefas)
  - Licensing (Licenciamento)
  - Log Truncation (Truncagem de log)
  - Archive (Arquivamento)
  - Core Service (Serviço do Core)
  - Export (Exportação)
  - Protection (Proteção)
  - Replication (Replicação)
  - Rollback (Reversão)
  - SMTP Server Settings (Configurações do servidor SMTP)
  - Enabled Trace logs (Logs de rastreamento ativados)
  - Cloud Configuration (Configuração da nuvem)
- Especifique o tipo de alerta (erro, advertência e informativo).
- Especifique para quem e para onde os alertas são enviados. As opções são:
  - Email Address (Endereço de e-mail)
  - Windows Events Logs (Logs de eventos do Windows)
  - Syslog Server (Servidor syslog)
- Especifique um limite de tempo para a repetição.
- Especifique o período de retenção para todos os eventos.

Configurar os grupos de notificações

Para configurar os grupos de notificações:

1. No Core, selecione a guia **Configuration** (Configuração).
2. Na opção **Manage** (Gerenciar), clique em **Events** (Eventos).
3. Clique em **Add Group** (Adicionar grupo).

   A caixa de diálogo **Add Notification Group** (Adicionar grupo de notificações) é exibida e mostra três painéis:

   - **General (Gerais)**
   - **Enable Events (Ativar eventos)**
   - **Notification Options (Opções de notificação)**
4. No painel **General** (Geral), digite as informações básicas do grupo de notificações descritas a seguir:

Caixa de texto	Descrição
Name (Nome)	Digite um nome para o grupo de notificações de evento, utilizado para identificar esse grupo.
Description (Descrição)	Digite uma descrição para o grupo de notificações de eventos, utilizada para descrever a finalidade desse grupo.

5. No painel **Enable Events** (Ativar eventos), selecione as condições para as quais você quer criar e relatar logs (alertas) de eventos.

   Você pode optar por criar alertas para:

   - **All Events (Todos os eventos)**
   - **Appliance Events (Eventos do dispositivo)**
   - **Boot CD (CD de inicialização)**
   - **Security (Segurança)**
   - **DatabaseRetention (Retenção de banco de dados)**
   - **LocalMount (Montagem local)**
   - **Clusters (Agrupamentos)**
   - **Notification (Notificação)**
   - **Power Shell Scripting (Scripts do PowerShell)**
   - **PushInstall (Instalação forçada)**
   - **Nightly Jobs (Tarefas noturnas)**
   - **Attachability (Capacidade de conexão)**
   - **Jobs (Tarefas)**
   - **Licensing (Licenciamento)**
   - **Log Truncation (Truncagem de log)**
   - **Archive (Arquivamento)**
   - **Core Service (Serviço do Core)**
   - **Export (Exportação)**
   - **Protection (Proteção)**
   - **Replication (Replicação)**
   - **Repository (Repositório)**
   - **Rollback (Reversão)**

- **Rollup (Implantação)**

6. No painel **Notification Options** (Opções de notificação), especifique como você quer lidar com o processo de notificação.

   As opções de notificação são:

Caixa de texto	Descrição
Notify by e-mail (Notificar por e-mail)	Atribua os destinatários da notificação por e-mail. Você pode optar por especificar vários endereços de e-mail separados, bem como cópias ocultas e de carbono. Você pode escolher: • **To: (Para)** • **CC: (Com cópia)** • **CCO: (Com cópia oculta)**
Notify by Windows Event Log (Notificar por log de eventos do Windows)	Selecione essa opção se quiser que os alertas sejam relatados através do Log de eventos do Windows. Ele é usado para especificar se a notificação dos alertas precisa ser relatada através do Log de eventos do Windows.
Notify by sys logd (Notificar por sys logd)	Selecione essa opção se quiser que os alertas sejam relatados através do sys logd. Especifique os detalhes do sys logd nas seguintes caixas de texto: • **Hostname: (Nome de host)** • **Port:1 (Porta:1)**

7. Clique em **OK**.

Configurar um servidor de e-mail e um modelo de notificação por e-mail

Se quiser receber notificações por e-mail sobre eventos, configure um servidor de e-mail e um modelo de notificação de e-mail.

NOTA: Você precisa também definir as configurações de grupo de notificações, incluindo a ativação da opção **Notify by email** (Notificar por e-mail), antes de as mensagens de alerta de e-mail serem enviadas. Para obter mais informações sobre a especificação de eventos para receber alertas de e-mail, consulte "Configurar os grupos de notificações para eventos do sistema" no Guia do Usuário do Dispositivo *Dell DL4300*.

Para configurar um servidor de e-mail e um modelo de notificação por e-mail:

1. No Core, selecione a guia **Configuration** (Configuração).
2. Na opção **Manage** (Gerenciar), clique em **Events** (Eventos).
3. No painel **Email SMTP Settings** (Configurações de SMTP do e-mail), clique em **Change** (Alterar).

   A caixa de diálogo de edição **Email Notification Configuration** (Configuração de notificação de e-mail) é exibida.
4. Selecione **Enable Email Notifications** (Ativar notificações de e-mail) e, em seguida, insira os detalhes para o servidor de e-mail descritos a seguir:

Caixa de texto	Descrição
SMTP Server (Servidor SMTP)	Digite o nome do servidor de e-mail que será usado pelo modelo de notificação por e-mail. A convenção de nomenclatura é o nome de host, o domínio e o sufixo; por exemplo **smtp.gmail.com**.
Port (Porta)	Digite um número de porta. Ele é usado para identificar a porta para o servidor de e-mail; por exemplo, a porta 587 para o Gmail. O padrão é 25.
Timeout (seconds) (Tempo limite (segundos))	Para especificar por quanto tempo será tentado realizar uma conexão antes do tempo limite expirar, digite um valor inteiro. Ele é usado para estabelecer o tempo, em segundos, ao tentar se conectar ao servidor de e-mail antes que o tempo limite expire. O padrão é 30 segundos.
TLS	Selecione esta opção se o servidor de e-mail usar uma conexão segura, como Transport Layer Security (TLS) ou Secure Sockets Layer (SSL).
Username (Nome de usuário)	Digite um nome de usuário para o servidor de e-mail.
Senha	Digite uma senha para acessar o servidor de e-mail.
De	Digite um endereço de e-mail de retorno. Ele é usado para especificar o endereço de e-mail de retorno para o modelo de notificação por e-mail; por exemplo, **noreply@localhost.com**.
Email Subject (Assunto do e-mail)	Digite o assunto para o modelo de e-mail. Ele é usado para definir o assunto do modelo de notificação por e-mail; por exemplo, `<hostname> - <level> <name>`.
E-mail	Digite as informações do corpo do modelo que descrevem o evento, quando ele ocorreu e a gravidade.

5. Clique em **Send Test Email** (Enviar e-mail de teste) e verifique os resultados.
6. Depois que estiver satisfeito com os resultados dos testes, clique em **OK**.

Configurar a redução da repetição

Para configurar a redução da repetição:

1. No Core Console, clique na guia **Configuration** (Configuração).
2. Na opção **Manage** (Gerenciar), clique em **Events** (Eventos).
3. Na área **Repetition Reduction** (Redução da repetição), clique em **Change** (Alterar).
   A caixa de diálogo Repetition Reduction (Redução da repetição) aparece.
4. Selecione **Enable Repetition Reduction** (Ativar repetição da redução).
5. Na caixa de texto **Store events for X minutes** (Armazenar eventos por X minutos), digite o número de minutos para armazenar os eventos para a redução da repetição.
6. Clique em **OK**.

Configurar a retenção do evento

Para configurar a retenção do evento:

1. No Core, clique na guia **Configuration** (Configuração).
2. Na opção **Manage** (Gerenciar), clique em **Events** (Eventos).
3. Em **Database Connection Settings** (Configurações de conexão com o banco de dados), clique em **Change** (Alterar).

   A caixa de diálogo **Database Connection Settings** (Configurações de conexão com o banco de dados) aparece.
4. Na caixa de texto **Retain event and job history for** (Reter histórico do evento e das tarefas por), digite o número de dias para reter informações sobre eventos.

   Por exemplo, você pode selecionar 30 dias (padrão).
5. Clique em **Save** (Salvar).

Gerenciar a recuperação

O Core pode restaurar os dados instantaneamente ou recuperar as máquinas para máquinas físicas ou virtuais a partir dos pontos de recuperação. Os pontos de recuperação contêm instantâneos do volume do agente capturados no nível do bloco. Esses instantâneos identificam o aplicativo, o que significa que todas as transações abertas e os logs das transações implantadas são concluídos e os caches são enviados ao disco antes de criar o instantâneo. O uso combinado de instantâneos que identificam o aplicativo e da Recuperação verificada permite que o Core realize vários tipos de recuperação, como:

- Recuperação de arquivos e pastas
- Recuperação de volumes de dados usando a Recuperação em tempo real
- Recuperação de volumes de dados para o Microsoft Exchange Server e o Microsoft SQL Server, usando a Recuperação em tempo real
- Restauração sem sistema operacional, usando a recuperação universal
- Restauração sem sistema operacional para hardware diferente, usando a recuperação universal
- Exportação ad-hoc e contínua para máquinas virtuais

Sobre as informações do sistema

O AppAssure permite ver as informações sobre o Core, que contêm informações do sistema, locais, volumes montados e as conexões do mecanismo do AppAssure.

Se você quiser desmontar pontos de recuperação individuais ou todos os que estão montados localmente em um núcleo, use a opção **Mount** (Montar) na guia **Tools** (Ferramentas).

Ver as informações do sistema

Para ver as informações do sistema:

1. Navegue até o Core e, em seguida, selecione a guia **Tools** (Ferramentas).
2. Na opção **Tools** (Ferramentas), clique em **System Info** (Informações do sistema).

Fazer o download de instaladores

Você pode fazer o download de instaladores no Core. Na guia **Tools** (Ferramentas), você pode escolher o download do Instalador do Agent ou do Utilitário de montagem local.

NOTA: Para ter acesso ao Instalador do Agent, consulte Fazer download e instalar o Instalador do Agent. Para obter mais informações sobre como implementar o Instalador do Agent, consulte o *Guia de Implementação do Dispositivo Dell DL4300*, disponível no site **Dell.com/support/home**. Para o acesso ao Instalador do utilitário de montagem local, consulte Sobre o Utilitário de montagem local e para obter mais informações sobre o utilitário, consulte Fazer download e instalar o utilitário Montagem local.

Sobre o instalador do Agent

O instalador do Agent é usado para instalar o aplicativo AppAssure Agent nas máquinas que serão protegidas pelo Core. Se você determinar que uma máquina exige o Instalador do Agent, pode fazer o download do instalador da web na guia **Tools** (Ferramentas) do Core .

NOTA: O download do Core é feito no Portal de licenças. Para fazer o download do instalador do Core, visite **https://licenseportal.com**.

Fazer o download e instalar o instalador do agente

Você pode fazer o download e implementar o instalador do agente em qualquer máquina que seja protegida pelo Core.

Para fazer o download e instalar o instalador do agente:

1. Faça o download do arquivo do instalador do Agent no Portal de licenças ou no Core.
   Por exemplo: **Agent-X64-5.3.x.xxxxx.exe**
2. Clique em **Save File** (Salvar arquivo).
   Para obter mais informações sobre a instalação do agentes, consulte o *Guia de Implementação do Dispositivo Dell DL4300* disponível em **Dell.com/support/home**.

Sobre o utilitário Montagem local

O utilitário Montagem local (LMU) é um aplicativo para download que permite montar um ponto de recuperação em um Core remoto a partir de qualquer máquina. Esse leve utilitário inclui os drivers `aavdisk` e `aavstor`, mas não é executado como um serviço. Quando você instalar o utilitário, por padrão, ele é instalado no diretório **C:\Program Files\AppRecovery\Local Mount Utility** e um atalho é mostrado na área de trabalho da máquina.

Embora o utilitário tenha sido projetado para o acesso remoto aos núcleos, você também pode instalar o LMU no Core. Quando executado em um núcleo, o aplicativo reconhece e mostra todas as montagens desse núcleo, incluindo as que foram efetuadas através do Core Console. Da mesma forma, as montagens realizadas no LMU também são mostradas no console.

Fazer download e instalar o utilitário Montagem local

Para fazer o download e instalar o LMU (Utilitário Montagem local):

1. Na máquina em que você quer instalar o LMU, acesse o Core Console digitando o URL do console no navegador e faça o login com o seu nome de usuário e senha.
2. No Core Console, clique na guia **Tools** (Ferramentas).
3. Na guia **Tools** (Ferramentas), clique em **Downloads**.
4. Em **Local Mount Utility** (Utilitário de montagem local), clique no link **Download web installer** (Fazer download do instalador da web).
5. Na janela **Opening LocalMountUtility-Web.exe** (Abrindo LocalMountUtility-Web.exe), clique em **Save File** (Salvar arquivo).

   O arquivo é salvo na pasta local de Downloads. Em alguns navegadores, a pasta será aberta automaticamente.
6. Na pasta **Downloads**, clique com o botão direito no executável **LocalMount Utility-Web** e clique em **Open** (Abrir).

   Dependendo da configuração da máquina, a janela **User Account Control** (Controle da conta do usuário) pode aparecer.
7. Se a janela **User Account Control** (Controle de conta de usuário) aparecer, clique em **Yes** (Sim) para permitir que o programa faça alterações na máquina.

   O assistente **Instalação do Utilitário de montagem local do AppAssure** inicia.
8. Na tela **Welcome** (Bem-vindo) do assistente **Instalação do utilitário Montagem local**, clique em **Next** (Avançar) para continuar até a página **License Agreement** (Contrato de licença).
9. Na página **License Agreement** (Contrato de licença), selecione **I accept the terms in the license agreement** (Eu aceito os termos do contrato de licença) e clique em **Next** (Avançar) para continuar até a página **Prerequisites** (Pré-requisitos).
10. Na página **Prerequisites** (Pré-requisitos), instale os pré-requisitos necessários e clique em **Next** (Avançar) para continuar até a página **Installation Options** (Opções de instalação).
11. Na página **Installation Options** (Opções de instalação), execute as seguintes tarefas:
    a. Escolha uma pasta de destino para o LMU, clicando no botão **Change** (Alterar).

       NOTA: A pasta de destino padrão é C:\Arquivos de Programas\AppRecovery \LocalMountUtility.
    b. Selecione se quer ou não **Allow Local Mount Utility** (Permitir Utilitário de montagem local) para enviar automaticamente as informações de uso e de diagnóstico para a AppAssure Software, Inc.
    c. Clique em **Next** (Avançar) para continuar até a página **Progress** (Andamento) e fazer download do aplicativo. O aplicativo faz o download da pasta de destino, com o andamento mostrado na respectiva barra . Quando terminar, o assistente avança automaticamente para a página **Completed** (Concluído).
12. Clique em **Finish (Concluir)** para fechar o assistente.

Adicionar um núcleo ao utilitário Montagem local

Para montar um ponto de recuperação, você precisa adicionar o núcleo ao LMU. Não há limite quanto ao número de núcleos que você pode adicionar.

Para adicionar um núcleo ao Utilitário de montagem local:

1. Na máquina em que o LMU está instalado, abra o LMU clicando duas vezes no ícone da área de trabalho.
2. Se a janela **User Account Control** (Controle de conta de usuário) abrir, clique em **Yes** (Sim) para permitir que o programa faça alterações na máquina.
3. No canto superior esquerdo da janela do Utilitário de montagem local do AppAssure, clique em **Add core** (Adicionar núcleo).
4. Na janela **Add Core** (Adicionar núcleo), digite as credenciais solicitadas descritas da seguinte forma:

Caixa de texto	Descrição
Nome do host	O nome do Núcleo a partir do qual você quer montar os pontos de recuperação. NOTA: Com a instalação do LMU em um núcleo, o LMU adiciona automaticamente a máquina localhost.
Porta	O número de porta usado para a comunicação com o Core. O número de porta padrão é 8006.
Usar minhas credenciais de usuário do Windows	Selecione essa opção se for usar as mesmas credenciais para acessar o Core e o Windows.
Usar credenciais específicas	Selecione essa opção se for usar credenciais diferentes para acessar o Core e o Windows.
Nome de usuário	O nome de usuário usado para acessar a máquina Core. NOTA: Essa opção está disponível somente se você optar por usar credenciais específicas.
Senha	A senha usada para acessar a máquina Core. NOTA: Essa opção está disponível somente se você optar por usar credenciais específicas.

5. Clique em **Connect** (Conectar).
6. Se você estiver adicionando múltiplos núcleos, repita as Etapas 3 a 5 , conforme necessário.

Explorar um ponto de recuperação montado usando o utilitário Montagem local

NOTA: Esse procedimento não é necessário se você estiver explorando um ponto de recuperação imediatamente após sua montagem, pois a pasta que contém o ponto de recuperação é aberta automaticamente na conclusão do procedimento de montagem.

Para explorar um ponto de recuperação montado usando o utilitário Montagem local:

1. Na máquina em que o LMU está instalado, abra o LMU clicando duas vezes no ícone da área de trabalho.
2. Na tela principal **Local Mount Recovery** (Recuperação da montagem local), clique em **Active mounts** (Montagens ativas).

A janela **Active mounts** (Montagens ativas) é aberta e mostra todos os pontos de recuperação montados.

3. Clique em **Explore** (Explorar) ao lado do ponto de recuperação a partir do qual você quer recuperar, para abrir a pasta de volumes desduplicados.

Montar um ponto de recuperação usando o utilitário Montagem local

Antes de montar um ponto de recuperação, o LMU deve se conectar ao Core no qual o ponto de recuperação está armazenado. Conforme descrito em Adicionar um núcleo ao utilitário Montagem local, o número de núcleos que podem ser adicionados ao LMU é ilimitado; no entanto, o aplicativo pode se conectar a somente um núcleo de cada vez. Por exemplo, se você montar um ponto de recuperação de um agente protegido por um núcleo e, em seguida, montar um ponto de recuperação de um agente protegido por um núcleo diferente, o LMU se desconecta automaticamente do primeiro núcleo para estabelecer uma conexão com o segundo.

Para montar um ponto de recuperação usando o utilitário Montagem local:

1. Na máquina em que o LMU está instalado, abra o LMU clicando duas vezes no ícone da área de trabalho.
2. Na janela principal do **AppAssure Local Mount Utility** (Utilitário Montagem local AppAssure), expanda o núcleo desejado na árvore de navegação para revelar os agentes protegidos.
3. Na árvore de navegação, selecione o agente desejado.

   Os pontos de recuperação aparecem no quadro principal.
4. Expanda o ponto de recuperação que você quer montar para revelar volumes de disco ou bancos de dados individuais.
5. Clique com o botão direito no ponto de recuperação que você quer montar e selecione uma das opções a seguir:
   - Mount (Montar)
   - Mount writable (Montar gravável)
   - Mount with previous writes (Montar com gravações prévias)
   - Advanced mount (Montagem avançada)
6. Na janela **Advanced Mount** (Montagem avançada), complete as opções descritas a seguir:

Caixa de texto	Descrição
Mount point path (Caminho do ponto de montagem)	Para selecionar um caminho para os pontos de recuperação diferentes do padrão , clique no botão **Browse** (Procurar).
Mount type (Tipo de montagem)	Selecione uma das seguintes opções: • Mount read-only (Montar somente leitura) • Mount writable (Montar gravável) • Mount read-only with previous writes (Montar somente leitura com gravações prévias)

7. Clique em **Mount** (Montar).

O LMU abre automaticamente a pasta que contém o ponto de recuperação montado.

NOTA: Quando você seleciona um ponto de recuperação já montado, a caixa de diálogo **Mounting** (Montagem) solicita que você desmonte o ponto de recuperação.

Desmontar um ponto de recuperação usando o utilitário Montagem local

Para desmontar um ponto de recuperação usando o utilitário Montagem local:

1. Na máquina em que o LMU está instalado, abra o LMU clicando duas vezes no ícone da área de trabalho.
2. Na tela principal **Local Mount Recovery** (Recuperação da montagem local), clique em **Active mounts** (Montagens ativas).

   A janela **Active mounts** (Montagens ativas) é aberta e mostra todos os pontos de recuperação montados.
3. Selecione uma das opções descritas na tabela abaixo para desmontar os pontos de recuperação.

Opção	Descrição
Desmontar	Desmonta apenas o ponto de recuperação adjacente. a. Clique em **Dismount** (Desmontar) ao lado do ponto de recuperação selecionado. b. Feche a janela.
Desmontar todos	Desmonta todos os pontos de recuperação montados. a. Clique em **Dismount all** (Desmontar todos). b. Na janela **Dismount all** (Desmontar todos), clique em **Yes** (Sim) para confirmar. c. Feche a janela.

Sobre o menu da bandeja de utilitários de montagem local

O menu da bandeja LMU está localizado na sua barra de tarefas da área de trabalho. Clique com o botão direito no ícone para revelar as seguintes opções:

Procurar pontos de recuperação	Abre a tela principal do LMU.
Montagens ativas	Abre a tela Montagens ativas.
Opção	Abre a tela Options (Opções), em que você pode alterar o **Default Mount Point Directory** (Diretório padrão do ponto de montagem), as **Default Core Credentials** (Credenciais padrão do Core) e o **Language** (Idioma) da interface do usuário do LMU.
Sobre	Abre a tela de abertura das informações de licenciamento.
Exit (Sair)	Fecha o aplicativo.

NOTA: O X no canto superior da tela principal minimiza o aplicativo para a bandeja.

Usar as opções do Core e do agente

Ao clicar com o botão direito no Core ou no agente na tela principal do LMU, você pode usar certas opções. Entre elas, estão:

- Opções do localhost
- Opções do Core remoto
- Opções do agente

Acessar as opções do localhost

Para acessar as opções do localhost, clique com o botão direito no Core ou no Agent e, em seguida, clique em **Reconnect** (Reconectar) ao Core. As informações do Core são atualizadas; por exemplo, os agentes adicionados recentemente.

Acessar as opções do núcleo remoto

Para acessar as opções do núcleo remoto, clique com o botão direito no núcleo ou no agente e, em seguida, selecione uma das opções de núcleo remoto da seguinte maneira:

Opção	Descrição
Reconectar ao núcleo	Atualiza as informações do núcleo, como agentes adicionados recentemente.
Remover núcleo	Apaga o núcleo do **utilitário Montagem local**.
Editar núcleo	Abre a janela **Edit Core** (Editar núcleo), em que você pode alterar o nome do host , a porta e as credenciais.

Acessar as opções do Agent

Para acessar as opções do Agent, clique com o botão direito no Core ou no agente e, em seguida, clique em **Refresh recovery points** (Atualizar pontos de recuperação). A lista de pontos de recuperação referentes ao agente selecionado é atualizada.

Gerenciar as políticas de retenção

Os instantâneos periódicos do backup de todos os servidores protegidos acumulam-se no Core com o passar do tempo. As políticas de retenção são usadas para reter os instantâneos do backup durante períodos mais longos e para ajudar no seu gerenciamento . A política de retenção é imposta por um processo de implantação noturna que ajuda a apagar backups obsoletos e antigos. Para obter informações sobre como configurar as políticas de retenção, consulte Personalizar as configurações da política de retenção.

Arquivamento em uma nuvem

Você pode arquivar os seus dados em uma nuvem transferindo-os por upload para uma variedade de provedores de nuvem diretamente do Core Console. As nuvens compatíveis são o Windows Azure, Amazon, Rackspace e todos os provedores baseados em OpenStack.

Para exportar um arquivamento para uma nuvem:

- Adicione sua conta da nuvem ao Core Console. Para obter mais informações, consulte Adicionar uma conta na nuvem.
- Arquive seus dados e exporte-os para uma conta na nuvem.
- Recupere os dados arquivados importando-os do local da nuvem.

Sobre arquivamento

As políticas de retenção impõem os períodos pelos quais os backups são armazenados em mídias de curto-prazo (rápidas e caras). Algumas vezes, certas empresas e requisitos técnicos demandam a retenção estendida desses backups, mas o uso de armazenamento rápido é um custo proibitivo. Portanto, esse requisito cria uma necessidade de armazenamento de longo prazo (lento e barato). Frequentemente, as empresas usam armazenamento de longo prazo para arquivamento de dados de conformidade e não conformidade. O recurso de arquivamento no AppAssure é usado para suportar a retenção estendida de dados de conformidade e não conformidade. Ele também é usado para fazer o seeding de dados de replicação para um núcleo de réplica remoto.

Criar um arquivamento

Para criar um arquivamento

1. No Core Console, clique na guia **Configuration** (Configuração).
2. Na opção **Manage** (Gerenciar), clique em **Archive** (Arquivamento).
   A caixa de diálogo **Create Archive** (Criar arquivamento) aparece.
3. Na caixa de diálogo **Create Archive** (Criar arquivamento), digite os detalhes do arquivamento da seguinte forma:

Caixa de texto	Descrição
Intervalo de datas	Para especificar o intervalo de datas, selecione as datas inicial e final.
Senha do arquivamento	Digite uma senha para o arquivamento, usada para estabelecer as credenciais de login a fim de proteger o arquivamento.
Confirmar	Digite novamente a senha para proteger o arquivamento; usado para validar as informações que você digitou na caixa de texto **Archive Password** (Senha do arquivamento).
Local de saída	Digite o local de saída, usado para definir o caminho do local em que você quer que o arquivamento resida. Isso pode ser um disco local ou um compartilhamento de rede. Por exemplo, **d:\work\archive** ou **\\servername \sharename** para caminhos de rede. **NOTA:** Se o local de saída for um compartilhamento de rede, digite um nome de usuário e senha para conexão ao compartilhamento.
Nome de usuário	Digite um nome de usuário, que é usado para estabelecer credenciais de login para o compartilhamento de rede.
Senha	Digite uma senha para o caminho da rede, que é usada para estabelecer credenciais de login para o compartilhamento de rede.
Tamanho máximo	Digite o espaço para usar para o arquivamento. Você pode selecionar entre: • Todo destino • Quantidade específica em MB ou GB
Reciclar ação	Selecione a ação adequada de reciclagem.

Caixa de texto	Descrição
Comentário	Digite as informações adicionais cuja captura é necessária para o arquivamento.

4. Clique em **Archive** (Arquivamento).

Configurar um arquivamento agendado

O recurso de Arquivamento agendado permite definir quando um arquivamento de uma máquina selecionada será automaticamente criado e salvo no local especificado. Isso atende às situações em que você gostaria de salvar arquivamentos frequentes de uma máquina, sem o inconveniente de precisar criá-los manualmente. Conclua as etapas no procedimento a seguir para programar o arquivamento automático.
Para configurar um arquivamento agendado:

1. No Core Console, clique na guia **Tools** (Ferramentas).
2. Na opção **Archive** (Arquivamento), clique em **Scheduled** (Agendado).
3. Na página Scheduled Archive (Arquivamento agendado), clique em **Add** (Adicionar).

   A caixa de diálogo **Add Archive Wizard** (Assistente para adicionar arquivamento) é mostrada.
4. Na página **Location** (Local) do **Add Archive Wizard** (Assistente para adicionar arquivamento), selecione uma das opções na lista suspensa **Location Type** (Tipo do local):
   - Local: local de saída - Digite o local para a saída. Define o caminho do local onde você quer que o arquivo resida.
   - Rede
     - Output location (Local de saída): digite o local para a saída. Define o caminho do local onde você quer que o arquivo fique.
     - User Name (Nome de usuário): digite um nome de usuário. Estabelece credenciais de login para o compartilhamento de rede.
     - Password (Senha): digite uma senha para o caminho de rede. Estabelece credenciais de login para o compartilhamento de rede.
   - Cloud
     - Account (Conta de nuvem): selecione uma conta na lista suspensa. Para selecionar uma conta de nuvem, ela precisa primeiro ter sido adicionada ao Core Console.
     - Container (Contêiner): selecione um contêiner associado à sua conta no menu suspenso.
     - Folder Name (Nome da pasta): digite um nome para a pasta na qual os dados arquivados serão salvos. O nome padrão é AppAssure-5-Archive-[DATA DA CRIAÇÃO]-[HORA DA CRIAÇÃO]
5. Clique em **Next** (Avançar).
6. Na página **Machines** (Máquinas) do assistente, selecione as máquinas protegidas que contêm os pontos de recuperação que você quer arquivar.
7. Clique em **Next** (Avançar)
8. Na página **Options** (Opções), selecione uma das seguintes ações de reciclagem na lista suspensa:
   - **Replace this Core** (Substituir este núcleo): substitui os dados arquivados existentes pertencentes a este núcleo, mas deixa os dados de outros núcleos intactos.
   - **Erase completely** (Apagar completamente): limpa todos os dados arquivados do diretório antes de gravar o novo arquivamento.
   - **Incremental**: permite adicionar pontos de recuperação a um arquivamento existente. Compara os pontos de recuperação para evitar duplicar os dados já existentes no arquivamento.
9. Na página **Schedule** (Agendamento), selecione uma das seguintes opções de frequência do envio dos dados:

- Daily: At time (Diariamente: no horário) – Selecione a hora do dia em que você quer criar um arquivamento diário.
- Semanal
  - At day of week (No dia da semana): selecione um dia da semana para criar automaticamente o arquivamento.
  - At time (No horário): selecione a hora do dia em que você quer criar um arquivamento diário.
- Mensalmente
  - At day of months (No dia do mês): selecione o dia do mês para criar automaticamente o arquivamento.
  - At time (No horário): selecione a hora do dia em que você quer criar um arquivamento diário.

10. Para pausar o arquivamento e retomá-lo mais tarde, selecione **Initial pause archiving** (Pausa inicial do arquivamento).

    Você pode pausar o arquivamento agendado se precisar de um tempo para preparar o local de destino antes que o arquivamento seja reiniciado. Se você não selecionar essa opção, o arquivamento iniciará no horário agendado.
11. Clique em **Finish** (Concluir).

Pausar ou retomar o arquivamento agendado

Se você optou anteriormente por pausar o arquivamento, ao executar o procedimento Configurar um arquivamento agendado, pode retomar o arquivamento agendado mais tarde.
Para pausar ou retomar o arquivamento agendado:

1. Navegue até o **Core Console** e, em seguida, clique na guia **Tools** (Ferramentas).
2. Na opção **Archive** (Arquivamento), clique em **Scheduled** (Agendado).
3. Na página **Scheduled Archive** (Arquivamento agendado), escolha uma das opções a seguir:
   - Selecione o arquivamento preferido, e em seguida, clique em uma das seguintes ações, conforme apropriado:
     - Pause (Pausar)
     - Resume (Retomar)
   - Ao lado do arquivamento preferido, clique no menu suspenso e, em seguida, clique em uma das ações a seguir, conforme apropriado:
     - Pause (Pausar)
     - Resume (Retomar)

   O status do arquivamento é mostrado na coluna **Schedule** (Agendamento).

Editar um arquivamento agendado

1. No Core Console, clique na guia **Tools** (Ferramentas).
2. Na opção **Archive** (Arquivamento), clique em **Scheduled** (Agendado).
3. Na página Scheduled Archive (Arquivamento agendado), clique no menu suspenso ao lado do arquivamento que você quer alterar e, em seguida, clique em **Edit** (Editar).

   A caixa de diálogo **Add Archive Wizard** (Assistente para adicionar arquivamento) é exibida.
4. Na página **Location** (Local) do **Add Archive Wizard** (Assistente para adicionar arquivamento), selecione uma das opções da lista suspensa **Location Type** (Tipo de local):

- Local: local de saída – Digite o local para a saída. Isso define o caminho do local onde você quer que o arquivamento resida.
- Rede
  - Output location (Local de saída): digite o local para a saída. Isso define o caminho do local onde você quer que o arquivamento resida.
  - User Name (Nome de usuário): digite um nome de usuário. Isso estabelece credenciais de login para o compartilhamento de rede.
  - Password (Senha): digite uma senha para o caminho de rede. Isso estabelece credenciais de login para o compartilhamento de rede.
- Cloud
  - Account (Conta de nuvem): selecione uma conta na lista suspensa. Para selecionar uma conta de nuvem, você precisa tê-la adicionado ao Core Console.
  - Container (Recipiente): selecione um recipiente associado à sua conta no menu suspenso.
  - Folder Name (Nome da pasta): digite um nome para a pasta na qual os dados arquivados serão salvos. O nome padrão é AppAssure-5-Archive-[DATA DA CRIAÇÃO]-[HORA DA CRIAÇÃO]

5. Clique em **Next** (Avançar).
6. Na página **Machines** (Máquinas) do assistente, selecione as máquinas protegidas que contêm os pontos de recuperação que você quer arquivar.
7. Clique em **Next** (Avançar)
8. Na página **Schedule** (Agendamento), selecione uma das seguintes opções de frequência do envio de dados:
   - Daily: At time (Diariamente: no horário) – Selecione a hora do dia em que você quer criar um arquivamento diário.
   - Weekly (Semanalmente)
     - At day of week (No dia da semana): selecione um dia da semana para criar automaticamente o arquivamento.
     - At time (No horário): selecione a hora do dia em que você quer criar um arquivamento diário.
   - Monthly (Mensalmente)
     - At day of months (No dia do mês): selecione o dia do mês no qual criar automaticamente o arquivamento.
     - At time (No horário): selecione a hora do dia em que você quer criar um arquivamento diário.
9. Para pausar o arquivamento e retomá-lo mais tarde, selecione **Initial pause archiving** (Pausa inicial do arquivamento).

   Você pode pausar o arquivamento agendado se precisar de um tempo para preparar o local de destino antes que o arquivamento seja reiniciado. Se você não selecionar essa opção, o arquivamento iniciará no horário agendado.
10. Clique em **Concluir**.

Verificar um arquivamento

Você pode analisar a integridade estrutural de um arquivo, executando uma verificação de arquivo. Essa verificação examina a presença de todos os arquivos necessários dentro do arquivamento. Para executar uma verificação de arquivamento, complete as etapas do procedimento descrito a seguir:

1. No Core Console, clique na guia **Tools** (Ferramentas).
2. Na opção **Archive** (Arquivamento), clique em **Check Archive** (Verificar arquivamento).

   A caixa de diálogo **Check Archive** (Verificar arquivamento) é exibida.

3. Selecione uma das seguintes opções na lista suspensa:
   - Local: local de saída – Digite o local para a saída. Isso define o caminho do local onde você quer que o arquivamento resida.
   - Network (Rede)
     - Output location (Local de saída): digite o local para a saída. Isso define o caminho do local onde você quer que o arquivamento resida.
     - User Name (Nome de usuário): digite um nome de usuário. Isso estabelece credenciais de login para o compartilhamento de rede.
     - Password (Senha): digite uma senha para o caminho de rede. Isso estabelece credenciais de login para o compartilhamento de rede.
   - Cloud
     - Account (Conta de nuvem): selecione uma conta na lista suspensa. Para selecionar uma conta de nuvem, você precisa tê-la adicionado ao Core Console.
     - Container (Recipiente): selecione um recipiente associado à sua conta no menu suspenso.
     - Folder Name (Nome da pasta): digite um nome para a pasta na qual os dados arquivados serão salvos. O nome padrão é AppAssure-5-Archive-[DATA DA CRIAÇÃO]-[HORA DA CRIAÇÃO]
4. Para executar também uma verificação de integridade da estrutura, selecione **Structure integrity** (integridade da estrutura).
5. Clique em **Check FIle** (Verificar arquivos).

Importar um arquivamento

Para importar um arquivamento:

1. No Core Console, selecione a guia **Configuration** (Configuração).
2. Na opção **Manage** (Gerenciar), clique em **Archive** (Arquivamento) e, em seguida, clique em **Import** (Importar).

   A caixa de diálogo **Import Archive** (Importar arquivamento) é exibida.
3. Na caixa de diálogo **Import Archive** (Importar arquivamento), digite os detalhes para importar o arquivamento descritos a seguir:

Caixa de texto	Descrição
Input Location (Local da entrada)	Selecione o local para a importação do arquivamento.
User name (Nome de usuário)	Para estabelecer o acesso para proteger o arquivamento, digite as credenciais de login.
Password (Senha)	Digite uma senha para acessar o arquivamento.

4. Clique em **Check File** (Verificar arquivo) para validar a existência do arquivamento para importar.

   A caixa de diálogo **Restore** (Restaurar) é exibida.
5. Na caixa de diálogo **Restore** (Restaurar), verifique o nome do núcleo de origem.
6. Selecione os agentes para importar do arquivamento.
7. Selecione o repositório.
8. Clique em **Restore** (Restaurar) para importar o arquivamento.

Gerenciar a capacidade de conexão do SQL

A configuração da capacidade de conexão do SQL permite que o Core conecte o banco de dados e os arquivos de log do SQL a um instantâneo de um SQL Server, usando uma instância local do Microsoft SQL Server. O teste de capacidade de conexão permite que o Core verifique a consistência dos bancos de dados do SQL e confirma se todos os arquivos de dados (MDF e LDF) estão disponíveis no instantâneo do backup. As verificações da capacidade de conexão podem ser realizadas sob demanda para pontos de recuperação específicos ou como parte de uma tarefa noturna.

A capacidade de conexão precisa de uma instância local do Microsoft SQL Server na máquina AppAssure Core. Essa instância precisa ser uma versão totalmente licenciada do SQL Server, adquirida da Microsoft ou de um revendedor licenciado. A Microsoft não permite o uso de licenças passivas do SQL.

A capacidade de conexão suporta o SQL Server 2005, 2008, 2008 R2, 2012 e 2014. A conta usada para realizar o teste precisa ter a função sysadmin na instância do SQL Server.

O formato de armazenamento em disco do SQL Server é o mesmo nos ambientes de 64 bits e 32 bits e a capacidade de conexão funciona nas duas versões. Um banco de dados que estiver desconectado de uma instância do servidor em um ambiente pode estar conectado na instância no outro ambiente.

CUIDADO: A versão do SQL Server no Core precisa ser igual ou mais recente que a versão do SQL Server em todos os agentes com o SQL Server instalado.

Configurar a capacidade de conexão do SQL

Antes de executar verificações da capacidade de conexão em bancos de dados protegidos do SQL, selecione uma instância local do SQL Server na máquina Core que será usada para executar as verificações descritas em relação à máquina agente.

NOTA: A capacidade de conexão requer uma instância local do Microsoft SQL Server na máquina AppAssure Core. Essa instância precisa ser uma versão totalmente licenciada do SQL Server, adquirida da Microsoft ou de um revendedor licenciado. A Microsoft não permite o uso de licenças passivas do SQL.

Para configurar os parâmetros da capacidade de conexão do SQL:

1. Navegue até o Core Console e, em seguida, clique na guia.
2. Clique em **Configuration** → **Settings** (Configuração > Parâmetros).
3. No painel Nightly Jobs (Tarefas noturnas), clique em **Change** (Alterar).

   A caixa de diálogo **Nightly Job** (Tarefa noturna) é exibida.
4. Selecione **Attachability Check Job** (Tarefa de verificação da capacidade de conexão) e, em seguida, clique em **Settings** (Configurações).
5. Use os menus suspensos para selecionar a instância do SQL Server instalada no Core, a partir das seguintes opções:

   Você pode escolher entre:

   - **SQL Server 2005**
   - **SQL Server 2008**
   - **SQL Server 2008 R2**
   - **SQL Server 2012**
   - **SQL Server 2014**
6. Selecione o tipo de credencial.

Você pode escolher entre:

- **Windows**
- **SQL**

7. Especifique as credenciais com privilégios de administrador para as instâncias do Windows ou SQL Server, descritas a seguir:

Caixa de texto	Descrição
Username (Nome de usuário)	Digite um nome de usuário para as permissões de login no SQL Server.
Password (Senha)	Digite uma senha para a capacidade de conexão do SQL; usada para controlar a atividade de login.

8. Clique em **Test Connection** (Testar conexão).

   NOTA: Se você inseriu as credenciais incorretamente, é mostrada uma mensagem alertando que o teste das credenciais falhou. Corrija as informações das credenciais e repita o teste de conexão.

9. Clique em **Save** (Salvar).

   Agora, as verificações da capacidade de conexão estão disponíveis para a execução nos bancos de dados protegidos do SQL Server.

10. Na janela Nightly Jobs (Tarefas noturnas), clique em **OK**.

    Agora, as verificações da capacidade de conexão são agendadas para ocorrer com as tarefas noturnas.

Configurar as verificações noturnas de capacidade de conexão do SQL e truncagem de log

Para configurar as verificações noturnas de capacidade de conexão do SQL e truncagem de log:

1. Na área de navegação à esquerda do Core, selecione a máquina para a qual você quer ter verificações noturnas da capacidade de conexão e truncagem de log e clique em **SQL Server Settings** (Configurações do SQL Server).
2. Navegue até o Core Console.
3. Clique em **Configuration** → **Settings** (Configuração > Parâmetros).
4. Na seção **Nightly Jobs** (Tarefas noturnas), clique em **Change** (Alterar).
5. Marque ou desmarque as seguintes configurações do servidor SQL com base nas necessidades da sua organização:
   - **Attachability Check Job (Tarefa de verificação de capacidade de conexão)**
   - **Log Truncation Job (Tarefa de truncagem de log) (modelo de recuperação simples apenas)**
6. Clique em **OK**.

   As configurações de capacidade de conexão e truncagem de log serão aplicadas ao servidor SQL protegido.

Gerenciar as verificações de capacidade de montagem do banco de dados do Exchange e truncagem de log

Quando você usar o AppAssure para fazer o backup dos Microsoft Exchange Servers, as verificações de capacidade de montagem podem ser realizadas em todos os bancos de dados do Exchange após cada instantâneo. Esse recurso de detecção da corrupção avisa os administradores sobre as falhas em

potencial e garante que todos os dados dos servidores do Exchange sejam recuperados satisfatoriamente em caso de falha.

NOTA: Os recursos de verificações de capacidade de montagem e truncagem de log somente se aplicam ao Microsoft Exchange 2007, 2010 e 2013. Além disso, a conta de serviço do AppAssure Agent precisa ser atribuída à função de Administrador organizacional no Exchange.

Configurar a capacidade de montagem do banco de dados do Exchange e truncagem de log

Você pode ver , ativar ou desativar as configurações do servidor de banco dados do Exchange , incluindo a verificação da capacidade de montagem automática, soma de verificação noturna ou truncagem do log noturno.

Para configurar a capacidade de montagem do banco de dados do Exchange e a truncagem de log:

1. Na área de navegação esquerda do Console Core, selecione a máquina para a qual você quer configurar a verificação da capacidade de montagem e a truncagem de log.

   A guia **Summary** (Resumo) da máquina selecionada é mostrada.
2. Clique em **Exchange Server Settings** (Configurações do Exchange Server).

   A caixa de diálogo **Exchange Server Settings** (Configurações do Exchange Server) aparece.
3. Marque ou desmarque as seguintes configurações do Exchange Server com base nas necessidades da sua organização:
   - **Ativar verificação automática da capacidade de montagem**
   - **Ativar verificação da soma de verificação noturna**
   - **Ativar a truncagem de log noturna**
4. Clique em **OK**.

   As configurações da capacidade de montagem e da truncagem de log surtem efeito para o Exchange Server protegido.

   NOTA: Para obter informações sobre como forçar a truncagem de log, consulte Forçar truncagem de log.

Forçar uma verificação da capacidade de montagem

Para forçar uma verificação da capacidade de montagem:

1. Na área de navegação à esquerda do Core Console, selecione a máquina para a qual você quer forçar a verificação da capacidade de montagem e, em seguida, clique na guia **Recovery Points** (Pontos de recuperação).
2. Clique em **>** (Avançar) próximo a um ponto de recuperação na lista para expandir a exibição.
3. Clique em Force **Mountability Check** (Verificação da capacidade de montagem).

   Uma mensagem avisa você a forçar uma verificação da capacidade de montagem.
4. Clique em **Yes** (Sim).

   NOTA: Para obter instruções sobre como exibir o status das verificações da capacidade de conexão, consulte Ver eventos e alertas.

   O sistema executa a verificação da capacidade de montagem.

Forçar as verificações de soma de verificação

Para forçar uma verificação de soma de verificação:

1. Na área de navegação esquerda do Core Console, selecione a máquina para forçar uma verificação de soma de verificação e, em seguida, clique na guia **Recovery Points** (Pontos de recuperação).
2. Clique em **>** ao lado de um ponto de recuperação na lista para expandir a exibição.
3. Clique em **Force Checksum Check** (Forçar verificação de soma de verificação).

   A janela **Force Attachability Check** (Forçar verificação da capacidade de conexão) solicitará que você indique se quer forçar uma verificação de soma de verificação.
4. Clique em **Yes** (Sim).

   O sistema realiza a verificação de soma de verificação.

   NOTA: Para obter informações sobre como ver o status da verificação da capacidade de conexão, consulte Ver eventos e alertas .

Forçar a truncagem de log

NOTA: Essa opção está disponível somente para máquinas Exchange ou SQL.

Para forçar a truncagem de log:

1. Navegue até o Core Console e, em seguida, clique na guia **Machines** (Máquinas).
2. Na guia **Machines** (Máquinas), execute um dos procedimentos a seguir:
   - Clique no hiperlink da máquina cujo log você quer truncar.
   - Ou, no painel de navegação, selecione a máquina cujo log você quer truncar.
3. No menu suspenso **Actions** (Ações) dessa máquina, clique em **Force Log Truncation** (Forçar truncagem de log).
4. Confirme se quer prosseguir com a truncagem de log.

Indicadores de status do ponto de recuperação

Depois que um ponto de recuperação é criado em um SQL ou Exchange Server protegido, o aplicativo é mostrado com um indicador de status da cor correspondente na tabela **Recovery Points** (Pontos de recuperação). A cor mostrada é baseada nas configurações de verificação da máquina protegida e no sucesso ou falha dessas verificações, conforme descrito nas tabelas a seguir.

NOTA: Para obter mais informações sobre como ver os pontos de recuperação, consulte Ver pontos de recuperação.

A tabela a seguir mostra os indicadores de status que são mostrados para os bancos de dados SQL.

Cores do status do ponto de recuperação para bancos de dados SQL

Cor do status	Descrição
Branco	Indica uma das seguintes condições: • Não existe um banco de dados SQL. • As verificações de capacidade de conexão não foram ativadas. • As verificações de capacidade de conexão ainda não foram executadas.

Cor do status	Descrição
Amarelo	Indica que o banco de dados SQL estava off-line e uma verificação não foi possível.
Vermelho	Indica uma falha na verificação da capacidade de conexão.
Verde	Indica que a verificação da capacidade de conexão foi aprovada.

A tabela a seguir mostra os indicadores de status que são mostrados para os bancos de dados Exchange.

Cores do status do ponto de recuperação para bancos de dados Exchange

Título do termo	Título da descrição
Branco	Indica uma das seguintes condições: • Não existe um banco de dados Exchange. • As verificações de capacidade de montagem não foram ativadas. NOTA: Isso pode se aplicar a certos volumes dentro de um ponto de recuperação.
Amarelo	Indica que as verificações de capacidade de montagem do banco de dados do Exchange estão ativadas, mas ainda não foram executadas.
Vermelho	Indica que a verificação da capacidade de montagem ou do checksum falhou em pelo menos um banco de dados.
Verde	Indica que a verificação da capacidade de montagem ou do checksum foi "aprovada".

NOTA: Os pontos de recuperação que não tiverem um banco de dados Exchange ou SQL associado são mostrados com um indicador de status branco. Nas situações em que os bancos de dados Exchange e SQL existem para o ponto de recuperação, o indicador de status mais grave é mostrado para o ponto de recuperação.

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.

Monitorar o status do dispositivo

Você pode monitorar o status dos subsistemas do dispositivo usando a guia **Appliance** (Dispositivo) da página **Overall Status** (Status geral). A página **Overall Status** (Status geral) mostra uma luz de status ao lado de cada subsistema, junto com uma descrição do status indicando a integridade do subsistema.

A página Overall Status (Status geral) também fornece links para ferramentas que analisam os detalhes de cada subsistema, que podem ser úteis para solucionar problemas de advertências ou erros. O link **System Administrator** (Administrador de sistema), disponível para os subsistemas de hardware do dispositivo e hardware de armazenamento, solicita que você faça o login no aplicativo System Administrator usado para gerenciar o hardware. Para obter mais informações sobre o aplicativo System Administrator, consulte o *Guia do usuário do OpenManage Server Administrator* em **dell.com/support/home**. O link **Provisioning Status** (Status do provisionamento), disponível para o subsistema de provisionamento do armazenamento, abre a tela **Tasks** (Tarefas) e mostra o status de provisionamento desse subsistema. Se o armazenamento estiver disponível para o provisionamento, um link para **Provision** (Provisionar) em **Actions** (Ações) aparecerá ao lado da tarefa de provisionamento.

Provisionar o armazenamento

O dispositivo configura o armazenamento interno disponível do DL4300 e qualquer compartimento de armazenamento externo conectado para:

- Repositórios do AppAssure

  NOTA: Se o HBA de canal de fibra estiver configurado, o processo de criação do repositório é manual. O AppAssure não criará um repositório automaticamente no diretório raiz. Para obter mais informações, consulte o *Guia de Implementação do Dispositivo Dell DL4300*.
- Espera virtual das máquinas protegidas

NOTA: Os MD1400s com unidades de 1 TB, 2 TB, 4 TB ou 6 TB (para alta capacidade) conectadas ao controlador H830 são suportados. Até quatro MD 1400s são suportados.

NOTA: A configuração do DL4300 de alta capacidade suporta o adaptador H830 PERC SAS ou dois HBAs de canal de fibra. Para obter mais informações sobre como configurar HBAs de canal de fibra , consulte o whitepaper *DL4xxx — Fibre Channel Implementation* (Implementação do canal de fibra) localizado em **dell.com/support/home**.

Antes de começar a provisionar o armazenamento no disco, determine o armazenamento que você quer para as máquinas virtuais de espera. Você pode alocar qualquer porcentagem da capacidade disponível para hospedar as máquinas virtuais de espera. Por exemplo, se estiver usando o Storage Resource

Management (SRM), você pode alocar até 100% da sua capacidade em qualquer dispositivo que está sendo provisionado para hospedar as máquinas virtuais. Usando o recurso AppAssure's Live Recovery (Recuperação em tempo real), você pode usar essas máquinas virtuais para substituir rapidamente qualquer servidor com falha que o dispositivo protege.

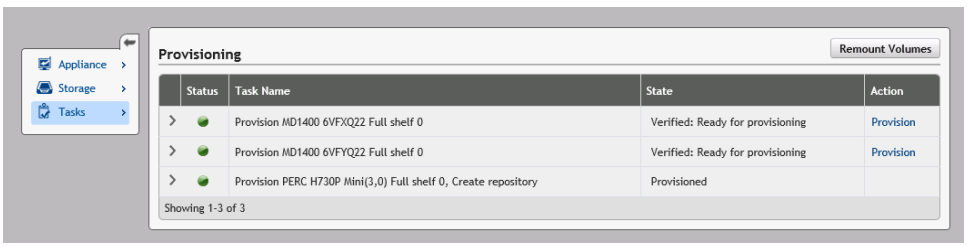
Com base em um ambiente médio que não precisa de máquinas virtuais de espera, você pode usar todo o armazenamento para fazer o backup de um número significativo de agentes. No entanto, se precisar de mais recursos para as máquinas virtuais de espera e fizer o backup de um número menor de máquinas agentes, você pode alocar mais recursos para as VMs maiores.

Quando você seleciona a guia **Appliance** (Dispositivo), o software AppAssure 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. Na guia **Appliance** (Dispositivo), clique em **Tasks** → **Provisioning** (Tarefas > Provisionamento).
   A tela **Provisioning** (Provisionamento) mostra a capacidade estimada para o provisionamento. Essa capacidade é usada para criar um novo Repositório do AppAssure.

   CUIDADO: Antes de continuar, confirme se as Etapas 2 a 4 foram seguidas neste procedimento.
2. Abra a janela **Provisioning Storage** (Armazenamento do provisionamento) clicando no botão **Provision** (Provisionar) na coluna Action (Ação) ao lado do armazenamento que você quer provisionar.
3. Na seção **Optional Storage Reserve** (Reserva do armazenamento opcional), marque a caixa ao lado de **Allocate a portion of the storage being provisioned for Standby Virtual Machines or other purposes** (Alocar uma parte do armazenamento que está sendo provisionado para as máquinas virtuais de espera ou outros fins) e indique uma porcentagem do armazenamento para alocar. Caso contrário, a porcentagem de armazenamento indicada na seção **Optional Storage Reserve** (Reserva de armazenamento opcional) será retirada de todos os discos conectados.
4. Clique em **Provision** (Provisionar).



Provisionar o armazenamento selecionado

Para provisionar o armazenamento selecionado:

1. Na guia **Appliance** (Dispositivo), clique em **Tasks (Tarefas)** → **Provisioning (Provisionamento)**.
   A tela **Provisioning** (Provisionamento) mostra a capacidade estimada para o provisionamento. Essa capacidade é usada para criar um novo Repositório do AppAssure.
2. Para provisionar somente uma parte do espaço disponível, clique em **Provision** (Provisionar) sob **Action** (Ação) ao lado do espaço de armazenamento que você quer provisionar.
   - Para criar novo repositório, selecione **Create a new repository** (Criar um novo repositório) e forneça um nome para o repositório.

Por padrão, Repositório 1 aparece como o nome do repositório. Você pode substituir esse nome.

- Para adicionar capacidade a um repositório existente, selecione **Expand the existing repository** (Expandir o repositório existente) e, em seguida, selecione o repositório na lista **Existing Repositories** (Repositórios existentes).

NOTA: Para adicionar capacidade, é recomendável expandir um repositório existente em vez de adicionar um novo. Os repositórios separados não usam a capacidade com a mesma eficiência, porque a desduplicação não pode ocorrer em repositórios separados.

3. Em **Optional Storage Reserve**(Reserva de armazenamento opcional) , selecione **Allocate a portion of the storage being provisioned for Standby Virtual Machines or other purposes** (Alocar uma parte do armazenamento que está sendo provisionado para as máquinas virtuais de espera ou outros fins) e , em seguida, especifique a porcentagem do armazenamento para alocar para as VMs.
4. Clique em **Provision** (Provisionar).

   O provisionamento do disco começa e o status da criação do repositório do AppAssure é mostrado na área **Status** da tela **Tasks** (Tarefas). O **State** (Estado) mostra **Provisioned** (Provisionado).
5. Para ver os detalhes depois que o provisionamento do disco terminar, clique em **>** ao lado da luz do status.

   A página **Tasks** (Tarefas) se expande e mostra o status, o repositório e os detalhes do disco virtual (se alocado).

Apagar a alocação de espaço para um disco virtual

Antes de começar este procedimento, determine qual disco virtual você quer apagar. No Core Console, selecione a guia **Appliance** (Dispositivo), clique em **Tasks** (Tarefas) e expanda o repositório que contém os discos virtuais para ver os detalhes do disco virtual.
Para apagar uma alocação de espaço para um disco virtual:

1. No aplicativo OpenManage Server Administrator, expanda **Storage** (Armazenamento).
2. Expanda o controlador que abriga o disco virtual e selecione **Virtual Disks** (Discos virtuais).
3. Selecione o disco virtual que você quer remover e selecione **Delete** (Apagar) no menu suspenso **Tasks** (Tarefas).
4. Depois de confirmar o apagamento, o espaço é mostrado na guia **Appliance** (Dispositivo) do Core Console, tela **Tasks** (Tarefas), como disponível para provisionamento.

Resolver tarefas com falha

O AppAssure relata falhas nas tarefas de verificação, provisionamento e recuperação com um evento na página inicial do Core Console e também na guia **Appliance** (Dispositivo) da tela **Tasks** (Tarefas).

Para entender como resolver uma tarefa com falha, selecione a guia **Appliance** (Dispositivo) e, em seguida, clique em **Tasks** (Tarefas). Expanda a tarefa com falha clicando em **>** ao lado do **Status** e confira a mensagem de erro e a ação recomendada.

Fazer upgrade de dispositivo

Para fazer upgrade de um dispositivo:

1. Faça download do **Utilitário de recuperação e atualização** de **dell.com/support** para o Backup DL4300 para o dispositivo de disco.
2. Copie o utilitário para a área de trabalho do dispositivo 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 funcionamento.
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 Windows Server, ASP .NET MVC3, LSI Provider, DL Applications, OpenManage Server Administrator e AppAssure 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: Como parte do processo de upgrade do software AppAssure Core, o Utilitário de recuperação e atualização avisa sobre a versão atualmente instalada do AppAssure e solicita que você confirme sequer fazer o upgrade do Core para a versão agregada ao utilitário. Não há suporte para downgrades do software AppAssure Core.
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. Faça download do **utilitário Recuperação e atualização** de **dell.com/support** para o dispositivo.
2. Copie o utilitário para a área de trabalho do dispositivo 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 funcionamento.
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 Windows Server, ASP .NET MVC3, LSI Provider, DL Applications, OpenManage Server Administrator e AppAssure 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 AppAssure 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 AppAssure Core.

   NOTA: Não há suporte para downgrade do software AppAssure 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 AppAssure 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

Sobre a proteção de estações de trabalho e servidores

Para proteger seus dados, adicione as estações de trabalho e os servidores que deseja proteger no Core Console; por exemplo, seu servidor Exchange, SQL Server ou servidor Linux.

NOTA: Nesta seção, geralmente a palavra *máquina* também se refere ao software AppAssure Agent instalado em sua máquina.

No Core Console, você pode identificar a máquina na qual um software AppAssure Agent está instalado e especificar quais volumes quer proteger, definir agendamentos para a proteção, adicionar medidas extras de segurança como criptografia e muito mais. Para obter mais informações sobre como acessar o Core Console para proteger estações de trabalho e servidores, consulte Proteger uma máquina.

Configurar a máquina

Depois de adicionar a proteção para as máquinas AppAssure, você pode modificar as configurações básicas (como o nome e nome do host), os parâmetros de proteção (alterar o agendamento de proteção para volumes na máquina, adicionar ou remover os volumes ou pausar proteção) e muito mais.

Ver e modificar as definições de configuração

Para ver e modificar as definições de configuração:

1. Depois que você tiver adicionado uma máquina protegida, execute um dos seguintes:
   - No Core Console, clique na guia **Machines** (Máquinas) e, em seguida, clique no hiperlink da máquina que você quer modificar.
   - No painel **Navigation** (Navegação), selecione a máquina que você quer modificar.
2. Clique na guia **Configuration** (Configuração).

   A página **Settings** (Configurações) é exibida.
3. Clique em **Edit** (Editar) para modificar as definições da máquina, conforme descrito na tabela a seguir.

Caixa de texto	Descrição
Display Name (Nome de exibição)	Digite um nome de exibição para a máquina. Um nome para essa máquina a ser mostrado no Core Console. Por padrão, esse é o nome de host da máquina. Você pode alterar o nome de exibição para algo que facilite mais a referência caso seja necessário.

Caixa de texto	Descrição
Host Name (Nome de host)	Digite um nome de host para a máquina.
Port (Porta)	Digite um número de porta para a máquina. O Core usa a porta para se comunicar com esta máquina.
Repository (Repositório)	Selecione um repositório para os pontos de recuperação. Exibe o repositório no núcleo no qual serão armazenados dados dessa máquina. NOTA: Esta definição só pode ser alteradas e não houver pontos de recuperação ou se o repositório anterior não estiver presente.
Encryption Key (Chave de criptografia)	Edite a chave de criptografia se necessário. Especifica se a criptografia é aplicada aos dados em cada volume na máquina que está armazenada no repositório.

Ver as informações do sistema para uma máquina

O Core Console mostra todas as máquinas que estão sendo protegidas, incluindo uma lista das máquinas e seus status.

Para ver as informações do sistema para uma máquina:

1. No Core Console, em **Protected Machines** (Máquinas protegidas), selecione a máquina para ver as informações detalhadas do sistema.
2. Clique na guia **Tools** (Ferramentas) dessa máquina.

   As informações sobre a máquina aparecem na página **System Information** (Informações do sistema). Os detalhes contêm o seguinte:

   - Nome do host
   - Versão do sistema operacional
   - Arquitetura do sistema operacional
   - Memória (física)
   - Nome de exibição
   - Nome de domínio totalmente qualificado
   - Tipo de máquina virtual (se aplicável)

   Informações detalhadas sobre os volumes contidos nessa máquina contêm:

   - Nome
   - ID do dispositivo
   - Sistema de arquivos
   - Capacidade (incluindo bruta, formatada e usada)
   - Processadores
   - Tipo de processadores
   - Adaptadores de rede
   - Endereços IP associados a esta máquina

Configurar os grupos de notificações para eventos do sistema

No AppAssure, você pode configurar como os eventos do sistema são relatados para a sua máquina por meio da criação de grupos de notificações que podem incluir alertas do sistema, de erros e assim por diante.

Para configurar grupos de notificações de eventos do sistema:

1. No Core Console, clique na guia **Machines** (Máquinas).
2. Na guia **Machines** (Máquinas), execute um dos procedimentos a seguir:
   - Clique no hiperlink para a máquina que você quer modificar.
   - No painel de navegação, selecione a máquina que você quer modificar.

   A guia **Summary** (Resumo) é exibida.
3. Clique na guia **Configuration** (Configuração) e, em seguida, clique em **Events** (Eventos).

   A página **Notification Groups** (Grupos de notificações) é exibida.
4. Clique em **Use custom alert settings** (Usar configurações de alerta personalizadas) e, em seguida, clique em **Apply** (Aplicar).

   A tela **Custom Notification Groups** (Personalizar grupos de notificações) é exibida.
5. Clique em **Add Group** (Adicionar grupo) para adicionar novos grupos de notificações para enviar uma lista dos eventos do sistema.

   A caixa de diálogo **Add Notification Group** (Adicionar grupo de notificações) é exibida.

   NOTA: Para usar as configurações de alerta padrão, selecione a opção de configurações de alerta **Use Core** (Usar Core).
6. Adicione as opções de notificação conforme descrito na tabela a seguir.

Caixa de texto	Descrição
Name (Nome)	Digite um nome para o grupo de notificações.
Description (Descrição)	Insira uma descrição para o grupo de notificações.
Enable Events (Ativar eventos)	Selecione quais eventos você quer compartilhar com este grupo de notificações. Você pode selecionar **All** (Todos) ou um subconjunto de eventos para incluir: • **BootCd (Cd de inicialização)** • **LocalMount (Montagem local)** • **Metadata (Metadados)** • **Clusters (Agrupamentos)** • **Notification (Notificação)** • **PowerShellScripting (Scripts do PowerShell)** • **PushInstall (Instalação forçada)** • **Attachability (Capacidade de conexão)** • **Jobs (Tarefas)** • **Licensing (Licenciamento)** • **LogTruncation (Truncagem de log)** • **Archive (Arquivamento)**

Caixa de texto	Descrição
	• **CoreService (Serviço do Core)** • **Export (Exportação)** • **Protection (Proteção)** • **Replication (Replicação)** • **Rollback (Reversão)** • **Rollup (Implantação)** Você também pode escolher selecionar por tipo: • **Info (Informações)** • **Warning (Advertência)** • **Error (Erro)** NOTA: Quando você escolhe selecionar por tipo, por padrão, os eventos adequados são ativados automaticamente. Por exemplo, se você escolher Warning, os eventos Attachability, Jobs, Licensing, Archive, CoreService, Export, Protection, Replication e Rollback são ativados.
Notification Options (Opções de notificação)	Selecione o método para especificar como lidar com as notificações. Você pode escolher uma das seguintes opções: • **Notify by Email** (Notificar por e-mail) – Especifique os endereços de e-mail para os quais enviar os eventos nas caixas de texto To (Para), CC (Com cópia) e BCC (Com cópia oculta). NOTA: Para receber e-mail, o SMTP precisa ter sido configurado anteriormente. • **Notify by Windows Event log** (Notificar por log de eventos do Windows) – O log de eventos do Windows controla a notificação. • **Notify by syslogd** (Notificar por syslogd) – Especifique o nome do host e a porta para os quais enviar os eventos. – **Host** – Digite o nome do host para o servidor. – **Port** (Porta) – Digite um número de porta para a comunicação com o servidor.

7. Clique em **OK** para salvar as alterações.
8. Para editar um grupo de notificações existente, clique em **Edit** (Editar) próximo ao grupo de notificações que você quer editar.

   A caixa de diálogo **Edit Notification Group** (Editar grupo de notificações) é mostrada para você possa editar as configurações.

Editar os grupos de notificações para eventos do sistema

Para editar os grupos de notificações para eventos do sistema:

1. Navegue até o Core Console e, em seguida, clique na guia **Machines** (Máquinas).
2. Na guia **Machines** (Máquinas), execute um dos procedimentos a seguir:
   - Clique no hiperlink da máquina que você quer modificar
   - Ou, no painel de navegação, selecione a máquina que você quer modificar.

   A guia **Summary** (Resumo) aparece.

3. Clique na guia **Configuration** (Configuração) e, em seguida, clique em **Events** (Eventos).
4. Clique em **Use custom alert settings** (Use configurações de alerta personalizadas) e, em seguida, clique em **Apply** (Aplicar).

   A tela **Custom Notification Groups** (Personalizar grupos de notificações) aparece.
5. Clique no ícone **Edit** (Editar) na coluna **Action** (Ação).

   A caixa de diálogo **Edit Notification Group** (Editar grupo de notificações) aparece.
6. Edite as opções de notificação conforme descrito na tabela a seguir.

Caixa de texto	Descrição
Nome	Representa o nome do grupo de notificações. NOTA: Você não pode editar o nome do grupo de notificações.
Descrição	Digite uma descrição para o grupo de notificações.
Ativar eventos	Selecione quais eventos você quer compartilhar com o grupo de notificações. Você pode selecionar **All** (Todos) ou um subconjunto de eventos para conter: • **BootCd** • **LocalMount** • **Metadados** • **Clusters** • **Notificação** • **PowerShellScripting** • **PushInstall** • **Capacidade de conexão** • **Tarefas** • **Licenciamento** • **LogTruncation** • **Arquivamento** • **CoreService** • **Exportar** • **Proteção** • **Replicação** • **Reversão** • **Implantação** Você também pode selecionar por tipo: • **Info** • **Advertência** • **Erro** NOTA: Quando você seleciona por tipo, por padrão, os eventos adequados são ativados automaticamente. Por exemplo, se você escolher Warning (Aviso), os eventos de Capacidade de conexão, Tarefas, Licenciamento, Arquivo, CoreService, Exportação, Proteção, Replicação e Reversão são ativados.

Caixa de texto	Descrição
Opções de notificação	Selecione o método para especificar como lidar com as notificações. Você pode escolher uma das seguintes opções: • **Notify by Email** (Notificar por e-mail) – Especifique os endereços de e-mail para os quais enviar os eventos nas caixas de texto To (Para), CC e BCC (CCO). NOTA: Para receber e-mail, o SMTP precisa ter sido configurado anteriormente. • **Notify by Windows Event log** (Notificar por log de eventos do Windows) – o log de eventos do Windows controla a notificação. • **Notify by syslogd** (Notificar por syslogd) – Especifique o nome do host e a porta para os quais enviar os eventos. – **Host** - Digite o nome do host para o servidor. – **Port** (Porta) – Digite um número de porta para a comunicação com o servidor.

7. Clique em **OK**.

Personalizar as configurações da política de retenção

A política de retenção para uma máquina especifica por quanto tempo os pontos de recuperação de uma máquina agente são armazenados no repositório. As políticas de retenção são usadas para reter os instantâneos do backup durante períodos mais longos e ajudar a gerenciá-los. Um processo de implantação impõe a política de retenção, além de ajudar na obsolescência e a apagar os backups antigos. Essa tarefa também é uma etapa do Processo de modificação das configurações do nó de cluster.

Para personalizar as configurações da política de retenção:

1. No Core Console, clique na guia **Machines** (Máquinas).
2. Na guia **Machines** (Máquinas), execute um dos procedimentos a seguir:
   - Clique no hiperlink para a máquina que você quer modificar.
   - No painel de navegação, selecione a máquina que você quer modificar.

   A guia **Summary** (Resumo) é exibida.
3. Clique na guia **Configuration** (Configuração) e, em seguida, clique em **Retention Policy** (Política de retenção).

   NOTA: Para usar a política de retenção padrão configurada para o Core, confirme se você selecionou a opção Use Core default retention policy (Usar a política de retenção padrão do Core).

   A tela **Retention Policy** (Política de retenção) é exibida
4. Para configurar as políticas personalizadas, clique em **Use custom retention policy** (Usar política de retenção personalizada).

   A tela **Custom Retention Policy** (Política de retenção personalizada) é exibida
5. Selecione **Enable Rollup** (Ativar implantação) e especifique os intervalos de tempo para reter os dados de backup, conforme a necessidade. As opções da política de retenção são descritas a seguir

Caixa de texto	Descrição
Keep all Recovery Points for n [retention time period] (Manter todos os pontos de recuperação por [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**. Você pode escolher entre: • **Days (Dias)** • **Weeks (Semanas)** • **Months (Meses)** • **Anos (Anos)**
... e, em seguida, manter um ponto de recuperação por hora por n [período de retenção]	Fornece um nível mais refinado de retenção; usado como um bloco de construção com uma 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. Você pode escolher entre: • **Days (Dias)** • **Weeks (Semanas)** • **Months (Meses)** • **Anos (Anos)**
... e, em seguida, manter um ponto de recuperação por dia por n [período de retenção]	Fornece um nível mais refinado de retenção; 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. Você pode escolher entre: • **Days (Dias)** • **Weeks (Semanas)** • **Months (Meses)** • **Anos (Anos)**
... e, em seguida, manter um ponto de recuperação por semana por n [período de retenção]	Fornece um nível mais refinado de retenção; 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. Você pode escolher entre: • **Weeks (Semanas)** • **Months (Meses)**

Caixa de texto	Descrição
	• **Anos (Anos)**
... e, em seguida, manter um ponto de recuperação por mês por n [período de retenção]	Fornece um nível mais refinado de retenção; 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. Você pode escolher entre: • **Months (Meses)** • **Anos (Anos)**
... e, em seguida, manter um ponto de recuperação por ano por n [período de retenção]	Digite um número que represente o período de retenção e, em seguida, selecione o período.

A caixa de texto Newest Recovery Point (Ponto de recuperação mais recente) mostra o ponto de recuperação mais novo . As configurações da política de retenção determinam o ponto de recuperação mais antigo.

A seguir se encontra um exemplo de como o período de retenção é calculado.

Manter todos os pontos de recuperação por 3 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 2 meses

... e, em seguida, manter um ponto de recuperação por mês por 1 ano

O ponto de recuperação mais novo é definido como o dia, mês e ano atual.

Nesse exemplo, o ponto de recuperação mais antigo pode ter um ano, quatro meses e seis dias de existência.

6. Clique em **Apply** (Aplicar) para salvar as alterações.
7. Para executar uma implantação com base na política de retenção atual da máquina, selecione **Force Rollup** (Forçar implantação) ou deixe a política de retenção que você definiu ser aplicada durante a implantação noturna.

Ver as informações de licença

Você pode ver as informações de status da atual licença do software AppAssure Agent instalado em uma máquina.

Para ver as informações de licença:

1. No Core Console, clique na guia **Machines** (Máquinas).
2. Na guia **Machines** (Máquinas), execute um dos procedimentos a seguir:
   - Clique no hiperlink da máquina que você quer ver.
   - No painel de navegação, selecione a máquina que você quer ver.
3. Clique na guia **Configuration** (Configuração) e, em seguida, clique em **Licensing** (Licenciamento).

   A tela **Status** mostra os detalhes do licenciamento do produto.

Modificar os cronogramas de proteção

No AppAssure, você pode modificar os cronogramas da proteção para volumes específicos em uma máquina.

Para modificar os cronogramas de proteção:

1. No Core Console, clique na guia **Machines** (Máquinas).
2. Na guia **Machines** (Máquinas), execute um dos procedimentos a seguir:
   - Clique no hiperlink para a máquina que você quer modificar.
   - No painel de navegação, selecione a máquina que você quer modificar.
3. Faça um dos seguintes:
   - Na tabela **Volumes** da guia **Summary** (Resumo) da máquina, clique no hiperlink do agendamento da proteção para o volume que você quer personalizar.
   - Clique na guia **Configuration** (Configuração) e, em seguida, clique em **Protection Settings** (Configurações da proteção). Na lista de volumes, clique no ícone **Edit** (Editar) ao lado do volume que você quer personalizar.

   A caixa de diálogo **Protection Schedule** (Cronograma de proteção) é mostrada.
4. Na caixa de diálogo **Protection Schedule** (Agendamento da proteção), edite as seguintes opções de agendamento, conforme necessário, para proteger seus dados. A tabela a seguir descreve as opções.

Opção	Descrição
Interval (Intervalo)	**Weekday** (Dia da semana) - Para proteger os dados em um intervalo específico (por exemplo, a cada 15 minutos), selecione o **intervalo**, e em seguida: • Para personalizar quando proteger os dados durante períodos de pico, você pode selecionar **Start Time** (Hora de início), **End Time** (Hora de término) e um **Interval** (Intervalo) nos menus suspensos. • Para proteger os dados durante as horas fora do pico, marque a caixa de seleção **Protection interval during off-peak times** (Intervalo de proteção durante as horas fora do pico) e, em seguida, selecione um intervalo para proteção no menu suspenso. **Weekends** (Fins de semana) - Para proteger os dados durante o fim de semana, marque a caixa de seleção **Protection interval during weekends** (Intervalo de proteção durante o fim de semana) e, em seguida, selecione um intervalo no menu suspenso.

Opção	Descrição
	NOTA: Se os bancos de dados e logs do SQL ou Exchange estiverem em diferentes volumes, os volumes precisam pertencer a um grupo de proteção.
Daily (Diariamente)	Para proteger os dados diariamente, selecione a opção **Daily** (Diariamente) e, em seguida, no menu suspenso **Protection Time** (Hora da proteção), selecione um horário para iniciar a proteção dos dados.
No Protection (Nenhuma proteção)	Para remover a proteção desse volume, selecione a opção **No Protection** (Nenhuma proteção).

Se quiser aplicar essas configurações personalizadas a todos os volumes nesta máquina, selecione **Apply to All Volumes** (Aplicar a todos os volumes).

5. Depois de fazer todas as alterações necessárias, clique em **OK**.

Modificar configurações da transferência

Você pode modificar as configurações para gerenciar os processos de transferência de dados para uma máquina protegida. As configurações de transferência descritas nesta seção são para o nível do agente. Para afetar transferência no nível do núcleo, consulte Modificar as configurações da fila de transferência.

CUIDADO: A alteração das configurações da transferência pode ter efeitos drásticos no seu ambiente. Antes de modificar os valores da configurações de transferência, consulte o Guia de Ajuste do Desempenho da Transferência na base de conhecimento do Dell AppAssure https://support.software.dell.com/appassure/kb.

Há três tipos de transferências:

Instantâneos	A transferência que faz o backup dos dados em sua máquina protegida.
Exportação de VM	Um tipo de transferência que cria uma máquina virtual com todos os parâmetros e informações de backup especificados pelo agendamento definido para proteger a máquina.
Reversão	Um processo que restaura as informações de backup contidas em um máquina protegida.

A transferência de dados envolve a transmissão de um volume de dados ao longo de uma rede, das máquinas do Agent para o Core. No caso da replicação, a transferência também ocorre do Core de origem para o Core de destino.

A transferência de dados pode ser otimizada para o seu sistema com certas configurações de opções do desempenho. Essas configurações controlam o uso da largura de banda dos dados durante o processo de backup das máquinas agentes, realização da exportação de VM ou reversão. Alguns fatores que afetam o desempenho na transferência de dados são:

- Número de transferências de dados do agente simultâneas
- Número de fluxos de dados simultâneos
- Quantidade de alterações dos dados em disco
- Largura de banda de rede disponível
- Desempenho do subsistema de disco do repositório

- Quantidade de memória disponível para o buffer dos dados

Você pode ajustar as opções de desempenho para oferecer um suporte melhor às necessidades da empresa e melhorar o desempenho com base no seu ambiente.

Para modificar as configurações de transferência:

1. No Core Console, escolha uma das opções a seguir:
   - Clique na guia **Machines** (Máquinas) e, em seguida, clique no hiperlink da máquina que você quer modificar.
   - No painel de navegação, clique na máquina que você quer modificar.
2. Na guia **Machines** (Máquinas), execute um dos procedimentos a seguir:
   - Clique no hiperlink da máquina que você quer modificar.
   - No painel de navegação, selecione a máquina que você quer modificar.
3. Clique na guia **Configuration** (Configuração) e, em seguida, clique em **Transfer Settings** (Configurações da transferência).

   As configurações atuais da transferência aparecem.
4. Na página **Transfer Settings** (Configurações da transferência), clique em **Change** (Alterar).

   A caixa de diálogo **Transfer Settings** (Configurações da transferência) aparece.
5. Digite as opções de **Configurações da transferência** para a máquina, conforme descrito na tabela a seguir.

Caixa de texto	Descrição
Prioridade	Configura a prioridade da transferência entre as máquinas protegidas. Permite atribuir a prioridade em comparação com outras máquinas protegidas. Selecione um número de 1 a 10, com 1 sendo a prioridade mais alta. A configuração padrão estabelece uma prioridade de 5. NOTA: A prioridade é aplicada às transferências que estão na fila.
Máximo de fluxos simultâneos	Configura o número máximo de links TCP enviados para o Core , a fim de serem processados em paralelo por agente. NOTA: A Dell recomenda configurar esse valor como 8. Se você sofrer bloqueio de pacotes, tente aumentar essa configuração.
Máximo de gravações simultâneas	Configura o número máximo de ações simultâneas de gravação no disco por conexão do agente. NOTA: A Dell recomenda configurar esse valor igual ao selecionado em Máximo de fluxos simultâneos. Se você sofrer perda de pacotes, configure esse valor um pouco mais baixo. Por exemplo, se o Máximo de fluxos simultâneos for 8, configure a opção como 7.
Máximo de novas tentativas	Configura o número máximo de novas tentativas para cada máquina protegida, se algumas das operações falharem.
Tamanho máximo do segmento	Especifica a maior quantidade de dados, em bytes, que um computador pode receber em um único segmento de TCP. A configuração padrão é 4194304.

Caixa de texto	Descrição
	CUIDADO: Não altere essa configuração padrão.
Profundidade máxima da fila de transferência	Especifica o número de comandos que podem ser enviados simultaneamente. Você pode ajustar essa opção para um número mais alto se o sistema tiver um grande número de operações simultâneas de E/S.
Leituras pendentes por fluxo	Especifica a forma como várias operações de leitura enfileiradas serão armazenadas no back-end. Essa configuração ajuda a controlar o enfileiramento dos agentes. **NOTA:** A Dell recomenda configurar esse valor como 24.
Gravadores excluídos	Selecione um gravador se quiser excluí-lo. Como os gravadores que aparecem na lista são específicos da máquina que você está configurando, pode ser que você não veja todos os gravadores na lista. Alguns gravadores que podem ser mostrados: • Gravador ASR • Gravador BITS • Gravador COM+ REGDB • Gravador de contadores de desempenho • Gravador de registro • Gravador de otimização da cópia de sombra • SQLServerWriter • Gravador do sistema • Gravador do programador de tarefas • Gravador do armazenamento de metadados VSS • Gravador WMI
Porta do servidor para dados de transferência	Configura a porta para as transferências. A configuração padrão é 8009.
Tempo limite da transferência	Especifica, em minutos e segundos, a quantidade de tempo para permitir que um pacote seja estático sem transferência.
Tempo limite do instantâneo	Especifica, em minutos e segundos, o tempo máximo para aguardar a obtenção de um instantâneo.
Tempo limite de leitura da rede	Especifica, em minutos e segundos, o tempo máximo para aguardar uma conexão de leitura. Se a leitura da rede não for feita nesse período, a operação será repetida.
Tempo limite da gravação da rede	Especifica, em segundos, o tempo máximo para aguardar uma conexão de gravação. Se a gravação da rede não for feita nesse período, a operação será repetida.

6. Clique em **OK**.

Reiniciar um serviço

Para reiniciar um serviço:

1. No Core Console, clique na guia **Machines** (Máquinas).
2. Na guia **Machines** (Máquinas), execute um dos procedimentos a seguir:
   - Clique no hiperlink da máquina que você quer reiniciar.
   - No painel **Navigation** (Navegação), selecione a máquina que você quer reiniciar.
3. Clique no botão **Tools** (Ferramentas) e, em seguida, clique em **Diagnostics** (Diagnóstico).
4. Selecione a opção **Restart Service** (Reiniciar serviço) e, em seguida, clique no botão **Restart Service** (Reiniciar serviço).

Ver os logs da máquina

Se houver qualquer erro ou problema com a máquina, consulte os logs para solucionar o problema.
Para ver os logs da máquina

1. No Core Console, clique na guia **Machines** (Máquinas).
2. Na guia **Machines** (Máquinas), execute um dos procedimentos a seguir:
   - Clique no hiperlink da máquina que contém os logs que você quer ver.
   - No painel **Navigation** (Navegação), selecione a máquina que contém os logs que você quer ver.
3. Clique no botão **Tools** (Ferramentas) e, em seguida, clique em **Diagnostics** (Diagnósticos).
4. Clique no link **View Log** (Ver log).

Proteger uma máquina

Este tópico descreve como começar a proteger os dados na máquina que você especificar.

NOTA: A máquina precisa ter o software Agent instalado para ficar protegida. Você pode optar por instalar o software Agent antes deste procedimento ou implantá-lo enquanto configura a proteção na caixa de diálogo **Connection** (Conexão). Para ver as etapas específicas para instalar o software Agent durante o processo de proteção de uma máquina, consulte Implantar o software Agent ao proteger um agente.

Quando você adiciona a proteção, precisa especificar o nome ou endereço IP da máquina a ser protegida , bem como os respectivos volumes, e definir o agendamento da proteção para cada volume.

Para proteger várias máquinas ao mesmo tempo , consulte Proteger várias máquinas .

Para proteger uma máquina:

1. Se você não o fez depois de instalar o software Agent, reinicialize a máquina na qual o software Agent foi instalado.
2. No Core Console, na máquina núcleo, escolha uma das opções a seguir:
   - Na guia **Home** (Página inicial), em **Protected machines** (Máquinas protegidas), clique em **Protect Machine** (Proteger máquina).
   - Selecione a guia **Machines** (Máquinas) e, no menu suspenso **Actions** (Ações), clique em **Protect Machine** (Proteger máquina).

   A caixa de diálogo **Connect** (Conectar) aparece.

3. Na caixa de diálogo **Connect** (Conectar), digite as informações sobre a máquina à qual você quer se conectar, conforme descrito na tabela a seguir.

Caixa de texto	Descrição
Host	O nome do host ou endereço IP da máquina que você quer proteger.
Port (Porta)	O número da porta em que o Core se comunica com o agente na máquina. O número de porta padrão é 8006.
Username (Nome de usuário)	O nome de usuário usado para conectar-se a esta máquina; por exemplo, administrador.
Password (Senha)	A senha usada para conectar-se a esta máquina.

4. Clique em **Connect** (Conectar) para conectar-se a esta máquina.

   NOTA: Se o software Agent ainda não foi instalado na máquina que você designou, siga o procedimento Implantar o software Agent ao proteger um agente. Reinicie a máquina agente depois de implantar o software Agent e, em seguida, continue para a próxima etapa.

5. Na caixa de diálogo **Protect** (Proteger), edite as configurações conforme necessário, como descrito na tabela a seguir.

Campo	Descrição
Nome de exibição	O nome do host ou o endereço IP que você especificou na caixa de diálogo **Connect** (Conectar) aparece nesse campo de texto. Opcionalmente, digite um novo nome para a máquina, a ser mostrado no Core Console. NOTA: Você pode também alterar o nome de exibição mais tarde; basta acessar a guia **Configuration** (Configuração) referente a uma máquina existente.
Repositório	Selecione o repositório no Core para armazenar os dados nesta máquina.
Chave de criptografia	Especifique se você quer aplicar a criptografia aos dados para cada volume desta máquina que será armazenado no repositório. NOTA: As configurações de criptografia para um repositório são definidas na guia **Configuration** (Configuração) do Core Console.
Pausar proteção inicialmente	Depois que você adiciona uma máquina para proteção, o AppAssure começa automaticamente a obter um instantâneo do banco de dados. Você pode marcar essa caixa de seleção para pausar a proteção inicialmente. Depois, precisará forçar um instantâneo manualmente quando estiver pronto para começar a proteger seus dados. Para obter mais informações sobre como forçar um instantâneo manualmente, consulte Forçar um instantâneo.
Grupos de volumes	Em Volume Groups (Grupos de volumes), você pode definir quais volumes quer proteger e estabelecer um agendamento de proteção. Para definir um agendamento de proteção padrão de 60 em 60 minutos em todos os volumes na máquina, clique em **Apply Default** (Aplicar padrão).

Campo	Descrição
	Você também pode selecionar qualquer volume na máquina e definir parâmetros de proteção para ele individualmente. As configurações iniciais aplicam um agendamento de proteção padrão de 60 em 60 minutos. Para modificar o agendamento de qualquer volume, clique em **Edit** (Editar) para esse volume. Em seguida, você pode definir o intervalo entre instantâneos (incluindo a definição de um agendamento separado para os fins de semana) ou especificar um horário diário para começar um instantâneo. Para obter mais informações sobre como editar o agendamento da proteção para um volume selecionado, consulte Criar agendamentos personalizados para volumes.

6. Clique em **Protect** (Proteger).

   Na primeira vez que a proteção é adicionada a uma máquina, uma imagem básica (que é um instantâneo de todos os dados nos volumes protegidos) começará imediatamente a ser transferida para o repositório no Core, a menos que você tenha especificado para pausar a proteção inicialmente.

   CUIDADO: Se você protegeu uma máquina Linux, não desmonte um volume protegido manualmente. Caso precise fazer isso, execute o seguinte o comando antes de desmontar o volume: bsctl -d [path_to_volume]. Nesse comando, [caminho do volume] não se refere ao ponto de montagem do volume, mas sim ao descritor de arquivo do volume; ele precisa estar em uma forma semelhante a este exemplo: /dev/sda1.

Implementar o software do agente ao proteger um agente

Você pode fazer download e implementar agentes durante o processo de adicionar um agente para proteção.

NOTA: Esse procedimento não é obrigatório se você já tiver instalado o software do agente em uma máquina que você deseja proteger.

Para implementar agentes durante o processo de adicionar um agente para proteção:

1. Na caixa de diálogo **Protect Machine** (Proteger máquina) → **Connect** (Conectar), depois de digitar as configurações adequadas de conexão, clique em **Connect** (Conectar).

   A caixa de diálogo **Deploy Agent** (Implementar agente) é mostrada.
2. Clique em **Yes** (Sim) para implementar remotamente o software do agente na máquina.

   A caixa de diálogo **Deploy Agent** (Implementar agente) é mostrada.
3. Digite as configurações de proteção e logon da seguinte forma:
   - **Host name** (Nome de host) — Especifica o nome de host ou o endereço IP da máquina que você quer proteger.
   - **Port** (Porta) — Especifica o número da porta na qual o AppAssure Core se comunica com o agente na máquina. O valor padrão é 8006.
   - **User name** (Nome de usuário) — Especifica o nome de usuário usado para se conectar a esta máquina; por exemplo, administrador.
   - **Password** (Senha) — Especifica a senha usada para se conectar a esta máquina.

- **Display name** (Nome de exibição) — Especifica um nome para a máquina que aparece no Core Console. O nome de exibição pode ser igual ao nome de host.
- **Protect machine after install** (Proteger máquina depois da instalação) — A seleção dessa opção permite que o AppAssure faça um instantâneo dos dados depois de adicionar a máquina para proteção. Essa opção é selecionada por padrão. Se desmarcá-la, você precisará forçar um instantâneo manualmente quando estiver pronto para iniciar a proteção dos dados. Para obter mais informações sobre como forçar um instantâneo manualmente, consulte o tópico "Forçar um instantâneo" no *Guia do Usuário do Dispositivo Dell DL4300*.
- **Repository** (Repositório) — Selecione o repositório no qual deseja armazenar dados desse agente.

  NOTA: Você pode armazenar dados de múltiplos agentes em um único repositório.
- **Encryption Key** (Chave de criptografia) — Especifica se a criptografia é aplicada aos dados de cada volume nessa máquina a serem armazenados no repositório.

  NOTA: Você define as configurações de criptografia para um repositório na guia **Configuration** (Configuração) no Core Console.

4. Clique em **Deploy** (Implementar).

   A caixa de diálogo **Deploy Agent** (Implementar agente) é fechada. O agente selecionado pode demorar um pouco para aparecer na lista de máquinas protegidas.

Criar agendamentos personalizados de volumes

Para criar agendamentos personalizados de volumes:

1. Na caixa de diálogo **Protect Machine** (Proteger máquina) (para obter informações sobre como acessar essa caixa de diálogo, consulte Proteger uma máquina), em **Volume Groups** (Grupos de volumes), selecione um volume para proteção e, em seguida, clique em **Edit** (Editar).

   A caixa de diálogo **Protection Schedule** (Agendamento de proteção) é exibida.
2. Na caixa de diálogo **Protection Schedule** (Agendamento de proteção), selecione uma das seguintes opções de agendamento para a proteção de seus dados descritas a seguir:

Caixa de texto	Descrição
Interval (Intervalo)	Você pode escolher entre: • **Weekday** (Dia da semana) – Para proteger os dados em um intervalo de tempo específico, selecione **Interval** (Intervalo) e, em seguida: – Para personalizar quando proteger os dados durante períodos de pico, você pode especificar uma **Start Time** (Hora de início), uma **End Time** (Hora de término) e um **Interval** (Intervalo) nos menus suspensos. – Para proteger os dados durante períodos fora do pico, selecione **Protection interval during off-peak times** (Intervalo de proteção durante períodos fora do pico) e, em seguida, selecione um intervalo para a proteção no menu suspenso **Time** (Horário). • **Weekends** (Fins de semana) – Para proteger os dados durante os fins de semana também, selecione **Protection interval during weekends** (Intervalo de proteção durante os fins de semana) e, em seguida, selecione um **Interval** (Intervalo) no menu suspenso.

Caixa de texto	Descrição
Daily (Diariamente)	Para proteger os dados em um base diária, selecione a opção **Daily protection** (Proteção diária) e, em seguida, no menu suspenso **Time** (Horário), selecione um horário para iniciar a proteção de dados.
No Protection (Nenhuma proteção)	Para remover a proteção desse volume, selecione a opção **No Protection** (Nenhuma proteção).

Se quiser aplicar essas configurações personalizadas a todos os volumes nesta máquina, selecione **Apply to All Volumes** (Aplicar a todos os volumes).

3. Depois de fazer todas as alterações necessárias, clique em **OK**.
4. Repita a etapa 2 e a etapa 3 para quaisquer volumes adicionais que você queira personalizar.
5. Na caixa de diálogo **Protect Machine** (Proteger máquina), clique em **Protect** (Proteger).

Modificar as configurações do Exchange Server

Se você quiser proteger os dados de um Microsoft Exchange Server, precisa fazer configurações adicionais no Core Console.

Para modificar as configurações do Exchange Server:

1. Depois de adicionar a máquina do Exchange Server para proteção, selecione a máquina no painel **Navigation** (Navegação) do Core Console.

   A guia **Summary** (Resumo) referente à máquina aparece.
2. Na guia **Summary** (Resumo), clique no link **Exchange Server Settings** (Configurações do Exchange Server).

   A caixa de diálogo **Exchange Server Settings** (Configurações do Exchange Server) aparece.
3. Na caixa de diálogo **Exchange Server Settings** (Configurações do Exchange Server), você pode selecionar ou desmarcar as seguintes configurações:
   - Ativar verificação automática da capacidade de montagem.
   - Ativar verificação da soma de verificação noturna. Você ainda pode personalizar essa configuração selecionando o seguinte:
     - Truncar automaticamente os logs do Exchange após a verificação satisfatória da soma de verificação
     - Truncar log antes de terminar a soma de verificação
4. Você pode também modificar as credenciais de login para o Exchange Server. Para fazer isso, role para baixo até a seção **Exchange Server Information** (Informações do Exchange Server) e, em seguida, clique em **Change Credentials** (Alterar credenciais).

   A caixa de diálogo **Set Exchange Credentials** (Configurar credenciais do Exchange) é mostrada.
5. Digite as novas credenciais e, em seguida, clique em **OK**.

Modificar as configurações do SQL Serer

Se você estiver protegendo os dados do Microsoft SQL Server, algumas configurações adicionais precisam ser definidas no Core Console.

Para modificar as configurações do SQL Server:

1. Depois de adicionar a máquina do SQL Server para proteção, selecione a máquina no painel **Navigation** (Navegação) do Core Console.

A guia **Summary** (Resumo) referente à máquina é exibida.

2. Na guia **Summary** (Resumo), clique no link SQL Server Settings (Configurações do SQL Server).

   A caixa de diálogo **SQL Server Settings** (Configurações do servidor SQL) é exibida.

3. Na caixa de diálogo **SQL Server Settings** (Configurações do SQL Server), edite as configurações a seguir, conforme necessário:
   - Ativar verificação da capacidade de conexão noturna
   - Truncar log após verificação da capacidade de conexão satisfatória (modelo de recuperação simples apenas)

4. Você pode também modificar as credenciais de login para o SQL Server. Para fazer isso, avance para baixo até a tabela **SQL Server Information** (Informações do SQL Server) e, em seguida, clique em **Change Credentials** (Alterar credenciais).

   A caixa de diálogo **Set SQL Server Credentials** (Configurar credenciais do SQL Server) é exibida.

5. Digite as novas credenciais e, em seguida, clique em **OK**.

Implantar um agente (instalação por push)

O AppAssure requer o microsoft.net para a instalação do agente. O microsoft.net precisa ser instalado em qualquer máquina cliente antes de instalar o agente, manualmente ou por um processo de instalação por push.
O AppAssure permite implantar o Instalador do AppAssure Agent em máquinas Windows individuais, para proteção. Conclua as etapas no procedimento a seguir para forçar o instalador a um agente. Para implantar os agentes em múltiplas máquinas ao mesmo tempo, consulte Implantar em múltiplas máquinas .

NOTA: Os agentes devem ser configurados com uma política de segurança que possibilite a instalação remota.

Para implantar um agente:

1. No Core Console, clique na guia **Machines** (Máquinas).
2. No menu suspenso **Actions** (Ações), clique em **Deploy Agent** (Implantar agente).

   A caixa de diálogo **Deploy Agent** (Implantar agente) aparece.

3. Na caixa de diálogo **Deploy Agent** (Implantar agente), digite as configurações de login, conforme descrito na tabela a seguir.

Caixa de texto	Descrição
Máquina	Digite o nome do host ou endereço IP da máquina que você quer implantar.
Nome de usuário	Digite o nome de usuário para conectar-se a esta máquina (por exemplo, administrador).
Senha	Digite a senha para conectar-se a esta máquina.
Automatic reboot after install (Reinicialização automática depois da instalação)	Selecione essa opção para especificar se o Core iniciará após a conclusão da implantação e da instalação do AppAssure Agent.

4. Clique em **Verify** (Verificar) para validar as credenciais que você digitou.

   A caixa de diálogo **Deploy Agent** (Implantar agente) mostra uma mensagem, indicando que a validação está sendo realizada.

5. Clique em **Abort** (Cancelar) se você quiser cancelar o processo de verificação.

Quando o processo de verificação terminar, aparece uma mensagem indicando que a verificação está concluída.

6. Clique em **Deploy** (Implantar).

   Aparece uma mensagem indicando que a implantação iniciou. Você pode ver o andamento na guia **Events** (Eventos).

7. Clique em **Show details** (Mostrar detalhes) para ver mais informações sobre o status da implantação do agente.
8. Clique em **OK**.

Replicar um novo agente

Ao adicionar um AppAssure Agent para proteção em um núcleo de origem, o AppAssure oferece a você a opção de replicar o novo agente para um núcleo de destino existente.

Para replicar um novo agente:

1. Navegue até o Core Console e clique na guia **Machines** (Máquinas).
2. No menu suspenso **Actions** (Ações), clique em **Protect Machine** (Proteger máquina).
3. Na caixa de diálogo **Protect Machine** (Proteger máquina), digite as informações conforme descrito na tabela a seguir.

Caixa de texto	Descrição
Host	Digite o nome do host ou endereço IP da máquina que você deseja proteger.
Port (Porta)	Digite o número da porta que o AppAssure Core usa para se comunicar com o agente na máquina.
Username (Nome de usuário)	Digite o nome de usuário usado para conectar-se a essa máquina. Por exemplo, Administrador.
Password (Senha)	Digite a senha usada para conectar-se a esta máquina.

4. Clique em **Connect** (Conectar) para conectar-se a essa máquina
5. Clique em **Show Advanced Options** (Mostrar opções avançadas) e edite as configurações a seguir conforme necessário.

Caixa de texto	Descrição
Display Name (Nome de exibição)	Digite um nome para a máquina a ser mostrado no Core Console.
Repository (Repositório)	Selecione o repositório no AppAssure Core onde os dados dessa máquina são armazenados.
Encryption Key (Chave de criptografia)	Especifique se a criptografia é aplicada aos dados para cada volume nessa máquina armazenado no repositório. NOTA: As configurações de criptografia para um repositório são definidas na guia **Configuration** (Configuração) no Core Console.
Remote Core (Núcleo remoto)	Especifique o núcleo de destino ao qual você deseja replicar o agente.

Caixa de texto	Descrição
Remote Repository (Repositório remoto)	O nome do repositório desejado no núcleo de destino no qual serão armazenados os dados replicados dessa máquina.
Pause (Pausar)	Marque essa caixa de seleção se você deseja pausar a replicação; por exemplo, para pausá-la até depois que o AppAssure salvar uma imagem de base do novo agente.
Programação	Selecione uma das seguintes opções: • Proteger todos os volumes com o cronograma padrão • Proteger volumes específicos com o cronograma personalizado NOTA: O cronograma padrão é a cada 15 minutos.
Initially pause protection (Pausar proteção inicialmente)	Marque essa caixa de seleção se você deseja pausar a proteção; por exemplo, para evitar que o AppAssure salve a imagem de base até depois dos horários de pico de uso.

6. Clique em **Protect** (Proteger).

Gerenciar as máquinas

Esta seção descreve uma variedade de tarefas que você pode executar ao gerenciar as suas máquinas, tal como remover uma máquina do seu ambiente AppAssure, configurar a replicação, forçar a truncagem de log, cancelar operações, entre outros.

Remover uma máquina

1. Navegue até o Core Console e, em seguida, clique na guia **Machines** (Máquinas).
2. Na guia **Machines** (Máquinas), execute um dos procedimentos a seguir:
   - Clique no hiperlink da máquina que você quer remover.
   - Ou, no painel de navegação, selecione a máquina que você quer remover.
3. No menu suspenso **Actions** (Ações), clique em **Remove Machines** (Remover máquinas) e, e seguida, selecione uma das opções descritas na tabela a seguir.

Opção	Descrição
Relationship Only (Apenas relação)	Remove o núcleo de origem da replicação mas mantém os pontos de recuperação replicados.
With Recovery Points (Com pontos de recuperação)	Remove o núcleo de origem da replicação e apaga todos os pontos de recuperação replicados recebidos da máquina.

Replicar dados do agente em uma máquina

A replicação é a relação entre os núcleos de origem e destino na mesma unidade, ou entre duas unidades com conexão lenta por cada agente. Quando a replicação é configurada entre dois núcleos, o

núcleo de origem transmite de forma assíncrona os dados de instantâneo incremental dos agentes selecionados para o núcleo de destino ou de origem. A replicação de saída pode ser configurada para um provedor de serviços gerenciados que ofereça serviço de recuperação de desastres e backup externo ou para um núcleo autogerenciado. Para replicar dados de agente em uma máquina:

1. No Core Console, clique na guia **Machines** (Máquinas).
2. Selecione a máquina que você deseja replicar.
3. No menu suspenso **Actions** (Ações), clique em **Replication** (Replicação) e depois execute uma das opções a seguir:
   - Se estiver configurando a replicação, clique em **Enable** (Ativar).
   - Se já tiver uma replicação atual configurada, clique em **Copy** (Copiar).

   A caixa de diálogo **Enable Replications** (Ativar replicações) é mostrada.
4. Na caixa de texto **Host**, digite um nome de host.
5. Em **Agents** (Agentes), selecione a máquina que possui o agente e os dados que você deseja replicar.
6. Caso seja necessário, marque a caixa de seleção **Use a seed drive to perform initial transfer** (Usar uma unidade de propagação para realizar transferência inicial).
7. Clique em **Add** (Adicionar).
8. Para pausar ou continuar a replicação, clique em **Replication** (Replicação) no menu suspenso **Actions** (Ações) e depoisclique em **Pause** (Pausar) ou **Resume** (Retomar) conforme necessário.

Configurar a prioridade de replicação para um agente

Para configurar a prioridade de replicação para um agente:

1. No Core Console, selecione a máquina protegida para a qual você deseja definir a prioridade de replicação e clique na guia **Configuration** (Configuração).
2. Clique em **Select Transfer Settings** (Selecionar configurações de transferência) e use a lista suspensa **Priority** (Prioridade) para selecionar uma das opções a seguir:
   - **Padrão**
   - **Highest (Mais alta)**
   - **Lowest (Mais baixa)**
   - **1**
   - **2**
   - **3**
   - **4**

   NOTA: A prioridade padrão é 5. Se um agente receber a prioridade 1 e outro agente receber a prioridade Mais alta, o agente com a prioridade Mais alta realiza a replicação antes do agente com a prioridade 1.
3. Clique em **OK**.

Cancelar as operações em uma máquina

Você pode cancelar operações atualmente em execução em uma máquina. Você pode especificar cancelar apenas um instantâneo atual ou cancelar todas as operações atuais, o que inclui exportações, replicações e assim por diante.

Para cancelar as operações em uma máquina:

1. No Core Console, clique na guia **Machines** (Máquinas).
2. Selecione a máquina para a qual você quer cancelar operações.
3. No menu suspenso **Actions** (Ações), clique em **Cancel** (Cancelar) e, em seguida, selecione uma das opções descritas a seguir:

Caixa de texto	Descrição
All Operations (Todas as operações)	Cancela todas as operações ativas nesta máquina.
Snapshot (Instantâneo)	Cancela o instantâneo atualmente em andamento.

Ver o status da máquina e outros detalhes

Para ver o status da máquina e outros detalhes:

1. No painel de navegação do Core Console, escolha uma das opções a seguir:
   - Selecione a guia **Machines** (Máquinas) e, em seguida, clique no hiperlink da máquina que você quer ver.
   - No painel de navegação, clique na máquina que você quer ver.

A guia **Summary** (Resumo) é mostrada.

As informações sobre a máquina são mostradas na página **Summary** (Resumo). Os detalhes mostrados contêm o seguinte:

- Nome do host
- Último instantâneo obtido
- Próximo instantâneo agendado
- Status da criptografia
- Número da versão
- Status da verificação da capacidade de montagem
- Status da verificação da soma de verificação
- Última truncagem de log realizada

Informações detalhadas sobre os volumes contidos nessa máquina também aparecem e contêm:

- Tamanho total
- Espaço usado
- Espaço livre

Se o SQL Server estiver instalado na máquina, as informações detalhadas sobre o servidor também são mostradas e contêm:

- Nome
- Caminho da instalação
- Versão
- Número da versão

- Nome do banco de dados
- Status on-line

Se o Exchange Server estiver instalado na máquina, as informações detalhadas sobre o servidor e os armazenamentos de e-mail também são mostradas e contêm:

- Nome
- Caminho da instalação
- Caminho dos dados
- Nome do caminho dos bancos de dados do Exchange
- Caminho do arquivo de log
- Prefixo do log
- Caminho do sistema
- Tipo de MailStore

Gerenciar múltiplas máquinas

Este tópico descreve as tarefas que os administradores realizam para implantar o software Agent simultaneamente em múltiplas máquinas Windows.

Para implantar e proteger múltiplos agentes, realize as seguintes tarefas:

1. Implante o AppAssure em múltiplas máquinas.
   Consulte Implantar em múltiplas máquinas.
2. Monitore a atividade de implementação em lote.
   Consulte Monitorar a implantação de múltiplas máquinas.
3. Proteja múltiplas máquinas.
   Consulte Proteger múltiplas máquinas.

   NOTA: Essa etapa pode ser ignorada se selecionou a opção Protect Machine After Install (Proteger máquina após a instalação) durante a implementação.
4. Monitore a atividade da proteção em lote.
   Consulte Monitorar a proteção de múltiplas máquinas.

Implantar em múltiplas máquinas

Você pode simplificar a tarefa de implantação do software AppAssure Agent para múltiplas máquinas Windows , usando o recurso de Implantação por volume do AppAssure. Você pode implantar por volume para:

- Máquinas em um host virtual VMware vCenter/ESXi
- Máquinas em um domínio do Active Directory
- Máquinas de qualquer outro host

O recurso de Implantação em massa detecta automaticamente as máquinas em um host e permite selecionar as que você quer implantar. Como alternativa, você pode digitar manualmente as informações da máquina e do host.

NOTA: As máquinas que você está implantando precisam ter acesso à Internet para fazer o download e instalar bits, pois o AppAssure usa a versão Web do Instalador do AppAssure Agent para implantar os componentes da instalação. Se o acesso à Internet não estiver disponível , você pode forçar o programa de instalação do AppAssure Agent na máquina Core. Para obter informações sobre como fazer isso, consulte Forçar o programa de instalação do Agent a partir da máquina Core. Você pode fazer o download de atualizações do Core e do Agent no Portal de licenças.

Forçar o programa de instalação do Agent a partir da máquina Core

Se os servidores que estão sendo implementados não tiverem acesso à Internet, você pode forçar o arquivo de instalação do agente a partir da máquina Core. O dispositivo inclui o arquivo do programa de instalação do agente.

NOTA: Faça o download das atualizações do Core e do Agent no Portal de licenças.

Para forçar o programa de instalação do Agent a partir da máquina Core:

1. A partir da máquina Core, copie o arquivo de instalação do Agent **Agent-X64–5.x.x.xxxxx.exe** para o diretório **C:\Arquivos de Programas\apprecovery\core\installers**.
2. No Core Console, selecione a guia **Configuration** (Configuração) e, em seguida, clique em **Settings** (Parâmetros).
3. Na seção **Deploy Settings** (Configurações da implantação), edite o **Agent Installer Name** (Nome do instalador do Agent).

Implantar em máquinas em um domínio do Active Directory

Antes de começar este procedimento, você precisa ter as informações do domínio e as credenciais de login para o servidor do Active Directory.

Para implantar o agente em várias máquinas em um domínio do Active Directory:

1. No Core Console, clique na guia **Tools** (Ferramentas) e, em seguida, clique em **Bulk Deploy** (Implantação em massa).
2. Na janela, clique em **Deploy Agent on Machines** (Implantar agente nas máquinas), clique em **Active Directory**.
3. Na caixa de diálogo **Connect to Active Directory** (Conectar ao Active Directory), digite as informações do domínio e as credenciais de login descritas na tabela a seguir:

Caixa de texto	Descrição
Domínio	O nome do host ou o endereço IP do domínio do Active Directory.
Nome de usuário	O nome de usuário usado para conectar-se ao domínio; por exemplo, Administrador.
Senha	A senha segura usada para conectar-se ao domínio.

4. Clique em **Connect** (Conectar).
5. Na caixa de diálogo **Add Machines from Active Directory** (Adicionar máquinas a partir do Active Directory) , selecione as máquinas em que você quer implantar o AppAssure Agent e, em seguida, clique em **Add** (Adicionar).

   As máquinas que você adicionou aparecem na janela **Deploy Agent on Machines** (Implantar Agent nas máquinas).
6. Digite a senha da máquina, selecione um repositório, adicione uma chave de criptografia, ou edite outras configurações para uma máquina, clique no link **Edit** (Editar) da máquina e, em seguida, faça o seguinte.

a. Na caixa de diálogo **Edit Settings** (Editar configurações), especifique as configurações conforme descrito na tabela a seguir:

Caixa de texto	Descrição
Nome do host	Automaticamente fornecido na etapa 3.
Nome da tela	Automaticamente atribuído com base no nome de host fornecido na etapa 3.
Porta	O número da porta em que o Core se comunica com o agente na máquina.
Nome de usuário	Automaticamente fornecido na etapa 3.
Senha	Digite a senha para a máquina.
Reinicialização automática depois da instalação	Especifique se quer reinicializar automaticamente a máquina após a implantação . NOTA: Essa opção é obrigatória se você quiser proteger a máquina automaticamente após a implantação, marcando a caixa **Protect Machine After Install** (Proteger máquina após a instalação).
Proteger máquina após a instalação	Especifique se quer proteger a máquina automaticamente após a implantação. Isso permite que você ignore a etapa **Proteger múltiplas máquinas**.
Repositório	Use a lista suspensa para selecionar o repositório do Core em que os dados das máquinas devem ser armazenados. O repositório selecionado é usado para todas as máquinas que serão protegidas. NOTA: Essa opção está disponível somente quando você selecionar **Protect Machine after Install** (Proteger máquina após a instalação).
Chave de criptografia	(Opcional) Use a lista suspensa para especificar se a criptografia deve ser aplicada aos dados na máquina que deve ser armazenada no repositório. A chave de criptografia é atribuída a todas as máquinas que serão protegidas. NOTA: Essa opção está disponível somente quando você selecionar **Protect Machine after Install** (Proteger máquina após a instalação)

b. Clique em **Save** (Salvar).

7. Para verificar se o AppAssure pode conectar-se a cada máquina satisfatoriamente, selecione cada máquina na janela **Deploy Agent on Machines** (Implantar agente nas máquinas) e clique em **Verify** (Verificar).
8. A janela **Deploy Agent on Machines** (Implantar agente nas máquinas) mostra um ícone ao lado de cada máquina que reflete sua prontidão para a implantação, da seguinte forma:

Caixa de texto	Descrição
Ícone Verde	O AppAssure pode conectar-se à máquina e ela está pronta para ser implantada.
Ícone Amarelo	O AppAssure pode conectar-se à máquina; no entanto, o agente já está emparelhado com uma máquina de núcleo.

Caixa de texto	Descrição
Ícone Vermelho	O AppAssure não pode conectar-se à máquina. O motivo pode ser que as credenciais de login estão incorretas, a máquina está desligada, o firewall está bloqueando o tráfego ou outro problema. Para corrigir, clique em **Edit Settings** (Editar as Configurações) na barra de ferramentas ou no link **Edit** (Editar) ao lado da máquina.

9. Depois que as máquinas forem verificadas satisfatoriamente, selecione cada máquina em que você quer implantar o AppAssure Agent e, em seguida, clique em **Deploy** (Implantar).
10. Se você escolher a opção **Protect machine after install** (Proteger máquina depois da instalação), após a implementação satisfatória as máquinas reinicializarão automaticamente e a proteção estará ativada.

Implantar máquinas em um host virtual VMware vCenter/ESXi

Antes de começar este procedimento, você precisa ter as informações do host local e credenciais de login para o host virtual VMware vCenter/ESXi.

NOTA: Todas as máquinas virtuais precisam ter ferramentas de VM instaladas; caso contrário, o AppAssure não consegue detectar o nome de host da máquina virtual para implantar. Em vez do nome de host , o AppAssure usa o nome da máquina virtual, o que pode causar problemas se o nome de host for diferente do nome da máquina virtual.

Para implantar várias máquinas em um host virtual VMware vCenter/ESXi:

1. No Core Console, clique na guia **Tools** (Ferramentas) e, em seguida, clique em **Bulk Deploy** (Implantar por volume).
2. Na janela **Deploy Agent on Machines** (Implantar agente nas máquinas), clique em **vCenter/ESXi**.
3. Na caixa de diálogo **Connect to VMware vCenter Server/ESXi** (Conectar a VMware vCenter Server/ESXi), digite as informações do host e as credenciais de login como a seguir e clique em **OK**.

Caixa de texto	Descrição
Host	Digite o nome ou endereço IP do host virtual VMware vCenter Server/ESX(i) .
User Name (Nome de usuário)	O nome de usuário usado para conectar-se ao host virtual; por exemplo, administrador.
Password (Senha)	Digite a senha usada para conectar-se a este host virtual.

4. Na caixa de diálogo **Add Machines from VMware vCenter Server/ESXi** (Adicionar máquinas a partir do VMware vCenter Server/ESXi), selecione as máquinas em que você quer implantar o AppAssure Agent e, em seguida, clique em **Add** (Adicionar).
5. Na janela **Deploy Agent on Machines** (Implantar agente nas máquinas), você pode ver as máquinas que adicionou. Se quiser selecionar um repositório, chave de criptografia ou outras configurações para uma máquina, marque a caixa de seleção ao lado da máquina e clique em **Edit Settings** (Editar configurações).

   Para obter os detalhes de cada configuração, consulte Implantar máquinas em um domínio do Active Directory.
6. Verifique se o AppAssure pode se conectar a cada máquina com êxito. Selecione cada máquina na janela **Deploy Agent on Machines** (Implantar agente nas máquinas) e, em seguida, clique em **Verify** (Verificar).
7. A janela **Deploy Agent on Machines** (Implantar agente nas máquinas) mostra um ícone ao lado de cada máquina que reflete sua prontidão para a implantação, da seguinte forma:

Caixa de texto	Descrição
Ícone verde	O AppAssure pode se conectar à máquina e ela está pronta para ser implantada.
Ícone amarelo	O AppAssure pode se conectar à máquina; no entanto, o agente já está emparelhado com uma máquina de núcleo.
Ícone vermelho	AppAssure não pode se conectar à máquina. O motivo pode ser que as credenciais de login estão incorretas, a máquina está desligada, o firewall está bloqueando o tráfego ou outro problema. Para corrigir, clique em **Edit Settings** (Editar configurações) na barra de ferramentas ou no link **Edit** (Editar) ao lado da máquina.

8. Depois que as máquinas forem verificadas satisfatoriamente, selecione cada máquina e clique em **Deploy** (Implantar).
9. Se você escolher a opção **Protect machine after install** (Proteger máquina depois da instalação), após a implementação satisfatória, as máquinas reinicializarão automaticamente e a proteção estará ativada.

Implantar em máquinas de qualquer outro host

Para implantar em máquinas de qualquer outro host:

1. No Core Console, clique na guia **Tools** (Ferramentas) e, em seguida, clique em **Bulk Deploy** (Implantação em massa).
2. Na janela **Deploy Agent on Machines** (Implantar agente nas máquinas), faça o seguinte:
   - Clique em **New** (Novo) para especificar múltiplas máquinas usando a caixa de diálogo **Add Machine** (Adicionar máquina); isso permite inserir um novo host da máquina, credenciais de login, repositório, chave de criptografia e outras informações. Para obter detalhes sobre cada configuração, consulte Implantar em máquinas em um domínio do Active Directory.

     Depois de digitar essas informações, clique em **OK** para adicioná-las à lista **Deploy Agent on Machines** (Implantar agente nas máquinas) ou clique em **OK & New** (OK e Novo) para adicionar outra máquina.

     NOTA: Se você quiser proteger a máquina automaticamente após a implantação, marque a caixa de seleção **Protect Machine after Install** (Proteger máquina após a instalação). Se você marcar a caixa , a máquina reinicializará automaticamente antes de ativar a proteção.
   - Clique em **Manually** (Manualmente) para especificar múltiplas máquinas em uma lista; cada linha representa uma máquina para implantar. Na caixa de diálogo **Add Machines Manually** (Adicionar máquinas manualmente), digite o endereço IP ou nome da máquina, o nome de usuário e a senha separados por um delimitador dois-pontos e porta da seguinte forma:

     ```
     hostname::username::password::port
     For example:
     10.255.255.255::administrator::&11@yYz90z::8006
     abc-host-00-1::administrator::99!zU$o83r::168
     ```
3. Na janela **Deploy Agent on Machines** (Implantar agente nas máquinas), veja as máquinas que você adicionou. Se quiser selecionar um repositório, chave de criptografia ou outras configurações para uma máquina, marque a caixa de seleção ao lado da máquina e clique em **Edit Settings** (Editar configurações).

   Para obter os detalhes de cada configuração, consulte Implantar máquinas em um domínio do Active Directory.
4. Verifique se o AppAssure pode conectar-se a cada máquina satisfatoriamente. Selecione cada máquina na janela **Deploy Agent on Machines** (Implantar agente nas máquinas) e, em seguida, clique em **Verify** (Verificar).

A janela **Deploy Agent on Machines** (Implantar agente nas máquinas) mostra um ícone ao lado de cada máquina que reflete sua prontidão para a implantação, da seguinte forma:

Caixa de texto	Descrição
Ícone Verde	O AppAssure pode conectar-se à máquina e ela está pronta para ser implantada.
Ícone Amarelo	O AppAssure pode conectar-se à máquina; no entanto, o agente já está emparelhado com uma máquina de núcleo.
Ícone Vermelho	O AppAssure não pode conectar-se à máquina. O motivo pode ser que as credenciais de login estão incorretas, a máquina está desligada, o firewall está bloqueando o tráfego ou outro problema. Para corrigir, clique em **Edit Settings** (Editar as configurações) na barra de ferramentas ou no link **Edit** (Editar) ao lado da máquina.

5. Depois que as máquinas forem verificadas satisfatoriamente, marque a caixa ao lado de cada máquina e clique em **Deploy** (Implantar).
6. Se você escolher a opção **Protect machine after install** (Proteger máquina depois da instalação), após a implementação satisfatória as máquinas reinicializarão automaticamente e a proteção estará ativada.

Monitorar a implantação de várias máquinas

Você pode ver o andamento da implantação do software do AppAssure Agent nas máquinas.

Para monitorar a implantação de várias máquinas:

1. No Core Console, clique na guia **Events** (Eventos), localize a tarefa de implantação na lista e clique no botão na coluna **Details** (Detalhes).

   A janela **Monitor Active Task** (Monitor de tarefa ativa) mostra os detalhes da implantação.

   Ela apresenta informações sobre o progresso geral, bem como o status de cada implantação individual. Os detalhes da tela incluem:

   - Start Time (Hora de início)
   - End Time (Hora de término)
   - Elapsed Time (Tempo decorrido)
   - Time Remaining (Tempo restante)
   - Progress (Andamento)
   - Phase (Fase)
2. Faça um dos seguintes:
   - Clique em **Open in New window** (Abrir em uma nova janela) para abrir uma nova janela para visualizar o andamento da implantação.
   - Clique em **Close** (Fechar) e as tarefas de implementação processarão em segundo plano.

Proteger múltiplas máquinas

Depois da implementação por volume do software Agent nas máquinas Windows, você precisa agora protegê-las para proteger os dados. Se você selecionou **Protect Machine After Install** (Proteger máquina depois da instalação) quando implantou o agente, pode pular este procedimento.

NOTA: As máquinas agentes precisam ser configuradas com uma política de segurança que possibilite a instalação remota.

Para proteger múltiplas máquinas:

1. No Core Console, clique na guia **Tools** (Ferramentas) e, em seguida, clique em **Bulk Protect** (Proteger em massa).

   A janela **Protect Machines** (Proteger máquinas) é exibida.
2. Adicione as máquinas que você quer proteger, clicando em uma das opções a seguir.

   Para obter detalhes sobre como completar cada opção, consulte Implementar múltiplas máquinas .
   - Clique em **Active Directory** (Diretório ativo) para especificar as máquinas em um domínio do Active Directory.
   - Clique em **vCenter/ESXi** para especificar as máquinas virtuais em um host virtual vCenter/ESXi.
   - Clique em **New** (Novo) para especificar múltiplas máquinas usando a caixa de diálogo Add Machine (Adicionar máquina).
   - Clique em **Manually** (Manualmente) para especificar múltiplas máquinas em uma lista, digitando o nome de host e as credenciais.
3. Na janela **Protect Machines** (Proteger máquinas), você pode ver as máquinas que adicionou. Se quiser selecionar um repositório, chave de criptografia ou outras configurações avançadas para uma máquina, marque a caixa de seleção ao lado da máquina e clique em **Edit Settings** (Editar configurações).
4. Especifique as configurações como a seguir e clique em **OK**.

Caixa de texto	Descrição
Username (Nome de usuário)	Digite o nome do usuário usado para conectar-se a esta máquina (por exemplo, Administrador).
Password (Senha)	Digite a senha usada para conectar-se a esta máquina.
Port (Porta)	Especifique o número da porta na qual o Core se comunica com o agente na máquina.
Repository (Repositório)	Selecione o repositório no Core onde os dados das máquinas estão armazenados. O repositório selecionado é usado para todas as máquinas que estão sendo protegidas.
Encryption Key (Chave de criptografia)	Especifique se a criptografia será aplicada ao agente nas máquinas que estão armazenadas no repositório. A chave de criptografia é atribuída a todas as máquinas que estão sendo protegidas.
Protection Schedule (Agendamento da proteção)	Especifique o agendamento de ocorrência da proteção da máquina. O agendamento padrão é de 60 minutos no horário de pico e 60 minutos nos fins de semana. Para editar o agendamento para atender às necessidades da sua empresa, clique em **Edit** (Editar). NOTA: Para obter mais informações, consulte Modificar os agendamentos de proteção.
Initially Pause Protection (Pausar proteção inicialmente)	Opcionalmente, você pode optar por pausar a proteção na primeira execução; ou seja, o núcleo não obtém instantâneos das máquinas até que você retome a proteção manualmente.

5. Verifique se o AppAssure pode se conectar a cada máquina com êxito. Para isso, marque a caixa de seleção ao lado de cada máquina na janela **Protect Machines** (Proteger máquinas) e clique em **Verify** (Verificar).

6. A janela **Protect Machines** (Proteger máquinas) mostra um ícone junto a cada máquina que se refere à sua prontidão para a implementação, da seguinte forma:

Ícone	Descrição
Ícone verde	O AppAssure pode se conectar à máquina e ela está pronta para ser protegida.
Ícone amarelo	O AppAssure pode se conectar à máquina; no entanto, o agente já está emparelhado com uma máquina de núcleo.
Ícone vermelho	AppAssure não pode se conectar à máquina. O motivo pode ser que as credenciais de login estão incorretas, a máquina está desligada, o firewall está bloqueando o tráfego ou outro problema. Para corrigir, clique em **Edit Settings** (Editar configurações) na barra de ferramentas ou no link **Edit** (Editar) ao lado da máquina.

7. Depois que as máquinas forem verificadas satisfatoriamente, marque a caixa ao lado de cada máquina e clique em **Protect** (Proteger).

Monitorar a proteção de múltiplas máquinas

Você pode monitorar o andamento enquanto o AppAssure aplica as políticas de proteção e os agendamentos às máquinas.

Para monitorar a proteção de várias máquinas:

1. Clique na guia **Machines** (Máquinas) para ver o status e o andamento da proteção.
   A página **Protected Machines** (Máquinas protegidas) aparece.
2. Clique na guia **Events** (Eventos) para ver as tarefas relacionadas, eventos e alertas.
   A página **Tasks** (Tarefas) aparece.

Caixa de texto	Descrição
Para ver as informações da tarefa	Conforme os volumes são transferidos, o status, hora de início e hora de término aparecem no painel **Tasks** (Tarefas). Clique em **Details** (Detalhes) para ver mais informações específicas sobre a tarefa.
Para ver informações de alerta	Conforme cada máquina protegida é adicionada, é registrado um alerta que detalha se a operação foi satisfatória ou se algum erro foi registrado. O nível do alerta, juntamente com a data da transação e mensagem, são mostrados. Se você quer remover todos os alertas da página, clique em **Dismiss All** (Ignorar todos).
Para ver as informações do evento	Os detalhes da máquina e dos dados transferidos são mostrados no painel **Events** (Eventos). O nível do evento, a data da transação e a hora da mensagem aparecem.

Gerenciar instantâneos e pontos de recuperação

Um ponto de recuperação é uma coleção de instantâneos salva de volumes de disco individuais e armazenados no repositório. Os instantâneos capturam e armazenam o estado de um volume de disco em um determinado ponto no tempo, enquanto os aplicativos que geram os dados ainda estão em uso. No AppAssure, você pode forçar um instantâneo, pausar instantâneos temporariamente e ver listas de pontos de recuperação atuais no repositório, além de apagá-los caso seja necessário. Pontos de recuperação são usados para restaurar máquinas protegidas ou para montar para um sistema local de arquivos.

Os instantâneos que o AppAssure coleta são capturados a nível de bloco e possuem reconhecimento de aplicativos. Isso significa que todos os logs de transações em andamento e transações em aberto são concluídos e caches são liberados para o disco antes de criar o instantâneo.

O AppAssure 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.

Ver pontos de recuperação

Para ver pontos de recuperação:

1. Na área de navegação esquerda do Core Console, selecione a máquina para a qual você deseja ver os pontos de recuperação e depois clique na guia **Recovery Points** (Pontos de recuperação).

Você pode ver informações sobre os pontos de recuperação da máquina conforme escrito na tabela a seguir:

Informações	Descrição
Status	Indica o status atual do ponto de recuperação.
Encrypted (Criptografado)	Indica se o ponto de recuperação está criptografado.
Contents (Conteúdo)	Lista os volumes incluídos no ponto de recuperação.
Type (Tipo)	Define um ponto de recuperação como de base ou diferencial.
Creation Date (Data de criação)	Mostra a data em que o ponto de recuperação foi criado.
Size (Tamanho)	Mostra a quantidade de espaço que o ponto de recuperação consome no repositório.

Ver um ponto de recuperação específico

Para ver um ponto de recuperação específico:

1. Na área de navegação à esquerda do Core Console, selecione a máquina cujos pontos de recuperação você quer ver e, em seguida, selecione a guia **Recovery Points** (Pontos de recuperação).
2. Clique em **>** ao lado de um ponto de recuperação na lista para ampliar a visualização.

   Você pode ver informações mais detalhadas sobre o conteúdo do ponto de recuperação para a máquina selecionada, bem como acessar uma variedade de operações que podem ser realizadas no ponto de recuperação, descritas na tabela a seguir:

Informações	Descrição
Ações	O menu **Actions** (Ações) inclui as seguintes operações que você pode realizar no ponto de recuperação selecionado: **Mount** (Montar) - Selecione essa opção para montar o ponto de recuperação selecionado. Para obter mais informações sobre a montagem de um ponto de

recuperação selecionado, consulte Montar um ponto de recuperação para uma máquina Windows.

Export (Exportar) - Com essa opção, você pode exportar o ponto de recuperação selecionado para o ESXi, estação de trabalho VMware ou HyperV. Para obter mais informações sobre como exportar pontos de recuperação selecionados, consulte Exportar informações de backup sobre a máquina Windows para uma máquina virtual.

Rollback (Reverter) - Selecione essa opção para realizar uma restauração do ponto de recuperação selecionado para um volume que você especificar. Para obter mais informações sobre como restaurar pontos de recuperação selecionados, consulte Iniciar uma restauração a partir do AppAssure Core.

3. Clique em **>** ao lado de um volume no ponto de recuperação selecionado para ampliar a visualização.

Você pode ver informações sobre o volume selecionado no ponto de recuperação ampliado conforme escrito na tabela a seguir:

Caixa de texto	Descrição
Título	Indica o volume específico no ponto de recuperação.
Raw Capacity (Capacidade bruta)	Indica a quantidade de espaço de armazenamento bruto em todo o volume.
Formatted Capacity (Capacidade formatada)	Indica a quantidade de espaço de armazenamento no volume que está disponível para dados após o volume ser formatado.
Used Capacity (Capacidade usada)	Indica a quantidade de espaço de armazenamento atualmente usado no volume.

Montar um ponto de recuperação para uma máquina Windows

No AppAssure, você pode montar um ponto de recuperação para uma máquina Windows, a fim de acessar os dados armazenados através de um sistema de arquivos local.

Para montar um ponto de recuperação para uma máquina Windows:

1. No Core Console, escolha uma das opções a seguir:
   - Selecione a guia **Machines** (Máquinas).

     a. Ao lado da máquina ou do cluster com o ponto de recuperação que você quer montar, selecione **Mount** (Montar) no menu suspenso **Actions** (Ações).
     b. Selecione um ponto de recuperação da lista, na caixa de diálogo **Mount Recovery Point** (Montar um ponto de recuperação) e, em seguida, clique em **Next** (Avançar).

     A caixa de diálogo **Mount Recovery Point** (Montar ponto de recuperação) aparece.
   - No Console Core, selecione a máquina que você quer montar em um sistema de arquivos local.

A guia **Summary** (Resumo) da máquina selecionada é mostrada.

a. Selecione a guia **Recovery Points** (Pontos de recuperação).
b. Na lista de pontos de recuperação, expanda o ponto de recuperação que você quer montar.
c. Nos detalhes expandidos desse ponto de recuperação, clique em **Mount** (Montar).

   A caixa de diálogo **Mount Recovery Point** (Montar ponto de recuperação) aparece.

2. Na caixa de diálogo **Mount** (Montar), edite as caixas de texto para a montagem de um ponto de recuperação, conforme descrito na tabela a seguir:

Caixa de texto	Descrição
Local de montagem: pasta local	Especifique o caminho usado para acessar o ponto de recuperação montado.
Imagens do volume	Especifique as imagens do volume que você quer montar.
Tipo de montagem	Especifique como quer acessar os dados para o ponto de recuperação montado: • Montar somente leitura. • Montar somente leitura com gravações prévias. • Montar gravável.
Crie um compartilhamento Windows para esta Montagem	Ou então, marque a caixa de seleção para especificar se o ponto de recuperação montado pode ser compartilhado e, em seguida, configure os direitos de acesso a ele, incluindo o nome do compartilhamento e os grupos de acesso.

3. Clique em **Mount** (Montar) para montar o ponto de recuperação.

Desmontar pontos de recuperação selecionados

Você pode desmontar os pontos de recuperação selecionados que estão montados localmente no Core.

Para desmontar pontos de recuperação selecionados:

1. No Core Console, clique na guia **Tools** (Ferramentas).
2. Na opção **Tools** (Ferramentas), clique em **System Info** (Informações do sistema).
3. Localize e selecione a tela instalada para o ponto de recuperação que você quer desmontar e, em seguida, clique em **Dismount** (Desmontar).

Desmontar todos os pontos de recuperação

Você pode desmontar todos os pontos de recuperação que estão montados localmente no Core.

Para desmontar todos os pontos de recuperação:

1. No Core Console, selecione a guia **Tools** (Ferramentas).
2. Na opção **Tools** (Ferramentas), clique em **System Info** (Informações do sistema).
3. Na seção **Local Mounts** (Montagens locais), clique em **Dismount All** (Desmontar todos).

Montar um volume de ponto de recuperação em uma máquina Linux

1. Crie um novo diretório para montar o ponto de recuperação (por exemplo, você pode usar o comando `mkdir`).
2. Verifique se o diretório existe (por exemplo, usando o comando `ls`).
3. Execute o utilitário **aamount** do AppAssure como raiz ou superusuário, por exemplo:

   ```
   sudo aamount
   ```
4. No prompt de montagem do AppAssure, 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 AppAssure Core.
6. Digite as credenciais de login do servidor de núcleo, ou seja, o nome de usuário e a senha.

   Uma lista mostra as máquinas protegidas por esse servidor do AppAssure. Ela mostra as máquinas encontradas por número de item da linha, endereço de host/IP e um número de ID para a máquina (por exemplo: `293cc667-44b4-48ab-91d8-44bc74252a4f`).
7. Digite o comando a seguir para mostrar uma lista dos pontos de recuperação atualmente montados para uma máquina especificada:

   ```
   lr <line_number_of_machine>
   ```

   NOTA: Você pode também inserir o número de identificação da máquina nesse comando em vez do número de item de linha.

   Uma lista mostra os pontos de recuperação básicos e incrementais da máquina. A lista inclui um número de item, marcação de data/hora,local do volume, tamanho do ponto de recuperação e um número de ID do volume que inclui um número de sequência no final (por exemplo, `293cc667-44b4-48ab-91d8-44bc74252a4f:2`), que identifica o ponto de recuperação.
8. Digite o seguinte comando para selecionar e montar esse ponto de recuperação no ponto de montagem/caminho especificado.

   ```
   m <volume_recovery_point_ID_number> <path>
   ```

   NOTA: Você pode também 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 do agente/máquina (gerado pelo lm), seguido pelo número de linha do ponto de recuperação e letra do volume, seguido pelo caminho, por exemplo, `m <machine_line_number> <recovery_point_line_number> <volume_letter> <path>`. Por exemplo, se a saída do `lm` mostrar três máquinas agentes, e você inserir o comando `lr` para número 2 e montar o volume b do ponto de recuperação 23 para **/tmp/mount_dir**, o comando será: `m 2 23 b /tmp/mount_dir`.

   CUIDADO: **Não desmonte um volume protegido Linux manualmente. Caso precise fazer isso, execute o seguinte comando antes de desmontar o volume: `bsctl -d <path to volume>`. Nesse comando, `<path to volume>` não se refere ao ponto de montagem do volume, mas sim ao descritor de arquivo do volume; ele precisa estar em uma forma semelhante a este exemplo: /dev/sda1.**

Remover pontos de recuperação

Você pode remover facilmente pontos de recuperação para uma máquina em particular a partir do repositório. Quando apagar pontos de recuperação no AppAssure, você pode especificar uma das seguintes opções:

Caixa de texto	Descrição
Delete All Recovery Points (Apagar todos os pontos de recuperação)	Remove todos os pontos de recuperação para a máquina agente selecionada a partir do Repositório.
Delete a Range of Recovery Points (Apagar uma faixa de pontos de recuperação)	Remove todos os pontos de recuperação em um intervalo especificado, antes do atual até e incluindo a imagem de base, que trata-se de todos os dados da máquina , bem como todos os pontos de recuperação após o atual até a próxima imagem de base .

NOTA: Você não pode recuperar os pontos de recuperação tiver apagado.

Para remover pontos de recuperação :

1. Na área de navegação à esquerda do Core Console, selecione a máquina cujos pontos de recuperação você quer ver e, em seguida, clique na guia **Recovery Points** (Pontos de recuperação).
2. Clique no menu **Actions** (Ações).
3. Selecione uma das seguintes opções:
   - Para apagar todos os pontos de recuperação atualmente armazenados, clique em **Delete All** (Apagar todos).
   - Para apagar um conjunto de pontos de recuperação em um intervalo de dados específico, clique em **Delete Range** (Excluir intervalo). A caixa de diálogo **Delete** (Apagar) é exibida. Na caixa de diálogo **Delete Range** (Apagar faixa), especifique o intervalo de pontos de recuperação que você quer apagar, utilizando uma data e hora de início e uma data e hora de término e, em seguida, clique em **Delete** (Apagar).

Apagar uma cadeia de pontos de recuperação órfãos

Um ponto de recuperação órfão é um instantâneo incremental que não está associado a uma imagem básica. Os instantâneos subsequentes continuam se baseando nesse ponto de recuperação . Sem a imagem básica, os pontos de recuperação resultantes são incompletos e pouco prováveis de conter os dados necessários para concluir a recuperação. Esses pontos de recuperação são considerados parte da cadeia do ponto de recuperação órfão . Se isso acontecer, a melhor solução consiste em apagar a cadeia e criar uma nova imagem básica.

NOTA: A capacidade de apagar uma cadeia de recuperação órfã não está disponível para pontos de recuperação replicados em um núcleo de destino.

Para apagar uma cadeia de pontos de recuperação órfãos:

1. No Core Console, selecione a máquina protegida da qual você quer apagar a cadeia de pontos de recuperação órfãos.
2. Clique na guia **Recovery Points** (Pontos de recuperação).
3. Em **Recovery Points** (Pontos de recuperação), expanda o ponto de recuperação órfão.

Esse ponto de recuperação é identificado na coluna **Type** (Tipo), como **Incremental Orphaned** (Órfão incremental).

4. Ao lado **Actions** (Ações), clique em **Delete** (Apagar).

   A janela **Delete Recovery Points** (Apagar pontos de recuperação) aparece.

5. Na janela **Delete Recovery Points** (Apagar pontos de recuperação), clique em **Yes** (Sim).

   CUIDADO: O apagamento desse ponto de recuperação apaga toda a cadeia de pontos de recuperação, incluindo todos os pontos de recuperação incrementais que ocorrem antes ou depois desse, até a próxima imagem básica. Essa operação não pode ser desfeita.

   A cadeia de pontos de recuperação órfãos será apagada.

Forçar um instantâneo

Forçar um instantâneo permite que você force a transferência de dados para a máquina protegida atual. Quando você força um instantâneo, a transferência é iniciada imediatamente ou é adicionada à fila. Somente os dados que foram alterados de um ponto de recuperação anterior são transferidos. Se não houver nenhum ponto de recuperação anterior, todos os dados dos volumes protegidos são transferidos, o que é conhecido como imagem de base.

Para forçar um instantâneo:

1. No Core Console, clique na guia **Machines** (Máquinas) e, em seguida, na lista de máquinas protegidas, selecione a máquina ou cluster com o ponto de recuperação para a qual você quer forçar um instantâneo.
2. Clique no menu suspenso **Actions** (Ações) para essa máquina, clique em **Force Snapshot** (Forçar instantâneo) e, em seguida, selecione uma das opções descritas a seguir:
   - **Force Snapshot** (Forçar instantâneo) – Tira um instantâneo incremental dos dados atualizados desde que o último instantâneo foi tirado.
   - **Force Base Image** Forçar imagem de base – Tira um instantâneo completo de todos os dados dos volumes da máquina.
3. Quando a notificação for exibida na caixa de diálogo **Transfer Status** (Status da transferência) em que o instantâneo foi colocado na fila, clique em **OK**.

   Uma barra de andamento aparece próxima à máquina na guia **Machines** (Máquinas) e mostra o progresso do instantâneo.

Pausar e retomar a proteção

Quando você pausa uma proteção, interrompe temporariamente todas as transferências de dados da máquina atual.

Para pausar e retomar a proteção:

1. No Core Console, clique na guia **Machines** (Máquinas).
2. Selecione a máquina cuja proteção você quer pausar.

   A guia **Summary** (Resumo) dessa máquina é exibida.
3. No menu suspenso **Actions** (Ações) dessa máquina, clique em **Pause** (Pausar).
4. Para retomar a proteção, clique em **Resume** (Retomar) no menu **Actions** (Ações).

Restaurar dados

Você pode recuperar ou restaurar instantaneamente os dados para as suas máquinas físicas (para Windows ou Linux), ou para as máquinas virtuais Windows a partir dos pontos de recuperação armazenados para máquinas Windows. Os tópicos desta seção descrevem como exportar um ponto de recuperação específico de máquinas Windows para uma máquina virtual ou como reverter uma máquina para um ponto de recuperação prévio.

Se você configurou a replicação entre dois núcleos (origem e destino), pode apenas exportar os dados do núcleo de destino depois que a replicação inicial terminar. Para obter detalhes, consulte Replicar dados do agente em uma máquina.

NOTA: Os sistemas operacionais Windows 8 e Windows Server 2012 que são inicializados a partir de partições FAT32 EFI não estão disponíveis para proteção ou recuperação, nem os volumes do Sistema de arquivos resilientes (ReFS) .

Backup

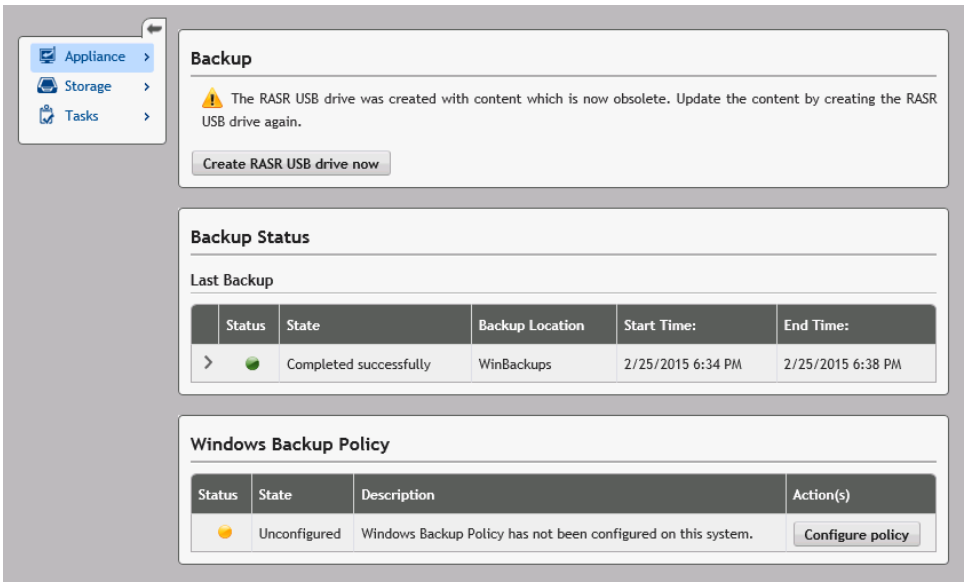
A guia Backup permite configurar a política de backup e recuperar o sistema através da chave USB RASR ou IDSDM. Para usar esse recurso, o disco virtual do Windows Backup precisa existir. Esse disco é criado durante o Assistente de configuração do**dispositivo AppAssure** . Para obter mais informações, consulte Autorrecuperação rápida do dispositivo no *Guia de Implementação do Dispositivo Dell DL43000* . Sem um disco virtual Windows Backup, não é possível configurar uma política ou criar backups do Windows.

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
   - Hora de início
   - Hora de término
   - Descrição do erro
   - Itens que foram incluídos no backup

   NOTA: As informações acima são mostradas independente de a Política de backup do Windows ser ou não executada.



Se um backup estiver em execução, as informações sobre o **Andamento atual do backup** e a **Hora de início** são mostradas.

Política de backup do Windows

Para configurar uma política de backup do Windows, execute o seguinte procedimento :

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:	• OS(C:) • RECUPERAÇÃO • Recuperação do zero • Estado do sistema Todos os itens acima são selecionados por padrão.
Selecione o horário para agendar o backup:	Digite o horário para agendar um backup.

4. Clique em **Configure** (Configurar).
   Uma vez configurado, você tem a opção de **Backup now** (Fazer backup agora), **Delete policy** (Apagar política) ou **View policy** (Ver política) na janela **Windows Backup Policy** (Política de backup do Windows).

Sobre exportar dados protegidos de máquinas Windows para máquinas virtuais

O AppAssure oferece suporte tanto para uma exportação única quanto para uma contínua (em suporte à espera virtual) de informações de backup do Windows para uma máquina virtual. Exportar os dados para uma máquina em espera virtual lhe proporciona uma cópia de alta disponibilidade dos dados. Se uma máquina protegida sair de operação, você pode inicializar a máquina virtual para depois realizar a recuperação.

O diagrama a seguir mostra uma implantação típica para exportar dados para uma máquina virtual.

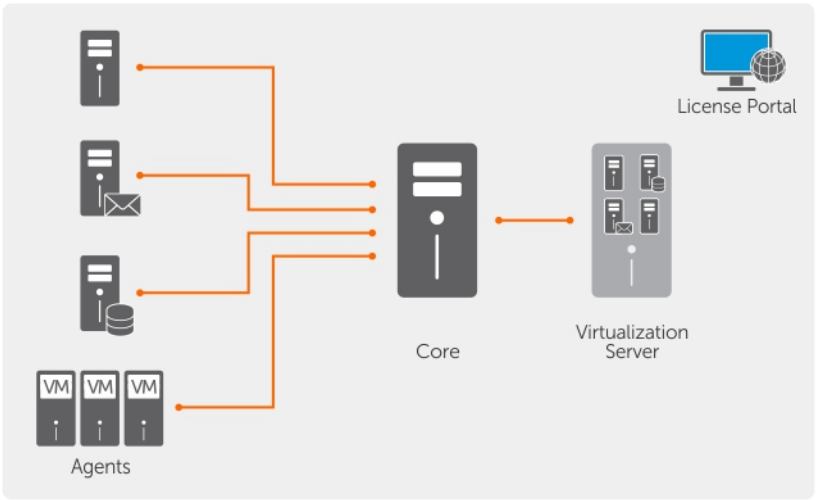


Figura 9. Exportar dados para uma máquina virtual

Você cria um espera virtual ao exportar continuamente dados protegidos de sua máquina Windows para uma máquina virtual. Ao exportar para uma máquina virtual, todos os dados de backup de um ponto de recuperação, além dos parâmetros definidos para o cronograma de exportação de sua máquina, serão exportados.

Você pode realizar a exportação virtual de pontos de recuperação de máquinas Linux ou Windows protegidas para VMware, ESXi, Hyper-V e Oracle VirtualBox.

NOTA: A guia Appliance (Dispositivo) mostra todas as máquinas virtuais, mas só oferece suporte para o gerenciamento de máquinas virtuais Hyper-V e ESXi. Para gerenciar as outras máquinas virtuais, use as ferramentas de gerenciamento do hipervisor.

NOTA: A máquina virtual para a qual você está exportando precisa ser uma versão licenciada do ESXi, estação de trabalho VMWare ou Hyper-V e não as versões grátis ou de período de testes.

Limitações do suporte para volumes dinâmicos e básicos

O AppAssure suporta a obtenção de instantâneos de todos os volumes dinâmicos e básicos. Além disso, o software também suporta a exportação de volumes dinâmicos simples que estejam em um único disco físico. Como o nome implica, volumes dinâmicos simples não são distribuídos, espelhados ou estendidos. Os volumes dinâmicos não simples têm geometrias de disco arbitrárias que não podem ser

totalmente interpretadas e, portanto, não podem ser exportadas. O AppAssure tem a capacidade de exportar volumes dinâmicos complexos ou não simples.

A versão do AppAssure 5.3.1.60393 adicionou uma caixa de seleção na interface do usuário, informando que as exportações estão restritas aos volumes dinâmicos simples. Antes da alteração da interface do usuário nessa versão, a opção de exportar discos dinâmicos complexos ou não simples parecia possível. Se você tentasse exportar esses discos, a tarefa de exportação falharia.

Exportar informações de backup sobre a máquina Windows para uma máquina virtual

No AppAssure você pode exportar dados de suas máquinas Microsoft Windows para uma máquina virtual (VMware, ESXi, Hyper-V e Oracle VirtualBox), exportando todas as informações de backup de um ponto de recuperação, bem como os parâmetros definidos para o agendamento da proteção para a sua máquina.

Para exportar as informações de backup do Windows para uma máquina virtual:

1. No Core Console, clique na guia **Machines** (Máquinas).
2. Na lista de máquinas protegidas, selecione a máquina ou cluster com o ponto de recuperação para o qual você quer exportar.
3. No menu suspenso **Actions** (Ações) referente a essa máquina, clique em **Export** (Exportar) e selecione o tipo de exportação que você quer realizar. Você pode escolher uma das seguintes opções:
   - Exportação do ESXi
   - Exportação da Estação de trabalho VMware
   - Exportação do Hyper-V
   - Exportação do Oracle VirtualBox

   A caixa de diálogo **Select Export Type** (Selecionar tipo de exportação) é mostrada.

Exportar dados do Windows usando a exportação ESXi

No AppAssure, você pode optar por exportar dados usando a exportação ESXi executando uma exportação contínua ou única.

Realizar uma exportação ESXi única

Para realizar uma exportação ESXi única:

1. Na caixa de diálogo **Select Export Type** (Selecionar tipo de exportação), clique em **One-time export** (Exportação a ser executada uma única vez).
2. Clique em **Next** (Avançar).

   A caixa de diálogo **ESXi Export - Select Recovery Point** (Exportação ESXi - Selecionar ponto de recuperação) aparece.
3. Selecione um ponto de recuperação para exportar e, em seguida, clique em **Next** (Avançar).

   A caixa de diálogo **Virtual Standby Recovery Point to VMware vCenter Server/ESXi** (Ponto de recuperação de espera virtual para o VMware vCenter Server/ESXi) aparece.

Definir informações de máquina virtual para realizar uma exportação ESXi

Para definir informações de máquina virtual para realizar uma exportação ESXi:

1. Na caixa de diálogo **Virtual Standby Recovery Point to VMware vCenter Server/ESXi** (Ponto de recuperação de espera virtual para o VMware vCenter Server/ESXi), digite os parâmetros para acessar a máquina virtual, descritos da seguinte forma:

Caixa de texto	Descrição
Host Name (Nome de host)	Digite um nome para a máquina do host.
Port (Porta)	Digite a porta da máquina host. A porta padrão é 443.
User Name (Nome de usuário)	Digite as credenciais de login da máquina do host.
Password (Senha)	Digite as credenciais de login da máquina do host.

2. Clique em **Connect** (Conectar).

Realizar uma exportação ESXi contínua (espera virtual)

Para executar uma exportação ESXi contínua (espera virtual):

1. Na caixa de diálogo **Select Export Type** (Selecionar tipo de exportação), clique em **Continuous (Virtual Standby)** (Contínua [espera virtual]).
2. Clique em **Next** (Avançar).

   A caixa de diálogo **Virtual Standby Recovery Point to VMware vCenter Server/ESXi** (Ponto de recuperação de espera virtual para o VMware vCenter Server/ESXi) aparece.
3. Digite os parâmetros para acessar a máquina virtual, conforme descrito abaixo.

Caixa de texto	Descrição
Host Name (Nome de host)	Digite um nome para a máquina do host.
Port (Porta)	Digite a porta da máquina host. A porta padrão é 443.
User Name (Nome de usuário)	Digite as credenciais de login da máquina do host.
Password (Senha)	Digite as credenciais de login da máquina do host.

4. Clique em Connect (Conectar).
5. Na guia **Options** (Opções), digite as informações da máquina virtual conforme descrito.

Caixa de texto	Descrição
Virtual Machine Name (Nome da máquina virtual)	Digite um nome para a máquina virtual que está sendo criada. Por exemplo, VM-0A1B2C3D4 NOTA: É recomendável usar um nome que seja derivado do nome do agente ou que corresponda ao nome do agente. Você também pode criar um nome derivado do tipo hipervisor, um endereço IP ou nome DNS.

Caixa de texto	Descrição
Memória	Especifique o uso de memória. Você pode escolher uma das seguintes opções: • Usar a mesma quantidade de memória RAM que a máquina de origem • Clique em **Use a specific amount of RAM** (Usar uma quantidade específica de memória RAM) para especificar quanta memória RAM será usada. Por exemplo, 4096 megabytes (MB). A quantidade mínima permitida é 512 MB e a quantidade máxima é determinada pela capacidade e pelas limitações da máquina de host (recomendado).
Datacenter ESXi	Digite um nome para o datacenter ESXi.
Host ESXi	Digite as credenciais do host ESXi.
Data Store (Armazenamento de dados)	Digite os detalhes do armazenamento de dados.
Version (Versão)	Selecione a versão da máquina virtual. NOTA: Para usar o vSphere Client para gerenciar máquinas virtuais, selecione a versão 8 ou anterior.
Resource Pool (Pool de recursos)	Digite um nome para o pool de recursos.

6. Clique em **Start Export** (Iniciar exportação).

Exportar dados do Windows usando a exportação de estação de trabalho VMware

No AppAssure, você pode optar por exportar dados usando a exportação de estação de trabalho VMware ao realizar uma exportação única ou contínua. Realize as etapas nos procedimentos a seguir para exportar usando a exportação de estação de trabalho VMware para o tipo de exportação apropriado.

Realizar uma exportação de estação de trabalho VMware única

Para realizar uma exportação de estação de trabalho VMware única:

1. Na caixa de diálogo **Select Export Type** (Selecionar tipo de exportação), clique em **One-time export** (Exportação a ser executada uma única vez).
2. Clique em **Next** (Avançar).

   A caixa de diálogo **VM Export - Select Recovery Point** (Exportação de MV – Selecionar ponto de recuperação) é exibida.
3. Selecione um ponto de recuperação para exportar e, em seguida, clique em **Next** (Avançar).

   A caixa de diálogo **Virtual Standby Recovery Point to VMware Workstation/Server** (Ponto de recuperação de espera virtual para estação de trabalho/servidor VMware) é exibida.

Definir as configurações uma única vez para realizar uma exportação de estação de trabalho VMware

Para definir as configurações únicas para realizar uma exportação de estação de trabalho VMware:

1. Na caixa de diálogo **Virtual Standby Recovery Point to VMware Workstation/Server** (Ponto de recuperação de espera virtual para a estação de trabalho/servidor VMware), digite os parâmetros para acessar a máquina virtual descritos a seguir:

Caixa de texto	Descrição
Target Path (Caminho de destino)	Especifique o caminho da pasta local ou do compartilhamento de rede no qual você deseja criar a máquina virtual. NOTA: Se você especificou um caminho de compartilhamento de rede, insira credenciais de login válidas para uma conta registrada no computador de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.
User Name (Nome de usuário)	Digite as credenciais de login da máquina virtual. • Se você especificou um caminho de compartilhamento de rede, você precisa digitar um nome de usuário válido para a conta que está registrada na máquina de destino. • Se você digitou um caminho local, não é necessário informar um nome de usuário.
Password (Senha)	Digite as credenciais de login da máquina virtual. • Se você especificou um caminho de compartilhamento de rede, você precisa digitar uma senha válida da conta que está registrada na máquina de destino. • Se você digitou um caminho local, não é necessário informar uma senha.

2. No painel **Export Volumes** (Exportar volumes), selecione os volumes para exportar. Por exemplo, **C:** e **D:**.
3. No painel Options (Opções), insira as informações da máquina virtual e da utilização da memória, conforme descrito a seguir:

Caixa de texto	Descrição
Virtual Machine (Máquina virtual)	Digite um nome para a máquina virtual que está sendo criada. Por exemplo, VM-0A1B2C3D4. NOTA: É recomendável usar um nome que seja derivado do nome do agente ou que corresponda ao nome do agente. Você também pode criar um nome derivado do tipo hipervisor, um endereço IP ou nome DNS.
Memória	Especifique a memória para a máquina virtual. • Clique em **Use the same amount of RAM as the source machine** (Usar a mesma quantidade de memória RAM que a máquina de origem) para especificar que a configuração de memória RAM é a mesma da máquina virtual de origem. • Clique em **Use a specific amount of RAM** (Usar uma quantidade específica de memória RAM) para especificar a quantidade de memória RAM para usar; por exemplo, 4096 MB. A quantidade mínima permitida é 512 MB e a

Caixa de texto	Descrição
	máxima é determinada pela capacidade e pelas limitações da máquina host. (recomendado)

4. Clique em **Export** (Exportar).

Realizar uma exportação de estação de trabalho VMware contínua (espera virtual)

Para realizar uma exportação de estação de trabalho VMware contínua (espera virtual):

1. Na caixa de diálogo **Select Export Type** (Selecionar tipo de exportação), clique em **Continuous (Virtual Standby)** (Contínua [espera virtual]) e clique em **Next** (Avançar).

   A caixa de diálogo **VM Export - Select Recovery Point** (Exportação de MV – Selecionar ponto de recuperação) é exibida.
2. Selecione um ponto de recuperação para exportar e, em seguida, clique em **Next** (Avançar).

   A caixa de diálogo **Virtual Standby Recovery Point to VMware Workstation/Server** (Ponto de recuperação de espera virtual para estação de trabalho/servidor VMware) é exibida.
3. Digite os parâmetros para acessar a máquina virtual descritos da seguinte maneira:

Caixa de texto	Descrição
Target Path (Caminho de destino)	Especifique o caminho da pasta local ou do compartilhamento de rede no qual você deseja criar a máquina virtual. **NOTA:** Se você especificou um caminho de compartilhamento de rede, insira credenciais de login válidas para uma conta registrada no computador de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.
User Name (Nome de usuário)	Digite as credenciais de login da máquina virtual. • Se você especificou um caminho de compartilhamento de rede, você precisa digitar um nome de usuário válido para a conta que está registrada na máquina de destino. • Se você digitou um caminho local, não é necessário informar um nome de usuário.
Password (Senha)	Digite as credenciais de login da máquina virtual. • Se você especificou um caminho de compartilhamento de rede, você precisa digitar uma senha válida da conta que está registrada na máquina de destino. • Se você digitou um caminho local, não é necessário informar uma senha.

4. No painel **Export Volumes** (Exportar volumes), selecione os volumes para exportar. Por exemplo, **C:** e **D:**.
5. No painel **Options** (Opções), digite as informações da máquina virtual e da utilização da memória, conforme descrito na tabela a seguir.

Caixa de texto	Descrição
Virtual Machine (Máquina virtual)	Digite um nome para a máquina virtual que está sendo criada. Por exemplo, `VM-0A1B2C3D4`.

Caixa de texto	Descrição
	NOTA: É recomendável usar um nome que seja derivado do nome do agente ou que corresponda ao nome do agente. Você também pode criar um nome derivado do tipo hipervisor, um endereço IP ou nome DNS.
Memória	Especifique a memória para a máquina virtual. • Clique em **Use the same amount of RAM as the source machine** (Usar a mesma quantidade de memória RAM que a máquina de origem) para especificar que a configuração de memória RAM é a mesma da máquina virtual de origem. • Clique em **Use a specific amount of RAM** (Usar uma quantidade específica de memória RAM) para especificar a quantidade de memória RAM para usar; como, por exemplo, 4096 MB. A quantidade mínima permitida é 512 MB e a máxima é determinada pela capacidade e pelas limitações da máquina host. (recomendado)

6. Clique em **Perform initial ad-hoc export** (Realizar exportação ad-hoc inicial) para testar a exportação dos dados.
7. Clique em **Save** (Salvar).

Exportar dados do Windows usando a exportação do Hyper-V

Você pode optar por exportar dados usando a exportação Hyper-V, com uma exportação de uma única vez ou contínua. Execute os procedimentos a seguir para exportar usando a exportação Hyper-V para o tipo apropriado de exportação.
O dispositivo DL suporta a primeira geração da exportação Hyper-V para os hosts a seguir:

- Windows 8
- Windows 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

O dispositivo DL suporta a segunda geração da exportação Hyper-V para os hosts a seguir:

- Windows 8.1
- Windows Server 2012 R2

NOTA: Nem todas as máquinas protegidas podem ser exportadas para os hosts de segunda geração do Hyper-V.

Apenas as máquinas protegidas com os seguintes sistemas operacionais Unified Extensible Firmware Interface (UEFI) suportam a exportação virtual para hosts Hyper-V de segunda geração:

- Windows 8 (UEFI)
- Windows 8.1 (UEFI)
- Windows Server 2012 (UEFI)
- Windows Server 2012R2 (UEFI)

NOTA: A exportação Hyper-V para a VM de segunda geração pode falhar se o host Hyper-V não tiver RAM suficiente alocada para realizar a exportação.

Conclua as etapas nos procedimentos a seguir para o tipo apropriado de exportação.

Realizar uma exportação do Hyper-V única

Para realizar uma exportação do Hyper-V única:

1. No Core Console, navegue até a máquina que você deseja exportar.
2. Na guia Summary (Resumo), clique em **Actions (Ações)** → **Export** → **One-time (Exportação única)**.

   O assistente **Export** (Exportar) é mostrado na página **Protected Machines** (Máquinas protegidas).
3. Selecione uma máquina para exportação e, em seguida, clique em **Next** (Avançar).
4. Na página **Recovery Points** (Pontos de recuperação), selecione o ponto de recuperação que você deseja exportar e depois clique em **Next** (Avançar).

Definir as configurações únicas para realizar uma exportação do Hyper-V

Para definir as configurações únicas para realizar uma exportação do Hyper-V:

1. Na caixa de diálogo do Hyper-V, clique em **Use local machine** (Usar máquina local) para realizar a exportação em Hyper-V para uma máquina local com a função de Hyper-V atribuída.
2. Clique na opção **Remote host** (Host remoto) para indicar que o servidor Hyper-V está situado em uma máquina remota. Se você selecionou a opção Host remoto, digite os parâmetros para o host remoto conforme descrito a seguir:

Caixa de texto	Descrição
Host Name (Nome do host)	Digite um endereço IP ou nome de host para o servidor Hyper-V. Ele representa o endereço IP ou nome de host do servidor Hyper-V remoto.
Port (Porta)	Digite um número de porta para a máquina. Ele representa a porta através da qual o núcleo se comunica com essa máquina.
User Name (Nome de usuário)	Digite o nome de usuário do usuário com privilégios administrativos para a estação de trabalho com o servidor Hyper-V. Ele é usado para especificar as credenciais de login da máquina virtual.
Password (Senha)	Digite a senha do usuário com privilégios administrativos na estação de trabalho com o servidor Hyper-V. Ela é usada para especificar as credenciais de login da máquina virtual.

3. Clique em **Next** (Avançar).
4. Na página **Virtual Machines Options** (Opções de máquinas virtuais), digite o caminho ou o local da máquina virtual na caixa de texto **VM Machine Location** (Local da máquina virtual). Por exemplo, **D:\export**. O local da máquina virtual precisa ter espaço suficiente para armazenar os metadados da MV e as unidades virtuais necessárias para a máquina virtual.
5. Digite um nome para a máquina virtual na caixa de texto **Virtual Machine Name** (Nome da máquina virtual).

   O nome que você digitar será mostrado na lista de máquinas virtuais do console do gerenciador do Hyper-V.
6. Clique em uma das seguintes opções:
   - **Use the same amount of RAM as the source machine** (Usar a mesma quantidade de memória RAM que a máquina de origem) - para identificar que o uso da memória RAM é idêntico entre máquinas virtuais e de origem.
   - **Use a specific amount of RAM** (Usar uma quantidade de memória RAM específica) - para especificar quanta memória a máquina virtual tem após a exportação; por exemplo, 4096 MB (recomendado).

7. Para especificar o formato de disco, ao lado de **Disk Format** (Formato do disco), clique em uma das seguintes opções:
   - **VHDX**
   - **VHD (Disco rígido virtual)**

   NOTA: A exportação do Hyper-V Export oferece suporte para formatos de disco em VHDX se a máquina de destino estiver executando o Windows 8 (Windows Server 2012) ou mais recente. Se o VHDX não for compatível com o seu ambiente, a opção está desativada.
8. Na página **Volumes**, selecione os volumes a serem exportados. Para que a máquina virtual seja um backup efetivo da máquina protegida, inclua a unidade de inicialização da máquina protegida. Por exemplo, C:\.

   Seus volumes selecionados não devem ser superiores a 2040 GB para o VHD. Se os volumes selecionados forem superiores a 2040 GB e o formato VHD for selecionado, será indicado um erro.
9. Na página **Summary** (Resumo), clique em **Finish** (Concluir) para concluir o assistente e iniciar a exportação.

Executar uma exportação contínua para Hyper-V (espera virtual)

NOTA: Apenas a configuração de 3 TB com 2 MVs do DL1000 oferece suporte para os recursos de exportação única e de exportação contínua (espera virtual).

Para executar uma exportação contínua para Hyper-V (espera virtual):

1. Na guia **Virtual Standby** (Espera virtual) do Core Console, clique em **Add** (Adicionar) para abrir o **Assistente de exportação**. Na página **Protected Machines** (Máquinas protegidas) do **Assistente de exportação**,
2. selecione a máquina que você quer exportar e clique em **Next** (Avançar).
3. Na guia **Summary** (Resumo), clique em **Export (Exportar) → Virtual Standby (Espera virtual)**.
4. Na caixa de diálogo Hyper-V, clique em **Use local machine** (Usar máquina local) para executar a exportação para Hyper-V para uma máquina local com a função Hyper-V atribuída.
5. Clique na opção **Remote host** (Host remoto) para indicar que o servidor Hyper-V está localizado em uma máquina remota. Se você selecionou a opção Remote host (Host remoto), digite os parâmetros do host remoto, conforme descrito a seguir:

Caixa de texto	Descrição
Host Name (Nome de host)	Digite um endereço IP ou um nome de host para o servidor Hyper-V. Ele representa o endereço IP ou o nome de host do servidor Hyper-V remoto.
Porta	Digite um número de porta para a máquina. Ele representa a porta através da qual o Núcleo se comunica com esta máquina.
Nome de Usuário	Digite o nome de usuário para o usuário com privilégios administrativos na estação de trabalho com o servidor Hyper-V. Ele é usado para especificar as credenciais de login da máquina virtual.
Senha	Digite a senha da conta de usuário com privilégios administrativos na estação de trabalho com o servidor Hyper-V. Ela é usada para especificar as credenciais de login da máquina virtual.

6. Na caixa de texto **VM Machine Location** (Local da máquina virtual) da página **Virtual Machines Options** (Opções de máquinas virtuais), digite o caminho ou o local da máquina virtual. Por exemplo, D:\export. O local da MV precisa ter espaço suficiente para guardar os metadados da MV e as unidades virtuais necessárias para a máquina virtual.
7. Digite um nome para a máquina virtual na caixa de texto **Virtual Machine Name** (Nome da máquina virtual).

O nome que você digitar será mostrado na lista de máquinas virtuais do console do Gerenciador do Hyper-V.

8. Clique em uma das opções a seguir:
   - **Use the same amount of RAM** (Usar a mesma quantidade de RAM) que a máquina de origem para identificar que o uso de RAM é idêntico na máquina virtual e na máquina de origem.
   - **Use a specific amount of RAM** (Usar uma quantidade específica de RAM) para especificar a quantidade de memória que a máquina virtual deve ter após a exportação; por exemplo, 4.096 MB (recomendado).
9. Para especificar a Geração, clique em uma das opções a seguir:
   - Generation 1 (Geração 1) (recomendada)
   - Generation 2 (Geração 2)
10. Para especificar o formato do disco, clique em uma das seguintes opções ao lado de **Disk Format** (Formado do disco):
    - **VHDX** (Padrão)
    - **VHD**

    NOTA: A exportação para Hyper-V suporta os formatos de disco VHDX apenas se a máquina de destino estiver rodando o Windows 8 (Windows Server 2012) ou posterior. Se o VHDX não for suportado em seu ambiente, a opção estará desabilitada. Na página Network Adapters (Adaptadores de rede), selecione o adaptador virtual que será conectado a um comutador.
11. Na página **Volumes**, selecione os volumes que você quer exportar. Para que a máquina virtual seja um backup efetivo da máquina protegida, adicione a unidade de inicialização da máquina protegida. Por exemplo, C:\.

    Os volumes selecionados não devem ser maiores do que 2.040 GB para VHD. Se os volumes selecionados forem maiores que 2.040 GB e o formato VHD estiver selecionado, você receberá uma mensagem de erro.
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 andamento da exportação na guia **Virtual Standby** (Espera virtual) ou **Events** (Eventos)

Exportar dados do Microsoft Windows usando a exportação do Oracle VirtualBox

No AppAssure, você pode optar por exportar os dados usando uma exportação do Oracle VirtualBox, realizando uma exportação executada uma única vez ou criando uma exportação contínua (para a espera virtual).

Conclua as etapas nos procedimentos a seguir para o tipo apropriado de exportação.

NOTA: Para executar este tipo de exportação, que você já deve ter o Oracle VirtualBox instalado na máquina do núcleo. Há suporte para o VirtualBox versão 4.2.18 ou superior em hosts Windows.

Realizar uma exportação Oracle VirtualBox a ser executada uma única vez

Execute as etapas descritas neste procedimento para realizar uma exportação Oracle VirtualBox a ser executada uma única vez.

Para realizar uma exportação Oracle VirtualBox a ser executada uma única vez:

1. No AppAssure Core Console, escolha uma das opções a seguir:
   - A partir da barra de botões, clique em **Export** (Exportar) para abrir o assistente de exportação e faça o seguinte:

1. Na caixa de diálogo **Select Export Type** (Selecionar tipo de exportação),clique em **One-time export** (Exportação a ser executada uma única vez) e, em seguida, clique em **Next** (Avançar).
2. Na página **Protected Machines** (Máquinas protegidas), selecione a máquina protegida que você quer exportar para uma máquina virtual e, em seguida, clique em **Next** (Avançar).

- Navegue até a máquina que você quer exportar e, em seguida, na guia **Summary** (Resumo) do menu suspenso **Actions** (Ações) referente a essa máquina, selecione **Export (Exportar)** > **One-time (Uma única vez)**.

O assistente de exportação é exibido na página **Recovery Points** (Pontos de recuperação).

2. Na página **Recovery Points** (Pontos de recuperação), selecione o ponto de recuperação do AppAssure Core que você quer exportar e, em seguida, clique em **Next** (Avançar).
3. Na página **Destination** (Destino) no Assistente de exportação, no menu suspenso **Recover to Virtual machine** (Recuperar para máquina virtual), selecione **VirtualBox** e, em seguida, clique em **Next** (Avançar).
4. Na página**Virtual Machine Options** (Opções da máquina virtual), selecione **Usar máquina Windows**.
5. Digite os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir.

Opção	Descrição
Virtual Machine Name (Nome da máquina virtual)	Digite um nome para a máquina virtual que está sendo criada. NOTA: O nome padrão é o nome da máquina de origem.
Target Path (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 especificar um caminho de compartilhamento de rede, precisará digitar credenciais de login válidas (nome de usuário e senha) para uma conta registrada no computador de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.
Memory (Memória)	Especifique o uso da memória para a máquina virtual, clicando em uma das seguintes opções : • Clique em **Use the same amount of RAM as the source machine** (Usar a mesma quantidade de RAM que na máquina de origem) para especificar que a configuração da RAM é a mesma que na máquina de origem. • Clique em **Use a specific amount of RAM** (Usar uma quantidade específica de memória RAM) para especificar a quantidade de memória RAM para usar; por exemplo, 4096 MB. A quantidade mínima permitida é 512 MB e a máxima é determinada pela capacidade e pelas limitações da máquina host. (recomendado)

6. Para especificar uma conta de usuário para a máquina virtual, selecione **Specify the user account for the exported virtual machine** (Especificar a conta de usuário exportada para a máquina virtual) e, em seguida, insira as informações a seguir. Isso refere-se a uma conta de usuário específica para a qual a máquina virtual será registrada, caso haja múltiplas contas de usuário na máquina virtual. Quando o login for efetuado na conta do usuário, apenas 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 Windows com VirtualBox.
   - **User name** (Nome de usuário) – Digite o nome do usuário para o qual a máquina virtual está registrada.

- **Password** (Senha) – Digite a senha dessa conta de usuário.

7. Clique em **Next** (Avançar).

   O nome que você digitar será mostrado na lista de máquinas virtuais do console Hyper-V Manager.

8. Na página Volumes, selecione o(s) volume(s) para exportar. Para que a máquina virtual seja um backup eficaz da máquina protegida, inclua a unidade de inicialização da máquina protegida. Por exemplo, C:\.
9. Na página **Summary** (Resumo), clique em **Finish** (Concluir) para concluir o assistente e iniciar a exportação.

   NOTA: Você pode monitorar o status e o andamento da exportação visualizando a guia **Virtual Standby** (Espera virtual) ou **Events** (Eventos).

Realizar uma exportação contínua Oracle VirtualBox (espera virtual)

Execute o procedimento descrito para criar uma Espera virtual e realizar uma exportação contínua para o Oracle VirtualBox.

Para realizar uma exportação contínua para o Oracle VirtualBox (espera virtual)

1. No AppAssure Core Console, escolha uma das opções a seguir:
   - Na guia **Virtual Standby** (Espera virtual), clique em **Add** (Adicionar) para abrir o Assistente de exportação. Na página **Protected Machines** (Máquinas protegidas) do Assistente de exportação, selecione a máquina protegida que você quer exportar e, em seguida, clique em **Next** (Avançar).
   - Navegue até a máquina que você quer exportar, e, na guia **Summary** (Resumo) do menu suspenso **Actions** (Ações) referente a essa máquina, clique em **Export (Exportar)** > **Virtual Standby (Espera virtual)**.
2. Na página **Destination** (Destino) no Assistente de exportação, no menu suspenso **Recover to Virtual machine** (Recuperar para máquina virtual), selecione **VirtualBox** e, em seguida, clique em **Next** (Avançar).
3. Na página**Virtual Machine Options** (Opções da máquina virtual), selecione **Use Windows machine** (Usar máquina Windows).
4. Digite os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir.

Opção	Descrição
Nome da máquina virtual	Digite um nome para a máquina virtual que está sendo criada. NOTA: É recomendável usar um nome que seja derivado do nome do agente ou que corresponda ao nome do agente. Você também pode criar um nome derivado do tipo de hipervisor, um endereço IP ou nome DNS.
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 especificar um caminho de compartilhamento de rede, precisará digitar credenciais válidas de login (nome de usuário e senha) para uma conta registrada no computador de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.
Memória	Especifique o uso da memória para a máquina virtual, clicando em uma das seguintes opções :

Opção	Descrição
	• Clique em **Use the same amount of RAM** (Usar a mesma quantidade de RAM) que na máquina de origem para identificar se o uso da RAM é idêntico entre as máquinas virtual e de origem. • Clique em **Use a specific amount of RAM** (Usar uma quantidade específica de RAM) para especificar a quantidade de memória RAM para usar; por exemplo, 4096 MB. A quantidade mínima permitida é 512 MB e a máxima é determinada pela capacidade e pelas limitações da máquina host. (recomendado)

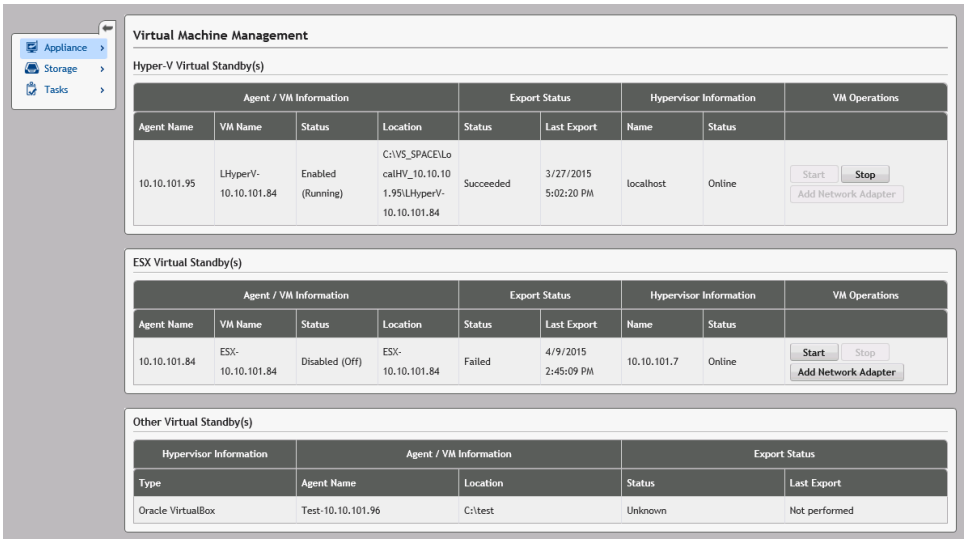
5. Para especificar uma conta de usuário para a máquina virtual, selecione **Specify the user account for the exported virtual machine** (Especificar a conta de usuário exportada para a máquina virtual) e, em seguida, insira as informações a seguir. Isso refere-se a uma conta de usuário específica para a qual a máquina virtual será registrada, caso haja múltiplas contas de usuário na máquina virtual. Quando o login for efetuado na conta do usuário, apenas 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 Windows com VirtualBox.
   - **User name** (Nome de usuário) - Digite o nome do usuário para o qual a máquina virtual está registrada.
   - **Password** (Senha) - Digite a senha dessa conta de usuário.
6. Selecione **Perform initial one-time export** (Realizar exportação a ser executada uma única vez) para realizar a exportação virtual imediatamente, e não depois do próximo instantâneo agendado.
7. Na página Volumes, selecione o(s) volume(s) para exportar. Para que a máquina virtual seja um backup eficaz da máquina protegida, inclua a unidade de inicialização da máquina protegida. Por exemplo, C:\.
8. Na página **Summary** (Resumo), clique em **Finish** (Concluir) para concluir o assistente e iniciar a exportação.

   NOTA: Você pode monitorar o status e o andamento da exportação visualizando a guia **Virtual Standby** (Espera virtual) ou **Events** (Eventos).

Gerenciamento de máquina virtual

A guia **VM Management (Gerenciamento de MV)** mostra o status das máquinas protegidas. Você pode iniciar, parar e adicionar adaptadores de rede (aplicável somente para máquinas virtuais Hyper-V e ESXi). Para navegar até a guia VM Management (Gerenciamento de MV), clique em **Appliance (Dispositivo)** → **VM Management (Gerenciamento de MV)**.

NOTA: Os botões Start (Iniciar), Stop (Parar) e Add (Adicionar) adaptador de rede podem demorar até 30 segundos para aparecer cada vez que a guia **Appliance (Dispositivo)** → **VM Management (Gerenciamento de MV)** é selecionada.



Gerenciamento de MV para espera(s) virtual(is) do Hyper-V e ESXi

Campo	Descrição
Informações do agente/MV	**Agent Name** (Nome do agente): indica o nome da máquina protegida para a qual você criou a espera virtual. **VM Name** (Nome da MV): indica o nome da MV. **NOTA:** É recomendável usar um nome que seja derivado do nome do agente ou que corresponda ao nome do agente. Você também pode criar um nome derivado do tipo hipervisor, um endereço IP ou nome DNS. **Status**: indica o status da máquina virtual. Os valores possíveis são: • Executando • Parado • Iniciando • Suspenso • Parando • Desconhecido (status temporário) **NOTA:** Os valores de status acima dependem do tipo de hipervisor. Nem todos os hipervisores mostram todos os valores de status. **Location** (Local): indica o local da MV. Por exemplo, D:\export. O local da MV precisa ter espaço suficiente para acomodar os metadados da MV e as unidades virtuais necessárias para a máquina virtual.
Status da exportação	**Status** 1. Indica os seguintes status de um processo de exportação: • Concluído • Falha • Em andamento

Campo	Descrição
	• Não realizado 2. Se uma exportação estiver em andamento, a porcentagem da exportação é mostrada. **Last Export** (Última exportação): indica a hora da última exportação.
Informações do hipervisor	**Name** (Nome): indica o nome do hipervisor no qual a MV é criada. **Status**: indica o status da conexão com os hipervisores Hyper-V e ESXi. • On-line • Off-line • Desconhecido (status temporário) NOTA: O status é mostrado apenas para os hipervisores Hyper-V e ESXi.
Operações da MV	Permite iniciar ou parar a máquina virtual e adicionar um adaptador de rede.

Gerenciamento de MV para outra(s) espera(s) virtual(is)

Campo	Descrição
Informações do hipervisor	**Type** (Tipo): indica o tipo de hipervisor.
Informações do agente/MV	**Agent Name** (Nome do agente): indica o nome da máquina protegida para a qual você criou a espera virtual. **Location** (Local): indica o local da MV. Por exemplo, D:\export. O local da MV precisa ter espaço suficiente para acomodar os metadados da MV e as unidades virtuais necessárias para a máquina virtual.
Status da exportação	**Status** 1. Indica os seguintes status de um processo de exportação: • Concluído • Falha • Em andamento • Não realizado 2. Se uma exportação estiver em andamento, a porcentagem da exportação é mostrada como uma barra de progresso. **Last Export** (Última exportação): indica a hora da última exportação.

Criar um adaptador de rede virtual

As máquinas virtuais precisam ter um ou mais Adaptadores de redes virtuais (VNAs) para a conexão à Internet. Uma MV precisa de um VNA para cada adaptador de rede real (RNA) na máquina protegida. O VNA e seu correspondente RNA precisam ter uma configuração similar. Você pode adicionar VNAs à sua MV ao criar a Espera virtual ou pode adicionar os VNAs posteriormente.

Ao criar uma espera virtual, haverá uma adaptador sugerido para cada adaptador na máquina protegida, quando você configura uma máquina virtual. Você pode adicionar ou remover todos ou alguns desses

adaptadores sugeridos. O número máximo de VNAs por MV depende do tipo de hipervisor. Para o Hyper-V você pode adicionar até 8 adaptadores para cada máquina virtual.

Para criar um adaptador de rede virtual:

1. Navegue até a página **VM Management** (Gerenciamento de MV).
2. Clique no botão **Add Network Adapter** (Adicionar adaptador de rede) associado à MV para adicionar um VNA.

   NOTA: Não adicione adaptadores a uma MV para uma Espera virtual que ainda esteja executado backups ou exportação das máquinas protegidas. Os VNAs adicionais podem causar falhas nas futuras operações de exportação.

   NOTA: É recomendável adicionar VNAs logo antes de iniciar a MV para a substituição da máquina protegida. Confirme se você parou ou interrompeu qualquer exportação pendente para a MV na guia da espera virtual.

   A janela **Virtual Network Adapters and Switches** (Adaptadores e comutadores de redes virtuais) aparece.
3. Clique em **Create** (Criar) para criar um adaptador de rede virtual .

   A janela **Create Virtual Network Adapter** (Criar adaptador de rede virtual) aparece.
4. Escolha um comutador virtual no menu suspenso.

   NOTA: Durante a seleção de comutadores virtuais para ESXi, a lista mostra apenas os comutadores com "MV" ou "Máquina virtual" em seus nomes. Selecione apenas um comutador do tipo **Virtual Machine Port Group** (Grupo de portas de máquina virtual); verifique o tipo do comutador no GUI do hipervisor do ESXi.
5. Clique em **Create** (Criar).

   NOTA: Para remover um adaptador de rede virtual, use o hipervisor da interface de gerenciamento.

Iniciar uma operação de MV

Para iniciar uma operação de MV:

1. Navegue até a janela **VM Management** (Gerenciamento de MV).
2. Clique no botão **Start** (Iniciar) associado à MV, para iniciar.

   NOTA: A GUI pode sofrer um atraso ao mostrar o status correto da máquina. O botão Start (Iniciar) pode permanecer desativado até 30 segundos após ter sido usado. Ele é ativado somente se a máquina virtual puder ser iniciada.

   NOTA: Não clique no botão Start (Iniciar) se uma tarefa de exportação da máquina virtual estiver em andamento ou provavelmente iniciará em breve. Verifique o agendamento da próxima tarefa de exportação, vendo as guias **Protected Machines** (Máquinas protegidas) e **Virtual Standby** (Espera virtual). Se uma tarefa de exportação estiver agendada para o futuro próximo, cancele ou pule a exportação ou aguarde a tarefa terminar antes de iniciar a máquina virtual . A exportação de dados falhará se for iniciada com a máquina virtual em execução, embora você possa iniciar uma máquina virtual quando uma tarefa de exportação estiver em execução.

NOTA: É recomendável não iniciar uma MV mantida como uma Espera virtual. As MVs de Espera virtual devem estar ativas ou ser iniciadas como substituição de uma máquina protegida que falhou. Se a máquina protegida ainda estiver ativa, primeiro pare ou interrompa qualquer exportação pendente para a MV na guia Virtual Standby (Espera virtual) , antes de iniciar a máquina virtual.

Parar uma operação de MV

Para interromper uma operação de MV:

1. Navegue até a janela **VM Management** (Gerenciamento de MV).
2. Clique no botão **Stop** (Parar) associado à MV para parar.

NOTA: O botão Stop (Parar) é ativado apenas se a máquina virtual estiver sendo executada atualmente e estiver disponível dentro de uma atualização de 30 segundos (aproximadamente) após iniciar a MV.

NOTA: O botão Start (Iniciar) é ativado dentro de 30 segundos (aproximadamente) após parar a máquina virtual.

NOTA: Depois que a MV protegida for restaurada, remova a MV do hipervisor e sua correspondente espera virtual. Recrie a espera virtual para a máquina protegida restaurada. Isso garante que a MV espera virtual espelhe precisamente a máquina protegida.

Executar uma reversão

No AppAssure, uma reversão é o processo de restauração dos volumes em uma máquina, a partir dos pontos de recuperação.

NOTA: A funcionalidade de reversão também é suportada para máquinas Linux protegidas, usando o utilitário de linha de comando `aamount`. Para obter mais informações, consulte Realizar uma reversão para uma máquina Linux usando a linha de comando.

Para realizar uma reversão:

1. No Core Console, faça uma das seguintes ações:
   - Clique na guia **Machines** (Máquinas) e, em seguida, faça o seguinte:

   a. Na lista de máquinas protegidas, marque a caixa de seleção ao lado da máquina que você quer exportar.
   b. No menu suspenso **Actions** (Ações) dessa máquina, clique em **Rollback** (Reverter).
   c. Na caixa de diálogo **Rollback — Select Recovery Point** (Reverter - Selecionar ponto de recuperação), selecione um ponto de recuperação para exportar e, em seguida, clique em **Next** (Avançar).
      - Na área de navegação esquerda do AppAssure Core Console, selecione a máquina que você quer reverter; isso abre a guia **Summary** (Resumo) desta máquina.
   d. Clique na guia **Recovery Points** (Pontos de recuperação) e, em seguida, selecione um ponto de recuperação na lista.
   e. Expanda os detalhes desse ponto de recuperação e, em seguida, clique em **Rollback** (Reverter).
2. Edite as opções de reversão conforme descrito na tabela a seguir.

Caixa de texto	Descrição
Máquina protegida	Especifique a máquina agente original como o destino da reversão. "Origem" refere-se ao agente a partir do qual foi criado o ponto de recuperação que está sendo usado para a reversão.
Instância do console de recuperação	Para restaurar o ponto de recuperação para qualquer máquina inicializada no modo URC, digite o nome de usuário e senha.

3. Clique em **Load Volumes** (Carregar volumes).

   A caixa de diálogo **Volume Mapping** (Mapeamento de volume) aparece.

   NOTA: O Core Console não mapeia automaticamente os volumes Linux. Para localizar um volume Linux, navegue até o volume que você quer reverter.

4. Selecione os volumes que você quer reverter.
5. Usando as opções **Destination** (Destino), selecione o volume de destino para o qual o volume selecionado será revertido.
6. Selecione uma das seguintes opções:
   - **Live Recovery** (Recuperação em tempo real). Quando essa opção é selecionada, a reversão dos volumes Windows acontece imediatamente. Selecionado por padrão.

     NOTA: A opção **Live Recovery** (Recuperação em tempo real) não está disponível para volumes Linux.

   - **Force Dismount** (Forçar desmontagem). Quando selecionado, força a desmontagem de qualquer ponto de recuperação montado antes de realizar a reversão. Selecionado por padrão.
7. Clique em **Rollback** (Reverter).

   O sistema começará o processo de reversão para o ponto de recuperação selecionado.

Realizar uma reversão para uma máquina Linux usando a linha de comando

Reversão é o processo de restaurar os volumes em uma máquina a partir dos pontos de recuperação. No AppAssure, você pode realizar uma reversão de volumes nas máquinas Linux protegidas usando o utilitário de linha de comando `aamount`.

CUIDADO: Não tente realizar uma reversão no volume do sistema ou raiz (/).

NOTA: O recurso de reversão é suportado para as máquinas Windows protegidas dentro do Console Core. Para obter mais informações, consulte Realizar uma reversão.

Para realizar uma reversão de um volume em uma máquina Linux:

1. Execute o utilitário AppAssure `aamount` como raiz, por exemplo:

   ```
   sudo aamount
   ```

2. No prompt de montagem do AppAssure, 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 AppAssure Core.
4. Digite as credenciais de login, ou seja, o nome de usuário e a senha, desse servidor.

   Uma lista mostra as máquinas que esse servidor do AppAssure protege. Ela mostra as máquinas do agente encontradas por número de item da linha, endereço de host/IP e um número de ID para a máquina (por exemplo: `293cc667-44b4-48ab-91d8-44bc74252a4f`).

5. Para ver a lista dos pontos de recuperação atualmente montados para a máquina especificada, digite o seguinte comando:

   `lr <machine_line_item_number>`

   NOTA: Você pode também inserir o número de identificação da máquina nesse comando em vez do número de item de linha.

   Uma lista mostra os pontos de recuperação básicos e incrementais da máquina. A lista inclui um número de item, marcação de data/hora,local do volume, tamanho do ponto de recuperação e um número de ID do volume que inclui um número de sequência no final (por exemplo, `"293cc667-44b4-48ab-91d8-44bc74252a4f:2"`), que identifica o ponto de recuperação.

6. Para selecionar um ponto de recuperação para reversão, digite o comando a seguir:

   `r [volume_recovery_point_ID_number] [path]`

   Esse número reverte a imagem do volume especificada pela ID do núcleo ao caminho especificado. O caminho para a reversão é o caminho para o descritor do arquivo do dispositivo e não é o diretório ao qual ele está montado.

   NOTA: Para identificar o ponto de recuperação, você pode também especificar um número de linha no comando, em vez do número de ID do ponto de recuperação. Nesse caso, use o número de linha do agente/máquina (da saída `lm`), seguido do número de linha do ponto de recuperação e a letra do volume, seguido pelo caminho, como **r [machine_line_item_number] [recovery_point_line_number] [volume_letter] [path]**. Nesse comando, [caminho] é o descritor de arquivo para o volume real.

   Por exemplo, se o comando `lm` mostra três máquinas de agente, e você digitar o comando `lr` para a máquina número 2 e quiser reverter o volume b do ponto de recuperação 23 para o volume que estava montado no diretório `/mnt/data`, o comando é: `r2 23 b /mnt/data`.

   NOTA: É possível reverter para /, mas apenas ao realizar uma restauração sem sistema operacional inicializada com o Live CD. Para obter mais informações, consulte Realizar uma restauração sem sistema operacional para uma máquina Linux.

7. Quando solicitado para continuar, digite `y` (yes) para indicar Sim.

   após a reversão, uma série de mensagens é mostrada para notificar você sobre o status.

8. Após a reversão, o utilitário `aamount` monta e reanexa automaticamente o módulo kernel ao volume revertido se o destino estiver previamente protegido e montado. Caso contrário, monte o volume de reversão no disco local e depois verifique se os arquivos são restaurados.

   Por exemplo, você pode usar o comando `sudo mount` e, em seguida, o comando `ls`.

   CUIDADO: Não desmonte um volume Linux protegido manualmente. Caso você precise desmontar manualmente um volume Linux protegido, precisa executar o seguinte comando antes de desmontá-lo: `bsctl -d [path to volume].`

   Nesse comando, [caminho do volume] não se refere ao ponto de montagem do volume, mas sim ao descritor do arquivo do volume; ele precisa estar em uma forma semelhante a: `/dev/sda1`.

Sobre a restauração sem sistema operacional para máquinas Windows

Os servidores, quando operam conforme o esperado, realizam as tarefas que estão configurados para fazer. Quando ocorre um evento catastrófico que torna o servidor inoperante, etapas imediatas são

necessárias para restaurá-lo às condições operacionais prévias. O processo normalmente é feito reformatando a máquina, reinstalando o sistema operacional, recuperando os dados através de backups e reinstalando os aplicativos de software.

O AppAssure oferece o recurso de executar uma restauração sem sistema operacional (BMR) para máquinas Windows independentemente do hardware ser similar ou diferente. Este processo engloba a criação de uma imagem de CD de inicialização, gravar a imagem em disco, inicializar o servidor de destino a partir do disco, conectar-se à instância do console de recuperação, mapear volumes, iniciar o recuperação e monitorar o processo. Depois que a restauração sem sistema operacional estiver concluída, você pode continuar a tarefa de carregar o sistema operacional e os aplicativos de software no servidor restaurado, seguido por suas configurações e definições únicas.

Outras circunstâncias nas quais você pode optar por executar uma restauração sem sistema operacional incluem upgrade de hardware ou substituição do servidor.

A funcionalidade de BMR também é suportada para máquinas Linux protegidas usando o utilitário de linha de comando `aamount`. Para obter mais informações,consulte Realizar uma restauração sem sistema operacional para uma máquina Linux.

Pré-requisitos para realizar uma restauração sem sistema operacional para uma máquina Windows

Antes que você possa iniciar o processo de restauração sem sistema operacional para uma máquina Windows, você precisa confirmar se as seguintes condições e critérios existem:

- Backups do servidor e do Core funcional
- Hardware para restaurar (novo ou antigo, semelhante ou diferente)
- CD virgem e software de gravação de CD
- Visualizador do VNC (opcional)
- Drivers de adaptador de rede e de armazenamento compatíveis com Windows 7 PE (32 bits) para o computador-alvo
- Controlador de armazenamento, RAID, AHCI e drivers de chipset para o sistema operacional de destino

NOTA: Os drivers do Controlador de armazenamento são necessários apenas se a restauração for realizada para um hardware diferente.

Roteiro para realizar uma restauração sem sistema operacional para uma máquina Windows

Para realizar uma BMR (Bare Metal Restore - Restauração sem sistema operacional) para uma máquina Windows:

1. Crie um CD de inicialização. Consulte Criar uma imagem ISO em CD inicializável.
2. Grave a imagem no disco.
3. Inicialize o servidor de destino a partir do CD de inicialização. Consulte Carregar um CD de inicialização.
4. Conecte-se ao disco de recuperação.
5. Mapeie os volumes. Consulte Mapear volumes.
6. Inicie a recuperação. Consulte Iniciar uma restauração a partir do AppAssure Core.
7. Monitore o andamento. Consulte Ver o andamento da recuperação.

Criar uma imagem ISO em CD inicializável

Para realizar uma BMR para uma máquina Windows, você precisa criar uma imagem ISO/CD inicialização no Core Console, o qual contém a interface do console de recuperação universal do AppAssure. O console de recuperação universal do AppAssure é um ambiente usado para restaurar a unidade do sistema ou todo o servidor diretamente do AppAssure Core.

A imagem ISO que você cria é personalizada para a máquina que está sendo restaurada; dessa forma, ela precisa conter os drivers corretos de armazenamento em massa e rede. Se você prever que vai realizar restaurações para um hardware diferente da máquina na qual está criando o CD inicializável, você precisa incluir os drivers do controlador de armazenamento e outros no CD inicializável; consulte Injetar drivers em um CD inicializável.

NOTA: A Organização Internacional para Padronização (ISO) é um órgão internacional de representantes de diversas organizações nacionais que determina e define os padrões de sistema de arquivos. O ISO 9660 é um padrão de sistema de arquivos usado em mídias de disco ótico para troca de dados. Ele oferece suporte para diversos sistemas operacionais, como o Windows. Uma imagem ISO é o arquivo dos dados arquivados ou imagem em disco que contém dados de todos os setores do disco, além do sistema de arquivos do disco.

Para criar uma imagem ISO em CD inicializável:

1. No Core Console onde o servidor que você deseja restaurar está localizado, selecione **Core** (Núcleo) e depois clique na guia **Tools** (Ferramentas).
2. Clique em **Boot CDs** (CDs inicializáveis).
3. Selecione **Actions** (Ações) e depois clique em **Create Boot ISO** (Criar ISO inicializável).

   A caixa de diálogos **Create Boot CD** (Criar ISO inicializável) é mostrada. Para preencher a caixa de diálogo, use os procedimentos a seguir.

Nomear o arquivo de CD de inicialização e definição do caminho

Para nomear o arquivo de CD de inicialização e definir o caminho:

Na caixa de diálogo **Create Boot CD** (Criar CD de inicialização), digite o caminho ISO onde deve ser armazenado a imagem de inicialização no servidor do núcleo.

Se o compartilhamento no qual você deseja armazenar a imagem estiver com pouco espaço em disco, você pode definir o caminho conforme for necessário; por exemplo, D:\nomedoarquivo.iso.

NOTA: A extensão do arquivo deve ser .iso. 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 fazem distinção entre maiúsculas e minúsculas. Não use espaços. Nenhum caractere de símbolo ou de pontuação é permitido.

Criar conexões

Para criar conexões:

1. Em **Connection Options** (Opções de conexão), faça o seguinte:
   - Para obter o endereço IP dinamicamente usando o protocolo de configuração de host dinâmico (DHCP), selecione **Obtain IP address automatically** (Obter endereço IP automaticamente).
   - Opcionalmente, para especificar um endereço IP estático para o console de recuperação, selecione **Use the following IP address** (Usar o seguinte endereço IP) e digite o endereço IP, a

máscara de sub-rede, o gateway padrão e o servidor DNS nos campos apropriados. Você precisa especificar todos esses campos.

2. Caso seja necessário, em **UltraVNC Options** (Opções de UltraVNC), selecione **Add UltraVNC** (Adicionar UltraVNC) e depois digite as opções de UltraVNC. As configurações de UltraVNC permitem que você gerencie remotamente o console de recuperação enquanto ele está em uso.

   NOTA: Essa etapa é opcional. Se você precisar de acesso remoto para o console de recuperação, você precisa configurar e usar o UltraVNC. Você não pode fazer login usando os serviços de terminal da Microsoft enquanto usa o CD de inicialização.

Injetar drivers em um CD de inicialização

A injeção de drivers é usada para facilitar a operabilidade entre o console de recuperação, o adaptador de rede e o armazenamento no servidor de destino.

Se estiver restaurando para um hardware diferente, você precisa injetar os drivers de controlador de armazenamento, RAID, AHCI, chipset e outros drivers no CD de inicialização. Esses drivers possibilitam que o sistema operacional detecte e opere todos os dispositivos corretamente.

NOTA: Tenha em mente que o CD de inicialização vai conter automaticamente drivers do Windows 7PE de 32 bits.

Para injetar drivers em um CD de inicialização:

1. Baixe os drivers do site do fabricante para o servidor e descompacte-os.
2. Compacte a pasta que contém os drivers usando um utilitário de compactação, como, por exemplo, o WinZip.
3. Na caixa de diálogo **Create Boot CD** (Criar CD de inicialização), in no painel **Drivers**, clique em **Add a Driver** (Adicionar um driver).
4. Para localizar o arquivo de driver compactado, navegue pelo sistema de arquivamento. Selecione o arquivo e clique em **Open** (Abrir).

   Os drivers inseridos aparecem realçados no painel **Drivers**.

Criar o CD de inicialização

Para criar um CD de inicialização após você ter nomeado o CD de inicialização e especificado o caminho, criado uma conexão e, opcionalmente, injetado os drivers na tela **Create Boot CD** (Criar CD de inicialização), clique em **Create Boot CD** (Criar CD de inicialização). A imagem ISO é então criada.

Ver o andamento da criação de imagem ISO

Para ver o andamento da criação de imagem ISO, selecione a guia **Events** (Eventos) e, em seguida, em **Tasks** (Tarefas), você pode monitorar o andamento da criação da imagem ISO.

NOTA: Você também pode ver o andamento da criação da imagem ISO na caixa de diálogo **Monitor Active Task** (Monitorar tarefa ativa).

Quando a criação da imagem ISO estiver concluída, ela estará disponível na página **Boot CDs** (CDs de inicialização), acessível através do menu **Tools** (Ferramentas).

Acessar a imagem ISO

Para acessar a imagem ISO, navegue até o caminho de saída que você especificou, ou clique no link para baixar a imagem para um local no qual você possa então carregá-la no novo sistema. Por exemplo, na unidade de rede.

Carregar um CD de inicialização

Depois de criar a imagem do CD de inicialização, inicie o servidor de destino com o CD de inicialização recém-criado.

NOTA: Se você criou o CD de inicialização usando o DHCP; anote o endereço IP e a senha.

Para carregar um CD de inicialização:

1. Navegue até o novo servidor, carregar o CD de inicialização e depois inicie a máquina.
2. Especifique para **Boot from CD-ROM** (Inicializar do CD-ROM), que carrega o seguinte::
   - Windows 7 PE
   - Software do AppAssure Agent

   O console de recuperação universal do AppAssure inicia e mostra o endereço IP e a senha de autenticação da máquina.
3. Registre o endereço IP mostrado no painel Network Adapters Settings (Configurações de adaptadores de rede) e a autenticação e a senha mostradas no painel Authentication (Autenticação). Você vai usar essas informações posteriormente no processo de recuperação de dados para registrar de volta no console.
4. Se quiser alterar o endereço IP, selecione-o e clique em **Change** (Alterar).

   NOTA: Se você especificou um endereço IP na caixa de diálogo Create Boot CD (Criar CD de inicialização), o console de recuperação universal utiliza e o mostra na tela **Network Adapter settings** (Configurações de adaptador de rede).

Injetar drivers no servidor de destino

Se estiver restaurando para um hardware diferente, você precisa injetar os drivers de controlador de armazenamento, RAID, AHCI, chipset e se já não estiverem no CD de inicialização. Esses drivers possibilitam que o SO opere todos os dispositivos em seu servidor de destino corretamente.

Se não tiver certeza sobre quais drivers seu servidor de destino exige, clique na guia System Info (Informações de sistema) no console de recuperação universal. Essa guia mostra todos os tipos de dispositivos e hardware de sistema para o servidor de destino para o qual você deseja restaurar.

NOTA: Tenha em mente que seu servidor de destino contém automaticamente drivers do Windows 7PE de 32 bits.

Para injetar drivers no servidor de destino:

1. Baixe os drivers do site do fabricante para o servidor e descompacte-os.
2. Compacte a pasta que contém os drivers usando um utilitário de compactação de arquivos (por exemplo, o Winzip) e copie-a para o servidor de destino.
3. No console de recuperação universal, clique em **Driver Injection** (Injeção de driver).
4. Para localizar o arquivo de driver compactado, navegue pelo sistema de arquivamento e selecione o arquivo.
5. Se você clicou em **Driver Injection** (Injeção de driver) na etapa 3, clique em **Add Driver** (Adicionar driver). Se você clicou em **Load driver** (Carregar driver) na etapa 3, clique em **Open** (Abrir).

   Os drivers selecionados são injetados e serão carregados no sistema operacional após você reinicializar o servidor de destino.

Iniciar uma restauração a partir do núcleo

Para iniciar uma restauração a partir do núcleo:

1. Se os NICs em qualquer sistema que está sendo restaurado forem agrupados (ligados), remova todos exceto um dos cabos de rede.

   NOTA: A restauração do AppAssure não reconhece NICs agrupados. O processo não é capaz de resolver qual NIC usar se detectar mais de uma conexão ativa.
2. Navegue de volta para o servidor de núcleo e abra o Core Console.
3. Na guia **Machines** (Máquinas), selecione a máquina a partir da qual você deseja restaurar dados.
4. Clique no menu **Actions** (Ações) da máquina, clique em **Recovery Points** (Pontos de recuperação) para ver uma lista de todos os pontos de recuperação da máquina.
5. Amplie o ponto de recuperação a partir do qual você deseja restaurar e, em seguida, clique em **Rollback** (Reverter).
6. Na caixa de diálogo **Rollback** (Reverter), em Choose **Destination** (Escolher destino), selecione **Recovery Console Instance** (Instância de console de recuperação).
7. Nas caixas de texto **Host** e **Password** (Senha), digite o endereço IP e a senha de autenticação do novo servidor para o qual você deseja restaurar dados.

   NOTA: Os valores de host e senha são as credenciais que você registrou na tarefa anterior. Para obter mais informações, consulte Carregar um CD de inicialização.
8. Clique em **Load Volumes** (Carregar volumes) para carregar os volumes de destino para a nova máquina.

Mapear volumes

Você pode optar por mapear os volumes para os discos no servidor de destino automática ou manualmente. No alinhamento automático, o disco é apagado e reparticionado e todos os dados são apagados. O alinhamento é realizado na ordem em que os volumes são apresentados na lista e os volumes são alocados aos discos adequadamente de acordo com o tamanho e assim por diante. Múltiplos volumes podem usar um disco. Se você mapear as unidades manualmente, não poderá usar o mesmo disco duas vezes.

No mapeamento manual, você já precisa ter a nova máquina corretamente formatada antes de restaurá-la. Para obter mais informações, consulte Iniciar uma restauração a partir do AppAssure Core.

Para mapear volumes:

1. Para mapear os volumes automaticamente, faça o seguinte:
   a. Na caixa de diálogo **RollbackURC**, selecione a guia **Automatically Map Volumes** (Mapear volumes automaticamente).
   b. Na área **Disk Mapping** (Mapeamento do disco) em **Source Volume** (Volume de origem), verifique se o volume de origem está selecionado e se os volumes adequados são apresentados na lista abaixo e estão selecionados.
   c. Se o disco de destino que é mapeado automaticamente for o volume de destino correto, selecione **Destination Disk** (Disco de destino).
   d. Clique em **Rollback** (Reverter) e, em seguida, vá para a etapa 3.
2. Para mapear os volumes manualmente, faça o seguinte:
   a. Na caixa de diálogo **RollbackURC**, selecione a guia **Manually Map Volumes** (Mapear volumes manualmente).

b. Na área **Volume Mapping** (Mapeamento do volume) em **Source Volume** (Volume de origem), verifique se o volume de origem está selecionado e se os volumes adequados são apresentados na lista abaixo e estão selecionados.

c. Em **Destination** (Destino), no menu suspenso , selecione o destino adequado que será o volume de destino para realizar a restauração do zero para o ponto de recuperação selecionado e, em seguida, clique em **Rollback** (Reverter).

3. Na caixa de diálogo de confirmação **RollbackURC**, analise o mapeamento da origem do ponto de recuperação e o volume de destino para a reversão. Para realizar a reversão, clique em **Begin Rollback** (Iniciar reversão).

   ATENÇÃO: Se você selecionar Begin Rollback (Iniciar reversão), todas as partições e dados existentes na unidade de destino serão removidos permanentemente e substituídos pelo conteúdo do ponto de recuperação selecionado, incluindo o sistema operacional e todos os dados.

Ver o andamento da recuperação

Para ver o andamento da recuperação:

1. Após iniciar o processo de reversão, a caixa de diálogo **Active Task** (Tarefa ativa) é mostrada, indicando que a ação de reversão foi iniciada.

   NOTA: Esta aparência da caixa de diálogo **Active Task** (Tarefa ativa) não indica a conclusão bem-sucedida da tarefa.

2. Opcionalmente, para monitorar o andamento da tarefa de reversão, na caixa de diálogo Active Task (Tarefa ativa), clique em **Open Monitor** (Abrir monitor). Você pode ver o andamento da recuperação, além dos horários inicial e final, através da janela **Monitor Open Task** (Monitorar tarefa em aberto).

   NOTA: Para retornar aos pontos de recuperação para a máquina de origem a partir da caixa de diálogo **Active Task** (Tarefa ativa), clique em **Close** (Fechar).

Iniciar o servidor de destino restaurado

Para iniciar o servidor de destino restaurado:

1. Navegue de volta ao servidor de destino e, na interface **AppAssure Universal Recovery Console** (Console de recuperação universal do AppAssure), clique em **Reboot** (Reinicializar) para iniciar a máquina.
2. Especifique para iniciar o Windows normalmente.
3. Faça login na máquina.

   O sistema é restaurado para seu estado antes da restauração sem sistema operacional.

Reparar problemas de inicialização

Tenha em mente que, você tiver restaurado para um hardware diferente, você precisa ter injetado os drivers de controlador de armazenamento, RAID, AHCI, chipset e outros se já não estiverem no CD de inicialização. Esses drivers possibilitam que o SO opere todos os dispositivos em seu servidor de destino corretamente.

Para reparar problemas de inicialização:

1. Se você passar por problemas ao iniciar o servidor de destino restaurado, abra o console de recuperação universal recarregando o CD de inicialização.
2. No console de recuperação universal, clique em **Driver Injection** (Injeção de driver).
3. Na caixa de diálogo Driver Injection (Injeção de driver), clique em **Reparar Boot Problems** (Problemas de inicialização).

Os parâmetros de inicialização no registro de inicialização de servidor de destino são reparados automaticamente.

4. No console de recuperação universal, clique em **Reboot** (Reinicializar).

Realizar uma restauração sem sistema operacional para uma máquina Linux

Você pode realizar uma Restauração sem sistema operacional (BMR) para uma máquina Linux, incluindo a reversão do volume do sistema. Usando o utilitário de linha de comando do AppAssure `aamount`, reverta para a imagem básica do volume de inicialização. Antes de poder realizar um BMR para uma máquina Linux, primeiro você precisa fazer o seguinte:

- Obtenha um arquivo do CD Live para BMR com o suporte do AppAssure, o qual inclui uma versão inicialização do Linux.

  NOTA: Você também pode baixar o CD Live para Linux no portal de licenças na página **https://licenseportal.com**.
- Certifique-se de que haja espaço suficiente no disco rígido para criar partições de destino na máquina de destino que vai conter os volumes de origem. Qualquer partição de destino deve no mínimo ter a mesma capacidade da partição de origem.
- Identifique o caminho da reversão, que é o caminho do descritor do arquivo do dispositivo. Para identificar o caminho do descritor do arquivo do dispositivo, use o comando `fdisk` em uma janela do terminal.

  NOTA: Antes de começar a usar os comandos do AppAssure, você pode instalar o utilitário Tela. Ele permite rolar a tela para ver mais dados, como uma lista de pontos de recuperação. Para obter informações sobre como instalar o utilitário Tela, consulte Instalar o utilitário Tela

Para iniciar uma restauração sem sistema operacional para uma máquina Linux:

1. Usando o CD Live que você recebeu do AppAssure, inicialize a máquina Linux e abra uma janela de terminal.
2. Caso seja necessário, crie uma nova partição de disco (por exemplo, ao executar o comando `fdisk` como raiz) e torne essa partição inicializável ao usar o comando `a`.
3. Execute o utilitário AppAssure `aamount` como raiz, por exemplo:

   ```
   sudo aamount
   ```
4. No prompt de montagem do AppAssure, 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 AppAssure Core.
6. Digite as credenciais de login, ou seja, o nome de usuário e a senha, desse servidor.

   Uma lista mostra as máquinas protegidas por esse servidor do AppAssure Core. Ela mostra as máquinas encontradas por número de item de linha, endereço de host/IP e um número de identificação para a máquina (por exemplo: `293cc667-44b4-48ab-91d8-44bc74252a4f`).
7. Para listar os pontos de recuperação atualmente montados para a máquina que você deseja restaurar, digite o comando a seguir:

   ```
   lr <machine_line_item_number>
   ```

   NOTA: Você pode também inserir o número de identificação da máquina nesse comando em vez do número de item de linha.

   É mostrada uma lista que indica os pontos de recuperação incrementais e de base para a máquina. Essa lista inclui um número de item de linha, carimbo de data/hora, local do volume, tamanho do

ponto de recuperação e um número de identificação para o volume que inclui um número de sequência no final(por exemplo, "293cc667-44b4-48ab-91d8-44bc74252a4f:2"), o qual identifica o ponto de recuperação.

8. Para selecionar um ponto de recuperação de imagem de base para reversão, digite o comando a seguir:

   `r <volume_base_image_recovery_point_ID_number> <path>`

   CUIDADO: Você precisa garantir que o volume do sistema não esteja montado.

   Esse número reverte a imagem do volume especificada pela ID do núcleo ao caminho especificado. O caminho para a reversão é o caminho para o descritor do arquivo do dispositivo e não é o diretório ao qual ele está montado.

   NOTA: Você também pode especificar um número de linha no comando, em vez do número de ID de ponto de recuperação para identificar o ponto de recuperação. Use o número de linha de agente/máquina (do comando lm), seguido do número de linha de ponto de recuperação e letra do volume, seguidos pelo caminho, como, **r <machine_line_item_number> <base_image_recovery_point_line_number> <volume_letter> <path>**. Nesse comando, **<caminho>** é o descritor de arquivo para o volume real.

9. Quando solicitado para continuar, digite `y` (yes) para indicar Sim.

   Após a reversão, uma série de mensagens é mostrada para notificar você sobre o status.

10. Após a reversão correta, caso seja necessário, atualize o registro de inicialização principal com o carregador de inicialização restaurado.

    NOTA: Reparar ou configurar o carregador de inicialização só é necessário se esse disco for novo. Se essa é uma simples reversão para o mesmo disco, não é necessário configurar o carregador de inicialização.

    CUIDADO: Não desmonte um volume Linux protegido manualmente. Caso você precise desmontar manualmente um volume Linux protegido, você precisa executar o seguinte comando antes de desmontar o volume: bsctl -d <path to volume>

    Nesse comando, o`<path to volume>` não se refere ao ponto de montagem do volume, mas sim ao descritor de arquivo do volume; ele deve estar no mesmo formato desse exemplo: **/dev/sda1**.

Instalar o utilitário Tela

Antes de começar a usar os comandos do AppAssure, você pode instalar o utilitário Tela. O utilitário permite que você role a tela para ver uma quantidade maior de dados, como uma lista de pontos de recuperação.

Para instalar o utilitário Tela:

1. Usando o arquivo do CD Live, inicie a máquina Linux.

   Uma janela de terminal é mostrada.

2. Digite o seguinte comando: `sudo apt-get install screen`.
3. Para iniciar o utilitário Tela, digite `screen` no prompt de comando.

Criar partições inicializáveis em uma máquina Linux

Para criar partições inicializáveis em uma máquina Linux usando a linha de comando:

1. Anexe todos os dispositivos usando o utilitário **bsctl** com o seguinte comando como raiz: `sudo bsctl --attach-to-device /dev/<restored volume>`

   NOTA: Repita essa etapa para cada volume restaurado.
2. Monte cada volume restaurado usando os seguintes comandos:

   ```
   mount /dev/<restored volume> /mnt

   mount /dev/<restored volume> /mnt
   ```

   NOTA: Algumas configurações do sistema podem incluir o diretório de inicialização como parte do volume raiz.
3. Monte metadados de instantâneo para cada volume restaurado usando os seguintes comandos:

   ```
   sudo bsctl --reset-bitmap-store /dev/<restored volume>

   sudo bsctl --reset-bitmap-store /dev/<restored volume>
   ```
4. Verifique se o identificador universal único (UUID) contém os novos volumes usando os comandos `blkid` ou `ll /dev/disk/by-uuid`.
5. Verifique se `/etc/fstab` contém os UUIDs corretos dos volumes de inicialização e rais.
6. Instale o carregador de inicialização GRUB usando os seguintes comandos:

   ```
   mount --bind /dev/ /mnt/dev

   mount --bind /proc/ /mnt/proc

   chroot/mnt/bin/bash

   grub-install/dev/sda
   ```
7. Verifique se o arquivo **/boot/grub/grub .conf**o arquivo o UUID correto para o volume raiz ou atualize-o conforme necessário usando um editor de texto.
8. Remova o CD Live da unidade de CD-ROM e reinicie a máquina Linux.

Ver eventos e alertas

Para ver eventos e alertas:

1. Faça o seguinte:
   - No Core Console, na guia Machines (Máquinas), clique no hiperlink da máquina cujos eventos você quer ver.
   - Na área **Navigation** (Navegação) esquerda do Console Core, selecione a máquina cujos eventos você quer ver.
2. Clique na guia **Events** (Eventos).

   Um log de todos os eventos para as tarefas e alertas atuais é mostrado.

5

Proteger clusters de servidor

Sobre a proteção do cluster de servidor

No AppAssure, a proteção do cluster de servidor está associada aos agentes AppAssure instalados nos nós de cluster individuais (isto é, cada máquina no cluster) e ao Core, que protege os agentes como se fossem uma máquina composta.

Você pode configurar facilmente um Core para proteger e gerenciar um cluster. No Core Console, um cluster é organizado como uma entidade separada, que atua como um "contêiner" para incluir os nós relacionados. Por exemplo, na área de navegação esquerda, o Core está no topo da árvore de navegação e os clusters são apresentados na lista sob o Core e contêm os nós associados individuais (nos quais os agentes do AppAssure estão instalados).

Nos níveis do Core e do cluster, você pode ver informações sobre o cluster, como a lista de nós relacionados e volumes compartilhados. Um cluster é mostrado no Core Console na guia Machines (Máquinas) e você pode alternar a exibição (usando Mostrar/Ocultar) para ver os nós incluídos no cluster. No nível do cluster, você pode também ver os metadados de cluster correspondentes do Exchange e do SQL para os nós do cluster. Você pode especificar as configurações de todo o cluster e dos volumes compartilhados nesse cluster ou navegar para um nó (máquina) individual no cluster para configurar apenas esse nó e os volumes locais associados.

Aplicativos e tipos de cluster suportados

Para proteger seu cluster corretamente, você precisa ter instalado o software AppAssure Agent em cada uma das máquinas ou nós do cluster. O AppAssure suporta as versões de aplicativo e as configurações de cluster listadas na tabela a seguir.

Tabela 4. Aplicativos e tipos de cluster suportados

Aplicativo	Versão do aplicativo e configuração de cluster relacionada	Windows Failover Cluster
Microsoft Exchange	2007 Single Copy Cluster (SCC)	2003, 2008, 2008 R2
	2007 Cluster Continuous Replication (CCR)	
	2010 Database Availability Group (DAG)	2008, 2008 R2
Microsoft SQL	2005, 2008, 2008 R2 Single Copy Cluster (SCC)	2003, 2008, 2008 R2
	2012 Single Copy Cluster (SCC)	2008, 2008 R2, 2012

Os tipos de disco suportados incluem:

- Discos de tabela de partição GUID (GPT) maiores que 2 TB
- Discos dinâmicos
- Discos básicos

Os tipos de montagem suportados incluem:

- Unidades compartilhadas que estão conectadas como letras de unidade (por exemplo, D:)
- Volumes dinâmicos simples em um único disco físico (e não volumes segmentados, espelhados ou estendidos)
- Unidades compartilhadas que estão conectadas como pontos de montagem

Proteger um cluster

Este tópico descreve como adicionar um cluster para proteção no AppAssure. Quando você adiciona um cluster para proteção, precisa especificar o nome do host ou o endereço IP do cluster, o aplicativo do cluster ou um dos nós de cluster ou máquinas que inclui o AppAssure Agent.

NOTA: Um repositório é usado para armazenar os instantâneos de dados capturados dos seus nós protegidos. Antes de começar a proteger os dados do cluster, configure pelo menos um repositório que será associado ao AppAssure Core.

Para obter informações sobre a configuração de repositórios, consulte Sobre repositórios.

Para proteger um cluster:

1. Faça um dos seguintes:
   - No Core Console, navegue até a guia **Home** (Início) e, em seguida, clique no botão **Protect Cluster** (Proteger cluster).
   - No Core Console, na guia **Machines** (Máquinas), clique em **Actions** (Ações) e, em seguida, clique em **Protect Cluster** (Proteger cluster).
2. Na caixa de diálogo **Connect to Cluster** (Conectar ao cluster), digite as seguintes informações:

Caixa de texto	Descrição
Host	O nome de host ou o endereço IP do cluster, o aplicativo de cluster ou um dos nós de cluster que você quer proteger. NOTA: Se você usar o endereço IP de um dos nós, esse nó precisa ter um agente AppAssure instalado e iniciado.
Port (Porta)	O número da porta na máquina na qual o AppAssure Core se comunica com o agente.
User name (Nome de usuário)	O nome de usuário do administrador do domínio usado para conectar a esta máquina: por exemplo, **nome_domínio\administrator** ou **administrator@nome_domínio.com** NOTA: O nome do domínio é obrigatório. Você não pode se conectar ao cluster usando o nome de usuário do administrador local.
Password (Senha)	A senha usada para conectar a esta máquina.

3. Na caixa de diálogo **Protect Cluster** (Proteger cluster), selecione um repositório para este cluster.
4. Para proteger o cluster com base nas configurações padrão, selecione os nós para a proteção padrão e clique em **Protect** (Proteger).

NOTA: As configurações padrão garantem que todos os volumes sejam protegidos com um agendamento a cada 60 minutos.

5. Para inserir configurações personalizadas para o cluster (por exemplo, para personalizar o agendamento de proteção dos volumes compartilhados), faça o seguinte:
   a. Clique em **Settings** (Configurações).
   b. Na caixa de diálogo **Volumes**, selecione o(s) volume(s) para proteger e clique em **Edit** (Editar).
   c. Na caixa de diálogo **Protection Schedule** (Agendamento da proteção) , selecione uma das opções de agendamento para proteger os seus dados descritas na tabela a seguir.

Caixa de texto	Descrição
Interval (Intervalo)	Você pode escolher entre: • **Weekday** (Dia da semana) – Para proteger os dados em um intervalo de tempo específico, selecione **Interval** (Intervalo) e, em seguida: – Para personalizar quando proteger os dados durante períodos de pico, você pode especificar uma hora de início, uma hora de término e um intervalo. – Para proteger os dados durante períodos fora do pico, marque a caixa de seleção **Protect during off-peak times** (Proteger durante períodos fora do pico) e, em seguida, selecione um intervalo para proteção. • **Weekends** (Fins de semana) – Para proteger os dados durante os fins de semana, marque a caixa de seleção **Protect during weekends** (Proteger durante os fins de semana) e, em seguida, selecione um intervalo.
Daily (Diariamente)	Para proteger os dados diariamente, selecione a opção **Daily** (Diariamente) e, em seguida, **Protection Time** (Horário da proteção), selecione um horário para iniciar a proteção dos dados.
No Protection (Nenhuma proteção)	Para remover a proteção desse volume, selecione a opção **No Protection** (Nenhuma proteção).

6. Depois de fazer todas as alterações necessárias, clique em **Save** (Salvar).
7. Para digitar as configurações personalizadas para um nó do cluster, selecione um nó e, em seguida, clique no link **Settings** (Configurações) ao lado do nó.
   • Repita a Etapa 5 para editar o agendamento da proteção.

   Para obter mais informações sobre como personalizar nós, consulte Proteger nós em um cluster .
8. Na caixa de diálogo **Protect Cluster** (Proteger cluster), clique em **Protect** (Proteger).

Proteger nós em um cluster

Este tópico descreve como proteger os dados de um nó de cluster ou de uma máquina que tem um agente AppAssure instalado. Quando você adiciona a proteção, precisa selecionar um nó na lista de nós disponíveis, além de especificar o nome de host e o nome de usuário e a senha do administrador do domínio.

Para proteger nós em um cluster:

1. Depois de adicionar um cluster, navegue até esse cluster e, em seguida, clique na guia **Machines** (Máquinas).
2. Clique no menu **Actions** (Ações) e, em seguida, clique em **Protect Cluster Node** (Proteger nó de cluster).
3. Na caixa de diálogo **Protect Cluster Node** (Proteger nó de cluster), selecione ou digite as seguintes informações conforme apropriado e, em seguida, clique em **Connect** (Conectar) para adicionar a máquina ou nó.

Caixa de texto	Descrição
Host	Uma lista suspensa de nós do cluster disponíveis para proteção.
Porta	O número da porta em que o Core se comunica com o agente no nó.
Nome de usuário	O nome de usuário do administrador do domínio utilizado para a conexão a este nó. Por exemplo, **example_domain\administrator** para **administrator@exemplo_domínio.com**.
Senha	A senha usada para conectar-se a esta máquina.

4. Clique em **Protect** (Proteger) para começar a proteger esta máquina com as configurações de proteção padrão.

   NOTA: As configurações padrão garantem que todos os volumes na máquina sejam protegidos com um agendamento a cada 60 minutos.

5. Para digitar as configurações personalizadas para esta máquina (por exemplo, para alterar o nome da tela, adicionar criptografia, ou personalizar o agendamento da proteção), clique em **Show Advanced Options** (Mostrar opções avançadas).
6. Edite as configurações a seguir conforme necessário, como descrito abaixo.

Caixa de texto	Descrição
Nome da tela	Digite um novo nome para a máquina, que será mostrado no Core Console.
Repositório	Selecione o repositório do Core em que os dados desta máquina serão armazenados.
Criptografia	Especifique se a criptografia será aplicada ao dados para cada volume desta máquina que será armazenado no repositório. NOTA: As configurações de criptografia para um repositório são definidas na guia **Configuration** (Configuração) do Core Console.
Programação	Selecione uma das seguintes opções. • Proteger todos os volumes com o agendamento padrão. • Proteja os volumes específicos com o agendamento personalizado. Em seguida, em **Volumes**, selecione um volume e clique em **Edit** (Editar). Para obter informações sobre a configuração personalizada de intervalos, consulte Proteger um cluster .

Processo de modificação das configurações do 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:

1. Faça o seguinte:
   - Navegue até o cluster que contém o nó que você quer modificar, clique na guia **Machines** (Máquinas) e selecione a máquina ou nó que você quer modificar.
   - Ou, no painel **Navigation** (Navegação), sob o cabeçalho **Cluster**, selecione a máquina ou nó que você quer modificar.
2. Para modificar e visualizar as configurações, consulte Ver e modificar as configurações.
3. Para configurar grupos de notificações para eventos do sistema, consulte Configurar grupos de notificações para eventos do sistema.
4. Para personalizar as configurações da política de retenção, consulte Personalizar configurações da política de retenção.
5. Para modificar o agendamento da proteção, consulte Modificar os agendamentos da proteção.
6. Para modificar configurações de transferência, consulte Modificar configurações de transferência .

Roteiro para definir as configurações do cluster

O roteiro para a definição das configurações do cluster envolve a execução das seguintes tarefas:

- Modificar as configurações do cluster
- Configurar as notificações de eventos do cluster
- Modificar a política de retenção do cluster
- Modificar os agendamentos de proteção do cluster
- Modificar as configurações de transferência do cluster

Modificar as configurações do cluster

Depois de adicionar um cluster, você pode facilmente modificar as configurações básicas (por exemplo, o nome de tela), da proteção (por exemplo, agendamentos da proteção, adicionar ou remover volumes e pausar proteção) e muito mais.

Para modificar as configurações do cluster:

1. Faça o seguinte:
   - No Core Console, clique na guia **Machines** (Máquinas) e, em seguida, selecione o cluster que você quer modificar.
   - Na área de navegação esquerda, selecione o cluster que você quer modificar.
2. Clique na guia **Configuration** (Configuração).

   A página **Configuration** (Configuração) aparece.
3. Clique em **Edit** (Editar) para modificar as configurações nesta página para o cluster, descrito da seguinte forma:

Caixa de texto	Descrição
Nome da tela	Digite um nome de tela para o cluster. O nome para este cluster é mostrado no Core Console. Por padrão, esse é o nome de host do cluster. Você pode alterar para um nome mais descritivo, se necessário.
Nome do host	Essa configuração representa o nome do host para o cluster. Ela é mostrada aqui apenas para fins informativos e não pode ser modificada.
Repositório	Digite o repositório do Core associado ao cluster. NOTA: Se os instantâneos desse cluster já foram obtidos, essa configuração é mostrada aqui apenas para fins informativos e não pode ser modificada.
Chave de criptografia	Edite e selecione uma chave de criptografia se necessário. Especifica se a criptografia será aplicada aos dados para cada volume deste cluster que será armazenado no repositório.

Configurar notificações de eventos do cluster

Você pode configurar como os eventos do sistema são relatados para o seu cluster, criando grupos de notificação. Esses eventos podem ser alertas ou erros do sistema.

Para configurar as notificações de eventos de cluster:

1. Faça o seguinte:
   - No Core Console, clique na guia **Machines** (Máquinas) e, em seguida, selecione o cluster que você quer modificar.
   - Na área de navegação à esquerda, selecione o cluster que você quer modificar.
2. Clique na guia **Configuration** (Configuração) e, em seguida, clique em **Events** (Eventos).
3. Selecione uma das opções descritas na tabela a seguir.

Caixa de texto	Descrição
Usar as configurações de alerta do Core	Adota as configurações usadas pelo núcleo associado: a. Clique em **Apply** (Aplicar). b. Conclua a Etapa 5.
Usar as configurações de alerta Personalizadas	Permite definir configurações personalizadas. Continue para a Etapa 4.

4. Se você selecionar **as configurações de alerta personalizadas**, clique em **Add Group** (Adicionar grupo) para adicionar um novo grupo de notificações para enviar uma lista dos eventos do sistema.
   A caixa de diálogo **Add Notification Group** (Adicionar grupo de notificações) é mostrada.
5. Adicione as opções de notificação conforme descrito na tabela a seguir.

Caixa de texto	Descrição
Nome	Digite um nome para o grupo de notificações.
Descrição	Digite uma descrição para o grupo de notificações.
Ativar eventos	Selecione os eventos para notificação; por exemplo, Clusters. Você também pode selecionar por tipo: • **Erro** • **Advertência** • **Info** NOTA: Quando você seleciona por tipo, por padrão, os eventos adequados são ativados automaticamente. Por exemplo, se você escolher Warning (Aviso), os eventos de Capacidade de conexão, Tarefas, Licenciamento, Arquivo, CoreService, Exportação, Proteção, Replicação e Reversão são ativados.
Opções de notificação	Selecione o método para especificar como lidar com as notificações. Você pode escolher uma das seguintes opções: • **Notify by Email** (Notificar por e-mail) – Especifique os endereços de e-mail para os quais enviar os eventos nas caixas de texto To (Para), CC e BCC (CCO). • **Notify by Windows Event log** (Notificar por log de eventos do Windows) – o log de eventos do Windows controla a notificação. • **Notify by syslogd** (Notificar por syslogd) – Especifique o nome do host e a porta para os quais enviar os eventos.

6. Clique em **OK** para salvar as alterações e, em seguida, clique em **Apply** (Aplicar).
7. Para editar um grupo de notificações existente, ao lado do grupo de notificação na lista, clique em **Edit** (Editar).

   A caixa de diálogo **Edit Notification Group** (Editar grupo de notificações) é aberta para você editar as configurações.

Modificar a política de retenção do cluster

A política de retenção de um cluster especifica por quanto tempo os pontos de recuperação para os volumes compartilhados do cluster são armazenados no repositório. As políticas de retenção são usadas para reter os instantâneos de backup por um período de tempo prolongado e ajudar a gerenciá-los. A política de retenção é imposta por um processo de implantação que ajuda a apagar os backups antigos e obsoletos.

1. Faça o seguinte:
   - No **Core Console**, clique na guia **Machines** (Máquinas) e, em seguida, selecione o cluster que você quer modificar.
   - Na área de navegação à esquerda, selecione o cluster que você quer modificar.
2. Clique na guia **Configuration** (Configuração) e, em seguida, clique em **Retention Policy** (Política de retenção).
3. Selecione uma das opções na tabela a seguir:

Caixa de texto	Descrição
Usar a política de retenção padrão do Core	Adota as configurações usadas pelo núcleo associado. Clique em **Apply** (Aplicar).
Usar a política de retenção personalizada	Permite definir configurações personalizadas.

NOTA: Se você selecionou **Custom alert settings** (Configurações de alerta personalizadas), siga as instruções para configurar uma política de retenção personalizada, conforme descrito em Personalizar configurações da política de retenção, a partir da Etapa 4.

Modificar os agendamentos de proteção do cluster

Você pode modificar os agendamentos de proteção somente se o cluster tiver volumes compartilhados.

Para modificar os agendamentos de proteção do cluster:

1. Faça um dos seguintes:
   - No Core Console, clique na guia **Machines** (Máquinas) e, em seguida, selecione o cluster que você quer modificar.
   - Na área de navegação à esquerda, selecione o cluster que você quer modificar.
2. Clique na guia **Configuration** (Configuração) e, em seguida, clique em **Protection Settings** (Configurações da proteção).
3. Siga as instruções para modificar as configurações da proteção conforme descrito em Modificar os agendamentos da proteção, a partir da Etapa 2.

Modificar as configurações de transferência do cluster

No AppAssure , você pode modificar as configurações para gerenciar os processos de transferência de dados para um cluster protegido.

NOTA: Você pode modificar as configurações de transferência do cluster somente se o cluster tiver volumes compartilhados.

Existem três tipos de transferências no AppAssure:

Caixa de texto	Descrição
Instantâneos	Faz o backup dos dados no cluster protegido.
Exportação de MV	Cria uma máquina virtual com todos os parâmetros e informações de backup especificados pelo agendamento definido para proteger o cluster.
Reversão	Restaura informações de backup para um cluster protegido.

Para modificar as configurações de transferência do cluster:

1. Faça o seguinte:
   - No Core Console, clique na guia **Machines** (Máquinas) e, em seguida, selecione o cluster que você quer modificar.
   - Na área de navegação esquerda, selecione o cluster que você quer modificar.
2. Clique na guia **Configuration** (Configuração) e, em seguida, clique em **Transfer Settings** (Configurações da transferência).

3. Modifique as configurações da proteção conforme descrito em Modificar os agendamentos da proteção, a partir da Etapa 2.

Converter um nó de cluster protegido em um agente

No AppAssure, você pode converter um nó de cluster protegido em um agente do AppAssure, de forma que ainda seja gerenciado pelo Core mas não faça mais parte do cluster. Isso é útil, por exemplo, se você quiser remover o nó do cluster, mas mantê-lo protegido.

Para converter um nó de cluster protegido em um agente:

1. Faça o seguinte:
   - No Core Console, clique na guia **Machines** (Máquinas) e selecione o cluster que contém a máquina que você quer converter. Clique na guia **Machines** (Máquinas) referente ao cluster.
   - Na área de navegação esquerda, selecione o cluster que contém a máquina que você quer converter e, em seguida, clique na guia **Machines** (Máquinas).
2. Selecione a máquina para converter, clique no menu suspenso **Actions** (Ações) na parte superior da guia Machines (Máquinas) e clique em **Convert to Agent** (Converter em agente).
3. Para adicionar a máquina novamente ao cluster, selecione a máquina e, em seguida, clique na guia **Summary** (Resumo), menu **Actions** (Ações) e **Convert to Node** (Converter em nó).

Ver informações de cluster do servidor

Ver as informações do sistema de cluster

Para ver as informações do sistema de cluster:

1. Faça o seguinte:
   - No Core Console, clique na guia **Machines** (Máquinas) e, em seguida, selecione o cluster que você quer ver.
   - Na área de **navegação** esquerda, selecione o cluster que você quer ver.
2. Clique na guia **Tools** (Ferramentas).

   A página **System Information** (Informações do sistema) mostra detalhes do sistema sobre o cluster, como nome, nós incluídos com o estado associado e versões do Windows e informações da interface de rede e da capacidade de volume.

Ver os eventos e alertas de cluster

Para obter mais informações sobre como ver eventos e alertas de uma máquina ou nó individual em um cluster, consulte Ver eventos e alertas.

Para ver os eventos e alertas de cluster:

1. Faça um dos seguintes:
   - No Core Console, clique na guia **Machines** (Máquinas) e, em seguida, selecione o cluster que você quer ver.
   - Na área **Navigation** (Navegação) à esquerda, em **Clusters**, selecione o cluster que você quer ver.
2. Clique na guia **Events** (Eventos).

   Um log mostra todos os eventos das tarefas atuais e os alertas para o cluster.
3. Para filtrar a lista de eventos, você pode marcar ou desmarcar as caixas de seleção **Active** (Ativo), **Complete** (Concluído) ou **Failed** (Falha) conforme apropriado.
4. Na tabela **Alerts** (Alertas), clique em **Dismiss All** (Ignorar todos) para ignorar todos os alertas na lista.

Ver as informações de resumo

Para ver as informações de resumo:

1. Faça um dos seguintes:
   - No Core Console, clique na guia **Machines** (Máquinas) e, em seguida, selecione o cluster que você quer ver.
   - Na área **Navigation** (Navegação) à esquerda, em **Clusters**, selecione o cluster que você quer ver.
2. Na guia **Summary** (Resumo), você pode ver informações como o nome e tipo do cluster, tipo de quórum (se aplicável) e o caminho do quórum (se aplicável).

   Essa guia também mostra informações rápidas sobre os volumes neste cluster, incluindo tamanho e agendamento da proteção.
3. Para atualizar essas informações, clique no menu suspenso **Actions** (Ações) e clique em **Refresh Metadata** (Atualizar metadados).

   Para obter mais informações sobre como ver o resumo e as informações de status para uma máquina ou nó individual em um cluster, consulte Ver o status da máquina e outros detalhes.

Trabalhar com pontos de recuperação do cluster

Um ponto de recuperação , também conhecido como um instantâneo, é uma cópia momentânea das pastas e arquivos para os volumes compartilhados em um cluster, que são armazenados no repositório. Os pontos de recuperação são usados para recuperar as máquinas protegidas ou montar um sistema de arquivos local. No AppAssure, você pode ver a lista de pontos de recuperação no repositório. Conclua o procedimento a seguir para analisar os pontos de recuperação.

NOTA: Se você estiver protegendo os dados de um cluster de servidor do DAG ou CCR, os pontos de recuperação associados não aparecem no nível do cluster. Eles ficam visíveis apenas no nível da máquina ou do nó.

Para obter mais informações sobre a exibição dos pontos de recuperação para cada máquina em um cluster, consulte Ver pontos de recuperação .

Para trabalhar com pontos de recuperação do cluster:

1. Faça o seguinte:
   - No Core Console, clique na guia **Machines** (Máquinas) e, em seguida, selecione o cluster cujos pontos de recuperação você quer ver.
   - Na área de navegação esquerda, em **Clusters**, selecione o cluster cujos pontos de recuperação você quer ver.
2. Clique na guia **Recovery Points** (Pontos de recuperação).
3. Para ver informações detalhadas sobre um ponto de recuperação específico, clique em **>** ao lado do ponto na lista para expandir a exibição.

   Para obter informações sobre as operações que podem ser realizadas com os pontos de recuperação , consulte Ver um ponto de recuperação específico.
4. Selecione um ponto de recuperação para montar.

   Para obter informações sobre como montar um ponto de recuperação, consulte Montar um ponto de recuperação para uma máquina Windows, a partir da Etapa 2.
5. Para apagar pontos de recuperação, consulte Remover pontos de recuperação .

Gerenciar instantâneos para um cluster

Você pode gerenciar instantâneos forçando um instantâneo ou pausando os instantâneos atuais. Forçar um instantâneo permite forçar uma transferência de dados para o cluster atualmente protegido. Quando você força um instantâneo, a transferência é iniciada imediatamente ou adicionada à fila. Somente os dados que foram alterados a partir de um ponto de recuperação anterior são transferidos. Se não houver um ponto de recuperação anterior, todos os dados (a imagem de base) nos volumes protegidos são transferidos. Quando você pausa um instantâneo, interrompe temporariamente todas as transferências de dados da máquina atual.

Para obter informações sobre como forçar instantâneos para as máquinas individuais em um cluster, consulte Forçar um instantâneo. Para obter informações sobre como pausar e retomar instantâneos para as máquinas individuais em um cluster, consulte Pausar e retomar proteção.

Forçar um instantâneo para um cluster

Para forçar um instantâneo para um cluster:

1. Faça o seguinte:
   - No Core Console, clique na guia **Machines** (Máquinas) e, em seguida, selecione o cluster cujos pontos de recuperação você quer ver.
   - Na área de navegação esquerda, em **Clusters**, selecione o cluster cujos pontos de recuperação você quer ver.
2. Na guia **Summary** (Resumo), clique no menu suspenso **Actions** (Ações) e, em seguida, clique em **Force Snapshot** (Forçar instantâneo).

Pausar e retomar instantâneos de cluster

Para pausar e retomar instantâneos de cluster:

1. Faça o seguinte:
   - No Core Console, clique na guia **Machines** (Máquinas) e, em seguida, selecione o cluster cujos pontos de recuperação você quer ver.
   - Na área de navegação esquerda, em **Clusters**, selecione o cluster cujos pontos de recuperação você quer ver.
2. Na guia **Summary** (Resumo), clique no menu suspenso Actions (Ações) e, em seguida, clique em **Pause Snapshots** (Pausar instantâneos).
3. Na caixa de diálogo **Pause Protection** (Pausar proteção), selecione uma das opções descritas da seguinte forma:

Caixa de texto	Descrição
Pausar até ser retomado	Pausa o instantâneo manualmente até que você retome a proteção. Para retomar a proteção, clique no menu **Actions** (Ações) e, em seguida, clique em **Resume** (Retomar).
Pausar por	Permite especificar uma quantidade de tempo em dias, horas e minutos para pausar os instantâneos.

Desmontar pontos de recuperação locais

Para desmontar pontos de recuperação locais:

1. Faça o seguinte:
   - No Core Console, clique na guia **Machines** (Máquinas) e, em seguida, selecione o cluster cujos pontos de recuperação você quer desmontar.
   - Na área de navegação à esquerda, selecione o cluster cujos pontos de recuperação você quer desmontar.
2. Na guia **Tools** (Ferramentas), sob o menu **Tools** (Ferramentas), clique em **Mounts** (Montagens).
3. Na lista de montagens locais, faça um dos seguintes:
   - Para desmontar uma única montagem local, localize e selecione a montagem para o ponto de recuperação que você quer desmontar e, em seguida, clique em **Dismount** (Desmontar).
   - Para desmontar todas as montagens locais, clique no botão **Dismount All** (Desmontar todos).

Realizar uma reversão para clusters e nós de cluster

A reversão é o processo de restaurar os volumes em uma máquina a partir dos pontos de recuperação. Para um cluster de servidores, a reversão é realizada no nível do nó (isto é, da máquina). Esta seção fornece diretrizes para realizar uma reversão de volumes de cluster.

Realizar uma reversão para clusters CCR (Exchange) e DAG

Para realizar uma reversão para clusters SCC (Exchange, SQL):

1. Desligue todos os nós, exceto um.
2. Realize a reversão usando o procedimento padrão da AppAssure para a máquina, conforme descrito em Realizar uma reversão e Realizar uma reversão para uma máquina Linux usando a linha de comando.
3. Quando a reversão terminar, monte todos os bancos de dados a partir dos 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** .

Realizar uma reversão para clusters SCC (Exchange, SQL)

Para realizar uma reversão para clusters SCC (Exchange, SQL):

1. Desligue todos os nós, exceto um.
2. Realize a reversão usando o procedimento padrão do AppAssure para a máquina, conforme descrito em Realizar uma reversão e Realizar uma reversão para uma máquina Linux usando a linha de comando.
3. Quando a reversão 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.

Replicar dados do cluster

Ao replicar os dados de um cluster, você configura a replicação no nível da máquina para as máquinas nesse cluster. Você pode também configurar a replicação para replicar os pontos de recuperação de volumes compartilhados. Por exemplo, se você tiver cinco agentes que quer replicar da origem para o destino.

Para obter mais informações e instruções sobre a replicação de dados, consulte Replicar dados do agente em uma máquina.

Remover um cluster da proteção

Para remover um cluster da proteção:

1. Faça o seguinte:
   - No Core Console, clique na guia **Machines** (Máquinas) e, em seguida, selecione o cluster que você quer remover.
   - Na área de navegação à esquerda, selecione o cluster que você quer remover para ver a guia **Summary** (Resumo).
2. Clique no menu suspenso **Actions** (Ações) e, em seguida, clique em **Remove Machine** (Remover máquina).
3. Selecione uma das seguintes opções.

Opção	Descrição
Keep Recovery Points (Manter pontos de recuperação)	Para manter todos os pontos de recuperação atualmente armazenados para este cluster.
Remove Recovery Points (Remover pontos de recuperação)	Para remover todos os pontos de recuperação atualmente armazenados para este cluster do repositório.

Remover nós de cluster da proteção

Conclua as etapas nos procedimentos a seguir para remover os nós de cluster da proteção. Se você quiser apenas remover um nó, consulte Converter um nó de cluster protegido em um agente. Para remover um nó de cluster da proteção.

1. Faça o seguinte:
   - No Core Console, clique na guia **Machines** (Máquinas) e selecione o cluster que contém o nó que você quer remover. Clique na guia **Machines** (Máquinas) referente ao cluster e selecione o nó que você quer remover.
   - Na área de navegação esquerda, sob o cluster associado, selecione o nó que você quer remover.
2. Selecione o menu suspenso **Actions** (Ações) e, em seguida, clique em **Remove Machine** (Remover máquina).
3. Selecione uma das opções descritas na tabela a seguir.

Opção	Descrição
Relationship Only (Apenas relação)	Remove o núcleo de origem da replicação mas mantém os pontos de recuperação replicados.
With Recovery Points (Com pontos de recuperação)	Remove o núcleo de origem da replicação e apaga todos os pontos de recuperação replicados recebidos da máquina.

Remover todos os nós em um cluster da proteção

Para remover todos os nós em um cluster da proteção:

1. Faça o seguinte:
   - No Core Console, clique na guia **Machines** (Máquinas) e selecione o cluster que contém os nós que você quer remover; em seguida, clique na guia **Machines** (Máquinas) referente ao cluster.
   - Na área de navegação esquerda, selecione o cluster que contém os nós que você quer remover e, em seguida, clique na guia **Machines** (Máquinas).
2. Clique no menu suspenso **Actions** (Ações) na parte superior da guia **Machines** (Máquinas) e, em seguida, clique em **Remove Machines** (Remover máquinas).
3. Selecione uma das opções descritas na tabela a seguir.

Opção	Descrição
Relationship Only (Apenas relação)	Remove o núcleo de origem da replicação mas mantém os pontos de recuperação replicados.
With Recovery Points (Com pontos de recuperação)	Remove o núcleo de origem da replicação e apaga todos os pontos de recuperação replicados recebidos da máquina.

Ver um relatório de cluster ou nó

Você pode criar e ver relatórios de conformidade e erros sobre as atividades do AppAssure referentes ao cluster e aos nós individuais. Os relatórios incluem informações da atividade do AppAssure sobre cluster, nó e volumes compartilhados. Para obter mais informações sobre os relatórios do AppAssure, consulte Sobre relatórios.

Para obter mais informações sobre as opções de exportação e impressão localizadas na barra de ferramentas de relatórios, consulte Sobre a barra de ferramentas de relatórios .

Para ver um relatório de cluster ou nó:

1. Faça o seguinte:
   - No Core Console, clique na guia **Machines** (Máquinas) e, em seguida, selecione o cluster ou nó para o qual você quer criar um relatório.
   - Na área **Navigation** (Navegação) esquerda, selecione o cluster ou nó para o qual você quer criar um relatório.
2. Clique na guia **Tools** (Ferramentas) e, no menu **Reports** (Relatórios), selecione uma das opções a seguir:
   - **Relatório de conformidade**

- **Relatório de erros**

3. No calendário suspenso **Start Time** (Hora de início), selecione uma data de início e, em seguida, digite a hora de início para o relatório.

   NOTA: Não há dados disponíveis antes do momento em que o AppAssure Core ou AppAssure Agent foi implementado.

4. No calendário suspenso **End Time** (Hora de término), selecione uma data de término e, em seguida, digite a hora de término para o relatório.
5. Clique em **Generate Report** (Gerar relatório).

   Se o relatório ocupar várias páginas, você pode clicar nos números de página ou nos botões de seta na parte superior da página de resultados do relatório ao longo dos resultados.

   Os resultados do relatório aparecem na página.
6. Para exportar os resultados do relatório para um dos formatos disponíveis – PDF, XLS, XLSX, RTF, MHT, HTML, TXT, CSV ou imagem – selecione o formato para exportação na lista suspensa e, em seguida, selecione uma das opções a seguir :
   - Clique no primeiro ícone **Save** (Salvar) para exportar um relatório e salvá-lo no disco.
   - Clique no segundo ícone **Save** (Salvar) para exportar um relatório e mostrá-lo em uma nova janela do navegador da Web.
7. Para imprimir os resultados do relatório, selecione uma das opções a seguir:
   - Clique no primeiro ícone **Printer** (Impressora) para imprimir todo o relatório.
   - Clique no segundo ícone **Printer** (Impressora) para imprimir a página atual do relatório.

6

Relatório

Sobre os relatórios

O dispositivo DL permite que você gere e veja a informações de conformidade, erro e dados resumidos de múltiplas máquinas agente e núcleos.

Você pode optar por ver os relatórios on-line, imprimir relatórios ou exportar e salvá-los em um dos diversos formatos compatíveis. Os formatos à sua escolha são:

- PDF
- XLS
- XLSX
- RTF
- MHT
- HTML
- TXT
- CSV
- Imagem

Sobre a barra de ferramentas de relatórios

A barra de ferramentas disponível para todos os relatórios permite que você imprima e salve de duas formas diferentes. A tabela a seguir descreve as opções para imprimir e salvar.

Ícone	Descrição
	Imprimir o relatório
	Imprimir a página atual
	Exportar um relatório e salvá-lo no disco
	Exportar um relatório e mostrá-lo em uma nova janela Use esta opção para copiar, colar e enviar por e-mail a URL para que outros vejam o relatório em um navegador da Web.

Sobre relatórios de conformidade

Relatórios de conformidade estão disponíveis para o núcleo e o AppAssure Agent. Eles fornecem a você uma maneira de ver o status dos trabalhos executados por um determinado núcleo ou agente. Trabalhos com falhas são mostrados com texto vermelho. Informações no relatório de conformidade do núcleo que não estejam associados a um agente aparecem em branco.

Detalhes sobre os trabalhos são apresentados em um visualização de coluna que inclui as seguintes categorias:

- Núcleo
- Agente protegido
- Tipo
- Resumo
- Status
- Erro
- Horário de início
- Horário de término
- Horário
- Trabalho total

Sobre relatórios de erros

Relatórios de erros são subconjuntos de relatórios de conformidade e estão disponíveis para núcleos e agentes AppAssure. Os relatórios de erros incluem apenas os trabalhos que falharam e que estão listados nos relatórios de conformidade e os compilam em um único relatório que pode ser impresso e exportado.

Detalhes sobre erros são apresentados em um visualização de coluna com as seguintes categorias:

- Núcleo
- Agente
- Tipo
- Resumo
- Erro
- Horário de início
- Horário de término
- Tempo decorrido
- Trabalho total

.

Sobre o relatório resumido de núcleo

O **Relatório resumido de núcleo** inclui informações sobre os repositórios no núcleo selecionado e sobre os agentes protegidos por esse núcleo. A informação é mostrada como dois resumos dentro de um único relatório.

Resumo de repositórios

A parte **Repositories** (Repositórios) do **relatório resumido de núcleo** inclui dados dos repositórios situados no núcleo selecionado. Detalhes sobre os repositórios são apresentados em uma visualização de coluna com as seguintes categorias:

- Nome
- Caminho de dados

- Caminho de metadados
- Espaço alocado
- Espaço usado
- Espaço livre
- Razão de compressão/desduplicação

Resumo de agentes

A parte **Agents** (Agentes) do **relatório resumido de núcleo** inclui dados para todos os agentes protegidos pelo núcleo selecionado.

Mais detalhes sobre os agentes são apresentados em uma visualização de coluna com as seguintes categorias:

- Nome
- Volumes protegidos
- Espaço total protegido
- Espaço protegido atual
- Taxa de mudança por dia (**média**, **mediana**)
- Estatísticas de trabalho (**aprovados**, **reprovados**, **cancelados**)

Gerar relatório para um núcleo ou agente

Para gerar relatório para um núcleo ou agente:

1. Navegue até o Core Console e selecione o núcleo ou o agente para o qual você deseja executar o relatório.
2. Clique na guia **Tools** (Ferramentas).
3. Na guia **Tools** (Ferramentas), amplie a seção **Reports** (Relatórios) na área de navegação esquerda.
4. Na área de navegação esquerda, selecione o relatório que você deseja executar. Os relatórios disponíveis dependem da seleção feita na etapa 1 e são descritos abaixo.

Máquina	Relatórios disponíveis
Núcleo	Relatório de conformidade Relatório resumido Relatório de erros
Agente	Relatório de conformidade Relatório de erros

5. No calendário suspenso **Start Time** (Horário inicial), selecione uma data inicial e depois digite um horário inicial para o relatório.

   NOTA: Não há dados disponíveis antes de quando o núcleo ou o agente foram implantados.
6. No calendário suspenso **End Time** (Horário final), selecione uma data final e depois digite um horário final para o relatório.
7. Na opção **Core Summary Report** (Relatório resumido), marque a caixa de seleção **All Time** (Todo o tempo) se você quiser que **horário inicial** e **horário final** englobem a vida útil do núcleo..

8. Para os relatórios **Core Compliance Report** (Relatório de conformidade de núcleo), ou **Core Errors Report** (Relatório de erros de núcleo), use a lista suspensa **Target Cores** (Núcleos de destino) para selecionar o núcleo do qual você deseja ver os dados.
9. Clique em **Generate Report** (Gerar relatório).

   Depois do relatório ser gerado, você pode usar a barra de ferramentas para imprimir ou exportar o relatório.

Sobre os relatórios de núcleo de console de gestão central

O dispositivo DL permite que você gere e veja informações de conformidade, erro e dados resumidos de vários núcleos. Detalhes sobre os núcleos são apresentados em visualizações de coluna com as mesmas categorias descritas nessa seção.

Gerar um relatório a partir do console de gestão central

Para gerar um relatório a partir do console de gestão central:

1. Na tela **Central Management Console Welcome** (Bem-vindo ao console de gestão central), clique no menu suspenso no canto superior direito.
2. No menu suspenso, clique em **Reports** (Relatórios) e depois selecione uma das opções a seguir:
   - **Relatório de conformidade**
   - **Relatório resumido**
   - **Relatório de falhas**
3. Na área de navegação esquerda, selecione os núcleos para os quais você deseja executar o relatório.
4. No calendário suspenso **Start Time** (Horário inicial), selecione uma data inicial e depois digite um horário inicial para o relatório.

   NOTA: Não há dados disponíveis antes de quando os núcleos foram implantados.
5. No calendário suspenso **End Time** (Horário final), selecione uma data final e depois digite um horário final para o relatório.
6. Clique em **Generate Report** (Gerar relatório).

   Depois do relatório ser gerado, você pode usar a barra de ferramentas para imprimir ou exportar o relatório.

7

Concluir uma recuperação total do dispositivo DL4300

As unidades de dados no dispositivo de Backup em disco DL4300 estão localizadas nos slots 0-11 e 14-17 e em formato RAID 6; elas podem suportar até duas falhas de unidade sem perda de dados. O sistema operacional reside nas unidades 12 e 13, que são formatadas como um disco virtual RAID 1. Se os dois discos falharem, você precisará substituir os discos rígidos e reinstalar o software necessário para o dispositivo funcionar novamente. Para concluir uma recuperação total do dispositivo, você deve:

- Criar uma partição RAID 1 para o sistema operacional
- Instalar o sistema operacional
- Executar o utilitário de atualização e recuperação
- Remontar os volumes

Criar uma partição RAID 1 para o sistema operacional

CUIDADO: É essencial realizar estas operações apenas nos discos virtuais RAID 1 que contêm o sistema operacional. Não siga essas operações nos discos RAID 6 que contêm dados.

Para criar uma partição RAID 1:

1. Confirme se os discos nos slots 12 e 13 são discos conhecidos e estão funcionando.
2. Inicialize o dispositivo de backup para disco DL4300 .
3. Quando solicitado durante o processo de inicialização, pressione <Ctrl> <R>.
   A tela **PERC BIOS Configuration Utility** (Utilitário de configuração do PERC BIOS) é mostrada.
4. Realce o controlador na parte superior da guia **VD Management** (Gerenciamento de VD) e pressione <F2> e, em seguida, selecione **Create New VD** (Criar novo VD).

   NOTA: Se o VD do RAID-1 OS já estiver presente, faça a sua inicialização rápida.
5. Na página **Virtual Disk Management** (Gerenciamento de disco virtual), selecione RAID 1 para Nível de RAID.
6. Selecione os dois discos na caixa **Physical Disks** (Discos físicos).

   NOTA: O tamanho do disco virtual não deve exceder 278,87 GB.
7. Digite um Nome VD, como "OS", identificando que este é o disco virtual que contém o sistema operacional.
8. Pressione <Tab> para mover o cursor para Inicializar e pressione <Enter>.

   NOTA: A inicialização realizada nesta fase é a inicialização rápida.
9. Clique em **OK** para finalizar a seleção ou pressione <Ctrl> <N> duas vezes.
   A página **Ctrl Mgt** (Gerenciamento de controle) aparece.
10. Navegue até o campo **Select boot device** (Selecionar dispositivo de inicialização) e selecione o disco virtual que contém o sistema operacional.

A capacidade desse disco é de aproximadamente 278 GB.

11. Selecione **Apply** (Aplicar) e pressione <Enter> .
12. Saia do **Utilitário de configuração do PERC BIOS** e pressione <Ctrl><Alt><Del> para reinicializar o sistema.

Instalar o sistema operacional

Use o utilitário Unified Server Configurator - Lifecycle Controller Enabled (USC-LCE) no dispositivo para recuperar o sistema operacional:

1. Localize a mídia de instalação do sistema operacional.
2. Confirme se você tem uma unidade para executar a mídia.

   Você pode usar uma unidade óptica USB ou um dispositivo de mídia virtual. A mídia virtual é suportada pelo iDRAC. Para obter mais informações sobre como configurar a mídia virtual através do iDRAC, consulte o Guia do usuário do dispositivo iDRAC do seu sistema.

   Se a mídia de instalação estiver corrompida ou ilegível, o USC pode não ser capaz de detectar a presença de uma unidade óptica suportada. Nesse caso, você pode receber uma mensagem de erro informando que nenhuma unidade óptica está disponível. Se a mídia não for válida (se for o CD ou DVD incorreto, por exemplo), uma mensagem aparecerá, solicitando que você insira a mídia de instalação correta.
3. Inicie o USC inicializando o sistema e pressionando a tecla <F10> dentro de 10 segundos depois que o logotipo da Dell for exibido.
4. Clique em **OS Deployment** (Implementação do sistema operacional) no painel esquerdo.
5. Clique em **Deploy OS** (Implementar sistema operacional) no painel direito.
6. Selecione o sistema operacional relevante e clique em **Next** (Avançar).

   O USC extrai os drivers necessários para o sistema operacional que você selecionou. Os drivers são extraídos para uma unidade USB interna chamada OEMDRV.

   NOTA: O processo para extrair os drivers pode levar alguns minutos.

   NOTA: Todos os drivers copiados pelo assistente OS Deployment (Implementação do sistema operacional) são removidos após 18 horas. Você deve concluir a instalação do sistema operacional no prazo de 18 horas para que os drivers copiados estejam disponíveis. Para remover os drivers antes do período de 18 horas terminar, reinicialize o sistema e pressione a tecla <F10> para inserir novamente o USC. O uso da tecla <F10> para cancelar a instalação do sistema operacional ou para inserir novamente o USC após a reinicialização, remove os drivers durante o período de 18 horas.
7. Depois que os drivers forem extraídos e o USC solicitar, insira a mídia de instalação do sistema operacional.

   NOTA: Ao instalar o sistema operacional Microsoft Windows, os drivers extraídos são instalados automaticamente durante a instalação do sistema operacional.

Executar o utilitário de atualização e recuperação

Para executar o utilitário Atualização e recuperação:

1. Faça download do **Recovery and Update Utility** (Utilitário Atualização e recuperação) de **dell.com/support**.
2. Copie o utilitário para a área de trabalho do dispositivo Backup to Disk (Backup para disco) DL4300 e extraia os arquivos.
3. Clique duas vezes em **launchRUU**.
4. Quando solicitado, clique em **Yes** (Sim) para confirmar que nenhum dos processos relacionados está em funcionamento.
5. Clique em **Start** (Iniciar) quando a tela **Recovery and update utility** (Utilitário de recuperação e atualização) for exibida.
6. Quando for solicitado reiniciar, clique em **OK**.

   O Windows Server Roles and Features, ASP .NET MVC3, LSI Provider, DL Applications, OpenManage Server Administrator e AppAssure Core Software são instalados como parte do utilitário de recuperação e atualização.
7. Reinicialize o sistema se for solicitado novamente.
8. Depois que todos os serviços e aplicativos forem instalados, clique em **Proceed** (Continuar).

   O assistente **AppAssure Appliance Recovery** (Recuperação do dispositivo AppAssure) é iniciado.
9. Conclua as etapas na fase **Collecting Information and Configuring** (Coletar informações e configurar) do assistente de recuperação do dispositivo AppAssure e, em seguida, clique em **Next** (Avançar).

   A fase **Disk Recovery** (Recuperação do disco) é iniciada.
10. Clique em **Next** (Avançar) depois de ver o alerta sobre o desligamento dos serviços do AppAssure.

    Os discos virtuais para os repositórios e quaisquer máquinas virtuais de espera são restaurados e os serviços do AppAssure são reiniciados. A recuperação está concluída.

8

Alterar manualmente o nome do host.

É recomendável que você selecione um nome de host durante a configuração inicial do Backup to Disk Appliance (Dispositivo de backup em disco) DL4300. Se você alterar o nome mais tarde, usando as **Propriedades do sistema Windows**, precisará realizar as seguintes etapas manualmente para garantir que o novo nome do host tenha efeito e o dispositivo funcione corretamente:

1. Parar o serviço do AppAssure Core
2. Apagar os certificados do servidor AppAssure
3. Apagar o Core Server e as chaves de registro
4. Alterar o nome de exibição no AppAssure
5. Atualizar sites confiáveis no Internet Explorer

Parar o serviço do Core

Para interromper os serviços do AppAssure Core:

1. Abra o **Windows Server Manager**.
2. Na árvore da esquerda, selecione **Configuration (Configuração)** → **Services (Serviços)**.
3. Clique com o botão direito em **AppAssure Core Service** (Serviço do AppAssure Core) e selecione **Stop** (Parar).

Apagar certificados do servidor

Para apagar os certificados do AppAssure Server:

1. Abra uma interface de linha de comando.
2. Digite **Certmgr** e pressione <Enter>.
3. Na janela **Certificate Manager** (Gerenciador de certificados) , selecione **Trusted Root Certification Authorities (Autoridades confiáveis de certificação da raiz)** → **Certificates (Certificados)**.
4. Apague qualquer certificado em que a coluna **Issue To** (Emitir para) mostre o antigo nome de host e a coluna **Intended Purpose** (Finalidade prevista) mostre **Server Authentication** (Autenticação de servidor).

Apagar o Core Server e as chaves de registro

Para apagar o Core Server e as chaves de registro:

1. Abra uma interface de linha de comando.
2. Digite **regedit** e pressione <Enter> para abrir o editor do Registro.
3. Na árvore, navegue até **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **AppRecovery** e abra o diretório do Core.

4. Apague os diretórios **webServer** e **serviceHost**.

Iniciar o Core com o novo nome do host

Para abrir o Core usando o novo nome do host que você criou manualmente:

1. Inicie os serviços do AppAssure Core.
2. Clique com o botão direito no ícone **AppAssure 5 Core** na área de trabalho e, em seguida, clique em **Properties** (Propriedades).
3. Substitua o antigo nome do servidor pelo novo `<server name:8006>`.

   Por exemplo, **https://<nome do servidor>:8006/apprecovery/admin/Core**.
4. Clique em **OK** e, em seguida, abra o AppAssure Core Console usando o ícone do **AppAssure 5 Core**.

Alterar o nome de exibição

Para alterar o nome de exibição:

1. Faça login no **AppAssure Console** (Console do AppAssure) como administrador.
2. Selecione a guia **Configuration** (Configuração) e, em seguida, clique no botão Change (Alterar) na barra **General** (Geral).
3. Digite o novo **Display Name** (Nome de exibição) e clique em **OK**.

Atualizar sites confiáveis no Internet Explorer

Para atualizar os sites confiáveis no Internet Explorer:

1. Abra o Internet Explorer.
2. Se os menus **Arquivo**, **Editar visualização** e outros não forem mostrados, pressione <F10>.
3. Clique no menu **Ferramentas** e selecione **Opções da Internet**.
4. Na janela **Opções da Internet**, clique na guia **Segurança**.
5. Clique em **Sites confiáveis** e depois clique em **Sites**.
6. Em **Adicionar este site à zona**, digite **https://[nome de exibição]**, usando o novo nome que você forneceu como nome de exibição.
7. Clique em **Adicionar**.
8. Em **Adicionar este site à zona**, digite **about:blank**.
9. Clique em **Adicionar**.
10. Clique em **Fechar** e depois em **OK**.

9

Apêndice A— Scripts

Sobre o script powershell

Windows PowerShell é um ambiente conectado ao Microsoft .NET Framework, projetado para a automação administrativa. O AppAssure inclui SDKs (Software Development Kits - Kits de desenvolvimento de software) abrangentes para o script PowerShell, que permitem que os administradores automatizem a administração e o gerenciamento de recursos da AppAssure executando os comandos através de scripts.

Assim, os usuários administrativos executam scripts PowerShell fornecidos pelo usuário nas ocorrências designadas. Por exemplo, antes ou depois de um instantâneo, verificações de capacidade de conexão e montagem e assim por diante. Os administradores podem executar scripts do AppAssure Core e do agente. Os scripts podem aceitar parâmetros e o resultado de um script é gravado no núcleo e nos arquivos de log do agente.

NOTA: Para tarefas noturnas, preserve um arquivo de script e o parâmetro de entrada JobType para distinguir entre as tarefas noturnas.

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: O Windows PowerShell é necessário e precisa ser instalado e configurado antes de usar e executar os scripts do AppAssure.

Pré-requisitos do script Powershell

Antes de usar e executar os scripts PowerShell para o AppAssure, você precisa ter o Windows PowerShell 2.0 instalado.

NOTA: Lembre-se de colocar o arquivo **powershell.exe.config** no diretório inicial do PowerShell. Por exemplo, **C:\WindowsPowerShell\powershell.exe**.

powershell.exe.config

```
<?xml version="1.0"?>
<configuration>
        <startup useLegacyV2RuntimeActivationPolicy="true">
        <supportedRuntime version="v4.0.30319"/>
<supportedRuntime version="v2.0.50727"/>
</startup>
</configuration>
```

Testar scripts

Se quiser testar os scripts que você pretende executar, pode fazê-lo utilizando o editor gráfico PowerShell, **powershell_ise**. Você precisa também adicionar o arquivo de configuração, **powershell_ise.exe.config** à mesma pasta do arquivo de configuração, **powershell.exe.config**.

NOTA: O arquivo de configuração, **powershell_ise.exe.config** precisa ter o mesmo conteúdo que o arquivo **powershell.exe.config**.

CUIDADO: Se o script pre-PowerShell ou post-PowerShell falhar, a tarefa também falha.

Parâmetros de entrada

Todos os parâmetros de entrada disponíveis são usados em scripts de amostra. Os parâmetros são descritos nas tabelas a seguir.

NOTA: Arquivos de script devem ter o mesmo nome que os arquivos de script de amostra.

Tabela 5. AgentTransferConfiguration (namespace Replay.Common.Contracts.Transfer)

Método	Descrição
`public uint MaxConcurrentStreams { get; set; }`	Obtém ou define o número máximo de conexões TCP simultâneas que o Core estabelece para o agente para a transferência de dados.
`public uint MaxTransferQueueDepth { get; set; }`	Quando uma faixa de blocos é lida a partir de um fluxo de transferência de dados, essa faixa é colocada em uma fila de produtor ou de consumidor, onde um consumidor possa lê-la e gravá-la para o objeto do período. Se o repositório gravar de forma mais lenta do que a rede lê, essa fila continua sendo preenchida. O ponto em que a fila está cheia e a leitura para, é a capacidade de transferência máxima da fila.
`public uint MaxConcurrentWrites { get; set; }`	Obtém ou define o número máximo de operações de gravação de bloco pendentes em um período em um dado momento. Se blocos adicionais forem recebidos quando muitas gravações de bloco estiverem pendentes, os blocos adicionais serão ignorados até que uma das gravações pendentes seja concluída.
`public ulong MaxSegmentSize { get; set; }`	Obtém ou define o número máximo de blocos contíguos para transferência em uma única solicitação. Dependendo dos testes, valores superiores ou inferiores podem ser ideais.
`public Priority Priority { get; set; }`	Obtém ou define a prioridade para solicitação de transferência.

Método	Descrição
`public int MaxRetries { get; set; }`	Obtém ou define o número máximo de vezes que uma transferência com falha é tentada novamente antes que a falha seja presumida.
`public Guid ProviderId{ get; set; }`	Obtém ou define a GUID do provedor VSS para uso de instantâneos neste host. Os administradores geralmente aceitam o padrão.
`public Collection<ExcludedWriter>ExcludedWriterIds { get; set; }`	Obtém ou define a coleção de IDs do gravador VSS, que é excluída deste instantâneo. O ID do gravador é determinado pelo nome do gravador. Esse nome é apenas para fins de documentação e não tem que ser exatamente igual ao nome do gravador.
`public ushort TransferDataServerPort { get; set; }`	Obtém ou define um valor contendo o porta TCP na qual aceitar conexões do Core para a transferência real de dados do agente para o Core. O agente tenta ouvir por essa porta, mas se a porta estiver em uso, o agente pode, em vez disso, usar uma porta diferente. O Core usa o número de porta especificado nas propriedades `BlockHashesUri` e `BlockDataUri` do objeto `VolumeSnapshotInfo` para cada volume encaixado (instantâneo).
`public TimeSpan SnapshotTimeout { get; set; }`	Obtém ou define o tempo para aguardar a conclusão de uma operação de instantâneo VSS antes de desistir e atingir o tempo limite.
`public TimeSpan TransferTimeout { get; set; }`	Obtém ou define o tempo de espera para se obter mais contato a partir do Core antes de abandonar o instantâneo.
`public TimeSpan NetworkReadTimeout { get; set; }`	Obtém ou define o tempo limite para operações de leitura da rede relacionadas a essa transferência.
`public TimeSpan NetworkWriteTimeout { get; set; }`	Obtém ou define o tempo limite para operações de gravação da rede relacionadas a essa transferência.

Tabela 6. BackgroundJobRequest (namespace Replay.Core.Contracts.BackgroundJobs)

Método	Descrição
`public Guid AgentId { get; set; }`	Obtém ou define o ID do agente.
`public bool IsNightlyJob { get; set; }`	Obtém ou define o valor indicando se a tarefa em segundo plano é uma tarefa noturna.
`public virtual bool InvolvesAgentId(Guid agentId)`	Determina o valor indicando se o agente concreto está envolvido na tarefa.

ChecksumCheckJobRequest (namespace Replay.Core.Contracts.Exchange.ChecksumChecks)

Herda seus valores do parâmetro, `DatabaseCheckJobRequestBase`.

DatabaseCheckJobRequestBase (namespace Replay.Core.Contracts.Exchange)

Herda seus valores do parâmetro, `BackgroundJobRequest`.

ExportJobRequest (namespace Replay.Core.Contracts.Export)

Herda seus valores do parâmetro, `BackgroundJobRequest`.

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 de memória da máquina de origem.
`public VirtualMachineLocation Location { get; set; }`	Obtém ou define a localização do alvo para esta exportação. Este é um resumo da classe base.
`public VolumeImageIdsCollection VolumeImageIds { get; private set; }`	Obtém ou define as imagens de volume para incluir na exportação da VM.
`public ExportJobPriority Priority { get; set; }`	Obtém ou define a prioridade para solicitação de exportação.

NightlyAttachabilityJobRequest (namespace Replay.Core.Contracts.Sql)

Herda seus valores do parâmetro, `BackgroundJobRequest`.

RollupJobRequest (namespace Replay.Core.Contracts.Rollup)

Herda seus valores do parâmetro, `BackgroundJobRequest`.

TakeSnapshotResponse (namespace Replay.Agent.Contracts.Transfer)

Método	Descrição
`public Guid SnapshotSetId { get; set; }`	Obtém ou define a GUID atribuída por VSS para este instantâneo.
`public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }`	Obtém ou define o coleção de informações do instantâneo para cada volume incluído no instantâneo.

TransferJobRequest (namespace Replay.Core.Contracts.Transfer)

Herda seus valores do parâmetro, `BackgroundJobRequest`.

Método	Descrição
`public VolumeNameCollection VolumeNames { get; set; }`	Obtém ou define a coleção de nomes de volume para transferência.
`public ShadowCopyType ShadowCopyType { get; set; }`	Obtém ou define o tipo de cópia para transferência. Valores disponíveis: `Unknown` (Desconhecida), `Copy` (Cópia) e `Full` (Completa).
`Public AgentTransferConfiguration TransferConfiguration { get; set; }`	Obtém ou define a configuração para transferência.

Método	Descrição
`public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }`	Obtém ou define a configuração para armazenamento.
`public string Key { get; set; }`	Gera uma chave pseudoaleatória (mas não protegida criptograficamente), que pode ser usada como uma senha de única vez para autenticar solicitações de transferência.
`public bool ForceBaseImage { get; set; }`	Obtém ou define o valor indicando se a imagem base foi forçada ou não.
`public bool IsLogTruncation { get; set; }`	Obtém ou define o valor indicando se a tarefa é uma truncagem de log ou não.

Tabela 7. TransferPostscriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)

Método	Descrição
`public VolumeNameCollection VolumeNames { get; set; }`	Obtém ou define a coleção de nomes de volume para transferência.
`public ShadowCopyType ShadowCopyType { get; set; }`	Obtém ou define o tipo de cópia para transferência. Valores disponíveis: `Unknown` (Desconhecida), `Copy` (Cópia) e `Full` (Completa).
`public AgentTransferConfiguration TransferConfiguration { get; set; }`	Obtém ou define a configuração para transferência.
`public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }`	Obtém ou define a configuração para armazenamento.
`public string Key { get; set; }`	Gera uma chave pseudoaleatória (mas não protegida criptograficamente), que pode ser usada como uma senha de única vez para autenticar solicitações de transferência.
`public bool ForceBaseImage { get; set; }`	Obtém ou define o valor indicando se a imagem base foi forçada.
`public bool IsLogTruncation { get; set; }`	Obtém ou define o valor indicando se a tarefa é uma truncagem de log.
`public uint LatestEpochSeenByCore { get; set; }`	Obtém ou define o valor de período mais recente.
`public Guid SnapshotSetId { get; set; }`	Obtém ou define a GUID atribuída por VSS para este instantâneo.
`public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }`	Obtém ou define o coleção de informações do instantâneo para cada volume incluído no instantâneo.

Tabela 8. TransferPrescriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)

Método	Descrição
`public VolumeNameCollection VolumeNames { get; set; }`	Obtém ou define a coleção de nomes de volume para transferência.
`public ShadowCopyType ShadowCopyType { get; set; }`	Obtém ou define o tipo de cópia para transferência. Valores disponíveis: `Unknown` (Desconhecida), `Copy` (Cópia) e `Full` (Completa).
`public AgentTransferConfiguration TransferConfiguration { get; set; }`	Obtém ou define a configuração para transferência.
`public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }`	Obtém ou define a configuração para armazenamento.
`public string Key { get; set;}`	Gera uma chave pseudoaleatória (mas não protegida criptograficamente), que pode ser usada como uma senha de única vez para autenticar solicitações de transferência.
`public bool ForceBaseImage { get; set; }`	Obtém ou define o valor indicando se a imagem base foi forçada.
`public bool IsLogTruncation { get; set; }`	Obtém ou define o valor indicando se a tarefa é uma truncagem de log.
`public uint LatestEpochSeenByCore { get; set; }`	Obtém ou define o valor de período mais recente.

Tabela 9. VirtualMachineLocation (namespace Replay.Common.Contracts.Virtualization)

Método	Descrição
`public string Description { get; set;}`	Obtém ou define uma descrição desse local, legível por humano.
`public string Method { get; set;}`	Obtém ou define o nome da máquina virtual (VM).

VolumeImageIdsCollection (namespace Replay.Core.Contracts.RecoveryPoints)

Herda seus valores do parâmetro, `System.Collections.ObjectModel.Collection<string>`.

Tabela 10. VolumeName (namespace Replay.Common.Contracts.Metadata.Storage)

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 codificada por URL do nome que pode ser passado adequadamente em um URL.

Método	Descrição
	NOTA: Há um problema conhecido em .NET 4.0 WCF (**https://connect.microsoft.com/ VisualStudio/feedback/ ViewFeedback.aspx? FeedbackID=413312**), que impede o funcionamento correto dos caracteres de escape de caminho em um modelo de URI. Como um nome de volume contém ambos "\" e "?", você deve substituir os caracteres especiais "\" e "?" por outros caracteres especiais.
`public string GetMountName()`	Retorna um nome para esse volume que é válido para a montagem da imagem de volume para algumas pastas.

VolumeNameCollection (namespace Replay.Common.Contracts.Metadata.Storage)

Herda seus valores do parâmetro, `System.Collections.ObjectModel.Collection<VolumeName>`.

Método	Descrição
`public override bool Equals(object obj)`	Determina se esta instância e um objeto especificado, que também deve ser um objeto `VolumeNameCollection`, têm o mesmo valor. (Sobrepõe `Object.Equals(Object)`.)
`public override int GetHashCode()`	Retorna o código hash para esse objeto `VolumeNameCollection`. (Sobrepõe `Object.GetHashCode()`.)

Tabela 11. VolumeSnapshotInfo (namesapce Replay.Common.Contracts.Transfer)

Método	Descrição
`public Uri BlockHashesUri { get; set;}`	Obtém ou define o URL no qual os hashes MD5 de blocos de volume podem ser lidos.
`public Uri BlockDataUri { get; set;}`	Obtém ou define o URL no qual os blocos de dados de volume podem ser lidos.

VolumeSnapshotInfoDictionary (namespace Replay.Common.Contracts.Transfer)

Herda seus valores do parâmetro, `System.Collections.Generic.Dictionary<VolumeName, VolumeSnapshotInfo>`.

Pretransferscript.ps1

O **PreTransferScript** é executado no lado do agente antes de transferir um instantâneo.

```
# 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 no lado do agente depois de transferir um instantâneo.

```
 # 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 lado do Core antes de qualquer tarefa de exportação.

```
# 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.StorageConfiguration
}
```

Postexportscript.ps1

O **PostExportScript** é executado no lado do Core depois de qualquer tarefa de exportação.

NOTA: Não há parâmetros de entrada para o **PostExportScript** quando usado para executar uma vez no agente exportado, depois da inicialização. O agente regular contém esse script na pasta de scripts do PowerShell como **PostExportScript.ps1**.

```
# 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 tarefa noturna no lado do Core. Ele tem o parâmetro **$JobClassName**, que ajuda a processar essas tarefas filhas separadamente.

```
 # 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 'AgentId:'
$NightlyAttachabilityJobRequestObject.AgentId;
                            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 'AgentId:' $RollupJobRequestObject.AgentId;
                    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 'AgentId:'
$ChecksumCheckJobRequestObject.AgentId;
                                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 depois de cada tarefa noturna no lado do Core. Ele tem o parâmetro **$JobClassName**, que ajuda a lidar com essas tarefas filhas separadamente.

```
 # 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 'AgentId:' $NightlyAttachabilityJobRequestObject.AgentId;
                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 'AgentId:' $RollupJobRequestObject.AgentId;
                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 'AgentId:' $ChecksumCheckJobRequestObject.AgentId;
                        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.Id;
                        echo 'Volumes:' $TakeSnapshotResponseObject.Volumes;
                }
                break;
```

```
            }
}
```

Amostras de script

As seguintes amostras de scripts foram fornecidas para ajudar os usuários administrativos a executar os scripts PowerShell.

Entre as amostras de scripts, etão:

- PreTransferScript.ps1
- PostTransferScript.ps1
- PreExportScript.ps1
- PostExportScript.ps1
- PreNightlyJobScript.ps1
- PostNightlyJobScript.ps1

10

Obter ajuda

Localizar a documentação e as atualizações de software

No console do AppAssure Core, há links diretos para a documentação do Dispositivo AppAssure e as atualizações do software. Para acessar os links, clique na guia **Appliance** (Dispositivo) e, em seguida, clique em **Overall Status** (Status geral). Os links para as atualizações de software e a documentação estão localizados na seção **Documentação**.

Como entrar em contato com a Dell

NOTA: Se não tiver uma conexão Internet ativa, você pode encontrar as informações de contato na sua fatura, nota de expedição, nota de compra ou no catálogo de produtos Dell.

A Dell fornece várias opções de serviço e atendimento on-line e por telefone. Se não tiver uma conexão de Internet ativa, você pode encontrar as informações de contato na sua fatura, nota de expedição, nota fiscal ou catálogo de produtos Dell. A disponibilidade varia de acordo com o país e o produto, e alguns serviços podem não estar disponíveis na sua região. Para entrar em contato com a Dell para tratar de assuntos de vendas, suporte técnico ou serviço de atendimento ao cliente, acesse **software.dell.com/support**.