Dell™ AppAssure™ 5

Guia do usuário

5.4.2

Legendas

CUIDADO: o ícone de CUIDADO indica a possibilidade de danos ao hardware ou perda de dados caso as instruções não sejam seguidas.

AVISO: o ícone de AVISO indica a possibilidade de danos à propriedade, ferimentos pessoais ou morte.

NOTA IMPORTANTE, **NOTA**, **DICA**, **MÓVEL** ou **VÍDEO:** o ícone de informações indica uma informação extra/de apoio.

Dell AppAssure 5Guia do usuário
Atualizado - Julho de 2014
Versão de software - 5.4.2

Conteúdo

1

Introdução ao AppAssure 5

Este capítulo fornece uma introdução e uma visão geral do Dell AppAssure 5. Ele descreve os recursos, a funcionalidade e a arquitetura, e consiste nos seguintes tópicos:

Sobre o AppAssure 5

O AppAssure 5 estabelece um novo padrão de proteção de dados unificada, combinando cópia de segurança, replicação e recuperação em uma única solução, projetada para ser a cópia de segurança mais rápida e confiável para a proteção de máquinas virtuais (VM), ambientes físicos e de nuvem.

O AppAssure 5 combina cópia de segurança e replicação em um produto de proteção de dados unificada e integrada, que também fornece reconhecimento do aplicativo para garantir uma recuperação confiável de dados de aplicativo a partir das cópias de segurança. O AppAssure 5 se baseia na nova arquitetura True Scale (patente pendente), que proporciona o desempenho de cópia de segurança mais rápido com objetivos de tempo de recuperação (RTO) e objetivos de ponto de recuperação (RPO) muito agressivos, próximos de zero.

O AppAssure 5 combina várias tecnologias exclusivas, inovadoras e avançadas:

- Live Recovery
- Verified Recovery
- Universal Recovery
- True Global Deduplication

Essas tecnologias são projetadas com integração segura para a recuperação após desastres na nuvem e proporcionam uma recuperação rápida e confiável. Com seu armazenamento de objetos escalável, o AppAssure 5 tem uma capacidade exclusiva de processar petabytes de dados muito rapidamente, com eliminação da deduplicação global de dados embutida, compressão, criptografia e replicação para qualquer infraestrutura de nuvem pública ou privada. Aplicativos e dados de servidor podem ser recuperados em minutos, para fins de retenção de dados e conformidade.

As ferramentas de cópia de segurança legadas atuais e ferramentas de cópia de segurança com VM da primeira geração são ineficientes e ineficazes. As ferramentas de cópia de segurança desatualizadas não têm capacidade de trabalhar com dados em grande escala e não oferecem o nível de desempenho e confiabilidade necessário para proteger aplicativos críticos para os negócios. A combinação dessas características com ambientes de TI complexos e mistos representa um desafio administrativo para os profissionais de TI e vulnerabilidades para os dados do sistema.

O AppAssure 5 enfrenta essa complexidade e ineficiência com a nossa tecnologia de core e suporte de ambientes com vários hypervisors, incluindo os que executam em VMware vSphere e Microsoft Hyper-V, que englobam nuvens públicas e privadas. O AppAssure 5 oferece esses avanços tecnológicos e, ao mesmo tempo, reduz drasticamente os custos de gerenciamento de TI e armazenamento.

Principais tecnologias do AppAssure 5

Detalhes sobre as principais tecnologias de core do AppAssure 5 são descritos nos tópicos a seguir.

Live Recovery

Live Recovery é uma tecnologia de recuperação instantânea para VMs ou servidores. Oferece acesso quase contínuo a volumes de dados em servidores virtuais ou físicos. É possível recuperar um volume inteiro com RTO próximo de zero e RPO de minutos.

a tecnologia de cópia de segurança e replicação do AppAssure 5 registra snapshots simultâneos de várias VMs ou servidores, proporcionando proteção quase instantânea de dados e do sistema. É possível retomar o uso do servidor diretamente do arquivo de cópia de segurança, sem esperar uma restauração completa para o armazenamento de produção. Os usuários mantêm a produtividade e os departamentos de TI reduzem as janelas de recuperação para cumprir os contratos de nível de serviço atuais de RTO e RPO, cada vez mais exigentes.

Verified Recovery

O Verified Recovery permite realizar testes de recuperação e confirmação de cópias de segurança de forma automatizada. Ele inclui, entre outros, os sistemas de arquivo Microsoft Exchange 2007, 2010 e 2013 e as diversas versões do Microsoft SQL Server 2005, 2008, 2008 R2 e 2012. O Verified Recovery fornece recuperabilidade de aplicativos e cópias de segurança em ambientes virtuais e físicos e oferece um algoritmo abrangente de verificação de integridade, baseado em chaves de SHA de 256 bits que verificam a correção de cada bloco do disco na cópia de segurança durante as operações de arquivamento, replicação e propagação de dados. Isso garante a identificação precoce da corrupção de dados e impede que os blocos de dados corrompidos sejam mantidos ou transferidos durante o processo de cópia de segurança.

Universal Recovery

A tecnologia Universal Recovery oferece uma flexibilidade ilimitada de restauração de máquina. É possível restaurar cópias de segurança de físico para virtual, virtual para virtual, virtual para físico ou físico para físico e fazer recuperações em hardware puro para tipos diferentes de hardware, por exemplo: P2V, V2V, V2P, P2P, P2C, V2C, C2P, C2V.

Também acelera os movimentos entre plataformas entre as máquinas virtuais, por exemplo: mover de VMware para Hyper-V ou de Hyper-V para VMware. Baseia-se na recuperação no nível de aplicativo, nível do item e nível do objeto: arquivos individuais, pastas, e-mail, itens de calendário, bancos de dados e aplicativos. Com o AppAssure 5, também é possível recuperar ou exportar de físico para a nuvem ou do virtual para a nuvem.

True Global Deduplication

O AppAssure 5 fornece a deduplicação global verdadeira, que reduz drasticamente os requisitos de capacidade do disco físico, oferecendo proporções de redução de espaço que passam de 50:1 e, mesmo assim, preenchem os requisitos de armazenamento de dados. A compressão embutida no nível do bloco da arquitetura True Scale e a deduplicação com desempenho com velocidade de linha, juntamente com a verificação de integridade embutida, impede que a corrupção dos dados afete a qualidade dos processos de cópia de segurança e arquivamento.

Recursos do produto do AppAssure 5

Usando o AppAssure 5, você pode gerenciar todos os aspectos de proteção e recuperação de dados críticos por meio dos seguintes recursos e funcionalidades. Eles incluem:

- Repositório
- True Global Deduplication
- Criptografia
- Replicação
- Recovery-as-a-Service (RaaS)
- Retenção e arquivamento
- Virtualização e nuvem
- Gerenciamento de eventos e alertas
- Portal de licenças
- Console da Web
- APIS de gerenciamento de serviço
- Atribuição de marca branca
- AppAssure 5 Assistentes

Repositório

O repositório AppAssure 5 usa o gerenciador de volume para deduplicação (DVM) para implementar um gerenciador de volume que oferece suporte para vários volumes, sendo que cada um deles pode residir em diversas tecnologias de armazenamento, como rede de área de armazenamento (SAN), armazenamento com conexão direta (DAS), armazenamento conectado à rede (NAS) ou armazenamento na nuvem. Cada volume consiste em um armazenamento de objeto escalável com deduplicação. O armazenamento de objetos escalável se comporta como um sistema de arquivos baseado em registros, em que a unidade de alocação de armazenamento é um bloco de dados com tamanho fixo, conhecido como registro. Esta arquitetura permite configurar o suporte do tamanho do bloco para compressão e deduplicação. As operações de rollup são reduzidas a operações de metadados a partir de operações com uso intenso do disco, porque o rollup não movimenta mais os dados, movimenta apenas os registros.

O DVM pode combinar um conjunto de armazenamentos de objetos em um volume, e eles podem ser expandidos pela criação de sistemas de arquivos adicionais. Os arquivos do armazenamento de objetos são pré-alocados e podem ser adicionados sob demanda conforme os requisitos de armazenamento se alteram. É possível criar até 255 repositórios independentes em um único AppAssure 5 Core e aumentar mais o tamanho de um repositório adicionando novas extensões de arquivo. Um repositório estendido pode conter até 4.096 extensões que abrangem diversas tecnologias de armazenamento. O tamanho máximo dos repositórios é 32 Exabytes. Um único core pode ter vários repositórios.

True Global Deduplication

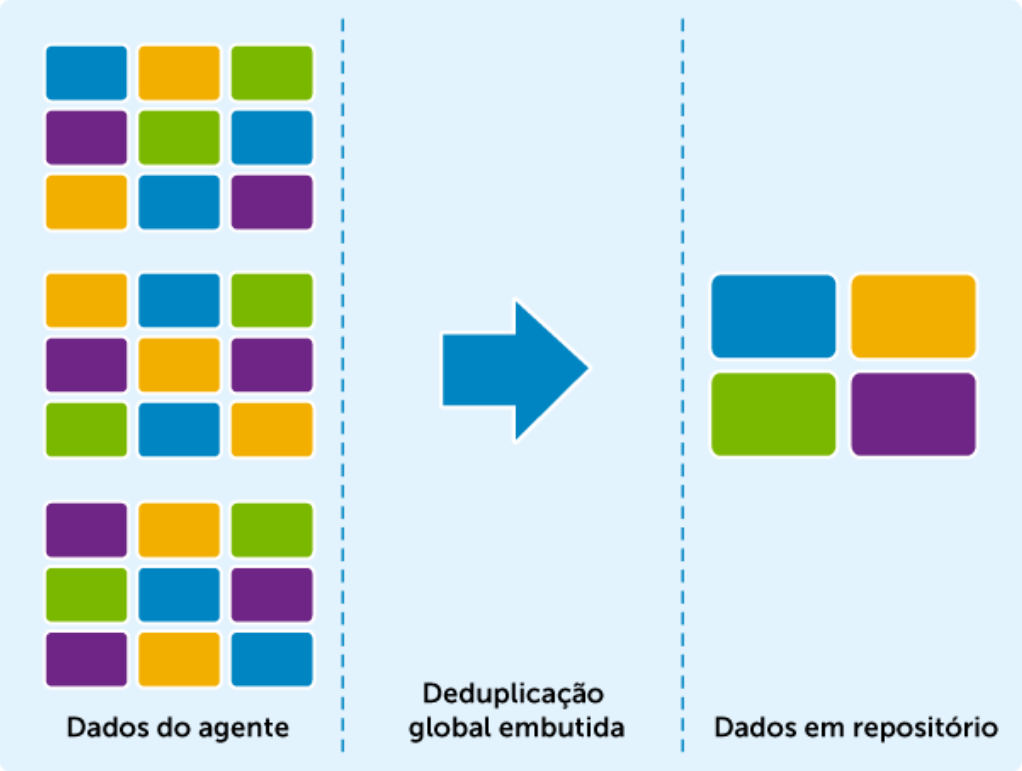
O True Global Deduplication é um método efetivo de redução das necessidades de armazenamento de cópia de segurança, eliminando dados redundantes ou deduplicados. A deduplicação é efetiva porque somente uma instância dos dados em várias cópias de segurança é armazenada no repositório. Os dados redundantes são armazenados, mas não fisicamente; eles são simplesmente substituídos por um indicador que aponta para a instância única dos dados no repositório.

Os aplicativos convencionais de cópia de segurança realizam cópias de segurança completas repetitivas semanalmente, mas o AppAssure 5 realiza cópias de segurança incrementais das máquinas no nível do bloco

para sempre. Essa abordagem incremental para sempre, em conjunto com a deduplicação de dados, ajuda a reduzir drasticamente o total de dados gravados no disco.

O layout de disco típico de um servidor é constituído pelo sistema operacional, aplicativos e dados. Na maioria dos ambientes, os administradores frequentemente usam um tipo em comum do servidor e do sistema operacional de desktop em vários sistemas, para que a implementação e o gerenciamento sejam efetivos. Quando a cópia de segurança é realizada no nível do bloco em várias máquinas ao mesmo tempo, ela fornece uma visualização mais granular daquilo que está (e do que não está) na cópia de segurança, independentemente da origem. Esses dados incluem o sistema operacional, os aplicativos e os dados de aplicativo de todo o ambiente.

Figura 1. True Global Deduplication



AppAssure 5 realiza a deduplicação de dados embutida baseada no destino. Isso significa que os dados de snapshot são transmitidos para o Core antes da deduplicação. O termo “deduplicação de dados embutida” significa simplesmente que a duplicação dos dados é eliminada antes da confirmação no disco. Isso é muito diferente da deduplicação na origem ou após o processo, na qual a duplicação dos dados é eliminada na origem antes da transmissão; no pós-processo, os dados são enviados em forma bruta para o destino, onde são analisados e a duplicação é eliminada depois da confirmação dos dados no disco. A deduplicação de dados na origem consome recursos preciosos do sistema na máquina, ao passo que a abordagem de eliminação da deduplicação de dados pós-processo requer que todos os dados necessários estejam no disco (uma sobrecarga maior de capacidade inicial) antes de começar o processo de deduplicação. Por outro lado, a deduplicação de dados embutida não requer capacidade de disco adicional e ciclos de CPU na origem nem no Core para o processo de deduplicação. Para concluir, os aplicativos convencionais de cópia de segurança realizam cópias de segurança completas repetitivas toda semana, mas o AppAssure 5 realiza cópias de segurança incrementais das máquinas no nível do bloco para sempre. Essa abordagem incremental para sempre, em conjunto com a deduplicação de dados, ajuda a reduzir drasticamente o total de dados gravados no disco, com uma proporção de redução de até 80:1.

Criptografia

O AppAssure 5 fornece criptografia integrada para proteger cópias de segurança e dados em repouso contra o uso e acesso sem autorização, garantindo a privacidade dos dados. O AppAssure 5 fornece criptografia forte. Ao fazer isso, as cópias de segurança de computadores protegidos ficam inacessíveis. Somente o usuário que tem 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 codificação (CBC) com chaves de 256 bits. A criptografia é realizada de forma embutida nos dados de snapshot, a velocidades de linha, sem afetar o desempenho. Isso acontece porque a implementação do DVM é multiprocessamento e usa a aceleração de hardware específica para o processador no qual ele está implementado.

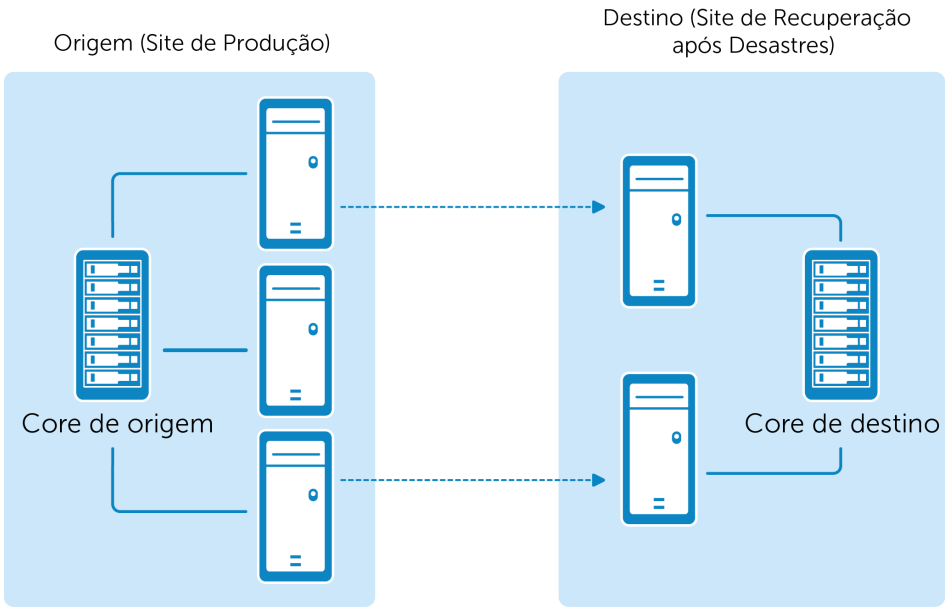
A criptografia está preparada para a multilocação. A deduplicação foi limitada especificamente aos registros que foram criptografados com a mesma chave; dois registros idênticos que foram criptografados com chaves diferentes não terão a deduplicação. Essa decisão de projeto impede que a deduplicação seja usada para vazar dados entre domínios de criptografia diferentes. Isso beneficia os provedores de serviços gerenciados, já que as cópias de segurança replicadas de vários locatários (clientes) podem ser armazenadas em um único core, sem que um locatário possa ver ou acessar os dados de outros locatários. Cada chave de criptografia de um locatário ativo cria um domínio de criptografia dentro do repositório, no qual somente o proprietário das chaves pode ver, acessar ou usar os dados. Em um cenário de multilocação, os dados são particionados e deduplicados dentro dos domínios de criptografia.

Nos cenários de replicação, o AppAssure 5 usa o SSL 3.0 para proteger as conexões entre os dois cores em uma topologia de replicação para impedir espionagem e adulteração.

Replicação

Replicação é o processo de copiar pontos de recuperação e transmiti-los a um local secundário para fins de recuperação após desastres. O processo exige uma solução com pares de origem/destino entre dois cores. A replicação é gerenciada por máquina protegida, ou seja, os snapshots de cópia de segurança de uma máquina protegida são replicados para o core da réplica de destino. Quando a replicação está configurada, o core de origem transmite de forma assíncrona e contínua os dados do snapshot incremental para o core de destino. É possível configurar essa replicação de saída para o data center da sua empresa ou para o site remoto de recuperação após desastres (ou seja, um core de destino “autogerenciado”) ou para um provedor de serviços gerenciados (MSP) que fornece serviços de cópia de segurança e recuperação após desastres fora do local. Ao replicar para um MSP, é possível usar fluxos de trabalho incorporados que permitem solicitar conexões e receber notificações de feedback automáticas.

Figura 2. Replicação



A replicação se otimiza com um algoritmo exclusivo de leitura-correspondência-gravação (RMW) acoplado fortemente à deduplicação. Na replicação RMW, o serviço de replicação de origem e destino faz a correspondência das chaves antes de transferir dados e, em seguida, replica somente os dados compactados, criptografados e de deduplicação pela WAN. Ao fazer isso, reduz em 10x os requisitos de largura de banda.

A replicação começa pela propagação, ou seja, a transferência inicial de imagens de base de deduplicação e snapshots incrementais dos agentes protegidos, que pode adicionar centenas ou milhares de gigabytes de dados. A replicação inicial pode ser propagada para o core de destino usando mídias externas. Normalmente, isso é útil para grandes conjuntos de dados ou sites com links lentos. Os dados do arquivo de propagação são compactados e criptografados e a duplicação é eliminada. Se o tamanho total do arquivo for superior ao espaço disponível na mídia removível, o arquivo pode ocupar vários dispositivos, com base no espaço disponível nas mídias. Durante o processo de propagação, os pontos de recuperação incremental replicam para o site de destino. Depois que o core de destino consome o arquivo de propagação, os pontos de recuperação incremental recém-replicados são sincronizados automaticamente.

Recovery-as-a-Service (RaaS)

Os provedores de serviços gerenciados (MSPs) podem aproveitar totalmente o AppAssure 5 como uma plataforma para oferecer a recuperação como serviço (RaaS). A RaaS facilita a recuperação completa na nuvem replicando os servidores físicos e virtuais do cliente, juntamente com seus dados, para a nuvem do provedor de serviços como máquinas virtuais para suportar o teste de recuperação ou operações reais de recuperação. Os clientes que desejam realizar recuperação na nuvem podem configurar a replicação nas máquinas protegidas nos cores locais para um provedor de serviços do AppAssure. Em caso de desastre, os MSPs podem realizar instantaneamente o provisionamento das máquinas virtuais para o cliente.

Os MSPs podem implementar uma infraestrutura de RaaS com multilocação baseada em AppAssure 5 que pode hospedar várias organizações ou unidades de negócios separadas (os locatários), que normalmente não compartilham segurança ou dados em um único servidor ou um grupo de servidores. Os dados de cada locatário são isolados e protegidos de outros locatários e do provedor de serviço.

Retenção e arquivamento

O AppAssure 5 oferece políticas flexíveis de cópia de segurança e retenção fáceis de configurar. A capacidade de ajustar as políticas de retenção às necessidades de uma organização não só ajuda a preencher os requisitos de conformidade, mas também faz isso sem comprometer os objetivos de tempo de recuperação (RTO).

As políticas de retenção impõem períodos de tempo em que as cópias de segurança são armazenadas em mídias de curto prazo (rápidas e caras). Às vezes, certos requisitos técnicos e de negócios exigem a retenção prolongada dessas cópias de segurança, mas o armazenamento rápido tem um custo proibitivo. Portanto, esse requisito gera uma necessidade de armazenamento de longo prazo (lento e barato). As empresas frequentemente usam o armazenamento de longo prazo para arquivar dados de conformidade e não conformidade. O recurso de arquivamento suporta retenções prolongadas para dados de conformidade e não conformidade, além de ser usado para propagar dados de replicação para um core de destino.

Figura 3. Política de retenção

No AppAssure 5, as políticas de retenção podem ser personalizadas para especificar o tempo durante o qual um ponto de recuperação de cópia de segurança é mantido. Conforme o fim do período de retenção dos pontos de recuperação se aproxima, eles vencem e são removidos do grupo de retenção. Normalmente, esse processo se torna ineficiente e acaba falhando, já que a quantidade de dados e o período de retenção começam a aumentar rapidamente. O AppAssure 5 resolve o problema do big data gerenciando a retenção de grandes quantidades de dados com políticas de retenção complexas e realizando operações de rollup para dados que estão vencendo, por meio de operações eficientes de metadados.

É possível realizar cópias de segurança com um intervalo de poucos minutos, e essas cópias de segurança vencem em dias, meses e anos. As políticas de retenção gerenciam o vencimento e a exclusão de cópias de segurança antigas. Um método simples em cascata define o processo de vencimento. Os níveis dentro da cascata são definidos em minutos, horas e dias; semanas, meses e anos. A política de retenção é imposta pelo processo noturno de rollup.

Para o arquivamento de longo prazo, o AppAssure 5 permite criar um arquivo do core de origem ou destino em qualquer mídia removível. O arquivo é otimizado internamente, e todos os dados do arquivo são compactados, criptografados e têm deduplicação. Se o tamanho total do arquivo for superior ao espaço disponível na mídia removível, o arquivo ocupará vários dispositivos com base no espaço disponível nas mídias. A recuperação a partir de um arquivo não requer um novo core; qualquer core pode ingerir o arquivo e recuperar dados se o administrador tiver a frase de acesso e as chaves de criptografia.

Virtualização e nuvem

O AppAssure 5 Core está preparado para a nuvem, ou seja, você pode utilizar a capacidade computacional da nuvem para a recuperação.

O AppAssure 5 pode exportar qualquer máquina protegida ou replicada para máquinas virtuais, como as versões licenciadas do VMware ou Hyper-V. As exportações podem ser ad hoc (uma de cada vez) ou contínuas. Nas exportações contínuas, a máquina virtual é atualizada de forma incremental depois de cada snapshot. As atualizações incrementais são muito rápidas e fornecem clones em estado de espera prontos para serem acionados com um clique em um botão. Os tipos suportados de exportação de máquina virtual são Workstation/Server do VMware em uma pasta, exportação direta para um host do vSphere/VMware ESX(i), exportação para o Oracle VirtualBox, Microsoft Hyper-V Server 2008 R2 e Hyper-V for Windows Server 2012 R2.

Gerenciamento de eventos e alertas

Além das APIs de REST HTTP, o AppAssure também inclui um conjunto amplo de recursos para a criação de logs e a notificação de eventos usando e-mail, syslog ou o Log de Eventos do Windows. As notificações por e-mail podem ser usadas para alertar os usuários ou grupos sobre o funcionamento ou o status de diversos eventos em resposta a um alerta. Os métodos do syslog e do Log de Eventos do Windows são usados para a criação de logs centralizada em um repositório, em ambientes com vários sistemas operacionais; por outro lado, em ambientes que só têm Windows, apenas o Log de Eventos do Windows é usado.

Portal de licenças

O Portal de licenças de software da Dell fornece ferramentas fáceis de usar para gerenciar os diretos de licença. É possível baixar, ativar, ver e gerenciar chaves de licença e criar um perfil de empresa para rastrear os ativos de licença. Além disso, o portal permite que os provedores de serviços e revendedores rastreiem e gerenciem as licenças de cliente.

Console da Web

O AppAssure 5 tem um console central baseado na Web que gerencia cores AppAssure 5 distribuídos a partir de um local central. Os MSPs e clientes corporativos com vários cores distribuídos podem implementar esse console para obter uma visualização unificada para um gerenciamento centralizado. O AppAssure 5 Central Management Console permite organizar os cores gerenciados em unidades organizacionais hierárquicas. Essas unidades organizacionais podem representar unidades de negócios, locais ou clientes para os MSPs com acesso baseado em função. Usando o console central, você também pode executar relatórios em todos os cores gerenciados.

APIS de gerenciamento de serviço

O AppAssure 5 vem com um conjunto de APIs de gerenciamento de serviços e fornece acesso programático a todas funcionalidades disponíveis por meio do AppAssure 5 Central Management Console. A API de gerenciamento de serviços é uma API de REST. Todas as operações de API são realizadas em SSL e autenticadas mutuamente por meio de certificados X.509 v3. O serviço de gerenciamento pode ser acessado de dentro do ambiente ou diretamente pela Internet, a partir de qualquer aplicativo que possa enviar e receber solicitações e respostas de HTTPS. A abordagem facilita a integração fácil a qualquer aplicativo da Web, como ferramentas de metodologia de gerenciamento de relacionamentos (RMM) ou sistemas de faturação. Um cliente de SDK para criação de scripts em PowerShell também está incluído no AppAssure 5.

Atribuição de marca branca

O AppAssure pode ter a marca alterada ou ser comercializado sem marca para parceiros corporativos e de OEM selecionados, de acordo com o programa de provedor de serviço Platinum. Com o programa de provedor de serviço Platinum, os parceiros podem usar seu nome, logotipo e cores no AppAssure, e fornecer o produto ou serviço com sua própria marca e visual para os clientes.

Como parceiro AppAssure, você pode ajustar o software para preencher seus requisitos de negócios. Para saber mais sobre o uso da sua marca AppAssure para suprir as suas necessidades de negócios, entre em contato com as AppAssurevendas pelo endereço sales@appassure.com para obter mais informações.

AppAssure 5 Assistentes

O assistente é um conjunto de etapas guiadas apresentadas ao usuário em uma janela pop-up para automatizar uma tarefa complexa ou mais. Por definição, os assistentes contêm duas páginas de informações (ou mais) para o usuário preencher. (Um pop-up de janela única é considerado simplesmente como uma caixa de diálogo). Os assistentes usam diversas convenções gráficas bastante conhecidas para coletar informações, como caixas de texto, botões de opções, caixas de verificação e menus suspensos.

Quando um assistente é iniciado, uma janela se abre acima da interface do usuário e o orienta em uma série de opções necessárias para realizar a tarefa. Você segue as informações apresentadas em cada página do assistente, conforme os seus requisitos, navegando pelas páginas do assistente por meio dos botões **Avançar** e **Voltar** . Ao terminar, você clica em um botão de enviar (para confirmar suas opções e realizar a tarefa) ou no botão **Cancelar** (para cancelar sem fazer alterações e voltar à UI a partir da qual você abriu o assistente).

O AppAssure 5 oferece vários assistentes, que podem ser divididos em duas categorias.

Primeiramente, há assistentes para instalar, atualizar ou remover o software AppAssure 5 e os componentes relacionados. Normalmente, eles são iniciados ao clicar duas vezes em um programa executável de instalador de software. Os instaladores podem ser acessados ao fazer o download de componentes específicos a partir do Portal de licenças de software da Dell.

Em segundo lugar, os assistentes estão disponíveis na interface de usuário do Core Console do AppAssure 5. Normalmente, eles são lançados ao clicar em um botão ou link rotulado com a função ou o resultado do assistente. Os assistentes dessa categoria são listados a seguir.

Tabela 1.

Nome do assistente	Iniciado por	Descrição
Guia de início rápido	Opção Guia de início rápido (menu Ajuda)	Unifica vários fluxos de trabalho para simplificar tarefas comuns do AppAssure 5. Guia o usuário no processo de proteger máquinas, configurar a replicação em novos agentes, exportar dados protegidos para máquinas virtuais, criptografar dados dos pontos de recuperação, configurar grupos de notificação por e-mail e configurar uma política de retenção.
Assistente de proteção de máquina	Botão Proteger máquina (barra de botões)	Configura a proteção em uma máquina que você especifica. Permite dar um nome à máquina para ser exibido no console do Core. Se o software Agent já estiver instalado, ele permite selecionar volumes para a proteção. Caso contrário, o assistente instalará o software e protegerá todos os volumes. Configura uma programação padrão de proteção ou permite configurar uma programação personalizada. Nas definições avançadas, é possível escolher (ou criar) um repositório e estabelecer a criptografia para os dados protegidos.
Assistente de proteção de diversas máquinas	Botão Proteção em massa (guia Inicial)	Configura a proteção em várias máquinas que você especifica, a partir de um servidor de domínio do Active Directory do Windows, um host virtual do VMware vCenter Server/ESX(i) ou manualmente (inserindo uma lista em um formato especificado).
Assistente de replicação	Link Adicionar core de destino (guia Replicação)	Configura a replicação a partir de um core primário (ou de origem) para que uma cópia dos dados protegidos esteja sempre disponível em um core de destino separado.
Assistente de restauração de máquina	Botão Restaurar (barra de botões)	Orienta durante o processo de restaurar dados a partir de um ponto de recuperação no core para uma máquina protegida.
Assistente de exportação	Botão Exportar (barra de botões), link Adicionar (guia Standby virtual)	Exporta dados do ponto de recuperação de uma máquina protegida para uma máquina virtual em qualquer formato de VM suportado. É possível realizar uma exportação única ou configurar o standby virtual para a exportação contínua.

Normalmente os assistentes definem ou configuram recursos no AppAssure 5, mas é possível modificar posteriormente a maioria desses aspectos a partir da guia Configuração no Console de Core.

2

Trabalho com o AppAssure 5 Core

Este capítulo descreve os vários aspectos do trabalho, configuração e gerenciamento do AppAssure 5 Core. Os seguintes tópicos estão incluídos:

- Acesso ao AppAssure 5 Core Console
- Navegação no AppAssure 5 Core Console
- Visualização e gerenciamento de máquinas protegidas
- Sobre o Guia de início rápido
- Sobre grupos personalizados
- Roteiro para configuração do AppAssure 5 Core
- Gerenciamento de licenças
- Gerenciamento das definições do AppAssure 5 Core
- Sobre repositórios
- Roteiro de gerenciamento de repositório
- Sobre o Trabalho de verificação da integridade do repositório
- Gerenciamento da segurança
- Gerenciando contas em nuvem
- Sobre a replicação
- Roteiro para definição da replicação
- Replicar em um core de destino autogerenciado
- Processo de replicação em um core de destino de terceiros
- Adição de uma máquina a uma replicação existente
- Consumo da unidade de seeding em um core de destino
- Gerenciamento definições de replicação
- Remoção da replicação
- Recuperação de dados replicados
- Roteiro de ativação e reativação pós-falha
- Gerenciamento de eventos
- Gerenciamento da recuperação
- Sobre informações do sistema
- Download de instaladores
- Sobre o Agent Installer
- Sobre o Local Mount Utility
- Gerenciamento das políticas de retenção
- Roteiro para arquivar em uma nuvem
- Noções básicas sobre arquivos

- Gerenciamento da capacidade de anexação do SQL e truncamento de log
- Gerenciamento de verificações da capacidade de montagem do banco de dados do Exchange e truncamento de log
- Indicadores de status de ponto de recuperação

Acesso ao AppAssure 5 Core Console

Execute as seguintes etapas para acessar o AppAssure 5 Core Console.

Para acessar o AppAssure 5 Core Console

- Execute um dos seguintes para acessar o AppAssure 5 Core Console:
  a Efetue login localmente no seu server do AppAssure 5 Core e depois selecione o ícone **Core Console**.
  b Ou digite uma das seguintes URLs no seu navegador da Web:
    - https://<yourCoreServerName>:8006/apprecovery/admin/core ou
    - https://<yourCoreServerIPaddress>:8006/apprecovery/admin/core

  NOTA: Como a interface do usuário do AppAssure 5 Core Console é dependente do JavaScript, o navegador da Web usado para acessar o Core Console deve ter o JavaScript ativado.

Navegação no AppAssure 5 Core Console

Ao efetuar login no AppAssure 5 Core Console na versão 5.4 e posterior, aparecerá uma interface do usuário (UI) atualizada. Os aspetos dessa nova UI são descritos na tabela a seguir.

Tabela 2.

Elemento da interface do usuário	Descrição
Guia de início rápido	O Guia de início rápido é um fluxo guiado de tarefas sugeridas para configurar e usar o AppAssure 5. A partir da versão 5.4, esse guia é aberto automaticamente cada vez que você efetuar login no Core Console (isso pode ser desativado). Também é possível abrir o Guia de início rápido a partir do novo menu Ajuda. Para obter mais informações sobre o Guia de início rápido, consulte Sobre o Guia de início rápido.
Barra de ícones	Inclui um ícone para cada guia do Core Console: Início, Replicação, Standby virtual, Eventos, Ferramentas e Configuração.
Menu Máquinas protegidas	Nesse menu é possível executar todas as ações antes acessíveis apenas na guia Máquinas. Para obter mais informações, consulte Visualização e gerenciamento de máquinas protegidas.

Tabela 2.

Elemento da interface do usuário	Descrição
Barra de botões	Contém botões acessíveis de qualquer lugar do Core Console, incluindo Proteger, Restaurar e Exportar. Esses botões iniciam assistentes para realizar tarefas frequentes, como proteger uma máquina, executar uma restauração a partir de um ponto de recuperação ou exportar dados para uma máquina virtual. O comportamento padrão ao clicar no botão **Proteger** é iniciar o Assistente de proteção de máquina. Além disso, o botão Proteger inclui três opções em um menu suspenso. A opção **Proteger máquina** também inicia o Assistente de proteção de máquina. A opção **Proteger cluster** permite que você se conecte a um cluster de servidor. A opção **Proteção em massa** abre o assistente de proteção de diversas máquinas para permitir que você proteja duas ou mais máquinas ao mesmo tempo.
Contagem de tarefas em execução	Mostra quantos trabalhos estão em execução no momento. Isso é dinâmico e se baseia no estado do sistema. Se clicar no menu suspenso, você verá um resumo do status de todos os trabalhos em execução. Clicando no X de um trabalho, é possível selecionar o cancelamento desse trabalho.
Menu suspenso de Ajuda	Este menu inclui as seguintes opções: **Ajuda** (que é link para o site Documentação do AppAssure 5), **Suporte** (que é link para o site Suporte do AppAssure 5, oferecendo acesso ao Live Chat, solicitações de suporte, conhecimento desses artigos e mais), Guia de início rápido (descrito acima), e **Sobre** (que abre a caixa de diálogo Sobre o Core AppAssure 5, incluindo informações sobre a versão).
Data e hora do servidor	A hora e a data atuais da máquina que executa o serviço do AppAssure 5 Core aparecem no canto superior direito do Core Console. Essa é o horário usado pelo sistema para os eventos. Por exemplo, ao aplicar as programações de proteção, o horário exibido no Core Console é usado. Isso é verdadeiro mesmo que o fuso horário seja diferente no server de banco de dados ou na máquina cliente onde o navegador está sendo executado.
Ajuda sensível ao contexto	No AppAssure 5 Core Console, cada vez que você clicar no ícone **Ajuda** (uma interrogação azul), uma janela redimensionável do navegador é aberta com dois frames. O frame esquerdo contém uma árvore de navegação que mostra os tópicos do *Guia do usuário do AppAssure 5*. O frame direito exibe o conteúdo para o tópico de ajuda selecionado. A qualquer momento, a árvore de navegação de ajuda se expande para exibir a localização do tópico selecionado em sua hierarquia. É possível procurar em todos os tópicos do Guia do usuário utilizando esse recurso de ajuda sensível ao contexto. Feche o navegador quando você terminar de pesquisar tópicos.

Os elementos conhecidos da UI incluem uma área de navegação à esquerda, o logotipo AppAssure (com links para o site de Suporte AppAssure 5 com links diretos para a Documentação do AppAssure) e um conjunto de controles em guias, conhecido como AppAssure 5 Core Console.

NOTA: Os usuários de versões anteriores talvez notem que a página Máquinas protegidas, anteriormente acessível na guia Máquinas, ao lado da guia Início do Core Console, foi movida. Todas as funções das máquinas protegidas agora podem ser acessadas no menu Máquinas protegidas na área de navegação à esquerda. Também é possível abrir a página Máquinas protegidas clicando no menu Máquinas protegidas.

Ao efetuar o login no Core Console, e ao clicar no ícone ou na guia Início a qualquer momento, a guia Início aparecerá e será automaticamente selecionada. É possível navegar para qualquer outra guia clicando no nome dela ou no ícone correspondente.

As outras guias acessíveis no Core na versão 5.4 e posterior incluem Replicação, Standby virtual, Eventos, Ferramentas e Configuração.

Visualização e gerenciamento de máquinas protegidas

Na interface do usuário do AppAssure 5, a partir da versão 5.4, aparece um menu Máquinas protegidas na área de navegação à esquerda. Por padrão, ele mostra uma lista de máquinas protegidas por esse Core (caso tenham sido configuradas).

NOTA: Antes das máquinas serem adicionadas ao Core para proteção, o menu Máquinas protegidas não tem máquinas relacionadas.

O menu Máquinas protegidas inclui um menu suspenso que relaciona as funções que podem ser realizadas em todas as máquinas protegidas. Clique na seta à direita de Máquina protegida para ver o menu e executar um dos seguintes:

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

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

- Forçar um snapshot da máquina selecionada (é possível escolher volumes na máquina e escolher um snapshot incremental ou uma imagem de base)
- Pausar a proteção da máquina selecionada (se estiver ativa)
- Retomar proteção (se estiver em pausa)
- Atualizar metadados
- Navegar até a guia Resumo da máquina selecionada
- Navegar até a guia Pontos de recuperação da máquina selecionada
- Navegar até a guia Eventos da máquina selecionada
- Navegar até a guia Ferramentas da máquina selecionada (ou selecionar qualquer função)
- Navegar até a guia Configuração da máquina selecionada
- Criar um rótulo personalizado exibido na lista de Máquinas protegidas

Se estiver gerenciando clusters a partir do core do AppAssure 5, o cluster também aparecerá no menu de navegação à esquerda. No menu suspenso de qualquer cluster, também é possível:

- Navegar até a guia Nós protegidos do cluster selecionado

Usando submenus suspensos expansíveis, é possível navegar rapidamente até determinadas funções de uma máquina.

- É possível acessar todas as funções na guia Ferramentas de uma máquina a partir do submenu suspenso expansível Ferramentas.
- É possível acessar todas as funções na guia Configuração de uma máquina a partir do submenu suspenso expansível Configuração.

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

Clique em qualquer máquina do menu Máquinas protegidas para abrir a guia Resumo dessa máquina. Para obter mais informações sobre o que você pode realizar na guia Resumo, consulte Sobre a guia Resumo.

Finalmente, clique diretamente no menu Máquinas protegidas para mostrar a guia Máquinas ou Máquinas protegidas na área de navegação principal, substituindo as guias Início, Replicação, Standby virtual, Eventos, Ferramentas e Configuração.

NOTA: Da guia Máquinas, é possível voltar à visualização de várias guias clicando no ícone Início na barra de ícones da área de navegação à esquerda.

Na guia Máquinas, no menu Ações, é possível proteger uma, duas ou mais máquinas ao mesmo tempo (proteção em massa), ou proteger um cluster. É possível implementar o software do Agent a uma ou múltiplas máquinas (implementação em massa) ou iniciar o assistente de Restauração de máquinas.

Ao selecionar qualquer máquina protegida, é possível, a partir do menu de configurações específico dela, forçar um snapshot, forçar o truncamento de arquivos de log de SQL, exportar para uma máquina virtual, montar um ponto de recuperação, visualizar pontos de recuperação para essa máquina, restaurar a máquina selecionada ou remover a proteção da máquina selecionada.

Sobre a guia Resumo

A guia Resumo é exibida como a primeira guia no AppAssure 5 Core Console quando você seleciona uma máquina do agente protegido. Ela contém, no mínimo, um painel de Resumo e um painel de Volumes.

Sobre o painel de Resumo

O painel de Resumo contém informações resumidas sobre a máquina protegida, incluindo o nome do host, a data e a hora do último snapshot, a data e a hora do próximo snapshot agendado, as informações sobre a chave de criptografia, e a versão do software do Agent carregada nessa máquina. Há um menu de Ações descrito abaixo.

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

Para todas as máquinas protegidas, no menu suspenso Ações do painel de Resumo, é possível fazer o seguinte:

- **Exportar uma máquina protegida para uma máquina virtual** utilizando uma exportação de uma vez ou atualizações contínuas a uma máquina virtual exportada. Para obter mais informações, consulte Sobre exportação de dados protegidos de máquinas com Windows para máquinas virtuais.
- **Pausar proteção para essa máquina**. Para obter mais informações, consulte Pausa e retomada da proteção.
- **Atualizar os metadados para essa máquina**. Para atualizar os metadados para uma máquina, no menu suspenso Ações, clique em **Atualizar metadados**.
- **Remover essa máquina da proteção**, escolhendo excluir ou manter os pontos de recuperação. Para obter mais informações, consulte Remoção de uma máquina.

As opções exibidas no menu suspenso Ações do painel de Resumo podem ser diferentes dependendo do tipo de máquina selecionada. Por exemplo, os SQL Servers incluem uma opção SQL com funções relacionadas no menu Ações. Os Servers Exchange incluem uma opção Exchange no menu de ações.

Para as máquinas do SQL Server protegidas, no menu suspenso Ações do painel de Resumo, é possível fazer o seguinte:

- **Forçar truncamento de log.** Para uma máquina do SQL Server, é possível forçar o truncamento dos registros do SQL Server, que identifica espaço livre no server do SQL. Para obter mais informações, consulte Forçamento do truncamento de log para uma máquina com SQL ou com Exchange.
- **Definir as credenciais do SQL Server.** Para uma máquina do SQL Server, é possível definir credenciais padrão para todas as instâncias, ou definir credenciais da instância para uma instância única. Para obter mais informações, consulte Definição de credenciais para SQL Servers.

Para as máquinas do Exchange Server protegidas, no menu suspenso Ações do painel de Resumo, é possível fazer o seguinte:

- **Forçar truncamento de log.** Para uma máquina do Exchange Server, é possível forçar o truncamento dos logs do Exchange, que libera espaço no server do Exchange. Para obter mais informações, consulte Forçamento do truncamento de log para uma máquina com SQL ou com Exchange.
- **Definir credenciais do Exchange Server.** Para uma máquina do Exchange Server, é possível definir ou modificar as configurações do Exchange Server, incluindo forçar o truncamento dos logs do Exchange Server, ou configurar credenciais para uma instância do server Exchange. Para obter mais informações, consulte Definição de credenciais para os Exchange Servers.

Sobre o Painel de Volumes

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

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

Sobre o Guia de início rápido

O Guia de início rápido é um recurso disponível no AppAssure 5 na versão 5.4 e posterior. Esse recurso fornece um fluxo guiado de tarefas sugeridas para configurar e usar o AppAssure 5.

O Guia de início rápido é exibido automaticamente na primeira vez em que você atualiza ou instala o AppAssure 5 Core e navega até o Core Console. Clique na página Bem-Vindo do **Guia de início** para ver as várias tarefas de configuração sugeridas. Navegue pelo guia usando as opções **Ignorar etapa** e **Voltar**. Quando tiver visto a última tarefa sugerida, clique em **Concluir** para fechar o guia.

É possível iniciar o Guia de início rápido novamente a qualquer momento. Também é possível ocultar a página Bem-Vindo do Guia de início rápido. Para obter mais informações sobre essas opções, consulte Início do Guia de início rápido.

A menos que você o oculte, o Guia de início rápido reaparecerá toda vez que for efetuado login no AppAssure 5 Core Console e acessada a guia Início. Para obter mais informações, consulte Ocultação do Guia de início rápido.

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

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

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

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

Tabela 3.

Função	Descrição resumida	Resultado da seleção da tarefa/link para o procedimento
Proteção	Proteção de uma máquina agente, um cluster de servers ou várias máquinas usando a proteção em massa	Clique em Proteger ou selecione **Proteger máquina** no menu suspenso para abrir o Assistente de proteção de máquina. Para obter informações sobre como executar o Assistente de proteção de máquina, consulte Proteção de uma máquina. Selecione **Proteger cluster** no menu suspenso para abrir a caixa de diálogo Conectar-se ao cluster. Para obter mais informações sobre como proteger um cluster, consulte Proteção de um cluster. Selecione **Proteção em massa** para abrir o Assistente de proteção de diversas máquinas. Para obter informações sobre como executar o Assistente de proteção de diversas máquinas, consulte Proteção de várias máquinas.
Replicação	Configuração da replicação de um core principal (origem) para um secundário (de destino)	Clique em **Replicação** para abrir a guia Replicação. É solicitado que um core de destino seja adicionado usando o Assistente de replicação. Para obter informações sobre o uso do Assistente de replicação para configurar a replicação em um core autogerenciado, consulte Replicar em um core de destino autogerenciado. Para obter informações gerais sobre replicação, consulte Roteiro para definição da replicação.
Exportação virtual	Realização de uma exportação única ou estabelecimento de exportação contínua de uma máquina agente protegida para uma máquina virtual	Clique em **Exportar** para realizar uma exportação de dados de sua máquina protegida para uma máquina virtual. É possível realizar uma exportação única ou configurar o standby virtual para exportação contínua para uma VM. Para obter informações sobre exportações virtuais, consulte Sobre exportação de dados protegidos de máquinas com Windows para máquinas virtuais.
Configuração	Permite definir configurações adicionais para o AppAssure 5 Core	Clique em **Configuração** para ver configurações de segurança (configuração de chaves de criptografia), notificações (configuração das notificações de eventos) e políticas de retenção (definição de critérios para rollup de pontos de recuperação do envelhecimento).
Configuração: Criptografia	Configuração de chave de criptografia que pode ser usada por um ou mais agentes	Clique em **Segurança** para abrir a página Segurança na guia Configuração. Solicita que você adicione uma chave de criptografia ou importe uma. Depois de fazer isso, você pode aplicá-la a um ou mais agentes. A criptografia é descrita no tópico Gerenciamento da segurança.
Configuração: Notificações	Configuração de notificações de eventos, avisos e alertas	Clique em **Eventos** para especificar os grupos de notificação de eventos, avisos e alertas. Para enviar estas informações por e-mail, você também deve estabelecer as definições do server de SMTP. Para obter informações sobre o gerenciamento de eventos, consulte o tópico Gerenciamento de eventos, incluindo os tópicos Configuração de grupos de notificação e Configuração de um server de e-mail.

Tabela 3.

Função	Descrição resumida	Resultado da seleção da tarefa/link para o procedimento
Configuração: Retenção	Visualização ou alteração da política de retenção padrão do Core	Clique em **Política de retenção** para abrir a página Política de retenção na guia Configuração. Daqui, é possível definir quanto tempo manter um ponto de recuperação antes de realizar rollup nele. Para obter informações conceituais sobre políticas de retenção, consulte o tópico Retenção e arquivamento. Para obter informações de procedimento, consulte Gerenciamento das políticas de retenção.
Restaurar	Restauração de dados de um ponto de recuperação do Core	Clique em **Restaurar** para abrir o Assistente de restauração de máquinas. Para obter mais informações sobre como restaurar dados, consulte o tópico Restauração de volumes a partir de um ponto de recuperação.

Início do Guia de início rápido

O Guia de início rápido é exibido automaticamente na primeira vez em que você atualiza ou instala o AppAssure 5 Core. A menos que você o oculte, o guia reaparece toda vez que você acessa a guia Início do Core Console.

Use o procedimento abaixo para abrir o Guia de início rápido a qualquer momento no Core Console.

Para iniciar o Guia de início rápido

1. Navegue até o AppAssure 5 Core Console.
2. No menu Ajuda, selecione **Guia de início rápido**.

   O Guia de início rápido é exibido.

Ocultação do Guia de início rápido

O Guia de início rápido é exibido automaticamente na primeira vez em que você atualiza ou instala o AppAssure 5 Core.

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

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

Para ocultar o Guia de início rápido a partir da página Bem-Vindo

- No AppAssure 5 Core Console, se a página Bem-Vindo do Guia de início rápido estiver aberta, faça o seguinte:
  - Se quiser ocultar a página Bem-Vindo do Guia de início rápido, selecione **Não exibir novamente**.

    NOTA: Essa opção ocultará a página Bem-Vindo da próxima vez que o Guia de início for aberto e todas as vezes seguintes até que o AppAssure 5 Core seja atualizado.

  - Se desejar ocultar o Guia de início rápido nesta sessão, clique em **Fechar**.

    O Guia de início rápido é fechado. Da próxima vez que for acessada a guia Início no Core Console, o Guia de início rápido reaparecerá.

    Também é possível abrir o Guia de início rápido no menu Ajuda, como descrito em Início do Guia de início rápido.

Para ocultar o Guia de início rápido a partir de qualquer página dele

- Em qualquer página do Guia de início rápido, clique em **Sair do guia.**

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

Sobre grupos personalizados

O AppAssure 5 Core mostra um menu Máquinas protegidas na área de navegação à esquerda. Ele inclui todas as máquinas adicionadas para proteção no seu AppAssure 5 Core. Se houver clusters protegidos, eles também aparecerão no menu Máquinas protegidas. Abaixo deles, se houver máquinas replicadas, elas aparecerão em um menu de máquinas replicadas sob o nome do Core replicado. É possível realizar ações de grupo para todas as máquinas dispostas sob um desses menus selecionando a seta à direita do nome do menu para acessar o menu suspenso.

Da mesma forma, é possível criar um grupo personalizado para ser exibido na área de navegação à esquerda, conforme descrito em Criação de grupos personalizados.

O ato de criar um grupo sempre acrescenta um membro do grupo (um agente protegido, cluster de servers ou agente replicado, com base em como foi iniciada a criação do grupo) ao novo grupo personalizado. O ideal é, então, adicionar mais membros ao grupo. Depois disso, é possível executar ações de grupo que se aplicam a todos os membros desse grupo personalizado, conforme descrito em Realização de ações de grupo.

Os grupos personalizados podem incluir agentes protegidos, agentes replicados e clusters de servers. Os clusters de servers se comportam igual aos agentes protegidos, exceto que um cluster de servers e seus nós se comportam como uma única entidade. Se você tentar adicionar um nó de um cluster de servers a um grupo, todo o cluster será adicionado.

Um grupo personalizado pode conter membros semelhantes ou diferentes. Para grupos de membros semelhantes, todas as ações do grupo se aplicam a todos os membros do grupo. Por exemplo, se você forçar um snapshot de um grupo personalizado de agentes protegidos, será feita cópia de segurança de cada agente. Para grupos com membros diferentes (por exemplo, agentes replicados e protegidos), se você aplicar uma ação de grupo, como forçar a replicação, isto se aplicará apenas aos agentes replicados.

É possível criar um ou mais grupos. Um único agente ou máquina replicada pode ser incluído em um ou mais grupos. Dessa forma, é possível agrupar máquinas em seu core da forma que você escolher e executar ações nesse grupo específico.

Cada grupo personalizado aparece na área de navegação à esquerda, com um rótulo que você atribuir. Os grupos com agentes protegidos padrão aparecem primeiro no grupo personalizado e os agentes replicados aparecem abaixo, conforme aplicável.

Incluir uma máquina em um grupo não a remove de seu local original. Por exemplo, se você tiver três máquinas protegidas chamadas Agente1, Agente2 e Agente3 e adicionar o Agente1 ao GrupoPersonalizado1, o Agente1 aparecerá em ambos os locais.

Para obter mais informações, consulte os seguintes tópicos:

- Criação de grupos personalizados
- Modificação de nomes de grupos personalizados
- Remoção de grupos personalizados
- Realização de ações de grupo
- Visualização de todas as máquinas de um grupo personalizado em uma página

Criação de grupos personalizados

Ao rolar o cursor sobre o nome de qualquer máquina no menu Máquinas protegidas ou Máquinas replicadas, verá uma seta que abre um menu suspenso. Nesse menu, é possível criar um rótulo personalizado.

Use o procedimento abaixo para criar um grupo personalizado.

Para criar um grupo personalizado

1 Navegue até o AppAssure 5 Core Console.

2 No menu Máquinas protegidas ou Máquinas replicadas, faça o seguinte:

   a Clique em uma máquina do menu.

b Clique no menu suspenso dessa máquina.

c Role e selecione **Rotulado como** e clique em **Novo rótulo**.

Aparecerá um novo menu, com uma caixa de texto em branco ao lado de um ícone de rótulo. A máquina selecionada é relacionada sob o grupo personalizado.

3 Insira um rótulo adequado para seu grupo personalizado.

Use um nome descritivo, que comunique a finalidade do grupo. Por exemplo, para agrupar máquinas agente por departamento, digite Departamento de contabilidade. Posteriormente, é possível renomear o grupo.

NOTA: Os rótulos precisam ter 50 caracteres ou menos. Você pode incluir um único espaço entre as palavras. Você precisa fornecer um rótulo para o seu grupo personalizado.

4 Quando estiver satisfeito com o nome do rótulo, clique na marca de verificação verde para salvar o nome.

A página é atualizada, mostrando seu grupo personalizado na área de navegação.

5 Opcionalmente, para adicionar outros agentes a esse grupo, navegue até o nome do agente no menu apropriado, clique no menu suspenso para abri-lo, role para baixo e selecione **Rotulado como**. Depois, clique no nome do grupo personalizado.

Agora você pode realizar ações de grupo nesse grupo. Para obter mais informações, consulte Realização de ações de grupo.

Modificação de nomes de grupos personalizados

Ao modificar o nome de um grupo personalizado, apenas o rótulo é alterado. Os nomes das máquinas continuam os mesmos.

Use o procedimento abaixo para modificar o nome de um grupo personalizado.

Para modificar o nome de um grupo personalizado

1 Navegue até o AppAssure 5 Core Console.

2 No menu Máquinas protegidas, role o cursor sobre o grupo personalizado que deseja modificar.

3 Clique no menu suspenso desse grupo e clique em **Editar**.

O nome do grupo personalizado se torna editável.

4 Digite um novo rótulo para o grupo personalizado. Quando estiver satisfeito com o nome do rótulo, clique na marca de verificação verde para salvar o nome. É possível editar esse nome mais tarde.

Use um nome descritivo, que comunique a finalidade do grupo. Por exemplo, para agrupar máquinas agente por departamento, digite Departamento de contabilidade.

NOTA: Os rótulos precisam ter 50 caracteres ou menos. Você pode incluir um único espaço entre as palavras. Você precisa fornecer um rótulo para o seu grupo personalizado.

5 Opcionalmente, para adicionar outros agentes a esse grupo, navegue até o nome do agente no menu apropriado, clique no menu suspenso para abri-lo, role para baixo e selecione **Rotulado como**. Depois, clique no nome do grupo personalizado.

Remoção de grupos personalizados

Quando um grupo personalizado é removido, ele é excluído do menu Máquinas protegidas. As máquinas que estavam no grupo não são removidas e ainda podem ser encontradas no menu padrão apropriado.

Use o procedimento abaixo para remover um grupo personalizado.

Para remover um grupo personalizado

1 Navegue até o AppAssure 5 Core Console.

2 No menu Máquinas protegidas, role o cursor sobre o grupo personalizado que deseja remover.

3 Clique no menu suspenso desse grupo e clique em **Remover rótulo**.

Aparece uma mensagem pedindo confirmação para a remoção do grupo. Confirme a ação.

A página é atualizada e o grupo personalizado é removido da área de navegação.

Realização de ações de grupo

É possível realizar ações de grupo em qualquer grupo que apareça na área de navegação à esquerda do AppAssure 5 Core Console. Se o grupo contiver membros diferentes (por exemplo, máquinas agente padrão e agentes replicados), as ações solicitadas serão realizadas apenas nos membros do grupo relevantes.

Use o procedimento abaixo para realizar ações de grupo em um grupo personalizado.

Para realizar ações de grupo

1 Navegue até o AppAssure 5 Core Console.

2 No menu Máquinas protegidas, role o cursor sobre o grupo personalizado no qual deseja realizar uma ação de grupo.

3 Clique no menu suspenso desse grupo e selecione uma ação, como a seguir:

- Para forçar um snapshot incremental ou imagem de base de um agente protegido, clique em Forçar snapshot ou Forçar imagem de base, conforme o caso. Para obter mais informações, consulte Forçar snapshot.
- Para pausar a proteção de um agente protegido, clique em **Pausar proteção** e especifique os parâmetros de retomada. Para obter mais informações, consulte Pausa e retomada da replicação.
- Para retomar a proteção de um agente cuja proteção tenha sido pausada, clique em Retomar proteção e confirme que deseja retomar. Para obter mais informações, consulte Pausa e retomada da replicação.
- Para atualizar as informações exibidas, clique em **Atualizar metadados**.
- Para pausar a replicação de um agente replicado do core de destino, em Replicação clique em **Pausar**. Para obter mais informações, consulte Pausa e retomada da replicação.
- Para retomar a replicação de um agente replicado para o qual a replicação foi pausada no core de destino, em Replicação clique em **Retomar**. Para obter mais informações, consulte Pausa e retomada da replicação.
- Para forçar a replicação de uma máquina agente replicada, clique em **Forçar**. Para obter mais informações, consulte Forçamento de replicação.
- Apenas para grupos personalizados, para modificar o rótulo deles, selecione **Editar**. Para obter mais informações, consulte Modificação de nomes de grupos personalizados.
- Apenas para grupos personalizados, para remover o grupo, selecione **Remover rótulo**. Para obter mais informações, consulte Remoção de grupos personalizados.

Visualização de todas as máquinas de um grupo personalizado em uma página

Clique no nome de um grupo personalizado para ver a guia Máquinas que relaciona todas as máquinas nesse grupo personalizado. É possível então realizar algumas funções em todas as máquinas a partir do menu Ações ou realizar funções individualmente selecionando os comandos de cada máquina individual.

Roteiro para configuração do AppAssure 5 Core

Antes de poder usar o AppAssure 5, é preciso configurar o AppAssure 5 Core.

Você pode realizar essas tarefas individualmente ou usar o Guia de início rápido para guiá-lo através dos processos de configuração do Core. O Guia de início rápido permite iniciar assistentes e etapas de configuração, ou apenas ver o fluxo recomendado de realização das tarefas de configuração.

Se o Guia de início rápido for usado na configuração, proteja primeiro a máquina usando o Assistente de proteção de máquina. Durante essa etapa, é solicitada a definição dos locais de armazenamento, incluindo a criação e o dimensionamento de um repositório. Esse guia também permitirá configurar a notificação de eventos, configurar chaves de criptografia, configurar a replicação, exportar para uma máquina virtual e visualizar ou alterar sua política de retenção. Se você tiver pontos de recuperação no Core, este guia permitirá a restauração de dados. Para obter mais informações sobre o Guia de início rápido, consulte Sobre o Guia de início rápido.

Ao realizar tarefas de configuração individualmente, será preciso executar certas tarefas de configuração iniciais, como a criação e configuração do repositório para armazenar snapshots de cópia de segurança, a definição opcional de chaves de criptografia para proteger os dados protegidos e notificações de tarefas, alertas e eventos.

A configuração inicial do AppAssure 5 Core envolve a compreensão de certos conceitos e a realização de determinadas operações iniciais. Para configurar o AppAssure 5 Core, realize as seguintes principais tarefas de configuração de core:

- **Criar um repositório**. Para obter mais informações sobre repositórios, consulte Criação de um repositório.
- **Configurar chaves de criptografia**. Para obter mais informações sobre a configuração de chaves de criptografia, consulte Adição de uma chave de criptografia.
- **Configurar notificação de eventos**. Para obter mais informações sobre a configuração de notificação de eventos, consulte Configuração de um server de e-mail.

Ao concluir a configuração inicial do AppAssure 5 Core, poderá proteger uma ou mais máquinas agente e realizar a recuperação. O AppAssure 5 inclui uma política de retenção padrão, que você talvez queira configurar de acordo com seus requisitos personalizados. Ao proteger bancos de dados SQL, é possível configurar a capacidade de anexação do SQL.

A configuração adicional do AppAssure 5 Core inclui as seguintes operações:

- **Proteger uma única máquina agente.** Para obter mais informações sobre como proteger uma máquina agente usando o Assistente de proteção de máquina, consulte Proteção de uma máquina.
- **Proteger várias máquinas agente.** Para obter mais informações sobre como proteger várias máquinas agente em uma etapa usando o Assistente de proteção de máquina, consulte Proteção de várias máquinas.
- **Restaurar dados de pontos de recuperação.** Para obter mais informações sobre a restauração de dados de pontos de recuperação usando o Assistente de restauração, consulte Sobre a restauração de dados de pontos de recuperação.
- **Configurar a política de retenção**. Para obter mais informações sobre a configuração de políticas de retenção, consulte Gerenciamento das políticas de retenção.
- **Configurar a capacidade de anexação do SQL**. Para obter mais informações sobre a configuração da capacidade de anexação do SQL, consulte Configuração das definições da capacidade de anexação do SQL.

Gerenciamento de licenças

O AppAssure 5 permite gerenciar licenças do AppAssure 5 diretamente do AppAssure 5 Core Console. Nesse console, é possível alterar a chave de licença e entrar em contato com o server de licença. Também é possível acessar o Portal de licenças de software da Dell na página de Aplicação de licença do console.

Essa página de Aplicação de licença inclui as seguintes informações:

- Tipo de licença
- Status da licença
- Tamanho do conjunto de licenças
- Número de máquinas protegidas
- Status da última resposta do server de aplicação de licenças
- Hora do último contato com o server de aplicação de licenças
- Nova tentativa programada de contato com o server de aplicação de licenças

Para obter mais informações, consulte o *Guia do usuário do portal de licenças*, localizado no site de documentação de Guias e notas de versão do AppAssure em https://support.software.dell.com/appassure/release-notes-guides.

Alteração de uma chave de licença

Execute as etapas deste procedimento para alterar uma chave de licença de dentro do AppAssure 5 Core Console.

Para obter informações sobre a obtenção de uma chave de licença consulte o *Guia do usuário do portal de licenças*, localizado no site de documentação de Guias e notas de versão do AppAssure em https://support.software.dell.com/appassure/release-notes-guides.

Para alterar uma chave de licença

1. Navegue até o AppAssure 5 Core Console e selecione a guia Configuração.
2. Clique em **Aplicação de licença**.

   A página Aplicação de licença é exibida.
3. Nos detalhes da licença, clique em **Alterar licença**.

   Aparece a caixa de diálogo Alterar chave de licença.
4. Na caixa de diálogo Alterar chave de licença, insira a nova chave de licença e clique em **OK**.

Contato com o server do Portal de licenças de software da Dell

O AppAssure 5 Core Console frequentemente entra em contato com o server do portal para permanecer atualizado com as mudanças feitas no Portal de licenças de software da Dell. Normalmente, a comunicação com o server do portal ocorre automaticamente em intervalos designados. No entanto, é possível iniciar a comunicação sob demanda.

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

Para entrar em contato com o server do portal

1. Navegue até o AppAssure 5 Core Console e clique na guia Configuração.
2. Clique em **Aplicação de licença**.

A página Aplicação de licença é exibida.

3 Na opção Server de licenças, clique em **Entrar em contato agora**.

Gerenciamento das definições do AppAssure 5 Core

As definições do AppAssure 5 Core são usadas para fazer várias definições de configuração e desempenho. A maioria das definições é configurada para o uso ideal, mas é possível alterar as seguintes definições, conforme necessário:

- Geral
- Atualizações
- Trabalhos noturnos
- Fila de transferência
- Definições de tempo limite do cliente
- Configuração do cache de deduplicação
- Configuração do mecanismo de reprodução
- Definições de implementação
- Definições de conexão do banco de dados
- Definições do server de SMTP
- Logs de acompanhamento ativados
- Configuração da nuvem

Alteração do nome de exibição do Core

Execute as etapas deste procedimento para alterar o nome de exibição do Core.

Para alterar o nome de exibição do Core

1 Navegue até o AppAssure 5 Core Console, clique na guia Configuração e depois em **Definições**.

A caixa de diálogo Definições gerais é exibida.

2 No painel Geral, clique em **Alterar**.

A caixa de diálogo Definições gerais é exibida.

3 Na caixa de texto Nome de exibição, insira um novo nome de exibição para o Core.

Esse é o nome que será exibido no AppAssure 5 Core Console. Você pode inserir até 64 caracteres.

4 Na caixa de texto Porta do server da Web, insira um número de porta para o server da Web. O padrão é 8006.

5 Em Porta de serviço, insira um número de porta para o serviço. O padrão é 8006.

6 Clique em **OK**.

Configuração das definições de atualização

O AppAssure 5 inclui o recurso de Atualização automática. Ao instalar o AppAssure 5 Core, é possível optar por atualizar automaticamente o software AppAssure 5 Core quando houver novas atualizações disponíveis e a frequência com que o sistema deve verificar se há atualizações.

NOTA: Para obter mais informações sobre a instalação do software AppAssure 5 Core, consulte o *Guia de implementação do Dell AppAssure 5*.

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

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

Para configurar as definições de atualização

1. Navegue até o AppAssure 5 Core Console, clique na guia Configuração e depois em **Definições**.
2. No painel Atualizações, clique em **Alterar**.

   A caixa de diálogo Definições de atualização é exibida.
3. Na caixa de texto Buscar novas atualizações, selecione a frequência de verificação e instalação de atualizações após os trabalhos noturnos serem concluídos. Você pode selecionar dentre as seguintes opções:
   - Nunca
   - Diariamente
   - Semanalmente
   - Mensalmente
4. Especifique como as atualizações serão tratadas, se estiverem disponíveis, escolhendo uma das seguintes opções:
   - **Instalá-las automaticamente (recomendado)** ou
   - **Notificar-me, mas não instalá-las**
5. Clique em **OK**.

Configuração de trabalhos noturnos para o Core

Quando a opção Trabalhos noturnos está ativada no AppAssure 5 Core, ela afeta todos os trabalhos de todos os agentes protegidos pelo Core. Por outro lado, se você tivesse que desativar essa opção, todos os agentes protegidos pelo Core seriam afetados.

Embora os trabalhos noturnos possam ser especificados em nível de Core ou de agente, algumas opções são específicas do respectivo nível. No nível de core, é possível optar por executar qualquer das seguintes opções de trabalho:

- Trabalho de verificação de capacidade de anexação
- Download dos logs das máquinas protegidas
- Verificar a integridade dos pontos de recuperação
- Trabalho de verificação de soma de verificação
- Rollup
- Trabalho de truncamento de log (apenas modelo de recuperação simples)
- Estatísticas do repositório de log
- Exclusão de eventos e trabalhos antigos

Para obter informações sobre especificação de opções de trabalho no nível do agente, consulte Personalização de trabalhos noturnos para uma máquina protegida.

Para configurar trabalhos noturnos para o Core

1. Navegue até o AppAssure 5 Core Console, clique na guia Configuração e depois em **Definições**.
2. No painel Trabalhos noturnos, clique em **Alterar**.

   A caixa de diálogo Trabalhos noturnos é exibida.
3. Selecione a opção de trabalhos noturnos que deseja definir para o Core. Você pode optar por selecionar todos ou selecionar individualmente apenas aqueles que se aplicam.
4. Clique em **OK**.

Ativação de uma verificação de montagem noturna

É possível optar por fazer o AppAssure 5 Core executar um trabalho noturno para cada agente, que verifica a integridade dos pontos de recuperação montando o ponto de recuperação mais recente para cada grupo de proteção e, em seguida, enumerando os arquivos e pastas de cada volume. A opção Verificar integridade dos pontos de recuperação examina então os pontos de recuperação para garantir que sejam válidos. É possível especificar no nível de Core a execução de verificações de montagem noturnas ou individualmente por agente. Por padrão, a opção Verificar integridade dos pontos de recuperação não está ativada.

Para ativar uma verificação de montagem noturna no Core

1. Navegue até o AppAssure 5 Core Console, clique na guia Configuração e depois em **Definições**.
2. No painel Trabalhos noturnos, clique em **Alterar**.

   A caixa de diálogo Trabalhos noturnos é exibida.
3. Selecione **Verificar integridade dos pontos de recuperação**.
4. Clique em **OK**.

Para ativar uma verificação de montagem noturna por agente

1. Navegue até o AppAssure 5 Core Console, clique na guia Configuração e depois em **Definições**.
2. No painel Trabalhos noturnos, clique em **Alterar**.

   A caixa de diálogo Trabalhos noturnos é exibida.
3. Clique no controle de seta para baixo para expandir a visualização dos agentes sob proteção.
4. Selecione o(s) agente(s) para o(s) qual(is) você deseja executar um trabalho noturno de realização de verificação de montagem.
5. Clique em **OK**.

Ajuste do horário do trabalho noturno

Execute as etapas deste procedimento para ajustar o horário do trabalho noturno.

Para ajustar o horário do trabalho noturno

1. Navegue até o AppAssure 5 Core Console, clique na guia Configuração e depois em **Definições**.
2. No painel Trabalhos noturnos, clique em **Alterar**.

   A caixa de diálogo Trabalhos noturnos é exibida.
3. Na caixa de texto Horário de trabalho noturno, insira um novo horário para a execução dos trabalhos noturnos.
4. Clique em **OK**.

Modificação das definições da fila de transferência

As definições da fila de transferência são em nível de core e estabelecem o número máximo de transferências simultâneas e de novas tentativas de transferência de dados.

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

Para modificar as definições da fila de transferência

1. Navegue até o AppAssure 5 Core Console, clique na guia Configuração e depois em **Definições**.
2. No painel Fila de transferência, clique em **Alterar**.

   Aparece a caixa de diálogo Fila de transferência.
3. Na caixa de texto Máximo de transferências simultâneas, insira um valor para atualizar o número de transferências simultâneas.

   Defina um número de 1 a 60. Quanto menor o número, menor a carga sobre a rede e outros recursos do sistema. À medida que o número de agentes processados aumenta, o mesmo acontece com a carga sobre o sistema.
4. Na caixa de texto Máximo de novas tentativas, insira um valor para atualizar o número máximo de novas tentativas.
5. Clique em **OK**.

Ajuste das definições de tempo limite do cliente

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

Para ajustar as definições de tempo limite do cliente

1. Navegue até o AppAssure 5 Core Console, clique na guia Configuração e depois em **Definições**.
2. Na área de configuração das Definições de tempo limite do cliente, clique em **Alterar**.

   Aparece a caixa de diálogo Definições de tempo limite do cliente.
3. Na caixa de texto Tempo limite de conexão, insira o número de minutos e segundos antes de ocorrer o tempo limite de uma conexão.
4. Na caixa de texto Tempo limite da UI de conexão, digite o número de minutos e segundos antes de ocorrer o tempo limite da UI de uma conexão.
5. Na caixa de texto Tempo limite de leitura/gravação, insira o número de minutos e segundos que você deseja que passem antes de ocorrer o tempo limite durante um evento de leitura/gravação.
6. Na caixa de texto Tempo limite de UI de leitura/gravação, digite o número de minutos e segundos que passarão antes de ocorrer o tempo limite da UI de leitura/gravação.
7. Clique em **OK**.

Noções básicas sobre tamanho do cache de deduplicação e locais de armazenamento

A deduplicação global reduz a quantidade de espaço de armazenamento em disco necessário para seus dados salvos em cópias de segurança. O gerenciador de volume de deduplicação (DVM) do AppAssure 5 combina um conjunto de locais de armazenamento em um único repositório. Cada repositório é deduplicado, armazenando cada bloco único uma vez fisicamente em disco, e utilizando referências virtuais ou indicadores a esses blocos em cópias de segurança subsequentes. Para identificar blocos duplicados, o AppAssure 5 inclui um cache de deduplicação que mantém referências para blocos únicos.

Por padrão, esse cache de deduplicação tem 1.5 GB em tamanho. Esse é um tamanho suficiente para muitos repositórios. Até esse cache ser excedido, seus dados são deduplicados em todo o repositório. Se a quantidade de informações redundantes for tão grande que o cache de deduplicação fique cheio, seu repositório não poderá mais tirar total vantagem de deduplicação adicional em todo seu repositório para dados recém-adicionados. A quantidade de dados salvos em seu repositório antes que o cache de deduplicação encha varia por tipo de dados salvos em cópias de segurança e é diferente para cada usuário.

É possível aumentar o tamanho do cache de deduplicação alterando a configuração do cache de deduplicação no AppAssure 5 Core. Para obter mais informações sobre como realizar isso, consulte o tópico Configuração das definições de cache de deduplicação.

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

Espaço em disco. Duas cópias do cache são armazenadas em disco: um cache primário, e um cache secundário, que é uma cópia paralela. Então, com um tamanho de cache padrão de 1.5 GB, 3 GB de armazenamento em disco são utilizados em seu sistema. À medida que você aumenta o tamanho do cache, a quantidade de espaço em disco utilizado continua proporcionalmente o dobro do tamanho do cache. Para garantir o desempenho adequado e resistente a erros, o Core altera de forma dinâmica a prioridade desses caches. Ambos são necessários, a única diferença é que o cache designado como principal é salvo primeiro.

Uso de RAM. Quando o AppAssure Core inicia, ele carrega o cache de deduplicação para a memória RAM. O uso da memória para seu sistema é, portanto, afetado pelo tamanho do cache. A quantidade total de RAM utilizada pelo Core depende de muitos fatores, incluindo quais operações são executadas, o número de usuários, o número de agentes, bem como o tamanho do cache de deduplicação. Toda operação realizada pelo Core (transferência, replicação, rollup e assim por diante) consome mais RAM. Depois que uma operação é concluída, o consumo de memória diminui cada vez mais. Contudo, os administradores devem considerar o requisito mais alto do carregamento de RAM para obterem operações eficientes.

As configurações padrão para o AppAssure 5 Core colocam os caches principal, secundário e de metadados no diretório do AppRecovery utilizado pelo AppAssure 5.

NOTA: Dependendo de suas configurações, o diretório do AppRecovery pode não estar visível no AppAssure 5 Core. Para ver esse diretório, você pode precisar alterar as Opções de pasta no painel de controle para exibir arquivos, pastas e unidades ocultas.

Supondo que o AppAssure 5 Core esteja instalado na unidade C, esses locais são normalmente os seguintes:

Tabela 4. Os locais de armazenamento padrão para configurações do cache de deduplicação

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

É possível alterar o local de armazenamento desses caches. Por exemplo, para aumentar a tolerância a erros, é possível alterar o local do seu cache secundário para uma unidade física diferente da principal, supondo que o AppAssure 5 Core tenha acesso ao local.

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

Configuração das definições de cache de deduplicação

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

Para configurar as definições de cache de deduplicação

1 Navegue até o AppAssure 5 Core Console, clique na guia Configuração e depois em **Definições**.

2 No painel Configuração do cache de deduplicação, clique em **Alterar**.

A caixa de diálogo Configuração do cache de deduplicação é exibida, permitindo especificar os locais de armazenamento de cache e o tamanho dele.

Uma vez que o cache principal e o secundário têm o mesmo tamanho, o armazenamento coletivo para esses dois caches exige duas vezes a quantidade de espaço da quantidade alocada para o tamanho do cache de deduplicação. Por exemplo, se você especificar a quantidade padrão de 1.5 GB para o tamanho do cache de deduplicação, precisará assegurar que cada um dos dois locais de armazenamento tenha, pelo menos, 1.5 GB. Em especial, se ambos os locais pertencerem à mesma unidade (por exemplo, a unidade C), deve haver pelo menos 3 GB de espaço livre em disco.

3 Se você desejar alterar o local do cache primário, na caixa de texto Local de cache primário, insira o caminho para um local de armazenamento acessível ao Core.

4 Se você desejar alterar o local do cache secundário, na caixa de texto Local de cache secundário, insira o caminho para um local de armazenamento acessível ao Core.

5 Se você desejar alterar o local do cache de metadados, na caixa de texto Local de cache de metadados, insira o caminho para um local de armazenamento acessível ao Core.

6 Se você desejar alterar o tamanho do cache de deduplicação, realize os seguintes:

a Na caixa de texto Tamanho do cache dedupe, insira um valor correspondente à quantidade de espaço que você desejar alocar para o cache de deduplicação.

Por exemplo, se desejar aumentar o tamanho do cache de deduplicação para 3 GB, insira 3 nesse campo.

b No campo suspenso do tamanho da unidade, selecione GB (gigabytes) ou TB (terabytes), conforme adequado, para especificar a unidade de medida para o valor na caixa de texto Tamanho do cache dedupe.

NOTA: A definição mínima de tamanho do cache é de 1,5 GB. Além disso, o tamanho do cache não pode exceder 50% da RAM instalada.

7 Clique em **OK**.

NOTA: É preciso reiniciar o serviço do Core para que as alterações entrem em vigor.

ModificaçãoAppAssure 5 das definições do mecanismo

Execute as etapas deste procedimento para modificar as definições de mecanismo do AppAssure 5.

Para modificar as definições do mecanismo do AppAssure 5

1 Navegue até o AppAssure 5 Core Console, clique na guia Configuração e depois em **Definições**.

2 No painel Configuração do mecanismo de reprodução, clique em **Alterar**.

É exibida a caixa de diálogo Configuração do mecanismo de reprodução.

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

Tabela 5.

Caixa de texto	Descrição
Endereço IP	Especifique o endereço IP escolhendo uma das seguintes opções: • Clique em **Automaticamente determinado** para usar o endereço IP preferencial do seu TCP/IP. • Ou clique em **Usar um endereço específico** para inserir manualmente um endereço IP.
Porta de preferência	Insira um número de porta ou aceite a definição padrão. A porta padrão é *8007*. A porta é usada para especificar o canal de comunicação do mecanismo do AppAssure.
Porta em uso	Representa a porta em uso para a configuração do mecanismo de reprodução.
Permitir atribuição automática de porta	Clique para permitir a atribuição automática de porta TCP.
Grupo de administradores	Insira um novo nome para o grupo de administração. O nome padrão é *BUILTIN\Administrators*.
Comprimento de I/O assíncrono mínimo	Insira um valor ou escolha a definição padrão. Descreve o comprimento mínimo assíncrono de entrada/saída. A definição padrão é *65536*.
Tamanho da memória intermediária de recebimento	Insira um tamanho de memória intermediária de entrada ou aceite a definição padrão. A definição padrão é *8192*.
Tamanho da memória intermediária de envio	Insira um tamanho de memória intermediária de saída ou aceite a definição padrão. A definição padrão é *8192*.
Tempo limite de leitura	Insira um valor de tempo limite de leitura ou escolha a definição padrão. A definição padrão é *00:05:00*.
Tempo limite de gravação	Insira um valor de tempo limite de gravação ou escolha a definição padrão. A definição padrão é *00:05:00*.
Sem atraso	Recomendamos deixar essa caixa de seleção desmarcada visto que, se isso não for feito, a eficiência da rede poderá ser afetada. Se for determinado que é preciso modificar essa configuração, entre em contato com o Suporte da Dell para obter orientações de como fazer isso.

4 Clique em **OK**.

Modificação das definições de implementação

Execute as etapas deste procedimento para modificar as definições de implementação.

Para modificar as definições de implementação

1 Navegue até o AppAssure 5 Core Console, clique na guia Configuração e depois em **Definições**.

2 No painel Definições de implementação, clique em **Alterar**.

A caixa de diálogo Definições de implementação é exibida.

3 Na caixa de texto Nome do Agent Installer, digite o nome do arquivo executável do agente. O padrão é Agent-web.exe.

4 Na caixa de texto Endereço do core, digite o endereço do core.

5 Na caixa de texto Falha no tempo limite de recebimento, insira o número de minutos a aguardar sem atividade antes do tempo limite.

6 Na caixa de texto Máximo de instalações paralelas, insira o número máximo de instalações que podem ser instaladas em paralelo.

7 Selecione uma ou ambas as seguintes definições opcionais:

- **Reinício automático após a instalação**
- **Proteger após implantação**

8 Clique em **OK**.

Modificação das definições de conexão do banco de dados

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

Para modificar as definições de conexão do banco de dados

1 Navegue até o AppAssure 5 Core Console, clique na guia Configuração e depois em **Definições**.

2 No painel Definições de conexão do banco de dados, realize um dos seguintes:

- Clique em **Restaurar padrão**.
- Ou clique em **Alterar**.

A caixa de diálogo Definições de conexão do banco de dados é exibida.

3 Insira as definições para modificar a conexão do banco de dados conforme descrito na tabela a seguir.

Tabela 6.

Caixa de texto	Descrição
Nome do host	Insira um nome de host para a conexão de banco de dados.
Port	Insira o número da porta para a conexão do banco de dados.
Nome de usuário	(opcional) Insira um nome de usuário para acessar e gerenciar as definições de conexão do banco de dados. Usado para especificar as credenciais de login para acessar a conexão do banco de dados.
Senha	(opcional) Insira uma senha para acessar e gerenciar as definições de conexão do banco de dados.
Reter histórico de eventos e trabalhos por, dias	Insira o número de dias de retenção do histórico de eventos e trabalhos para a conexão de banco de dados.
Tamanho do conjunto de conexão máximo	Define o número máximo de conexões de banco de dados em cache para permitir a reutilização dinâmica. A definição padrão é 100.
Tamanho do conjunto de conexão mínimo	Define o número mínimo de conexões de banco de dados em cache para permitir a reutilização dinâmica. A definição padrão é 0.

4 Clique em **Testar conexão** para confirmar as definições.

5 Clique em **Salvar**.

Sobre repositórios

Um repositório é usado para armazenar os snapshots capturados a partir de suas estações de trabalho e servers protegidos. O repositório pode residir em tecnologias de armazenamento diferentes, como rede de área de armazenamento (SAN), armazenamento por conexão direta (DAS) ou armazenamento conectado à rede (NAS).

Ao criar um repositório, o AppAssure 5 Core pré-aloca o espaço de armazenamento necessário para os dados e metadados no local especificado. É possível criar até 255 repositórios independentes em um único core, que

abrangem diferentes tecnologias de armazenamento. Além disso, é possível aumentar o tamanho de um repositório adicionando novas extensões ou especificações de arquivo. Um repositório estendido pode conter até 4096 extensões que abrangem diversas tecnologias de armazenamento.

Os principais conceitos e considerações sobre repositórios incluem:

- O repositório se baseia no Sistema de arquivos de objeto escalável do AppAssure.
- Todos os dados armazenados dentro de um repositório são globalmente deduplicados.
- O Sistema de arquivos de objeto escalável proporciona um desempenho de I/O escalável em conjunto com deduplicação global de dados, criptografia e gerenciamento de retenção.

NOTA: Os repositórios do AppAssure 5 devem ser armazenados em dispositivos de armazenamento primários. Dispositivos de armazenamento de arquivamento como Domínio de dados não são suportados devido a limitações de desempenho. De forma semelhante, os repositórios não devem ser armazenados em arquivadores NAS organizados em níveis na nuvem, pois esses dispositivos tendem a ter limitações de desempenho quando usados como armazenamento primário.

Roteiro de gerenciamento de repositório

Antes de poder usar o AppAssure 5, é preciso configurar um ou mais repositórios no server do AppAssure 5 Core. Um repositório armazena seus dados protegidos. Mais especificamente, armazena os snapshots capturados de seus servers protegidos no seu ambiente.

Quando você configura um repositório, pode executar uma variedade de tarefas, como especificar onde localizar o armazenamento de dados no server do Core, quantas localizações devem ser adicionadas a cada repositório, o nome do repositório, quantas operações atuais os repositórios suportam, e assim por diante.

Ao criar um repositório, o Core pré-aloca o espaço necessário para armazenar os dados e metadados no local especificado. É possível criar até 255 repositórios independentes em um único core. Para aumentar ainda mais o tamanho de um único repositório, é possível adicionar novos locais de armazenamento ou volumes.

Gerenciar um repositório envolve a criação, configuração e visualização de um repositório, e inclui as seguintes operações:

- **Acessar o Core Console.** Para obter mais informações sobre como acessar o AppAssure 5 Core Console, consulte Acesso ao AppAssure 5 Core Console.
- **Criar um repositório.** Para obter mais informações sobre a criação de um repositório, consulte Criação de um repositório.
- **Visualizar detalhes de repositório.** Para obter mais informações sobre a visualização de detalhes de repositórios, consulte Visualização de detalhes de um repositório.
- **Modificar definições de repositório.** Para obter mais informações sobre a modificação de definições de repositório, consulte Modificação das definições de repositório.
- **Adicionar um novo local de armazenamento.** Para obter mais informações sobre adicionar um novo local de armazenamento, consulte Adição de um local de armazenamento a um repositório existente.
- **Verificar um repositório.** Para obter mais informações sobre a verificação de repositórios, consulte Verificação de um repositório.
- **Excluir um repositório.** Para obter mais informações sobre a exclusão de repositórios, consulte Exclusão de um repositório.

Criação de um repositório

Execute as seguintes etapas para criar um repositório.

Para criar um repositório

1 No AppAssure 5 Core Console, realize um dos seguintes:

- Na página Inicial, no painel de Repositórios clique em **Adicionar novo repositório**.
- Clique na guia Configuração e, na página Repositórios, clique em **Adicionar novo**.

A caixa de diálogo Adicionar novo repositório é exibida.

2 Insira as informações conforme descrito na tabela a seguir.

Tabela 7.

Caixa de texto	Descrição
Nome do repositório	Insira o nome de exibição do repositório. Por padrão, essa caixa de texto consiste na palavra *Repositório* e um número de índice, que corresponde ao número do novo repositório. Você pode alterar o nome conforme necessário. Você pode inserir até 40 caracteres.
Operações simultâneas	Defina o número de solicitações simultâneas que você deseja que o repositório suporte. Por padrão, o valor é *64*.
Comentários	Como opção, insira uma nota descritiva sobre esse repositório. É possível digitar até 254 caracteres.

3 Clique em **Adicionar local de armazenamento** para definir o local de armazenamento específico ou o volume do repositório.

AVISO: Se o repositório do AppAssure que você está criando nessa etapa for removido mais tarde, todos os arquivos no local de armazenamento do seu repositório serão excluídos. Se você não definir uma pasta dedicada para armazenar os arquivos do repositório, os arquivos serão armazenados na raiz; excluir o repositório também excluirá todo o conteúdo da raiz, resultando em perda de dados catastrófica.

NOTA: Os repositórios do AppAssure 5 devem ser armazenados em dispositivos de armazenamento primários. Dispositivos de armazenamento de arquivamento como Domínio de dados não são suportados devido a limitações de desempenho. De forma semelhante, os repositórios não devem ser armazenados em arquivadores NAS organizados em níveis na nuvem, pois esses dispositivos tendem a ter limitações de desempenho quando usados como armazenamento primário.

A caixa de diálogo Adicionar local de armazenamento é exibida.

4 Na área Local de armazenamento, especifique a forma de adicionar o arquivo ao local de armazenamento. Você pode selecionar adicionar o arquivo no disco local ou no compartilhamento de CIFS.

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

Tabela 8.

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

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

Tabela 9.

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

5 Na área Configuração de armazenamento, clique em **Mais detalhes** e insira os detalhes do local de armazenamento, como descrito na tabela a seguir.

Tabela 10.

Caixa de texto	Descrição
Tamanho	Defina o tamanho ou capacidade do local de armazenamento. O padrão é 250 MB. Você pode selecionar dentre os seguintes: • MB • GB • TB **NOTA:** O tamanho que você especificar não pode exceder o tamanho do volume. Se o local de armazenamento for um volume NTFS (Sistema de arquivos de nova tecnologia) usando o Windows XP ou Windows 7, o limite de tamanho do arquivo é 16 TB. Se o local de armazenamento for um volume NTFS usando o Windows 8, Windows 8.1 ou Windows Server 2012, 2012 R2, o limite de tamanho do arquivo é 256 TB. **NOTA:** Para que o AppAssure 5 valide o sistema operacional, o Windows Management Instrumentation (WMI) deve ser instalado no local de armazenamento pretendido.
Política de cache de gravação	A política de cache de gravação controla como o Gerenciador de cache do Windows é usado no repositório e ajuda a ajustar o repositório para que o melhor desempenho seja obtido com diferentes configurações. Defina o valor para um dos seguintes: • Ligado • Desligado • Sincronizar Se definido como *Ligado*, que é o padrão, o Windows controla o armazenamento em cache. **NOTA:** Definir a política de cache de gravação como *Ligado* pode resultar em desempenho mais rápido. Se você estiver usando uma versão do Windows Server anterior à Server 2012, a definição recomendada é *Desligado*. Se definido como *Desligado*, o AppAssure 5 controla o armazenamento em cache. Se definido como *Sincronizar*, o Windows controla o armazenamento em cache, além da entrada/saída síncrona.

Tabela 10.

Caixa de texto	Descrição
Bytes por setor	Especifique o número de bytes que você deseja incluir em cada setor. O valor padrão é *512*.
Média de bytes por registro	Especifique a média de bytes por registro. O valor padrão é *8192*.

6 Clique em **Salvar**.

A tela Repositórios é exibida para incluir o local de armazenamento recém-adicionado.

7 Como opção, repita da Etapa 3 à Etapa 6 para adicionar outros locais de armazenamento ao repositório.

8 Clique em **Criar** para criar o repositório.

O repositório é exibido na guia Configuração.

Visualização de detalhes de um repositório

Execute as seguintes etapas para visualizar os detalhes de um repositório.

Para visualizar detalhes de um repositório

- No AppAssure 5 Core Console, clique na guia Configuração.

  A página Repositórios é exibida.
- Clique no símbolo de maior que (>) ao lado da coluna Status do repositório cujos detalhes você deseja visualizar.
- No ícone Definições ao lado da coluna Taxa de compressão, é possível realizar as seguintes ações em um repositório:
  - Modificar definições
  - Adicionar um local de armazenamento
  - Verificar o repositório
  - Excluir o repositório
- Os detalhes exibidos do repositório também incluem os locais de armazenamento e as estatísticas. Os detalhes do local de armazenamento incluem:
  - Caminho de metadados
  - Caminho de dados
  - Tamanho

  As informações estatísticas disponíveis para visualização incluem:
  - Deduplicação
  - I/O de registro
  - Mecanismo de armazenamento

  O nível de detalhes disponíveis para deduplicação é relatado como o número de ocorrências de deduplicação de bloco, erros de deduplicação de bloco e taxa de compressão de bloco.

  Os detalhes renderizados para o I/O de registro consistem na taxa (MB/s), taxa de leitura (MB/s) e taxa de gravação (MB/s).

  Os detalhes do mecanismo de armazenamento incluem a taxa (MB/s), taxa de leitura (MB/s) e taxa de gravação (MB/s).

Modificação das definições de repositório

Depois de adicionar um repositório, você pode modificar as definições dele, como a descrição ou o máximo de operações simultâneas. Também é possível adicionar um novo local de armazenamento para o repositório. Para obter mais informações sobre adicionar um novo local de armazenamento, consulte Adição de um local de armazenamento a um repositório existente.

Para modificar as definições de repositório

1 No AppAssure 5 Core Console, clique na guia Configuração.

A página Repositórios é exibida.

2 Clique no ícone Definições ao lado da coluna Taxa de compressão abaixo do botão Ações e depois em **Definições**.

A caixa de diálogo Definições do repositório é exibida.

3 Edite as informações de repositório conforme descrito na tabela a seguir.

Tabela 11.

Caixa de texto	Descrição
Nome do repositório	Representa o nome de exibição do repositório. Por padrão, essa caixa de texto consiste na palavra Repositório e um número de índice, que corresponde ao número do repositório. NOTA: Não é possível editar o nome do repositório.
Descrição	Como opção, insira uma nota descritiva sobre o repositório.
Máximo de operações simultâneas	Defina o número de solicitações simultâneas que você deseja que o repositório suporte.
Ativar deduplicação	Desmarque essa caixa de seleção para desativar a deduplicação ou selecione-a para ativar a deduplicação. NOTA: Alterar essa definição se aplica apenas a cópias de segurança feitas após a definição ser feita. Os dados existentes ou replicados de outro core ou importados de um arquivo manterão no lugar os valores de deduplicação no momento em que os dados forem capturados de um agente.
Ativar compressão	Desmarque essa caixa de seleção para desativar a compressão ou selecione-a para ativar a compressão. NOTA: Essa definição se aplica apenas a cópias de segurança feitas após a definição ser alterada. Os dados existentes ou replicados de outro core ou importados de um arquivo manterão no lugar os valores de compressão no momento em que os dados forem capturados de um agente.

4 Clique em **Salvar**.

Adição de um local de armazenamento a um repositório existente

Adicionar um local de armazenamento permite definir onde você deseja que o repositório ou o volume seja armazenado. Execute as etapas do procedimento a seguir para especificar o local de armazenamento do repositório ou do volume.

Para adicionar um local de armazenamento a um repositório existente

1 Clique no ícone Definições ao lado da coluna Taxa de compressão abaixo do botão Ações e depois em **Adicionar local de armazenamento**.

A caixa de diálogo Adicionar local de armazenamento é exibida.

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

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

Tabela 12.

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

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

Tabela 13.

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

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

Tabela 14.

Caixa de texto	Descrição
Tamanho	Defina o tamanho ou capacidade do local de armazenamento. O tamanho padrão é de 250 MB. Você pode selecionar dentre os seguintes: • MB • GB • TB **NOTA:** O tamanho que você especificar não pode exceder o tamanho do volume. Se o local de armazenamento for um volume NTFS (Sistema de arquivos de nova tecnologia) usando o Windows XP ou Windows 7, o limite de tamanho do arquivo é 16 TB. Se o local de armazenamento for um volume NTFS usando o Windows 8, Windows 8.1 ou Windows Server 2012, 2012 R2, o limite de tamanho do arquivo é 256 TB. **NOTA:** Para que o AppAssure 5 valide o sistema operacional, o Windows Management Instrumentation (WMI) deve ser instalado no local de armazenamento pretendido.
Política de cache de gravação	A política de cache de gravação controla como o Gerenciador de cache do Windows é usado no repositório e ajuda a ajustar o repositório para que o melhor desempenho seja obtido com diferentes configurações. Defina o valor para um dos seguintes: • Ligado • Desligado • Sincronizar Se definido como *Ligado*, que é o padrão, o Windows controla o armazenamento em cache. **NOTA:** Definir a política de cache de gravação como *Ligado* pode resultar em desempenho mais rápido. Se você estiver usando uma versão do Windows Server anterior à Server 2012, a definição recomendada é *Desligado*. Se definido como *Desligado*, o AppAssure 5 controla o armazenamento em cache. Se definido como *Sincronizar*, o Windows controla o armazenamento em cache, além da entrada/saída síncrona.
Bytes por setor	Especifique o número de bytes que você deseja incluir em cada setor. O valor padrão é *512*.
Média de bytes por registro	Especifique a média de bytes por registro. O valor padrão é *8192*.

4 Clique em **Salvar**.

A tela Repositórios é exibida para incluir o local de armazenamento recém-adicionado.

5 Como opção, repita da Etapa 3 à Etapa 6 para adicionar outros locais de armazenamento ao repositório.

6 Clique em **OK**.

Verificação de um repositório

O AppAssure 5 fornece a capacidade de realizar uma verificação de diagnóstico de um volume de repositório quando ocorrem erros. Os erros de Core podem ser o resultado do seu desligamento incorreto, falha de hardware, e assim por diante.

NOTA: Este procedimento deve ser realizado apenas para fins de diagnóstico, por exemplo, em caso de falha de hardware, desligamento incorreto do Core, falha ao importar o repositório, e assim por diante.

Para verificar um repositório

1. Clique no ícone Definições ao lado da coluna Taxa de compressão abaixo do botão Ações e depois em **Verificar**.

   A caixa de diálogo Verificar repositório é exibida.

2. Na caixa de diálogo Verificar repositório, clique em **Verificar**.

   NOTA: Ao executar uma verificação, todas as tarefas ativas associadas a esse repositório serão canceladas. Antes de a verificação começar, será exibida uma mensagem pedindo que você confirme que deseja prosseguir com a verificação. Aconselhamos e incentivamos a reconstruir o cache dos pontos de recuperação nesse ponto para atualizá-lo, visto que a falha de uma verificação resultará em você ter de restaurar o repositório a partir de um arquivo.

Exclusão de um repositório

Execute as etapas deste procedimento para excluir um repositório.

Para excluir um repositório

1. Clique no ícone Definições ao lado da coluna Taxa de compressão abaixo do botão Ações e depois em **Excluir**.
2. Na caixa de diálogo Excluir repositório, clique em **Excluir**.

   Aparece uma mensagem de aviso pedindo para confirmar a exclusão.
3. Clique em **Sim** para confirmar a exclusão do repositório.

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

Sobre o Trabalho de verificação da integridade do repositório

Nas versões anteriores, a replicação incluía o processo de copiar pontos de recuperação do core de destino para o core de origem regularmente. O rollup dos pontos de recuperação do envelhecimento ocorreram somente no core de origem. Os pontos de recuperação mais antigos combinados foram sincronizados diariamente durante a execução do trabalho noturno.

Começando com a versão 5.4.1, o AppAssure 5 inclui a capacidade de definir políticas de retenção discrepantes entre os core de destino e de origem, contanto que os core de destino e de origem sejam da mesma versão (5.4.1 ou posterior). Isso permite que os administradores do AppAssure configurem o rollup em um core de destino a uma taxa diferente (presumivelmente mais rápida) no core de origem. Da mesma forma, é possível definir uma política de retenção personalizada para qualquer agente replicado, fazer o rollup dos pontos de recuperação a uma taxa mais rápida e com menos granularidade no core de destino do que no core de origem, poupando espaço. Para obter mais informações, consulte Personalização das definições de política de retenção para um agente.

Alguns clientes experimentaram inconsistências nos pontos de recuperação que foram replicados para um core de destino antes do AppAssure 5 versão 5.3.6. Para tratar deste problema, o AppAssure 5 versão 5.4.1 e posterior inclui um novo trabalho de verificação de integridade que deve ser executado em cada repositório antes que seja possível configurar políticas de retenção diferentes entre o core de origem e um core de destino, ou configurar uma política de retenção em um agente replicado.

Quando o trabalho de confirmação de integridade é executado, o sistema confirma a integridade de todos os dados armazenados no repositório especificados, garantindo que seja possível recuperar os dados de cada Snapshot ou imagem de base. Se a verificação de integridade detectar algum problema com os dados em seu repositório, o trabalho para imediatamente. Os detalhes do evento para aquele trabalho no core solicitam que você entre em contato com o suporte do Dell AppAssure, de forma que é possível marcar o horário para trabalhar com um representante da Dell a fim realizar procedimentos adicionais de identificação e correção de inconsistências de dados.

△ **CUIDADO: É previsto que a execução deste trabalho leve um período de tempo prolongado com base nos dados de seu repositório e no sistema de armazenamento subjacente. Enquanto o trabalho está em execução, nenhuma outra transação pode ser executada naquele repositório, incluindo transferências (cópias de segurança do Snapshot e da imagem de base, e replicação), trabalhos noturnos e assim por diante.**

É possível executar outras operações em outros repositórios enquanto o trabalho de verificação de integridade está em execução.

ⓘ **NOTA:** Este trabalho verifica a integridade de *todo o conteúdo* dentro do repositório. Para obter informações sobre o trabalho de verificação do repositório, que pode ser usado para verificar a fim de garantir que um repositório está em condições de ser montado e usado, consulte Verificação de um repositório.

Este é um trabalho ad hoc disponível para ser executado em cada repositório. A Dell recomenda a realização do trabalho de verificação da integridade uma única vez em cada repositório em um core de destino replicado no caso da atualização da versão 5.3.x.

Você *não* precisa executar este trabalho:

- Em um novo repositório em um core de destino criado na versão 5.4.1 ou posterior.
- Em um core de origem.
- Se você já tiver executado o trabalho de verificação de integridade neste repositório.
- Se você não tiver usado a replicação.

Para obter instruções sobre como executar esta verificação, consulte o procedimento Executando o trabalho de verificação de integridade em um repositório.

Executando o trabalho de verificação de integridade em um repositório

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

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

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

Para executar o trabalho de verificação da integridade do repositório

1 Navegue até o AppAssure 5 Core Console, clique na guia **Configuração** e depois em **Repositórios**.

A página Repositórios é exibida, mostrando a lista de repositórios associada a este Core.

2 Clique no menu suspenso do repositório que deseja verificar, selecione **Verificar Integridade**.

É exibida uma mensagem de confirmação.

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

3 Na caixa de diálogo Repositório de verificação de integridade, para realizar a verificação de integridade, clique em **Sim**.

A caixa de diálogo Verificar repositório é fechada, todos os trabalhos enfileirados em andamento são cancelados e começa o trabalho de verificação da integridade.

4 Para monitorar o andamento do trabalho de verificação de integridade de um repositório, incluindo a determinação das etapas adicionais necessárias depois da verificação, clique na guia **Eventos**.

5 Na guia Eventos, clique em **Exibir detalhes** do trabalho para visualizar mais informações sobre o status do trabalho.

- Se você vir um erro em alguma tarefas subordinada, observe o erro e forneça as informações para o representante do suporte técnico da Dell.
- Se o trabalho de verificação de integridade concluir todas as tarefas subordinadas, você pode estabelecer uma política de retenção personalizada para este repositório.

Gerenciamento da segurança

O AppAssure 5 Core pode criptografar os dados de snapshot do agente dentro do repositório. Em vez de criptografar todo o repositório, o AppAssure 5 permite especificar uma chave de criptografia durante a proteção de um agente em um repositório, o que permite que as chaves sejam reutilizadas em diferentes agentes. A criptografia não afeta o desempenho, visto que cada chave de criptografia ativa cria um domínio de criptografia. Portanto, deixando um único core suportar multilocação ao hospedar vários domínios de criptografia. Em um ambiente de multilocação, os dados são particionados e deduplicados dentro dos domínios de criptografia. Como você gerencia as chaves de criptografia, a perda do volume não pode vazar as chaves.

Os principais conceitos e considerações sobre segurança incluem:

- A criptografia é feita usando AES de 256 bits no modo Cipher Block Chaining (CBC), que é compatível com SHA-3.
- A deduplicação opera dentro de um domínio de criptografia para garantir a privacidade.
- A criptografia é realizada sem impacto no desempenho.
- É possível adicionar, remover, importar, exportar, modificar e excluir as chaves de criptografia configuradas no AppAssure 5 Core.
- Não há limite para o número de chaves de criptografia que podem ser criadas no Core.

Adição de uma chave de criptografia

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

Para adicionar uma chave de criptografia

1 Navegue até o AppAssure 5 Core Console, clique na guia Configuração e depois selecione **Segurança**.

A página Chaves de criptografia é exibida.

2 No menu suspenso Ações, selecione **Adicionar chave de criptografia**.

Aparece a caixa de diálogo Criar chave de criptografia.

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

Tabela 15.

Caixa de texto	Descrição
Nome	Insira um nome para a chave de criptografia.
Descrição	Insira um comentário para a chave de criptografia. Usado para fornecer detalhes adicionais da chave de criptografia.
Frase de acesso	Insira uma frase de acesso. Usada para controlar o acesso.
Confirmar frase de acesso	Insira novamente a frase de acesso. Usado para confirmar a entrada da frase de acesso.

4 Clique em **OK**.

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

△ **CUIDADO: O AppAssure 5 usa a criptografia AES de 256 bits no modo Cipher Block Chaining (CBC) com chaves de 256 bits. Embora o uso de criptografia seja opcional, a Dell recomenda fortemente que você estabeleça uma chave de criptografia e que proteja a frase de acesso definida. Armazene a frase de acesso em um local seguro, pois ela é essencial para a recuperação dos dados. Sem a frase de acesso, não é possível executar a recuperação dos dados.**

Edição de uma chave de criptografia

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

Para editar uma chave de criptografia

1 Navegue até o AppAssure 5 Core Console, clique na guia Configuração e depois selecione **Segurança**.

A página Chaves de criptografia é exibida.

2 No menu suspenso Configuração da chave de criptografia que você deseja modificar, selecione **Editar**.

Aparece a caixa de diálogo Editar chave de criptografia.

3 Na caixa de diálogo Editar chave de criptografia, edite o nome ou a descrição da chave de criptografia e clique em **OK**.

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

Alteração da frase de acesso de uma chave de criptografia

Execute as etapas deste procedimento para alterar a frase de acesso de uma chave de criptografia.

Para alterar a frase de acesso de uma chave de criptografia

1 Navegue até o AppAssure 5 Core Console, clique na guia Configuração e depois selecione **Segurança**.

A página Chaves de criptografia é exibida.

2 No menu suspenso Configuração da chave de criptografia que você deseja modificar, selecione **Alterar frase de acesso**.

Aparece a caixa de diálogo Alterar frase de acesso.

3 Na caixa de diálogo Alterar frase de acesso, insira a nova frase de acesso para a criptografia e depois insira novamente a frase de acesso para confirmar o que inseriu.

4 Clique em **OK**.

A caixa de diálogo é fechada e a frase de acesso é atualizada.

△ **CUIDADO: O AppAssure 5 usa a criptografia AES de 256 bits no modo Cipher Block Chaining (CBC) com chaves de 256 bits. Recomendamos que você proteja a frase de acesso definida. Armazene a frase de acesso em um local seguro, pois ela é essencial para a recuperação dos dados. Sem a frase de acesso, não é possível executar a recuperação dos dados.**

Importação de uma chave de criptografia

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

Para importar uma chave de criptografia

1 Navegue até o AppAssure 5 Core Console, clique na guia Configuração e depois selecione **Segurança**.

A página Chaves de criptografia é exibida.

2 No menu suspenso Ações, selecione **Importar**.

Aparece a caixa de diálogo Importar chave.

3 Na caixa de diálogo Importar chave, clique em **Procurar** para localizar a chave de criptografia que você deseja importar, selecione a chave e clique em **Abrir**.

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

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

Exportação de uma chave de criptografia

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

Para exportar uma chave de criptografia

1 Navegue até o AppAssure 5 Core Console, clique na guia Configuração e depois selecione **Segurança**.

2 No menu suspenso Configuração da chave de criptografia que você deseja exportar, selecione **Exportar**.

Aparece a caixa de diálogo Exportar chave.

3 Na caixa de diálogo Exportar chave, clique em **Salvar arquivo** para salvar e armazenar as chaves de criptografia em um local seguro e clique em **OK**.

Remoção de uma chave de criptografia

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

Para remover uma chave de criptografia

1 Navegue até o AppAssure 5 Core Console, clique na guia Configuração e depois selecione **Segurança**.

2 No menu suspenso Configuração da chave de criptografia que você deseja remover, selecione **Remover**.

Você verá uma mensagem confirmando a ação de remover a chave de criptografia.

3 Na caixa de diálogo Remover chave, confirme que deseja remover a chave de criptografia.

NOTA: Remover uma chave de criptografia não remove a criptografia dos dados.

A caixa de diálogo é fechada e a chave de criptografia removida não aparece mais na página Chaves de criptografia.

Gerenciando contas em nuvem

É possível definir links para contas de provedores de armazenamento em nuvem existentes no AppAssure 5. Depois de associar suas credenciais com as configurações da Nuvem no Core Console, é possível arquivar os dados na nuvem, e importar os dados arquivados dela.

Consulte os seguintes tópicos para gerenciar suas contas em nuvem no AppAssure 5:

- Adicionar uma conta em nuvem
- Editar uma conta em nuvem
- Configuração das definições da conta em nuvem
- Remover uma conta em nuvem

Adicionar uma conta em nuvem

Antes que possa exportar seus dados arquivados para uma nuvem, você deve adicionar as informações da conta em seu provedor da nuvem ao AppAssure 5 Core Console. Para adicionar uma conta em nuvem, execute as etapas do procedimento a seguir.

Adicionar uma conta em nuvem

1. No AppAssure 5 Core Console, clique na guia Ferramentas.
2. No menu à esquerda, clique em **Nuvens**.
3. Na página Nuvens, clique em **Adicionar nova conta**.

   A caixa de diálogo Adicionar nova conta é aberta.
4. Selecione um provedor de nuvem compatível da lista suspensa Tipo de nuvem.
5. Insira os detalhes descritos na tabela a seguir com base no tipo de nuvem selecionado no Etapa 4.

Tipo de nuvem	Caixa de texto	Descrição
Microsoft Azure	Nome da conta de armazenamento	Insira o nome de sua conta de armazenamento do Windows Azure.
	Chave de acesso	Insira a chave de acesso para sua conta.
	Nome de exibição	Crie um nome de exibição para esta conta em AppAssure 5. Por exemplo, Windows Azure 1.
Amazon S3	Chave de acesso	Insira a chave de acesso para sua conta em nuvem da Amazon.
	Chave secreta	Insira a chave secreta para esta conta.
	Nome de exibição	Crie um nome de exibição para esta conta em AppAssure 5. Por exemplo, Amazon 1.

Tipo de nuvem	Caixa de texto	Descrição
Fornecido pelo OpenStack	Nome de usuário	Insira o nome de usuário para sua conta em nuvem baseada no OpenStack.
	Chave API	Insira a chave API para sua conta.
	Nome de exibição	Crie um nome de exibição para esta conta em AppAssure 5. Por exemplo, OpenStack 1.
	ID do locatário	Insira seu ID do locatário para esta conta.
	URL de autenticação	Insira a URL de autenticação para esta conta.
Rackspace Cloud Block Storage	Nome de usuário	Insira o nome de usuário para sua conta em nuvem do Rackspace.
	Chave API	Insira a chave API para esta conta.
	Nome de exibição	Crie um nome de exibição para esta conta em AppAssure 5. Por exemplo, Rackspace 1.

6 Clique em **Adicionar**.

A caixa de diálogo fecha, e sua conta aparece na página Nuvens do Core Console.

Editar uma conta em nuvem

Se for necessário alterar as informações para se conectar à sua conta em nuvem, por exemplo, para atualizar a senha ou editar o nome de exibição, é possível fazer isso na guia Ferramentas do Core Console. Execute as etapas do procedimento a seguir para editar uma conta em nuvem.

Editar uma conta em nuvem

1 No AppAssure 5 Core Console, clique na guia Ferramentas.

2 No menu à esquerda, clique em **Nuvens**.

3 Ao lado da conta em nuvem que desejar editar, clique no menu suspenso, e depois clique em **Editar**.

A janela Editar conta é aberta.

4 Edite os detalhes conforme necessário e clique em **Salvar**.

NOTA: Não é possível editar o tipo de nuvem.

Configuração das definições da conta em nuvem

As definições de configuração em nuvem permitem que você determine a quantidade de vezes que AppAssure 5 deve tentar se conectar à sua conta em nuvem, e quanto tempo deve passar para essas tentativas antes que o tempo delas acabe. Execute as etapas do procedimento a seguir para configurar as definições da conexão para sua conta em nuvem.

Configurar definições da conta em nuvem

1 No AppAssure 5 Core Console, clique na guia Configuração.

2 No menu à esquerda, clique em **Configurações**.

3 Na página Configurações, role para baixo até Configuração da nuvem.

4 Clique no menu suspenso ao lado da conta em nuvem que você desejar configurar, e depois realize os passos a seguir:

- Clique em **Editar**.

  A caixa de diálogo Configuração da nuvem é exibida.

a Use as setas para cima e para baixo para editar as seguintes opções:

- **Tempo limite de solicitação.** Exibido em minutos e segundos, ele determina a quantidade de tempo que AppAssure 5 deve passar em uma única tentativa para se conectar à conta em nuvem quando houver um atraso. As tentativas de conexão irão parar depois da quantidade de tempo inserida.
- **Tentar a contagem novamente.** Determina a quantidade de tentativas que AppAssure 5 deve realizar antes de determinar que a conta em nuvem não possa ser atingida.
- **Tamanho da memória intermediária de gravação.** Determina o tamanho da memória intermediária reservada para gravar dados arquivados na nuvem.
- **Tamanho da memória intermediária de leitura.** Determina o tamanho do bloqueio reservado para ler dados arquivados da nuvem.

b Clique em **Avançar**.

- Clique em **Redefinir**.

  Volta a configuração às seguintes definições padrão:

  - **Tempo limite de solicitação:** 01:30 (minutos e segundos)
  - **Tentar a contagem novamente:** 3 (tentativas)

Remover uma conta em nuvem

Se você interromper seu serviço em nuvem, ou decidir parar de usá-lo em um Core específico, você pode desejar remover sua conta em nuvem do Core Console. Execute as etapas do procedimento a seguir para remover uma conta em nuvem.

Remover uma conta em nuvem

1 No AppAssure 5 Core Console, clique na guia Ferramentas.

2 No menu à esquerda, clique em **Nuvens**.

3 Ao lado da conta em nuvem que desejar editar, clique no menu suspenso, e depois clique em **Remover**.

4 Na janela Excluir conta, clique em **Sim** para confirmar que deseja remover a conta.

5 Se a conta em nuvem estiver atualmente em uso, uma segunda janela pergunta se você ainda deseja removê-la. Clique em **Sim** para confirmar.

> **NOTA:** Remover uma conta atualmente em uso faz com que todos os trabalhos de arquivamento para esta conta falhem.

Sobre a replicação

Esta seção fornece informações conceituais e de procedimentos para ajudá-lo a entender e configurar a replicação no AppAssure 5.

Replicação é o processo de copiar pontos de recuperação e transmiti-los a um local secundário para fins de recuperação após desastres. O processo exige uma solução com pares de origem/destino entre dois cores. O core de origem copia os pontos de recuperação dos agentes protegidos e, em seguida, transmite-os de forma assíncrona e contínua para um core de destino em um site remoto de recuperação após desastres. O lugar fora do local pode ser um data center de propriedade da empresa (core autogerenciado), um local de terceiros de um provedor de serviços gerenciados (MSPs) ou um ambiente de nuvem. Ao replicar para um MSP, é possível usar fluxos de trabalho incorporados que permitem solicitar conexões e receber notificações automáticas de feedback.

Os possíveis cenários de replicação incluem:

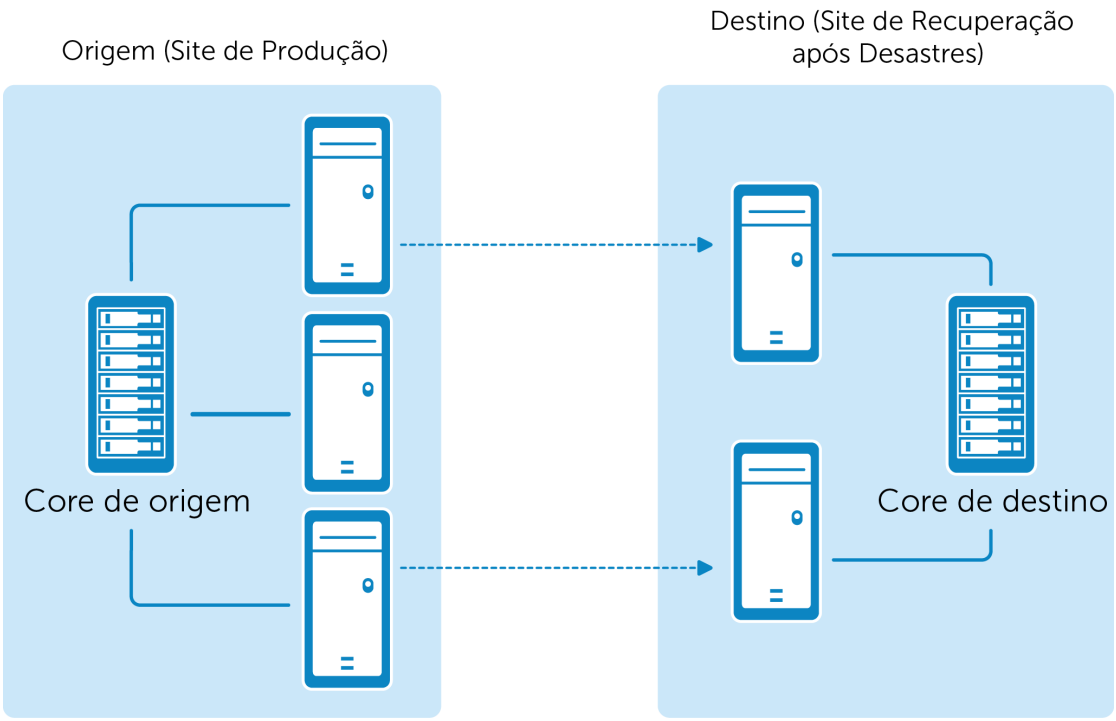
- **Replicação para uma localização local.** O core de destino situa-se em um centro de dados local ou localização no local e a replicação é sempre mantida. Nessa configuração, a perda do Core não impediria a recuperação.
- **Replicação para uma localização externa.** O core de destino está localizado em uma instalação de recuperação após desastres externa para recuperação em caso de perda.
- **Replicação mútua.** Dois centros de dados em dois locais diferentes, cada um contendo um core, que são agentes de proteção e que servem de cópia de segurança externa de recuperação após desastres um para o outro. Nesse cenário, cada core replica os agentes do Core que está localizado no outro centro de dados.
- **Replicação hospedada e na nuvem.** Os parceiros MSP do AppAssure mantêm vários cores de destino em um centro de dados ou uma nuvem pública. Em cada um desses cores, o parceiro MSP permite que um ou mais dos seus clientes replique os pontos de recuperação a partir de um core de origem no local do cliente para o core de destino do MSP por uma taxa.

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

As possíveis configurações de replicação incluem:

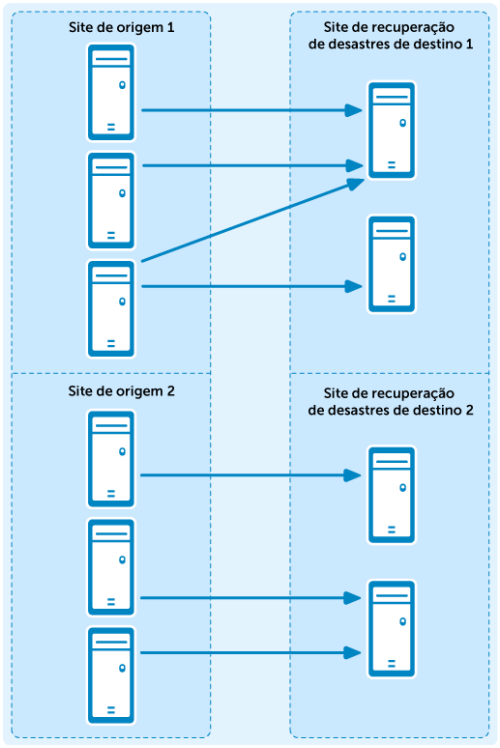
- **Ponto a ponto.** Replica um único agente a partir de um único core de origem para um único core de destino.

Figura 4. Configuração ponto a ponto



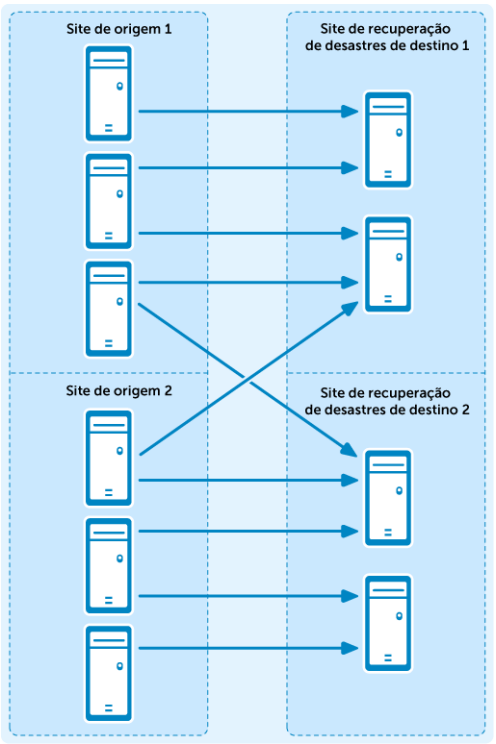
- **Multiponto a ponto.** Replica agentes a partir de vários cores de origem para um único core de destino.

Figura 5. Configuração multiponto a ponto



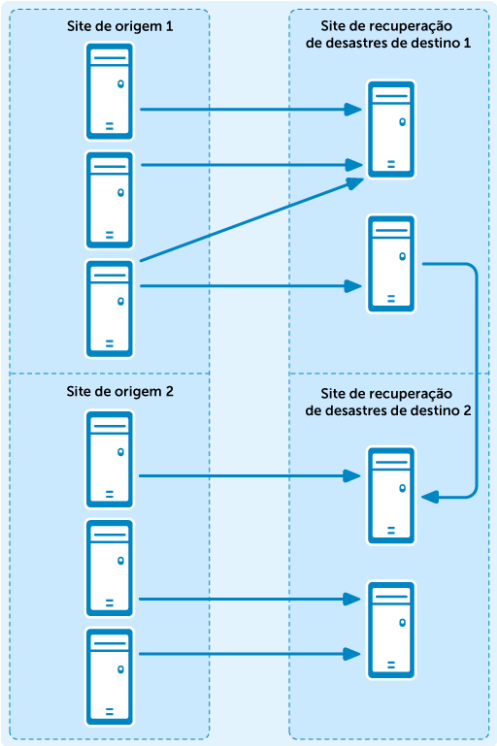
- **Ponto a multiponto.** Replica um agente a partir de um único core de origem para mais de um core de destino.

Figura 6. Configuração ponto a multiponto



- **Saltos múltiplos.** Replica um agente replicado de um core de destino para outro core de destino, produzindo uma opção adicional de ativação pós-falha ou de recuperação.

Figura 7. Configuração de saltos múltiplos



Sobre propagação

A replicação começa pela propagação, ou seja, a transferência inicial de imagens de base de deduplicação e Snapshot sincrementais dos agentes protegidos, que pode acrescentar centenas ou milhares de gigabytes de dados. A replicação inicial pode ser propagada para o core de destino por uma conexão de rede ou criando e salvando uma unidade de seeding em mídia externa e, depois, transferindo os dados iniciais para o core de destino. Normalmente, essa unidade de seeding é útil para grandes conjuntos de dados ou sites com links lentos.

NOTA: Embora seja possível propagar os dados da base por uma conexão de rede, isso não é recomendado. A propagação inicial envolve quantidades de dados potencialmente muito grandes, o que pode sobrecarregar uma conexão WAN típica. Por exemplo, se os dados de propagação medirem 10 GB e o link WAN transferir 24 Mbps, a transferência pode demorar cerca de uma hora para ser concluída.

Os dados do arquivo de propagação são compactados e, opcionalmente, criptografados e deduplicados. Se o tamanho total do arquivo for superior ao espaço disponível na mídia removível, o arquivo pode ocupar vários dispositivos, com base no espaço disponível nas mídias. Após a replicação ser estabelecida, todos os pontos de recuperação criados após o estabelecimento da unidade de seeding são replicados para o local de destino antes da transferência dos dados arquivados. Quando a unidade de seeding é consumida, os dados arquivados são sincronizados com os pontos de recuperação replicados presentes no repositório do core de destino.

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

- A primeira parte envolve a cópia, que é a gravação dos dados replicados iniciais em uma fonte de mídia removível. Há duas opções de cópia: a duplicação de pontos de recuperação ainda não replicados a partir do core de origem para um dispositivo de armazenamento removível local, como unidade USB, ou duplicação de todos os pontos de recuperação existentes [opção Construir cadeias de RP (corrigir órfãos)]. Após a cópia estar concluída, você deve transportar a unidade do local do core de origem para o local remoto do core de destino.

- A segunda parte é consumir, o que ocorre quando um core de destino recebe a unidade transportada e copia os dados replicados no repositório. O core de destino consome então os pontos de recuperação e os usa para formar agentes replicados.

  NOTA: Embora a replicação de snapshots incrementais possa ocorrer entre os cores de origem e de destino antes de a propagação ser concluída, os snapshots replicados transmitidos da origem para o destino permanecem "órfãos" até que os dados iniciais sejam consumidos, e eles são combinados com as imagens de base replicadas. Para obter mais informações sobre pontos de recuperação órfãos, consulte Exclusão de uma cadeia de pontos de recuperação órfãos.

Como grandes quantidades de dados precisam ser copiadas para o dispositivo de armazenamento portátil, recomenda-se o uso de uma conexão eSATA, USB 3.0 ou outra de alta velocidade com o dispositivo.

Sobre ativação e a reativação pós-falha no AppAssure 5

No caso de uma interrupção grave na qual há falha do seu core de origem e agentes, o AppAssure 5 suporta a ativação e a reativação pós-falha em ambientes replicados. Ativação pós-falha refere-se à mudança para um AppAssure 5 Core redundante ou de destino de espera em caso de falha do sistema ou encerramento anormal de um core de origem e de agentes associados. O principal objetivo da ativação pós-falha é iniciar um novo agente idêntico àquele que falhou e que estava protegido pelo core de origem que falhou. O objetivo secundário é mudar o core de destino para um novo modo a fim de que ele proteja o agente de ativação pós-falha da mesma forma que o core de origem protegeu o agente inicial, antes da falha. O core de destino pode recuperar instâncias de agentes replicados e iniciar imediatamente a proteção nas máquinas de ativação pós-falha.

Reativação pós-falha é o processo de restaurar um agente e core de volta aos seus estados originais (antes da falha). O principal objetivo da reativação pós-falha é restaurar o agente (na maioria dos casos, é uma nova máquina que substitui um agente com falha) a um estado idêntico ao último estado do novo agente temporário. Depois de restaurado, é protegido por um core de origem restaurado. A replicação também é restaurada, e o core de destino atua novamente como destino de replicação. Para obter mais informações, consulte Roteiro de ativação e reativação pós-falha.

Sobre replicação e pontos de recuperação criptografados

Embora a unidade de seeding não contenha cópias de segurança do registro de core de origem e dos certificados, ela contém as chaves de criptografia do core de origem se os pontos de recuperação que estão sendo replicados de origem para o destino estiverem criptografados. Os pontos de recuperação replicados permanecem criptografados depois de transmitidos para o core de destino. Os proprietários ou administradores do core de destino precisam da frase de acesso para recuperar os dados criptografados.

Sobre políticas de retenção para replicação

As políticas de retenção nos cores de origem e de destino não estão sincronizadas. Rollup e exclusão ad hoc são executadas de forma independente em cada core na ação inicial, bem como durante os trabalhos ad hoc noturnos.

Para obter mais informações sobre as políticas de retenção, consulte Gerenciamento das políticas de retenção.

Considerações de desempenho para transferência de dados replicados

Se a largura de banda entre o core de origem e o de destino não puder acomodar a transferência de pontos de recuperação armazenados, a replicação começa com propagação do core de destino com imagens de base e pontos de recuperação dos servers protegidos selecionados no core de origem. O processo de propagação pode

ser realizado a qualquer momento, como parte da transferência inicial de dados para servir de base para a replicação regularmente programada, ou no caso de restabelecer a replicação de uma máquina anteriormente replicada cuja replicação tinha sido pausada ou excluída. Nesse caso, a opção Criar cadeia de ponto de recuperação deixaria copiar os pontos de recuperação ainda não replicados para uma unidade de propagação.

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

- **Taxa de alteração.** A taxa de alteração é a taxa de acumulação da quantidade de dados protegidos. A taxa depende da quantidade de dados alterados em volumes protegidos e do intervalo de proteção dos volumes. Se um conjunto de blocos altera o volume, reduzir o intervalo de proteção reduz a taxa de alteração.
- **Largura de banda.** A largura de banda é a velocidade de transferência disponível entre o core de origem e o de destino. É vital que a largura de banda seja superior à taxa de alteração para que a replicação acompanhe os pontos de recuperação criados pelos snapshots. Devido à quantidade de dados transmitidos de um core para outro, vários fluxos paralelos podem ser necessários para se obter velocidades por fio de uma conexão Ethernet de 1GB.

  NOTA: A largura de banda especificada pelo ISP 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 haja largura de banda livre suficiente para replicação a fim de acomodar a taxa de alteração.

- **Número de agentes.** É importante considerar o número de agentes protegidos por core de origem e quantos você pretende replicar no destino. O AppAssure 5 permite executar a replicação com base em server protegido, de modo que você pode decidir replicar alguns servers. Se todos os servers protegidos precisarem ser replicados, isso afetará drasticamente a taxa de alteração, em especial se a largura de banda entre os cores de origem e de destino for insuficiente para a quantidade e o tamanho dos pontos de recuperação a serem replicados.

Dependendo da configuração de rede, a replicação pode ser um processo demorado.

A Taxa de alteração máxima por Tipo de conexão de WAN é mostrada na tabela abaixo com exemplos da largura de banda necessária por gigabyte para uma taxa de alteração razoável.

Tabela 16.

Banda larga	Largura de banda	Taxa de alteração máxima
DSL	768 Kbps ou mais	330 MB por hora
Cabo	1 Mbps ou mais	429 MB por hora
T1	1,5 Mbps ou mais	644 MB por hora
Fibra	20 Mbps ou mais	8,38 GB por hora

NOTA: Para obter resultados ideais, respeite as recomendações relacionadas na tabela acima.

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

Roteiro para definição da replicação

Para replicar os dados usando o AppAssure 5, é preciso configurar os cores de origem e de destino para a replicação. Depois de configurar a replicação, é possível replicar dados do agente, monitorar e gerenciar a replicação, e realizar a recuperação.

A realização da replicação no AppAssure 5 envolve as seguintes operações:

- **Definir um repositório no core de destino.** Para obter mais informações sobre adicionar um repositório ao core de destino, consulte Criação de um repositório.
- **Configurar a replicação autogerenciada.** Para obter mais informações sobre replicar em um core de destino autogerenciado, consulte Replicar em um core de destino autogerenciado.

- **Configurar a replicação de terceiros.** Para obter mais informações sobre replicar em um core de destino de terceiros, consulte Processo de replicação em um core de destino de terceiros.
- **Replicar um agente existente.** Para obter mais informações sobre replicar um agente já protegido pelo core de origem, consulte Adição de uma máquina a uma replicação existente.
- **Consumir a unidade de seeding.** Para obter mais informações sobre consumir dados da unidade de seeding no core de destino, consulte Consumo da unidade de seeding em um core de destino.
- **Definir a prioridade de replicação de um agente.** Para obter mais informações sobre prioridades na replicação de agentes, consulte Definição da prioridade de replicação de um agente.
- **Definir uma programação de replicação para um agente.** Para obter mais informações sobre a definição de uma programação de replicação, consulte Programação de replicação.
- **Monitorar replicação conforme necessário.** Para obter mais informações sobre monitoramento de replicação, consulte Monitoramento de replicação.
- **Gerenciar as definições de replicação conforme necessário.** Para obter mais informações sobre gerenciamento das definições de replicação, consulte Gerenciamento definições de replicação.
- **Recuperar dados replicados em caso de desastre ou perda de dados.** Para obter mais informações sobre a recuperação de dados replicados, consulte Recuperação de dados replicados.

Replicar em um core de destino autogerenciado

Um core autogerenciado é um core ao qual você tem acesso, muitas vezes porque é gerenciado por sua empresa em um local externo. A replicação pode ser executada totalmente no core de origem, a menos que você escolha executar a propagação dos seus dados. A propagação exige que você consuma a unidade de seeding no core de destino depois de configurar a replicação no core de origem.

NOTA: Essa configuração se aplica à Replicação para localização externa e à Replicação mútua. O AppAssure 5 Core deve ser instalado em todas as máquinas de origem e de destino. Se estiver configurando o AppAssure 5 para replicação Multiponto a ponto, será preciso realizar essa tarefa em todos os cores de origem e no core de destino único.

Execute as etapas do procedimento a seguir para configurar seu core de origem a fim de replicar em um core de destino autogerenciado.

Para replicar um core de destino autogerenciado

1 Navegue até o AppAssure 5 Core Console e clique na guia ou no ícone Replicação.

2 Na guia Replicação, clique em **Adicionar core de destino**.

O Assistente de replicação é exibido.

3 Na página Core de destino do Assistente de replicação, selecione **Tenho meu próprio core de destino** e insira as informações conforme descrito na tabela a seguir.

NOTA: Com o AppAssure 5, é possível replicar no Dell DL-4000. Para obter informações sobre esse recurso, consulte as *Notas de versão do Dell AppAssure 5* ou a Base de conhecimento do AppAssure 5 do .

Tabela 17.

Caixa de texto	Descrição
Nome do host	Insira o nome do host ou o endereço IP da máquina do Core na qual está replicando.
Port	Insira o número da porta pela qual o AppAssure 5 Core se comunicará com a máquina. O número de porta padrão é *8006*.

Tabela 17.

Caixa de texto	Descrição
Nome de usuário	Insira o nome de usuário para acessar a máquina.
Senha	Insira a senha para acessar a máquina.

- Se o Core que você deseja adicionar foi emparelhado com este core de origem anteriormente, você pode fazer o seguinte:
  a Selecione **Usar um core de destino existente**.
  b Selecione o core de destino na lista suspensa.
  c Clique em **Avançar**.
  d Vá para a Etapa 7.

4 Clique em **Avançar**.

> **NOTA:** Se não existir repositório no core de destino, aparecerá um aviso informando que é possível parear o core de origem com o de destino, mas que não poderá replicar agentes nesse local até que um repositório seja estabelecido. Para obter informações sobre como definir um repositório em um core, consulte Criação de um repositório.

5 Na página Detalhes, digite um nome para essa configuração de replicação, por exemplo, SourceCore1.

- Se você estiver reiniciando ou reparando uma configuração de replicação anterior, selecione **Meu Core foi migrado e eu gostaria de reparar a replicação**.

6 Clique em **Avançar**.

7 Na página Agentes, selecione os agentes que deseja replicar e use as listas suspensas na coluna Repositório para selecionar um repositório para cada agente.

8 Se desejar realizar o processo de propagação para a transferência dos dados de base, execute as seguintes etapas:

> **NOTA:** Como grandes quantidades de dados precisam ser copiadas para o dispositivo de armazenamento portátil, recomenda-se o uso de uma conexão eSATA, USB 3.0 ou outra de alta velocidade com o dispositivo.

a Na página Agentes, selecione *Usar uma unidade de seeding para realizar a transferência inicial*.
- Se você atualmente tem um ou mais agentes replicando em um core de destino, poderá incluí-los na unidade de seeding, selecionando **Com já replicado**.

b Clique em **Avançar**.

c Na página Local da unidade de propagação, use a lista suspensa **Tipo de local** para selecionar entre os seguintes tipos de destino:
- Local
- Rede
- Nuvem

d Insira os detalhes do arquivo, como descrito na tabela a seguir, com base no tipo de localização que você selecionou no Etapa c.

Tabela 18.

Opção	Caixa de texto	Descrição
Local	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, d:\work\archive.
Rede	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, \\servername\sharename.
	Nome de usuário	Insira um nome de usuário. Ele é usado para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira uma senha para o caminho de rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta em nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é AppAssure-5-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

e Clique em **Avançar**.

f Na página Opções da unidade de seeding, insira as informações conforme descrito na tabela a seguir.

Tabela 19.

Item	Descrição
Tamanho máximo	Grandes arquivos de dados podem ser divididos em vários segmentos. Selecione o tamanho máximo do segmento que deseja reservar para criar a unidade de seeding efetuando uma das seguintes ações: • Selecione **Destino inteiro** para reservar todo o espaço disponível no caminho fornecido na página Local da unidade de seeding para uso futuro (por exemplo, se o local for D:\work\archive, todo o espaço disponível na unidade D: será reservado se for necessário para copiar a unidade de seeding, mas não será reservado imediatamente após o início do processo de cópia). • Selecione a caixa de texto em branco, insira uma quantidade e depois selecione uma unidade de medida na lista suspensa para personalizar o espaço máximo que você deseja reservar.
ID do cliente (opcional)	Como opção, insira o ID do cliente que foi atribuído a você pelo provedor de serviços.
Reciclar ação	Caso o caminho já tenha uma unidade de seeding, selecione uma das seguintes opções: • **Não reutilizar.** Não substituir ou apagar quaisquer dados de propagação existentes no local. Se o local não estiver vazio, a gravação da unidade de seeding falhará. • **Substituir este Core.** Substitui quaisquer dados de propagação preexistentes pertencentes a este core, porém deixando os dados de outros cores intactos. • **Apagar completamente.** Apaga todos os dados do diretório antes de gravar a unidade de seeding.

Tabela 19.

Item	Descrição
Comentários	Insira um comentário descrevendo a unidade de seeding.
Adicionar todos os agentes à unidade de seeding	Selecione esta opção para replicar todos os agentes no core de origem usando a unidade de seeding. Esta opção é selecionada por padrão.
Construir cadeias de RP (corrigir órfãos)	Selecione esta opção para replicar toda a cadeia do ponto de recuperação na unidade de seeding. Esta opção é selecionada por padrão. **NOTA:** A propagação típica no AppAssure 5.4 replica apenas o último ponto de recuperação na unidade de seeding, o que reduz a quantidade de tempo e espaço necessária para a criação da unidade de seeding. A opção de construir cadeias do ponto de recuperação (RP) na unidade de seeding exige espaço suficiente na unidade de seeding para armazenar os mais recentes pontos de recuperação dos agentes especificados, e a tarefa pode levar mais tempo para ser concluída.
Usar formato compatível	Selecione essa opção para criar a unidade de seeding em um formato compatível com versões novas e antigas do AppAssure 5 Core. **NOTA:** O formato atual da unidade de seeding não é compatível com versões 5.3 do Core. Os arquivos criados no AppAssure 5.3 são compatíveis com o AppAssure 5.4.

g Realize um dos procedimentos a seguir:

- Se você tiver desmarcado a caixa de seleção **Adicionar todos os agentes à unidade de seeding**, clique em **Avançar**.
- Se tiver selecionado **Adicionar todos os agentes à unidade de seeding**, vá para a Etapa 9.

h Na página Agentes, selecione os agentes que você deseja replicar no core de destino usando a unidade de seeding.

9 Clique em **Concluir**.

10 Se tiver criado uma unidade de seeding, envie-a para seu core de destino.

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

Processo de replicação em um core de destino de terceiros

Um core de terceiros é um core de destino gerenciado e mantido por um MSP. Replicar em um core gerenciado por terceiros não exige que o cliente tenha acesso ao core de destino.

O processo de replicação em um core de terceiros envolve tarefas que devem ser executadas pelo cliente, bem como por terceiros. Depois de o cliente enviar uma solicitação de replicação nos cores de origem, o MSP deve executar a configuração do core de destino, revisando a solicitação.

NOTA: Essa configuração se aplica a replicação hospedada e na nuvem. O AppAssure 5 Core deve ser instalado em todas as máquinas de core de origem. Se estiver configurando o AppAssure 5 para replicação Multiponto a ponto, será preciso realizar essa tarefa em todos os cores de origem.

Para replicar em um core de destino gerenciado por terceiros, execute as seguintes tarefas:

1 Envio de uma solicitação de replicação para um provedor de serviços de terceiros

2 Revisão de uma solicitação de replicação de um cliente ou Desconsideração de uma solicitação de replicação de um cliente

Envio de uma solicitação de replicação para um provedor de serviços de terceiros

Se você for um usuário final que assina um core gerenciado por terceiros, como um MSP, execute as etapas deste procedimento para enviar uma solicitação de replicação ao seu provedor de serviços de terceiros.

Para enviar uma solicitação de replicação a um provedor de serviços de terceiros

1 Navegue até o AppAssure 5 Core e clique na guia Replicação ou no símbolo de replicação na coluna à esquerda.

2 Na guia Replicação, clique em **Adicionar core de destino**.

O Assistente de replicação é exibido.

3 Na página Core de destino do Assistente de replicação, selecione **Eu possuo uma assinatura com um terceiro que oferece cópia de segurança em outro local e serviços de recuperação após desastres** e, depois, insira as informações conforme descrito na tabela a seguir.

Tabela 20.

Caixa de texto	Descrição
Nome do host	Insira o nome de host, endereço IP ou FQDN da máquina de core de terceiros.
Port	Insira o número da porta lhe foi fornecido pelo seu provedor de serviços de terceiros. O número de porta padrão é *8006*.

- Se o Core que você deseja adicionar foi emparelhado com este core de origem anteriormente, você pode fazer o seguinte:

  a Selecione **Usar um core de destino existente**.

  b Selecione o core de destino na lista suspensa.

  c Clique em **Avançar**.

  d Vá para a Etapa 7.

4 Clique em **Avançar**.

5 Na página Detalhes, insira as informações conforme descrito na tabela a seguir.

Tabela 21.

Caixa de texto	Descrição
Endereço de e-mail	Insira o endereço de e-mail associado à sua assinatura de serviço de terceiros.
ID do cliente (opcional)	Como opção, insira o ID do cliente que foi atribuído a você pelo provedor de serviços.

6 Clique em **Avançar**.

7 Na página Agentes, selecione os agentes que deseja replicar no core de terceiros.

8 Se desejar realizar o processo de propagação para a transferência dos dados de base, execute as seguintes etapas.

NOTA: Como grandes quantidades de dados precisam ser copiadas para o dispositivo de armazenamento portátil, recomenda-se o uso de uma conexão eSATA, USB 3.0 ou outra de alta velocidade com o dispositivo.

a Na página Agentes, selecione *Usar uma unidade de seeding para realizar a transferência inicial*.

- Se você atualmente tem um ou mais agentes replicando em um core de destino, poderá incluí-los na unidade de seeding, selecionando **Com já replicado**.

b Clique em **Avançar**.

c Na página Local da unidade de propagação, use a lista suspensa **Tipo de local** para selecionar entre os seguintes tipos de destino:

- Local
- Rede
- Nuvem

d Insira os detalhes do arquivo, como descrito na tabela a seguir, com base no tipo de localização que você selecionou no Etapa c.

Tabela 22.

Opção	Caixa de texto	Descrição
Local	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, d:\work\archive.
Rede	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, \\servername\sharename.
	Nome de usuário	Insira um nome de usuário. Ele é usado para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira uma senha para o caminho de rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta em nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é AppAssure-5-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

e Clique em **Avançar**.

f Na página Opções da unidade de seeding, insira as informações conforme descrito na tabela a seguir.

Tabela 23.

Item	Descrição
Tamanho máximo	Grandes arquivos de dados podem ser divididos em vários segmentos. Selecione a quantidade máxima de espaço que você deseja reservar para criar a unidade de seeding efetuando uma das seguintes ações: • Selecione **Destino inteiro** para reservar todo o espaço disponível no caminho fornecido na página Local da unidade de seeding (por exemplo, se o local for D:\work\archive, todo o espaço disponível na unidade D: será reservado). • Selecione a caixa de texto em branco, insira uma quantidade e depois selecione uma unidade de medida na lista suspensa para personalizar o espaço máximo que você deseja reservar.
ID do cliente (opcional)	Como opção, insira o ID do cliente que foi atribuído a você pelo provedor de serviços.

Tabela 23.

Item	Descrição
Reciclar ação	Caso o caminho já tenha uma unidade de seeding, selecione uma das seguintes opções: • **Não reutilizar.** Não substituir ou apagar quaisquer dados de propagação existentes no local. Se o local não estiver vazio, a gravação da unidade de seeding falhará. • **Substituir este Core.** Substitui quaisquer dados de propagação preexistentes pertencentes a este core, porém deixando os dados de outros cores intactos. • **Apagar completamente.** Apaga todos os dados do diretório antes de gravar a unidade de seeding.
Comentários	Insira um comentário descrevendo a unidade de seeding.
Adicionar todos os agentes à unidade de seeding	Selecione esta opção para replicar todos os agentes no core de origem usando a unidade de seeding. Esta opção é selecionada por padrão.
Construir cadeias de RP (corrigir órfãos)	Selecione esta opção para replicar toda a cadeia do ponto de recuperação na unidade de seeding. Esta opção é selecionada por padrão. **NOTA:** A propagação típica no AppAssure 5.4 replica apenas o último ponto de recuperação na unidade de seeding, o que reduz a quantidade de tempo e espaço necessária para a criação da unidade de seeding. A opção de construir cadeias do ponto de recuperação (RP) na unidade de seeding exige espaço suficiente na unidade de seeding para armazenar os mais recentes pontos de recuperação dos agentes especificados, e a tarefa pode levar mais tempo para ser concluída.
Usar formato compatível	Selecione essa opção para criar a unidade de seeding em um formato compatível com versões novas e antigas do AppAssure 5 Core. **NOTA:** O formato atual da unidade de seeding não é compatível com versões 5.3 do Core. Os arquivos criados no AppAssure 5.3 são compatíveis com o AppAssure 5.4.

g Realize um dos procedimentos a seguir:

- Se você tiver desmarcado a caixa de seleção **Adicionar todos os agentes à unidade de seeding**, clique em **Avançar**.
- Se tiver selecionado **Adicionar todos os agentes à unidade de seeding**, vá para a Etapa 9.

h Na página Agentes, selecione os agentes que você deseja replicar no core de destino usando a unidade de seeding.

9 Clique em **Concluir**.

10 Se tiver criado uma unidade de seeding, envie-a conforme indicado pelo seu provedor de serviços de terceiros.

Revisão de uma solicitação de replicação de um cliente

Depois que o usuário final concluir o procedimento Envio de uma solicitação de replicação para um provedor de serviços de terceiros, uma solicitação de replicação será enviada do core de origem para o core de destino de terceiros. Como terceiro, você pode revisar a solicitação e aprová-la para começar a replicação para seu cliente, ou pode negá-la para impedir que a replicação ocorra.

Escolha entre as opções a seguir:

- Aprovação de uma solicitação de replicação
- Negação de uma solicitação de replicação

Aprovação de uma solicitação de replicação

Execute o procedimento a seguir para aprovar uma solicitação de replicação em um core de destino de terceiros.

Para aprovar uma solicitação de replicação

1. No core de destino, abra o AppAssure 5 Core Console e clique na guia ou no ícone Replicação.
2. Na guia Replicação, clique em **Solicitações pendentes (#)**.

   A seção Solicitações de replicação pendentes é exibida.
3. Em Solicitações de replicação pendentes, clique no menu suspenso ao lado da solicitação que deseja revisar e depois clique em **Revisar**.

   A janela Revisar solicitações de replicação é exibida.

   NOTA: As informações que aparecem na seção Identidade do core de origem dessa janela são determinadas pela solicitação executada pelo cliente.
4. Em Identidade do core de origem, realize um dos procedimentos a seguir:
   - Selecione Substituir um Core replicado existente e selecione um core na lista suspensa.
   - Selecione Criar um novo Core de origem e confirme se o Nome do Core, Endereço de e-mail do cliente e ID do cliente fornecidos estão corretos. Edite as informações conforme necessário.
5. Em Agentes, selecione as máquinas às quais se aplica a aprovação e use as listas suspensas na coluna Repositório para selecionar o repositório apropriado a cada máquina.
6. Como opção, na caixa de texto Comentário, insira uma descrição ou mensagem para ser incluída na resposta ao cliente.
7. Clique em **Enviar resposta**.

   A replicação é aceita.

Negação de uma solicitação de replicação

Execute as etapas do procedimento a seguir para negar uma solicitação de replicação enviada a um core de terceiros a partir de um cliente.

Para negar uma solicitação sem revisá-la, consulte Desconsideração de uma solicitação de replicação de um cliente.

Para negar uma solicitação de replicação

1. No core de destino, abra o AppAssure 5 Core Console e clique na guia ou no ícone Replicação.
2. Na guia Replicação, clique em **Solicitações pendentes (#)**.

   A seção Solicitações de replicação pendentes é exibida.
3. Em Solicitações de replicação pendentes, clique no menu suspenso ao lado da solicitação que deseja revisar e depois clique em **Revisar**.

   A janela Revisar solicitações de replicação é exibida.
4. Clique em **Negar**.

   A replicação é negada. A notificação de negação aparece sob Alertas na guia Eventos do core de origem.

Desconsideração de uma solicitação de replicação de um cliente

Como prestador de serviço de terceiros de um core de destino, você tem a opção de ignorar uma solicitação de replicação enviada por um cliente. Essa opção pode ser usada se a solicitação tiver sido enviada por engano ou se você quiser negar uma solicitação sem revisá-la.

Para obter mais informações sobre solicitações de replicação, consulte Revisão de uma solicitação de replicação de um cliente.

Execute o procedimento a seguir para ignorar uma solicitação de replicação de um cliente.

Para ignorar uma solicitação de replicação de um cliente

1. No core de destino, abra o AppAssure 5 Core Console e clique na guia ou no ícone Replicação.
2. Na guia Replicação, clique em **Solicitações pendentes (#)**.

   A seção Solicitações de replicação pendentes é exibida.
3. Em Solicitações de replicação pendentes, clique no menu suspenso ao lado da solicitação que deseja ignorar e depois clique em **Ignorar**.
4. Na caixa de diálogo Desconsideração de solicitação, clique em **Sim** para confirmar o comando.

   Uma notificação de que a solicitação foi ignorada é enviada ao core de origem, e a solicitação é removida da guia Replicação do core de destino.

Adição de uma máquina a uma replicação existente

Após a replicação ser estabelecida entre um core de origem e de destino, é possível adicionar novos agentes para replicar no destino. Execute as etapas do procedimento a seguir para adicionar um novo agente a um core de destino pareado para replicação.

Para obter mais informações sobre a replicação, consulte Sobre a replicação e Replicar em um core de destino autogerenciado.

Para adicionar uma máquina a uma replicação existente

1. No AppAssure 5 Core Console, clique no ícone ou guia Replicação.
2. Clique no menu suspenso ao lado do core de destino ao qual deseja replicar uma nova máquina e depois clique em **Adicionar máquinas**.

   O Assistente de replicação se abre na página Agentes.
3. Na página Agentes, selecione os agentes que deseja replicar e use as listas suspensas na coluna Repositório para selecionar um repositório para cada agente.
4. Se desejar realizar o processo de propagação para a transferência dos dados de base, execute as seguintes etapas:

   NOTA: Como grandes quantidades de dados precisam ser copiadas para o dispositivo de armazenamento portátil, recomenda-se o uso de uma conexão eSATA, USB 3.0 ou outra de alta velocidade com o dispositivo.

   a. Na página Agentes, selecione *Usar uma unidade de seeding para realizar a transferência inicial*.
      - Se você atualmente tem um ou mais agentes replicando em um core de destino, poderá incluí-los na unidade de seeding, selecionando **Com já replicado**.

   b. Clique em **Avançar**.

c Na página Local da unidade de seeding, use a lista suspensa **Tipo de local** para selecionar entre os seguintes tipos de destino:

- Local
- Rede
- Nuvem

d Insira os detalhes do arquivo, como descrito na tabela a seguir, com base no tipo de localização que você selecionou no Etapa c.

Tabela 24.

Opção	Caixa de texto	Descrição
Local	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, d:\work\archive.
Rede	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, \\servername\sharename.
	Nome de usuário	Insira um nome de usuário. Ele é usado para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira uma senha para o caminho de rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta em nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é AppAssure-5-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

e Clique em **Avançar**.

f Na página Opções da unidade de seeding, insira as informações conforme descrito na tabela a seguir.

Tabela 25.

Item	Descrição
Tamanho máximo	Grandes arquivos de dados podem ser divididos em vários segmentos. Selecione a quantidade máxima de espaço que você deseja reservar para criar a unidade de seeding efetuando uma das seguintes ações: • Selecione **Destino inteiro** para reservar todo o espaço disponível no caminho fornecido na página Local da unidade de seeding (por exemplo, se o local for D:\work\archive, todo o espaço disponível na unidade D: será reservado). • Selecione a caixa de texto em branco, insira uma quantidade e depois selecione uma unidade de medida na lista suspensa para personalizar o espaço máximo que você deseja reservar.
ID do cliente (opcional)	Como opção, insira o ID do cliente que foi atribuído a você pelo provedor de serviços.

Tabela 25.

Item	Descrição
Reciclar ação	Caso o caminho já tenha uma unidade de seeding, selecione uma das seguintes opções: • **Não reutilizar.** Não substituir ou apagar quaisquer dados de propagação existentes no local. Se o local não estiver vazio, a gravação da unidade de seeding falhará. • **Substituir este Core.** Substitui quaisquer dados de propagação preexistentes pertencentes a este core, porém deixando os dados de outros cores intactos. • **Apagar completamente.** Apaga todos os dados do diretório antes de gravar a unidade de seeding.
Comentários	Insira um comentário descrevendo a unidade de seeding.
Adicionar todos os agentes à unidade de seeding	Selecione esta opção para replicar todos os agentes no core de origem usando a unidade de seeding. Esta opção é selecionada por padrão.
Construir cadeias de RP (corrigir órfãos)	Selecione esta opção para replicar toda a cadeia do ponto de recuperação na unidade de seeding. Esta opção é selecionada por padrão. **NOTA:** A propagação típica no AppAssure 5.4 replica apenas o último ponto de recuperação na unidade de seeding, o que reduz a quantidade de tempo e espaço necessária para a criação da unidade de seeding. A opção de construir cadeias do ponto de recuperação (RP) na unidade de seeding exige espaço suficiente na unidade de seeding para armazenar os mais recentes pontos de recuperação dos agentes especificados, e a tarefa pode levar mais tempo para ser concluída.
Usar formato compatível	Selecione essa opção para criar a unidade de seeding em um formato compatível com versões novas e antigas do AppAssure 5 Core. **NOTA:** O formato atual da unidade de seeding não é compatível com versões 5.3 do Core. Os arquivos criados no AppAssure 5.3 são compatíveis com o AppAssure 5.4.

g Realize um dos procedimentos a seguir:

- Se você tiver desmarcado a caixa de seleção **Adicionar todos os agentes à unidade de seeding**, clique em **Avançar**.
- Se tiver selecionado **Adicionar todos os agentes à unidade de seeding**, vá para a Etapa 5.

h Na página Agentes, selecione os agentes que você deseja replicar no core de destino usando a unidade de seeding.

5 Clique em **Concluir**.

Consumo da unidade de seeding em um core de destino

Execute o procedimento a seguir para consumir os dados da unidade de seeding no core de destino.

NOTA: Esse procedimento é necessário apenas se uma unidade de seeding tiver sido criada como parte de Replicar em um core de destino autogerenciado ou Processo de replicação em um core de destino de terceiros.

Para consumir a unidade de seeding em um core de destino

1 Se a unidade de seeding tiver sido salva em um dispositivo de armazenamento portátil, como uma unidade USB, conecte a unidade ao core de destino.

2 No core de destino, abra o AppAssure 5 Core Console e clique na guia ou no ícone Replicação.

3 Na guia Replicação, em Replicação de entrada, clique no menu suspenso, no core de origem correto e, em seguida, clique em **Consumir**.

Será exibida a janela Consumir.

4 Para **Tipo de localização**, selecione uma das seguintes opções a partir da lista suspensa:

- Local
- Rede
- Nuvem

5 Insira os detalhes do arquivo, como descrito na tabela a seguir, com base no tipo de localização que você selecionou no Etapa 4.

Tabela 26.

Opção	Caixa de texto	Descrição
Local	Local	Insira o caminho para o arquivo.
Rede	Local	Insira o caminho para o arquivo.
	Nome de usuário	Insira o nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira a senha para o caminho da rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter mais informações, consulte Adicionar uma conta em nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira o nome da pasta na qual os dados arquivados são salvos, por exemplo, AppAssure-5-Arquivo-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

6 Clique em **Verificar arquivo**.

O Core procura o arquivo.

Depois de localizar o arquivo, as seguintes caixas de texto aparecem na janela Consumir pré-preenchida com os dados obtidos em Etapa 4, Etapa 5 e o arquivo. O Período exibe as datas dos pontos de recuperação mais antigos e mais novos contidos na unidade de seeding. Qualquer comentário inserido quando a unidade de seeding foi criada é importado automaticamente.

7 Na janela Consumir, em Agentes, selecione as máquinas para as quais deseja consumir dados.

8 Clique em **Consumir**.

9 Para monitorar o progresso do consumo de dados, clique na guia Eventos.

Abandono de uma unidade de seeding pendente

Se você criar uma unidade de seeding com a intenção de consumi-la no core de destino, mas optar por não enviá-la para o local remoto, um link para a Unidade de seeding pendente permanecerá na guia de replicação do core de origem. Nesse caso, você talvez queira abandonar a unidade de seeding pendente em favor de dados diferentes ou mais atuais.

Execute as etapas do procedimento a seguir para abandonar uma unidade de seeding pendente.

NOTA: Esse procedimento remove o link da unidade pendente do AppAssure 5 Core Console no core de origem. Não remove a unidade do local de armazenamento no qual ela foi salva. Abandonar a unidade replica automaticamente todos os pontos de recuperação da unidade de seeding abandonada durante o próximo trabalho de replicação.

Para abandonar uma unidade de seeding pendente

1. No core de origem, abra o AppAssure 5 Core Console e clique na guia ou no ícone Replicação.
2. Na guia Replicação, clique em **Unidades de seeding pendentes (#)**.

   A seção Unidades de seeding pendentes aparece. Ela inclui o nome do core de destino remoto, a data e hora em que a unidade de seeding foi criada e o intervalo de dados dos pontos de recuperação incluídos na unidade de seeding.
3. Em Unidades de seeding pendentes, clique no menu suspenso da unidade que deseja abandonar e em **Abandonar**.

   A janela Unidades de seeding pendentes aparece.
4. Na janela Unidades de seeding pendentes, clique em **Sim** para confirmar.

   A unidade de seeding é removida.

   Se não houver mais unidades de seeding no core de origem, o link Unidades de seeding pendentes (#) e a seção Unidades de seeding pendentes serão removidos da guia Replicação.

Gerenciamento definições de replicação

O AppAssure 5 permite monitorar, programar e ajustar a replicação em nível global, de core e de agente.

É possível editar as seguintes definições de replicação:

- Para programar trabalhos de replicação, consulte Programação de replicação.
- Para monitorar o progresso de um trabalho de replicação, consulte Monitoramento de replicação.
- Para pausar ou retomar um trabalho de replicação em pausa, consulte Pausa e retomada da replicação.
- Para forçar a replicação de um agente de entrada ou saída, consulte Forçamento de replicação.
- Para gerenciar as definições de todos os cores de destino e procedimentos de replicação, consulte Gerenciamento de definições para replicação de saída.
- Para gerenciar as definições de um core de destino individual, consulte Alteração das definições do core de destino.
- Para gerenciar as definições de prioridade de um agente individual sendo replicado em um core de destino; consulte Definição da prioridade de replicação de um agente.

Programação de replicação

É possível usar o programador de replicação para definir o momento, como em um dia específico ou fora do horário de pico, para a transferência de dados replicados do core de origem para o de destino.

Para programar a replicação

1. No AppAssure 5 Core Console, clique no ícone ou guia Replicação.
2. Na guia Replicação, clique no menu suspenso ao lado do core para o qual deseja programar uma replicação e depois clique em **Programar**.

   Abre-se a Programação de replicação para [NomeCore].

3 Selecione uma das três opções a seguir:

- **Sempre.** Replica após cada novo snapshot, verificação de soma de verificação e verificação de capacidade de anexação, e depois da conclusão de trabalhos noturnos.
- **Diário (Iniciar replicação somente durante o período especificado).** Começa a replicar apenas dentro do intervalo de tempo fornecido.

    a Na caixa de texto **De**, digite o primeiro horário em que a replicação deve começar.

    b Na caixa de texto **A**, digite o último horário em que a replicação deve começar.

NOTA: Se a replicação estiver em andamento quando terminar o tempo programado, o trabalho de replicação é concluído depois do período de tempo alocado.

- **Personalizado.** Replica apenas dentro do intervalo de tempo fornecido no momento especificado da semana.

    a Ao lado de Dias da semana, na caixa de texto **De**, insira o primeiro horário em que a replicação deve ocorrer em um dia da semana. Depois, na caixa de texto **A**, insira o último horário em que a replicação deve ocorrer em um dia da semana.

    b Ao lado de Fins de semana, na caixa de texto **De**, insira o primeiro horário em que a replicação deve ocorrer em fins de semana. Depois, na caixa de texto **A**, insira o último horário em que a replicação deve ocorrer em fins de semana.

4 Clique em **Salvar**.

A programação é aplicada a todas as replicações do core de destino selecionado.

Monitoramento de replicação

Quando a replicação está definida, é possível monitorar o status das tarefas de replicação dos cores de origem e de destino. É possível atualizar as informações de status, visualizar detalhes de replicação, e muito mais.

Para monitorar a replicação

1 No Core Console, clique no ícone ou guia Replicação.

2 Nessa guia, é possível visualizar informações sobre tarefas de replicação e monitorar o status delas, conforme descrito na tabela a seguir.

Tabela 27.

Seção	Descrição	Ações disponíveis
Solicitações de replicação pendentes	Relaciona seu ID de cliente, endereço de e-mail e nome de host quando uma solicitação de replicação é enviada a um provedor de serviços de terceiros. Isso é relacionado aqui até que a solicitação seja aceita pelo MSP.	No menu suspenso, clique em **Ignorar** para ignorar ou rejeitar a solicitação.
Unidades de seeding pendentes	Relaciona as unidades de seeding gravadas, mas ainda não consumidas pelo core de destino. Inclui o nome de core remoto, data de criação e o período.	No menu suspenso, clique em **Abandonar** para abandonar ou cancelar o processo de propagação.

Tabela 27.

Seção	Descrição	Ações disponíveis
Replicação de saída	Relaciona todos os cores de destino nos quais o core de origem está replicando. Inclui o nome do core de destino, o estado de existência, o número de máquinas agente sendo replicadas e o progresso de uma transmissão de replicação.	Em um core de origem, no menu suspenso, é possível selecionar as seguintes opções: • **Detalhes.** Relaciona a ID, URI, nome de exibição, estado, ID do cliente, endereço de e-mail e comentários para o core replicado. • **Alterar definições.** Relaciona o nome de exibição e permite editar o host e a porta do core de destino. • **Excluir.** Permite excluir o core de destino do core de origem. Fazer isso cessa toda a replicação para esse core. • **Programar.** Permite definir uma programação personalizada para replicação nesse core de destino. • **Adicionar máquinas.** Permite selecionar um host em uma lista suspensa, selecionar agentes protegidos para replicação e criar uma unidade de seeding para a transferência inicial do novo agente.
Replicação de entrada	Relaciona todas as máquinas de origem a partir das quais o destino recebe os dados replicados. Inclui o nome de core remoto, estado, máquinas e progresso.	Em um core de destino, no menu suspenso, é possível selecionar as seguintes opções: • **Detalhes.** Relaciona o ID, nome do host, ID do cliente, endereço de e-mail e comentários para o core replicado. • **Consumir.** Consome os dados iniciais da unidade de seeding e os salva no repositório local. • **Excluir.** Permite excluir o core de origem do core de destino. Fazer isso cessa toda a replicação desse core.

Pausa e retomada da replicação

É possível pausar a replicação temporariamente para os cores de origem (saída) ou de destino (entrada).

Para pausar e retomar uma replicação

1 No Core Console, clique na guia Replicação.

2 Use o sinal de maior que (>) para expandir o core de origem ou de destino adequado.

3 Selecione o(s) agente(s) que deseja pausar para replicar, clique no menu suspenso ao lado de Nome do agente e clique em **Pausar** para pausar temporariamente a replicação.

O status da máquina aparece como “Estabelecido (em pausa)” na coluna Estado.

4 Para retomar a replicação, selecione o agente em pausa, clique no menu suspenso Nome do agente e em **Retomar**.

Forçamento de replicação

Execute as etapas do procedimento a seguir para forçar a replicação a partir do core de origem ou de destino.

Para forçar a replicação

1 No AppAssure 5 Core Console, clique no ícone ou guia Replicação.

2 Use o sinal de maior que (>) para expandir o core de origem ou de destino adequado.

3 Realize um dos procedimentos a seguir:

- Clique no menu suspenso ao lado do agente para o qual deseja forçar a replicação e depois clique em **Forçar**.
- Selecione o(s) agente(s) que deseja forçar a replicar, clique no menu suspenso ao lado de Nome do agente e clique em **Forçar**.

4 Na caixa de diálogo, você tem a opção de selecionar **Restaurar apenas cadeias de Ponto de recuperação órfãs** para reparar cadeias órfãs de pontos de recuperação dessa máquina no core de destino.

5 Clique em **Sim**.

Gerenciamento de definições para replicação de saída

As alterações feitas nessas definições afetam a transferência de dados para todos os cores de destino associados a esse core de origem.

Para gerenciar definições para replicação de saída

1 No Core Console, clique no ícone ou guia Replicação.

2 Clique em **Definições**.

3 Na janela Definições de replicação, edite as definições de replicação, como descrito na tabela a seguir.

Tabela 28.

Opção	Descrição
Duração do cache (segundos)	Especificar a quantidade de tempo entre cada solicitação de status de core de destino feita pelo core de origem.
Tempo limite da sessão de imagem do volume (minutos)	Especificar a quantidade de tempo que o core de origem gasta tentando transferir uma imagem de volume para o core de destino.

Tabela 28.

Opção	Descrição
Máximo de fluxos paralelos	Especificar o número de conexões de rede permitidas a serem utilizadas ao mesmo tempo por um único agente para replicar os dados da máquina.
Velocidade máxima de transferência (MB/s)	Especificar o limite de velocidade para a transferência de dados replicados.

4 Clique em **Salvar**.

Alteração das definições do core de destino

O AppAssure 5 permite alterar as definições de host e de porta para cores de destino individuais.

Para alterar as definições de core de destino

1 No AppAssure 5 Core Console, clique no ícone ou guia Replicação.

2 Ao lado do core de destino apropriado, clique no menu suspenso e em **Alterar definições**.

Aparece a janela Definições.

3 Edite uma das opções descritas na tabela a seguir.

Tabela 29.

Opção	Descrição
Host	Insira o host do core de destino.
Port	Insira uma porta para que o core de destino use para comunicação com o core de origem. NOTA: A porta padrão é 8006.

4 Clique em **Salvar**.

Definição da prioridade de replicação de um agente

Execute as etapas abaixo para editar as definições que priorizam quando o agente é replicado.

Para definir a prioridade de replicação de um agente

1 No AppAssure 5 Core Console, clique no ícone ou guia Replicação.

2 Ao lado do core de destino, clique no sinal de maior que (>) para expandir os agentes de replicação.

3 Clique no menu suspenso do agente que deseja priorizar e clique em Definições.

4 Use a lista suspensa Prioridade para selecionar uma das seguintes opções. Você pode selecionar entre 1 (mais alto) e 10 (mais baixo). A definição padrão é 5.

5 Clique em **Salvar**.

Remoção da replicação

É possível descontinuar a replicação e remover as máquinas protegidas da replicação de várias maneiras. As opções incluem:

- Remoção de um agente da replicação no core de origem
- Remoção de um agente no core de destino

- Remoção de um core de destino da replicação
- Remoção de um core de origem da replicação

> **NOTA:** Remover um core de origem resulta na remoção de todos os agentes replicados protegidos por esse core.

Remoção de um agente da replicação no core de origem

Execute as etapas deste procedimento para remover um agente da replicação no core de origem.

Para remover um agente da replicação no core de origem

1. No core de origem, abra o AppAssure 5 Core Console e clique na guia ou no ícone Replicação.
2. Expanda a seção Replicação de saída.
3. No menu suspenso da máquina agente que deseja remover da replicação, clique em **Excluir**.
4. Na caixa de diálogo Replicação de saída, clique em **Sim** para confirmar a exclusão.

Remoção de um agente no core de destino

Execute as etapas deste procedimento para remover um agente no core de destino.

Para remover um agente no core de destino

1. No core de destino, abra o AppAssure 5 Core Console e clique na guia ou no ícone Replicação.
2. Expanda a seção Replicação de entrada.
3. No menu suspenso da máquina agente que deseja remover da replicação, clique em **Excluir**.
4. Se você deseja excluir todos os pontos de recuperação replicados recebidos dessa máquina, além de remover o agente, selecione **Com pontos de recuperação**.
5. Na caixa de diálogo Replicação de entrada, clique em **Sim** para confirmar a exclusão.

Remoção de um core de destino da replicação

Execute as etapas deste procedimento para remover um core de destino da replicação.

Para remover um core de destino da replicação

1. No core de origem, abra o AppAssure 5 Core Console e clique na guia ou no ícone Replicação.
2. Em Replicação de saída, clique no menu suspenso ao lado do core remoto que deseja excluir e em **Excluir**.
3. Na caixa de diálogo Replicação de saída, clique em **Sim** para confirmar a exclusão.

Remoção de um core de origem da replicação

Execute as etapas deste procedimento para remover um core de origem da replicação.

> **NOTA:** Remover um core de origem resulta na remoção de todos os agentes replicados protegidos por esse core.

Para remover um core de origem da replicação

1. No core de destino, abra o AppAssure 5 Core Console e clique na guia ou no ícone Replicação.
2. Em Replicação de entrada, no menu suspenso, clique em **Excluir**.
3. Se você deseja excluir todos os pontos de recuperação replicados recebidos dessa máquina, além de remover o core de origem, selecione **Com pontos de recuperação**.
4. Na caixa de diálogo Replicação de entrada, clique em **Sim** para confirmar a exclusão.

Recuperação de dados replicados

A funcionalidade de replicação “Dia a dia” é mantida no core de origem, enquanto apenas o core de destino é capaz de executar as funções necessárias para a recuperação após desastres.

Para a recuperação após desastres, o core de destino pode usar os pontos de recuperação replicados para recuperar os agentes protegidos e o core. É possível executar as seguintes opções de recuperação no core de destino:

- Montar pontos de recuperação. Para obter mais informações, consulte Montagem de um ponto de recuperação de uma máquina com Windows.
- Rollback para pontos de recuperação. Para obter mais informações, consulte Restauração de volumes a partir de um ponto de recuperação ou Restauração de volumes em uma máquina com Linux usando a linha de comando.
- Realizar uma exportação de máquina virtual (VM). Para obter mais informações, consulte Exportação de dados de uma máquina com Windows para uma máquina virtual.
- Realizar uma bare metal restore (BMR). Para obter mais informações, consulte Roteiro de realização de uma bare metal restore em máquinas com Windows.
- Realizar reativação pós-falha (no caso de haver um ambiente de replicação de ativação/reativação pós-falha definido). Para obter mais informações, consulte Realização da reativação pós-falha.

Roteiro de ativação e reativação pós-falha

Ao encontrar uma situação de desastre em que seu core de origem e agente associado falham, você poderá ativar a ativação pós-falha no AppAssure 5 para mudar a proteção para seu core de ativação pós-falha idêntico (de destino) e ativar um agente novo (replicado) idêntico ao agente com falha. Depois que seu core de origem e agentes tiverem sido reparados, será possível realizar a reativação pós-falha para restaurar os dados a partir do core e agente com falha de volta ao core de origem e agente. No AppAssure 5, a ativação e reativação pós-falha envolvem os seguintes procedimentos.

- **Definição de seu ambiente para ativação pós-falha.** Consulte a seção Definição de um ambiente para ativação pós-falha.
- **Execução da ativação pós-falha do core de destino e do agente associado.** Consulte a seção Realização de ativação pós-falha no core de destino.
- **Restauração de um core de origem com a realização da reativação pós-falha.** Consulte a seção, Realização de ativação pós-falha no core de destino

Definição de um ambiente para ativação pós-falha

Definir seu ambiente para ativação pós-falha exige que você tenha um AppAssure 5 Core de origem e de destino e os agentes associados definidos para replicação. Execute as etapas deste procedimento para definir a replicação para ativação pós-falha.

Para definir um ambiente para ativação pós-falha

1. Instale um AppAssure 5 Core para a origem e outro AppAssure 5 Core para o destino. Para obter mais informações, consulte o *Guia de implementação doDell AppAssure 5*.
2. Instale um AppAssure 5 Agent a ser protegido pelo core de origem. Para obter mais informações, consulte o *Guia de implementação doDell AppAssure 5*.
3. Crie um repositório no core de origem e um no core de destino. Para obter mais informações, consulte Criação de um repositório.
4. Adicione o agente para proteção sob o core de origem. Para obter mais informações, consulte Proteção de uma máquina.
5. Defina a replicação do core de origem para o de destino e replique o agente protegido com todos os pontos de recuperação. Siga as instruções na seção Replicar em um core de destino autogerenciado para adicionar o core de destino no qual replicar.

Realização de ativação pós-falha no core de destino

Ao encontrar uma situação de desastre em que seu core de origem e agentes associados falham, você poderá ativar a ativação pós-falha no AppAssure 5 para mudar a proteção para seu core de ativação pós-falha idêntico (de destino). O core de destino torna-se o único core que protege os dados em seu ambiente e, então, você ativa um novo agente para substituir temporariamente o agente com falha.

Para realizar a ativação pós-falha no core de destino

1. Navegue até o AppAssure 5 Core Console no core de destino e clique na guia ou no ícone Replicação.
2. Em Replicação de entrada, expanda os detalhes do core de origem selecionado.
3. Clique no menu suspenso do agente preferido e em **Ativação pós-falha**.

   A caixa de diálogo Ativação pós-falha aparece e relaciona as próximas etapas necessárias para executar uma ativação pós-falha.

   - Para descontinuar quaisquer tarefas de replicação em andamento nesse agente, selecione **Cancelar trabalho de replicação se estiver em execução**.
4. Clique em **Continuar**.
5. Na área de navegação à esquerda, em Máquinas protegidas, selecione a máquina que tem o agente do AppAssure 5 associado com pontos de recuperação.
6. Exporte as informações do ponto de recuperação de cópia de segurança nesse agente para uma máquina virtual. Para obter mais informações, consulte Exportação de dados de uma máquina com Windows para uma máquina virtual.
7. Inicie a máquina virtual que agora inclui as informações de cópia de segurança exportadas. É preciso aguardar o software de driver do dispositivo ser instalado.
8. Reinicie a máquina virtual e espere que o serviço do agente comece.
9. Volte ao AppAssure 5 Core Console para o core de destino e confirme se o novo agente aparece na área de navegação à esquerda em Máquinas protegidas e na guia Replicação sob Replicação de entrada.
10. Force vários snapshots e confirme se eles são executados corretamente. Para obter mais informações, consulte Forçar snapshot.
11. Agora, continue com a realização da reativação pós-falha. Consulte a próxima seção, Realização da reativação pós-falha.

Realização da reativação pós-falha

Depois de reparar ou substituir o core de origem e os agentes com falha, é preciso mover os dados de suas máquinas com falha para restaurar as máquinas de origem.

Para realizar a reativação pós-falha

1. Navegue até o AppAssure 5 Core Console no core de destino e clique na guia ou no ícone Replicação.
2. Em Replicação de entrada, selecione o agente de ativação pós-falha e expanda os detalhes.
3. No menu Ações, clique em **Reativação pós-falha**.

   A caixa de diálogo Reativação pós-falha é aberta e descreve as etapas que precisam ser seguidas antes de clicar no botão Continuar para executar a reativação pós-falha.
4. Clique em **Cancelar**.
5. Se a máquina com falha estiver executando o Microsoft SQL Server ou o Microsoft Exchange Server, interrompa esses serviços.
6. Force um snapshot da máquina. Para obter mais informações, consulte Forçar snapshot.
7. Desligue a máquina com falha.
8. Crie um arquivo do agente com falha e envie-o para o disco ou um local de compartilhamento de rede. Para obter mais informações, consulte a seção Criação de um arquivo.
9. Após a criação do arquivo, navegue até o AppAssure 5 Core Console no core de origem recém-reparado e clique na guia Ferramentas.
10. Importe o arquivo que você acabou de criar na Etapa 8. Para obter mais informações, consulte a seção Importação de um arquivo.
11. Volte ao Core Console no core de destino e clique na guia Replicação.
12. Em Replicação de entrada, selecione o agente de ativação pós-falha e expanda os detalhes.
13. No menu suspenso do agente, clique em **Reativação pós-falha**.
14. Na caixa de diálogo Reativação pós-falha, clique em **Continuar**.
15. Desligue a máquina que contém o agente exportado criado durante a ativação pós-falha.
16. Realize uma bare metal restore (BMR) do core de origem e do agente. Para obter mais informações, consulte Roteiro de realização de uma bare metal restore em máquinas com Windows.

    > **NOTA:** Ao ativar a restauração, como descrito em Seleção de um ponto de recuperação e início da BMR, você precisará usar os pontos de recuperação importados do core de destino para o agente na máquina virtual.
17. Aguarde a reinicialização da BMR e o reinício do serviço do agente e, em seguida, visualize e registre os detalhes da conexão de rede da máquina.
18. Navegue até o Core Console no core de origem, navegue até a máquina e modifique as definições de proteção da máquina para adicionar os novos detalhes de conexão de rede. Para obter mais informações, consulte Configuração das definições de máquina.
19. Navegue até o Core Console no core de destino e exclua o agente da guia Replicação. Para obter mais informações, consulte Remoção da replicação.
20. No Core Console do core de origem, defina novamente a replicação entre origem e destino clicando na guia Replicação e depois adicione o core de destino para a replicação. Para obter mais informações, consulte a seção Replicar em um core de destino autogerenciado.Remoção da replicação

Gerenciamento de eventos

Gerenciar eventos de core auxilia com o monitoramento do funcionamento e do uso do AppAssure 5 Core. O Core inclui conjuntos predefinidos de eventos, que podem ser usados para notificar os administradores sobre problemas críticos no Core ou nos trabalhos de cópia de segurança.

Na seção Eventos da seção de Configuração da guia Configuração, é possível gerenciar grupos de notificação, definições SMTP de e-mail, redução de repetição e retenção de evento. A opção Grupos de notificação do AppAssure 5 permite gerenciar grupos de notificação, a partir dos quais é possível:

- Especificar um evento para o qual você deseja gerar um alerta para o seguinte:
- Especificar o tipo de alerta.
- Especificar a quem e onde os alertas são enviados. As opções incluem:
- Especificar um limite de tempo para repetição.
- Especificar o período de retenção para todos os eventos.

Configuração de grupos de notificação

Execute as etapas deste procedimento para configurar os grupos de notificação para alertas.

NOTA: Deve-se também configurar as definições do server SMTP se desejar enviar alertas como mensagens de e-mail, conforme descrito neste procedimento. Para obter mais informações sobre como definir as definições do server de e-mail, consulte Configuração de um server de e-mail.

Para configurar grupos de notificação

1 Navegue até o AppAssure 5 Core, clique na guia Configuração e depois em **Eventos**.

2 Clique em **Adicionar grupo**.

A caixa de diálogo Adicionar grupo de notificação é exibida.

A caixa de diálogo Adicionar grupo de notificação contém uma área de descrição geral e duas guias:

- Habilitar alertas
- Opções de notificação

3 Insira as informações básicas para o grupo de notificação, conforme descrito na tabela a seguir.

Tabela 30.

Caixa de texto	Descrição
Nome	Insira um nome para o grupo de notificação de evento. Usado para identificar o grupo de notificação de evento. Estas informações são obrigatórias.
Descrição	Insira uma descrição para o grupo de notificação de evento. Usado para descrever o objetivo do grupo de notificação de evento. Estas informações são opcionais.

4 Na guia Habilitar alertas, defina o conjunto de eventos do sistema que deseja registrar em log, criar relatórios e para o qual deseja ser alertado, como segue:

- Se desejar criar alertas para todos os eventos, selecione **Todos os alertas**.
- Se desejar criar alertas específicos para erros, avisos, mensagens informativas ou uma combinação desses, ao lado de Selecionar tipos, clique na opção apropriada:
  - Erro (ícone de triângulo vermelho)
  - Aviso (ícone de triângulo amarelo)
  - Informações (círculo azul)
  - Restaurar padrão (seta curvada)

- Se desejar criar alertas para eventos específicos, faça o seguinte:
    a Clique no símbolo de maior que (>) ao lado de Todos os alertas para expandir, visualizar e exibir os grupos de eventos relacionados para os quais é possível definir alertas. As categorias de grupo de eventos incluem:
        - Todos os eventos
        - Exchange
        - Atualização automática
        - Cache de deduplicação
        - Verificação de ponto de recuperação
        - Montagem remota
        - CD de inicialização
        - Segurança
        - Retenção do banco de dados
        - Montagem local
        - Metadados
        - Clusters
        - Notificação
        - Scripts do Power Shell
        - Instalação de envio por push
        - Capacidade de anexação
        - Trabalhos
        - Aplicação de licença
        - Truncamento de log
        - Arquivo
        - Serviço do Core
        - Exportar
        - Proteção
        - Replicação
        - Repositório
        - Reversão (Restauração)
        - Rollup
    b Para visualizar eventos individuais em qualquer grupo, clique no símbolo de maior que (>) ao lado do grupo relevante e selecione os eventos específicos para os quais deseja registrar, emitir relatórios e definir alertas.
    c Para definir alertas para todos os eventos dentro de qualquer grupo, marque a caixa de seleção ao lado desse grupo.

5 Clique na guia Opções de notificação.

6 Na guia Opções de notificação, especifique como lidar com o processo de notificação.

A tabela a seguir descreve as opções de notificação.

Tabela 31.

Caixa de texto	Descrição
Notificar por e-mail	Designe os destinatários da notificação de e-mail. É possível optar por especificar vários endereços de e-mail separados, bem como cópias carbono e ocultas. Você pode selecionar: • Para: • CC: • BCC:
Notificar pelo Log de eventos do Windows	Selecione essa opção se deseja que os alertas sejam comunicados por meio do Log de Eventos do Windows.
Notificar por sys logd	Selecione essa opção se deseja que os alertas sejam comunicados por meio de syslogd. Especifique os detalhes do syslogd nas seguintes caixas de texto: • Host: • Porta:
Notificar por alertas do sistema	Selecione esta opção se você deseja que o alerta seja exibido como uma pop-up na parte inferior direita da tela.

7 Clique em **OK**.

Você verá uma mensagem indicando que o nome do grupo de notificação definido não pode ser alterado após a criação do grupo. Outras propriedades dentro do grupo de notificação podem ser alteradas a qualquer momento.

- Se você estiver satisfeito com o nome do grupo, confirme essa mensagem e salve o seu trabalho.
- Se quiser alterar o nome do grupo, clique em **Não** para voltar à janela Criar grupo de notificação, atualize o nome do grupo e outras definições de grupo de notificação e salve seu trabalho.

Configuração de um server de e-mail

Execute as etapas deste procedimento para configurar um server de e-mail.

NOTA: Você também deve configurar as definições de grupo de notificação, incluindo a ativação da opção Notificar por e-mail, antes de as mensagens de alerta por e-mail serem enviadas. Para obter mais informações sobre especificação de eventos para recepção de alertas de e-mail, consulte Configuração de grupos de notificação.

Para configurar um server de e-mail

1 Navegue até o AppAssure 5 Core, clique na guia Configuração e depois em **Eventos**.

2 No painel Definições de e-mail, clique em **Server de SMTP**.

A caixa de diálogo Definições de server de SMTP é exibida.

3 Insira os detalhes do server de e-mail conforme descrito na tabela a seguir.

Tabela 32.

Caixa de texto	Descrição
Server de SMTP	Digite o nome do server de e-mail a ser usado pelo modelo de notificação de e-mail. A convenção de nomenclatura inclui o nome do host, domínio e sufixo; por exemplo, smtp.gmail.com.
De	Insira o endereço de e-mail de devolução. Usado para especificar o endereço de e-mail de devolução para o modelo de notificação de e-mail; por exemplo, noreply@localhost.com.

Tabela 32.

Caixa de texto	Descrição
Nome de usuário	Insira um nome de usuário do server de e-mail.
Senha	Insira a senha associada ao nome de usuário necessário para acessar o server de e-mail.
Port	Insira um número de porta. Utilizado para identificar a porta do server de e-mail; por exemplo, porta 587 para o Gmail. O padrão é *25*.
Tempo limite (segundos)	Insira um valor de número inteiro para especificar quanto tempo deve-se tentar se conectar ao server de e-mail. Utilizado para estabelecer o tempo em segundos antes de ocorrer o tempo limite. O padrão é 60 *segundos*.
TLS	Selecione essa opção se o server de e-mail usar uma conexão segura, como Transport Layer Security (TLS) ou Secure Sockets Layer (SSL).

4 Clique em **Enviar e-mail de teste** e faça o seguinte:

a Na caixa de diálogo Enviar e-mail de teste, insira um endereço de e-mail de destino para a mensagem de teste e clique em **Enviar**.

b Se a mensagem de teste falhar, saia da caixa de diálogo de erro e da caixa de diálogo Enviar e-mail de teste e revise suas definições de configuração do server de e-mail. Depois, repita a Etapa 4.

c Quando a mensagem de teste for bem-sucedida, clique em **OK** para confirmar o êxito da operação.

d Verifique a conta de e-mail para a qual você enviou a mensagem com o e-mail de teste.

e Quando estiver satisfeito com os resultados de seus testes, retorne à caixa de diálogo Definições do server de SMTP e clique em **Salvar** para fechar a caixa de diálogo e salvar as definições.

Configuração de um modelo de notificação de e-mail

Execute as etapas deste procedimento para configurar um modelo de notificação de e-mail. Esse modelo é usado pelo seu server de e-mail SMTP para enviar notificações sobre eventos do AppAssure 5 por e-mail.

NOTA: Você também deve configurar um server de e-mail e as definições de grupo de notificação, incluindo a ativação da opção **Notificar por e-mail**, antes de as mensagens de alerta por e-mail serem enviadas. Para obter mais informações sobre como configurar um server de e-mail para o envio de alertas, consulte Configuração de um server de e-mail. Para obter mais informações sobre especificação de eventos para recepção de alertas de e-mail, consulte Configuração de grupos de notificação.

Para configurar um modelo de notificação de e-mail

1 Navegue até o AppAssure 5 Core, clique na guia Configuração e depois em **Eventos**.

2 No painel Definições de e-mail, clique em **Alterar**.

Aparece a caixa de diálogo Editar configuração de notificação de e-mail.

3 Selecione **Ativar notificações de e-mail**.

4 Na caixa de texto Assunto do e-mail, insira um assunto para o modelo de e-mail.

O Assunto do e-mail é usado para definir o assunto do modelo de notificação por e-mail, por exemplo, <hostname> - <nível> <nome>.

5 Na caixa de texto E-mail, insira as informações do corpo do modelo que descrevem o evento, quando ocorreu e a gravidade.

6 Clique em **Enviar e-mail de teste** e faça o seguinte:

a Na caixa de diálogo Enviar e-mail de teste, insira um endereço de e-mail de destino para a mensagem de teste e clique em **Enviar**.

b Se a mensagem de teste falhar, saia da caixa de diálogo de erro e da caixa de diálogo Enviar e-mail de teste, clique em **OK** para salvar as definições do modelo de e-mail atuais e modificar as definições do server de e-mail, conforme descrito no procedimento Configuração de um server de e-mail, sem deixar de inserir novamente a senha da conta de e-mail. Salve essas definições e volte a esse procedimento.

c Quando a mensagem de teste for bem-sucedida, clique em **OK** para confirmar o êxito da operação.

d Verifique a conta de e-mail para a qual você enviou a mensagem com o e-mail de teste.

e Quando estiver satisfeito com os resultados de seus testes, retorne à caixa de diálogo Editar configuração de notificação de e-mail e clique em **OK** para fechar a caixa de diálogo e salvar as definições.

Configuração da redução de repetição

Execute as etapas deste procedimento para configurar a redução de repetição dos eventos.

Para configurar a redução de repetição

1 Na página inicial do AppAssure 5 Core, clique no menu suspenso Configuração e clique em **Eventos**.

2 Na área Redução de repetição, clique em **Alterar**.

A caixa de diálogo Redução de repetição é exibida.

3 Selecione **Ativar redução de repetição**.

4 Na caixa de texto **Armazenar eventos para**, use as setas para cima e para baixo a fim de inserir o número de minutos a armazenar os eventos para redução de repetição.

5 Clique em **OK**.

Configuração da retenção de eventos

Execute as etapas deste procedimento para configurar a retenção de eventos.

Para configurar a retenção de eventos

1 Na página inicial do AppAssure 5 Core, clique no menu suspenso Configuração e clique em **Definições**.

2 Em Definições de conexão do banco de dados, clique em **Alterar**.

A caixa de diálogo Definições de conexão do banco de dados é exibida.

3 Na caixa de texto **Reter histórico de eventos e trabalhos por**, digite o número de dias pelos quais deseja reter as informações sobre eventos; por exemplo, *30 dias* (padrão).

4 Clique em **Salvar**.

Gerenciamento da recuperação

O AppAssure 5 Core pode restaurar instantaneamente dados ou recuperar máquinas para máquinas físicas ou virtuais a partir dos pontos de recuperação. Os pontos de recuperação contêm snapshots de volume de agentes capturados no nível do bloco. Esses snapshots reconhecem o aplicativo, ou seja, todas as transações abertas e os registros de transações contínuas são concluídos e os caches são descarregados em disco antes da criação do

snapshot. O uso de snapshots que reconhecem aplicativos em conjunto com o Verified Recovery permite que o Core realize vários tipos de recuperações, incluindo:

- Recuperação de arquivos e pastas
- Recuperação de volumes de dados usando Live Recovery
- Recuperação de volumes de dados para Microsoft Exchange Server e Microsoft SQL Server, usando Live Recovery
- Bare metal restore, usando o Universal Recovery
- Bare metal restore para hardware diferente, usando o Universal Recovery
- Exportação ad hoc e contínua para máquinas virtuais

Sobre informações do sistema

O AppAssure 5 permite visualizar informações sobre o AppAssure 5 Core, incluindo informações do sistema, volumes locais e montados, e conexões do mecanismo do AppAssure.

Se você desejar desmontar pontos de recuperação individuais ou todos eles, montados localmente em um core, poderá fazer isso a partir da opção Montar na guia Ferramentas. Para obter mais informações sobre desmontagem de pontos de recuperação, consulte Desmontagem de pontos de recuperação selecionados e Desmontagem de todos os pontos de recuperação.

Visualização de informações do sistema

Execute as etapas deste procedimento para visualizar as informações do sistema.

Para visualizar informações do sistema

1. Navegue até o AppAssure 5 Core e selecione a guia Ferramentas.
2. Na opção Ferramentas, clique em **Informações do sistema**.

Download de instaladores

O AppAssure 5 permite baixar instaladores a partir do AppAssure 5 Core. Na guia Ferramentas, é possível escolher baixar o Agent Installer ou do Local Mount Utility.

NOTA: Para acessar o Agent Installer, consulte Download do Agent Installer. Para obter mais informações sobre a implementação do Agent Installer, consulte o *Guia de implementação do Dell AppAssure 5*. Para acessar o Instalador do Local Mount Utility, consulte Sobre o Local Mount Utility e, para obter mais informações sobre o Local Mount Utility, consulte Download e instalação do Local Mount Utility.

Sobre o Agent Installer

O Agent Installer é usado para instalar o aplicativo AppAssure 5 Agent em máquinas que devem ser protegidas pelo AppAssure 5 Core. Se você determinar que possui uma máquina que exige o Agent Installer, poderá baixar o instalador da Web a partir da guia Ferramentas do AppAssure 5 Core.

NOTA: O download do Core é realizado a partir do Portal de licenças de software da Dell. Para obter mais informações ou baixar o AppAssure 5 Core installer, acesse https://licenseportal.com.

Download do Agent Installer

É possível baixar o AppAssure 5 Agent Installer e implementá-lo em qualquer máquina que será protegida pelo AppAssure 5 Core. Execute as etapas deste procedimento para baixar o instalador da Web.

Para baixar o AppAssure 5 Agent Installer

1 Baixe o arquivo do AppAssure 5 Agent installer no Portal de licenças de software da Dell ou no AppAssure 5 Core. Por exemplo:

```
Agent-X64-5.2.1.xxxxx.exe
```

2 Clique em **Salvar arquivo**.

Para obter mais informações sobre a instalação de agentes, consulte o *Guia de implementação do Dell AppAssure 5*.

Sobre o Local Mount Utility

O Local Mount Utility (LMU) é um aplicativo que pode ser adquirido via download, que permite a montagem de um ponto de recuperação em um AppAssure 5 Core remoto a partir de qualquer máquina. O utilitário leve inclui os drivers *aavdisk* e *aavstor*, mas não executa como um serviço. Quando o utilitário é instalado, por padrão, ele é instalado no diretório C:\Program Files\AppRecovery\Local Mount Utility, e um atalho aparece na área de trabalho da máquina.

Embora o utilitário tenha sido projetado para o acesso remoto aos cores, também é possível instalar o LMU em um AppAssure 5 Core. Quando executado em um core, o aplicativo reconhece e exibe todas as montagens desse core, incluindo montagens realizadas por meio do AppAssure 5 Core Console. Da mesma forma, as montagens realizadas no LMU também aparecem no console.

Download e instalação do Local Mount Utility

O AppAssure 5 permite baixar o Local Mount Utility diretamente do AppAssure 5 Core Console. Realize as etapas a seguir para fazer o download do utilitário e instalá-lo.

Para fazer o download do Local Mount Utility e instalá-lo

1 Na máquina em que você deseja instalar o LMU, acesse o AppAssure 5 Core Console inserindo a URL do console no seu navegador e fazendo login com o seu nome de usuário e senha.

2 No AppAssure 5 Core Console, clique na guia Ferramentas.

3 Na guia Ferramentas, clique em **Downloads**.

4 Em Local Mount Utility, clique no link **Baixar instalador da web**.

5 Na janela Abrindo LocalMountUtility-Web.exe, clique em **Salvar arquivo.**

O arquivo é salvo na pasta local Downloads. Em alguns navegadores, a pasta é aberta automaticamente.

6 Na pasta Downloads, clique com o botão direito no arquivo executável LocalMountUtility-Web e clique em **Abrir**.

Dependendo da configuração da máquina, a janela Controle da conta do usuário pode aparecer.

7 Se a janela Controle da conta do usuário aparecer, clique em **Sim** para permitir que o programa faça alterações na máquina.

O Assistente de instalação do AppAssure Local Mount Utility é aberto.

8 Na tela Bem-Vindo do Assistente de instalação do AppAssure Local Mount Utility, clique em **Avançar** para ir à página Acordo de licença.

9 Na página Acordo de licença, selecione **Eu aceito os termos do acordo de licença** e, em seguida, clique em **Avançar** para ir à página Pré-requisitos.

10 Na página Pré-requisitos, instale os pré-requisitos necessários e clique em **Avançar** para continuar na página Opções de instalação.

11 Na página Opções de instalação, realize as tarefas a seguir:

a Escolha uma pasta de destino para o LMU clicando no botão **Alterar**.

NOTA: A pasta de destino padrão é C:\Program Files\AppRecovery\LocalMountUtility.

b Selecione se você deseja (ou não) **permitir que o Local Mount Utility envie automaticamente informações de diagnóstico e uso para a AppAssure Software, Inc.**

c Selecione **os componentes opcionais: Mailbox Restore**.

d Clique em **Avançar** para ir à página Progresso e baixar o aplicativo.

O aplicativo é transferido por download para a pasta de destino. O progresso é exibido na barra de progresso. Ao terminar, o assistente avança automaticamente para a página Concluído.

12 Clique em **Concluir** para fechar o assistente.

Adição de um Core ao Local Mount Utility

Para montar um ponto de recuperação, é necessário adicionar o Core ao LMU. Não há limite em relação à quantidade de cores que podem ser adicionados.

Execute o procedimento a seguir para configurar o LMU adicionando um core.

Para adicionar um core ao Local Mount Utility

1 Na máquina em que o LMU está instalado, inicie o LMU clicando duas vezes no ícone na área de trabalho.

2 Se a janela Controle da conta do usuário aparecer, clique em **Sim** para permitir que o programa faça alterações na máquina.

3 No canto superior esquerdo da janela AppAssure Local Mount Utility, clique em **Adicionar core**.

4 Na caixa de diálogo Adicionar Core, insira as credenciais solicitadas, descritas na tabela a seguir.

Tabela 33.

Opção	Descrição
Nome do host	O nome do Core a partir do qual você deseja montar pontos de recuperação. **NOTA:** Se você estiver instalando o LMU em um core, o LMU adicionará a máquina localhost automaticamente.
Port	O número da porta usada para se comunicar com o Core. O número de porta padrão é 8006.
Use minhas credenciais de usuário do Windows	Selecione esta opção se as credenciais que você usa para acessar o Core forem iguais às credenciais do Windows.
Use credenciais específicas	Selecione essa opção se as credenciais que você usa para acessar o Core forem diferentes das credenciais do Windows.
Nome de usuário	O nome de usuário utilizado para acessar a máquina do Core. **NOTA:** Essa opção fica disponível apenas se você opta por usar credenciais específicas.
Senha	A senha usada para acessar a máquina do Core. **NOTA:** Essa opção fica disponível apenas se você opta por usar credenciais específicas.

5 Clique em **Conectar**.

6 Se você estiver adicionando vários cores, repita da Etapa 3 à Etapa 5 conforme necessário.

Montagem de um ponto de recuperação usando o Local Mount Utility

Antes de montar um ponto de recuperação, o Local Mount Utility (LMU) precisa se conectar ao Core no qual o ponto de recuperação está armazenado. Como descrito no procedimento Adição de um Core ao Local Mount Utility, o número de cores que podem ser adicionados ao LMU é ilimitado; no entanto, o aplicativo pode ser conectado somente a um core por vez. Por exemplo, se você montar um ponto de recuperação de um agente protegido por um core e depois montar um ponto de recuperação de um agente protegido por outro core, o LMU automaticamente se desconectará do primeiro core para estabelecer uma conexão com o segundo core.

Realize o procedimento a seguir para montar um ponto de recuperação em um core remoto usando o LMU.

Para montar um ponto de recuperação usando o Local Mount Utility

1 Na máquina em que o LMU está instalado, inicie o LMU clicando duas vezes no ícone na área de trabalho.

2 Na janela principal do AppAssure Local Mount Utility, expanda o Core na árvore de navegação para revelar os agentes protegidos.

3 Na árvore de navegação, selecione o agente a partir do qual deseja montar um ponto de recuperação.

Os pontos de recuperação são exibidos na estrutura principal.

4 Expanda o ponto de recuperação que você deseja montar para revelar volumes de disco individuais ou bancos de dados.

5 Clique com o botão direito no ponto de recuperação que você deseja montar e selecione uma das opções a seguir:

- Montagem
- Montagem gravável
- Montagem com gravações anteriores
- Montagem avançada

a Se você tiver selecionado Montagem avançada, na janela Montagem avançada, execute as opções descritas na tabela a seguir.

Tabela 34.

Opção	Descrição
Caminho de ponto de montagem	Clique no botão **Procurar** para selecionar um caminho para os pontos de recuperação diferente do caminho padrão dos pontos de montagem.
Tipo de montagem	Selecione uma das opções a seguir: • Montagem de apenas leitura • Montagem gravável • Montagem de apenas leitura com gravações anteriores

b Clique em **Montagem**.

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

NOTA: Se for selecionado um ponto de recuperação que já está montado, a caixa de diálogo Montando perguntará se deve desmontar o ponto de recuperação.

Exploração de um ponto de recuperação montado usando o Local Mount Utility

Execute o procedimento a seguir para explorar um ponto de recuperação que permaneceu montado desde uma sessão anterior.

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

Para explorar um ponto de recuperação montado usando o Local Mount Utility

1. Na máquina em que o LMU está instalado, inicie o LMU clicando duas vezes no ícone na área de trabalho.
2. Na tela principal do Local Mount Recovery, clique em **Montagens ativas.**

   A janela Montagens ativas é aberta e exibe todos os pontos de recuperação montados.
3. Clique em **Explorar** ao lado do ponto de recuperação a partir do qual deseja fazer a recuperação a fim de abrir a pasta de volumes deduplicados.

Desmontagem de um ponto de recuperação usando o Local Mount Utility

Execute o procedimento a seguir para desmontar um ponto de recuperação em um core remoto usando o LMU.

Para desmontar um ponto de recuperação usando o Local Mount Utility

1. Na máquina em que o LMU está instalado, clique duas vezes no ícone do Local Mount Utility no desktop para iniciar o programa.
2. Na tela principal do Local Mount Recovery, clique em **Montagens ativas.**

   A janela Montagens ativas é aberta e exibe todos os pontos de recuperação montados.
3. Realize um dos procedimentos a seguir:
   - Para desmontar um ponto de recuperação, selecione um ponto que deseja desmontar e, em seguida, clique em **Desmontar**.
   - Para desmontar todos os pontos de recuperação montados, clique em **Desmontar tudo** e, em seguida, clique em **Sim** na caixa de diálogo Desmontar tudo para confirmar.
4. Para fechar a janela Montagens ativas, clique no X no canto superior direito.
5. Para minimizar o aplicativo LMU, clique no X no canto superior direito da janela do Local Mount Utility.
6. Para fechar o aplicativo LMU, clique com o botão direito do mouse no AppAssure ícone do Local Mount Utility no menu da bandeja do LMU e selecione **Sair**.

Sobre o menu da bandeja do Local Mount Utility

O menu da bandeja do LMU está localizado na barra de tarefas da área de trabalho. Clique com o botão direito do mouse no ícone para revelar as opções descritas na tabela a seguir:

Tabela 35.

Opção	Descrição
Buscar pontos de recuperação	Abre a janela principal do LMU.
Montagens ativas	Abre a caixa de diálogo Montagens ativas no alto da janela principal do LMU.

Tabela 35.

Opção	Descrição
Opções	Abre a caixa de diálogo Opções no alto da janela principal do LMU. Na caixa de diálogo Opções, você pode alterar o diretório do ponto de montagem Padrão e as credenciais do Core padrão para a interface de usuário do LMU.
Sobre	Revela as informações de aplicação de licença do Local Mount Utility.
Sair	Fecha o aplicativo LMU. NOTA: Ao clicar no X no canto superior da janela principal do LMU, o aplicativo é minimizado para a bandeja, em vez de ser fechado.

Uso das opções do AppAssure 5 Core e do Agent

Ao clicar com o botão direito do mouse no AppAssure 5 Core ou Agent na tela principal do LMU, certas opções podem ser realizadas. Eles incluem:

- Opções de localhost
- Opções de Core remoto
- Opções de agente

Acesso às opções de localhost

Execute a etapa deste procedimento para acessar as opções de localhost.

Para acessar as opções de localhost

- Clique com o botão direito do mouse no AppAssure 5 Core ou Agent e depois clique em **Reconectar ao core**.

  As informações do Core são atualizadas; por exemplo, agentes adicionados recentemente.

Acesso às opções de Core remoto

Execute as etapas deste procedimento para acessar as opções de core remoto.

Para acessar as opções de core remoto

- Clique com o botão direito do mouse no AppAssure 5 Core ou Agent e selecione uma das opções de core remoto, como descrito na tabela a seguir.

  Tabela 36.

Opção	Descrição
Reconectar ao core	Atualiza as informações do Core, como agentes adicionados recentemente.
Remover core	Exclui o Core do Local Mount Utility.
Editar core	Abre a janela Editar Core, onde é possível alterar o nome de host, a porta e as credenciais.

Acessar as opções de Agent

Execute as etapas neste procedimento para acessar as opções de Agent.

Para acessar as opções de Agent

- Clique com o botão direito do mouse no AppAssure 5 Core ou Agent e depois clique em **Atualizar pontos de recuperação**.

  A lista de pontos de recuperação do agente selecionado é atualizada.

Gerenciamento das políticas de retenção

Snapshots de cópia de segurança periódicos de todos os servers protegidos se acumulam no Core ao longo do tempo. As políticas de retenção são usadas para reter snapshots de cópia de segurança por períodos mais longos e para ajudar com o gerenciamento desses snapshots de cópia de segurança. A política de retenção é imposta pelo processo noturno de rollup que ajuda no processo de envelhecimento e exclusão das cópias de segurança antigas. Para obter informações sobre a configuração de políticas de retenção, consulte Personalização das definições de política de retenção para um agente.

Roteiro para arquivar em uma nuvem

Quando os dados atingirem o final de um período de retenção, você pode desejar ampliar essa retenção criando um arquivo dos dados antigos. Quando você arquiva dados, há sempre uma dúvida de onde armazená-los. O AppAssure 5 permite que você carregue seus arquivos a uma variedade de provedores de nuvem diretamente do Core Console. As nuvens compatíveis incluem o Windows Azure, Amazon, Rackspace, e qualquer fornecedor baseado no OpenStack.

Exportar um arquivo a uma nuvem utilizando o AppAssure 5 envolve os seguintes procedimentos:

- **Adicione sua conta em nuvem ao AppAssure 5 Core Console.** Para obter informações, consulte Adicionar uma conta em nuvem.
- **Arquive seus dados e exporte-os para sua conta em nuvem.** Para obter informações, consulte Criação de um arquivo.
- **Retomar dados arquivados importando-os do local da nuvem.** Para obter informações, consulte Importação de um arquivo.

Noções básicas sobre arquivos

As políticas de retenção impõem períodos em que as cópias de segurança são armazenadas em mídias de curto prazo (rápidas e caras). Às vezes, certos requisitos técnicos e de negócios exigem a retenção prolongada desses backups, mas o armazenamento rápido tem um custo proibitivo. Portanto, esse requisito gera uma necessidade de armazenamento de longo prazo (lento e barato). As empresas frequentemente usam o armazenamento de longo prazo para arquivar dados de conformidade e não conformidade. O recurso de arquivo do AppAssure 5 é usado para oferecer suporte à retenção estendida de dados compatíveis e não compatíveis. Também é usado para executar propagação de dados de replicação para um core de réplica remota.

Criação de um arquivo

Execute as etapas deste procedimento para criar um arquivo.

Para criar um arquivo

1 Navegue até o AppAssure 5 Core Console e clique na guia Ferramentas.

2 Na opção Arquivo, clique em **Criar**.

O assistente Adicionar arquivo é aberto.

3 Na página Criar do assistente Adicionar Arquivo, selecione uma das seguintes opções a partir da lista suspensa Tipo de Localização:

- Local
- Rede
- Nuvem

4 Insira os detalhes do arquivo, como descrito na tabela a seguir, com base no tipo de localização que você selecionou no Etapa 3.

Tabela 37.

Opção	Caixa de texto	Descrição
Local	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, d:\work\archive.
Rede	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, \\servername\sharename.
	Nome de usuário	Insira um nome de usuário. Ele é usado para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira uma senha para o caminho de rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter informações, consulte Adicionar uma conta em nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é AppAssure-5-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

5 Clique em **Avançar**.

6 Na página Máquinas do assistente, selecione quais máquinas protegidas ou máquinas contêm os pontos de recuperação que deseja arquivar.

7 Clique em **Avançar**.

8 Na página Opções, insira as informações conforme descrito na tabela a seguir.

Caixa de texto	Descrição
Tamanho máximo	Grandes arquivos de dados podem ser divididos em vários segmentos. Selecione a quantidade máxima de espaço que você deseja reservar para criar o arquivo efetuando uma das seguintes ações: • Selecione **Destino Inteiro** para reservar todo o espaço disponível no caminho fornecido em Etapa 4. (por exemplo, se o local for D:\work\archive, todo o espaço disponível na unidade D: será reservado). • Selecione a caixa de texto em branco, use as setas para cima e para baixo para inserir uma quantidade e depois selecione uma unidade de medida na lista suspensa para personalizar o espaço máximo que você deseja reservar. **NOTA:** Os arquivos da nuvem do Amazon são automaticamente divididos em segmentos de 50 GB. Os arquivos da nuvem do Windows Azure são automaticamente divididos em segmentos de 200 GB.
Reciclar ação	Selecione uma das seguintes opções de ação de reciclagem: • **Não reutilizar.** Não substitui ou apaga nenhum dado arquivado existente no local. Se o local não estiver vazio, a gravação do arquivo falhará. • **Substituir este Core.** Substitui quaisquer dados arquivados preexistentes pertencentes a este core, porém deixa os dados de outros cores intactos. • **Apagar completamente.** Apaga todos os dados arquivados do diretório antes de gravar o novo arquivo. • **Incremental.** Permite que você adicione pontos de recuperação a um arquivo existente. Compara pontos de recuperação para evitar duplicação de dados que já existem no arquivo.
Comentários	Insira qualquer informação adicional necessária para o arquivo. O comentário será exibido se você importar o arquivo mais tarde.
Usar formato compatível	Selecione essa opção para arquivar seus dados em um formato compatível com versões antigas dos cores. **NOTA:** O novo formato oferece melhor desempenho, contudo, não é compatível com os cores mais antigos.

9 Clique em **Avançar**.

10 Na página Intervalo de data, insira a Data de início e a Data de expiração dos pontos de recuperação a serem arquivados.

- Para inserir uma hora, clique na hora exibida (padrão, 8h) para revelar as barras deslizantes para selecionar horas e minutos.
- Para inserir uma data, clique na caixa de texto para revelar o calendário, e depois clique no dia de sua preferência.

11 Clique em **Concluir**.

Configuração do arquivo agendado

O recurso Arquivo agendado permite que você defina uma hora para que um arquivo de uma máquina selecionada seja automaticamente criado e salvo em um local especificado. Isso abriga situações em que você deseje arquivos frequentes de uma máquina a serem salvos, sem a inconveniência de precisar criar os arquivos manualmente. Execute as etapas do procedimento a seguir para programar o arquivamento automático agendado.

Definir um arquivo agendado

1 Navegue até o AppAssure 5 Core Console e clique na guia Ferramentas.

2 Na opção Arquivo, clique em **Agendado**.

3 Na página Arquivo Agendado, clique em **Adicionar**.

O assistente Adicionar arquivo é aberto.

4 Na página Local do assistente Adicionar arquivo, selecione uma das seguintes opções a partir da lista suspensa Tipo de localização:

- Local
- Rede
- Nuvem

5 Insira os detalhes do arquivo, como descrito na tabela a seguir, com base no tipo de localização que você selecionou no Etapa 4.

Tabela 38.

Opção	Caixa de texto	Descrição
Local	Local de saída	Insira a localização para a saída. Define o caminho do local onde você deseja que o arquivo resida, por exemplo, d:\work\archive.
Rede	Local de saída	Insira a localização para a saída. Define o caminho do local onde você deseja que o arquivo resida, por exemplo, \\servername\sharename.
	Nome de usuário	Insira um nome de usuário. Estabelece credenciais de logon para o compartilhamento de rede.
	Senha	Insira uma senha para o caminho de rede. Estabelece credenciais de logon para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter informações, consulte Adicionar uma conta em nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é AppAssure-5-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

6 Clique em **Avançar**.

7 Na página Máquinas do assistente, selecione quais máquinas protegidas contêm os pontos de recuperação que deseja arquivar.

8 Clique em **Avançar**.

9 Na página Opções, selecione uma das seguintes Ações de reciclagem na lista suspensa:

- **Substituir este Core.** Substitui quaisquer dados arquivados existentes pertencentes a este core, porém deixa os dados de outros cores intactos.
- **Apagar completamente.** Apaga todos os dados arquivados do diretório antes de gravar o novo arquivo.
- **Incremental.** Permite que você adicione pontos de recuperação a um arquivo existente. Compara pontos de recuperação para evitar duplicação de dados que já existem no arquivo.

10 Na página Programar, selecione uma das seguintes opções de Enviar frequência de dados:

- Diariamente
- Semanalmente
- Mensalmente

11 Insira as informações descritas na tabela a seguir dependendo de sua seleção do Etapa 10.

Opção	Caixa de texto	Descrição
Diariamente	Na hora	Selecione a hora do dia que você deseja criar o arquivo diário.
Semanalmente	No dia de semana	Selecione um dia da semana no qual deseja criar automaticamente o arquivo.
	Na hora	Selecione a hora do dia que você deseja criar o arquivo diário.
Mensalmente	No dia do mês	Selecione o dia do mês no qual deseja criar automaticamente o arquivo.
	Na hora	Selecione a hora do dia que você deseja criar o arquivo diário.

12 Para pausar o arquivamento para retomar posteriormente, selecione **Pausa inicial do arquivamento**.

> **NOTA:** Talvez você deseje pausar o arquivo agendado se precisar de tempo para preparar o local de destino antes de arquivar os resumos. Se você não selecionar essa opção, o arquivamento começa no horário agendado.

13 Clique em **Concluir**.

Pausar ou resumir arquivo agendado

Pode haver vezes que deseje pausar um trabalho de arquivo agendado, como quando precisar alterar o local do arquivo de destino. Além disso, se escolheu pausar inicialmente o arquivamento quando realizou o procedimento Configuração do arquivo agendado, você provavelmente desejará retomar o arquivo agendado no futuro. Execute as etapas do procedimento a seguir para pausar ou retomar o arquivo agendado.

Pausar ou retomar o arquivamento automático

1 Navegue até o AppAssure 5 Core Console e clique na guia Ferramentas.

2 Na opção Arquivo, clique em **Agendado**.

3 Na página Arquivo agendado, realize um dos procedimentos a seguir:

- Selecione o arquivo de preferência, e depois clique em uma das seguintes ações disponíveis:
  - Pause
  - Resume
- Ao lado do arquivo de preferência, clique no menu suspenso e em uma das seguintes ações disponíveis, conforme adequado:
  - Pause
  - Resume

O status do arquivo é exibido na coluna Programar.

Editar um arquivo agendado

AppAssure 5 permite que você altere os detalhes de um arquivo agendado. Para editar um arquivo agendado, execute as etapas do procedimento a seguir.

Editar um arquivo de programação

1 Navegue até o AppAssure 5 Core Console e clique na guia Ferramentas.

2 Na opção Arquivo, clique em **Agendado**.

3 Na página Arquivo agendado, clique no menu suspenso ao lado do arquivo que você deseja alterar, e depois clique em **Editar**.

O assistente Adicionar arquivo é aberto.

4 Na página Local do assistente Adicionar arquivo, selecione uma das seguintes opções a partir da lista suspensa Tipo de localização:

- Local
- Rede
- Nuvem

5 Insira os detalhes do arquivo, como descrito na tabela a seguir, com base no tipo de localização que você selecionou no Etapa 4.

Tabela 39.

Opção	Caixa de texto	Descrição
Local	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, d:\work\archive.
Rede	Local de saída	Insira a localização para a saída. Usado para definir o caminho de localização onde você deseja que o arquivo resida, por exemplo, \\servername\sharename.
	Nome de usuário	Insira um nome de usuário. Ele é usado para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira uma senha para o caminho de rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter informações, consulte Adicionar uma conta em nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é AppAssure-5-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

6 Clique em **Avançar**.

7 Na página Máquinas do assistente, selecione quais máquinas protegidas contêm os pontos de recuperação que deseja arquivar.

8 Clique em **Avançar**.

9 Na página Programar, selecione uma das seguintes opções de Enviar frequência de dados:

- Diariamente
- Semanalmente
- Mensalmente

10 Insira as informações descritas na tabela a seguir dependendo de sua seleção do Etapa 9.

Opção	Caixa de texto	Descrição
Diariamente	Na hora	Selecione a hora do dia que você deseja criar o arquivo diário.
Semanalmente	No dia de semana	Selecione um dia da semana no qual deseja criar automaticamente o arquivo.
	Na hora	Selecione a hora do dia que você deseja criar o arquivo diário.
Mensalmente	No dia do mês	Selecione o dia do mês no qual deseja criar automaticamente o arquivo.
	Na hora	Selecione a hora do dia que você deseja criar o arquivo diário.

11 Para pausar o arquivamento para retomar posteriormente, selecione **Pausa inicial do arquivamento**.

> **NOTA:** Talvez você deseje pausar o arquivo agendado se precisar de tempo para preparar o local de destino antes de arquivar os resumos. Se você não selecionar essa opção, o arquivamento começa no horário agendado.

12 Clique em **Concluir**.

Verificando um arquivo

É possível fazer uma varredura de um arquivo para integridade estrutural realizando uma verificação do arquivo. Isso verifica a presença de todos os arquivos necessários dentro do arquivo. Para realizar uma verificação do arquivo, execute as etapas do procedimento a seguir.

Para verificar um arquivo

1 Navegue até o AppAssure 5 Core Console e clique na guia Ferramentas.

2 Na opção Arquivo, clique em **Verificar arquivo**.

3 A caixa de diálogo Verificar arquivo é exibida.

4 Para **Tipo de localização**, selecione uma das seguintes opções a partir da lista suspensa:

- Local
- Rede
- Nuvem

5 Insira os detalhes do arquivo, como descrito na tabela a seguir, com base no tipo de localização que você selecionou no Etapa 4.

Tabela 40.

Opção	Caixa de texto	Descrição
Local	Local	Insira o caminho para o arquivo.
Rede	Local	Insira o caminho para o arquivo.
	Nome de usuário	Insira o nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira a senha para o caminho da rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter informações, consulte Adicionar uma conta em nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira o nome da pasta na qual os dados arquivados são salvos, por exemplo, AppAssure-5-Arquivo-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

6 Para realizar também uma verificação da integridade da estrutura, selecione **Integridade da estrutura**.

7 Clique em **Verificar arquivo**.

Importação de um arquivo

Quando desejar recuperar dados arquivados, é preciso importar o arquivo inteiro a um local especificado. Depois, você poderá procurar os dados. Para importar um arquivo, execute as etapas do procedimento a seguir.

Para importar um arquivo

1 Navegue até o AppAssure 5 Core Console e selecione a guia Ferramentas.

2 Na opção Arquivo, clique em **Importar**.

3 Para **Tipo de localização**, selecione uma das seguintes opções a partir da lista suspensa:

- Local
- Rede
- Nuvem

4 Insira os detalhes do arquivo, como descrito na tabela a seguir, com base no tipo de localização que você selecionou no Etapa 3.

Tabela 41.

Opção	Caixa de texto	Descrição
Local	Local	Insira o caminho para o arquivo.
Rede	Local	Insira o caminho para o arquivo.
	Nome de usuário	Insira o nome de usuário. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
	Senha	Insira a senha para o caminho da rede. Ela é usada para estabelecer credenciais de login para o compartilhamento de rede.
Nuvem	Conta	Selecione uma conta da lista suspensa. **NOTA:** Para selecionar uma conta da nuvem, você deve primeiro tê-la adicionado no Core Console. Para obter informações, consulte Adicionar uma conta em nuvem.
	Contêiner	Selecione um contêiner associado à sua conta no menu suspenso.
	Nome da pasta	Insira o nome da pasta na qual os dados arquivados são salvos, por exemplo, AppAssure-5-Arquivo-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

5 Clique em **Verificar arquivo** para validar a existência do arquivo a ser importado.

6 Na caixa de diálogo, verifique o nome do core de origem exibido na lista suspensa do Core.

7 Selecione os agentes a serem importados do arquivo.

8 Selecione o repositório no qual os dados arquivados serão salvos.

NOTA: O repositório selecionado deve ser o mesmo repositório em que todos os atuais pontos de recuperação para o agente selecionado são armazenados.

9 Clique em **Restaurar** para importar o arquivo.

Gerenciamento da capacidade de anexação do SQL e truncamento de log

A configuração da capacidade de anexação do SQL permite que o AppAssure 5 Core anexe arquivos de banco de dados e log do SQL Server em um snapshot de um server SQL usando uma instância local do Microsoft SQL Server. O teste da capacidade de anexação permite que o Core verifique a consistência dos bancos de dados SQL e garanta que todos os arquivos de dados (arquivos MDF e LDF) estejam disponíveis no snapshot de cópia de segurança. As verificações da capacidade de anexação podem ser executadas sob demanda para pontos de recuperação específicos ou como parte de um trabalho noturno.

A capacidade de anexação exige uma instância local do Microsoft SQL Server na máquina do AppAssure 5 Core. Essa instância precisa ser uma versão totalmente licenciada do SQL Server adquirida da Microsoft ou através de um revendedor licenciado. A Microsoft não permite o uso de licenças SQL passivas.

A capacidade de anexação suporta SQL Server 2005, 2008, 2008 R2, 2012 e 2014. À conta usada para realizar o teste deve ser concedida a função sysadmin na instância do SQL Server.

O formato de armazenamento em disco do SQL Server é o mesmo em ambientes de 64 e 32 bits, e a capacidade de anexação funciona em ambas as versões. Um banco de dados separado da instância do server que está sendo executado em um ambiente pode ser anexado em uma instância de server que é executado em outro ambiente.

O truncamento de log identifica o espaço livre disponível nos registros do banco de dados do SQL, mas não os minimiza. É possível programar o truncamento de log para acontecer com trabalhos noturnos ou você pode forçá-lo sob demanda. Para forçar truncamento de log, consulte Forçamento do truncamento de log para uma máquina com SQL ou com Exchange.

NOTA: A versão do SQL Server no Core deve ser igual ou mais recente que aquela em todas as máquinas agente com o SQL Server instalado.

Esta seção inclui os seguintes tópicos:

- Configuração das definições da capacidade de anexação do SQL
- Configuração das verificações noturnas de capacidade de anexação do SQL e truncamento de log para todas as máquinas protegidas

Para obter mais informações sobre o gerenciamento de máquinas protegidas que utilizam o SQL Server, consulte Modificação das definições do SQL Server ou Personalização de trabalhos noturnos para uma máquina protegida.

Configuração das definições da capacidade de anexação do SQL

Antes de executar verificações da capacidade de anexação de bancos de dados SQL protegidos, primeiro é preciso selecionar uma instância local do SQL Server na máquina do Core que será usada para executar as verificações em relação à máquina agente.

NOTA: A capacidade de anexação exige uma instância local do Microsoft SQL Server na máquina do AppAssure 5 Core. Essa instância precisa ser uma versão totalmente licenciada do SQL Server adquirida da Microsoft ou através de um revendedor licenciado. A Microsoft não permite o uso de licenças SQL passivas.

Execute as etapas deste procedimento para configurar as definições de capacidade de anexação do SQL.

Para configurar as definições da capacidade de anexação do SQL

1. Navegue até o AppAssure 5 Core e clique na guia Configuração.
2. Clique em **Definições**.
3. No painel Trabalhos noturnos, clique em **alterar**.

   A caixa de diálogo Trabalhos noturnos é exibida.

4 Selecione **Trabalho de verificação de capacidade de anexação** e clique em **Definições**.

A caixa de diálogo Configuração é exibida, permitindo que você escolha a instância local do SQL Server a fim de utilizar para a realização das verificações da capacidade de anexação dos SQL Server databases protegidos.

5 Use os menus suspensos para selecionar a instância do SQL Server instalado no Core a partir das seguintes opções:

- SQL Server 2005
- SQL Server 2008
- SQL Server 2008 R2
- SQL Server 2012
- SQL Server 2014

NOTA: As opções que aparecem na lista suspensa são preenchidas com base nas instâncias locais do SQL Server em seu ambiente.

6 Selecione o tipo de credencial. Você pode selecionar dentre:

- Windows ou
- SQL

7 Especifique as credenciais com privilégios administrativos para instâncias do Windows ou do SQL Server, conforme descrito na tabela a seguir.

Tabela 42.

Caixa de texto	Descrição
Nome de usuário	Insira um nome de usuário para obter permissões de login no SQL Server.
Senha	Insira uma senha para a capacidade de anexação do SQL. Usada para controlar a atividade de login.

8 Clique em **Testar conexão**.

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

9 Clique em **Salvar**.

As verificações da capacidade de anexação agora estão disponíveis para serem executadas em bancos de dados protegidos do SQL Server.

10 Na janela Trabalhos noturnos, clique em **OK**.

As verificações da capacidade de anexação agora são programadas para acontecer com os trabalhos noturnos.

Configuração das verificações noturnas de capacidade de anexação do SQL e truncamento de log para todas as máquinas protegidas

É possível visualizar, ativar ou desativar as definições do server do banco de dados do SQL, incluindo verificação da capacidade de anexação e truncamento de log noturno na caixa de diálogo Trabalhos noturnos acessada a partir do Core. As alterações feitas aqui se aplicam a todas as máquinas SQL protegidas pelo Core.

Execute as etapas deste procedimento para que o sistema realize verificações noturnas de capacidade de anexação dos pontos de recuperação do SQL Server.

Para configurar verificações noturnas de capacidade de anexação do SQL e truncamento de log

1. Navegue até o AppAssure 5 Core e clique na guia Configuração.
2. Clique em **Definições**.
3. Na seção Trabalhos noturnos, clique em **Alterar**.
4. Selecione ou desmarque as definições do SQL Server com base nas necessidades da sua organização:
   - Trabalho de verificação de capacidade de anexação
   - Trabalho de truncamento de log (apenas modelo de recuperação simples)
5. Clique em **OK**.

   As definições de capacidade de anexação e de truncamento de log entrarão em vigor no SQL Server protegido.

Gerenciamento de verificações da capacidade de montagem do banco de dados do Exchange e truncamento de log

Ao usar o AppAssure 5 para fazer cópias de segurança de Microsoft Exchange Servers, poderão ser feitas verificações de montabilidade em todos os bancos de dados Exchange após cada snapshot. Esse recurso de detecção de corrupção alerta os administradores sobre possíveis falhas e garante que todos os dados nos Exchange servers sejam recuperados com êxito em caso de falha.

O truncamento de log minimiza o tamanho dos registros a partir de um banco de dados do Exchange diariamente quando agendado para acontecer com trabalhos noturnos. Para obter informações sobre o forçamento do truncamento de log, consulte Forçamento do truncamento de log para uma máquina com SQL ou com Exchange.

NOTA: As verificações de montabilidade somente se aplicam ao Microsoft Exchange 2007, 2010 e 2013. Além disso, a conta de serviço do AppAssure 5 Agent deve ter a função de Administrador organizacional atribuída a ela no Exchange.

Para obter mais informações sobre o gerenciamento de máquinas protegidas que utilizam o Exchange Server, consulte Gerenciamento de máquinas com Exchange e SQL Server.

Configuração de verificações de soma de verificação do banco de dados do Exchange noturno e truncamento de log

É possível visualizar, ativar ou desativar as definições do server do banco de dados do Exchange, incluindo verificação automática de capacidade de montagem, verificação de soma de verificação noturna ou truncamento de log noturno, na guia de Configuração do nível do Core. As alterações feitas nas configurações nessa guia se aplicam a todas as máquinas Exchange protegidas pelo Core.

Execute as etapas deste procedimento para configurar as definições de montabilidade e truncamento de log do banco de dados do Exchange.

Para configurar a montabilidade de banco de dados do Exchange e o truncamento de log

1. Navegue até o AppAssure 5 Core e clique na guia Configuração.
2. Clique em **Definições**.
3. Na seção Trabalhos noturnos, clique em **Alterar**.

4 Selecione ou desmarque as definições do Exchange Server com base nas necessidades da sua organização:

- Trabalho de verificação de soma de verificação
- Registros truncados do Exchange

5 Clique em **OK**.

As definições de soma de verificação e de truncamento de log entrarão em vigor no Exchange Server protegido.

NOTA: Para obter informações sobre o forçamento do truncamento de log, consulte Forçamento do truncamento de log para uma máquina com SQL ou com Exchange.

Indicadores de status de ponto de recuperação

Depois que um ponto de recuperação é criado em um SQL ou Exchange server protegido, o aplicativo exibe um indicador de status colorido correspondente na tabela Pontos de recuperação. A cor exibida se baseia nas definições de verificação da máquina protegida e no êxito ou fracasso dessas verificações, conforme descrito nas tabelas Cores de status de ponto de recuperação para bancos de dados SQL e Cores de status de ponto de recuperação para bancos de dados do Exchange, a seguir.

NOTA: Para obter mais informações sobre como visualizar pontos de recuperação, consulte Visualização de pontos de recuperação.

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

A tabela a seguir relaciona os indicadores de status exibidos para bancos de dados SQL.

Tabela 43.

Cor de status	Descrição
Branco	Indica a existência de uma das seguintes condições: • Não existe banco de dados do SQL, • As verificações da capacidade de anexação não foram ativadas; ou • As verificações da capacidade de anexação ainda não foram executadas.
Amarelo	Indica que o banco de dados do SQL estava offline e não foi possível executar a verificação.
Vermelho	Indica falha na verificação de capacidade de anexação.
Verde	Indica que a verificação de capacidade de anexação foi aprovada.

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

A tabela a seguir relaciona os indicadores de status exibidos para bancos de dados Exchange.

Tabela 44.

Cor de status	Descrição
Branco	Indica a existência de uma das seguintes condições: • Não existe banco de dados do Exchange; ou • As verificações da montabilidade não foram ativadas. **NOTA:** Isso pode se aplicar a determinados volumes dentro de um ponto de recuperação.
Amarelo	Indica que as verificações da montabilidade do banco de dados do Exchange estão ativadas, mas ainda não foram executadas.
Vermelho	Indica que as verificações de montabilidade ou de soma de verificação falharam em pelo menos um banco de dados.
Verde	Indica que a verificação de montabilidade ou a verificação de soma de verificação foi aprovada.

NOTA: Os pontos de recuperação que não têm banco de dados do Exchange ou do SQL associado a eles aparecerão com indicador de status branco. Em situações em que existe banco de dados do Exchange e do SQL para o ponto de recuperação, o indicador de status mais grave é exibido no ponto de recuperação.

3

Proteção de estações de trabalho e servers

Este capítulo descreve como proteger, configurar e gerenciar as máquinas agente em seu ambiente do AppAssure. Ele inclui as seguintes seções:

- Sobre a proteção de estações de trabalho e servers
- Sobre programações de proteção
- Proteção de uma máquina
- Configuração das definições de máquina
- Visualização do diagnóstico do sistema
- Gerenciamento das definições de trabalho do Core
- Implementação de um agente (instalação de envio por push)
- Gerenciamento de máquinas
- Gerenciamento de várias máquinas
- Gerenciamento de snapshots e pontos de recuperação
- Gerenciamento dos SQL e Exchange Servers
- Sobre a restauração de dados de pontos de recuperação
- Sobre exportação de dados protegidos de máquinas com Windows para máquinas virtuais
- Noções básicas sobre Bare Metal Restore
- Roteiro de realização de uma bare metal restore em máquinas com Windows
- Gerenciamento de uma imagem de inicialização do Windows
- Início de uma bare metal restore no Windows
- Confirmação de um bare metal restore
- Roteiro de realização de uma bare metal restore em máquinas com Linux
- Gerenciamento de uma imagem de inicialização do Linux
- Gerenciamento de partições Linux
- Início de uma bare metal restore no Linux
- Confirmação da bare metal restore na linha de comando
- Visualização de tarefas, alertas e eventos

Sobre a proteção de estações de trabalho e servers

Para proteger seus dados usando o AppAssure 5, é preciso adicionar as estações de trabalho e servers para proteção no AppAssure 5 Core Console; por exemplo, seu Exchange server, SQL Server, server Linux, e assim por diante.

NOTA: Neste capítulo, em geral a palavra *"máquina"* também se refere ao software AppAssure 5 Agent instalado nesta máquina.

No AppAssure 5 Core Console, é possível identificar a máquina na qual um AppAssure 5 Agent está instalado e especificar que volumes proteger, por exemplo, um espaço de armazenamento do Microsoft Windows. É possível definir as programações de proteção, adicionar medidas adicionais de segurança, como criptografia, e muito mais. Para obter mais informações sobre como acessar o AppAssure 5 Core Console para proteger estações de trabalho e servers, consulte Proteção de uma máquina.

Limitações de suporte para volumes dinâmicos e básicos

O AppAssure 5 suporta a obtenção de snapshots de todos os volumes dinâmicos e básicos. O AppAssure 5 também suporta a exportação de volumes dinâmicos simples que estão em um único disco físico. Como o próprio nome indica, os volumes dinâmicos simples não são volumes distribuídos, espelhados ou estendidos.

Discos dinâmicos (com exceção de discos dinâmicos simples, conforme descrito anteriormente) não estão disponíveis para seleção no Assistente de exportação. Volumes dinâmicos não simples têm geometrias de disco arbitrárias, que não podem ser totalmente interpretadas. Logo, o AppAssure 5 não suporta a exportação de volumes dinâmicos complexos ou não simples.

Uma notificação aparece na interface do usuário para avisar que as exportações são limitadas e estão restritas a volumes dinâmicos simples. Se você tentar exportar algo que não seja um volume único simples, a tarefa de exportação falhará.

Sobre programações de proteção

Uma programação de proteção define quando as cópias de segurança são transferidas de máquinas agente protegidas para o AppAssure 5 Core.

As programações de proteção são inicialmente definidas usando o Assistente de proteção de máquina ou o Assistente de proteção de diversas máquinas. É possível então modificar a programação existente a qualquer momento na guia Resumo de uma máquina agente específica.

NOTA: Para obter informações sobre a proteção de uma única máquina, consulte Proteção de uma máquina. Para obter informações sobre proteção em massa (de várias máquinas), consulte Proteção de várias máquinas. Para obter informações sobre personalização de períodos de proteção ao proteger um agente usando um desses assistentes, consulte Criação de programações de proteção personalizadas. Para obter informações sobre a modificação de uma programação de proteção existente, consulte Modificação das programações de proteção.

O AppAssure 5 oferece uma programação de proteção padrão, com dois períodos de proteção definidos. O primeiro período é para dias de semana (de segunda a sexta-feira), com um único período de tempo definido (0h-23h59). O intervalo padrão (o período entre os snapshots) é de 60 minutos.

O segundo período é para fins de semana (sábado e domingo). O intervalo padrão também é de 60 minutos.

Quando a proteção é ativada pela primeira vez, a programação é ativada. Assim, ao usar as definições padrão, independentemente da hora do dia atual, a primeira cópia de segurança ocorrerá a cada hora cheia (0h, 1h, 2h, e assim por diante).

A primeira transferência de cópia de segurança salva no Core é chamada de snapshot de imagem de base. Todos os dados em todos os volumes especificados (incluindo o sistema operacional, aplicativos e definições) são salvos no Core. Depois disso, os snapshots incrementais (cópias de segurança menores, compostas apenas de dados alterados no agente desde a última cópia de segurança) são salvos regularmente no core, com base no intervalo definido (por exemplo, a cada 60 minutos).

É possível criar uma programação personalizada para alterar a frequência de cópias de segurança. Por exemplo, uma alteração simples que pode ser feita é alterar o intervalo do período de dia da semana para 20 minutos, resultando em três snapshots a cada hora. Ou é possível aumentar o intervalo nos fins de semana, quando há pouco tráfego, de 60 para 180 minutos, resultando em snapshots a cada três horas.

Também podem ser definidos horários de pico e fora do pico para os dias da semana. Para fazer isso usando o Assistente de programação de proteção, altere a hora padrão inicial e final para um intervalo menor de tempo (por exemplo, 8h-16h59) e defina um intervalo adequado (por exemplo, 20 minutos). Isso representa cópias de segurança frequentes nos períodos de pico.

Daí, selecione **Tirar snapshots nos períodos restantes** e defina um intervalo (possivelmente maior) apropriado (de 180 minutos, por exemplo). Essas definições determinam um período fora do horário de pico que inclui todos os períodos de segunda a sexta-feira que estão fora do período de pico definido. Isso resulta em snapshots a cada três horas, de 0h a 7h59 e de 17h a 23h59.

Outras opções na página do Assistente de programação de proteção incluem a definição da hora de proteção diária. Isso resulta em uma única cópia de segurança diária no período definido (a definição padrão é 12h).

A opção de pausar inicialmente a proteção impede a ocorrência de uma imagem de base (e, de fato, impede todas as cópias de segurança) até que a proteção seja retomada explicitamente. Quando você estiver pronto para começar a proteger as suas máquinas com base na programação de proteção estabelecida, você deve retomar explicitamente a proteção. Para obter mais informações sobre a retomada da proteção, consulte Pausa e retomada da proteção. Como opção, caso queira proteger uma máquina imediatamente, você pode forçar um snapshot. Para obter mais informações, consulte Forçar snapshot.

Proteção de uma máquina

Este tópico descreve como começar a proteger os dados em uma única máquina especificada usando o Assistente de proteção de máquina.

NOTA: A máquina deve ter o software AppAssure 5 Agent instalado para ser protegida. É possível optar por instalar o software Agent antes deste procedimento ou implementá-lo na máquina agente como parte da conclusão do Assistente de proteção de máquina. Para obter mais informações sobre a instalação do software Agent, consulte “Instalação de Agents em máquinas com Windows” no *Guia de implementação do Dell AppAssure 5*.

Se o software Agent não estiver instalado antes de proteger uma máquina, não será possível selecionar volumes específicos para proteção como parte desse assistente. Nesse caso, por padrão, todos os volumes na máquina agente serão incluídos para proteção.

O AppAssure 5 suporta a proteção e recuperação de máquinas configuradas com partições EISA. O suporte também foi estendido para máquinas com Windows 8 e 8.1, e Windows 2012 e 2012 R2, que usam o Windows Recovery Environment (Windows RE).

Para proteger várias máquinas ao mesmo tempo, consulte Proteção de várias máquinas.

Ao adicionar proteção, é preciso definir as informações de conexão, como o endereço IP e a porta, e fornecer credenciais para a máquina que deseja proteger. Como opção, você pode fornecer um nome de exibição para aparecer no Core Console em vez do endereço IP. Defina também a programação de proteção da máquina.

Esse processo inclui etapas opcionais que podem ser acessadas se você selecionar uma configuração avançada, incluindo adicionar um novo repositório ou especificar um existente, e opcionalmente adicionar criptografia aos dados salvos no Core dessa máquina.

O fluxo de trabalho do assistente pode ser ligeiramente diferente com base no seu ambiente. Por exemplo, se o software Agent estiver instalado na máquina que você deseja proteger, não será solicitada a instalação dele

com o assistente. De forma semelhante, se um repositório já existir no Core, você não será solicitado a criar outro.

Para proteger uma máquina

1 Se o software AppAssure 5 Agent já estiver instalado na máquina que você deseja proteger, mas ela ainda não foi reiniciada, faça isso agora.

2 Na máquina do core, navegue até o AppAssure 5 Core Console e, na barra de botões, clique em **Proteger**.

Aparece o Assistente de proteção de máquina.

3 Na página Bem-Vindo, selecione as opções de instalação apropriadas:

- Se não for preciso definir um repositório ou estabelecer a criptografia, selecione **Típico**.
- Se você precisar criar um repositório ou definir um repositório diferente para cópias de segurança da máquina selecionada, ou ainda se desejar estabelecer a criptografia usando o assistente, selecione **Avançado (exibir etapas opcionais)**.
- Como opção, se você não quiser ver a página Bem-Vindo do Assistente de proteção de máquina no futuro, selecione a opção **Ignorar a página Bem-Vindo na próxima vez que o assistente for aberto**.

4 Quando estiver satisfeito com suas seleções na página Bem-Vindo, clique em **Avançar**.

A página Conexão é exibida.

5 Na página Conexão, insira as informações sobre a máquina à qual deseja se conectar, conforme descrito na tabela a seguir, e clique em **Avançar**.

Tabela 45.

Caixa de texto	Descrição
Host	O nome de host ou endereço IP da máquina que deseja proteger.
Port	O número da porta pela qual o AppAssure 5 Core se comunica com o Agent na máquina. O número de porta padrão é 8006.
Nome de usuário	O nome de usuário utilizado para se conectar a essa máquina; por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
Senha	A senha usada para se conectar à máquina.

6 Se a página Proteção for exibida em seguida no Assistente de proteção de máquina, vá para a Etapa 7.

Se a página Instalar Agent aparecer em seguida no Assistente de proteção de máquina, isso indicará que o software Agent ainda não está instalado na máquina designada. Clique em **Avançar** para instalar o software Agent.

> **NOTA:** O software Agent deve ser instalado na máquina que você deseja proteger, e a máquina deve ser reiniciada antes que possa fazer a cópia de segurança no Core. Para fazer o instalador reiniciar a máquina agente, selecione a opção **Após a instalação, reiniciar a máquina automaticamente (recomendado)** antes de clicar em **Avançar**.

A página Proteção é exibida.

7 Como opção, se você quiser um nome que não seja o endereço IP para ser exibido no AppAssure 5 Core Console dessa máquina agente, no campo Nome de exibição, digite um nome na caixa de diálogo.

Você pode inserir até 64 caracteres.

8 Selecione a programação de proteção adequada, como descrito a seguir.

- Para usar a programação de proteção padrão, na opção Definições da programação, selecione **Proteção padrão (snapshots horários de todos os volumes)**.

Com uma programação de proteção padrão, o Core tirará snapshots da máquina agente uma vez a cada hora. Para alterar as definições de proteção a qualquer momento depois de fechar o assistente, incluindo escolher quais volumes proteger, vá até a guia Resumo da máquina agente específica.

- Para definir uma programação de proteção diferente, na opção Definições de programação, selecione **Proteção personalizada**.

9 Prossiga com a configuração da seguinte maneira:

- Se a configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção padrão tiver sido especificada, clique em **Concluir** para confirmar suas escolhas, fechar o assistente e proteger a máquina especificada.
- Da primeira vez que a proteção for adicionada a uma máquina, a imagem de base (isto é, um snapshot de todos os dados dos volumes protegidos) será transferida para o repositório no AppAssure 5 Core de acordo com a programação definida, a não ser que tenha sido especificado pausar inicialmente a proteção.
- Se a configuração Típico tiver sido selecionada para o Assistente de proteção de máquina e a proteção personalizada tiver sido especificada, clique em **Avançar** para definir uma programação de proteção personalizada. Para obter detalhes sobre a definição de uma programação de proteção personalizada, consulte Criação de programações de proteção personalizadas.
- Se a configuração Avançado tiver sido selecionada para o Assistente de proteção de máquina, além da proteção padrão, clique em **Avançar** e vá para a Etapa 12 para ver as opções de repositório e criptografia.
- Se a configuração Avançado tiver sido selecionada para o Assistente de proteção de máquina e a proteção personalizada tiver sido especificada, clique em **Avançar** e vá para a Etapa 10 para escolher os volumes a proteger.

10 Na página Volumes de proteção, selecione os volumes na máquina agente que deseja proteger. Se você não deseja incluir na proteção algum volume relacionado, clique na coluna Verificar para limpar a seleção. Depois, clique em **Avançar**.

NOTA: Normalmente, é uma boa prática proteger, no mínimo, o volume Reservado pelo sistema e o volume em que se encontra o sistema operacional (normalmente a unidade C).

11 Na página Programação de proteção, defina uma programação de proteção personalizada.

12 Na página Repositório, realize um dos procedimentos a seguir:

- Se você deseja armazenar os dados dessa máquina para proteção em um repositório existente, selecione **Utilizar um repositório existente**, selecione o repositório apropriado na lista e clique em **Avançar**.

  A página Criptografia é exibida. Como opção, vá para a Etapa 17 para definir a criptografia.

- Se você deseja criar um novo local de armazenamento no Core, faça o seguinte:

  a Selecione **Criar um repositório**.

  b Na página Repositório, no campo **Nome**, especifique o nome do repositório que deseja criar.

  Em geral é a palavra Repositório e um número de índice, que corresponde ao número do novo repositório (por exemplo, **Repository1**). Você pode alterar o nome conforme necessário. Você pode inserir até 40 caracteres. Esse nome precisa ser exclusivo desse core.

  NOTA: Ao especificar o nome do repositório, use somente caracteres alfanuméricos ou o hífen. Nenhum outro símbolo ou caractere de pontuação é permitido. Não use combinações de letras que especificam comandos ou palavras reservadas (como con, prn, aux ou null) ou que representam portas (como com ou lpt).

  c No campo **Local**, insira um caminho de diretório para o repositório. Por exemplo, em um computador local, digite **C:\Repository**. Esse local precisa ser exclusivo desse core. Se

você estiver armazenando o repositório em uma unidade compartilhada, insira no formato \\servidor\compartilhamento.

CUIDADO: Se você excluir o repositório no futuro, o programa Instalador removerá todo o conteúdo do caminho do repositório. Por esse motivo, não crie o local de armazenamento na raiz (por exemplo, c:\), o que pode resultar na perda de todos os dados armazenados no volume.

d Se o repositório for armazenado em um volume compartilhado, no campo **Nome de usuário**, insira o nome de usuário com privilégios para acessar a unidade compartilhada e, no campo **Senha**, insira a senha desse usuário.

e No campo **Caminho de metadados**, insira o caminho onde deseja que os metadados sejam armazenados. Esse deve ser um subdiretório do local de armazenamento. Por exemplo, se o local de armazenamento for C:\Repository, digite **C:\Repository\Metadata**. Esse precisa ser um caminho exclusivo desse core.

13 Depois de inserir todos os dados necessários na página Repositório, clique em **Avançar** .

A página Configuração do repositório é exibida.

14 Especifique o tamanho do repositório.

NOTA: Se o local de armazenamento for um volume NTFS (Sistema de arquivos de nova tecnologia) usando o Windows XP ou Windows 7, o limite de tamanho do arquivo é 16 TB.

Se o local de armazenamento for um volume NTFS usando o Windows 8, Windows 8.1 ou Windows Server 2012, 2012 R2, o limite de tamanho do arquivo é 256 TB.

Para que o AppAssure 5 valide o sistema operacional, o Windows Management Instrumentation (WMI) deve ser instalado no local de armazenamento pretendido.

15 Para especificar bytes por setor, bytes por registro ou controlar a política de cache de gravação, selecione **Exibir opções avançadas** e, em seguida, insira os detalhes do local de armazenamento, como descrito na tabela a seguir.

Tabela 46.

Caixa de texto	Descrição
Bytes por setor	Especifique o número de bytes que você deseja incluir em cada setor. O valor padrão é *512*.
Bytes por registro	Especifique a média de bytes por registro. O valor padrão é *8192*.
Política de cache de gravação	A política de cache de gravação controla como o Gerenciador de cache do Windows é usado no repositório e ajuda a ajustar o repositório para que o melhor desempenho seja obtido com diferentes configurações. Defina o valor para um dos seguintes: • Ligado • Desligado • Sincronizar Se definido como *Ligado*, que é o padrão, o Windows controla o armazenamento em cache. **NOTA:** Definir a política de cache de gravação como *Ligado* pode resultar em desempenho mais rápido. Se você estiver usando uma versão do Windows Server anterior à Server 2012, a definição recomendada é *Desligado*. Se definido como *Desligado*, o AppAssure 5 controla o armazenamento em cache. Se definido como *Sincronizar*, o Windows controla o armazenamento em cache, além da entrada/saída síncrona.

16 Quando estiver satisfeito com as informações de configuração do repositório inseridas, clique em **Avançar**.

A página Criptografia é exibida.

17 Como opção, para habilitar a criptografia, na página Criptografia, selecione **Habilitar criptografia**.

O campo Chave de criptografia é exibido na página Criptografia.

NOTA: Se você habilitar a criptografia, ela será aplicada a dados de todos os volumes protegidos para essa máquina agente.

É possível alterar as definições mais tarde na guia Configuração no AppAssure 5 Core Console.

Para obter mais informações sobre criptografia, consulte o tópico Gerenciamento da segurança.

CUIDADO: O AppAssure 5 usa a criptografia AES de 256 bits no modo Cipher Block Chaining (CBC) com chaves de 256 bits. Embora o uso de criptografia seja opcional, a Dell recomenda fortemente que você estabeleça uma chave de criptografia e que proteja a frase de acesso definida. Armazene a frase de acesso em um local seguro, pois ela é essencial para a recuperação dos dados. Sem a frase de acesso, não é possível executar a recuperação dos dados.

18 Insira as informações conforme descrito na tabela a seguir para adicionar uma chave de criptografia para o Core.

Tabela 47.

Caixa de texto	Descrição
Nome	Insira um nome para a chave de criptografia.
Descrição	Insira uma descrição para fornecer detalhes adicionais da chave de criptografia.
Frase de acesso	Insira a frase de acesso usada para controlar o acesso.
Confirmar frase de acesso	Insira novamente a frase de acesso que você acabou de inserir.

19 Clique em **Concluir** para salvar e aplicar suas definições.

Da primeira vez que a proteção for adicionada a uma máquina, a imagem de base (isto é, um snapshot de todos os dados dos volumes protegidos) será transferida para o repositório no AppAssure 5 Core de acordo com a programação definida, a não ser que tenha sido especificado pausar inicialmente a proteção.

Criação de programações de proteção personalizadas

Ao definir a proteção usando o Assistente de proteção de máquina ou o Assistente de proteção de várias máquinas, é preciso definir uma programação de proteção.

A programação de proteção padrão inclui dois períodos de proteção definidos: um para dias de semana e outro para fins de semana. O intervalo de tempo padrão para ambos é de 0h a 23h59, abrangendo um período total de 24 horas. O intervalo padrão para ambos os períodos de proteção é de 60 minutos.

Usando o assistente, é possível personalizar as programações de proteção, podendo escolher entre períodos ou um período de proteção diário.

A seleção de períodos permite visualizar a programação de proteção padrão e fazer os ajustes necessários. A seleção de um período de proteção diário faz o AppAssure 5 efetuar a cópia de segurança das máquinas protegidas designadas uma vez por dia em um horário especificado.

Ao usar períodos, você pode fazer alterações simples na programação de proteção padrão. Por exemplo, você talvez queira simplesmente alterar o intervalo na programação padrão de dia da semana para cada 20 minutos, resultando em cópias de segurança três vezes por hora em vez de uma vez por hora.

É possível criar também programações de proteção mais complexas. Por exemplo, é possível criar períodos de pico e fora do pico para dias da semana, como descrito em Sobre programações de proteção.

Finalmente, ao proteger uma ou várias máquinas usando o assistente, é possível inicialmente pausar a proteção, o que define a programação de proteção sem iniciá-la. Quando você estiver pronto para começar a proteger as suas máquinas com base na programação de proteção estabelecida, você deve retomar explicitamente a proteção. Para obter mais informações sobre a retomada da proteção, consulte Pausa e retomada da proteção. Como opção, caso queira proteger uma máquina imediatamente, você pode forçar um snapshot. Para obter mais informações, consulte Forçar snapshot.

NOTA: Para obter informações conceituais sobre programações de proteção, consulte Sobre programações de proteção. Para obter informações sobre a proteção de uma única máquina, consulte Proteção de uma máquina. Para obter informações sobre proteção em massa (de várias máquinas), consulte Proteção de várias máquinas. Para obter informações sobre personalização de períodos de proteção ao proteger um agente usando um desses assistentes, consulte Criação de programações de proteção personalizadas. Para obter informações sobre a modificação de uma programação de proteção existente, consulte Modificação das programações de proteção.

Execute as etapas deste procedimento para criar programações personalizadas para a proteção de dados em máquinas agente ao definir a proteção usando um assistente.

Para criar programações personalizadas

1 Na página Programação de proteção do Assistente de proteção de máquina ou do Assistente de proteção de diversas máquinas, para alterar a programação de intervalo para qualquer período, faça o seguinte:

   a Selecione **Períodos**.

   Os períodos existentes são exibidos e podem ser modificados. Os campos editáveis incluem hora inicial, hora final e intervalo (em minutos) de cada período.

   b Clique no campo de intervalo e digite um intervalo adequado em minutos.

   Por exemplo, destaque o intervalo existente e substitua-o pelo valor **20** para realizar snapshots a cada 20 minutos durante esse período.

2 Para criar um período de pico e fora do pico nos dias da semana, altere o intervalo de tempo do período em dias da semana para que ele não inclua um período de 24 horas, defina um intervalo ideal para o pico, selecione **Tirar snapshots no período restante** e defina um intervalo fora do pico, fazendo o seguinte:

   a Selecione **Períodos**.

   Os períodos existentes são exibidos e podem ser modificados.

   b Clique na caixa **De** para alterar a hora inicial desse período.

   A caixa de diálogo Selecionar hora é exibida.

   c Arraste os controles deslizantes de Horas e Minutos, conforme apropriado, até a hora inicial desejada e clique em **Concluído**. Para especificar a hora atual, clique em **Agora**.

   Por exemplo, arraste o controle Horas para exibir o horário 08:00 AM

   d Clique na caixa **A** para alterar a hora final desse período.

   A caixa de diálogo Selecionar hora é exibida.

   e Arraste os controles deslizantes de Horas e Minutos, conforme apropriado, até a hora inicial desejada e clique em **Concluído**. Para especificar a hora atual, clique em **Agora**.

   Por exemplo, arraste o controle Horas para exibir o horário 04:59 AM

3 Para definir uma única hora do dia para uma única cópia de segurança diária, selecione **Tempo de proteção diária** e insira a hora no formato HH:MM. Por exemplo, para fazer uma cópia de segurança diária às 21h, insira 21:00.

4 Para definir a programação sem iniciar as cópias de segurança, selecione **Pausar proteção inicialmente**.

Depois de pausar a proteção no assistente, ela permanece em pausa até que você a retome explicitamente. Depois de retomar a proteção, as cópias de segurança ocorrerão com base na programação estabelecida. Para obter mais informações sobre a retomada da proteção, consulte Pausa e retomada da proteção.

5 Quando estiver satisfeito com as alterações feitas na sua programação de proteção, clique em **Concluir** ou **Avançar**, conforme o caso. Retorne ao procedimento do assistente apropriado para concluir os requisitos restantes.

Modificação das programações de proteção

Uma programação de proteção define quando as cópias de segurança são transferidas de máquinas agente protegidas para o AppAssure 5 Core. As programações de proteção são inicialmente definidas usando o Assistente de proteção de máquina ou o Assistente de proteção de diversas máquinas.

É possível modificar a programação de proteção existente a qualquer momento na guia Resumo de uma máquina agente específica.

NOTA: Para obter informações conceituais sobre programações de proteção, consulte Sobre programações de proteção. Para obter informações sobre a proteção de uma única máquina, consulte Proteção de uma máquina. Para obter informações sobre proteção em massa (de várias máquinas), consulte Proteção de várias máquinas. Para obter informações sobre personalização de períodos de proteção ao proteger um agente usando um desses assistentes, consulte Criação de programações de proteção personalizadas. Para obter informações sobre a modificação de uma programação de proteção existente, consulte Modificação das programações de proteção.

Execute as etapas deste procedimento para modificar uma programação de proteção existente para volumes de uma máquina protegida.

Para modificar programações de proteção

1 Navegue até o AppAssure 5 Core Console.

2 Na lista de máquinas protegidas, selecione a máquina com uma programação de proteção definida que você deseja alterar.

A guia Resumo é exibida para a máquina.

3 Selecione os volumes da máquina protegida que você deseja alterar e clique em **Definir uma programação**. Para selecionar todos os volumes de uma só vez, clique na caixa de seleção na linha de cabeçalho.

Inicialmente, todos os volumes compartilham a mesma programação de proteção. Normalmente, é uma boa prática proteger, no mínimo, o volume Reservado pelo sistema e o volume em que se encontra o sistema operacional (normalmente a unidade C).

A caixa de diálogo Programação de proteção é exibida.

4 Na caixa de diálogo Programação de proteção, se você já tiver criado um modelo de programação de proteção e quiser aplicá-lo a esse agente, selecione o modelo na lista suspensa e depois vá para a Etapa 10.

5 Se você quiser salvar essa nova programação de proteção como um modelo, insira um nome para o modelo na caixa de texto.

6 Se você quiser remover um período existente da programação, desmarque as caixas de seleção ao lado de cada opção de período. Entre as opções estão:

- **Seg.-Sex.** Esse intervalo de tempo indica uma semana típica de cinco dias de trabalho.
- **Sáb.-Dom.** Esse intervalo de tempo indica um fim de semana típico.

7 Se a hora inicial e final do dia da semana forem 0h a 23h59, existe um único período. Para alterar a hora inicial e final de um período definido, faça o seguinte:

a Selecione o período adequado.

b Clique na caixa **Hora inicial** para alterar a hora inicial desse período.

A caixa de diálogo Selecionar hora é exibida.

c Arraste os controles deslizantes de Horas e Minutos, conforme apropriado, até a hora inicial desejada e clique em **Concluído**. Para especificar a hora atual, clique em **Agora**.

Por exemplo, arraste o controle Horas para exibir o horário 08:00 AM

d Clique na caixa **Hora final** para alterar a hora final desse período.

A caixa de diálogo Selecionar hora é exibida.

e Arraste os controles deslizantes de Horas e Minutos, conforme apropriado, até a hora inicial desejada e clique em **Concluído**. Para especificar a hora atual, clique em **Agora**.

Por exemplo, arraste o controle Horas para exibir o horário 04:59 AM

f Altere o intervalo de acordo com suas necessidades. Por exemplo, ao definir um período de pico, altere o intervalo de 60 para 20 minutos para tirar snapshots três vezes por hora.

8 Se um período diferente de 0h a 23h59 tiver sido definido no Etapa 7, então se desejar que as cópias de segurança ocorram nos intervalos de tempo restantes, será preciso adicionar períodos adicionais para definir a proteção, fazendo o seguinte:

a Clique em **+ Adicionar período.**

Sob a categoria apropriada (dias de semana ou fins de semana), um novo período aparece. Se o primeiro período começou depois de 0h, o AppAssure 5 inicia automaticamente esse período à 0h. De acordo com o exemplo acima, esse segundo período inicia à 0h. Pode ser necessário ajustar horas ou minutos das horas inicial e final.

b Arraste os controles deslizantes de Horas e Minutos, conforme apropriado, até a hora inicial ou final, conforme o caso.

Por exemplo, defina a hora inicial em 0h e a hora final em 7h59.

c Altere o intervalo de acordo com suas necessidades. Por exemplo, ao definir um período fora do pico, altere o intervalo de 60 para 120 minutos para tirar snapshots a cada duas horas.

9 Se necessário, continue a criar períodos adicionais, definindo horas iniciais e finais e intervalos conforme apropriado.

NOTA: Se você quiser remover um período que adicionou, clique no **X** na extrema direita desse período. Caso tenha sido um erro remover o período, clique em **Cancelar**.

10 Quando sua programação de proteção atender às suas necessidades, clique em **Aplicar**.

A caixa de diálogo Programação de proteção é fechada.

Gerenciamento de máquinas com Exchange e SQL Server

As opções específicas para o Exchange Server e o SQL Server são exibidas no AppAssure 5 Core Console quando uma instância do software e bancos de dados associados são detectados em servers protegidos. Esta seção inclui os seguintes tópicos específicos para o gerenciamento de máquinas protegidas que utilizam o Exchange Server ou o SQL Server:

Esta seção inclui os seguintes tópicos:

- Modificação das definições do Exchange Server
- Forçamento de uma verificação de capacidade de montagem de um banco de dados do Exchange
- Forçamento de verificações de soma de verificação de pontos de recuperação do Exchange Server
- Modificação das definições do SQL Server
- Forçamento de uma verificação de capacidade de anexação do SQL Server
- Forçamento do truncamento de log para uma máquina com SQL ou com Exchange

Modificação das definições do Exchange Server

Se você estiver protegendo dados de um Microsoft Exchange server, precisará configurar as definições adicionais no AppAssure 5 Core Console.

Para modificar as definições do Exchange Server

1. Depois de incluir a máquina do Exchange Server na proteção, navegue até o AppAssure 5 Core Console e selecione a máquina no painel Navegação.

   A guia Resumo é exibida para a máquina.

2. Na guia Resumo, no menu suspenso **Ações**, clique em **Exchange** e, no menu suspenso sensível ao contexto, selecione a ação que deseja realizar.
   - Se desejar truncar os registros do server do Exchange, clique em **Forçar truncamento de log**.
   - Se desejar definir credenciais para um server do Exchange único, clique em **Definir credenciais**, e na caixa de diálogo Editar credenciais do Exchange, faça o seguinte:
     f. No campo de texto Nome de usuário, insira o nome de usuário com permissões para o Exchange Server, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
     g. No campo de texto Senha, insira a senha associada ao nome de usuário especificado para se conectar ao Exchange Server.
     h. Clique em **OK** para confirmar as configurações e feche a caixa de diálogo.

Forçamento de uma verificação de capacidade de montagem de um banco de dados do Exchange

Execute as etapas deste procedimento para forçar o sistema a realizar uma verificação de montabilidade de um ponto específico de recuperação do Exchange Server.

NOTA: Para ter a capacidade de forçar uma verificação de capacidade de montagem, um banco de dados do Exchange deve estar presente em um volume protegido. Se o AppAssure 5 não detecta a presença de um banco de dados, a função de verificação de capacidade de montagem não é exibida no Core Console.

Para forçar uma verificação de montabilidade

1. Na área de navegação esquerda do AppAssure 5 Core Console, selecione a máquina para a qual deseja forçar a verificação de montabilidade e clique na guia **Pontos de recuperação**.
2. Clique no símbolo de maior que **>** próximo ao ponto de recuperação na lista para expandir a visualização.
3. Clique em **Verificar**, e depois em **Forçar verificação de capacidade de montagem**.

   Uma janela pop-up é exibida perguntando se você deseja forçar uma verificação de montabilidade.
4. Clique em **Sim**.

   O sistema realiza a verificação de montabilidade.

   NOTA: Para obter instruções sobre como visualizar o status das verificações de capacidade de anexação, consulte Visualização de tarefas, alertas e eventos.

Forçamento de verificações de soma de verificação de pontos de recuperação do Exchange Server

Execute as etapas deste procedimento para forçar o sistema a realizar uma verificação de soma de verificação de um ponto específico de recuperação do Exchange Server.

NOTA: Para ter a capacidade de forçar uma verificação de soma de verificação, um banco de dados do Exchange deve estar presente em um volume protegido. Se o AppAssure 5 não detecta a presença de um banco de dados, a função de verificação de soma de verificação não é exibida no Core Console.

Para forçar uma verificação de soma de verificação

1 Na área de navegação esquerda do AppAssure 5 Core Console, selecione a máquina para a qual deseja forçar a verificação de soma de verificação e clique na guia **Pontos de recuperação**.

2 Clique no símbolo de maior que **>** próximo ao ponto de recuperação na lista para expandir a visualização.

3 Clique em **Verificar**, e depois em **Forçar a verificação de soma de verificação**.

Aparecerá a janela Forçar verificação de capacidade de anexação onde você pode indicar se deseja forçar a verificação de soma de verificação.

4 Clique em **Sim**.

O sistema realiza a verificação de soma de verificação.

NOTA: Para obter informações sobre como visualizar o status das verificações de capacidade de anexação, consulte Visualização de tarefas, alertas e eventos.

Modificação das definições do SQL Server

Se você estiver protegendo dados de um Microsoft SQL Server, precisará configurar as definições adicionais no AppAssure 5 Core Console.

Para modificar as definições do SQL Server

1 Depois de incluir a máquina do SQL Server na proteção, no AppAssure 5 Core Console, selecione a máquina no painel Navegação.

A guia Resumo é exibida para a máquina.

2 Na guia Resumo, clique no menu suspenso **Ações** e, no menu suspenso sensível ao contexto, selecione a ação que deseja realizar.

- Se desejar truncar os registros do server do SQL ou do Exchange, clique em **Forçar truncamento de log**.
- Se desejar definir credenciais padrão para todas as instâncias do SQL Server database, clique em **Definir credenciais padrão para todas as instâncias** e, na caixa de diálogo Editar credenciais padrão, faça o seguinte:
    a No campo de texto Nome de usuário, insira o nome de usuário com permissões para todos os SQL Servers associados, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
    b No campo de texto Senha, insira a senha associada ao nome de usuário especificado para se conectar ao server.ke do SQL conforme descrito na tabela a seguir.
    c Clique em **OK** para confirmar as configurações e feche a caixa de diálogo.
- Se desejar definir credenciais para uma instância do SQL Server database, clique em **Definir credenciais da instância** e, na caixa de diálogo Editar credenciais da instância, faça o seguinte:
    a Selecione o tipo de credencial (Padrão, Windows ou SQL)
    b No campo de texto Nome de usuário, insira o nome de usuário com permissões para o SQL Server, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
    c No campo de texto Senha, insira a senha associada ao nome de usuário especificado para se conectar ao SQL Server.
    d Clique em **OK** para confirmar as configurações e feche a caixa de diálogo.

Forçamento de uma verificação de capacidade de anexação do SQL Server

Execute as etapas deste procedimento para forçar o sistema a realizar uma verificação de capacidade de anexação de um ponto específico de recuperação do SQL Server.

NOTA: Para ter a capacidade de forçar uma verificação de capacidade de anexação, um banco de dados do SQL deve estar presente em um volume protegido. Se o AppAssure 5 não detecta a presença de um banco de dados, a função de verificação da capacidade de anexação não é exibida no Core Console.

Para forçar uma verificação de capacidade de anexação do SQL Server

1. Na área de navegação esquerda do AppAssure 5 Core, selecione a máquina para a qual deseja forçar a verificação de capacidade de anexação e clique na guia **Pontos de recuperação**.
2. Clique no símbolo de maior que > próximo ao ponto de recuperação na lista para expandir a visualização.
3. Clique em **Verificar**, e depois em **Forçar a verificação da capacidade de anexação**.

   Aparecerá a janela Forçar verificação de capacidade de anexação onde você pode indicar se deseja forçar a verificação de capacidade de anexação.
4. Clique em **Sim**.

   O sistema realiza a verificação de capacidade de anexação.

   NOTA: Para obter informações sobre como visualizar o status das verificações de capacidade de anexação, consulte Visualização de tarefas, alertas e eventos.

Forçamento do truncamento de log para uma máquina com SQL ou com Exchange

O truncamento de log está disponível para máquinas que utilizam o SQL Server ou o Exchange Server. Execute as etapas deste procedimento para forçar o truncamento de log.

NOTA: Quando o truncamento de log é realizado para uma máquina com Exchange, o tamanho dos logs é reduzido. Quando realizado em uma máquina com SQL, o truncamento identifica o espaço livre em um disco, mas não reduz o tamanho dos logs.

Para forçar o truncamento de log

1. No AppAssure 5 Core Console, navegue até a máquina protegida na qual deseja forçar o truncamento de log.
2. Na guia Resumo da máquina protegida, clique no menu suspenso **Ações** e execute um dos procedimentos a seguir:
   - Se a máquina protegida usa SQL Server, selecione **SQL** e clique em **Forçar truncamento de log**.
   - Se a máquina protegida usa Exchange Server, selecione **Exchange** e clique em **Forçar truncamento de log**.
3. Clique em **Sim** para confirmar que deseja forçar o truncamento de log.

Personalização de trabalhos noturnos para uma máquina protegida

Os trabalhos noturnos podem ser configurados no nível do Core e no nível da máquina na guia Configuração adequada. Quando as configurações de trabalho noturno são alteradas no nível do Core, as alterações são aplicadas a todas as máquinas relevantes protegidas por esse Core. As alterações feitas nos trabalhos noturnos no nível da máquina substituem as alterações feitas no nível do Core.

Execute as etapas do procedimento a seguir para realizar alterações em trabalhos noturnos em uma única máquina.

Personalizar trabalhos noturnos para uma máquina protegida

1 Na área de navegação à esquerda do AppAssure 5 Core, selecione a máquina para a qual deseja personalizar trabalhos noturnos.

A guia Resumo da máquina selecionada é exibida.

2 Clique na guia Configuração para a máquina, e depois em **Configurações**.

3 Ao lado de Trabalhos noturnos, clique em **Alterar**.

A caixa de diálogo Trabalhos noturnos é exibida.

4 Selecione os trabalhos que deseja incluir nos trabalhos noturnos ou desmarque as opções que deseja omitir para essa máquina.

> **NOTA:** As opções podem variar por máquina. Por exemplo, uma máquina protegida que utiliza o Exchange Server poderá incluir os logs de trabalho de verificação de soma de verificação e de truncamento do Exchange.

5 Clique em **OK**.

> **NOTA:** Os resultados desse procedimento aplicam-se apenas à máquina protegida selecionada. Para serem aplicados em outro local, repita o procedimento para cada máquina que desejar personalizar. Para alterar as configurações de trabalho noturno para todas as máquinas protegidas por um Core, consulte Configuração de trabalhos noturnos para o Core, Configuração das verificações noturnas de capacidade de anexação do SQL e truncamento de log para todas as máquinas protegidas ou Configuração de verificações de soma de verificação do banco de dados do Exchange noturno e truncamento de log.

Pausa e retomada da proteção

Ao pausar a proteção, você interrompe temporariamente todas as transferências de dados da máquina selecionada para o AppAssure 5 Core. Ao retomar a proteção, o AppAssure 5 Core segue os requisitos da programação de proteção, fazendo a cópia de segurança de seus dados regularmente com base nessa programação.

É possível pausar a proteção de qualquer máquina agente do AppAssure 5:

- Ao estabelecer a proteção usando o Assistente de proteção de máquina ou o Assistente de proteção de diversas máquinas.
- No menu Máquinas protegidas na área de navegação à esquerda do AppAssure 5 Core (pausando a proteção de todos os agentes).
- Na página Máquinas protegidas (acessível ao clicar no menu Máquinas protegidas).
- Em uma máquina protegida específica no menu Máquinas protegidas.
- Na guia Resumo de qualquer máquina agente protegida.

Se você pausar a proteção usando o Assistente de proteção de máquina ou o Assistente de proteção de diversas máquinas, ela será pausada até ser retomada explicitamente.

Se você pausar a proteção fora de um assistente, poderá escolher se quer fazer isso até ela ser retomada ou por um período designado (especificado em qualquer combinação de dias, horas e minutos). Se você pausar por um período, quando esse tempo acabar, o sistema retomará automaticamente a proteção com base na programação de proteção.

É possível retomar a proteção de qualquer agente do AppAssure 5 em pausa:

- No menu Máquinas protegidas na área de navegação à esquerda do AppAssure 5 Core (retomando a proteção de todos os agentes).
- Em uma máquina protegida específica no menu Máquinas protegidas.
- Na página Máquinas protegidas (acessível ao clicar no menu Máquinas protegidas).
- Na guia Resumo de qualquer máquina agente protegida.

Use o procedimento a seguir para pausar ou retomar a proteção, conforme o caso.

Para pausar e retomar a proteção

1 No AppAssure 5 Core Console, para pausar ou retomar a proteção de todas as máquinas, clique no menu suspenso **Máquinas protegidas** na área de navegação à esquerda.

- Caso queira pausar a proteção, faça o seguinte:
  a Selecione **Pausar proteção**.

  A caixa de diálogo Pausar proteção é exibida.

  b Selecione a definição apropriada, usando uma das opções descritas abaixo, e clique em **OK**.

  - Se quiser pausar a proteção até retomá-la explicitamente, selecione **Pausar até ser retomada**.
  - Se você quiser pausar a proteção por um período específico, selecione **Pausar por** e depois, nos controles de Dias, Horas e Minutos, digite ou selecione o período de pausa apropriado, conforme o caso.
- Caso queira retomar a proteção, faça o seguinte:
  a Selecione **Retomar proteção**.

  A caixa de diálogo Retomar proteção é exibida.

  b Na caixa de diálogo Retomar proteção, selecione **Sim**.

  A caixa de diálogo Retomar proteção é fechada e a proteção é retomada para todas as máquinas.

2 Para pausar ou retomar a proteção de uma única em qualquer guia, na área de navegação à esquerda, na lista de máquinas protegidas, clique na seta à direita da máquina que deseja operar.

- Caso queira pausar a proteção, faça o seguinte:
  a Selecione **Pausar proteção**.

  A caixa de diálogo Pausar proteção é exibida.

  b Selecione a definição apropriada, usando uma das opções descritas abaixo, e clique em **OK**.

  - Se quiser pausar a proteção até retomá-la explicitamente, selecione **Pausar até ser retomada**.
  - Se você quiser pausar a proteção por um período específico, selecione **Pausar por** e depois, nos controles de Dias, Horas e Minutos, digite ou selecione o período de pausa apropriado, conforme o caso.
- Caso queira retomar a proteção, faça o seguinte:
  a Selecione **Retomar proteção**.

  A caixa de diálogo Retomar proteção é exibida.

  b Na caixa de diálogo Retomar proteção, selecione **Sim**.

  A caixa de diálogo Retomar proteção é fechada e a proteção é retomada para a máquina selecionada.

3 Para pausar ou retomar a proteção de uma única máquina na guia Resumo, navegue até a máquina que deseja operar.

A guia Resumo é exibida para a máquina selecionada.

- Caso queira pausar a proteção, faça o seguinte:
  a No menu suspenso **Ações** dessa máquina, selecione **Pausar proteção**.

  A caixa de diálogo Pausar proteção é exibida.

  b Selecione a definição apropriada, usando uma das opções descritas abaixo, e clique em **OK**.

- Se quiser pausar a proteção até retomá-la explicitamente, selecione **Pausar até ser retomada**.
- Se você quiser pausar a proteção por um período específico, selecione **Pausar por** e depois, nos controles de Dias, Horas e Minutos, digite ou selecione o período de pausa apropriado, conforme o caso.

- Caso queira retomar a proteção, faça o seguinte:

  a Selecione **Retomar proteção**.

  A caixa de diálogo Retomar proteção é exibida.

  b Na caixa de diálogo Retomar proteção, selecione **Sim**.

  A caixa de diálogo Retomar proteção é fechada e a proteção é retomada para a máquina selecionada.

Configuração das definições de máquina

Depois de adicionar proteção para máquinas no AppAssure, é fácil modificar as definições básicas da configuração de máquina (nome, nome de host, e assim por diante), definições de proteção (mudando a programação de proteção para volumes da máquina, adicionando ou removendo volumes ou pausando a proteção), e muito mais. Esta seção descreve as várias maneiras de visualizar e modificar as definições da máquina no AppAssure.

Visualização e modificação das definições de configuração

Execute as etapas deste procedimento para modificar e visualizar as definições de configuração.

Essa tarefa também é uma das etapas do Processo de modificação das definições de nó de cluster.

Para visualizar e modificar as definições de configuração

1 No AppAssure 5 Core Console, navegue até a máquina da qual deseja visualizar e modificar as definições de configuração.

2 Clique na guia Configuração.

A página Definições é exibida.

3 Clique em **Alterar** para modificar as definições da máquina, como descrito na tabela a seguir.

Tabela 48.

Caixa de texto	Descrição
Nome de exibição	Insira um nome de exibição para a máquina. O nome dessa máquina será exibido no AppAssure 5 Core Console. Por padrão, esse é o nome de host da máquina. Se necessário, é possível mudá-lo para algo mais amigável.
Nome do host	Insira um nome de host para a máquina.
Port	Insira um número de porta para a máquina. A porta é usada pelo Core para se comunicar com essa máquina.

Tabela 48.

Caixa de texto	Descrição
Chave de criptografia	Edite a chave de criptografia se necessário. Especifica se a criptografia deve ser aplicada aos dados de todos os volumes da máquina armazenada no repositório.
Repositório	Selecione um repositório para os pontos de recuperação. Exibe o repositório no AppAssure 5 Core no qual devem ser armazenados os dados dessa máquina. NOTA: Essa definição pode ser alterada apenas se não houver pontos de recuperação ou o repositório anterior estiver ausente.

Visualização das informações do sistema de uma máquina

O AppAssure 5 Core Console fornece acesso fácil a todas as máquinas que estão sendo protegidas.

Execute as etapas deste procedimento para visualizar as informações detalhadas do sistema de uma máquina protegida.

Para visualizar informações do sistema de uma máquina

1. Na área de navegação à esquerda do Core Console, em Máquinas protegidas, selecione a máquina da qual deseja exibir informações detalhadas do sistema.
2. Clique na guia Ferramentas dessa máquina, que abre exibindo a página Informações do sistema.

   A página Informações do sistema exibe informações detalhadas sobre a máquina, incluindo:

   - Nome do host
   - Versão de OS
   - Arquitetura de OS
   - Memória (Física)
   - Nome de exibição
   - Nome de domínio totalmente qualificado
   - Tipo de máquina virtual (se aplicável)

   Informações detalhadas sobre os volumes contidos nessa máquina também são exibidas e incluem:

   - Nome
   - ID do dispositivo
   - Sistemas de arquivos
   - Capacidade (incluindo Bruta, Formatada e Usada)

   Outras informações da máquina que são exibidas incluem:

   - Processadores
   - Adaptadores de rede
   - Endereços IP associados a essa máquina

Configuração de grupos de notificação para eventos de sistema

No AppAssure 5, é possível configurar como os eventos do sistema são relatados por uma máquina individual criando grupos de notificação. Esses eventos podem ser alertas do sistema, erros, e assim por diante.

Para configurar grupos de notificação para eventos de sistema

1 No AppAssure 5 Core Console, navegue até a máquina que deseja modificar.

A guia Resumo é exibida.

2 Clique na guia Configuração e em **Eventos**.

Aparece a página Grupos de notificação.

3 Clique em **Usar definições de alerta personalizadas**.

A tela Grupos de notificação personalizados é exibida.

4 Clique em **Adicionar grupo** para adicionar novos grupos de notificação para o envio de uma lista de eventos do sistema.

A caixa de diálogo Adicionar grupo de notificação é exibida.

> **NOTA:** Para usar as definições de alerta padrão, selecione a opção **Usar definições de alerta do Core**.

5 Adicione as opções de notificação conforme descrito na tabela a seguir.

Tabela 49.

Caixa de texto	Descrição
Nome	Insira um nome para o grupo de notificação.
Descrição	Insira uma descrição para o grupo de notificação.

Tabela 49.

Caixa de texto	Descrição
Habilitar alertas	Selecione os eventos a compartilhar com esse grupo de notificação. É possível selecionar **Todos** ou um subconjunto de eventos que inclui: • Exchange • Atualização automática • Cache de deduplicação • Verificação de ponto de recuperação • Montagem remota • CD de inicialização • Segurança • Retenção do banco de dados • Montagem local • Metadados • Clusters • Notificação • Scripts do Power Shell • Instalação de envio por push • Capacidade de anexação • Trabalhos • Aplicação de licença • Truncamento de log • Arquivo • Serviço do Core • Exportar • Proteção • Replicação • Repositório • Reversão (Restauração) • Rollup **NOTA:** Ao decidir selecionar por tipo, como padrão, os eventos apropriados são automaticamente ativados. Por exemplo, se você escolher *Aviso*, os eventos Capacidade de anexação, Trabalhos, Aplicação de licença, Arquivo, CoreService, Exportação, Proteção, Replicação e Reversão (Restauração) são ativados.

Opções de notificação	Selecione o método para especificar como lidar com as notificações.
	Você pode selecionar dentre as seguintes opções:
	• **Notificar por e-mail**. É preciso especificar a quais endereços de e-mail enviar os eventos nas caixas de texto Para, CC e, opcionalmente, Cco.
	NOTA: Para receber e-mail, o SMTP deve ser configurado antes.
	• **Notificar pelo log de eventos do Windows**. O Log de eventos de Windows controla a notificação.
	• **Notificar por syslogd**. É preciso especificar a qual nome de host e porta enviar os eventos.
	  • **Host.** Insira o nome de host para o server.
	  • **Porta.** Insira o número da porta para a comunicação com o server.
	• **Notificar através de alertas do sistema.** Selecione esta opção se você deseja que o alerta seja exibido como uma pop-up na parte inferior direita da tela.

6 Clique em **OK** para salvar suas alterações.

7 Para editar um grupo de notificação existente, clique em **Editar** ao lado do grupo de notificação que **deseja editar**.

A caixa de diálogo Editar grupo de notificação é exibida para que as definições possam ser editadas.

Edição de grupos de notificação para eventos de sistema

Execute as etapas do procedimento a seguir para editar grupos de notificação para eventos de sistema.

Para editar grupos de notificação para eventos de sistema

1 No AppAssure 5 Core Console, navegue até a máquina que deseja modificar.

A guia Resumo é exibida.

2 Clique na guia Configuração e em **Eventos**.

3 Clique em **Usar definições de alerta personalizadas**.

A tela Grupos de notificação personalizados é exibida.

4 Clique no ícone Editar na coluna Ação.

A caixa de diálogo Editar grupo de notificação é exibida.

5 Edite as opções de notificação conforme descrito na tabela a seguir.

Tabela 50.

Caixa de texto	Descrição
Nome	Representa o nome do grupo de notificação. **NOTA:** Não é possível editar o nome do grupo de notificação.
Descrição	Insira uma descrição para o grupo de notificação.

Tabela 50.

Caixa de texto	Descrição
Habilitar alertas	Selecione os eventos a compartilhar com o grupo de notificação. É possível selecionar **Todos** ou um subconjunto de eventos que inclui: • Exchange • Atualização automática • Cache de deduplicação • Verificação de ponto de recuperação • Montagem remota • CD de inicialização • Segurança • Retenção do banco de dados • Montagem local • Metadados • Clusters • Notificação • Scripts do Power Shell • Instalação de envio por push • Capacidade de anexação • Trabalhos • Aplicação de licença • Truncamento de log • Arquivo • Serviço do Core • Exportar • Proteção • Replicação • Repositório • Reversão (Restauração) • Rollup Também é possível optar por selecionar por tipo, incluindo: Informações, Aviso e Erro. **NOTA:** Ao decidir selecionar por tipo, como padrão, os eventos apropriados são automaticamente ativados. Por exemplo, se você escolher *Aviso*, os eventos Capacidade de anexação, Trabalhos, Aplicação de licença, Arquivo, CoreService, Exportação, Proteção, Replicação e Reversão (Restauração) são ativados.

Tabela 50.

Caixa de texto	Descrição

Opções de notificação	Selecione o método para especificar como lidar com as notificações. As opções são:
	• **Notificar por e-mail**. É preciso especificar a quais endereços de e-mail enviar os eventos nas caixas de texto Para, CC e, opcionalmente, Cco.
	NOTA: Para receber e-mail, o SMTP deve ser configurado antes.
	• **Notificar pelo log de eventos do Windows**. O Log de eventos de Windows controla a notificação.
	• **Notificar por syslogd**. É preciso especificar o nome de host e a porta aos quais enviar os eventos.
	  • **Host.** Insira o nome de host para o server.
	  • **Porta.** Insira o número da porta para a comunicação com o server.
	• **Notificar através de alertas do sistema.** Selecione esta opção se você deseja que o alerta seja exibido como uma pop-up na parte inferior direita da tela.

6 Clique em **OK**.

Configuração das definições da política de retenção padrão do Core

A política de retenção do Core especifica por quanto tempo os pontos de recuperação de uma máquina de Agent são armazenados no repositório. A política de retenção é imposta pelo processo de rollup, realizado durante o processo de trabalho noturno. Nesse momento, os pontos de recuperação além da idade especificada na política de retenção são combinados em menos pontos de recuperação que abrangem um período menos granular. Aplicar a política de retenção em base noturna resulta no rollup contínuo de cópias de segurança antigas e, com o tempo, os pontos de recuperação mais antigos são excluídos, com base nos requisitos especificados nessa política de retenção.

Diferentes definições de retenção podem ser configuradas para cores de origem e de destino.

NOTA: Esse tópico é específico para personalizar as definições de política de retenção no AppAssure 5 Core. Ao salvar as definições de política de retenção personalizadas no Core, você estabelece as definições de política de retenção padrão que podem ser aplicadas a todas as máquinas agente protegidas por esse Core. Para obter mais informações sobre a personalização das definições de políticas de retenção para máquinas agente individuais, consulte Personalização das definições de política de retenção para um agente.

Para configurar as definições da política de retenção padrão do Core

1 Navegue até o AppAssure 5 Core Console, clique na guia Configuração e depois em **Política de retenção**.

Aparece a tela Política de retenção, exibindo as opções de política de retenção do Core.

2 Especifique a definição principal que determina por quanto tempo os snapshots de cópia de segurança inicial são retidos e depois passe a definir um conjunto de requisitos de rollup em cascata que determina os intervalos nos quais os pontos de recuperação devem passar por rollup.

As opções da política de retenção são descritas na tabela a seguir.

Tabela 51.

Caixa de texto	Descrição
Manter todos os pontos de recuperação por *n* [*período de retenção*]	Especifica o período de retenção para os pontos de recuperação. Insira um número para representar o período de retenção e a seguir selecione o período de tempo. O padrão é *3* dias. Você pode selecionar dentre: Dias, Semanas, Meses ou Anos
…e depois manter um Ponto de recuperação por hora por *n* [*período de retenção*]	Fornece um nível mais granular de retenção. Ele é usado como um bloco de construção com a definição principal para definir por quanto tempo os pontos de recuperação serão mantidos. Insira um número para representar o período de retenção e a seguir selecione o período de tempo. O padrão é *2* dias. Você pode selecionar dentre: Dias, Semanas, Meses ou Anos
…e depois manter um Ponto de recuperação por dia por *n* [*período de retenção*]	Fornece um nível mais granular de retenção. Ele é usado como um bloco de construção para definir por quanto tempo os pontos de recuperação serão mantidos. Insira um número para representar o período de retenção e a seguir selecione o período de tempo. O padrão é *4* dias. Você pode selecionar dentre: Dias, Semanas, Meses ou Anos
…e depois manter um Ponto de recuperação por semana por *n* [*período de retenção*]	Fornece um nível mais granular de retenção. Ele é usado como um bloco de construção para definir por quanto tempo os pontos de recuperação serão mantidos. Insira um número para representar o período de retenção e a seguir selecione o período de tempo. O padrão é *3* semanas. Você pode selecionar dentre: Semanas, Meses ou Anos
…e depois manter um Ponto de recuperação por mês por *n* [*período de retenção*]	Fornece um nível mais granular de retenção. Ele é usado como um bloco de construção para definir por quanto tempo os pontos de recuperação serão mantidos. Insira um número para representar o período de retenção e a seguir selecione o período de tempo. O padrão é *2 meses*. Você pode selecionar dentre: Meses ou Anos
…e depois manter um Ponto de recuperação por ano por *n* [*período de retenção*]	Insira um número para representar o período de retenção e a seguir selecione o período de tempo. Você pode selecionar dentre: Anos

A caixa de texto Ponto de recuperação mais novo exibe o ponto de recuperação mais recente. O ponto de recuperação mais antigo será determinado pelas definições da política de retenção.

O seguinte é um exemplo de como o período de retenção é calculado.

Manter todos os pontos de recuperação por *3 dias*.

…e depois manter um Ponto de recuperação por hora por *3 dias*

…e depois manter um Ponto de recuperação por dia por *4 dias*

…e depois manter um Ponto de recuperação por semana por *3 semanas*

…e depois manter um Ponto de recuperação por mês por *2 meses*

…e depois manter um Ponto de recuperação por ano por *1 ano*

O Ponto de recuperação mais novo é definido para o dia, mês e ano atuais.

Neste exemplo, o ponto de recuperação mais antigo teria 1 ano, 4 meses e 6 dias.

3 Em Definições, no campo de texto **Número de rollups simultâneos**, insira um valor numérico.

Essa configuração determina o número de operações de rollup que podem ser realizadas ao mesmo tempo. Definir o número acima de 1 resultará em menos tempo para concluir o processo de rollup, mas colocará uma carga mais pesada no Core enquanto os rollups ocorrem.

> **NOTA:** Como regra geral, defina esse valor em 1. Se as operações de rollup demorarem muito, incremente em um dígito, e verifique o desempenho do sistema para garantir que a alteração é construtiva em seu ambiente.

4 Clique em **Aplicar**.

A política de retenção definida será aplicada durante o rollup noturno.

Também será possível aplicar essas definições ao especificar a política de retenção para qualquer máquina agente individual. Para obter mais informações sobre a definição de políticas de retenção para uma máquina agente, consulte Personalização das definições de política de retenção para um agente.

Personalização das definições de política de retenção para um agente

A política de retenção de uma máquina especifica por quanto tempo os pontos de recuperação são armazenados no repositório. Normalmente, cada agente usa a política de retenção padrão estabelecida para o core, a menos que você especifique uma política de retenção personalizada, conforme descrito neste procedimento.

Começando com a versão 5.4.1, o AppAssure 5 a capacidade de definir políticas de retenção discrepantes entre um agente e o core de origem e o agente replicado correspondente no core de destino.

Use este procedimento para definir uma política de retenção personalizada para um agente, incluindo um agente replicado.

> **NOTA:** Em atualizações de ambiente do AppAssure 5 versão 5.3.x para a versão 5.4.1 ou superior, se você quiser personalizar uma política de retenção para um agente replicado, primeiramente precisa atualizar os cores de origem e de destino 5.4.1 e, em seguida, realizar o trabalho de verificação de integridade em cada repositório no core de destino. A conclusão deste trabalho tende a levar um bom tempo, com base no tamanho de seu repositório e no sistema de armazenamento subjacente. Para obter mais informações sobre este trabalho, consulte Sobre o Trabalho de verificação da integridade do repositório. Para obter mais informações sobre como executar este trabalho, consulte Executando o trabalho de verificação de integridade em um repositório.

Essa tarefa também é uma das etapas do Processo de modificação das definições de nó de cluster.

Para personalizar as definições de política de retenção

1 No AppAssure 5 Core Console, navegue até a máquina que deseja modificar.

2 Clique na guia Configuração.

A página Definições é exibida.

3 No painel Trabalhos noturnos, clique em **Alterar**.

A caixa de diálogo Trabalhos noturnos é exibida.

4 Para especificar os intervalos de tempo a reter os dados de cópia de segurança, conforme necessário, selecione a opção **Rollup** e clique em **Definições**.

É exibida a caixa de diálogo Configuração da política de retenção.

5 Se você estiver personalizando as definições de políticas de retenção para um agente replicado e receber uma notificação de cautela para a verificação de integridade que está executando em seu repositório, prossiga com esta etapa. De outra forma, vá para Etapa 6.

a Se você está preparado para executar este trabalho, clique em **Verificar integridade**

b Clique em **Sim** para confirmar o trabalho de verificação de integridade.

CUIDADO: Esse processo pode levar um bom tempo, com base no tamanho de seu repositório. Durante este tempo, você não poderá realizar nenhuma outra ação (Snapshots, replicação, exportação virtual e assim por diante) no repositório. Para obter mais informações sobre este trabalho, consulte Sobre o Trabalho de verificação da integridade do repositório.

- Depois que o trabalho de Verificação da integridade concluir todos as sub-rotinas com sucesso, retorna para este procedimento e continua coma próxima etapa.

6 Na caixa de diálogo Configuração, realize um dos procedimentos a seguir:

- Para definir uma política de retenção personalizada para este agente, selecione a opção **Usar a política de retenção personalizada** e, em seguida, clique em **Salvar**. A política padrão é aplicada a este agente.
- Para definir uma política de retenção personalizada para este agente, selecione a opção **Usar a política de retenção personalizada** e, em seguida, continue na próxima etapa.

7 Insira a programação personalizada para reter os pontos de recuperação, conforme descrito na tabela a seguir.

Tabela 52.

Caixa de texto	Descrição
Manter todos os pontos de recuperação por *n* [*período de retenção*]	Especifica o período de retenção para os pontos de recuperação. Insira um número para representar o período de retenção e a seguir selecione o período de tempo. O padrão é *3* dias. Você pode selecionar dentre: Dias, Semanas, Meses e Anos
…e depois manter um Ponto de recuperação por hora por *n* [*período de retenção*]	Fornece um nível mais granular de retenção. Ele é usado como um bloco de construção com a definição principal para definir por quanto tempo os pontos de recuperação serão mantidos. Insira um número para representar o período de retenção e a seguir selecione o período de tempo. O padrão é *2 dias*. Você pode selecionar dentre: Dias, Semanas, Meses e Anos
…e depois manter um Ponto de recuperação por dia por *n* [*período de retenção*]	Fornece um nível mais granular de retenção. Ele é usado como um bloco de construção para definir por quanto tempo os pontos de recuperação serão mantidos. Insira um número para representar o período de retenção e a seguir selecione o período de tempo. O padrão é *4 dias*. Você pode selecionar dentre: Dias, Semanas, Meses e Anos
…e depois manter um Ponto de recuperação por semana por *n* [*período de retenção*]	Fornece um nível mais granular de retenção. Ele é usado como um bloco de construção para definir por quanto tempo os pontos de recuperação serão mantidos. Insira um número para representar o período de retenção e a seguir selecione o período de tempo. O padrão é *3 semanas*. Você pode selecionar dentre: Semanas, Meses e Anos
…e depois manter um Ponto de recuperação por mês por *n* [*período de retenção*]	Fornece um nível mais granular de retenção. Ele é usado como um bloco de construção para definir por quanto tempo os pontos de recuperação serão mantidos. Insira um número para representar o período de retenção e a seguir selecione o período de tempo. O padrão é *2 meses*. Você pode selecionar dentre: Meses e Anos
…e depois manter um Ponto de recuperação por ano por *n* [*período de retenção*]	Insira um número para representar o período de retenção e a seguir selecione o período de tempo. Você pode selecionar dentre: Anos

A caixa de texto Ponto de recuperação mais novo exibe o ponto de recuperação mais recente. O ponto de recuperação mais antigo será determinado pelas definições da política de retenção.

O seguinte é um exemplo de como o período de retenção é calculado.

Manter todos os pontos de recuperação por *3 dias*.

…e depois manter um Ponto de recuperação por hora por *3 dias*

…e depois manter um Ponto de recuperação por dia por *4 dias*

…e depois manter um Ponto de recuperação por semana por *3 semanas*

…e depois manter um Ponto de recuperação por mês por *2 meses*

…e depois manter um Ponto de recuperação por ano por *1 ano*

O Ponto de recuperação mais novo é definido para o dia, mês e ano atuais.

Neste exemplo, o ponto de recuperação mais antigo teria 1 ano, 4 meses e 6 dias.

8 Clique em **Salvar**.

Visualização das informações da licença

É possível visualizar informações atuais de status da licença do software AppAssure 5 Agent instalado em uma máquina.

Para visualizar informações da licença

1 No AppAssure 5 Core Console , navegue até a máquina que deseja visualizar.

2 Clique na guia Configuração e em **Aplicação de licença**.

Aparece a tela Status e apresenta os seguintes detalhes sobre a aplicação de licença do produto:

- Data de expiração
- Status da licença
- Tipo de licença
- Tipo de agente

Modificação das definições de transferência

No AppAssure 5, é possível modificar as definições para gerenciar os processos de transferência de dados para uma máquina protegida. As definições de transferência descritas nesta seção são no nível de agente. Para fazer transferências no nível de core, consulte Modificação das definições da fila de transferência.

O AppAssure 5 suporta o Windows 8 e o Windows Server 2012 para transferências normais, de base e incrementais, bem como para restauração, bare metal restore e exportação de máquina virtual.

Há três tipos de transferência no AppAssure 5:

- **Snapshot.** Faz a cópia de segurança de dados na sua máquina protegida. São possíveis dois tipos de snapshots: a imagem de base de todos os dados protegidos e um snapshot incremental de dados atualizados desde o último snapshot. Esse tipo de transferência cria pontos de recuperação que são armazenados no repositório associado ao Core. Para obter mais informações, consulte Gerenciamento de snapshots e pontos de recuperação.
- **Exportação de máquina virtual.** Cria uma máquina virtual (VM) a partir de um ponto de recuperação, contendo todos os dados da cópia de segurança da máquina protegida, bem como o sistema operacional e os drivers e dados associados para garantir que a VM seja inicializável. Para obter mais informações, consulte Sobre exportação de dados protegidos de máquinas com Windows para máquinas virtuais.
- **Restaurar**. Restaura as informações de cópia de segurança para uma máquina protegida. Para obter mais informações, consulte Restauração de volumes a partir de um ponto de recuperação.

NOTA: O volume inteiro é sempre regravado durante a restauração de sistemas Windows usando partições do sistema EFI.

A transferência de dados no AppAssure 5 envolve a transmissão de um volume de dados ao longo de uma rede a partir de máquinas do AppAssure 5 Agent para o Core. No caso de replicação, a transferência também ocorre do Core de origem ou fonte para o Core de destino.

A transferência de dados pode ser otimizada para seu sistema por meio de determinadas definições de opções de desempenho. Essas definições controlam o uso de largura de banda de dados durante o processo de cópia de segurança de máquinas agente, realizando exportação de VM ou uma restauração. Estes são alguns fatores que afetam o desempenho da transferência de dados:

- Número de transferências simultâneas de dados de agentes
- Número de fluxos simultâneos de dados
- Quantidade de alterações de dados no disco
- Largura de banda de rede disponível
- Desempenho do subsistema do disco do repositório
- Quantidade de memória disponível para armazenamento em buffer dos dados

É possível ajustar as opções de desempenho para melhor atender às suas necessidades de negócios e fazer o ajuste do desempenho com base em seu ambiente.

Para modificar as definições da transferência

1 No AppAssure 5 Core Console, navegue até a máquina que deseja modificar.

2 Clique na guia Configuração e em **Definições de transferência**.

As definições atuais de transferência são exibidas.

3 Na página Definições de transferência, clique em **Alterar**.

A caixa de diálogo Definições de transferência é exibida.

4 Insira as opções de Definições de transferência para a máquina, como descrito na tabela a seguir.

Tabela 53.

Caixa de texto	Descrição
Prioridade	Define a prioridade de transferência entre máquinas protegidas. Permite atribuir prioridade por comparação com outras máquinas protegidas. Selecione um número de 1 a 10, sendo 1 a maior prioridade. A definição padrão estabelece uma prioridade de 5. **NOTA:** A prioridade é aplicada às transferências que estão na fila.
Máximo de fluxos simultâneos	Define o número máximo de links TCP enviados para o Core para serem processados em paralelo por agente. **NOTA:** A Dell recomenda definir esse valor em 8. Se houver perda de pacotes, tente aumentar essa definição.
Máximo de gravações simultâneas	Define o número máximo de ações simultâneas de gravação em disco por conexão de agente. **NOTA:** A Dell recomenda defini-lo com o mesmo valor selecionado para Máximo de fluxos simultâneos. Se houver perda de pacotes, defina um valor ligeiramente mais baixo; por exemplo, se Máximo de fluxos simultâneos for 8, mude este para 7.
Usar o Número máximo de novas tentativas padrão do Core	Selecione essa opção para usar o número de tentativas padrão para cada máquina protegida, se algumas das operações não forem concluídas.

Tabela 53.

Caixa de texto	Descrição
Tamanho máximo do segmento	Especifica a maior quantidade de dados, em bytes, que um computador pode receber em um único segmento TCP. A definição padrão é 4194304. **CUIDADO: Não altere essa configuração padrão.**
Profundidade máxima da fila de transferência	Especifica a quantidade de comandos que podem ser enviados simultaneamente. É possível ajustá-la para um número maior se o seu sistema possuir um número elevado de operações simultâneas de entrada/saída.
Leituras pendentes por fluxo	Especifica quantas operações de leitura em fila serão armazenadas no back-end. Essa definição ajuda a controlar as filas de agentes. **NOTA:** A Dell recomenda definir esse valor em 24.
Gravadores excluídos	Selecione um gravador que deseja excluir. Como os gravadores que aparecem na lista são específicos para a máquina que você está configurando, você não verá todos os gravadores em sua lista. Por exemplo, alguns gravadores que você pode ver incluem: • Gravador ASR • Gravador COM+ REGDB • Gravador de contadores de desempenho • Gravador de registro • Gravador Shadow Copy Optimization • SQLServerWriter • Gravador de sistema • Gravador do programador de tarefas • Gravador de armazenamento de metadados VSS • Gravador WMI
Porta do server de dados de transferência	Define a porta para transferências. A definição padrão é 8009.
Tempo limite de transferência	Especifica em minutos e segundos o tempo a permitir que um pacote permaneça estático sem transferência.
Tempo limite de snapshot	Especifica em minutos e segundos o tempo máximo a aguardar para tirar um snapshot.
Tempo limite de leitura da rede	Especifica em minutos e segundos o tempo máximo a aguardar por uma conexão de leitura. Se a leitura de rede não puder ser realizada naquele tempo, a operação será tentada novamente.
Tempo limite de gravação da rede	Especifica o tempo máximo em segundos a aguardar por uma conexão de gravação. Se a gravação de rede não puder ser realizada naquele tempo, a operação será tentada novamente.

5 Clique em **OK**.

Visualização do diagnóstico do sistema

No AppAssure 5, as informações de diagnóstico estão disponíveis para que você visualize os dados do log da máquina de qualquer máquina protegida. Além disso, é possível visualizar e carregar informações de diagnóstico do Core. Para obter mais informações sobre como visualizar os logs da máquina, consulte Visualização de logs da máquina e, quanto ao carregamento de logs, consulte Carregamento de logs de máquina.

Visualização de logs da máquina

Se você encontrar quaisquer erros ou problemas com a máquina, poderá ser útil visualizar os logs.

Para visualizar os logs de máquina no Core Console

1. Navegue até o AppAssure 5 Core Console.
2. Clique na guia Ferramentas e em **Diagnóstico**.
3. Clique em **Visualizar log**.

   Aparecerá a caixa de diálogo Baixar do log do Core.
4. Selecione **Clique aqui para começar o download**.

   Aparecerá uma mensagem para alertá-lo sobre o arquivo que você está baixando e se deseja abri-lo ou salvá-lo.
5. Escolha seu método preferido para manipular o arquivo de log.

Para visualizar os logs de máquina em uma máquina protegida

1. Navegue até o AppAssure 5 Core Console e selecione a máquina da qual deseja visualizar os dados do log.
2. Clique na guia Ferramentas e em **Diagnóstico**.
3. Clique em **Visualizar log**.

Carregamento de logs de máquina

Execute as etapas do procedimento a seguir para carregar os logs de máquina.

Para carregar os logs de máquina

1. Navegue até o AppAssure 5 Core Console.
2. Clique na guia Ferramentas e em **Diagnóstico**.
3. Clique em **Carregar log**.

   Aparecerá a caixa de diálogo Carregar o log do Core.
4. Selecione **Clique aqui para começar a carregar**.

   A guia Eventos exibe para visualização o progresso do carregamento de informações de log do core e todas as máquinas protegidas.

Gerenciamento das definições de trabalho do Core

Os trabalhos do Core são criados automaticamente quando você inicia operações, como replicação. A seção Definições de trabalho da guia Configuração permite determinar as definições para cada trabalho, incluindo o número de trabalhos que devem ocorrer de uma vez e quantas vezes um trabalho deve ser tentado, caso um erro de rede ou outro erro de comunicação impeça que o trabalho seja bem-sucedido de início.

Edição das definições de trabalho do Core

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

Para editar as definições de trabalho do core

1 No AppAssure 5 Core Console, realize um dos procedimentos a seguir:

- Clique na guia Configuração e em **Definições de trabalho**.
- No menu suspenso, clique na guia Configuração e em **Definições de trabalho**.

2 Na página Definições de trabalho, clique em **Editar** no trabalho cujas definições você deseja alterar.

3 A janela Definições de trabalho [NomedoTrabalho] é aberta.

4 Use as setas para cima e para baixo para definir o número das seguintes opções:

- Máximo de trabalhos simultâneos
- Contagem de tentativas

5 Clique em **Salvar**.

Adição de trabalhos ao Core

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

Para adicionar trabalhos ao core

1 No AppAssure 5 Core Console, realize um dos procedimentos a seguir:

- Clique na guia Configuração e em **Definições de trabalho**.
- No menu suspenso, clique na guia Configuração e em **Definições de trabalho**.

2 Na página Definições de trabalho, clique em **Adicionar**.

Aparecerá a janela Definições de trabalho.

3 Na janela Definições de trabalho, insira as informações descritas na tabela a seguir.

Tabela 54.

Opção	Descrição
Trabalho	Use a lista suspensa para selecionar um dos seguintes trabalhos: • AdHocDeleteRecoveryPointsJob • AutoUpdateJob • BackupJob • BootCdBuilderJob • CheckAgentRecoveryPointsJob • ChecksumCheckJob • CollectDiagnosticInfoJob • DeleteAgentJob • DeleteAllRecveryPointsJob • DeleteAllRecoveryPointsJob • DeleteRecoveryPointsChainJob • DeleteVolumeImagesJob • DownloadExchangeDllsJob • DownloadFromCloudJob • ExportJob • ImportJob • IndexFileDeleteJob • LocalMountRecoveryPointJob • MaintainRepositoryJob • MountabilityCheckJob • NightlyAttachabilityJob • PersistDedupeCacheJob • PushInstallJob • RecoveryPointAttachabilityJob • RollbackJob • RollupJob • UploadCoreLogsJob • UploadExchangeDllsJob • UploadToCloudJob
Máx. de trabalhos simultâneos	Insira o número máximo de trabalhos que devem operar de uma só vez. **NOTA:** O número máximo de trabalhos permitido é de 50. O mínimo é um.
Contagem de tentativas	Insira o número de vezes que o Core deve tentar executar com êxito o trabalho.

4 Clique em **Salvar**.

Implementação de um agente (instalação de envio por push)

O AppAssure 5 permite implementar o AppAssure 5 Agent Installer em máquinas Windows individuais para proteção. Execute as etapas do procedimento a seguir para enviar por push o instalador para um agente.

Para implementar agentes em várias máquinas ao mesmo tempo, consulte Implementação em várias máquinas.

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

Para implementar um agente

1 No AppAssure 5 Core Console, na área de navegação à esquerda, clique em Máquinas protegidas para abrir a página Máquinas.

2 No menu suspenso **Ações**, clique em **Implementar Agent**.

A caixa de diálogo Implementar Agent é exibida.

3 Na caixa de diálogo Implementar Agent, insira as definições de login, como descrito na tabela a seguir.

Tabela 55.

Caixa de texto	Descrição
Máquina	Insira o nome de host ou o endereço IP da máquina agente que deseja implementar.
Nome de usuário	Insira o nome de usuário para se conectar a essa máquina; por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
Senha	Insira a senha para se conectar a essa máquina
Reinício automático após a instalação	Selecione para especificar se o Core deve iniciar após a conclusão da implementação e instalação do AppAssure 5 Agent Installer.

4 Clique em **Confirmar** para validar as credenciais inseridas.

A caixa de diálogo Implementar Agent exibe uma mensagem para indicar que a validação está sendo realizada. Clique em **Abortar** se quiser cancelar o processo de confirmação. Após a conclusão do processo de confirmação, será exibida uma mensagem indicando que a confirmação foi concluída.

5 Clique em **Implementar**.

É exibida uma mensagem indicando que a implementação foi iniciada. É possível visualizar o progresso na guia Eventos. Clique em **Exibir detalhes** para visualizar mais informações sobre o status da implementação do agente.

6 Clique em **OK**.

Gerenciamento de máquinas

Esta seção descreve uma variedade de tarefas que podem ser realizadas no gerenciamento de suas máquinas, como remover uma máquina do seu ambiente do AppAssure, definir uma replicação, forçar o truncamento de log, cancelar operações, e muito mais.

Remoção de uma máquina

Execute as etapas do procedimento a seguir para remover uma máquina da proteção no seu ambiente do AppAssure.

Para remover uma máquina

1 No AppAssure 5 Core Console, navegue até a máquina que deseja remover.

2 No menu suspenso **Ações**, clique em **Remover máquinas** e depois selecione uma das opções descritas na tabela a seguir.

Tabela 56.

Opção	Descrição
Manter pontos de recuperação	Mantém todos os pontos de recuperação atualmente armazenados desta máquina.
Remover pontos de recuperação	Remove do repositório todos os pontos de recuperação atualmente armazenados desta máquina.

Cancelamento de operações em uma máquina

É possível cancelar operações atualmente em execução em uma máquina. Você pode especificar o cancelamento de apenas um snapshot atual ou cancelar todas as operações atuais, incluindo exportações, replicações, e assim por diante.

Para cancelar operações em uma máquina

1 No AppAssure 5 Core Console, navegue até a máquina da qual deseja cancelar operações.

2 Clique na guia Eventos.

3 Expanda os detalhes de evento referentes ao evento ou operação que deseja cancelar.

4 Clique em **Cancelar**.

Visualização do status da máquina e outros detalhes

Execute a etapa deste procedimento para visualizar o status e outros detalhes de uma máquina.

Para visualizar o status da máquina e outros detalhes

- No AppAssure 5 Core Console, navegue até a máquina protegida que deseja visualizar.

  As informações sobre a máquina são exibidas na guia Resumo. Os detalhes exibidos incluem:

  - Nome do host
  - Último snapshot tirado
  - Próximo snapshot programado
  - Status da criptografia
  - Número da versão

  Se o Exchange Server estiver instalado na máquina, informações detalhadas sobre o server também serão exibidas, incluindo:

  - Última verificação de capacidade de montagem bem-sucedida realizada
  - Última verificação de soma de verificação bem-sucedida realizada
  - Último truncamento de log realizado

As informações dos detalhes sobre os volumes contidos nessa máquina também são exibidas e incluem:

- Nome
- Tipo de sistema de arquivos
- Uso de espaço
- Programação
- Programação atual
- Próximo snapshot
- Tamanho total

Se o SQL Server estiver instalado na máquina, informações detalhadas sobre o server também serão exibidas, incluindo:

- Status online
- Nome
- Caminho de instalação
- Versão

Se o Exchange Server estiver instalado na máquina, informações detalhadas sobre o server e os armazenamentos de e-mail também serão exibidas, incluindo:

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

Gerenciamento de várias máquinas

Este tópico descreve as tarefas que os administradores realizam para implementar o software AppAssure 5 Agent simultaneamente em várias máquinas com Windows.

Para implementar e proteger vários agentes, realize as seguintes tarefas:

1 Implementar o AppAssure 5 em várias máquinas. Consulte Implementação em várias máquinas.

2 Monitorar a atividade de implementação em lote. Consulte Confirmação da implementação em várias máquinas.

3 Proteger várias máquinas. Consulte Proteção de várias máquinas.

> **NOTA:** Essa etapa pode ser ignorada se você tiver selecionado a opção **Proteger máquina após instalação** durante a implementação.

4 Monitorar a atividade de proteção em lote. Consulte Monitoramento da proteção de várias máquinas.

Implementação em várias máquinas

É possível simplificar a tarefa de implementar o software AppAssure 5 Agent em várias máquinas com Windows usando o recurso de implementação em massa do Dell AppAssure 5. Do Core Console, é possível especificamente implementar em massa em:

- Máquinas em um domínio Active Directory
- Máquinas em um host virtual VMware vCenter/ESX(i)
- Máquinas em qualquer outro host

O recurso de implementação em massa detecta automaticamente as máquinas em um host e permite selecionar aqueles nas quais deseja implementar. Como alternativa, é possível inserir manualmente as informações de host e máquina.

NOTA: É possível usar o recurso de implementação em massa para implementar o software do Agent em até 50 máquinas agente. As máquinas nas quais você está implementando devem ter acesso à Internet para baixar e instalar bits, visto que o AppAssure 5 usa a versão para Web do AppAssure 5 Agent Installer para implementar os componentes de instalação. Se não estiver disponível o acesso à Internet, será preciso baixar manualmente o AppAssure 5 Agent Installer a partir do Portal de licenças de software da Dell e implementar o instalador nas máquinas.

Para obter mais informações, consulte o *Guia do usuário do portal de licenças*, localizado no site de documentação de Guias e notas de versão do AppAssure em https://support.software.dell.com/appassure/release-notes-guides.

Implementação em máquinas em um domínio Active Directory

Antes de iniciar este procedimento, é preciso ter as informações de domínio e credenciais de login para o server Active Directory.

Para implementar em várias máquinas em um domínio Active Directory

1. No AppAssure 5 Core Console , clique na guia Ferramentas e depois em **Implementação em massa**.
2. Na janela Implementar Agent nas máquinas, clique em **Active Directory**.
3. Na caixa de diálogo Conectar-se ao Active Directory, insira as informações de domínio e credenciais de login, conforme descrito na tabela a seguir.

   Tabela 57.

Caixa de texto	Descrição
Domínio	O nome de host ou endereço IP do domínio Active Directory.
Nome de usuário	O nome de usuário utilizado para se conectar ao domínio, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
Senha	A senha usada para se conectar ao domínio.

4. Clique em **Conectar.**
5. Na caixa de diálogo Adicionar máquinas do Active Directory, selecione as máquinas às quais deseja implementar o AppAssure 5 Agent e clique em **Adicionar**.

   As máquinas adicionadas são exibidas na janela Implementar Agent nas máquinas. O sistema confirma todas as máquinas que você adicionou automaticamente.
6. Como opção, você pode confirmar qualquer máquina selecionando-a e depois clicando em **Confirmar** na barra de ferramentas.

7 Verifique o ícone e a mensagem de status de cada máquina na página Implementar Agents em máquinas. Eles refletem a preparação de cada máquina para implementação, como segue:

- Ícone verde - o AppAssure 5 pode se conectar à máquina e está pronto para ser implementado.
- Ícone amarelo - o AppAssure 5 pode se conectar à máquina; contudo, o AppAssure 5 Agent na máquina já está pareado com um AppAssure 5 Core.
- Ícone vermelho - o AppAssure 5 não pode se conectar à máquina. Isso talvez ocorra porque as credenciais de login estão incorretas, a máquina está desligada, o firewall está bloqueando o tráfego, ou outro problema.

  NOTA: O software Agent não será implementado em nenhuma máquina com um ícone de status vermelho.

- Se a mensagem de status de cada máquina indicar que ela está pronta para implementação, vá para a Etapa 9.
- Como opção, se a mensagem de status mostrar um link Detalhes, clique em **Detalhes** para determinar se consegue corrigir o problema.

8 Para corrigir problemas relacionados a qualquer máquina que mostre um status vermelho, ou para habilitar a proteção automática, alterar as informações de porta ou autenticação, alterar o nome de exibição, especificar um repositório ou estabelecer uma chave de criptografia, clique em **Definições** na barra de ferramentas ou no link **Editar** ao lado da máquina e depois faça o seguinte:

a Na caixa de diálogo Editar definições, especifique as definições, como descrito na tabela a seguir.

Tabela 58.

Caixa de texto	Descrição
Nome do host	Fornecido automaticamente da Etapa 3.
Nome de usuário	*Fornecido automaticamente da* Etapa 3.
Senha	*Insira a senha da máquina.*
Reinício automático após a instalação	Obrigatória. Reinicia a máquina após a implementação, o que é necessário antes de proteger qualquer máquina agente.
Proteger máquina após instalação	Selecionado por padrão. Se estiver selecionado, o sistema protegerá a máquina automaticamente após a implementação. (Isso permite ignorar Proteção de várias máquinas.)
Nome de exibição	Atribuído automaticamente com base no nome de host fornecido na Etapa 3. Esse é o nome que aparece no Core Console da máquina selecionada.
Port	O número da porta pela qual o AppAssure 5 Core se comunica com o agente na máquina. A porta padrão é 8006.
Repositório	Use a lista suspensa para selecionar o repositório no AppAssure 5 Core no qual os dados das máquinas especificadas devem ser armazenados. Essa opção está disponível apenas quando você seleciona **Proteger máquina após instalação**.
Chave de criptografia	(Opcional) Use a lista suspensa para especificar se a criptografia deve ser aplicada aos dados na máquina especificada. A chave de criptografia é atribuída a todas as máquinas que estão sendo protegidas. **NOTA:** Essa opção está disponível apenas quando você seleciona **Proteger máquina após instalação**.

b Clique em **Salvar**.

9 Após as máquinas serem confirmadas com êxito, selecione cada máquina para a qual deseja implementar o AppAssure 5 Agent e clique em **Implementar**.

Se você prosseguiu com a proteção de um agente que já está protegido por outro Core, a proteção será interrompida e a máquina agora será protegida por este Core.

Se for escolhida a opção **Proteger máquina após instalação**, após a implementação bem-sucedida, as máquinas serão reiniciadas automaticamente e a proteção será ativada.

Implementação em máquinas em um host virtual VMware vCenter/ESX(i)

Antes de iniciar este procedimento, é preciso ter as informações de localização do host e credenciais de login do host virtual VMware vCenter/ESX(i).

NOTA: Todas as máquinas virtuais devem ter Ferramentas de VM instaladas; caso contrário, o AppAssure 5 não consegue detectar o nome do host da máquina virtual na qual implementar. Em vez do nome do host, o AppAssure 5 usa o nome da máquina virtual, o que pode causar problemas se o nome do host for diferente do nome da máquina virtual.

Para implementar em várias máquinas em um host virtual vCenter/ESX(i)

1 Navegue até o AppAssure 5 Core Console, clique na guia Ferramentas e depois em **Implementação em massa**.

2 Na janela Implementar Agent nas máquinas, clique em **vCenter/ESX(i)**.

3 Na caixa de diálogo Conectar-se ao vCenter Server/ESX(i), insira as informações de host e credenciais de login, conforme descrito a seguir, e clique em **Conectar**.

Tabela 59.

Caixa de texto	Descrição
Host	O nome ou endereço IP do host virtual VMware vCenter Server/ESX(i).
Port	A porta usada para se conectar ao host virtual. A definição padrão é 443.
Nome de usuário	O nome de usuário utilizado para se conectar ao host virtual; por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
Senha	A senha usada para se conectar ao host virtual.

4 Na caixa de diálogo Adicionar máquinas do VMware vCenter Server/ESX(i), faça o seguinte:

   a Em Opções, insira o nome de usuário e senha das máquinas virtuais selecionadas.

   b Explore as máquinas, expandindo ou recolhendo os clusters, conjuntos de recursos, vApps e máquinas virtuais, por meio de cliques nas setas ao lado de cada nó.

   c Selecione as máquinas às quais deseja implementar e clique em **Adicionar**.

   As máquinas adicionadas são exibidas na janela Implementar Agent nas máquinas. O sistema confirma todas as máquinas que você adicionou automaticamente.

5 Como opção, você pode confirmar qualquer máquina, o status da máquina ou editar as definições de conexão dela, como descrito na Etapa 6 à Etapa 8 do procedimento Implementação em máquinas em um domínio Active Directory.

6 Após as máquinas serem confirmadas com êxito, marque a caixa ao lado de cada máquina para a qual deseja implementar o AppAssure 5 Agent e clique em **Implementar**.

   Se você prosseguiu com a proteção de um agente que já está protegido por outro Core, a proteção será interrompida e a máquina agora será protegida por este Core.

   Se for escolhida a opção **Proteger máquina após instalação**, após a implementação bem-sucedida, as máquinas serão reiniciadas automaticamente e a proteção será ativada.

Implementação em máquinas em qualquer outro host

Para implementar em várias máquinas em qualquer outro host

1. Navegue até o AppAssure 5 Core Console, clique na guia Ferramentas e depois em **Implementação em massa**.
2. Na janela Implementar Agent nas máquinas, realize um dos procedimentos a seguir:
   - Clique em **Novo** para inserir um novo host de máquina, credenciais de login, nome de exibição opcional, repositório, chave de criptografia e outras informações. Para obter detalhes de cada definição, consulte Implementação em máquinas em um domínio Active Directory.

     Após inserir essas informações, clique em **OK** para adicioná-las à lista Implementar Agent nas máquinas ou clique em **OK e Novo** para adicionar outra máquina.

     > **NOTA:** Se você quiser proteger automaticamente a máquina após a implementação, marque a caixa **Proteger máquina após instalação**. Se você marcar a caixa, a máquina será reiniciada automaticamente antes de ativar a proteção.

   - Para especificar várias máquinas em uma lista, clique em **Manualmente**, insira os detalhes da máquina na caixa de diálogo Adicionar máquinas manualmente e clique em **Adicionar**. Para cada máquina, será preciso inserir o endereço IP ou nome da máquina, o nome de usuário, a senha separada por um delimitador de dois-pontos duplo e a porta, como mostrado no seguinte formato:

     ```
     host :: login :: senha :: porta
     ```

     Por exemplo:

     ```
     10.255.255.255::administrator::&11@yYz90z::8006
     ```

     ```
     abc-host-00-1::administrator::99!zU$o83r::168
     ```

   As máquinas adicionadas são exibidas na janela Implementar Agent nas máquinas. O sistema confirma todas as máquinas que você adicionou automaticamente.
3. Como opção, você pode confirmar qualquer máquina, o status da máquina ou editar as definições de conexão dela, como descrito na Etapa 6 à Etapa 8 do procedimento Implementação em máquinas em um domínio Active Directory.
4. Após as máquinas serem confirmadas com êxito, marque a caixa ao lado de cada máquina para a qual deseja implementar o AppAssure 5 Agent e clique em **Implementar**.

   Se você prosseguiu com a proteção de um agente que já está protegido por outro Core, a proteção será interrompida e a máquina agora será protegida por este Core.

   Se for escolhida a opção **Proteger máquina após instalação**, após a implementação bem-sucedida, as máquinas serão reiniciadas automaticamente e a proteção será ativada.

Confirmação da implementação em várias máquinas

Depois de fazer a implementação em massa do software AppAssure 5 Agent em duas ou mais máquinas, poderá confirmar o êxito visualizando cada máquina agente relacionada no menu Máquinas protegidas.

Também é possível visualizar informações sobre o processo de implementação em massa na guia Eventos. Execute as etapas deste procedimento para confirmar a implementação.

Para confirmar a implementação em várias máquinas

1. Navegue até o AppAssure 5 Core Console, clique na guia Eventos e em **Alertas**.
2. Navegue até a guia Início do AppAssure 5 Core e clique na guia **Eventos**.

   Aparecem eventos de alerta na lista, mostrando a hora que o evento iniciou e uma mensagem. Para cada implementação bem-sucedida do software Agent, você verá um alerta indicando que a máquina protegida foi adicionada.

3 Como opção, clique em qualquer link de uma máquina protegida.

A guia Resumo da máquina selecionada é exibida, mostrando informações pertinentes, incluindo:

- O nome de host da máquina protegida
- O último snapshot, se aplicável
- O horário programado do próximo snapshot, com base na programação de proteção selecionada
- A chave de criptografia, se houver, utilizada para esse agente protegido.
- A versão do software Agent.

Proteção de várias máquinas

É possível adicionar simultaneamente duas ou mais máquinas do Windows para proteção no AppAssure 5 Core usando o Assistente de proteção de diversas máquinas. Esse recurso é chamado de proteção em massa.

Tal como acontece com a proteção de máquinas agente individuais, a proteção em massas exige que o software AppAssure 5 Agent seja instalado em cada máquina que você deseja proteger e que a máquina seja reiniciada após a instalação do software Agent. Há mais de um método de implementar o software Agent em várias máquinas simultaneamente. Por exemplo:

- É possível instalar o software Agent em diversas máquinas usando o recurso de implementação em massa, acessado na guia Ferramentas. (Se você tiver selecionado **Proteger máquina após instalação** quando implementou o Agent, poderá ignorar este procedimento.) Para obter mais informações sobre o uso de implementação em massa, consulte Implementação em várias máquinas.
- É possível implementar o software Agent como parte desse assistente.

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

O fluxo de trabalho do Assistente de proteção de diversas máquinas pode ser ligeiramente diferente com base no seu ambiente. Por exemplo, se o software Agent estiver instalado nas máquinas que você deseja proteger, não será solicitada a instalação dele a partir do assistente. De forma semelhante, se um repositório já existir no Core, você não será solicitado a criar outro.

Esse processo inclui etapas opcionais que podem ser acessadas se você selecionar uma configuração avançada. Isso inclui funções de repositório (é possível especificar um repositório existente do AppAssure 5 para salvar snapshots ou criar um novo). Também é possível adicionar criptografia aos dados salvos no Core dessa máquina.

Para proteger várias máquinas

1 Se o software AppAssure 5 Agent já estiver instalado nas máquinas que deseja proteger, mas elas ainda não foram reiniciadas, faça isso agora.

2 Na máquina do Core, navegue até o AppAssure 5 Core Console, clique no menu suspenso ao lado do ícone Proteger e selecione **Proteção em massa**.

Aparece o Assistente de proteção de diversas máquinas.

3 Na página Bem-Vindo, selecione as opções de instalação apropriadas:

- Se não for preciso definir um repositório ou estabelecer a criptografia, selecione **Típico**.
- Se você precisar criar um repositório ou definir um repositório diferente para cópias de segurança das máquinas selecionadas, ou ainda se desejar estabelecer a criptografia usando o assistente, selecione **Avançado (exibir etapas opcionais)**.
- Como opção, se você não quiser ver a página Bem-Vindo do Assistente de proteção de máquina no futuro, selecione a opção **Ignorar a página Bem-Vindo na próxima vez que o assistente for aberto**.

4 Quando estiver satisfeito com suas seleções na página Bem-Vindo, clique em **Avançar**.

A página Conexão é exibida.

5 Selecione o método adequado para identificar as máquinas que você deseja adicionar para a proteção.

As máquinas devem estar operando e acessíveis para conexão a elas. Para obter uma conexão bem-sucedida utilizando o Active Directory, a proteção em massa e a implementação em massa devem ser mais bem-sucedidas se conectadas nas máquinas como o administrador do domínio.

- Para identificar as máquinas que deseja proteger em um domínio Active Directory, selecione **Conectar-se ao Active Directory**, insira as credenciais, como descrito na tabela a seguir, e clique em **Avançar**. Vá para a Etapa 7.
- Para identificar as máquinas que deseja proteger em um host virtual VMware vCenter/ESX(i), selecione **Conectar-se ao vCenter/ESX(i)**, insira as credenciais, como descrito na tabela a seguir, e clique em **Avançar**. Vá para a Etapa 7.

Tabela 60.

Caixa de texto	Descrição
Host	O nome de host ou endereço IP do domínio Active Directory ou do host virtual VMware vCenter Server/ESX(i).
Nome de usuário	O nome de usuário utilizado para se conectar ao domínio; por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
Senha	A senha usada para se conectar ao domínio.

NOTA: Todas as máquinas virtuais devem ter Ferramentas de VM instaladas. Caso contrário, o AppAssure 5 não consegue detectar o nome do host da máquina virtual na qual implementar o software do Agent, e não poderá protegê-la. Em vez do nome do host, o AppAssure 5 usa o nome da máquina virtual, o que pode causar problemas se o nome do host for diferente do nome da máquina virtual.

- Para adicionar as máquinas manualmente, selecione **Adicionar as máquinas manualmente** e clique em **Avançar**.

Aparece a página Máquinas.

6 Na página Máquinas, para especificar as máquinas manualmente, digite os detalhes da conexão de cada máquina em uma linha separada e depois clique em **Avançar**. Utilize o seguinte formato:

```
host :: login :: senha :: porta
```

NOTA: O parâmetro da porta é opcional. Se omitido, será utilizada a porta 8006 por padrão. Se você desejar especificar uma porta diferente da 8006, então é necessário incluir esse parâmetro.

7 Na página Máquinas, para especificar as máquinas identificadas de um domínio Active Directory ou de um host virtual VMware vCenter/ESX(i), selecione na lista cada máquina apropriada que deseja proteger. Certifique-se de que desmarcou a opção da caixa de seleção para qualquer máquina que você não deseja proteger nesse momento. Quando estiver satisfeito, clique em **Avançar**.

O sistema confirma todas as máquinas que você adicionou automaticamente.

8 Se a página Proteção for exibida em seguida no Assistente de proteção de diversas máquinas, vá para a Etapa 12.

Se o software Agent ainda não tiver sido implementado nas máquinas que você deseja proteger ou se alguma das máquinas especificadas não puder ser protegida por outro motivo, as máquinas selecionadas aparecerão na página Avisos de máquinas. O sistema confirma todas as máquinas que você adicionou automaticamente.

9 Como opção, na página Avisos de máquinas, você pode confirmar qualquer máquina selecionando-a e depois clicando em **Confirmar** na barra de ferramentas.

10 Como opção, na página Avisos de máquinas, selecione **Após a instalação do Agent, reiniciar as máquinas automaticamente**.

NOTA: A Dell recomenda essa opção. Reinicie as máquinas agente antes de protegê-las.

11 Se o status indicar que a máquina está acessível, clique em **Avançar** para instalar o software Agent.

A página Proteção é exibida.

12 Na página Proteção, selecione a programação de proteção adequada, como descrito a seguir.

- Se desejar usar a programação de proteção padrão, na opção Definições de programação, selecione **Proteção padrão (snapshots horários de todos os volumes)**.
- Se desejar definir uma programação de proteção diferente, na opção Definições de programação, selecione **Proteção personalizada** e clique em **Avançar**.

13 Prossiga com a configuração da seguinte maneira:

- Se a configuração Típico tiver sido selecionada para o Assistente de proteção de diversas máquinas, além da proteção padrão, clique em **Concluir** para confirmar suas escolhas, fechar o assistente e proteger a máquina especificada.
- Se a configuração Típico para o Assistente de proteção de diversas máquinas e a proteção personalizada específica tiverem sido selecionadas, na página Proteção, clique em **Avançar**, e na página Programação de proteção, defina uma programação personalizada conforme descrito no tópico Criação de programações de proteção personalizadas, e clique em **Concluir** para confirmar suas escolhas, feche o assistente e proteja as máquinas especificadas.
- Se a configuração Avançado tiver sido selecionada para o Assistente de proteção de máquina, clique em **Avançar** e vá para a Etapa 14 a fim de ver as opções de repositório e criptografia.

14 Na página Repositório, se você deseja armazenar os dados de todas as máquinas especificadas para proteção em um repositório existente, selecione **Utilize um repositório existente**, selecione o repositório apropriado na lista e clique em **Avançar** e prossiga para Etapa 19.

Se você deseja criar um novo local de armazenamento no Core, faça o seguinte:

a Selecione **Criar um repositório**.

b Na página Repositório, no campo **Nome**, especifique o nome do repositório que deseja criar.

Em geral é a palavra Repositório e um número de índice, que corresponde ao número do novo repositório (por exemplo, **Repository1**). Você pode alterar o nome conforme necessário. Você pode inserir até 40 caracteres. Esse nome precisa ser exclusivo desse core.

NOTA: Ao especificar o nome do repositório, use somente caracteres alfanuméricos ou o hífen. Nenhum outro símbolo ou caractere de pontuação é permitido. Não use combinações de letras que especificam comandos ou palavras reservadas (como con, prn, aux ou nul) ou que representam portas (como com ou lpt).

c No campo **Local**, insira um caminho de diretório para o repositório. Por exemplo, em um computador local, digite **C:\Repository**. Esse local precisa ser exclusivo desse core. Se você estiver armazenando o repositório em uma unidade compartilhada, insira no formato \\servidor\compartilhamento.

CUIDADO: Se você excluir o repositório no futuro, o programa Instalador removerá todo o conteúdo do caminho do repositório. Por esse motivo, não crie o local de armazenamento na raiz (por exemplo, c:\), o que pode resultar na perda de todos os dados armazenados no volume.

d Se o repositório for armazenado em um volume compartilhado, no campo **Nome de usuário**, insira o nome de usuário com privilégios para acessar a unidade compartilhada e, no campo **Senha**, insira a senha desse usuário.

e No campo **Caminho de metadados**, insira o caminho onde deseja que os metadados sejam armazenados. Esse deve ser um subdiretório do local de armazenamento. Por exemplo, se o local de armazenamento for C:\Repository, digite **C:\Repository\Metadata**. Esse precisa ser um caminho exclusivo desse core.

15 Depois de inserir todos os dados necessários na página Repositório, clique em **Avançar** .

A página Configuração do repositório é exibida.

16 Especifique o tamanho do repositório.

NOTA: Se o local de armazenamento for um volume NTFS (Sistema de arquivos de nova tecnologia) usando o Windows XP ou Windows 7, o limite de tamanho do arquivo é 16 TB.

Se o local de armazenamento for um volume NTFS usando o Windows 8, Windows 8.1 ou Windows Server 2012, 2012 R2, o limite de tamanho do arquivo é 256 TB.

Para que o AppAssure 5 valide o sistema operacional, o Windows Management Instrumentation (WMI) deve ser instalado no local de armazenamento pretendido.

17 Para especificar bytes por setor, bytes por registro ou controlar a política de cache de gravação, selecione **Exibir opções avançadas** e, em seguida, insira os detalhes do local de armazenamento, como descrito na tabela a seguir.

Tabela 61.

Caixa de texto	Descrição
Bytes por setor	Especifique o número de bytes que você deseja incluir em cada setor. O valor padrão é *512*.
Bytes por registro	Especifique a média de bytes por registro. O valor padrão é *8192*.
Política de cache de gravação	A política de cache de gravação controla como o Gerenciador de cache do Windows é usado no repositório e ajuda a ajustar o repositório para que o melhor desempenho seja obtido com diferentes configurações. Defina o valor para um dos seguintes: • Ligado • Desligado • Sincronizar Se definido como *Ligado*, que é o padrão, o Windows controla o armazenamento em cache. **NOTA:** Definir a política de cache de gravação como *Ligado* pode resultar em desempenho mais rápido. Se você estiver usando uma versão do Windows Server anterior à Server 2012, a definição recomendada é *Desligado*. Se definido como *Desligado*, o AppAssure 5 controla o armazenamento em cache. Se definido como *Sincronizar*, o Windows controla o armazenamento em cache, além da entrada/saída síncrona.

18 Quando estiver satisfeito com as informações de configuração do repositório inseridas, clique em **Avançar**.

A página Criptografia é exibida.

19 Como opção, para habilitar a criptografia, na página Criptografia, selecione **Habilitar criptografia**.

O campo Chave de criptografia é exibido na página Criptografia.

NOTA: Se você habilitar a criptografia, ela será aplicada a dados de todos os volumes protegidos das máquinas especificadas para proteção. É possível alterar as definições mais tarde na guia Configuração no AppAssure 5 Core Console. Para obter mais informações sobre criptografia, consulte Gerenciamento da segurança.

CUIDADO: O AppAssure 5 usa a criptografia AES de 256 bits no modo Cipher Block Chaining (CBC) com chaves de 256 bits. Embora o uso de criptografia seja opcional, a Dell recomenda fortemente que você estabeleça uma chave de criptografia e que proteja a frase de acesso definida. Armazene a frase de acesso em um local seguro, pois ela é essencial para a recuperação dos dados. Sem a frase de acesso, não é possível executar a recuperação dos dados.

20 Insira as informações conforme descrito na tabela a seguir para adicionar uma chave de criptografia para o Core.

Tabela 62.

Caixa de texto	Descrição
Nome	Insira um nome para a chave de criptografia.
Descrição	Insira uma descrição para fornecer detalhes adicionais da chave de criptografia.
Frase de acesso	Insira a frase de acesso usada para controlar o acesso.
Confirmar frase de acesso	Insira novamente a frase de acesso que você acabou de inserir.

21 Clique em **Concluir** para salvar e aplicar suas definições.

O assistente é fechado. O software do agente é implementado nas máquinas especificadas, se necessário, e as máquinas são adicionadas à proteção no Core.

Monitoramento da proteção de várias máquinas

É possível monitorar o progresso à medida que o AppAssure 5 aplica as programações e políticas de proteção às máquinas.

Para monitorar a proteção de várias máquinas

- No AppAssure 5 Core Console, navegue até a guia AppAssure 5 **Início** e clique na guia **Eventos**.

  A guia Eventos é exibida, dividida em Tarefas, Alertas e Eventos. À medida que os volumes são transferidos, o status e as horas inicial e final são exibidos no painel Tarefas.

  Também é possível filtrar as tarefas por status (ativa, em espera, concluída e com falha). Para obter mais informações, consulte Visualização de tarefas.

  NOTA: Para ver apenas as tarefas que estão esperando para serem realizadas, certifique-se de selecionar o ícone Tarefas em espera.

  À medida que cada máquina protegida é adicionada, um alerta é registrado no log, relacionando se a operação foi bem-sucedida ou se foram registrados erros no log. Para obter mais informações, consulte Visualização de alertas.

  Para obter informações sobre visualização de todos os eventos, consulte Visualização de todos os eventos.

Gerenciamento de snapshots e pontos de recuperação

Um ponto de recuperação é uma coleção de snapshots tirados de volumes de disco individuais e armazenados no repositório. Os snapshots capturam e armazenam o estado de um volume de disco em determinado momento, enquanto os aplicativos que geram os dados ainda estão em uso. No AppAssure 5, é possível forçar um snapshot, pausar temporariamente os snapshots e visualizar as listas de pontos de recuperação atuais no repositório, além de excluí-los se necessário. Os pontos de recuperação são utilizados para restaurar as máquinas protegidas ou para montar um sistema de arquivos local.

Os snapshots capturados pelo AppAssure 5 são feitos no nível do bloco e reconhecem o aplicativo. Isso significa que todas as transações abertas e os logs de transação contínua são concluídos e os caches são descarregados em disco antes da criação do snapshot.

O AppAssure 5 usa um driver de filtro de volume de baixo nível, que se anexa aos volumes montados e depois rastreia todas as alterações no nível de bloco para o próximo snapshot iminente. O Microsoft Volume Shadow Services (VSS) é usado para facilitar snapshots consistentes de falhas de aplicativos.

Visualização de pontos de recuperação

Execute as etapas do procedimento a seguir para visualizar os pontos de recuperação.

Para visualizar pontos de recuperação

1 No AppAssure 5 Core Console, navegue até a máquina protegida da qual deseja visualizar os pontos de recuperação.

2 Clique na guia Pontos de recuperação.

Você pode visualizar informações sobre os pontos de recuperação da máquina conforme a descrição na tabela a seguir.

Tabela 63.

Informações	Descrição
Status	Indica o status atual do ponto de recuperação.
Criptografado	Indica se o ponto de recuperação é criptografado.
Conteúdo	Relaciona os volumes incluídos no ponto de recuperação.
Tipo	Define um ponto de recuperação como uma imagem de base ou um snapshot (diferencial) incremental.
Data de criação	Exibe a data em que o ponto de recuperação foi criado.
Tamanho	Exibe a quantidade de espaço que o ponto de recuperação consome no repositório.

Visualização de um ponto de recuperação específico

Execute as etapas do procedimento a seguir para visualizar detalhes sobre um ponto de recuperação específico.

Para visualizar um ponto de recuperação específico

1 No AppAssure 5 Core Console, navegue até a máquina protegida da qual deseja visualizar os pontos de recuperação.

2 Clique na guia Pontos de recuperação.

3 Clique no símbolo de maior que > próximo ao ponto de recuperação na lista para expandir a visualização.

Você pode visualizar informações mais detalhadas sobre o conteúdo do ponto de recuperação da máquina selecionada, bem como acessar uma variedade de operações que podem ser realizadas no ponto de recuperação, como descrito na tabela a seguir.

Tabela 64.

Informações	Descrição
Ações	O menu Ações inclui as seguintes operações que podem ser realizadas no ponto de recuperação selecionado: **Montar**. Selecione essa opção para montar o ponto de recuperação selecionado. Para obter mais informações, consulte Montagem de um ponto de recuperação de uma máquina com Windows. **Exportar**. Usando a opção Exportar, é possível exportar o ponto de recuperação selecionado para ESXi, VMWare Workstation, HyperV ou Virtual Box. Para obter mais informações, consulte Exportação de dados de uma máquina com Windows para uma máquina virtual. **Restaurar**. Selecione essa opção para restaurar do ponto de recuperação selecionado em um volume especificado. Para obter mais informações, consulte Seleção de um ponto de recuperação e início da BMR. **Verificar.** Se a máquina protegida possui um SQL Server instalado, selecione essa opção para forçar uma verificação de soma de verificação ou de capacidade de montagem. Para obter mais informações, consulte Forçamento de verificações de soma de verificação de pontos de recuperação do Exchange Server. Se a máquina protegida possui um Exchange Server instalado, selecione essa opção para forçar uma verificação de capacidade de anexação. Para obter mais informações, consulte Forçamento de uma verificação de capacidade de montagem de um banco de dados do Exchange.
Conteúdo	A área Conteúdo inclui uma linha para cada volume no ponto de recuperação expandido, relacionando as seguintes informações de cada volume: **Status**. Indica o status atual do ponto de recuperação. **Título**. Relaciona o volume específico no ponto de recuperação. **Tipo**. Indica se um ponto de recuperação específico é uma imagem de base ou um snapshot (diferencial) incremental. **Tamanho**. Exibe a quantidade de espaço que o ponto de recuperação consome no repositório.

4 Clique no símbolo de maior que (>) ao lado de um volume no ponto de recuperação selecionado para expandir a visualização.

Você pode visualizar informações sobre o volume selecionado no ponto de recuperação expandido, conforme descrito na tabela a seguir.

Tabela 65.

Caixa de texto	Descrição
Título	Indica o volume específico no ponto de recuperação.
Sistemas de arquivos	Indica o tipo do sistema de arquivos para o volume selecionado.
Capacidade bruta	Indica a quantidade de espaço de armazenamento bruto em todo o volume.
Capacidade formatada	Indica a quantidade de espaço de armazenamento no volume que está disponível para dados após o volume ser formatado.
Capacidade usada	Indica a quantidade de espaço de armazenamento atualmente em uso no volume.

Montagem de um ponto de recuperação de uma máquina com Windows

No AppAssure 5, você pode montar um ponto de recuperação de uma máquina com Windows para acessar dados armazenados por meio de um sistema de arquivos local.

NOTA: Ao montar pontos de recuperação de dados restaurados de máquinas com Windows com deduplicação de dados ativada, será preciso garantir que a deduplicação também está ativada no server do Core.

Para montar um ponto de recuperação de uma máquina com Windows

1 No AppAssure 5 Core Console, navegue até a máquina que deseja montar em um sistema de arquivos local.

A guia Resumo da máquina selecionada é exibida.

2 Clique na guia Pontos de recuperação.

3 Na lista de pontos de recuperação, clique no símbolo de maior que (>) para expandir o ponto de recuperação que deseja montar.

4 Nos detalhes expandidos desse ponto de recuperação, clique em **Montar**.

A caixa de diálogo Montar pontos de recuperação é exibida.

5 Na caixa de diálogo Montar ponto de recuperação, edite as definições de montagem de um ponto de recuperação, conforme descrito na tabela a seguir.

Tabela 66.

Opção	Descrição
Local de montagem: Pasta local	Especifique o caminho usado para acessar o ponto de recuperação montado.
Opções de montagem: Tipo de montagem	Especifique o modo de acessar os dados do ponto de recuperação montado: • Montagem de apenas leitura • Montagem de apenas leitura com gravações anteriores • Montagem gravável
Imagens de volume	Especifique as imagens de volume que deseja montar
Criar um compartilhamento do Windows para essa montagem	Como opção, marque a caixa de seleção para especificar se o ponto de recuperação montado pode ser compartilhado e defina os direitos de acesso a ele, incluindo o nome de compartilhamento e os grupos permitidos.

6 Clique em **Montar** para montar o ponto de recuperação.

NOTA: Se você desejar copiar diretórios ou arquivos de um ponto de recuperação montado para outra máquina com Windows, use o Windows Explorer para copiá-los com as permissões padrão ou permissões de acesso do arquivo original. Para obter mais detalhes, consulte Restauração de um diretório ou arquivo usando o Windows Explorer a Restauração de um diretório ou arquivo e preservação das permissões usando o Windows Explorer.

7 Como opção, enquanto a tarefa estiver em andamento, você poderá visualizar seu progresso no menu suspenso Tarefas em execução no Core Console ou visualizar informações detalhadas na guia Eventos. Para obter mais informações sobre o monitoramento de eventos do AppAssure 5, consulte Visualização de tarefas, alertas e eventos.

Desmontagem de pontos de recuperação selecionados

Execute as etapas deste procedimento para desmontar os pontos de recuperação selecionados que estão montados no Core.

NOTA: Ao desmontar um ponto de recuperação montado remotamente, isso é denominado *desconectar*.

Para desmontar pontos de recuperação selecionados

1. No AppAssure 5 Core Console, clique no menu suspenso Ferramentas e em **Montagens**.

   A página de Montagens aparece. Há um painel para Montagens locais (pontos de recuperação montados a partir do Core) e outro para Montagens remotas (pontos de recuperação montados por meio do Local Mount Utility). Em cada painel, os respectivos pontos de recuperação montados aparecem na lista.

2. Para os pontos de recuperação que você deseja desmontar, faça o seguinte:

   - No painel **Montagens locais**, para cada ponto de recuperação montado localmente na lista que você deseja desmontar, clique em **Desmontar**.
   - No painel **Montagens remotas**, para cada ponto de recuperação montado remotamente na lista que você deseja desmontar, clique em **desconectar**.

3. Na caixa de diálogo Desmontagem dos pontos de recuperação, clique em **Sim** para confirmar.
4. Confirme que os pontos de recuperação montados anteriormente não são mais exibidos na lista de Montagens remotas ou locais, conforme adequado.

Desmontagem de todos os pontos de recuperação

Execute as etapas deste procedimento para desmontar todos os pontos de recuperação que estão montados no Core.

NOTA: Ao desmontar um ponto de recuperação montado remotamente, isso é denominado *desconectar*.

Para desmontar todos os pontos de recuperação

1. No AppAssure 5 Core Console, clique no menu suspenso Ferramentas e em **Montagens**.

   A página de Montagens aparece. Há um painel para Montagens locais (pontos de recuperação montados a partir do Core) e outro para Montagens remotas (pontos de recuperação montados por meio do Local Mount Utility). Em cada painel, os respectivos pontos de recuperação montados aparecem na lista.

2. Para os pontos de recuperação que você deseja desmontar, faça o seguinte:

   - No painel Montagens locais, para desmontar todos os pontos de recuperação montados localmente, clique em **Desmontar todos**.
   - No painel Montagens remotas, para desmontar todos os pontos de recuperação montados remotamente, clique em **Desconectar todos**.

3. Na caixa de diálogo Desmontagem de todos os pontos de recuperação, clique em **Sim** para confirmar.
4. Confirme que todos os pontos de recuperação locais ou remotos foram desmontados ou desconectados, conforme apropriado.

Montagem de um volume de ponto de recuperação em máquina com Linux

No utilitário `aamount` no AppAssure 5, é possível montar remotamente um volume de um ponto de recuperação como um volume local para uma máquina com Linux.

NOTA: Ao realizar este procedimento, não tente montar pontos de recuperação na pasta /tmp, que contém os arquivos aavdisk.

Para montar um volume de ponto de recuperação em máquina com Linux

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

   ```
   sudo aamount
   ```

4. No prompt de montagem do AppAssure, insira o seguinte comando para relacionar as máquinas protegidas.

   ```
   lm
   ```

5. Quando solicitado, insira o endereço IP ou nome de host do seu server do AppAssure Core.
6. Insira as credenciais de login do server do Core, ou seja, o nome de usuário e a senha.

   Será exibida uma lista das máquinas que estão protegidas pelo servidor AppAssure. Cada máquina é identificada por: número de item de linha, host/endereço IP e número de ID da máquina.

   Por exemplo: 293cc667-44b4-48ab-91d8-44bc74252a4f
7. Insira o seguinte comando para relacionar os pontos de recuperação que estão disponíveis para uma máquina especificada:

   ```
   lr <line_number_of_machine
   ```

   NOTA: Observe que você também pode inserir o número de ID da máquina neste comando em vez do número do item de linha.

   Uma lista exibe e inclui os pontos de recuperação de base e incremental da máquina. Essa lista inclui um número de item de linha, data/carimbo de data e hora, localização do volume, tamanho de ponto de recuperação e número de ID do volume que inclui um número de sequência no fim, que identifica o ponto de recuperação.

   Por exemplo, 293cc667-44b4-48ab-91d8-44bc74252a4f:2
8. Insira o seguinte comando para selecionar e montar o ponto de recuperação especificado no ponto/caminho de montagem especificado.

   ```
   m <volume_recovery_point_ID_number> <caminho>
   ```

   NOTA: Você também pode especificar um número de linha no comando em vez do número de ID do ponto de recuperação para identificar o ponto de recuperação. Nesse caso, você usaria o número de linha de agente/máquina (da saída lm), seguido do número da linha do ponto de recuperação e letra de volume, seguido pelo caminho, como, m <machine_line_number> <recovery_point_line_number> <volume_letter> <caminho>. Por exemplo, se a saída `lm` relacionar três máquinas agente e você inserir o comando `lr` para o número 2 e montar o volume b do ponto de recuperação 23 em /tmp/mount_dir o comando será:
   `m 2 23 b /tmp/mount_dir`
9. Para confirmar se a montagem foi bem-sucedida, insira o seguinte comando, que deve relacionar o volume remoto anexado:

   ```
   l
   ```

Desmontando um ponto de recuperação em máquina com Linux

Complete as etapas neste procedimento para desmontar um ponto de recuperação em uma máquina Linux.

Para desmontar um ponto de recuperação em máquina com Linux

1 Execute o utilitário, do AppAssure, `aamount` como raiz ou como superusuário, por exemplo:

```
sudo aamount
```

2 No prompt de montagem do AppAssure, insira o seguinte comando para relacionar as máquinas protegidas.

```
lm
```

3 Quando solicitado, insira o endereço IP ou nome de host do seu server do AppAssure Core.

4 Insira as credenciais de login (nome de usuário e a senha) do server do Core.

Será exibida uma lista das máquinas que estão protegidas pelo servidor AppAssure.

5 Insira o seguinte comando para relacionar os pontos de recuperação que estão disponíveis para uma máquina especificada:

```
lr <line_number_of_machine
```

> **NOTA:** Observe que você também pode inserir o número de ID da máquina neste comando em vez do número do item de linha.

Uma lista exibe e inclui os pontos de recuperação de base e incremental da máquina. Essa lista inclui um número de item de linha, data/carimbo de data e hora, localização do volume, tamanho de ponto de recuperação e número de ID do volume que inclui um número de sequência no fim, que identifica o ponto de recuperação.

Por exemplo, 293cc667-44b4-48ab-91d8-44bc74252a4f:2

6 Execute o comando `l ou list` para obter uma lista dos dispositivos Network Block Device (NBD). Se você montar um ponto de recuperação, receberá um caminho para o NBD-device depois de executar o comando `l ou list`.

7 Insira o seguinte comando para desmontar um ponto de recuperação:

```
unmount <path_of_nbd-device>
```

8 Execute o comando `l ou list` para garantir que a desmontagem do ponto de recuperação foi bem-sucedida.

Remoção dos pontos de recuperação

É fácil remover do repositório os pontos de recuperação de determinada máquina. Ao excluir pontos de recuperação no AppAssure 5, especifique uma das seguintes opções.

- **Excluir todos os pontos de recuperação.** Remove do repositório todos os pontos de recuperação da máquina agente selecionada.
- **Excluir um intervalo de pontos de recuperação**. Remove todos os pontos de recuperação em um intervalo especificado antes do atual, até e incluindo a imagem de base, ou seja, todos os dados da máquina, além de todos os pontos de recuperação após o atual até a próxima imagem de base.

> **NOTA:** Não é possível recuperar os pontos de recuperação excluídos.

Para remover pontos de recuperação

1 No AppAssure 5 Core Console, navegue até a máquina da qual deseja visualizar os pontos de recuperação.

2 Clique na guia Pontos de recuperação.

3 Clique no menu **Ações**.

4 Selecione uma das opções a seguir:

- Para excluir todos os pontos de recuperação atualmente armazenados, clique em **Excluir tudo**.

- Para excluir um conjunto de pontos de recuperação em um intervalo de dados específico, clique em **Excluir intervalo**.

  A caixa de diálogo Excluir será exibida.

  - Na caixa de diálogo Excluir intervalo, especifique o intervalo de pontos de recuperação que deseja excluir usando uma data e hora inicial e final e clique em **Excluir**.

Exclusão de uma cadeia de pontos de recuperação órfãos

Um ponto de recuperação órfão é um snapshot incremental que não está associado a uma imagem de base. Snapshots subsequentes continuam a se acumular sobre esse ponto de recuperação. No entanto, sem a imagem de base, os pontos de recuperação resultantes são incompletos e é improvável que contenham os dados necessários para concluir uma recuperação. Esses pontos de recuperação são considerados parte da cadeia de pontos de recuperação órfãos. Se essa situação ocorrer, a melhor solução é excluir a cadeia e criar uma nova imagem de base.

Para obter mais informações sobre como forçar uma imagem de base, consulte Forçar snapshot.

Para excluir uma cadeia de pontos de recuperação órfãos

1. No AppAssure 5 Core Console, navegue até a máquina protegida da qual deseja excluir a cadeia de pontos de recuperação órfãos.
2. Clique na guia Pontos de recuperação.
3. Em Pontos de recuperação, expanda o ponto de recuperação órfão.

   Esse ponto de recuperação é chamado, na coluna Tipo, de “Incremental, Órfão”.
4. A seguir, em Ações, clique em **Excluir**.

   Aparece a janela Excluir pontos de recuperação.
5. Na janela Excluir pontos de recuperação, clique em **Sim**.

△ **CUIDADO: Excluir esse ponto de recuperação exclui toda a cadeia de pontos de recuperação, incluindo os pontos de recuperação incremental que ocorrem antes ou depois dela, até a próxima imagem de base. Essa operação não pode ser desfeita.**

A cadeia de pontos de recuperação órfãos é excluída.

Forçar snapshot

Forçar um snapshot permite forçar uma transferência de dados para a máquina protegida atual. Ao forçar um snapshot, a transferência começa imediatamente ou é adicionada à fila. Somente os dados que foram alterados em relação a um ponto de recuperação anterior são transferidos. Se não existir um ponto de recuperação anterior, todos os dados nos volumes protegidos são transferidos, o que é chamado de imagem de base.

ⓘ **NOTA:** O AppAssure 5 suporta Windows 8, Windows 8.1, Windows Server 2012 e Windows Server 2012 R2 para transferências de base e incrementais.

Para forçar um snapshot

1. No AppAssure 5 Core Console, navegue até a máquina ou cluster com o ponto de recuperação no qual deseja forçar um snapshot.
2. Na guia Resumo da seção Volumes, especifique os volumes para os quais se deve fazer snapshots e, em seguida, clique no botão **Forçar snapshot** ou **Forçar imagem de base**.

Tabela 67.

Opção	Descrição
Forçar snapshot	Faz um snapshot incremental dos dados atualizados desde a captura do último snapshot.
Forçar imagem de base	Tira um snapshot completo de todos os dados nos volumes da máquina.

Gerenciamento dos SQL e Exchange Servers

Quando você protege os SQL Servers e Exchange Servers, há funções específicas para esses tipos de server que você pode realizar. Elas incluem:

- **Forçamento do truncamento de log do server.** Os SQL Servers e Exchange Servers incluem os logs de server. O processo para truncar os logs do SQL identifica o espaço disponível no server. Quando você truncar logs do server do Exchange, além de identificar o espaço disponível, o processo libera mais espaço no server. Para obter informações sobre o forçamento do truncamento de log, consulte Forçamento do truncamento de log para uma máquina com SQL ou com Exchange.
- **Definição de credenciais para o respectivo server.** Os servers do Exchange permitem que você defina credenciais para a máquina protegida na guia Resumo para o server protegido. Os SQL Servers permitem que você defina credenciais para uma máquina com SQL Server protegida, ou defina credenciais padrão para todos os SQL Servers.
    - Para obter informações sobre a definição de credenciais para os servers Exchange, consulte Definição de credenciais para os Exchange Servers.
    - Para obter informações sobre a definição de credenciais para os servers SQL, consulte Definição de credenciais para SQL Servers.
    - Para obter informações sobre a realização de outras ações acessíveis a todos os agentes protegidos na guia Resumo do agente, consulte Sobre a guia Resumo.

Definição de credenciais para os Exchange Servers

Depois que você proteger dados em um server do Microsoft Exchange, é possível definir credenciais de login no AppAssure 5 Core Console.

Para definir credenciais para um server do Exchange

1 Depois de incluir a máquina do Exchange Server na proteção, navegue até o AppAssure 5 Core Console e selecione a máquina no painel Navegação.

A guia Resumo é exibida para a máquina.

2 Na guia Resumo, no menu suspenso **Ações**, clique em **Exchange** e, no menu suspenso sensível ao contexto, selecione a ação que deseja realizar.

3 Para definir credenciais para um server do Exchange único, clique em **Definir credenciais** e, na caixa de diálogo Editar credenciais do Exchange, faça o seguinte:

a No campo de texto Nome de usuário, insira o nome de usuário com permissões para o Exchange Server, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).

b No campo de texto Senha, insira a senha associada ao nome de usuário especificado para se conectar ao Exchange Server.

c Clique em **OK** para confirmar as configurações e feche a caixa de diálogo.

Definição de credenciais para SQL Servers

Depois que você proteger dados em um server SQL Exchange, é possível definir credenciais de login no AppAssure 5 Core Console.

Para definir credenciais para SQL Servers

1 Depois de incluir a máquina do SQL Server na proteção, no AppAssure 5 Core Console, selecione a máquina no painel Navegação.

A guia Resumo é exibida para a máquina.

2 Na guia Resumo, clique no menu suspenso **Ações** e, no menu suspenso sensível ao contexto, selecione a ação que deseja realizar.

- Se desejar definir credenciais padrão para todas as instâncias do SQL Server database, clique em **Definir credenciais padrão para todas as instâncias** e, na caixa de diálogo Editar credenciais padrão, faça o seguinte:
  - a No campo de texto Nome de usuário, insira o nome de usuário com permissões para todos os SQL Servers associados, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
  - b No campo de texto Senha, insira a senha associada ao nome de usuário especificado para se conectar ao SQL Server.
  - c Clique em **OK** para confirmar as configurações e feche a caixa de diálogo.
- Se desejar definir credenciais para uma instância do SQL Server database, clique em **Definir credenciais da instância** e, na caixa de diálogo Editar credenciais da instância, faça o seguinte:
  - a Selecione o tipo de credencial (Padrão, Windows ou SQL)
  - b No campo de texto Nome de usuário, insira o nome de usuário com permissões para o SQL Server, por exemplo, Administrador (ou, se a máquina estiver em um domínio, [nome do domínio]\Administrador).
  - c No campo de texto Senha, insira a senha associada ao nome de usuário especificado para se conectar ao SQL Server.
  - d Clique em **OK** para confirmar as configurações e feche a caixa de diálogo.

Sobre a restauração de dados de pontos de recuperação

O AppAssure 5 protege seus dados em máquinas com Windows e Linux. As cópias de segurança de máquinas agente protegidas são salvas no AppAssure 5 Core como pontos de recuperação. Use esses pontos de recuperação para restaurar seus dados usando um dos três métodos disponíveis.

No AppAssure 5 Core Console, é possível restaurar volumes inteiros a partir de um ponto de recuperação de um volume que não é do sistema, substituindo os volumes na máquina de destino. É possível fazer isso em máquinas com Windows ou Linux. Para obter informações, consulte Restauração de volumes a partir de um ponto de recuperação.

Também é possível restaurar volumes inteiros em máquinas com Linux a partir de pontos de recuperação usando a linha de comando do agente Linux. Para obter mais informações sobre como usar o utilitário aamount da linha de comando, consulte Restauração de volumes em uma máquina com Linux usando a linha de comando.

Não é possível restaurar um volume que contenha o sistema operacional diretamente de um ponto de recuperação, porque a máquina para a qual você está restaurando está usando o sistema operacional e os drivers que estão incluídos no processo de restauração. Se você deseja restaurar a partir de um ponto de recuperação em agente um volume do sistema (por exemplo, a unidade C da máquina do Agent), realize uma bare metal restore (BMR). Isso envolve a criação de uma imagem inicializável a partir do ponto de recuperação,

incluindo o sistema operacional e os arquivos de configuração, além dos dados, e o início da máquina de destino a partir dessa imagem inicializável para concluir a restauração. A imagem inicializável é diferente se a máquina que você deseja restaurar usa um sistema operacional Windows ou Linux.

Se você deseja restaurar a partir de um ponto de recuperação em um volume do sistema em uma máquina com Windows, consulte Roteiro de realização de uma bare metal restore em máquinas com Windows.

Se você deseja restaurar a partir de um ponto de recuperação em um volume do sistema em uma máquina com Linux, consulte Roteiro de realização de uma bare metal restore em máquinas com Linux.

Finalmente, em contraste com a restauração de volumes inteiros, é possível montar um ponto de recuperação a partir de uma máquina com Windows e navegar pelas pastas e arquivos individuais para recuperar apenas um conjunto específico de arquivos. Para obter mais informações, consulte Restauração de um diretório ou arquivo usando o Windows Explorer. Se for preciso fazer isso e preservar as permissões de arquivos originais (por exemplo, ao restaurar uma pasta de usuário em um server de arquivos), consulte Restauração de um diretório ou arquivo e preservação das permissões usando o Windows Explorer.

Os tópicos desta seção descrevem informações sobre como restaurar dados em máquinas físicas. Para obter mais informações sobre a exportação de dados protegidos de máquinas com Windows para máquinas virtuais, consulte Sobre exportação de dados protegidos de máquinas com Windows para máquinas virtuais.

NOTA: Ao recuperar dados em máquinas com Windows, se o volume que você está restaurando está com a deduplicação de dados do Windows ativada, será preciso ter certeza que a deduplicação também está ativada no server do Core.

O AppAssure 5 suporta o Windows 8, Windows 8.1, Windows Server 2012 e Windows Server 2012 R2 para transferências normais (de base e incrementais), bem como para restauração de dados, bare metal restore e exportações virtuais.

Para obter mais informações sobre os tipos de volumes suportados e não suportados para cópia de segurança e recuperação, consulte Limitações de suporte para volumes dinâmicos e básicos.

Restauração de volumes a partir de um ponto de recuperação

É possível restaurar volumes em uma máquina protegida a partir dos pontos de recuperação armazenados no AppAssure 5 Core. No AppAssure 5.4 e posterior, esse processo usa o Assistente de restauração de máquinas.

NOTA: Em versões anteriores, esse processo era conhecido como realizar uma reversão.

O AppAssure 5 suporta a proteção e recuperação de máquinas configuradas com partições EISA. O suporte também foi estendido para máquinas com Windows 8, Windows 8.1, Windows Server 2012 e Windows 2012 R2 que usam o Windows Recovery Environment (Windows RE).

É possível iniciar uma restauração a partir de qualquer local no AppAssure 5 Core Console clicando no ícone **Restaurar** na barra de botões do AppAssure 5. Ao iniciar uma restauração dessa maneira, é preciso especificar qual das máquinas protegidas no Core você deseja restaurar e, depois, explorar até o volume que deseja restaurar.

Ou explore na UI do Core Console em uma máquina específica, expanda os pontos de recuperação para os volumes dessa máquina e, no ponto de recuperação adequado, selecione **Restaurar**. Se uma restauração for iniciada dessa maneira, siga este procedimento começando com a Etapa 5.

Se você deseja restaurar um ponto de recuperação em uma máquina com Linux, primeiro desmonte o disco no qual vai restaurar os dados.

Se você deseja restaurar a partir de um ponto de recuperação em um volume do sistema, ou restaurar a partir de um ponto de recuperação utilizando um CD de inicialização, você deve realizar uma Bare Metal Restore (BMR). Para obter informações sobre a BMR, consulte Noções básicas sobre Bare Metal Restore, e para obter informações de pré-requisitos para sistemas operacionais Windows ou Linux, consulte Pré-requisitos para realizar uma bare metal restore em uma máquina com Windows e Pré-requisitos para realização de uma bare metal restore em máquinas com Linux, respectivamente. É possível acessar as funções da BMR a partir do Core

Console conforme descrito no roteiro para cada sistema operacional. Também é possível realizar uma BMR a partir do assistente de Restauração de máquinas. Esse procedimento irá direcioná-lo ao ponto adequado no assistente para o procedimento Gerenciamento de uma imagem de inicialização do Windows e inicialização de uma BMR a partir do assistente de Restauração de máquinas.

Execute o procedimento abaixo para restaurar volumes em um ponto de recuperação.

Para restaurar volumes em um ponto de recuperação

1 Para restaurar um volume em uma máquina protegida no ícone Restaurar, navegue até o Core Console e clique em **Restaurar** na barra de botões do AppAssure 5.

O Assistente de restauração de máquinas é exibido.

2 Na página Máquinas protegidas, selecione a máquina protegida da qual deseja restaurar os dados e clique em **Avançar**.

> **NOTA:** A máquina protegida deve ter o software Agent instalado e deve ter pontos de recuperação a partir dos quais você realizará a operação de restauração.

Aparece a página Pontos de recuperação.

3 Na lista de pontos de recuperação, procure o snapshot que deseja restaurar da máquina agente.

- Se necessário, use os botões de navegação na parte inferior da página para exibir pontos de recuperação adicionais.
- Como opção, se quiser limitar a quantidade de pontos de recuperação que aparecem na página Pontos de recuperação do assistente, você pode filtrar por volumes (se definidos) ou por data de criação do ponto de recuperação.

4 Clique em qualquer ponto de recuperação para selecioná-lo e em **Avançar**.

Aparece a página Destino.

5 Na página Destino, escolha a máquina para a qual deseja restaurar os dados da seguinte forma:

- Se você deseja restaurar os dados a partir do ponto de recuperação selecionado para a mesma máquina agente (por exemplo, Machine1), e se os volumes que deseja restaurar não incluem o volume do sistema, selecione **Recuperar em uma máquina protegida (apenas volumes que não são do sistema)**, confirme se a máquina de destino (Machine1) está selecionada e clique em **Avançar**.

  A página Mapeamento de volume é exibida. Vá para a Etapa 9.

- Se você deseja restaurar os dados a partir do ponto de recuperação selecionado em uma máquina protegida diferente (por exemplo, substituir o conteúdo da Machine2 pelos dados da Machine1), selecione **Recuperar em uma máquina protegida (apenas volumes que não são do sistema)**, selecione a máquina de destino (por exemplo, Machine2) na lista e clique em **Avançar**.

  A página Mapeamento de volume é exibida. Vá para a Etapa 9.

- Se você deseja restaurar a partir do ponto de recuperação selecionado na mesma máquina ou em uma máquina diferente usando um CD de inicialização, isso é considerado uma bare metal restore (BMR). Para obter informações sobre a BMR, consulte Noções básicas sobre Bare Metal Restore.

  > **NOTA:** A realização de uma BMR tem requisitos específicos, com base no sistema operacional da máquina do agente que você deseja restaurar. Para entender esses pré-requisitos, consulte Pré-requisitos para realizar uma bare metal restore em uma máquina com Windows e Pré-requisitos para realização de uma bare metal restore em máquinas com Linux, respectivamente.

  Se os volumes que deseja restaurar não incluem o volume do sistema, selecione **Recuperar em qualquer máquina de destino usando um CD de inicialização**. Esta opção irá notificá-lo a criar um CD de inicialização.

  - Para continuar e criar o CD de inicialização com as informações do ponto de recuperação selecionado utilizando o assistente de Restauração de máquinas, clique em **Avançar** e vá

para a Gerenciamento de uma imagem de inicialização do Windows e inicialização de uma BMR a partir do assistente de Restauração de máquinas.

- Se você já criou o CD de inicialização e a máquina de destino foi iniciada utilizando-o, vá para Etapa 8 do tópico Gerenciamento de uma imagem de inicialização do Windows e inicialização de uma BMR a partir do assistente de Restauração de máquinas.

- Se você deseja restaurar a partir de um ponto de recuperação em um volume do sistema (por exemplo, a unidade C da máquina agente chamada Machine1), isso também é considerado uma BMR. Selecione **Recuperar em qualquer máquina de destino usando um CD de inicialização**. Esta opção irá notificá-lo a criar um CD de inicialização.

  - Para continuar e criar o CD de inicialização com as informações do ponto de recuperação selecionado utilizando o assistente de Restauração de máquinas, clique em Avançar e vá para a Gerenciamento de uma imagem de inicialização do Windows e inicialização de uma BMR a partir do assistente de Restauração de máquinas.

  - Se você já criou o CD de inicialização, vá para a etapa 6.

6 Inicie a máquina que você deseja restaurar utilizando o CD de inicialização. Para obter mais informações para BMR em uma máquina com Windows, consulte Carregamento do CD de inicialização e início da máquina de destino, e para BMR em uma máquina com Linux, consulte Carregamento do Live DVD e início da máquina de destino.

7 De volta ao server do Core, na página Destino do assistente de Restauração de máquinas, selecione **Já possuo um CD de inicialização executando na máquina de destino** e insira as informações sobre a máquina à qual deseja se conectar, conforme descrito na tabela a seguir.

Tabela 68.

Caixa de texto	Descrição
Endereço IP	O endereço IP da máquina na qual deseja restaurar. É idêntico ao endereço IP exibido no URC.
Chave de autenticação	A senha específica para se conectar ao server selecionado. É idêntico à chave de autenticação exibida no URC.

8 Clique em **Avançar**.

Se as informações de conexão inseridas correspondem ao URC, e se o Core e o server de destino podem identificar um ao outro corretamente na rede, os volumes do ponto de recuperação selecionado são carregados, e a página Mapeamento de disco é exibida.

Para concluir sua BMR a partir do assistente de Restauração de máquinas, vá para Etapa 8 do tópico Gerenciamento de uma imagem de inicialização do Windows e inicialização de uma BMR a partir do assistente de Restauração de máquinas.

NOTA: Embora o AppAssure 5 suporte as partições FAT32 e ReFS, atualmente, apenas a restauração completa e a BMR são suportadas, visto que existe uma limitação do driver com ReFS, de modo que a restauração é implementada em modo de usuário, exportação da VM, e assim por diante. Se um Core está protegendo pelo menos um volume agente que contém o sistema de arquivos ReFS, ele deve ser instalado no Windows 8/2012, que fornece suporte nativo ao formato ReFS, caso contrário, a funcionalidade será limitada e operações que envolvem tarefas como a montagem de uma imagem de volume não funcionarão. O AppAssure 5 Core Console apresentará as mensagens de erro aplicáveis a essas ocorrências.

A bare metal restore da configuração de discos de espaços de armazenamento (um recurso do Windows 8.1) também não é suportada nesta versão. Para obter detalhes, consulte o *Guia de implementação do Dell AppAssure 5*.

9 Na página Mapeamento de volume, para cada volume no ponto de recuperação que você deseja restaurar, selecione o volume de destino apropriado. Se você não deseja restaurar um volume, na coluna Volumes de destino, selecione **Não restaurar**.

10 Selecione **Exibir opções avançadas** e faça o seguinte:

- Para restaurar em máquinas com Windows, se quiser usar o Live Recovery, selecione **Live Recovery**.

  Usando a tecnologia de recuperação instantânea Live Recovery no AppAssure 5, é possível recuperar ou restaurar instantaneamente os dados em suas máquinas físicas ou virtuais a partir de pontos de recuperação armazenados de máquinas com Windows, incluindo espaços de armazenamento do Microsoft Windows. O Live Recovery não está disponível para máquinas com Linux.

- Se deseja forçar a desmontagem, selecione **Forçar desmontagem**.

  Se você não forçar uma desmontagem antes de restaurar os dados, a restauração pode falhar com um erro de volume em uso.

11 Vá para a Etapa 12.

12 Se os volumes que você deseja restaurar contiverem bancos de dados do SQL ou Microsoft Exchange, na página Desmontar bancos de dados , será solicitado que você os desmonte. Como opção, se você quiser remontar esses bancos de dados após a restauração ser concluída, selecione **Remontar automaticamente todos os bancos de dados após o ponto de recuperação ser restaurado**. Depois, clique em **Concluir**.

13 Clique em **OK** para confirmar a mensagem de status de que o processo de restauração foi iniciado.

14 Como opção, para monitorar o progresso de sua ação de restauração, no Core Console, clique em **Eventos**. Para obter mais informações, consulte Visualização de tarefas, alertas e eventos.

Restauração de volumes em uma máquina com Linux usando a linha de comando

No AppAssure 5, é possível restaurar volumes em suas máquinas Linux protegidas usando o utilitário de linha de comando `aamount`.

NOTA: Esse processo antes era chamado de reversão.

Ao realizar este procedimento, não tente montar pontos de recuperação na pasta /tmp, que contém os arquivos aavdisk.

A restauração de volumes também é suportada em suas máquinas protegidas no AppAssure 5 Core Console. Consulte Restauração de volumes a partir de um ponto de recuperação para obter mais informações.

CUIDADO: Não tente restaurar o volume de sistema ou raiz (/).

Para restaurar volumes em uma máquina com Linux usando a linha de comando

1 Execute o utilitário AppAssure `aamount` como raiz, por exemplo:

```
sudo aamount
```

2 No prompt de montagem do AppAssure, insira o seguinte comando para relacionar as máquinas protegidas.

```
lm
```

3 Quando solicitado, insira o endereço IP ou nome de host do seu server do AppAssure 5 Core.

4 Insira as credenciais de login desse server, ou seja, o nome de usuário e a senha.

Aparece uma lista que mostra as máquinas protegidas por esse server AppAssure 5. Ela relaciona as máquinas agente encontradas por número de item de linha, host/endereço IP e número de ID da máquina (por exemplo: 293cc667-44b4-48ab-91d8-44bc74252a4f).

5 Insira o seguinte comando para relacionar os pontos de recuperação atualmente montados para a máquina especificada:

```
lr <machine_line_item_number>
```

NOTA: Observe que você também pode inserir o número de ID da máquina neste comando em vez do número do item de linha.

Uma exibição em lista exibe os pontos de recuperação de base e incremental da máquina. Essa lista inclui um número de item de linha, data/carimbo de data e hora, localização do volume, tamanho de ponto de recuperação e número de ID do volume que inclui um número de sequência no fim (por exemplo,
”293cc667-44b4-48ab-91d8-44bc74252a4f:2”), que identifica o ponto de recuperação.

6 Insira o seguinte comando para selecionar um ponto de recuperação a restaurar:

```
r <volume_recovery_point_ID_number> <caminho>
```

Esse comando restaura a imagem do volume especificada pelo ID do Core para o caminho especificado. O caminho para a restauração é o do descritor de arquivo de dispositivo e não o diretório no qual está montado.

NOTA: Você também pode especificar um número de linha no comando em vez do número de ID do ponto de recuperação para identificar o ponto de recuperação. Nesse caso, você usaria o número de linha de agente/máquina (da saída lm), seguido do número da linha do ponto de recuperação e letra de volume, seguido pelo caminho, como, r <machine_line_item_number> <recovery_point_line_number> <volume_letter> <caminho>. Nesse comando, <caminho> é o descritor de arquivo do volume real.

Por exemplo, se a saída `lm` relacionar três máquinas agente e você inserir o comando `lr` para o número `2`, e quiser restaurar o ponto de recuperação `23` do volume `b` no volume montado no diretório `/mnt/data`, o comando será:

```
r2 23 b /mnt/data
```

É possível restaurar para /, mas apenas ao realizar uma Bare Metal Restore ao ser inicializado com um Live DVD. Para obter mais informações, consulte Início de uma bare metal restore no Linux.

7 Quando solicitado a continuar, insira `y`, para Sim.

Depois que a restauração continuar, uma série de mensagens será exibida para notificá-lo sobre o status.

8 Após a restauração bem-sucedida, o utilitário `aamount` montará e reanexará automaticamente o módulo do kernel ao volume restaurado se o destino antes estava protegido e montado. Caso contrário, será necessário montar o volume restaurado no disco local e, em seguida, confirmar se os arquivos estão restaurados (por exemplo, é possível usar o comando `sudo mount` e depois o comando `ls`.)

Restauração de um diretório ou arquivo usando o Windows Explorer

É possível usar o Windows Explorer para copiar e colar os diretórios e arquivos de um ponto de recuperação montado em qualquer máquina com Windows. Isso pode ser útil quando você quiser distribuir apenas uma parte de um ponto de recuperação para seus usuários.

Ao copiar arquivos e diretórios, as permissões de acesso do usuário que está realizando a operação de cópia são utilizadas e aplicadas aos diretórios e arquivos colados. Se você quiser restaurar diretórios e arquivos para seus usuários e preservar as permissões de arquivos originais (por exemplo, ao restaurar uma pasta de usuário em um server de arquivos), consulte Restauração de um diretório ou arquivo e preservação das permissões usando o Windows Explorer.

Para restaurar um diretório ou arquivo usando o Windows Explorer

1 Monte o ponto de recuperação que contém os dados que você deseja restaurar. Para obter detalhes, consulte Montagem de um ponto de recuperação de uma máquina com Windows.

2 No Windows Explorer, navegue até o ponto de recuperação montado e selecione os diretórios e arquivos que deseja restaurar. Clique com o botão direito do mouse e selecione **Copiar**.

3 No Windows Explorer, navegue até o local da máquina onde você deseja restaurar os dados. Clique com o botão direito do mouse e selecione **Colar**.

Restauração de um diretório ou arquivo e preservação das permissões usando o Windows Explorer

É possível usar o Windows Explorer para copiar e colar os diretórios e arquivos de um ponto de recuperação montado em qualquer máquina com Windows e, ao mesmo tempo, preservar as permissões de acesso dos arquivos.

Por exemplo, se você precisar restaurar uma pasta acessada somente por usuários específicos em um server de arquivos, poderá usar os comandos **Copiar** e **Colar com permissões** para garantir que os arquivos restaurados retenham as permissões que restringem o acesso. Dessa forma, é possível evitar ter que aplicar manualmente as permissões aos diretórios e arquivos restaurados.

NOTA: O comando Colar com permissões é instalado com o AppAssure 5 Core e Agent. Não está disponível no Local Mount Utility.

Para restaurar um diretório ou arquivo e preservar as permissões usando o Windows Explorer

1 Monte o ponto de recuperação que contém os dados que você deseja restaurar. Para obter detalhes, consulte Montagem de um ponto de recuperação de uma máquina com Windows.

2 No Windows Explorer, navegue até o ponto de recuperação montado e selecione os diretórios e arquivos que deseja restaurar. Clique com o botão direito do mouse e selecione **Copiar**.

3 No Windows Explorer, navegue até o local da máquina onde você deseja restaurar os dados. Clique com o botão direito do mouse e selecione **Colar com permissões**.

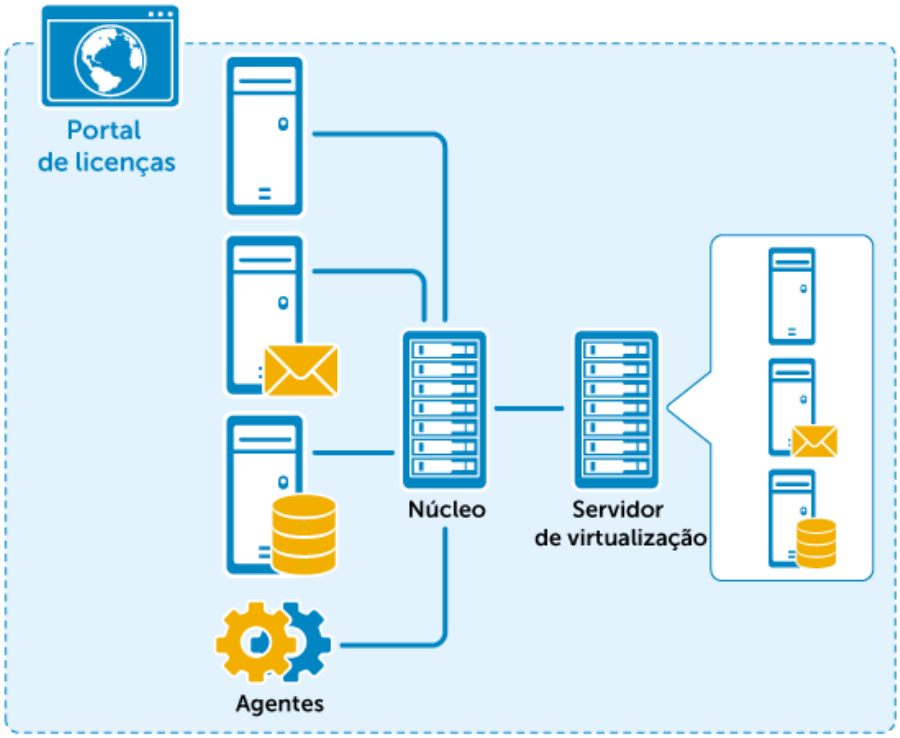
NOTA: Nessa etapa, se o comando **Colar com permissões** estiver desabilitado no menu do botão direito, o Windows Explorer não terá conhecimento dos arquivos que você deseja copiar. Repita a Etapa 2 para habilitar o comando **Colar com permissões** no menu do botão direito.

Sobre exportação de dados protegidos de máquinas com Windows para máquinas virtuais

O AppAssure 5 suporta a exportação única ou contínua (suporte a standby virtual) de informações de cópia de segurança do Windows para uma máquina virtual. Exportar seus dados para uma máquina Virtual Standby fornece-lhe uma cópia de alta disponibilidade dos dados. Se uma máquina protegida ficar inativa, você poderá inicializar a máquina virtual e realizar a recuperação.

O diagrama a seguir mostra uma implementação típica de exportação de dados para uma máquina virtual.

Figura 8. Implementação de standby virtual



Ao exportar para uma máquina virtual, todos os dados de cópia de segurança de um ponto de recuperação, bem como os parâmetros definidos para a programação de proteção da sua máquina são exportados. Também é possível criar um “standby virtual” fazendo dados protegidos serem continuamente exportados de sua máquina protegida para uma máquina virtual.

É possível realizar uma exportação virtual dos pontos de recuperação para suas máquinas protegidas com agente Windows ou Linux ao VMware, ESXi, Hyper-V e VirtualBox.

NOTA: Para ESXi, VMware Workstation ou Hyper-V, a versão da máquina virtual deve ser uma versão licenciada dessas máquinas virtuais e não as versões gratuitas ou de teste.

Se a replicação estiver definida entre dois cores (origem e destino), será possível exportar dados do core de destino apenas após a replicação inicial estar concluída.

Gerenciamento de exportações

O Standby virtual é um processo físico para virtual (P2V) que cria uma máquina virtual ou clone de uma máquina protegida ou agente. O standby virtual pode ser criado usando um processo de exportação ad hoc ou de atualização contínua. Um standby virtual criado usando uma atualização contínua é atualizado de forma incremental depois de cada snapshot capturado do agente de origem.

NOTA: O AppAssure 5 suporta a exportação do Hyper-V para Window 8, Window 8.1, Windows Server 2012 e 2012 R2.

Na guia Standby virtual do Core Console, é possível visualizar o status das exportações atualmente definidas, incluindo as exportações únicas e contínuas para standby virtual. Nessa guia, é possível realizar uma variedade de ações para gerenciar as exportações, incluindo pausar, parar ou remover as exportações. Também é possível visualizar uma fila de futuras exportações.

Para gerenciar exportações

1 No Core Console, navegue até a guia Standby virtual.

Na guia Standby virtual, é possível visualizar uma tabela de definições de exportação salvas, incluindo as informações descritas na tabela a seguir.

Tabela 69.

Coluna	Descrição
Status	O status da configuração de standby virtual, exibido como ícone. Podem aparecer os seguintes ícones de status: • Ícone verde - Standby virtual configurado com sucesso, ativo e não pausado. A próxima exportação de Standby virtual será realizada logo após o próximo snapshot. • Ícone amarelo - Standby virtual em pausa e ainda salvo pelo Core. No entanto, após uma nova transferência, o trabalho de exportação não será iniciado automaticamente e não haverá novas exportações de Standby virtual para esse agente.
Nome da máquina	O nome da máquina de origem.
Destino	A máquina virtual e o caminho para o qual os dados estão sendo exportados.
Tipo de exportação	O tipo de plataforma de máquina virtual para a exportação, como ESXi, VMware, Hyper-V ou VirtualBox.
Última exportação	Data e hora da última exportação. Se uma exportação acaba de ser adicionada, mas não foi concluída, será exibida uma mensagem informando que a exportação ainda não foi realizada. Se uma exportação tiver falhado ou tiver sido cancelada, também será exibida uma mensagem correspondente.

2 Para gerenciar as definições de exportação salvas, selecione uma exportação e clique em um dos seguintes:

- **Pausar** - para pausar a exportação.
- **Retomar** - para reiniciar uma exportação em pausa.
- **Forçar** - para forçar uma nova exportação. Essa opção pode ser útil quando o standby virtual está em pausa e é retomado, o que significa que o trabalho de exportação será reiniciado somente após uma nova transferência. Se não quiser esperar a nova transferência, poderá forçar uma exportação.

3 Para remover uma exportação do sistema, clique em **Remover**. Ao remover uma exportação, ela é permanentemente removida do sistema e você não poderá reiniciá-la.

4 Para visualizar detalhes sobre as exportações ativas atualmente na fila a serem concluídas, clique em **Exibir fila de exportação**.

É exibida a tabela Fila de exportação na tabela Standby virtual e inclui as informações descritas na tabela a seguir.

Tabela 70.

Coluna	Descrição
Nome da máquina	O nome da máquina de origem.
Destino	A máquina virtual e o caminho para o qual os dados estão sendo exportados.
Tipo de exportação	O tipo de plataforma de máquina virtual para a exportação, como ESXi, VMware, Hyper-V ou VirtualBox.
Tipo de programação	O tipo de exportação (Única ou Contínua).
Status	O progresso da exportação, exibido como porcentagem em uma barra de progresso.

5 Para gerenciar o número de exportações que podem ser executadas ao mesmo tempo, faça o seguinte:

- Na tabela Fila de exportação, clique em **Máximo de exportações simultâneas**.
- Na caixa de diálogo Máximo de exportações simultâneas, insira um número e clique em **Salvar**. O padrão é 5.

6 Para cancelar uma exportação na Fila de exportação, selecione uma exportação na tabela Fila de exportação e clique em **Cancelar**.

7 Para adicionar uma nova exportação de standby virtual, é possível clicar em **Adicionar** para iniciar o Assistente de exportação. Para obter mais informações sobre a definição de standby virtual para uma máquina virtual específica, consulte um dos seguintes tópicos:

- Realização de uma exportação ESXi contínua (Standby virtual)
- Realização de uma exportação VMware Workstation contínua (Standby virtual)
- Realização de uma exportação do Hyper-V contínua (Standby virtual)
- Realização de uma exportação do VirtualBox contínua (Standby virtual)
- Exportação de informações de cópia de segurança da máquina com Linus para uma máquina virtual

Exportação de dados de uma máquina com Windows para uma máquina virtual

No AppAssure 5 é possível exportar os dados de suas máquinas com Windows para uma máquina virtual (VMware, ESXi, Hyper-V e VirtualBox) exportando todas as informações de cópia de segurança de um ponto de recuperação, bem como os parâmetros definidos da programação de proteção da sua máquina.

Para exportar informações de cópia de segurança do Windows para uma máquina virtual

- No AppAssure 5 Core Console, navegue até a máquina que deseja exportar. Na guia Resumo, no menu suspenso **Ações**, clique em **Exportar** e selecione o tipo de exportação que deseja realizar (Única ou Standby virtual). O Assistente de exportação é exibido.

  Vá aos seguintes tópicos para obter mais informações sobre exportação de dados do Windows para um tipo específico de máquina virtual.

  - Exportação de dados do Windows usando a exportação ESXi
  - Exportação de dados do Windows usando a exportação VMware Workstation
  - Exportação de dados do Windows usando a exportação Hyper-V
  - Exportação de dados do Windows Data para VirtualBox

Exportação de dados do Windows usando a exportação ESXi

No AppAssure 5, é possível optar por exportar dados para o ESXi, realizando uma exportação única, ou estabelecendo uma exportação contínua (para standby virtual). Execute as etapas dos procedimentos a seguir do tipo apropriado de exportação.

Realização de uma exportação ESXi única

Execute as etapas deste procedimento para realizar uma exportação única para o ESXi.

Para realizar uma exportação ESXi única

1 No AppAssure 5 Core Console, realize um dos procedimentos a seguir:

- Na barra de botões, clique em **Exportar** para iniciar o Assistente de exportação, e faça o seguinte:
    a Na página Selecionar tipo de exportação, selecione **Exportação única**, e clique em **Avançar**.
    b Na página Máquinas protegidas, selecione a máquina protegida que deseja exportar para uma máquina virtual, e clique em **Avançar**.
- Navegue até a máquina que deseja exportar e, na guia Resumo, no menu suspenso Ações dessa máquina, clique em **Exportar**> **Única**.

  O Assistente de exportação é exibido na página de Pontos de recuperação.

2 Na página Pontos de recuperação, selecione o ponto de recuperação do AppAssure 5 Core que deseja exportar e clique em **Avançar**.

Definição de informações da máquina virtual para realizar uma exportação ESXi

Execute as etapas deste procedimento para definir as informações da máquina virtual.

Para definir as informações da máquina virtual para realizar uma exportação ESXi

1 Na página Destino do Assistente de exportação, no menu suspenso Recuperar na máquina virtual, selecione **ESX(i)**.

2 Insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir e clique em **Avançar**.

Tabela 71.

Opções	Descrição
Nome do host	Insira um nome para a máquina de host.
Port	Insira a porta para a máquina de host. O padrão é 443.
Nome de usuário	Insira as credenciais de login para a máquina de host.
Senha	Insira as credenciais de login para a máquina de host.

3 Na página Opções de máquina virtual, insira as informações conforme descrito na tabela a seguir.

Tabela 72.

Opção	Descrição
Conjunto de recursos	Selecione um conjunto de recursos na lista suspensa.
Armazenamento de dados	Selecione um armazenamento de dados na lista suspensa.
Nome da máquina virtual	Insira um nome para a máquina virtual.
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • **Usar a mesma quantidade de RAM da máquina de origem** • **Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB** A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.
Aprovisionamento de disco	Selecione o tipo de aprovisionamento de disco como Thin ou Thick.

Tabela 72.

Opção	Descrição
Mapeamento de disco	Especifique o tipo de mapeamento de disco como Automático ou Manual.
Versão	Selecione a versão da máquina virtual.

4 Clique em **Avançar**.

5 Na página Volumes, selecione os volumes que deseja exportar e clique em **Avançar**.

6 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Realização de uma exportação ESXi contínua (Standby virtual)

Execute as etapas deste procedimento para realizar uma exportação contínua para o ESXi.

Para realizar uma exportação ESXi contínua (standby virtual)

1 No AppAssure 5 Core Console, realize um dos procedimentos a seguir:

- Na guia Standby virtual, clique em **Adicionar** para iniciar o Assistente de exportação. Na página Máquinas protegidas do Assistente de exportação, selecione a máquina protegida que deseja exportar e clique em **Avançar**.
- Navegue até a máquina que deseja exportar e, na guia Resumo do menu suspenso Ações dessa máquina, clique em **Exportar** > **Standby virtual**.

2 Na página Destino do Assistente de exportação, no menu suspenso Recuperar na máquina virtual, selecione **ESXi**.

3 Insira as informações para acessar a máquina virtual, conforme descrito na tabela a seguir, e clique em **Avançar**.

Tabela 73.

Opção	Descrição
Nome do host	Insira um nome para a máquina de host.
Port	Insira a porta para a máquina de host. O padrão é 443.
Nome de usuário	Insira as credenciais de login para a máquina de host.
Senha	Insira as credenciais de login para a máquina de host.

4 Na página Opções de máquina virtual, insira as informações conforme descrito na tabela a seguir.

Tabela 74.

Opção	Descrição
Conjunto de recursos	Selecione um conjunto de recursos na lista suspensa.
Armazenamento de dados	Selecione um armazenamento de dados na lista suspensa.
Nome da máquina virtual	Insira um nome para a máquina virtual.

Tabela 74.

Opção	Descrição
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • **Usar a mesma quantidade de RAM da máquina de origem** • **Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB** A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.
Aprovisionamento de disco	Selecione o tipo de aprovisionamento de disco como Thin ou Thick.
Mapeamento de disco	Especifique o tipo de mapeamento de disco conforme adequado (Automático, Manual ou com VM).
Versão	Selecione a versão da máquina virtual.
Realize uma exportação ad-hoc inicial	Selecione para realizar a exportação virtual imediatamente em vez de após o próximo snapshot programado (opcional)

5 Clique em **Avançar**.

6 Na página Volumes, selecione os volumes que deseja exportar e clique em **Avançar**.

7 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Exportação de dados do Windows usando a exportação VMware Workstation

No AppAssure 5, é possível optar por exportar dados para o VMware Workstation, realizando uma exportação única, ou estabelecendo uma exportação contínua (para standby virtual). Execute as etapas dos procedimentos a seguir do tipo apropriado de exportação.

Realização de uma exportação VMware Workstation única

Execute as etapas deste procedimento para realizar uma exportação única para VMware Workstation.

Para realizar uma exportação VMware Workstation única

1 No AppAssure 5 Core Console, realize um dos procedimentos a seguir:

- Na barra de botões, clique em **Exportar** para iniciar o Assistente de exportação, e faça o seguinte:
  - a Na página Selecionar tipo de exportação, selecione **Exportação única**, e clique em **Avançar**.
  - b Na página Máquinas protegidas, selecione a máquina protegida que deseja exportar para uma máquina virtual, e clique em **Avançar**.
- Navegue até a máquina que deseja exportar e, na guia Resumo, no menu suspenso Ações dessa máquina, clique em **Exportar**> **Única**.

  O Assistente de exportação é exibido na página de Pontos de recuperação.

2 Na página Pontos de recuperação, selecione o ponto de recuperação do AppAssure 5 Core que deseja exportar e clique em **Avançar**.

Determinação das definições únicas para realizar uma exportação VMware Workstation

Execute as etapas deste procedimento para determinar as definições de realização de uma exportação única VMware Workstation.

Para determinar as definições únicas para realizar uma exportação VMware Workstation

1 Na página Destino do Assistente de exportação, no menu suspenso Recuperar na máquina virtual, selecione **VMware Workstation** e clique em **Avançar**.

2 Na página Opções de máquina virtual, insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir.

Tabela 75.

Opção	Descrição
Local	Especifique o caminho da pasta local ou compartilhamento de rede no qual você deseja criar a máquina virtual. **NOTA:** Se você especificou um caminho de compartilhamento de rede, será preciso inserir credenciais de login válidas para uma conta que está registrada na máquina de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.
Nome de usuário	Insira as credenciais de login do local de rede para a exportação. • Se você especificou um caminho de compartilhamento de rede, será preciso inserir um nome de usuário válido para uma conta que está registrada na máquina de destino. • Se você inseriu um caminho local, um nome de usuário não é necessário.
Senha	Insira as credenciais de login do local de rede para a exportação. • Se você especificou um caminho de compartilhamento de rede, será preciso inserir uma senha válida para uma conta que está registrada na máquina de destino. • Se você inseriu um caminho local, uma senha não é necessária.
Nome da máquina virtual	Insira um nome para a máquina virtual sendo criada, por exemplo, VM-0A1B2C3D4. **NOTA:** O nome padrão é o nome da máquina de origem.
Versão	Especifique a versão do VMware Workstation da máquina virtual. Você pode selecionar dentre: • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • **Usar a mesma quantidade de RAM da máquina de origem** • **Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB** A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

3 Clique em **Avançar**.

4 Na página Volumes, selecione os volumes para exportar, por exemplo, C:\ e D:\, e clique em **Avançar**.

5 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Realização de uma exportação VMware Workstation contínua (Standby virtual)

Execute as etapas deste procedimento para realizar uma exportação contínua para VMware Workstation.

Para realizar uma exportação VMware Workstation contínua (standby virtual)

1 No AppAssure 5 Core Console, realize um dos procedimentos a seguir:

- Na guia Standby virtual, clique em **Adicionar** para iniciar o Assistente de exportação. Na página Máquinas protegidas do Assistente de exportação, selecione a máquina protegida que deseja exportar e clique em **Avançar**.
- Navegue até a máquina que deseja exportar e, na guia Resumo do menu suspenso Ações dessa máquina, clique em **Exportar**> **Standby virtual**.

2 Na página Destino do Assistente de exportação, no menu suspenso Recuperar na máquina virtual, selecione **VMware Workstation** e clique em **Avançar**.

3 Na página Opções de máquina virtual, insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir.

Tabela 76.

Opção	Descrição
Caminho de destino	Especifique o caminho da pasta local ou compartilhamento de rede no qual você deseja criar a máquina virtual. **NOTA:** Se você especificou um caminho de compartilhamento de rede, será preciso inserir credenciais de login válidas para uma conta que está registrada na máquina de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.
Nome de usuário	Insira as credenciais de login do local de rede para a exportação. • Se você especificou um caminho de compartilhamento de rede, será preciso inserir um nome de usuário válido para uma conta que está registrada na máquina de destino. • Se você inseriu um caminho local, um nome de usuário não é necessário.
Senha	Insira as credenciais de login do local de rede para a exportação. • Se você especificou um caminho de compartilhamento de rede, será preciso inserir uma senha válida para uma conta que está registrada na máquina de destino. • Se você inseriu um caminho local, uma senha não é necessária.
Máquina virtual	Insira um nome para a máquina virtual sendo criada, por exemplo, VM-0A1B2C3D4. **NOTA:** O nome padrão é o nome da máquina de origem.
Versão	Especifique a versão do VMware Workstation da máquina virtual. Você pode selecionar dentre: • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • **Usar a mesma quantidade de RAM da máquina de origem** • **Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB** A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

4 Selecione **Realizar exportação personalizada inicial** para realizar a exportação virtual imediatamente em vez de após o próximo snapshot programado.

5 Clique em **Avançar**.

6 Na página Volumes, selecione os volumes para exportar, por exemplo, C:\ e D:\, e clique em **Avançar**.

7 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Exportação de dados do Windows usando a exportação Hyper-V

No AppAssure 5, é possível optar por exportar dados utilizando a Exportação do Hyper-V, realizando uma exportação única, ou estabelecendo uma exportação contínua (para Standby Virtual).

O AppAssure 5 suporta exportação de primeira geração do Hyper-V para os seguintes hosts:

- Windows 8
- Windows 8,1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

O AppAssure 5 suporta exportação de segunda geração do Hyper-V para os seguintes hosts:

- Windows 8,1
- Windows Server 2012 R2

NOTA: Nem todas as máquinas protegidas podem ser exportadas a hosts de segunda geração do Hyper-V.

Somente máquinas protegidas com os seguintes sistemas operacionais da Interface Unificada de Firmware Extensível (UEFI) suportam exportação virtual para hosts de segunda geração do Hyper-V:

- Windows 8 (UEFI)
- Windows 8.1 (UEFI)
- Windows Server 2012 (UEFI)
- Windows Server 2012R2 (UEFI)

NOTA: A exportação do Hyper-V para VM de segunda geração poderá falhar caso o host do Hyper-V não tenha RAM suficiente alocada para realizar a exportação.

Execute as etapas dos procedimentos a seguir do tipo apropriado de exportação.

Realização de uma exportação do Hyper-V única

Execute as etapas deste procedimento para realizar uma exportação única para o Hyper-V.

Para realizar uma exportação do Hyper-V única

1 No AppAssure 5 Core Console, realize um dos procedimentos a seguir:

- Na barra de botões, clique em **Exportar** para iniciar o Assistente de exportação, e faça o seguinte:

a Na página Selecionar tipo de exportação, selecione **Exportação única**, e clique em **Avançar**.

b Na página Máquinas protegidas, selecione a máquina protegida que deseja exportar para uma máquina virtual, e clique em **Avançar**.

- Navegue até a máquina que deseja exportar e, na guia Resumo, no menu suspenso Ações dessa máquina, clique em **Exportar**> **Única**.

  O Assistente de exportação é exibido na página de Pontos de recuperação.

2 Na página Pontos de recuperação, selecione o ponto de recuperação do AppAssure 5 Core que deseja exportar e clique em **Avançar**.

Determinação das definições únicas para realizar uma exportação do Hyper-V

Execute as etapas deste procedimento para determinar as definições de realização de uma exportação única do Hyper-V.

Para determinar as definições únicas para realizar uma exportação do Hyper-V

1 Na página Destino do Assistente de exportação, no menu suspenso Recuperar na máquina virtual, selecione **Hyper-V**.

2 Para exportar para uma máquina local com a função Hyper-V atribuída, clique em **Usar a máquina local**.

3 Para indicar que o server Hyper-V está localizado em uma máquina remota, clique na opção **Host remoto** e insira as informações do host remoto, conforme descrito na tabela a seguir.

Tabela 77.

Caixa de texto	Descrição
Nome do host	Insira um endereço IP ou nome de host para o server Hyper-V. Ele representa o endereço IP ou nome de host do server Hyper-V remoto.
Port	Insira um número de porta para a máquina. Ele representa a porta através da qual o Core se comunica com esta máquina.
Nome de usuário	Insira o nome de usuário para o usuário com privilégios administrativos para a estação de trabalho com o server Hyper-V. Ele é usado para especificar as credenciais de login para a máquina virtual.
Senha	Insira a senha da conta de usuário com privilégios administrativos na estação de trabalho com o server Hyper-V. Ele é usado para especificar as credenciais de login para a máquina virtual.

4 Clique em **Avançar**.

5 Na página Opções de máquina virtual na caixa de texto Local da máquina de VM, insira o caminho para a máquina virtual, por exemplo, D:\export. Isso é usado para identificar o local da máquina virtual.

> **NOTA:** Você precisa especificar o local da máquina virtual para os servers Hyper-V local e remoto. O caminho precisa ser um caminho de local válido para o server Hyper-V. Diretórios não existentes são automaticamente criados. Você não deve tentar criá-los manualmente. A exportação para pastas compartilhadas, por exemplo, \\Dados\Compartilhamento, não é permitida.

6 Insira o nome da máquina virtual na caixa de texto **Nome da máquina virtual**.

O nome inserido será exibido na lista de máquinas virtuais no console do Hyper-V Manager.

7 Para especificar o uso da memória, clique em um dos seguintes:

- **Usar a mesma quantidade de RAM da máquina de origem** - para identificar que o uso de RAM é idêntico entre as máquinas virtual e de origem.
- **Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB**

  A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

8 Para especificar o formato do disco, próximo a Formato do disco, clique em um dos seguintes:

- **VHDX**
- **VHD**

> **NOTA:** A exportação do Hyper-V suporta formatos de disco VHDX se a máquina de destino estiver executando o Windows 8 (Windows Server 2012) ou mais recente. Se o formato VHDX não for suportado por seu ambiente, a opção será desativada.
>
> Se desejar exportar para a geração Hyper-V 2, somente o formato de disco VHDX é suportado.

9 Para especificar a geração do Hyper-V a fim de utilizar para exportação, clique em um dos seguintes:

- Geração 1
- Geração 2

> **NOTA:** Somente a geração 2 oferece suporte à opção de inicialização segura.

10 Especifique o adaptador de rede adequado para a VM exportada.

11 Na página Volumes, selecione os volumes para exportar, por exemplo, C:\.

> **NOTA:** Se os volumes selecionados forem maiores do que as alocações máximas adequadas suportadas pelo aplicativo conforme indicado abaixo, ou exceder a quantidade de espaço disponível, será exibido um erro.

- Para o formato de disco VHDX, seus volumes selecionados não devem ser maiores do que 64 TB.
- Para o formato de disco VHD, seus volumes selecionados não devem ser maiores do que 2040 GB.

12 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

> **NOTA:** Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Realização de uma exportação do Hyper-V contínua (Standby virtual)

Execute as etapas deste procedimento para realizar uma exportação contínua para o Hyper-V

Para realizar uma exportação do Hyper-V contínua (Standby virtual)

1 No AppAssure 5 Core Console, realize um dos procedimentos a seguir:

- Na guia Standby virtual, clique em **Adicionar** para iniciar o Assistente de exportação. Na página Máquinas protegidas do Assistente de exportação, selecione a máquina protegida que deseja exportar e clique em **Avançar**.
- Navegue até a máquina que deseja exportar e, na guia Resumo do menu suspenso Ações dessa máquina, clique em **Exportar** > **Standby virtual**.

2 Para exportar para uma máquina local com a função Hyper-V atribuída, clique em **Usar a máquina local**.

3 Para indicar que o server Hyper-V está localizado em uma máquina remota, clique na opção **Host remoto** e insira os parâmetros do host remoto, conforme descrito na tabela a seguir.

Tabela 78.

Caixa de texto	Descrição
Nome do host	Insira um endereço IP ou nome de host para o server Hyper-V. Ele representa o endereço IP ou nome de host do server Hyper-V remoto.
Port	Insira um número de porta para a máquina. Ele representa a porta através da qual o Core se comunica com esta máquina.

Tabela 78.

Caixa de texto	Descrição
Nome de usuário	Insira o nome de usuário para o usuário com privilégios administrativos para a estação de trabalho com o server Hyper-V. Ele é usado para especificar as credenciais de login para a máquina virtual.
Senha	Insira a senha da conta de usuário com privilégios administrativos na estação de trabalho com o server Hyper-V. Ele é usado para especificar as credenciais de login para a máquina virtual.

4 Clique em **Avançar**.

5 Na página Opções de máquina virtual na caixa de texto Local da máquina de VM, insira o caminho para a máquina virtual, por exemplo, D:\export. Isso é usado para identificar o local da máquina virtual.

NOTA: Você precisa especificar o local da máquina virtual para os servers Hyper-V local e remoto. O caminho precisa ser um caminho de local válido para o server Hyper-V. Diretórios não existentes são automaticamente criados. Você não deve tentar criá-los manualmente. A exportação para pastas compartilhadas, por exemplo, \\Dados\Compartilhamento, não é permitida.

6 Insira o nome da máquina virtual na caixa de texto **Nome da máquina virtual**.

O nome inserido será exibido na lista de máquinas virtuais no console do Hyper-V Manager.

7 Para especificar o uso da memória, clique em um dos seguintes:

- **Usar a mesma quantidade de RAM da máquina de origem** - para identificar que o uso de RAM é idêntico entre as máquinas virtual e de origem.
- **Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB**

  A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

8 Para especificar o formato do disco, próximo a Formato do disco, clique em um dos seguintes:

- **VHDX**
- **VHD**

NOTA: A exportação do Hyper-V suporta formatos de disco VHDX se a máquina de destino estiver executando o Windows 8 (Windows Server 2012) ou mais recente. Se o formato VHDX não for suportado por seu ambiente, a opção será desativada.

Se desejar exportar para a geração Hyper-V 2, somente o formato de disco VHDX é suportado.

9 Para especificar a geração do Hyper-V a fim de utilizar para exportação, clique em um dos seguintes:

- Geração 1
- Geração 2

NOTA: Somente a geração 2 oferece suporte à opção de inicialização segura.

10 Especifique o adaptador de rede adequado para a VM exportada.

11 Na página Volumes, selecione os volumes para exportar, por exemplo, C:\.

NOTA: Se os volumes selecionados forem maiores do que as alocações máximas adequadas suportadas pelo aplicativo conforme indicado abaixo, ou exceder a quantidade de espaço disponível, será exibido um erro.

- Para o formato de disco VHDX, seus volumes selecionados não devem ser maiores do que 64 TB.
- Para o formato de disco VHD, seus volumes selecionados não devem ser maiores do que 2040 GB.

12 Selecione **Realizar exportação personalizada inicial** para realizar a exportação virtual imediatamente em vez de após o próximo snapshot programado.

13 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Exportação de dados do Windows Data para VirtualBox

No AppAssure 5, é possível optar por exportar dados utilizando a Exportação do VirtualBox, realizando uma exportação única, ou estabelecendo uma exportação contínua (para standby virtual). Execute as etapas dos procedimentos a seguir do tipo apropriado de exportação.

NOTA: Para realizar esse tipo de exportação, é preciso ter o VirtualBox instalado na máquina do Core. O Virtual Box Versão 4.2.18 ou superior é suportado para hosts Windows.

Realização de uma exportação de VirtualBox única

Execute as etapas deste procedimento para realizar uma exportação única para o VirtualBox.

Para realizar uma exportação única para o VirtualBox

1 No AppAssure 5 Core Console, realize um dos procedimentos a seguir:

- Na barra de botões, clique em **Exportar** para iniciar o Assistente de exportação, e faça o seguinte:
  - a Na página Selecionar tipo de exportação, selecione **Exportação única**, e clique em **Avançar**.
  - b Na página Máquinas protegidas, selecione a máquina protegida que deseja exportar para uma máquina virtual, e clique em **Avançar**.
- Navegue até a máquina que deseja exportar e, na guia Resumo, no menu suspenso Ações dessa máquina, clique em **Exportar**> **Única**.

  O Assistente de exportação é exibido na página de Pontos de recuperação.

2 Na página Pontos de recuperação, selecione o ponto de recuperação do AppAssure 5 Core que deseja exportar e clique em **Avançar**.

3 Na página Destino do Assistente de exportação, no menu suspenso Recuperar na máquina virtual, selecione **VirtualBox** e clique em **Avançar**.

4 Na página Opções de máquina virtual, selecione **Usar a máquina do Windows**.

5 Insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir.

Tabela 79.

Opção	Descrição
Nome da máquina virtual	Insira um nome para a máquina virtual sendo criada. **NOTA:** O nome padrão é o nome da máquina de origem.

Tabela 79.

Opção	Descrição
Caminho de destino	Especifique um caminho de destino local ou remoto para criar a máquina virtual. **NOTA:** O caminho de destino não deve ser um diretório raiz. Se você especificou um caminho de compartilhamento de rede, será preciso inserir credenciais de login válidas (nome de usuário e senha) para uma conta que está registrada na máquina de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • **Usar a mesma quantidade de RAM da máquina de origem** • **Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB** A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

6 Para especificar uma conta de usuário para a máquina virtual, selecione **Especifique a conta de usuário para a máquina virtual exportada** e insira as seguintes informações. Isso se refere a uma conta de usuário específica para a qual a máquina virtual será registrada caso existam múltiplas contas de usuários na máquina virtual. Quando essa conta de usuário estiver conectada, somente esse usuário verá essa máquina virtual no gerenciador do VirtualBox. Se uma conta não for especificada, a máquina virtual será registrada para todos os usuários existentes na máquina com Windows e VirtualBox.

- **Nome de usuário** - insira o nome de usuário com o qual a máquina virtual é registrada.
- **Senha** - insira a senha dessa conta de usuário.

7 Clique em **Avançar**.

8 Na página Volumes, selecione os volumes para exportar, por exemplo, C:\ e D:\, e clique em **Avançar**.

9 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Realização de uma exportação do VirtualBox contínua (Standby virtual)

Execute as etapas deste procedimento para criar um Standby virtual e realizar uma exportação contínua para o VirtualBox.

Para realizar uma exportação do VirtualBox contínua (standby virtual)

1 No AppAssure 5 Core Console, realize um dos procedimentos a seguir:

- Na guia Standby virtual, clique em **Adicionar** para iniciar o Assistente de exportação. Na página Máquinas protegidas do Assistente de exportação, selecione a máquina protegida que deseja exportar e clique em **Avançar**.
- Navegue até a máquina que deseja exportar e, na guia Resumo do menu suspenso Ações dessa máquina, clique em **Exportar** > **Standby virtual**.

2 Na página Destino do Assistente de exportação, no menu suspenso Recuperar na máquina virtual, selecione **VirtualBox** e clique em **Avançar**.

3 Na página Opções de máquina virtual, selecione **Usar a máquina do Windows**.

4 Insira os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir.

Tabela 80.

Opção	Descrição
Nome da máquina virtual	Insira um nome para a máquina virtual sendo criada. **NOTA:** O nome padrão é o nome da máquina de origem.
Caminho de destino	Especifique um caminho de destino local ou remoto para criar a máquina virtual. **NOTA:** O caminho de destino não deve ser um diretório raiz. Se você especificou um caminho de compartilhamento de rede, será preciso inserir credenciais de login válidas (nome de usuário e senha) para uma conta que está registrada na máquina de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • **Usar a mesma quantidade de RAM da máquina de origem** • **Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB** A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

5 Para especificar uma conta de usuário para a máquina virtual, selecione **Especifique a conta de usuário para a máquina virtual exportada** e insira as seguintes informações. Isso se refere a uma conta de usuário específica para a qual a máquina virtual será registrada caso existam múltiplas contas de usuários na máquina virtual. Quando essa conta de usuário estiver conectada, somente esse usuário verá essa máquina virtual no gerenciador do VirtualBox. Se uma conta não for especificada, a máquina virtual será registrada para todos os usuários existentes na máquina com Windows e VirtualBox.

- **Nome de usuário** - insira o nome de usuário com o qual a máquina virtual é registrada.
- **Senha** - insira a senha dessa conta de usuário.

6 Selecione **Realizar exportação personalizada inicial** para realizar a exportação virtual imediatamente em vez de após o próximo snapshot programado.

7 Clique em **Avançar**.

8 Na página Volumes, selecione os volumes para exportar, por exemplo, C:\ e D:\, e clique em **Avançar**.

9 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Exportação de informações de cópia de segurança da máquina com Linus para uma máquina virtual

Com o AppAssure 5 é possível exportar dados de uma máquina com Linux para uma máquina virtual VirtualBox. Uma exportação inclui todas as informações de cópia de segurança de um ponto de recuperação, bem como os parâmetros definidos para a programação de proteção da sua máquina.

NOTA: O Virtual Box Versão 4.2.18 ou superior é suportado. Se a máquina com Linux estiver hospedando o VirtualBox, então a exportação do VirtualBox para Linux exige uma conexão SSH do Core para a máquina com Linux.

Realização de uma exportação de VirtualBox única

Execute as etapas deste procedimento para realizar uma exportação única para o VirtualBox.

Para realizar uma exportação única para o VirtualBox

1 No AppAssure 5 Core Console, navegue até a máquina com Linux que deseja exportar.

2 Na guia Resumo, no menu suspenso Ações dessa máquina, clique em **Exportar** e depois selecione **Única**.

O Assistente de exportação é exibido na página Máquinas protegidas.

3 Selecione uma máquina para exportar e depois clique em **Avançar**.

4 Na página Pontos de recuperação, selecione o ponto de recuperação que deseja exportar e clique em **Avançar**.

5 Na página Destino do Assistente de exportação, no menu suspenso Recuperar na máquina virtual, selecione **VirtualBox** e clique em **Avançar**.

6 Na página Opções de máquina virtual, se estiver utilizando uma conexão SSH, selecione **Máquina remota do Linux**.

7 Insira as informações sobre a máquina virtual conforme descrito na tabela a seguir.

Tabela 81.

Opção	Descrição
Nome de host do VirtualBox	Insira um endereço IP ou nome de host para o server VirtualBox. Este campo representa o endereço IP ou nome de host do server VirtualBox remoto.
Port	Insira um número de porta para a máquina. Este número representa a porta através da qual o Core se comunica com esta máquina.
Nome da máquina virtual	Insira um nome para a máquina virtual sendo criada. **NOTA:** O nome padrão é o nome da máquina de origem.
Caminho de destino	Especifique um caminho de destino para criar a máquina virtual. **NOTA:** Recomenda-se criar uma pasta raiz a partir da raiz para que a máquina virtual seja executa a partir da raiz. Se você não usar a raiz, será preciso criar uma pasta de destino manualmente na máquina de destino antes de configurar a exportação. Também será preciso conectar ou carregar manualmente a máquina virtual após a exportação.
Nome de usuário	Nome de usuário da conta na máquina de destino, por exemplo, raiz.
Senha	Senha para a conta de usuário na máquina de destino.
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • **Usar a mesma quantidade de RAM da máquina de origem** • **Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB** A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

8 Na página Volumes, selecione os volumes de dados a exportar e clique em **Avançar**.

9 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Realização de uma exportação do VirtualBox contínua (Standby virtual)

Execute as etapas deste procedimento para criar um Standby virtual e realizar uma exportação contínua para o VirtualBox.

Para realizar uma exportação do VirtualBox contínua (standby virtual)

1 No AppAssure 5 Core Console, realize um dos procedimentos a seguir:

- Na guia Standby virtual, clique em **Adicionar** para iniciar o Assistente de exportação. Na página Máquinas protegidas do Assistente de exportação, selecione a máquina protegida que deseja exportar e clique em **Avançar**.
- Navegue até a máquina que deseja exportar e, na guia Resumo do menu suspenso Ações dessa máquina, clique em **Exportar** > **Standby virtual**.

2 Na página Destino do Assistente de exportação, no menu suspenso Recuperar para a máquina virtual, selecione **VirtualBox**.

3 Na página Opções de máquina virtual, selecione **Máquina remota do Linux**.

4 Insira as informações sobre a máquina virtual conforme descrito na tabela a seguir.

Tabela 82.

Opção	Descrição
Nome de host do VirtualBox	Insira um endereço IP ou nome de host para o server VirtualBox. Este campo representa o endereço IP ou nome de host do server VirtualBox remoto.
Port	Insira um número de porta para a máquina. Este número representa a porta através da qual o Core se comunica com esta máquina.
Nome da máquina virtual	Insira um nome para a máquina virtual sendo criada. **NOTA:** O nome padrão é o nome da máquina de origem.
Caminho de destino	Especifique um caminho de destino para criar a máquina virtual. **NOTA:** Recomenda-se criar uma pasta raiz a partir da raiz para que a máquina virtual seja executa a partir da raiz. Se você não usar a raiz, será preciso criar uma pasta de destino manualmente na máquina de destino antes de configurar a exportação. Também será preciso conectar ou carregar manualmente a máquina virtual após a exportação.
Nome de usuário	Nome de usuário da conta na máquina de destino, por exemplo, raiz.
Senha	Senha para a conta de usuário na máquina de destino.
Memória	Especifique o uso de memória da máquina virtual clicando em um dos seguintes: • **Usar a mesma quantidade de RAM da máquina de origem** • **Usar uma quantidade específica de RAM e a seguir especificar a quantidade em MB** A quantidade mínima é de 1024 MB e a máxima permitida pelo aplicativo é 65536 MB. A quantidade máxima de utilização de memória é limitada pela quantidade de RAM disponível para a máquina do host.

5 Selecione **Realizar exportação personalizada inicial** para realizar a exportação virtual imediatamente em vez de após o próximo snapshot programado.

6 Clique em **Avançar**.

7 Na página Volumes, selecione os volumes de dados a exportar e clique em **Avançar**.

8 Na página Resumo, clique em **Concluir** para concluir o assistente e iniciar a exportação.

NOTA: Você pode monitorar o status e o progresso da exportação visualizando as guias Standby virtual e Eventos.

Noções básicas sobre Bare Metal Restore

Os servers, se estiverem operando como esperado, realizam as tarefas que estão configurados para fazer. É somente quando eles falham que as coisas mudam. Quando ocorre um evento catastrófico, deixando um server inoperante, medidas imediatas são necessárias para restaurar a funcionalidade total da máquina.

O AppAssure 5 fornece a capacidade de realizar uma bare metal restore (BMR) em suas máquinas com Windows ou Linux. A BMR é um processo que restaura a configuração completa do software de um sistema específico. A operação de restauração recupera não só os dados do server, mas também reformata o disco rígido e reinstala o sistema operacional e todos os aplicativos de software. Para realizar uma BMR, especifique um ponto de recuperação de uma máquina protegida e reverta (realize uma restauração) para a máquina física ou virtual designada. Se estiver realizando uma restauração em um volume do sistema, isso é considerado uma BMR. Se estiver realizando uma restauração e for necessário um CD de inicialização, isso também é considerado uma BMR. Outras circunstâncias em que você pode decidir realizar uma bare metal restore incluem atualização de hardware ou substituição do server. Em ambos esses casos, você realiza uma restauração a partir de um ponto de recuperação para o hardware atualizado ou substituído.

O AppAssure 5 oferece suporte aos sistemas operacionais Windows 8, 8.1 e Windows Server 2012, 2012 R2 inicializados a partir de partições FAT32 EFI disponíveis para proteção ou recuperação, bem como volumes ReFS (Resilient File System).

NOTA: A bare metal restore da configuração de discos de espaços de armazenamento (um recurso do Windows 8.1) também não é suportada nesta versão.

Atualmente, apenas a restauração completa e a BMR são suportadas, visto que existe uma limitação do driver com ReFS, de modo que a restauração é implementada em modo de usuário, exportação da VM, e assim por diante. Se um Core está protegendo pelo menos um volume agente que contém o sistema de arquivos ReFS, ele deve ser instalado em um Windows 8, Windows 8.1, Windows Server 2012 ou uma máquina com Windows Server 2012 R2, desde que esses sistemas operacionais ofereçam suporte nativo ao formato ReFS. Caso contrário, a funcionalidade será limitada, e operações que envolvem tarefas, como a montagem de uma imagem de volume, não funcionarão. O AppAssure 5 Core Console apresentará as mensagens de erro aplicáveis a essas ocorrências.

Apenas os sistemas operacionais Linux suportados estão disponíveis para proteção ou recuperação. Eles incluem Ubuntu, Red Hat Enterprise Linux, CentOS e SUSE Linux Enterprise Server (SLES). Para obter detalhes, consulte o *Guia de implementação do Dell AppAssure 5*.

É possível realizar uma BMR em máquinas físicas ou virtuais. Um benefício adicional é que o AppAssure 5 permite realizar uma BMR quer o hardware seja *semelhante*, quer *diferente*. Realizar uma BMR no AppAssure 5 separa o sistema operacional de uma plataforma específica, proporcionando portabilidade.

Exemplos de realização de uma BMR para hardwares semelhantes incluem a substituição do disco rígido do sistema existente ou troca de server com falha por uma máquina idêntica.

Exemplos de realização de uma BMR para hardwares diferentes incluem a restauração de um sistema com falha com um server produzido por um fabricante diferente ou com configuração diferente. Esse processo envolve a criação de uma imagem de CD de inicialização, gravação da imagem em disco, inicialização do server de destino a partir da imagem de inicialização, conexão com a instância do console de recuperação, mapeamento dos volumes, início da recuperação e monitoramento do processo. Depois que a bare metal restore for concluída, você poderá continuar com a tarefa de carregar o sistema operacional e os aplicativos de software no server restaurado, seguida pelo estabelecimento de definições exclusivas necessárias para sua configuração.

A bare metal restore é usada não apenas em cenários de recuperação após desastres, mas também para migração de dados ao atualizar ou substituir servers.

Embora a BMR seja suportada para máquinas virtuais, também é interessante notar que é mais fácil realizar uma exportação virtual para uma VM do que realizar uma BMR em uma máquina física. Para obter mais informações sobre como realizar uma exportação de VM para máquinas virtuais, consulte o procedimento adequado para a VM suportada.

- Para obter mais informações sobre como realizar uma exportação de VM usando ESXi, consulte Exportação de dados do Windows usando a exportação ESXi.

- Para obter mais informações sobre como realizar uma exportação de VM usando VMware Workstation, consulte Exportação de dados do Windows usando a exportação VMware Workstation.
- Para obter mais informações sobre como realizar uma exportação de VM usando Hyper-V, consulte Exportação de dados do Windows usando a exportação Hyper-V.
- Para obter mais informações sobre como realizar uma exportação de VM usando VirtualBox, consulte Exportação de dados do Windows Data para VirtualBox.
- Para obter mais informações sobre como realizar uma exportação de VM de uma máquina Linux protegida, consulte Exportação de informações de cópia de segurança da máquina com Linus para uma máquina virtual.

Para realizar uma BMR em uma máquina com Windows, consulte o roteiro específico para Windows, incluindo os pré-requisitos. Para obter mais informações, consulte Roteiro de realização de uma bare metal restore em máquinas com Windows.

Também é possível realizar uma BMR a partir do assistente de Restauração de máquinas. Para fazer isso, inicie com o procedimento Restauração de volumes a partir de um ponto de recuperação e, quando for direcionado nesse procedimento, vá até Gerenciamento de uma imagem de inicialização do Windows e inicialização de uma BMR a partir do assistente de Restauração de máquinas.

Para realizar uma BMR em uma máquina com Linux, consulte o roteiro específico para Linux, incluindo os pré-requisitos. Além de realizar uma BMR usando o utilitário de linha de comando aamount, agora ela pode ser realizada de dentro da UI do Core Console. O roteiro leva em conta ambas as abordagens. Para obter mais informações, consulte Roteiro de realização de uma bare metal restore em máquinas com Linux.

Roteiro de realização de uma bare metal restore em máquinas com Windows

Para realizar uma bare metal restore em máquinas com Windows, realize as tarefas a seguir.

- **Gerenciar uma imagem de inicialização do Windows**. Essa imagem ISO do CD de inicialização será usada para iniciar a unidade de destino, a partir da qual é possível acessar o Universal Recovery Console para se comunicar com as cópias de segurança no Core. Consulte Gerenciamento de uma imagem de inicialização do Windows.
    - Se você precisar de mídia física para iniciar a máquina de destino, precisará **transferir a imagem ISO do CD de inicialização para a mídia**. Consulte Transferência da imagem ISO do CD de inicialização para a mídia.
    - Em todos os casos, será preciso **carregar a imagem de inicialização no server de destino e iniciar o server** da imagem de inicialização. Consulte Carregamento do CD de inicialização e início da máquina de destino.
- **Iniciar uma bare metal restore para Windows**. Depois que a máquina de destino é iniciada a partir do CD de inicialização, é possível iniciar a BMR. Consulte Início de uma bare metal restore no Windows.
    - Será preciso **iniciar uma restauração a partir de um ponto de recuperação do Core**. Consulte Seleção de um ponto de recuperação e início da BMR.
    - Será preciso **mapear os volumes**. Consulte Mapeamento de volumes para uma bare metal restore.
    - Se a restauração for em hardware diferente e o armazenamento e drivers de rede necessário não estiverem presentes no CD de inicialização, talvez seja necessário carregar os drivers a partir de um dispositivo de mídia portátil. Para obter mais informações, consulte Carregamento de drivers usando o Universal Recovery Console.
    - Se a restauração for em hardware diferente e todos os drivers necessários estiverem presentes no CD de inicialização, será necessário **injetar drivers nos dispositivos de hardware** que não estavam na configuração anterior, mas estão incluídos no sistema que substitui o server. Para obter mais informações, consulte Injeção de drivers em seu server de destino.

- **Realização de uma BMR a partir do assistente de Restauração de máquinas**. De forma opcional, os processos para gerenciamento de uma imagem de inicialização do Windows e para iniciar a BMR, incluindo todas as subtarefas, podem ser realizados a partir do assistente de Restauração de máquinas. Para obter informações sobre iniciar o assistente, consulte as etapas 1 até 5 do Restauração de volumes a partir de um ponto de recuperação, e depois consulte Gerenciamento de uma imagem de inicialização do Windows e inicialização de uma BMR a partir do assistente de Restauração de máquinas.
- **Confirmação de um bare metal restore**. Após iniciar o procedimento de bare metal restore, você pode confirmar e monitorar o progresso. Consulte Confirmação de um bare metal restore.
    - É possível **monitorar o progresso de sua restauração**. Consulte Visualização do progresso da recuperação.
    - Depois de concluída, você pode **iniciar o server restaurado**. Consulte Início de um server de destino restaurado
    - **Solucionar problemas do processo de BMR**. Consulte Solução de problemas de conexões com o Universal Recovery Console e Reparação de problemas de inicialização.

Pré-requisitos para realizar uma bare metal restore em uma máquina com Windows

Antes de iniciar o processo de realização de uma bare metal restore de uma máquina com Windows, é preciso garantir que as seguintes condições e critérios estejam presentes:

- **Cópias de segurança da máquina que você deseja restaurar.** É preciso ter um AppAssure 5 Core funcional que contenha pontos de recuperação do server protegido que você deseja restaurar.
- **Hardware para restaurar (novo ou antigo, similar ou não).** A máquina de destino deve atender aos requisitos de instalação de um agente; para obter mais detalhes, consulte o *Guia de implementação do Dell AppAssure 5*.
- **Software e mídia de imagem.** É preciso ter um CD ou DVD virgem e um software de gravação de disco ou de criação de imagem ISO. Se gerenciar máquinas remotamente usando software de computação de rede virtual, como o UltraVNC, você precisará ter também o VNC Viewer.
- **Drivers do adaptador de rede e de armazenamento compatíveis.** Se a restauração for para hardware diferente, é preciso ter drivers de armazenamento compatível com Windows 7 PE (32 bits) e drivers do adaptador de rede para a máquina de destino, incluindo drivers de RAID, AHCI e chipset para o sistema operacional de destino, conforme o caso.
- **Partições e espaço de armazenamento, conforme apropriado.** Certifique-se que há espaço suficiente no disco rígido para criar partições de destino na máquina de destino que conterá os volumes de origem. Todas as partições de destino devem ser pelo menos do mesmo tamanho da partição de origem original.
- **Partições compatíveis.** Os sistemas operacionais Windows 8, Windows 8.1, Windows Server 2012 e Windows Server 2012 R2 que são inicializados a partir de partições FAT32 EFI que estão disponíveis para proteção ou recuperação, da mesma forma que os volumes Resilient File System (ReFS). As partições UEFI são tratadas como simples volumes FAT32. Transferências incrementais são totalmente suportadas e protegidas. O AppAssure 5 fornece suporte de sistemas UEFI para BMR, incluindo discos GPT de particionamento automático.

Gerenciamento de uma imagem de inicialização do Windows

A bare metal restore para Windows exige uma imagem de inicialização chamada de CD de inicialização, criada pela definição de parâmetros no AppAssure 5 Core Console. Essa imagem é adaptada às suas necessidades específicas. Use a imagem para iniciar a máquina de destino do Windows. Com base nas particularidades do seu ambiente, pode ser preciso transferir esta imagem para uma mídia física como um CD ou DVD. Você deve,

então, carregar virtual ou fisicamente a imagem de inicialização e iniciar o server Windows a partir da imagem de inicialização.

Esse processo é uma etapa do Roteiro de realização de uma bare metal restore em máquinas com Windows.

Para gerenciar uma imagem de inicialização do Windows, você pode realizar as seguintes tarefas:

- Criação de uma imagem ISO de um CD de inicialização para Windows
- Definição dos parâmetros de imagem ISO do CD de inicialização
- Transferência da imagem ISO do CD de inicialização para a mídia
- Carregamento do CD de inicialização e início da máquina de destino

NOTA: Esse processo descreve como gerenciar uma imagem do CD de inicialização da caixa de diálogo Criar CD de inicialização. Também é possível realizar essas etapas a partir de um assistente de Restauração de máquinas, começando da página CD de Inicialização do assistente. Acesse isso quando especificar **Recuperar em qualquer máquina de destino usando um CD de inicialização** a partir da página Destino do assistente.

Para obter instruções passo a passo para gerenciar uma imagem de inicialização do Windows a partir do assistente de Restauração de máquinas como parte de uma bare metal restore, consulte Gerenciamento de uma imagem de inicialização do Windows e inicialização de uma BMR a partir do assistente de Restauração de máquinas.

Criação de uma imagem ISO de um CD de inicialização para Windows

A primeira etapa ao realizar uma bare metal restore (BMR) de uma máquina com Windows é criar o arquivo do CD de inicialização no AppAssure 5 Core Console. Trata-se de uma imagem ISO inicializável que contém a interface do Universal Recovery Console (URC) do AppAssure 5, um ambiente usado para restaurar a unidade do sistema ou o server inteiro diretamente do AppAssure 5 Core.

A imagem ISO do CD de inicialização criada é adaptada à máquina que está sendo restaurada e, portanto, deve conter os drivers corretos de rede e de armazenamento em massa. Se for prevista a restauração em hardware diferente da máquina em que o ponto de recuperação se originou, inclua o controlador de armazenamento e outros drivers no CD de inicialização. Para obter informações sobre como injetar esses drivers no CD de inicialização, consulte Injeção de drivers em um CD de inicialização.

NOTA: A Organização Internacional de Padronização (ISO) é um órgão internacional de representantes de diversas organizações nacionais que define padrões para sistemas de arquivos. ISO 9660 é uma norma de sistema de arquivos usada em mídia de disco óptico para troca de dados, e ela suporta vários sistemas operacionais, incluindo Windows. Uma imagem ISO é a imagem de disco ou arquivo, que contém dados para todos os setores do disco, bem como o sistema de arquivos do disco.

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Windows. Faz parte do processo de Gerenciamento de uma imagem de inicialização do Windows.

Para criar uma imagem ISO de um CD de inicialização

1. No AppAssure 5 Core Console em que o server que você precisa restaurar está protegido, selecione o Core e clique na guia Ferramentas.
2. Clique em **CDs de inicialização**.
3. Selecione **Ações** e clique em **Criar CD de inicialização**.

   A caixa de diálogo Criar CD de inicialização é exibida. Use os procedimentos a seguir para concluir a caixa de diálogo.

Definição dos parâmetros de imagem ISO do CD de inicialização

Depois de abrir a caixa de diálogo Criar CD de inicialização, vários parâmetros podem ser necessários. Com base nas particularidades de sua situação, realize as tarefas a seguir, conforme necessário, para definir as propriedades de uma imagem ISO do CD de inicialização a ser usada em uma bare metal restore.

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Windows. Faz parte do processo de Criação de uma imagem ISO de um CD de inicialização para Windows.

Nomeação do arquivo do CD de inicialização e definição do caminho

Execute a etapa a seguir para dar um nome ao arquivo do CD de inicialização e definir o caminho onde a imagem ISO será armazenada.

Essa tarefa é uma etapa no processo de Definição dos parâmetros de imagem ISO do CD de inicialização. Faz parte do processo de Criação de uma imagem ISO de um CD de inicialização para Windows.

Para dar um nome ao arquivo do CD de inicialização e definir o caminho

- Na caixa de diálogo Criar CD de inicialização, em Opções de saída, na caixa de texto Caminho de saída, insira o caminho onde deseja armazenar a imagem ISO do CD de inicialização no server do Core.

  Se a unidade compartilhada na qual você deseja armazenar a imagem estiver com pouco espaço em disco, defina o caminho conforme necessário; por exemplo, D:\filename.iso.

  NOTA: A extensão do arquivo deve ser .iso. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen, barra invertida (apenas como delimitador de caminho) e ponto (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

Criação de conexões

Execute as seguintes etapas para criar as conexões.

Essa tarefa é uma etapa no processo de Definição dos parâmetros de imagem ISO do CD de inicialização. Faz parte do processo de Criação de uma imagem ISO de um CD de inicialização para Windows.

Para criar conexões

1. Em Opções de conexão, realize um dos procedimentos a seguir:
   - Para obter o endereço IP dinamicamente usando o protocolo DHCP (Dynamic Host Configuration Protocol), selecione **Obter o endereço IP automaticamente**.
   - Como opção, a fim de especificar um endereço IP estático para o console de recuperação, selecione **Use o seguinte endereço IP** e insira o endereço IP, a máscara de sub-rede, o gateway padrão e o server DNS nos campos apropriados. É preciso especificar todos esses quatro campos.
2. Se necessário, em Opções de UltraVNC, selecione **Adicionar UltraVNC** e insira a Senha de UltraVNC e a Porta de UltraVNC.

   As definições de UltraVNC permitem gerenciar remotamente o console de recuperação enquanto ele está em uso.

   NOTA: Essa etapa é opcional. Se você precisar de acesso remoto ao console de recuperação, precisará configurar e usar o UltraVNC. Não é possível efetuar login usando Microsoft Terminal Services enquanto o CD de inicialização é utilizado.

Especificação de um Ambiente de Recuperação

A imagem do CD de inicialização deverá ser criada para que o CD de inicialização (físico ou virtual) seja montável no hardware que você está restaurando. Você deve especificar a arquitetura mais bem adequada para essa máquina.

Essa tarefa é uma etapa no processo de Definição dos parâmetros de imagem ISO do CD de inicialização. Faz parte do processo de Criação de uma imagem ISO de um CD de inicialização para Windows.

Conclua a seguinte etapa para especificar um ambiente de recuperação

- No Ambiente de Recuperação, selecione a partir das opções de notificação conforme descrito na tabela a seguir.

  Tabela 83.

Opção	Descrição
OS Windows de 64 bits	Para restaurar em qualquer máquina com Windows e arquitetura de 64 bits, incluindo máquinas com uma BIOS UEFI
OS Windows de 32 bits	Para restaurar em qualquer máquina com arquitetura de 32 bits (x86)

Injeção de drivers em um CD de inicialização

A imagem de CD de inicialização exige que os drivers de armazenamento reconheçam as unidades de server e os drivers do adaptador de rede a fim de se comunicarem com o AppAssure 5 Core pela rede.

Um conjunto genérico de drivers do controlador de armazenamento e de adaptador de rede do Windows 7 PE de 32 bits é incluído automaticamente ao gerar um CD de inicialização para Windows. Isso atenderá aos requisitos de sistemas Dell mais recentes. Sistemas de outros fabricantes ou sistemas Dell mais antigos podem exigir uma injeção de drivers de controlador de armazenamento e de adaptador de rede ao criar o CD de inicialização. Se você descobrir que o CD de inicialização criado não contém os drivers necessários para executar a restauração, também poderá carregá-los na máquina de destino usando o URC. Para obter mais informações, consulte Carregamento de drivers usando o Universal Recovery Console.

Ao criar o CD de inicialização, a injeção de drivers é usada para facilitar a interoperabilidade entre o console de recuperação, o adaptador de rede e o armazenamento no server de destino.

Os dados restaurados a partir do ponto de recuperação incluem drivers para o hardware usado anteriormente. Se for feita uma bare metal restore para um hardware diferente, será preciso injetar também drivers do controlador de armazenamento no sistema operacional que está sendo restaurado usando o URC após os dados terem sido restaurados para a unidade. Isso permite que o sistema operacional restaurado seja inicializado usando o novo conjunto de hardware. Depois que o OS é inicializado após a restauração, é possível baixar e instalar os drivers adicionais necessários para que o OS possa interagir com seu novo hardware.

Para obter mais informações, consulte Injeção de drivers em seu server de destino.

Essa tarefa é uma etapa no processo de Definição dos parâmetros de imagem ISO do CD de inicialização. Faz parte do processo de Criação de uma imagem ISO de um CD de inicialização para Windows.

Execute as etapas a seguir para injetar drivers do controlador de armazenamento e do adaptador de rede em um CD de inicialização.

Para injetar drivers em um CD de inicialização

1. Baixe os drivers no website do fabricante do server e descompacte-os.
2. Compacte cada driver em um arquivo .zip, usando um utilitário de compressão adequado (por exemplo, WinZip).
3. Na caixa de diálogo Criar CD de inicialização, no painel Drivers, clique em **Adicionar um driver**.
4. Navegue pelo sistema de arquivamento para localizar o arquivo do driver compactado, selecione-o e clique em **Abrir**.

   Os drivers injetados aparecem em destaque no painel Drivers.
5. Repita a Etapa 3 e a Etapa 4, conforme o caso, até que todos os drivers tenham sido injetados.

Criação da imagem ISO do CD de inicialização

Essa tarefa é uma etapa no processo de Definição dos parâmetros de imagem ISO do CD de inicialização. Faz parte do processo de Criação de uma imagem ISO de um CD de inicialização para Windows.

Execute a etapa a seguir para criar a imagem ISO do CD de inicialização.

Para criar uma imagem ISO de um CD de inicialização

- Depois de ter dado nome ao arquivo do CD de inicialização e especificado o caminho, criado uma conexão e, opcionalmente, injetado os drivers, na tela Criar CD de inicialização, clique em **Criar CD de inicialização**.

  A imagem ISO é então criada e salva com o nome do arquivo fornecido.

Visualização do progresso de criação da imagem ISO

Essa tarefa é uma etapa no processo de Definição dos parâmetros de imagem ISO do CD de inicialização. Faz parte do processo de Criação de uma imagem ISO de um CD de inicialização para Windows.

Execute a etapa a seguir para visualizar o progresso de criação da imagem ISO.

Para visualizar o progresso de criação da imagem ISO

- Selecione a guia Eventos e, em seguida, em Tarefas, é possível monitorar o progresso da construção da imagem ISO. Para obter mais informações sobre o monitoramento de eventos do AppAssure 5, consulte Visualização de tarefas, alertas e eventos.

  Quando a criação da imagem ISO estiver concluída, ela aparecerá na página CDs de inicialização, acessível no menu Ferramentas.

Acesso à imagem ISO

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Windows. Faz parte do processo de Gerenciamento de uma imagem de inicialização do Windows.

Execute a etapa a seguir para acessar a imagem ISO.

Para acessar a imagem ISO

- Para acessar a imagem ISO, navegue até o caminho de saída especificado ou clique no link para baixar a imagem em um local do qual é possível carregá-la para o novo sistema; por exemplo, uma unidade de rede.

Transferência da imagem ISO do CD de inicialização para a mídia

Quando você cria o arquivo de CD de inicialização, ele é armazenado como imagem ISO no caminho especificado. Você deve ser capaz de montar essa imagem como unidade no server no qual está realizando uma bare metal restore.

É possível gravar a imagem ISO do CD de inicialização em mídia de CD ou DVD acessível na inicialização do sistema.

Se a máquina for iniciada do CD de inicialização, o Universal Recovery Console será iniciado automaticamente.

Caso esteja realizando uma BMR em uma máquina virtual, esta etapa não é necessária. Basta carregar a imagem ISO em uma unidade e editar as definições dessa VM para iniciar essa unidade.

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Windows. Faz parte do processo de Gerenciamento de uma imagem de inicialização do Windows.

Carregamento do CD de inicialização e início da máquina de destino

Depois de criar a imagem do CD de inicialização, é preciso inicializar o server de destino com o CD de inicialização recém-criado.

NOTA: Se o CD de inicialização tiver sido criado usando DHCP, será preciso capturar o endereço IP e a senha.

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Windows. Faz parte do processo de Gerenciamento de uma imagem de inicialização do Windows.

Para carregar um CD de inicialização e iniciar a máquina de destino

1. Navegue até o novo server e carregue a imagem do CD de inicialização a partir do local apropriado. Especifique se o server inicializará a partir da imagem de CD de inicialização.
2. Inicie a máquina, o que irá carregar o seguinte:
   - Windows 7 PE
   - Software AppAssure 5 Agent

   O AppAssure Universal Recovery Console é iniciado e exibe o endereço IP e a senha de autenticação da máquina.

   NOTA: Uma nova senha temporária é gerada cada vez que a máquina é iniciada com o CD de inicialização. Anote o endereço IP exibido no painel Definições de adaptadores de rede e a senha de autenticação exibida no painel Autenticação. Você precisará dessas informações durante o processo de recuperação de dados para acessar novamente o console.
3. Caso queira alterar o endereço IP, selecione-o e clique em **Alterar**.

   NOTA: Se um endereço IP tiver sido especificado na caixa de diálogo Criar CD de inicialização, o Universal Recovery Console o usará e exibirá na tela de definições do adaptador de rede.

Depois de iniciada com o CD de inicialização, essa máquina está pronta para o usuário se conectar a ela a partir do Core para dar início ao processo de bare metal restore.

Gerenciamento de uma imagem de inicialização do Windows e inicialização de uma BMR a partir do assistente de Restauração de máquinas

Restaurar volumes a partir de um ponto de recuperação utilizando um CD de inicialização ou restaurar um volume de sistema é considerado uma realização de uma bare metal restore. Antes de realizar uma BMR, consulte Pré-requisitos para realizar uma bare metal restore em uma máquina com Windows ou Pré-requisitos para realização de uma bare metal restore em máquinas com Linux, conforme adequado. Se desejar iniciar sua BMR em uma máquina com Windows a partir do Core Console, consulte Roteiro de realização de uma bare metal restore em máquinas com Windows.

Se desejar iniciar sua BMR a partir do assistente de Restauração de máquinas, na página Destino desse assistente, selecione a opção **Recuperar em qualquer máquina de destino usando um CD de inicialização**, e siga este procedimento. O gerenciamento de uma imagem de inicialização do Windows por meio do assistente inclui iniciar a criação do CD de inicialização, a definição do caminho para a imagem na máquina do Core, a seleção do ambiente de recuperação adequado para o hardware que você deseja restaurar, a definição, de forma opcional, dos parâmetros de conexão para o agente restaurado para utilizar a rede ou UltraVNC, a inserção, de forma opcional, de drivers para hardware que você deseja restaurar e a transferência, de forma opcional, da imagem de inicialização para mídias físicas. Esse processo também inclui inicializar a máquina na qual você deseja restaurar os dados a partir do CD; conexão com o Universal Recovery Console; mapeamento de volumes; e inicialização da bare metal restore a partir do ponto de recuperação selecionado no core.

NOTA: Esse processo descreve como gerenciar uma imagem do CD de inicialização do assistente de Restauração de máquinas como parte do processo para realizar uma BMR utilizando esse assistente. Também é possível gerenciar uma imagem de inicialização da caixa de diálogo Criar CD de inicialização. Para obter informações sobre o gerenciamento de uma imagem do CD de inicialização fora do assistente de Restauração de máquinas, consulte Gerenciamento de uma imagem de inicialização do Windows.

Para gerenciar uma imagem de inicialização do Windows e iniciar uma BMR a partir do assistente de Restauração de máquinas

1 Na página CD de inicialização, faça o seguinte:

a No campo de texto **Caminho de saída**, digite o caminho onde a imagem ISO do CD de inicialização deve ser armazenada.

Se a unidade compartilhada na qual você deseja armazenar a imagem estiver com pouco espaço em disco, defina o caminho conforme necessário; por exemplo, D:\filename.iso.

NOTA: A extensão do arquivo deve ser .iso. Ao especificar o caminho, use somente caracteres alfanuméricos, hífen, barra invertida (apenas como delimitador de caminho) e ponto (somente para separar domínios e nomes de host). As letras de A a Z não diferenciam maiúsculas e minúsculas. Não use espaços. Nenhum outro símbolo ou caractere de pontuação é permitido.

b Em **Ambiente,** selecione a arquitetura mais adequada ao hardware que você está restaurando:

- Para restaurar em qualquer máquina com Windows e arquitetura de 64 bits, selecione **Windows 8 de 64 bits (necessário para máquinas configuradas com uma bios UEFI)**.
- Para restaurar em qualquer máquina com arquitetura de 32 bits (x86), selecione **Windows 7 32 bits**.

2 Como opção, para definir os parâmetros de rede para o agente restaurado ou para usar UltraVNC, selecione **Exibir opções avançadas** e faça um dos seguintes:

- Para estabelecer uma conexão de rede para a máquina restaurada, selecione **Use o seguinte endereço IP**, como descrito na tabela a seguir.

Tabela 84.

Opção	Descrição
Endereço IP	Especifique um endereço IP ou nome de host da máquina restaurada.
Máscara de sub-rede	Especifique a máscara de sub-rede da máquina restaurada.
Gateway padrão	Especifique o gateway padrão da máquina restaurada.
DNS Server	Especifique o server de nome de domínio da máquina restaurada.

- Para definir as informações de UltraVNC, selecione **Adicionar UltraVNC**, como descrito na tabela a seguir.

  Use essa opção se você precisar de acesso remoto ao console de recuperação. Não é possível efetuar login usando Microsoft Terminal Services enquanto o CD de inicialização é utilizado

Tabela 85.

Opção	Descrição
Senha	Especifique uma senha para essa conexão UltraVNC.
Port	Especifique uma porta para essa conexão UltraVNC. A porta padrão é 5900.

3 Quando estiver satisfeito com suas seleções na página CD de inicialização, clique em **Avançar**.

4 Como opção, na página Injeção de drivers, para injetar um driver, faça o seguinte:

a Selecione **Adicionar um arquivo de drivers**

b Navegue até um arquivo ZIP que contém o arquivo, selecione o arquivo ZIP e clique em **Abrir**.

O arquivo é carregado e aparece na página Injeção de drivers.

c Depois, clique em **Avançar**.

5 Na página Imagem ISO, é possível ver o status enquanto a imagem ISO do CD de inicialização é criada. Quando o CD de inicialização for bem-sucedido, clique em **Avançar**.

A página Conexão é exibida.

6 Nesse ponto, você quer iniciar a máquina agente para a qual deseja restaurar os dados a partir do CD de inicialização.

- Se você puder inicializar a máquina agente de uma imagem ISO do CD de inicialização, faça-o agora.
- Caso contrário, copie a imagem ISO para a mídia física (CD ou DVD), coloque o disco na máquina agente, configure a máquina para carregar a partir do CD de inicialização e reinicie a partir desse CD.

NOTA: Talvez seja necessário alterar as definições de BIOS da máquina agente para garantir que o volume carregado primeiro seja o CD de inicialização.

A máquina agente, quando iniciada a partir do CD de inicialização, exibe a interface do Universal Recovery Console (URC). Esse ambiente é usado para restaurar a unidade do sistema ou volumes selecionados diretamente do AppAssure 5 Core. Observe o endereço IP e as credenciais da chave de autenticação no URC, que são atualizados cada vez que é feita uma inicialização a partir do CD de inicialização.

7 De volta ao Core Console na página Conexão, insira as informações de autenticação a partir da instância de URC da máquina que você deseja restaurar, como segue:

a Na caixa de texto Endereço IP, insira o endereço IP da máquina na qual está restaurando a partir de um ponto de recuperação.

b Na caixa de texto Chave de autenticação, insira as informações do URC.

c Depois, clique em **Avançar**.

A página Mapeamento de disco é exibida.

8 Caso queira mapear volumes automaticamente, faça o seguinte. Caso queira mapear volumes automaticamente, vá para Etapa 9.

a Selecione **Mapeamento de volume automático**.

b Na área Mapeamento de volume automático, à esquerda, selecione os volumes que deseja restaurar. Como opção, se você não deseja restaurar um volume relacionado, desmarque a opção.

NOTA: Pelo menos um volume deve ser selecionado para realizar a restauração.

c No lado direito, selecione o disco de destino para a restauração.

d Clique em **Avançar** e vá para Etapa 10.

9 Caso queira mapear volumes manualmente, faça o seguinte:

a Selecione **Mapeamento de volume manual**.

b Na área Mapeamento de volume manual, na lista suspensa Volumes de destino de cada volume, selecione os volumes que deseja restaurar. Como opção, se você não deseja restaurar um volume relacionado, desmarque a opção.

NOTA: Pelo menos um volume deve ser selecionado para realizar a restauração.

c Quando estiver satisfeito, clique em **Concluir**.

△ **CUIDADO: Se você selecionar Concluir, 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.**

O Assistente de restauração de máquinas fecha e os dados são restaurados dos volumes selecionados do ponto de recuperação na máquina de destino.

Vá para a Etapa 13.

10 Na página Visualização de mapeamento de disco, revise os parâmetros das ações de restauração selecionadas. Para realizar a restauração, clique em **Concluir**.

△ **CUIDADO: Se você selecionar Concluir, 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.**

11 Se os volumes que deseja restaurar contiverem bancos de dados do SQL ou Microsoft Exchange, e se você estiver realizando uma Live Restore, na página Desmontar bancos de dados, será solicitado que você os desmonte. Como opção, se você quiser remontar esses bancos de dados após a restauração ser concluída, selecione **Remontar automaticamente todos os bancos de dados após o ponto de recuperação ser restaurado**. Depois, clique em **Concluir**.

12 Clique em **OK** para confirmar a mensagem de status de que o processo de restauração foi iniciado.

13 Como opção, para monitorar o progresso de sua ação de restauração, no Core Console, clique em **Eventos**. Para obter mais informações, consulte Visualização de tarefas, alertas e eventos.

Início de uma bare metal restore no Windows

Antes de iniciar uma bare metal restore (BMR) em uma máquina com Windows, certas condições devem ser satisfeitas.

Para restaurar um ponto de recuperação salvo no Core, é necessário ter o hardware apropriado disponível. Para obter mais informações, consulte Pré-requisitos para realizar uma bare metal restore em uma máquina com Windows.

A máquina com Windows de destino da BMR deve ser iniciada usando a imagem do CD de inicialização. Para obter mais informações, consulte Gerenciamento de uma imagem de inicialização do Windows.

A primeira etapa é selecionar o ponto de recuperação apropriado, depois iniciar a restauração no hardware especificando o endereço IP e uma senha temporária obtida no Universal Recovery Console.

A seguir, você precisa mapear as unidades e iniciar a restauração.

O ponto de recuperação inclui drivers do hardware anterior. Se for feita uma restauração para um hardware diferente, será preciso injetar drivers do controlador de armazenamento no sistema operacional que está sendo restaurado usando o URC após os dados terem sido restaurados na unidade. Isso permite que o sistema operacional restaurado seja inicializado usando o novo conjunto de hardware. Depois que o OS é inicializado após a restauração, é possível baixar e instalar os drivers adicionais necessários para que OS possa interagir com seu novo hardware.

Para iniciar uma BMR no AppAssure 5 Core Console, realize as seguintes tarefas.

- Seleção de um ponto de recuperação e início da BMR
- Mapeamento de volumes para uma bare metal restore
- Carregamento de drivers usando o Universal Recovery Console
- Injeção de drivers em seu server de destino

Esse processo é uma etapa do Roteiro de realização de uma bare metal restore em máquinas com Windows.

Seleção de um ponto de recuperação e início da BMR

Depois que o Universal Recovery Console estiver acessível na máquina em que você deseja realizar uma BMR, será preciso selecionar o ponto de recuperação que deseja restaurar. Navegue até o Core Console para selecionar que ponto de recuperação você deseja carregar e designar o console de recuperação como o destino para os dados restaurados.

NOTA: Essa etapa é necessária para realizar BMR em todas as máquinas com Windows e opcional para executar BMR em máquinas com Linux.

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Windows. Faz parte do processo de Início de uma bare metal restore no Windows.

Se for feita uma BMR em uma máquina com Linux no Core Console, essa tarefa também será uma etapa do Roteiro de realização de uma bare metal restore em máquinas com Linux. Faz parte do processo de Início de uma bare metal restore em uma máquina com Linux usando a linha de comando.

Execute as etapas deste procedimento para selecionar um ponto de recuperação no Core e restaurar na máquina de destino física ou virtual de BMR.

Para selecionar um ponto de recuperação e iniciar a BMR

1. Navegue até o AppAssure 5 Core Console e, na lista de máquinas protegidas, clique no nome do server protegido em que deseja executar a bare metal restore.

   A guia Resumo da máquina selecionada é exibida.

2. Clique na guia Pontos de recuperação.
3. Na lista de pontos de recuperação, clique no símbolo de maior que (>) para expandir o ponto de recuperação que deseja restaurar.
4. Nos detalhes expandidos desse ponto de recuperação, no menu Ações, clique em **Restaurar**.

   O Assistente de restauração de máquinas é exibido.

5. Selecione **Recuperar em qualquer máquina de destino usando um CD de inicialização**.
6. Selecione **Eu já tenho um CD de inicialização em execução na máquina de destino.**

   Os campos de autenticação ficam acessíveis.

7. Insira as informações sobre a máquina à qual deseja se conectar, conforme descrito na tabela a seguir.

   Tabela 86.

Caixa de texto	Descrição
Endereço IP	O endereço IP da máquina na qual deseja restaurar. É idêntico ao endereço IP exibido no URC.
Chave de autenticação	A senha específica para se conectar ao server selecionado. É idêntico à chave de autenticação exibida no URC.

8. Clique em **Avançar**.

   Se as informações de conexão inseridas correspondem ao URC, e se o Core e o server de destino podem identificar um ao outro corretamente na rede, os volumes do ponto de recuperação selecionado são carregados, e a página Mapeamento de disco é exibida. Nesse caso, sua próxima etapa é mapear volumes.

NOTA: Embora o AppAssure 5 suporte as partições FAT32 e ReFS, atualmente, apenas a restauração completa e a BMR são suportadas, visto que existe uma limitação do driver com ReFS, de modo que a restauração é implementada em modo de usuário, exportação da VM, e assim por diante. Se um Core está protegendo pelo menos um volume agente que contém o sistema de arquivos ReFS, ele deve ser instalado em máquinas com Windows 8, Windows 8.1, Windows Server 2012 e Windows Server 2012 R2, quem fornece suporte nativo ao formato ReFS. Caso contrário, a funcionalidade será limitada, e operações que envolvem tarefas, como a montagem de uma imagem de volume, não funcionarão. O AppAssure 5 Core Console apresentará as mensagens de erro aplicáveis a essas ocorrências.

A bare metal restore da configuração de discos de espaços de armazenamento (um recurso do Windows 8.1) também não é suportada nesta versão. Para obter detalhes, consulte o *Guia de implementação do Dell AppAssure 5*.

Mapeamento de volumes para uma bare metal restore

Depois de se conectar ao Universal Recovery Console, você precisará mapear volumes entre aqueles relacionados no ponto de recuperação e os volumes existentes no hardware de destino para realizar a restauração.

O AppAssure 5 tenta mapear volumes automaticamente. Se você aceitar o mapeamento padrão, o disco na máquina de destino será limpo e reparticionado e quaisquer dados anteriores serão excluídos. O alinhamento é realizado na ordem em que os volumes estão relacionados no ponto de recuperação e os volumes são alocados aos discos de forma adequada de acordo com o tamanho, e assim por diante. Supondo que haja espaço suficiente na unidade de destino, nenhum particionamento será necessário ao utilizar o alinhamento automático do disco. Um disco pode ser usado em diversos volumes. Se você mapear manualmente as unidades, observe que não poderá usar o mesmo disco duas vezes.

Para o mapeamento manual, é preciso ter a nova máquina corretamente formatada antes de restaurá-la. A máquina de destino deve ter uma partição separada para cada volume no ponto de recuperação, incluindo o volume reservado do sistema. Para obter mais informações, consulte Início de uma bare metal restore no Windows.

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Windows. Faz parte do processo de Início de uma bare metal restore no Windows.

Se for feita uma BMR em uma máquina com Linux no Core Console, essa tarefa também será uma etapa do Roteiro de realização de uma bare metal restore em máquinas com Linux. Faz parte do processo de Início de uma bare metal restore no Linux.

Execute as etapas deste procedimento para mapear um volume.

Para mapear volumes para uma bare metal restore

1 Caso queira mapear volumes automaticamente, faça o seguinte. Caso queira mapear volumes automaticamente, vá para a Etapa 2

   a Na página Mapeamento de disco do Assistente de restauração de máquinas, selecione a guia Mapear volumes automaticamente.

   b Na área Mapeamento de disco, em Volume de origem, confirme se o volume de origem está selecionado e se os volumes adequados estão relacionados abaixo dele e estão selecionados.

      NOTA: Em geral, em uma BMR, deve-se restaurar, no mínimo, o volume reservado do sistema e o volume do sistema (em geral, mas nem sempre, o volume C:\).

   c Como opção, se você não deseja restaurar um volume relacionado, desmarque a opção sob o volume de origem. Pelo menos um volume deve ser selecionado para realizar a BMR.

   d Se o disco de destino automaticamente mapeado for o volume de destino correto, selecione **Disco de destino** e confirme se todos os volumes adequados estão selecionados.

   e Clique em **Restaurar** e vá para a Etapa 3.

2 Caso queira mapear volumes manualmente, faça o seguinte:

   a Na página Mapeamento de disco do Assistente de restauração de máquinas, selecione a guia Mapear volumes manualmente.

   NOTA: Se não existirem volumes na unidade da máquina na qual você está realizando uma BMR, não será possível ver essa guia ou mapear manualmente os volumes.

   b Na área Mapeamento de volume, em Volume de origem, confirme se o volume de origem está selecionado e se os volumes adequados estão relacionados abaixo dele e estão selecionados.

   c Em Destino, a partir do menu suspenso, selecione o destino apropriado que é o volume de destino para realizar a bare metal restore do ponto de recuperação selecionado e clique em **Restaurar**.

3 Na caixa de diálogo de confirmação, revise o mapeamento da origem do ponto de recuperação e do volume de destino da restauração. Para realizar a restauração, clique em **Começar a restauração**.

CUIDADO: Se você selecionar Começar a restauração, todas as partições e dados existentes na unidade de destino serão removidos permanentemente e substituídos por conteúdo do ponto de recuperação selecionado, incluindo o sistema operacional e todos os dados.

Carregamento de drivers usando o Universal Recovery Console

Ao criar um CD de inicialização, você pode adicionar drivers necessários à imagem ISO. Depois de inicializar a máquina de destino, você também pode carregar drivers de armazenamento ou de rede de dentro do Universal Recovery Console (URC). Esse recurso permite adicionar os drivers esquecidos que não foram incluídos na imagem ISO, mas são necessários para uma bare metal restore bem-sucedida.

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Windows. Faz parte do processo de Início de uma bare metal restore no Windows.

Execute as etapas do procedimento a seguir para carregar drivers usando o URC.

Para carregar drivers usando o Universal Recovery Console

1 Em uma máquina conectada à Internet, baixe e salve os drivers necessários para um dispositivo de mídia portátil, como uma unidade USB.

2 Remova a mídia da máquina conectada e insira-a no server de destino de inicialização.

3 No URC do server de destino, na guia Console, clique em **Carregar driver**.

4 Na janela Selecionar driver, navegue até o local do driver, selecione-o e clique em **Abrir**.

5 Repita conforme necessário para cada driver que você deseja carregar.

Injeção de drivers em seu server de destino

Se você estiver restaurando em um hardware diferente, precisará injetar os drivers de controlador de armazenamento, RAID, AHCI, chipset e outros drivers se eles não estiverem no CD de inicialização. Esses drivers permitem que o sistema operacional opere com sucesso todos os dispositivos em seu server de destino depois que o sistema for reiniciado após o processo de restauração.

Se você não tem certeza de quais drivers são necessários para o server de destino, clique na guia Informações do sistema do Universal Recovery Console. Essa guia mostra todos os tipos de hardware e de dispositivos do sistema do server de destino para o qual você deseja restaurar.

NOTA: O server de destino contém automaticamente alguns drivers genéricos do Windows 7 PE de 32 bits que funcionarão em alguns sistemas.

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Windows. Faz parte do processo de Início de uma bare metal restore no Windows.

Execute a tarefa a seguir para injetar drivers em seu server de destino.

Para injetar drivers em seu server de destino

1. Baixe os drivers no website do fabricante do server e descompacte-os.
2. Compacte cada driver em um arquivo .zip, usando um utilitário de compressão adequado (por exemplo, WinZip) e copie-o para o server de destino.
3. No Universal Recovery Console, clique em **Injeção de drivers.**
4. Navegue pelo sistema de arquivamento para localizar o arquivo do driver compactado e selecione-o.
5. Se você clicou em Injeção de drivers na etapa 3, clique em **Adicionar driver**. Se você clicou em Carregar driver na etapa 3, clique em **Abrir**.

   Os drivers selecionados serão injetados e carregados no sistema operacional depois que o server de destino for reiniciado.
6. Repita da Etapa 3 à Etapa 5, conforme o caso, até que todos os drivers tenham sido injetados.

Confirmação de um bare metal restore

Depois de realizar uma bare metal restore, você poderá confirmar o progresso da restauração. Quando a ação for concluída com sucesso, você poderá iniciar o server restaurado. Algumas etapas de resolução de problemas são incluídas se houver dificuldades para se conectar ao Universal Recovery Console a fim de concluir a restauração e para reparar problemas de inicialização com a máquina restaurada.

Você pode realizar as seguintes tarefas:

- Visualização do progresso da recuperação
- Início de um server de destino restaurado
- Solução de problemas de conexões com o Universal Recovery Console
- Reparação de problemas de inicialização

Esse processo é uma etapa do Roteiro de realização de uma bare metal restore em máquinas com Windows.

Visualização do progresso da recuperação

Execute as etapas deste procedimento para visualizar o progresso da restauração de dados de um ponto de recuperação (incluindo bare metal restore) iniciado no AppAssure 5 Core Console.

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Windows. Faz parte do processo de Confirmação de um bare metal restore.

Para visualizar o progresso da recuperação

1. Depois de iniciar o processo de restauração de dados de um ponto de recuperação, enquanto a tarefa estiver em andamento, você pode visualizar seu progresso no menu suspenso Tarefas em execução no Core Console.
2. É possível visualizar informações detalhadas na guia Eventos. Para obter mais informações sobre o monitoramento de eventos do AppAssure 5, consulte Visualização de tarefas, alertas e eventos.

Início de um server de destino restaurado

Execute as etapas deste procedimento para iniciar o server de destino restaurado.

NOTA: Antes de iniciar o server de destino restaurado, confirme se a recuperação foi bem-sucedida. Para obter mais informações, consulte Visualização do progresso da recuperação.

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Windows. Faz parte do processo de Confirmação de um bare metal restore.

Para iniciar um server de destino restaurado

1. Navegue de volta ao server de destino e confirme se o AppAssure Universal Recovery Console está ativo.
2. Ejete o CD de inicialização (ou desconecte a mídia física com a imagem do CD de inicialização) do server restaurado.
3. No Universal Recovery Console, na guia Console, clique em **Reinicializar**.
4. Especifique para iniciar o sistema operacional normalmente.
5. Efetue login na máquina. O sistema deve ser restaurado ao seu estado capturado no ponto de recuperação.

Solução de problemas de conexões com o Universal Recovery Console

Encontramos a seguir as etapas da solução de problemas de conexão com a imagem do CD de inicialização como parte do processo de Seleção de um ponto de recuperação e início da BMR.

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Windows. Faz parte do processo de Confirmação de um bare metal restore.

Se um erro for exibido indicando que o Core não pôde se conectar ao server remoto, existem várias causas possíveis.

- Confirme se o endereço IP e a senha atual exibidos no URC são idênticos às informações inseridas na caixa de diálogo Instância do console de recuperação.
- Para alcançar o server no qual irá restaurar dados, o Core deve ser capaz de identificar o server na rede. Para determinar se isso é possível, você pode abrir um prompt de comando no Core e fazer um ping do endereço IP do server de BMR de destino. Também é possível abrir um prompt de comando no server de destino e fazer um ping para o endereço IP do AppAssure 5 Core.
- Confirme se as definições do adaptador de rede são compatíveis entre o Core e o server de BMR de destino.

Reparação de problemas de inicialização

Execute as etapas deste procedimento para reparar problemas de inicialização. Lembre-se de que, se você tiver restaurado em um hardware diferente, precisará ter injetado o driver do controlador de armazenamento, RAID, AHCI, chipset e outros drivers, se eles já não estiverem no CD de inicialização. Esses drivers permitem que o sistema operacional opere com sucesso todos os dispositivos em seu server de destino. Para obter mais informações, consulte Injeção de drivers em seu server de destino.

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Windows. Faz parte do processo de Confirmação de um bare metal restore.

Execute o procedimento a seguir para reparar problemas de inicialização no seu server de destino.

Para reparar problemas de inicialização

1. Abra o Universal Recovery Console recarregando o CD de inicialização.
2. No Universal Recovery Console, clique em **Injeção de drivers.**
3. Na caixa de diálogo Injeção de drivers, clique em **Reparar problemas de inicialização**.

   Os parâmetros de inicialização no registro de inicialização do server de destino são reparados automaticamente.
4. No Universal Recovery Console, clique em **Reinicializar.**

Roteiro de realização de uma bare metal restore em máquinas com Linux

No AppAssure 5 é possível realizar uma bare metal restore (BMR) em uma máquina com Linux, incluindo uma restauração do volume do sistema. Ao restaurar uma máquina com Linux, você irá reverter para o ponto de recuperação do volume de inicialização. A funcionalidade de BMR é suportada usando o utilitário de linha de comando aamount e de dentro da UI do Core Console.

Para realizar uma bare metal restore em máquinas com Linux, realize as tarefas a seguir.

- **Gerenciamento de uma imagem de inicialização do Linux**. Essa imagem ISO do DVD de inicialização Linux Live é usada para iniciar a unidade de destino, a partir da qual é possível acessar o Universal Recovery Console para se comunicar com as cópias de segurança no Core. Consulte Gerenciamento de uma imagem de inicialização do Linux.
    - Se você precisar de mídia física para iniciar a máquina Linux de destino, precisará transferir a imagem ISO para a mídia. Consulte Transferência da imagem ISO do Live DVD para mídia.
    - Em todos os casos, será preciso carregar a imagem de inicialização no server de destino e iniciar o server da imagem de inicialização. Consulte Carregamento do Live DVD e início da máquina de destino.
- **Gerenciamento de partições**. Pode ser necessário criar ou montar as partições antes de realizar uma BMR em uma máquina com Linux. Consulte Gerenciamento de partições Linux.
    - O sistema Linux no qual você está realizando uma BMR deve ter as mesmas partições dos volumes de origem no ponto de recuperação. Talvez seja necessário criar partições adicionais no sistema de destino. Consulte Criação de partições na unidade de destino.
    - Montar partições. Se estiver sendo feita uma BMR manual, será preciso primeiro montar partições. Consulte Montagem de partições a partir da linha de comando. As etapas para montar partições estão incluídas no processo de realização da BMR na linha de comando. Consulte Início de uma bare metal restore em uma máquina com Linux usando a linha de comando.

      Se você usar particionamento automático para BMR dentro do Core Console, não precisará montar partições. O AppAssure 5 restaurará as mesmas partições incluídas nos pontos de recuperação que estão sendo restaurados.
- **Iniciar uma bare metal restore para Linux**. Depois que a máquina de destino é iniciada da imagem de inicialização do Live DVD, é possível iniciar a BMR. As tarefas exigidas dependem de se isso será feito na interface com o usuário do AppAssure ou na linha de comando usando o utilitário aamount. Consulte Início de uma bare metal restore no Linux.
    - Se for usado o Core Console, será preciso iniciar uma restauração em um ponto de recuperação do Core. Consulte Seleção de um ponto de recuperação e início da BMR.
    - Se for usado o Core Console, será preciso mapear os volumes na UI. Consulte Mapeamento de volumes para uma bare metal restore.
    - Como opção, ao restaurar da linha de comando, você poderá iniciar o utilitário de tela para melhorar sua capacidade de rolar e ver os comandos no console do terminal. Para obter informações, consulte Início do utilitário Screen.
    - Se usar aamount, todas as tarefas serão realizadas na linha de comando. Para obter informações, consulte Início de uma bare metal restore em uma máquina com Linux usando a linha de comando.
- **Confirmação de um bare metal restore**. Após iniciar o procedimento de bare metal restore, você pode confirmar e monitorar o progresso. Consulte Confirmação da bare metal restore na linha de comando.
    - É possível monitorar o progresso de sua restauração. Consulte Visualização do progresso da recuperação.
    - Depois de concluída, você pode iniciar o server restaurado. Consulte Início de um server de destino restaurado.
    - Solucionar problemas do processo de BMR. Consulte Solução de problemas de conexões com o Universal Recovery Console e Reparação de problemas de inicialização.

Pré-requisitos para realização de uma bare metal restore em máquinas com Linux

Antes de iniciar o processo de realização de uma bare metal restore em uma máquina com Linux, é preciso garantir que as seguintes condições e critérios estejam presentes:

- **Cópias de segurança da máquina que você deseja restaurar.** É preciso ter um AppAssure 5 Core funcional que contenha pontos de recuperação do server protegido que você deseja restaurar.
- **Hardware para restaurar (novo ou antigo, similar ou não).** A máquina de destino deve atender aos requisitos de instalação de um agente; para obter mais detalhes, consulte o *Guia de implementação do Dell AppAssure 5*.
- **Imagem de inicialização do Live DVD**. Obtenha a imagem ISO do Linux Live DVD, que inclui uma versão inicializável do Linux. Baixe-o do Portal de licenças de software da Dell em https://licenseportal.com. Se houver problemas para baixar o Live DVD, entre em contato com o suporte do Dell AppAssure.
- **Software e mídia de imagem.** Se usar mídia física, é preciso ter um CD ou DVD virgem e um software de gravação de disco ou de criação de imagem ISO.
- **Drivers do adaptador de rede e de armazenamento compatíveis.** Se a restauração for para hardware diferente, é preciso ter drivers de armazenamento compatíveis e drivers do adaptador de rede para a máquina de destino, incluindo drivers de RAID, AHCI e chipset para o sistema operacional de destino, conforme o caso.
- **Partições e espaço de armazenamento, conforme apropriado.** Certifique-se que há espaço suficiente no disco rígido para criar partições de destino na máquina de destino que conterá os volumes de origem. Todas as partições de destino devem ser pelo menos do mesmo tamanho da partição de origem original.
- **Restaurar caminho.** Identifique o caminho da restauração, que é o caminho do descritor de arquivo de dispositivo. Para identificar o caminho do descritor de arquivo de dispositivo, use o comando `fdisk` de uma janela de terminal.

Gerenciamento de uma imagem de inicialização do Linux

Uma bare metal restore para Linux exige uma imagem de inicialização do Live DVD, que pode ser baixada do Portal de licenças de software da Dell. Use essa imagem para iniciar a máquina de destino com Linux. Com base nas particularidades do seu ambiente, pode ser preciso transferir esta imagem para uma mídia física como um CD ou DVD. Você deve, então, carregar virtual ou fisicamente a imagem de inicialização e iniciar o server Linux a partir da imagem de inicialização.

NOTA: O Live DVD antes era conhecido como Live CD.

Você pode realizar as seguintes tarefas:

- Download de uma imagem ISO de inicialização para Linux
- Transferência da imagem ISO do Live DVD para mídia
- Carregamento do Live DVD e início da máquina de destino

O gerenciamento de uma imagem de inicialização do Linux é uma etapa do Roteiro de realização de uma bare metal restore em máquinas com Linux.

Download de uma imagem ISO de inicialização para Linux

A primeira etapa ao realizar uma bare metal restore (BMR) em uma máquina com Linux é baixar a imagem ISO do Live DVD para Linux do Portal de licenças de software da Dell. O Live DVD funciona com todos os sistemas de arquivo Linux suportados pelo AppAssure 5, e inclui uma versão inicializável do Linux, um utilitário de tela e a interface do Universal Recovery Console (URC) do AppAssure. O Universal Recovery Console do AppAssure 5 é um ambiente usado para restaurar a unidade do sistema ou o server inteiro diretamente do AppAssure 5 Core.

NOTA: A Organização Internacional de Padronização (ISO) é um órgão internacional de representantes de diversas organizações nacionais que define padrões para sistemas de arquivos. ISO 9660 é uma norma de sistema de arquivos usada em mídia de disco óptico para troca de dados, e ela suporta vários sistemas operacionais. Uma imagem ISO é a imagem de disco ou arquivo, que contém dados para todos os setores do disco, bem como o sistema de arquivos do disco.

É preciso baixar a imagem ISO do Live DVD que corresponde à sua versão do AppAssure 5. A versão atual do Live DVD está disponível no Portal de licenças de software da Dell em https://licenseportal.com. Se precisar de uma versão diferente, entre em contato com o Suporte do Dell AppAssure.

NOTA: Para obter mais informações sobre o Portal de licenças de software da Dell, consulte o *Guia do usuário do portal de licenças*, localizado no site de documentação de Guias e notas de versão do AppAssure em https://support.software.dell.com/appassure/release-notes-guides.

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Windows. Faz parte do processo de Gerenciamento de uma imagem de inicialização do Linux.

Execute as etapas deste procedimento para baixar a imagem ISO do Live DVD.

Para baixar uma imagem ISO de inicialização para Linux

1. Efetue login no Portal de licenças de software da Dell em https://licenseportal.com.
2. Acesse a área **Downloads**.
3. Role para baixo até Aplicativos com base em Linux e, na seção do Live DVD para Linux, clique em **Baixar**.
4. Salve a imagem ISO do Live DVD. Se você estiver restaurando uma máquina virtual, poderá salvá-la em um local de rede e definir a VM para iniciar da unidade de CD ou DVD associada à imagem ISO.
5. Se a restauração for de uma máquina física, grave a imagem ISO do CD de inicialização em um CD ou DVD a partir do qual a máquina de destino pode ser iniciada. Para obter mais informações, consulte Transferência da imagem ISO do Live DVD para mídia.

Transferência da imagem ISO do Live DVD para mídia

Quando você baixa o arquivo do Live DVD para Linux, ele é armazenado como imagem ISO no caminho especificado. Você deve ser capaz de inicializar a máquina Linux de destino com a imagem do Live DVD.

É possível gravar a imagem ISO do CD de inicialização em mídia de CD ou DVD.

Se a máquina for iniciada do Live DVD, o Universal Recovery Console será iniciado automaticamente.

Caso esteja realizando uma BMR em uma máquina virtual, esta etapa não é necessária. Basta carregar a imagem ISO em uma unidade e editar as definições dessa VM para iniciar essa unidade.

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Windows. Faz parte do processo de Gerenciamento de uma imagem de inicialização do Linux.

Carregamento do Live DVD e início da máquina de destino

Depois de obter a imagem ISO do Live DVD, é preciso iniciar a máquina Linux com o Live DVD recém-criado.

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Windows. Faz parte do processo de Gerenciamento de uma imagem de inicialização do Linux.

Para carregar um Live DVD e iniciar a máquina de destino

1. Navegue até o novo server e carregue a imagem do Live DVD a partir do local apropriado. Especifique se o server será iniciado da imagem do Live DVD.
2. Inicie a máquina.

   É exibida uma tela de abertura do AppAssure e uma janela de terminal se abre, exibindo o endereço IP e a senha de autenticação da máquina.

   NOTA: Uma nova senha temporária é gerada cada vez que a máquina é iniciada com a imagem do Live DVD.
3. Anote o endereço IP e a senha de autenticação exibidos na tela de introdução. Você precisará dessas informações durante o processo de recuperação de dados para acessar novamente o console.

Depois que a máquina de destino com Linux é iniciada com o Live DVD, essa máquina fica pronta para o usuário se conectar a ela a partir do Core para iniciar o processo de bare metal restore. É possível realizar esse processo usando um de dois métodos:

- Ativação de uma restauração a partir do AppAssure 5 Core Console. Para obter mais informações, consulte Início de uma bare metal restore no Linux.
- Ativação de uma restauração a partir da linha de comando usando o utilitário aamount. Para obter mais informações, consulte Início de uma bare metal restore em uma máquina com Linux usando a linha de comando.

Gerenciamento de partições Linux

Ao realizar uma BMR, a unidade de destino na qual você restaurará os dados deve ter as mesmas partições do ponto de recuperação que está sendo restaurado. Talvez seja necessário criar partições para atender a esse requisito.

É possível iniciar a restauração na linha de comando usando o utilitário aamount ou no AppAssure 5 Core Console. Se a restauração for feita usando a interface com o usuário, primeiro será preciso montar as partições.

Você pode realizar as seguintes tarefas:

- Criação de partições na unidade de destino
- Formatação de partições na unidade de destino
- Montagem de partições a partir da linha de comando

O gerenciamento de partições no Linux é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Linux.

Criação de partições na unidade de destino

Muitas vezes, ao fazer uma BMR, a unidade de destino é um novo volume que pode ser composto de uma única partição. A unidade na máquina de destino deve ter a mesma tabela de partições do ponto de recuperação, incluindo o tamanho dos volumes. Se a unidade de destino não contiver as mesmas partições, será preciso criá-las antes de realizar a bare metal restore. Use o utilitário fdisk para criar partições na unidade de destino iguais às partições na unidade de origem.

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Linux. Faz parte do processo de Gerenciamento de partições Linux.

Para criar partições na unidade de destino

1 Como opção, você pode iniciar o utilitário Screen. Depois de iniciado, ele permanece ativo até que você reinicialize a máquina.

> **NOTA:** Para obter mais informações, consulte Início do utilitário Screen.

2 Na linha de comando, insira o seguinte comando e pressione **Enter** para alterar os privilégios para execução como administrador e depois relacionar as partições de disco existentes:

```
sudo fdisk -l
```

Uma lista com todos os volumes é exibida.

Esse exemplo supõe que o volume que você deseja particionar é /dev/sda. Se seu volume é diferente (por exemplo, em unidades mais antigas, pode ser /dev/hda), altere os comandos adequadamente.

3 Para criar uma nova partição de inicialização, insira o seguinte comando e pressione **Enter**:

```
sudo fdisk /dev/sda
```

4 Para criar uma nova partição de inicialização, insira o seguinte comando e pressione **Enter**:

```
n
```

5 Para criar uma nova partição primária, insira o seguinte comando e pressione **Enter**:

```
p
```

6 Para especificar o número de partição, insira-o e pressione **Enter**. Por exemplo, para especificar a partição 1, digite 1 e, em seguida, pressione **Enter**.

7 Para usar o primeiro setor, 2048, pressione **Enter**.

8 Aloque uma quantidade adequada para a partição de inicialização, inserindo o sinal de mais e a quantidade de alocação e pressionando **Enter**.

Por exemplo, para alocar 500 M para a partição de inicialização, digite o seguinte e pressione **Enter**:

```
+500M
```

9 Para alternar um sinalizador inicializável para a partição de inicialização (para tornar a partição inicializável), digite o seguinte comando e pressione **Enter**:

```
a
```

10 Para atribuir um sinalizador inicializável à partição adequada, digite o número da partição e pressione **Enter**. Por exemplo, para atribuir um sinalizador inicializável para a partição 1, digite 1 e pressione **Enter**.

11 Para salvar todas as alterações no utilitário fdisk, digite o seguinte comando e pressione **Enter**:

```
w
```

Formatação de partições na unidade de destino

Depois de criar partições em um novo volume na unidade de destino, você deverá formatá-las antes que elas sejam montadas. Se essa situação se aplicar a você, siga este procedimento para formatar partições em formatos Ext3, Ext4 ou XFS.

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Linux. Faz parte do processo de Gerenciamento de partições Linux.

Para formatar partições na unidade de destino

1 Como opção, você pode iniciar o utilitário Screen. Depois de iniciado, ele permanece ativo até que você reinicialize a máquina.

> **NOTA:** Para obter mais informações, consulte Início do utilitário Screen.

2 Na linha de comando, insira o seguinte comando e pressione **Enter** para alterar os privilégios para execução como administrador e depois relacionar as partições de disco existentes:

```
sudo fdisk -l
```

Uma lista com todos os volumes é exibida.

Esse exemplo supõe que a partição que você deseja formatar é /dev/sda1. Se seu volume é diferente (por exemplo, em unidades mais antigas, pode ser /dev/hda), altere os comandos adequadamente.

3 Selecione um dos seguintes comandos dependendo do formato que você deseja utilizar a partição de destino:

- Para formatar uma partição no formato Ext3, insira o seguinte comando e pressione **Enter**:

  ```
  sudo mkfs.ext3 /dev/sda1
  ```

- Para formatar uma partição no formato Ext4, insira o seguinte comando e pressione **Enter**:

  ```
  sudo mkfs.ext4 /dev/sda1
  ```

- Para formatar uma partição no formato xfs, insira o seguinte comando e pressione **Enter**:

  ```
  sudo mkfs.xfs /dev/sda1
  ```

A partição selecionada é formatada de acordo.

4 De forma opcional, se você precisar formatar outras partições, repita esse procedimento.

Montagem de partições a partir da linha de comando

Se for feita uma BMR usando o AppAssure 5 Core Console, será preciso primeiro montar as partições adequadas na máquina de destino. Realize isso na linha de comando do Universal Recovery Console.

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Linux. Faz parte do processo de Gerenciamento de partições Linux.

Execute as etapas deste procedimento para montar partições na máquina com Linux antes de fazer uma restauração.

Para montar partições a partir da linha de comando

1 Na linha de comando, insira o seguinte comando e pressione **Enter** para alterar os privilégios para execução como administrador e depois relacionar as partições de disco existentes:

```
sudo fdisk -l
```

Uma lista com todos os volumes é exibida.

2 Formate todas as partições de que precisará para realizar a BMR no diretório de montagem. Elas devem corresponder aos volumes do ponto de recuperação. Por exemplo, se o volume que você deseja montar é chamado sda1 e o diretório de montagem é mnt, digite o seguinte comando e pressione **Enter**:

3 Monte todas as partições de que precisará para realizar a BMR no diretório de montagem. Elas devem corresponder aos volumes do ponto de recuperação. Por exemplo, se o volume que você deseja montar é chamado sda1 e o diretório de montagem é mnt, digite o seguinte comando e pressione **Enter**:

```
mount /dev/sda1 /mnt
```

4 Repita a Etapa 3 conforme necessário até ter montado todos os volumes necessários.

Depois que os volumes estiverem montados, é possível fazer uma restauração para a máquina com Linux de destino a partir do AppAssure 5 Core Console. Consulte Início de uma bare metal restore no Linux.

Início de uma bare metal restore no Linux

Antes de iniciar uma bare metal restore (BMR) em uma máquina com Linux, certas condições devem ser satisfeitas.

Para restaurar um ponto de recuperação salvo no Core, é necessário ter o hardware apropriado disponível. Para obter mais informações, consulte Pré-requisitos para realização de uma bare metal restore em máquinas com Linux.

A máquina com Linux de destino da BMR deve ser iniciada usando a imagem de inicialização do Live DVD. Para obter mais informações, consulte Gerenciamento de uma imagem de inicialização do Linux.

O número de volumes na máquina com Linux a ser restaurada deve corresponder ao número de volumes no ponto de recuperação. Também é preciso decidir se deseja restaurar a partir do AppAssure 5 Core Console ou da linha de comando usando aamount. Para obter mais informações, consulte Gerenciamento de partições Linux.

Se a restauração for feita a partir da UI do Core Console, a primeira etapa para iniciar a BMR é selecionar o ponto de recuperação apropriado, depois iniciar a restauração no hardware especificando o endereço IP e uma senha temporária obtida a partir do Universal Recovery Console. A seguir, você precisa mapear as unidades e iniciar a restauração.

Para iniciar uma BMR no AppAssure 5 Core Console, realize as seguintes tarefas.

- Seleção de um ponto de recuperação e início da BMR
- Mapeamento de volumes para uma bare metal restore
- Seleção de um ponto de recuperação e início da BMR

Se a restauração for feita da linha de comando usando o utilitário aamount, primeiro será preciso definir os privilégios apropriados, montar volumes, executar o aamount, obter informações sobre o Core na lista de máquinas, conectar-se ao core, obter uma lista de pontos de recuperação, selecionar o ponto de recuperação do qual deseja reverter em bare metal restore e iniciar a restauração.

Como opção, você pode iniciar o utilitário Screen.

Para iniciar uma BMR na linha de comando, realize as tarefas a seguir.

- Início do utilitário Screen
- Início de uma bare metal restore em uma máquina com Linux usando a linha de comando

Esse processo é uma etapa do Roteiro de realização de uma bare metal restore em máquinas com Windows.

Início do utilitário Screen

O Live DVD inclui o utilitário Screen, disponível ao inicializar a partir do Live DVD no Universal Recovery Console. O Screen permite aos usuários gerenciar vários shells simultaneamente em uma única sessão Secure Shell (SSH) ou janela de console. Isso permite realizar uma tarefa em uma janela de terminal (como confirmar volumes montados) e, enquanto isso é executado, abrir ou alternar para outra instância de shell e realizar outra tarefa (como executar o utilitário aamount).

O utilitário Screen também tem seu próprio buffer de rolagem para trás, o que permite rolar a tela para ver maiores quantidades de dados, como a lista de pontos de recuperação.

NOTA: O utilitário Screen é fornecido para sua conveniência; seu uso é opcional.

O utilitário Screen inicia na máquina inicializada com o Live DVD por padrão. Contudo, se você fechou esse aplicativo, é preciso iniciar o utilitário Screen a partir do Live DVD usando o procedimento abaixo.

Para iniciar o utilitário Screen

- Se a máquina foi inicializada a partir do Live DVD, na janela do terminal, digite **screen** e pressione **Enter**.

  O utilitário Screen é iniciado.

Início de uma bare metal restore em uma máquina com Linux usando a linha de comando

Depois que a imagem ISO do Live DVD estiver acessível na máquina na qual você deseja realizar uma BMR e o número e tamanho dos volumes forem correspondentes entre a máquina de destino e o ponto de recuperação no qual deseja executar a bare metal restore, será possível iniciar essa restauração na linha de comando usando o utilitário `aamount`.

Se desejar realizar uma BMR usando a UI do AppAssure 5 Core Console, consulte Seleção de um ponto de recuperação e início da BMR.

NOTA: Ao realizar este procedimento, não tente montar pontos de recuperação na pasta /tmp, que contém os arquivos aavdisk.

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Linux. Faz parte do processo de Início de uma bare metal restore em uma máquina com Linux usando a linha de comando.

Execute as etapas deste procedimento para selecionar um ponto de recuperação no Core para reverter para a máquina de destino física ou virtual da BMR.

Para realizar uma bare metal restore em uma máquina com Linux usando a linha de comando

1 Para executar o utilitário AppAssure `aamount` como raiz, digite o seguinte comando e pressione **Enter**:

```
sudo aamount
```

2 Para relacionar as máquinas protegidas, digite o seguinte comando e pressione **Enter**:

```
lm
```

3 Quando solicitado, insira as informações de conexão do AppAssure 5 Core, como descrito na tabela a seguir, e pressione **Enter** após cada comando obrigatório:

Tabela 87.

Caixa de texto	Descrição	Obrigatório
Endereço IP do AppAssure Core ou nome de host	O endereço IP ou nome de host do AppAssure 5 Core.	Sim
Domínio	O domínio do AppAssure 5 Core. Opcional.	Não
Usuário	O nome de usuário de um usuário administrativo no Core	Sim
Senha	A senha usada para conectar o usuário administrativo ao Core.	Sim

Aparece uma lista que mostra as máquinas protegidas pelo AppAssure 5 Core. Ela relaciona as máquinas encontradas por número de item de linha, nome de exibição do host ou endereço IP e número de ID da máquina.

4 Para relacionar os pontos de recuperação da máquina que você deseja restaurar, digite o comando Relacionar os pontos de recuperação usando a seguinte sintaxe e pressione **Enter**:

```
lr <machine_line_item_number>
```

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

Uma lista exibe os pontos de recuperação de base e incremental da máquina. Essa lista inclui:

- Número de item de linha
- Carimbo de data e hora
- Uma lista de volumes com letras dentro do ponto de recuperação
- Localização do volume

- Tamanho do ponto de recuperação
- Um número de ID do volume que inclui um número de sequência no fim, identificando o ponto de recuperação

5 Para selecionar o ponto de recuperação de uma restauração, insira o seguinte comando e pressione **Enter**:

```
r <recovery_point_ID_number> <caminho>
```

CUIDADO: É preciso garantir que o volume do sistema não esteja montado.

NOTA: Se a máquina foi iniciada do Live DVD, o volume do sistema não estará montado.

Esse comando reverte a imagem do volume especificada pelo ID do Core para o caminho especificado. O caminho da restauração é o do descritor de arquivo de dispositivo e não o diretório no qual está montado.

NOTA: Você também pode especificar um número de linha no comando em vez do número de ID do ponto de recuperação para identificar o ponto de recuperação. Nesse caso, use o número de linha de agente/máquina (da saída `lm`), seguido do número da linha do ponto de recuperação e da letra de volume (da lista de volumes com letras dentro do ponto de recuperação), seguidos pelo caminho. Por exemplo:

```
r <machine_line_item_number> <base_image_recovery_point_line_number>
<volume_letter> <caminho>
```

Por exemplo, digite:

```
r 1 24 a /dev/sda1
```

Nesse comando, *<caminho>* é o descritor de arquivo do volume real.

6 Quando solicitado a continuar, insira **y**, para Sim, e pressione **Enter**.

Depois que a restauração iniciar, uma série de mensagens será exibida para notificá-lo do status de conclusão da restauração.

NOTA: Se você receber uma mensagem de exceção, os detalhes sobre essa exceção poderão ser encontrados no arquivo aamount.log. O arquivo aamount.log encontra-se em /var/log/appassure.

7 Depois de uma restauração bem-sucedida, saia do aamount digitando `exit` e pressione **Enter**.

8 A próxima etapa é confirmar a restauração. Para obter mais informações, consulte Confirmação da bare metal restore na linha de comando.

Confirmação da bare metal restore na linha de comando

A Dell recomenda realizar as seguintes etapas para confirmar se uma bare metal restore foi concluída na linha de comando.

- Realização de uma verificação do sistema de arquivos no volume restaurado
- Criação de partições inicializáveis na máquina com Linux restaurada usando a linha de comando

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Linux.

Realização de uma verificação do sistema de arquivos no volume restaurado

Depois de executar uma bare metal restore na linha de comando, você deve realizar uma verificação do sistema de arquivos no volume restaurado para garantir que os dados restaurados do ponto de recuperação não foram corrompidos.

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Linux. Faz parte do processo de Confirmação da bare metal restore na linha de comando.

Realize a tarefa abaixo para realizar uma verificação do sistema de arquivos no volume restaurado.

Para realizar uma verificação do sistema de arquivos no volume restaurado

1. Na linha de comando do Universal Recovery Console da máquina com Linux que você restaurou, para confirmar se as partições adequadas estão montadas, digite o seguinte comando e pressione **Enter**:

   ```
   df
   ```

2. Se o volume restaurado não estiver montado, vá para a Etapa 3. Se o volume restaurado estiver montado, desmonte-o digitando o seguinte comando e pressionando **Enter**:

   ```
   umount <volume>
   ```

3. Execute uma verificação do sistema de arquivos nos volumes restaurados digitando o seguinte comando e pressionando Enter:

   ```
   fsck <volume>
   ```

   Se o retorno do fsck for limpo, o sistema de arquivos estará confirmado.

4. Monte os volumes adequados novamente digitando o seguinte comando no formato `mount <volume> <pasta>` e depois pressione **Enter**.

   Por exemplo, se o caminho do volume for prod/sda1 e a pasta que você deseja montar for mnt, digite o seguinte e pressione **Enter**:

   ```
   mount /dev/sda1 /mnt
   ```

Criação de partições inicializáveis na máquina com Linux restaurada usando a linha de comando

Depois de executar uma verificação limpa do sistema de arquivos no volume restaurado, crie partições inicializáveis.

O GNU Grand Unified Bootloader (GRUB) é um carregador de inicialização que permite aos administradores configurar qual sistema operacional ou configuração de kernel específica será utilizado para iniciar o sistema. Após uma BMR, o arquivo de configuração do GRUB deve ser modificado para que a máquina use o identificador universal exclusivo (UUID) apropriado para o volume raiz. Antes dessa etapa, é preciso montar os volumes raiz e de inicialização e verificar os UUIDs de cada um. Isso garante que você consiga inicializar a partir da partição.

NOTA: Esse procedimento aplica-se a máquinas com Linux que executam o SLES e CentOS/RHEL, que utilizam GRUB1. Se estiver utilizando o Ubuntu, que utiliza o GRUB2, é possível usar uma ferramenta para inicializar e reparar o GRUB2. Um exemplo de uma ferramenta adequada para a ferramenta Boot-Repair documentada pode ser encontrado em https://help.ubuntu.com/community/Boot-Repair.

Essa tarefa é uma das etapas do Roteiro de realização de uma bare metal restore em máquinas com Linux. Faz parte do processo de Confirmação da bare metal restore na linha de comando.

Realize a tarefa abaixo para criar partições inicializáveis usando a linha de comando.

Para criar partições inicializáveis em uma máquina com Linux utilizando a linha de comando

1 Na linha de comando do Universal Recovery Console da máquina com Linux que você restaurou, anexe todos os dispositivos usando o utilitário bsctl com o seguinte comando como raiz:

```
sudo bsctl --attach-to-device /<restored volume path>
```

Por exemplo, se o caminho do volume for dev/sda1 e a pasta que você deseja montar for mnt, digite o seguinte e pressione **Enter**:

```
sudo bsctl --attach-to-device /dev/sda1 mnt
```

2 Repita essa etapa para cada volume restaurado.

3 É preciso montar o volume raiz primeiro e, depois, o volume de inicialização. Monte cada volume restaurado usando os seguintes comandos:

a Para montar o volume raiz, digite o seguinte comando e pressione **Enter**:

```
mount /<restored volume[root]> /mnt
```

Por exemplo, se /dev/sda2 for o volume raiz, digite **mount /dev/sda2 /mnt** e pressione **Enter**.

b Para montar o volume de inicialização, digite o seguinte comando e pressione **Enter**:

```
mount /<restored volume[boot]> /mnt/boot
```

Por exemplo, se /dev/sda1 for o volume de inicialização, digite **mount /dev/sda1 /mnt/boot** e pressione **Enter**.

> **NOTA:** Algumas configurações do sistema podem incluir o diretório de inicialização como parte do volume raiz.

4 Se o tamanho do volume estiver aumentando, ou seja, se o volume de destino da nova máquina com Linux for maior do que o volume no ponto de recuperação, será preciso excluir todos os arquivos de dados de bitmap existentes e recriá-los, conforme descrito da Etapa 5 à Etapa 8,

Se os volumes de origem e de destino forem do mesmo tamanho, vá para Etapa 9 a fim de redefinir o armazenamento de bitmap.

Em ambas as situações, será preciso mapeá-los, como descrito na Etapa 10.

> **CUIDADO: Essa é uma etapa crítica antes de mapear volumes. Se você mapear um volume e, em seguida, excluir o arquivo manualmente, poderá corromper o volume.**

5 Se o tamanho do volume estiver aumentando, exclua o armazenamento de dados existente digitando o seguinte comando e pressionando **Enter**:

```
rm -rf <mount point>/.blksnap/data
```

Por exemplo, se o seu volume restaurado foi montado em /mnt/sda1, digite o seguinte comando e pressione **Enter**:

```
rm -rf /mnt/sda1/.blksnap/data
```

6 Agora, é preciso excluir o armazenamento de bitmap existente digitando o seguinte comando e pressionando **Enter**:

```
rm -rf <mount point>/.blksnap/bitmap
```

Por exemplo, se o seu volume restaurado foi montado em /mnt/sda1, digite o seguinte comando e pressione **Enter**:

```
rm -rf /mnt/sda1/.blksnap/bitmap
```

7 Se você tiver excluído os armazenamentos de dados e de bitmap existentes, recrie o armazenamento de dados digitando o seguinte comando e pressionando **Enter**:

```
sudo bsctl --create-data-store <restored root volume path>
```

Por exemplo, digite o seguinte comando e pressione **Enter**:

```
sudo bsctl --create-data-store /dev/sda1
```

8 Repita isso para o armazenamento de bitmap digitando o seguinte comando e pressionando **Enter**:

```
sudo bsctl --create-bitmap-store <restored root volume path>
```

Por exemplo, digite o seguinte comando e pressione **Enter**:

```
sudo bsctl --create-bitmap-store /dev/sda1
```

9 Se os volumes de origem e de destino forem do mesmo tamanho, redefina o armazenamento de bitmap digitando o seguinte comando e pressionando **Enter**:

```
sudo bsctl --reset-bitmap-store <restored volume path>
```

Por exemplo, digite o seguinte comando e pressione **Enter**:

```
sudo bsctl --reset-bitmap-store /dev/sda1
```

10 Para todas as situações, mapeie os metadados de snapshot de cada volume restaurado usando o seguinte comando e, em seguida, pressione **Enter**:

```
sudo bsctl --map-bitmap-store <restored volume path>
```

Por exemplo, digite o seguinte comando e pressione **Enter**:

```
sudo bsctl --map-bitmap-store /dev/sda1
```

11 Confirme se os dispositivos estão mapeados digitando **bsctl -l** pressionando **Enter**.

12 Obtenha o identificador universal exclusivo (UUID) dos novos volumes usando o comando `blkid`. Digite o seguinte comando e pressione **Enter**:

```
blkid [volume]
```

NOTA: Também é possível usar o comando `ls -l /dev/disk/by-uuid`.

13 Obtenha o UUID por meio de `mount /etc/fstab` e compare-o aos UUIDs dos volumes raiz (para Ubuntu e CentOS) e de inicialização (para CentOS e RHEL) digitando o seguinte comando e pressionando **Enter**:

```
less /mnt/etc/fstab
```

14 Obtenha o UUID por meio de `mount /etc/mtab` e compare-o aos UUIDs dos volumes raiz (para Ubuntu e CentOS) e de inicialização (para CentOS e RHEL) digitando o seguinte comando e pressionando **Enter**:

```
less /mnt/etc/mtab
```

15 Se a BMR estiver sendo realizada em um disco novo na máquina de destino, comente a partição de swap em fstab no seu volume raiz.

16 A modificação dos caminhos fstab e mtab deve ocorrer no volume restaurado e não no Live DVD. Não há necessidade de modificar os caminhos do Live DVD. Prepare a instalação do Grand Unified Bootloader (GRUB) digitando os seguintes comandos. Depois de cada comando, pressione **Enter**:

```
mount --bind /dev /mnt/dev
```

```
mount --bind /proc /mnt/proc
```

17 Localize o arquivo `grub.conf` em seu volume montado e abra-o usando um editor de texto.

A localização do grub.conf varia dependendo das versões do OS e do GRUB instalado. As localizações mais prováveis incluem **<root path>/boot/grub/grub.conf**, **<root path>/boot/grub/grub.cfg** ou **<root path>/etc/grub.conf**.

18 No grub.conf, localize todas as linhas que contêm “root=<root device uuid>” e substitua-o pelo UUID correto do volume raiz. Caso contrário, atualize cada instância para root=<root device uuid>. Também é possível usar o caminho do dispositivo raiz. Como nos exemplos acima, se o caminho do dispositivo raiz for /dev/sda2, altere todas as instâncias para root=/dev/sda2.

19 Remova todas as entradas “rd_LVM_LV=” do arquivo grub.conf, salve o arquivo e saia do editor de texto.

20 Altere o diretório raiz digitando o seguinte comando e pressionando **Enter**:

```
chroot /mnt /bin/bash
```

21 Se estiver usando o SLES, instale o GRUB digitando os seguintes comandos, pressionando **Enter** depois de cada um:

```
grub-install.unsupported --recheck /dev/sda
grub-install.unsupported /dev/sda
grub-install --recheck /dev/sda
grub-install /dev/sda
```

22 Para distribuições Linux que não sejam o SLES, instale o GRUB digitando o seguinte comando e pressionando **Enter**:

```
grub-install/dev/sda
```

> **NOTA:** Se for instalar em SUSE, ao instalar o GRUB, não serão necessários parâmetros. Por exemplo, o comando para instalar o GRUB em SUSE é simplesmente grub-install. Depois, pressione **Enter**.

23 Remova o disco do Live DVD da unidade de CD-ROM ou DVD e reinicie a máquina com Linux.

Visualização de tarefas, alertas e eventos

A guia Eventos no Core Console exibe um log de todos os eventos de sistema relacionados ao AppAssure 5 Core. Ao visualizar a guia Eventos de uma máquina selecionada, você vê um log de todos os eventos do sistema relacionados a essa máquina específica.

O conteúdo da guia Eventos está dividido em três seções: Tarefas, Alertas e Eventos, onde você pode visualizar detalhes sobre cada evento, conforme apropriado.

É possível definir a forma de notificação de vários eventos configurando os grupos de notificação. Para obter mais informações, consulte Configuração de grupos de notificação.

Execute as etapas dos procedimentos abaixo para visualizar as tarefas, alertas ou todos os eventos, respectivamente.

Visualização de tarefas

Uma tarefa é um trabalho que o AppAssure 5 Core deve realizar, como transferir dados em uma cópia de segurança programada regular ou realizar uma restauração a partir de um ponto de recuperação.

Quando uma tarefa está em execução, ela é relacionada no menu suspenso Tarefas em execução no alto do Core Console.

Também é possível visualizar todas as tarefas do AppAssure 5 Core ou todas as tarefas associadas a uma máquina específica.

Para visualizar as tarefas

1 Para visualizar todas as tarefas do AppAssure 5 Core, navegue até a guia Inicial do AppAssure 5 Core e clique na guia **Eventos**.

Se você quiser visualizar as tarefas de uma máquina protegida específica, navegue até a guia Eventos dessa máquina.

2 Para visualizar apenas as tarefas, no canto superior esquerdo da página, clique em **Tarefas**.

A lista de eventos é filtrada para exibir apenas as tarefas do Core ou da máquina selecionada.

3 Como opção, para filtrar a lista de tarefas por palavra-chave, data inicial, data final ou qualquer combinação, faça o seguinte:

a Para filtrar por palavra-chave, insira-a na caixa de texto Pesquisar palavra-chave.

b Para filtrar por data e hora inicial, insira-as utilizando uma das seguintes opções:

- Na caixa de texto De, digite a data e hora em formato MM/DD/AAAA HH:MM AM/PM. Por exemplo, para pesquisar a partir do primeiro dia de janeiro de 2014 às 8h da manhã, insira 1/1/2013 8:00 AM.
- Para selecionar a data e hora atuais, clique no widget Calendário na caixa de texto De e clique em **Agora**.
- Clique no widget Calendário, selecione a data e a hora usando o calendário e os controles deslizantes e, em seguida, clique em **Concluído**.

c Para refinar ainda mais a lista de tarefas que aparece, você também pode definir uma data e hora final no mesmo formato.

A lista de tarefas é filtrada imediatamente com base nos critérios selecionados.

4 Como opção, você pode filtrar as tarefas que aparecem na lista da seguinte forma:

- Para ver apenas as tarefas ativas, clique no ícone **Tarefas ativas**.
- Para ver apenas as tarefas que estão esperando para serem realizadas, clique no ícone **Tarefas em espera**.
- Para ver apenas as tarefas que foram concluídas, clique no ícone **Tarefas concluídas**.
- Para ver apenas as tarefas com falha, clique no ícone **Tarefas com falha**.

5 Para exportar a lista de tarefas, selecione um formato na lista e clique em **Exportar o relatório**.

É possível exportar usando os seguintes formatos:

Tabela 88.

Formato	Descrição
PDF	Portable Document Format
XLS	Pasta de trabalho do Excel 1997 - 2003
XLSX	Pasta de trabalho do Excel
RTF	Rich Text Format
CSV	Valores separados por vírgula

6 Clique no ícone **Detalhes do trabalho** de qualquer tarefa para iniciar uma nova janela com os detalhes da tarefa, incluindo:

- Hora inicial
- Hora final
- Status
- Tempo decorrido
- Progresso
- Taxa
- Trabalho total (porcentagem concluída)
- Tarefas subordinadas, se for o caso

Visualização de alertas

Um alerta é uma notificação relacionada a uma tarefa ou evento. Os tipos de alertas incluem erros, avisos ou informações.

É possível exibir todos os alertas do AppAssure 5 Core ou todos os alertas associados a uma máquina específica.

Para visualizar alertas

1 Para exibir todos os alertas do AppAssure 5 Core, navegue até a guia Início do AppAssure 5 Core e clique na guia **Eventos**.

Se você quiser visualizar os alertas de uma máquina protegida específica, navegue até a guia Eventos dessa máquina.

2 Para visualizar apenas os alertas, no canto superior esquerdo da página, clique em **Alertas**.

A lista de eventos é filtrada para exibir apenas os alertas do Core ou da máquina selecionada.

3 De forma opcional, se você quiser remover todos os alertas, clique em **Descartar tudo**.

Visualização de todos os eventos

É possível visualizar todos os eventos de um AppAssure 5 Core ou todos os eventos associados a uma máquina específica.

Para visualizar eventos

1 Para visualizar todos os eventos do AppAssure 5 Core, navegue até a guia **Inicial** do AppAssure 5 Core e clique na guia **Eventos**.

Se você quiser visualizar os eventos de uma máquina protegida específica, navegue até a guia Eventos dessa máquina.

2 Para visualizar todos os eventos, no canto superior esquerdo da página, clique em **Eventos**.

Todos os eventos são exibidos para o Core ou a máquina selecionada.

4

Proteção de clusters de servers

Este capítulo descreve como proteger informações nos clusters do Microsoft SQL Server ou Exchange Server usando o AppAssure 5. Os seguintes tópicos estão incluídos:

Sobre a proteção de cluster de servers no AppAssure 5

No AppAssure 5, a proteção de cluster de servers está associada aos AppAssure 5 Agents instalados em nós de cluster individuais (ou seja, máquinas individuais no cluster) e ao AppAssure 5 Core, que protege esses agentes como se fossem uma máquina composta.

É fácil configurar um AppAssure 5 Core para proteger e gerenciar um cluster. No Core Console, um cluster é organizado como entidade separada, que atua como contêiner que inclui os nós relacionados. Por exemplo, na área de navegação à esquerda, no menu Máquinas protegidas, os clusters protegidos são relacionados. Diretamente abaixo de cada cluster, os nós individuais associados ou máquinas agente aparecem. Cada um desses é uma máquina protegida na qual o software AppAssure 5 Agent é instalado. Se você clicar no cluster, a guia aparece no Core Console

Nos níveis de Core e cluster, é possível visualizar informações sobre o cluster, como a lista de nós relacionados e volumes compartilhados. Um cluster aparece no Core Console na guia Nós protegidos e é possível alternar a visualização (usando Exibir/ocultar) para visualizar os nós incluídos no cluster. No nível de cluster, também é possível visualizar os metadados de clusters correspondentes do Exchange e SQL para os nós do cluster. É possível especificar definições para todo o cluster e os volumes compartilhados nesse cluster ou então navegar até um nó (máquina) individual do cluster para configurar as definições apenas para esse nó e os volumes locais associados.

Aplicativos e tipos de cluster suportados

Para proteger seu cluster corretamente, é preciso ter o AppAssure 5 Agent instalado em cada uma das máquinas ou nós do cluster. O AppAssure 5 suporta as versões de aplicativos e as configurações de cluster relacionadas na tabela a seguir.

Tabela 89.

Aplicativo	Versão do aplicativo e configuração do cluster relacionado	Cluster de ativação pós-falha do Windows
Microsoft Exchange Server	2007 Single Copy Cluster (SCC) 2007 Cluster Continuous Replication (CCR)	2003, 2008, 2008 R2
	2010 Grupo de disponibilidade de banco de dados (DAG)	2008, 2008 R2
	2013 Grupo de disponibilidade de banco de dados (DAG)	2008 R2 SP1, 2012, 2012 R2
Microsoft SQL Server	2005	2003, 2008, 2008 R2
	2008, 2008 R2 Single Copy Cluster (SCC)	2003, 2008, 2008 R2, 2012, 2012 R2
	2012, 2014 Single Copy Cluster (SCC)	2008, 2008 R2, 2012, 2012 R2
	2012, 2014 Grupos de Disponibilidade	Server 2012, 2012 R2

Os tipos de disco suportados incluem:

- Discos de tabela de partição GUID (GPT) maiores que 2 TB
- Discos básicos

Os tipos de montagem suportados incluem:

- Unidades compartilhadas conectadas como letras de unidade (por exemplo, D:)
- Volumes dinâmicos simples em um único disco físico (volumes não distribuídos, espelhados ou estendidos)
- Unidades compartilhadas conectadas como pontos de montagem

Suporte Limitado para Cluster Shared Volumes

O AppAssure 5 suporta a cópia de segurança nativa de cluster shared volumes (CSV) somente nos agentes do Windows 2008 R2.

- O suporte para cluster shared volumes é limitado a agentes que usam o Windows 2008 R2.
- Para outros sistemas operacionais, o serviço do agente pode ser executado em todos os nós em um cluster e o cluster pode ser protegido como um cluster dentro do AppAssure core. No entanto, os volumes compartilhados por cluster não serão exibidos no Core Console e não estarão disponíveis para proteção. Todos os discos locais (como o volume do sistema operacional) estarão disponíveis para proteção.

A tabela a seguir descreve o suporte atual no AppAssure 5 Core para cluster shared volumes.

Tabela 90. Compatibilidade para cluster shared volumes no AppAssure 5

Suporte aos cluster shared volumes no AppAssure 5	Proteger, replicar, rollup, montar arquivo		Reverter/restaurar volumes CSV		Exportação virtual para Hyper-V CSV	
Versão do AppAssure	5.3	5.4	5.3	5.4	5.3	5.4
Windows 2008 R2	Sim	Sim	Não	Sim	Sim	Sim

Tabela 90. Compatibilidade para cluster shared volumes no AppAssure 5

Suporte aos cluster shared volumes no AppAssure 5	Proteger, replicar, rollup, montar arquivo		Reverter/restaurar volumes CSV		Exportação virtual para Hyper-V CSV	
Windows 2012	Não	Não	Não	Não	Não	Não
Windows 2012 R2	Não	Não	Não	Não	Não	Não

Proteção de um cluster

Este tópico descreve como adicionar um cluster para proteção no AppAssure 5. Ao adicionar um cluster para proteção, você precisa especificar o nome do host ou endereço IP do cluster, o aplicativo de cluster ou um dos nós do cluster ou máquinas que inclui o AppAssure 5 Agent.

NOTA: Um repositório é usado para armazenar os snapshots de dados capturados a partir de seus nós protegidos. Antes de começar a proteger os dados em seu cluster, você deve ter definido pelo menos um repositório associado ao seu AppAssure 5 Core.

Para obter informações sobre definição de repositórios, consulte Sobre repositórios.

Para proteger um cluster

1 No Core Console, navegue até a guia Inicial e clique no botão **Proteger cluster**.

2 Na caixa de diálogo Conectar-se ao cluster, insira as seguintes informações e depois clique em **Conectar**.

Tabela 91.

Caixa de texto	Descrição
Host	O nome do host ou endereço IP do cluster, o aplicativo de cluster ou um dos nós do cluster.
Port	O número da porta na máquina pela qual o AppAssure 5 Core se comunica com o Agent. A porta padrão é 8006.
Nome de usuário	O nome de usuário do administrador de domínio usado para se conectar a essa máquina; por exemplo, domain_name\administrator ou administrator@domain_name.com **NOTA:** O nome de domínio é obrigatório. Não é possível conectar-se ao cluster usando o nome de usuário do administrador local.
Senha	A senha usada para se conectar à máquina.

3 Na caixa de diálogo Proteger cluster, selecione um repositório para esse cluster.

4 Para proteger o cluster com base em definições padrão, selecione os nós de proteção padrão e clique em **Proteger**.

NOTA: As definições padrão garantem que todos os volumes sejam protegidos com uma programação a cada 60 minutos.

5 Para inserir as definições personalizadas do cluster (por exemplo, para personalizar a programação de proteção dos volumes compartilhados), faça o seguinte:

a Clique em **Definições**.

b Na caixa de diálogo Volumes, selecione o(s) volume(s) a proteger e clique em **Editar**.

c Na caixa de diálogo Programação de proteção, selecione uma das opções de programação para proteger seus dados, conforme descrito na tabela a seguir.

Tabela 92.

Caixa de texto	Descrição

Intervalo	Você pode selecionar dentre:
	• **Dia da semana.** Para proteger dados em um intervalo específico, selecione **Intervalo**, e depois:
	  • Para personalizar quando proteger os dados durante os horários de pico, você pode especificar uma hora inicial, hora final e um intervalo.
	  • Para proteger dados nas horas fora do pico, marque a caixa de seleção **Proteger fora dos horários de pico** e selecione um intervalo para a proteção.
	• **Fins de semana.** Para proteger dados também nos fins de semana, marque a caixa de seleção **Proteger durante fins de semana** e selecione um intervalo.

Diariamente	Para proteger dados em base diária, selecione a opção **Diariamente** e depois, para Hora de proteção, selecione uma hora para começar a proteger os dados.
Sem proteção	Para remover a proteção desse volume, selecione a opção **Sem proteção**.

6 Depois de fazer todas as alterações necessárias, clique em **Salvar**.

7 Para inserir as definições personalizadas de um nó do cluster, selecione o nó e clique no link **Definições** ao lado dele.

- Repita a Etapa 5 para editar a programação de proteção.

Para obter mais informações sobre a personalização de nós, consulte Proteção de nós em um cluster.

8 Na caixa de diálogo Proteger cluster, clique em **Proteger**.

Proteção de nós em um cluster

Este tópico descreve como proteger os dados em um nó de cluster ou máquina com um AppAssure 5 Agent instalado. Ao adicionar proteção, é preciso selecionar um nó na lista de nós disponíveis, além de especificar o nome do host e o nome de usuário, e a senha do administrador do domínio.

Para proteger nós em um cluster

1 No AppAssure 5 Core Console, depois de adicionar o cluster, navegue até o cluster que deseja proteger.

A guia Resumo do cluster selecionado é exibida.

2 Clique na guia Nós protegidos e, no menu **Ações**, selecione **Proteger nó de cluster**.

3 Na caixa de diálogo Proteger nó de cluster, selecione ou insira, conforme o caso, as seguintes informações e clique em **Conectar** para adicionar a máquina ou o nó.

Tabela 93.

Caixa de texto	Descrição
Host	Uma lista suspensa de nós disponíveis para proteção no cluster.
Port	O número da porta pela qual o AppAssure 5 Core se comunica com o Agent no nó.
Nome de usuário	O nome de usuário do administrador de domínio usado para se conectar a esse nó; por exemplo, example_domain\administrator ou administrator@example_domain.com.
Senha	A senha usada para se conectar à máquina.

4 Clique em **Proteger** para começar a proteger essa máquina com as definições de proteção padrão.

NOTA: As definições padrão garantem que todos os volumes da máquina sejam protegidos com uma programação a cada 60 minutos.

5 Para inserir as definições personalizadas dessa máquina (por exemplo, alterar o nome de exibição, adicionar criptografia ou personalizar a programação de proteção), clique em **Exibir opções avançadas**.

6 Se necessário, edite as seguintes definições, conforme descrito na tabela a seguir.

Tabela 94.

Caixa de texto	Descrição
Nome de exibição	Digite um novo nome para a máquina a ser exibido no Core Console.
Repositório	Selecione o repositório no AppAssure 5 Core no qual os dados dessa máquina devem ser armazenados.
Criptografia	Especifique se a criptografia deve ser aplicada aos dados de todos os volumes dessa máquina a serem armazenados no repositório. **NOTA:** As definições de criptografia de um repositório são definidas na guia Configuração do AppAssure 5 Core Console.
Programação	Selecione uma das seguintes opções. • Proteger todos os volumes com uma programação padrão • Proteger volumes específicos com uma programação personalizada. Depois, em Volumes, selecione um volume e clique em **Editar**. Para obter mais informações sobre a definição de intervalos personalizados, consulte a Etapa 5 em Proteção de um cluster.

Processo de modificação das definições de nó de cluster

Depois de ter adicionado a proteção para nós do cluster, é fácil modificar as definições básicas dessas máquinas ou nós (por exemplo, nome de exibição, nome de host, e assim por diante), definições de proteção (por exemplo, alteração da programação de proteção para volumes locais da máquina, adição ou remoção de volumes ou pausa na proteção), e muito mais.

Para modificar as definições do nó de cluster, é preciso executar as seguintes tarefas:

1 No AppAssure 5 Core Console, navegue até o cluster que contém o nó que deseja modificar e selecione a máquina ou nó que deseja modificar.

2 Para modificar e visualizar as definições de configuração, consulte Configuração de grupos de notificação para eventos de sistema.

3 Para configurar grupos de notificação para eventos de sistema, consulte Visualização e modificação das definições de configuração.

4 Para personalizar as definições de política de retenção, consulte Personalização das definições de política de retenção para um agente.

5 Para modificar a programação de proteção, consulte Modificação das programações de proteção.

6 Para modificar as definições da transferência, consulte Modificação das definições de transferência.

Roteiro de configuração de definições de cluster

O roteiro de configuração de definições de cluster envolve realizar as seguintes tarefas:

- **Modificar definições de cluster.** Para obter mais informações sobre a modificação de definições de cluster, consulte Modificação das definições de cluster.

- **Configurar as notificações de eventos de cluster.** Para obter mais informações sobre a configuração de notificação de evento de cluster, consulte Configuração de notificações de eventos de cluster.
- **Modificar a política de retenção de cluster.** Para obter mais informações sobre a modificação da política de retenção de cluster, consulte Modificação da política de retenção de cluster.
- **Modificar as programações de proteção de cluster.** Para obter mais informações sobre a modificação de programações de proteção de cluster, consulte Modificação de programações de proteção de cluster.
- **Modificar as definições de transferência de cluster.** Para obter mais informações sobre a modificação de definições de transferência de cluster, consulte Modificação das definições de transferência de cluster.

Modificação das definições de cluster

Depois de ter adicionado um cluster, é fácil modificar as definições básicas (por exemplo, nome de exibição), definições de proteção (por exemplo, programações de proteção, adição ou remoção de volumes ou pausa na proteção), e muito mais.

Para modificar definições de cluster

1 No AppAssure 5 Core Console, navegue até o cluster que deseja modificar.

2 Clique na guia Configuração.

A página Definições é exibida.

3 Clique em **Editar** para modificar as definições nessa página do cluster, como descrito na tabela a seguir.

Tabela 95.

Caixa de texto	Descrição
Nome de exibição	Insira um nome de exibição para o cluster. O nome desse cluster será exibido no AppAssure 5 Core Console. Por padrão, esse é o nome de host do cluster. Se necessário, é possível mudá-lo para algo mais descritivo.
Repositório	Insira o repositório de Core associado ao cluster. **NOTA:** Se já tiverem sido feitos snapshots desse cluster, essa definição estará relacionada aqui apenas para fins informativos e não poderá ser modificada.
Chave de criptografia	Edite e selecione uma chave de criptografia se necessário. Especifica se a criptografia deve ser aplicada aos dados de todos os volumes desse cluster a ser armazenado no repositório.

Configuração de notificações de eventos de cluster

É possível configurar como os eventos do sistema são relatados para seu cluster criando grupos de notificação. Esses eventos podem ser alertas do sistema ou erros. Execute as etapas deste procedimento para configurar os grupos de notificação para eventos.

Para configurar as notificações de eventos de cluster

1 No AppAssure 5 Core Console, navegue até o cluster que deseja modificar.

2 Clique na guia Configuração e em **Eventos**.

3 Selecione uma das opções descritas na tabela a seguir.

Tabela 96.

Opção	Descrição
Usar definições de alerta do Core	Adota as definições usadas pelo core associado: • Clique em **Aplicar** e execute a Etapa 5.
Usar definições de alerta personalizadas	Permite configurar definições personalizadas: • Vá para a Etapa 4.

4 Se tiver selecionado definições de alerta personalizadas, faça o seguinte:

a Clique em **Adicionar grupo** para adicionar um novo grupo de notificação para o envio de uma lista de eventos do sistema.

A caixa de diálogo Adicionar grupo de notificação é aberta.

b Adicione as opções de notificação conforme descrito na tabela a seguir.

Tabela 97.

Caixa de texto	Descrição
Nome	Insira um nome para o grupo de notificação.
Descrição	Insira uma descrição para o grupo de notificação.
Habilitar eventos	Selecione os eventos para notificação, por exemplo, Clusters. Também é possível optar por selecionar por tipo: • Erro • Aviso • Informações **NOTA:** Ao decidir selecionar por tipo, como padrão, os eventos apropriados são automaticamente ativados. Por exemplo, se você escolher Aviso, os eventos Capacidade de anexação, Trabalhos, Aplicação de licença, Arquivo, CoreService, Exportação, Proteção, Replicação e Reversão são ativados.
Opções de notificação	Selecione o método para especificar como lidar com as notificações. Você pode selecionar dentre as seguintes opções: • **Notificar por e-mail**. Especifique a quais endereços de e-mail enviar os eventos nas caixas de texto Para, CC e Cco. • **Notificar pelo log de eventos do Windows**. O Log de eventos de Windows controla a notificação. • **Notificar por syslogd.** Especifique o nome de host e a porta aos quais enviar os eventos.

c Clique em **OK** para salvar suas alterações e clique em **Aplicar**.

5 Para editar um grupo de notificação existente, ao lado de um grupo de notificação na lista, clique em **Editar**.

A caixa de diálogo Editar grupo de notificação é exibida para que as definições possam ser editadas.

Modificação da política de retenção de cluster

A política de retenção de um cluster especifica por quanto tempo os pontos de recuperação de volumes compartilhados do cluster são armazenados no repositório. As políticas de retenção são usadas para reter snapshots de cópia de segurança por períodos mais longos e para ajudar com o gerenciamento desses snapshots de cópia de segurança. A política de retenção é imposta pelo processo de rollup que ajuda no processo de envelhecimento e exclusão das cópias de segurança antigas.

Para modificar a política de retenção de cluster

1 No AppAssure 5 Core Console, navegue até o cluster que deseja modificar.

2 Clique na guia Configuração e em **Política de retenção**.

3 Selecione uma das opções na tabela a seguir.

Tabela 98.

Opção	Descrição
Usar política de retenção padrão do Core	Adota as definições usadas pelo core associado. • Clique em **Aplicar**.
Usar a política de retenção personalizada	Permite configurar definições personalizadas.

NOTA: Se você tiver selecionado definições de alerta personalizadas, siga as instruções para definir uma política de retenção personalizada, conforme descrito em Personalização das definições de política de retenção para um agente.

Modificação de programações de proteção de cluster

No AppAssure 5, é possível modificar as programações de proteção somente se seu cluster tiver volumes compartilhados.

Para modificar as programações de proteção de cluster

1 No AppAssure 5 Core Console, navegue até o cluster que deseja modificar e selecione-o.

2 Siga as instruções para modificar as definições de proteção, conforme descrito em Modificação das programações de proteção.

Modificação das definições de transferência de cluster

No AppAssure 5, é possível modificar as definições para gerenciar os processos de transferência de dados de um cluster protegido.

NOTA: É possível modificar as definições da transferência de cluster somente se seu cluster tiver volumes compartilhados.

Há três tipos de transferência no AppAssure 5:

- **Snapshots.** Faz a cópia de segurança de dados no seu cluster protegido.
- **Exportação da VM.** Cria uma máquina virtual com todas as informações de cópia de segurança e parâmetros especificados pela programação definida para proteger o cluster.
- **Restaurar**. Restaura as informações de cópia de segurança de um cluster protegido.

Para modificar as definições de transferência de cluster

1 No AppAssure 5 Core Console, navegue até o cluster que deseja modificar.

2 Clique na guia Configuração e em **Definições de transferência**.

3 Modifique as definições de proteção, conforme descrito em Modificação das programações de proteção.

Conversão de um nó de cluster protegido em um Agent

No AppAssure 5, é possível converter um nó de cluster protegido em um AppAssure 5 Agent de modo que ele ainda seja gerenciado pelo Core, mas não faça mais parte do cluster. Isso é útil, por exemplo, se você precisar remover do cluster o nó de cluster, mas ainda mantê-lo protegido.

Para converter um nó de cluster protegido em Agent

1. No AppAssure 5 Core Console, navegue até o cluster que contém a máquina que deseja converter e clique em **Nós protegidos**.
2. Na página Nós protegidos do nó específico que você deseja converter, clique no menu suspenso **Ações** e selecione **Converter em Agent**.
3. Para adicionar a máquina de volta ao cluster, selecione-a e depois, na guia **Resumo** do menu Ações, selecione **Converter para nó de cluster** e clique em **Sim** para confirmar a ação.

Visualização de informações de cluster de servers

Execute as etapas dos procedimentos a seguir para visualizar informações de resumo, evento, alerta e assim por diante referentes aos clusters de servers.

Visualização de informações do sistema de cluster

Execute as etapas deste procedimento para visualizar as informações detalhadas do sistema de um cluster.

Para visualizar as informações do sistema do cluster

1. No AppAssure 5 Core Console, navegue até o cluster que deseja visualizar.
2. Clique na guia Ferramentas.

   Aparece a página de informações do sistema e mostra detalhes do sistema sobre o cluster, como nome, nós incluídos com estado associado e versões do Windows, informações de interface de rede e de capacidade de volume.

Visualização de tarefas, eventos e alertas de cluster

Execute as etapas deste procedimento para visualizar eventos e alertas de um cluster.

Para obter informações sobre visualização de eventos e alertas de uma máquina ou nó individual em um cluster, consulte Visualização de tarefas, alertas e eventos.

Para visualizar tarefas, eventos e alertas de cluster

1. No AppAssure 5 Core Console, navegue até o cluster que deseja visualizar.
2. Clique na guia Eventos, que se abre para mostrar todas as tarefas desse cluster.
3. É possível filtrar as tarefas exibidas desse cluster. Para obter mais informações, consulte Visualização de tarefas.
4. Para visualizar apenas os alertas, no canto superior esquerdo da página, clique em **Alertas**.

   A lista de eventos é filtrada para exibir apenas os alertas do cluster ou nó selecionado.

5 Como opção, se você quiser remover todos os alertas da página, clique em **Descartar tudo**.

6 Para visualizar todos os eventos, no canto superior esquerdo da página, clique em **Eventos**.

Todos os eventos são exibidos para o cluster ou nó selecionado.

Visualização de informações de resumo

Execute as etapas deste procedimento para visualizar as informações de resumo de um cluster, incluindo informações sobre o quórum associado ao cluster.

Para visualizar as informações de resumo

1 No AppAssure 5 Core Console, navegue até o cluster que deseja visualizar.

2 Na guia Resumo, é possível visualizar informações como nome do cluster, tipo de cluster, tipo de quórum (se aplicável) e caminho do quórum (se aplicável). Essa guia também mostra informações de relance sobre os volumes nesse cluster, incluindo o tamanho e programação de proteção. Se aplicável, também é possível visualizar informações do SQL Server ou Exchange Server para um cluster diferente.

3 Para que essas informações fiquem mais atualizadas, clique no menu suspenso **Ações** e em **Atualizar metadados**.

Para obter informações sobre visualização de informações de resumo e status de uma máquina ou nó individual no cluster, consulte Visualização do status da máquina e outros detalhes.

Trabalho com pontos de recuperação de cluster

Um ponto de recuperação, também chamado de snapshot, é uma cópia pontual das pastas e arquivos dos volumes compartilhados em um cluster, que estão armazenados no repositório. Os pontos de recuperação são utilizados para recuperar as máquinas protegidas ou para montar um sistema de arquivos local. No AppAssure 5, é possível visualizar as listas de pontos de recuperação no repositório. Execute as etapas do procedimento a seguir para revisar os pontos de recuperação.

NOTA: Se você estiver protegendo dados a partir de um cluster de servers DAG ou CCR, os pontos de recuperação associados não aparecerão no nível de cluster. Estarão visíveis apenas no nível de nó ou máquina.

Para obter informações sobre visualização de pontos de recuperação de máquinas individuais em um cluster, consulte Visualização de pontos de recuperação.

Para trabalhar com pontos de recuperação de cluster

1 No AppAssure 5 Core Console, navegue até o cluster do qual deseja visualizar os pontos de recuperação.

2 Clique na guia Pontos de recuperação.

3 Para visualizar informações detalhadas de um ponto de recuperação específico, clique no símbolo de maior que (>) ao lado de um ponto de recuperação na lista para expandir a visualização.

4 Para obter informações sobre as operações que podem ser executadas nos pontos de recuperação, consulte Visualização de um ponto de recuperação específico.

5 Selecione um ponto de recuperação para montar.

Para obter informações sobre como montar um ponto de recuperação, consulte Montagem de um ponto de recuperação de uma máquina com Windows.

6 Para excluir pontos de recuperação, consulte Remoção dos pontos de recuperação.

Gerenciamento de snapshots em um cluster

No AppAssure 5, é possível gerenciar snapshots forçando-os ou pausando os atuais. Forçar um snapshot permite forçar uma transferência de dados para o cluster atualmente protegido. Ao forçar um snapshot, a transferência começa imediatamente ou é adicionada à fila. Somente os dados que foram alterados em relação a um ponto de recuperação anterior são transferidos. Se não existir um ponto de recuperação anterior, todos os dados (a imagem de base) nos volumes protegidos são transferidos. Ao pausar o snapshot, você interrompe temporariamente todas as transferências de dados da máquina atual.

Para obter informações sobre como forçar snapshots de máquinas individuais em um cluster, consulte Forçar snapshot. Para obter informações sobre como pausar e retomar snapshots de máquinas individuais em um cluster, consulte Pausa e retomada da proteção.

Forçar snapshot em um cluster

Execute as etapas deste procedimento para forçar um snapshot de cluster.

Para forçar um snapshot em um cluster

1. No AppAssure 5 Core Console, navegue até o cluster do qual deseja visualizar os pontos de recuperação.
2. Na guia Resumo, clique no menu suspenso **Ações** e depois em **Forçar snapshot**.

Pausa e retomada de snapshots de cluster

Execute as etapas deste procedimento para pausar e retomar um snapshot de cluster.

Para pausar e retomar os snapshots de cluster

1. No AppAssure 5 Core Console, navegue até o cluster do qual deseja visualizar os pontos de recuperação.
2. Na guia Resumo, clique no menu suspenso **Ações** e depois em **Pausar snapshots**.
3. Na caixa de diálogo Pausar proteção, selecione uma das opções descritas na tabela a seguir.

Tabela 99.

Opção	Descrição
Pausar até que retomado	Pausa o snapshot até você retomar manualmente a proteção. • Para retomar a proteção, clique no menu **Ações** e depois em **Retomar**.
Pausar por	Permite especificar uma quantidade de tempo em dias, horas e minutos para pausar os snapshots.

Desmontagem de pontos de recuperação locais

Execute as etapas deste procedimento para desmontar os pontos de recuperação que estão montados localmente.

Para desmontar pontos de recuperação locais

1. No AppAssure 5 Core Console, navegue até o cluster do qual deseja desmontar os pontos de recuperação.
2. Na guia Ferramentas, no menu Ferramentas, clique em **Montagens**.
3. Na lista de montagens locais, realize um dos procedimentos a seguir:

- Para desmontar uma única montagem local, localize e selecione a montagem do ponto de recuperação que deseja desmontar e, em seguida, clique em **Desmontar**.
- Para desmontar todas as montagens locais, clique no botão **Desmontar tudo**.

Realização de uma restauração em clusters e nós do cluster

A restauração é o processo de restaurar os volumes em uma máquina a partir de pontos de recuperação. Para um cluster de servers, realize a restauração no nível de nó ou da máquina. Esta seção fornece orientações sobre como realizar uma restauração em volumes de cluster.

Realização de uma restauração em clusters de CCR (Exchange) e DAG

Execute as etapas deste procedimento para realizar uma restauração em clusters de CCR (Exchange) e DAG.

Para executar uma restauração em clusters de CCR (Exchange) e DAG

1. Desative todos os nós, com exceção de um.
2. Execute uma restauração usando o procedimento padrão do AppAssure 5 para a máquina, como descrito em Restauração de volumes a partir de um ponto de recuperação e Restauração de volumes em uma máquina com Linux usando a linha de comando.
3. Quando a restauração for concluída, monte todos os bancos de dados para os volumes de cluster.
4. Ative todos os outros nós.
5. Para o Exchange, navegue até o Console de gerenciamento do Exchange e, para cada banco de dados, execute a operação **Atualizar cópia de banco de dados**.

Realização de uma restauração em clusters de SCC (Exchange, SQL)

Execute as etapas deste procedimento para realizar uma restauração em clusters de SCC (Exchange, SQL).

Para realizar uma restauração em clusters de SCC (Exchange, SQL)

1. Desative todos os nós, com exceção de um.
2. Execute uma restauração usando o procedimento padrão do AppAssure 5 para a máquina, como descrito em Restauração de volumes a partir de um ponto de recuperação e Restauração de volumes em uma máquina com Linux usando a linha de comando.
3. Depois que a restauração for concluída, monte todos os bancos de dados a partir dos volumes de cluster.
4. Ative todos os outros nós, um por um.

> **NOTA:** Não é preciso executar nenhuma reversão no disco de quórum. Ele pode ser regenerado automaticamente ou usando a funcionalidade do serviço de cluster.

Replicação de dados de cluster

Ao replicar dados de um cluster, você deve replicar todo o cluster. Por exemplo, se você selecionar um nó para replicar, o cluster será selecionado automaticamente. Da mesma forma, se você selecionar o cluster, todos os nós desse cluster também serão selecionados.

Para obter mais informações e instruções sobre a replicação de dados, consulte Roteiro para definição da replicação.

Remoção de um cluster da proteção

Execute as etapas do procedimento a seguir para remover um cluster da proteção.

Para remover um cluster da proteção

1. No AppAssure 5 Core Console, navegue até o cluster que deseja remover.
2. Clique no menu suspenso **Ações** e depois em **Remover cluster**.
3. Selecione uma das seguintes opções.

Tabela 100.

Opção	Descrição
Manter pontos de recuperação	Para manter todos os pontos de recuperação atualmente armazenados deste cluster.
Remover pontos de recuperação	Para remover do repositório todos os pontos de recuperação atualmente armazenados deste cluster.

Remoção de nós de cluster da proteção

Execute as etapas dos procedimentos a seguir para remover nós de cluster da proteção.

Se quiser apenas remover um nó do cluster, consulte Conversão de um nó de cluster protegido em um Agent.

Para remover um nó de cluster da proteção

1. No AppAssure 5 Core Console, navegue até a guia do cluster Nós protegidos.
2. Clique no menu suspenso Ações e depois em **Remover nó**.
3. Selecione uma das opções descritas na tabela a seguir.

Tabela 101.

Opção	Descrição
Manter pontos de recuperação	Para manter todos os pontos de recuperação atualmente armazenados desta máquina ou nó.
Remover pontos de recuperação	Para remover do repositório todos os pontos de recuperação atualmente armazenados desta máquina ou nó.

Remoção de todos os nós em um cluster da proteção

Execute as etapas deste procedimento para remover todos os nós em um cluster da proteção.

CUIDADO: Se você remover todos os nós do cluster, o cluster também será removido.

Para remover todos os nós em um cluster da proteção

1. No AppAssure 5 Core Console, navegue até a guia do cluster Nós protegidos.
2. Na guia Nós Protegidos, selecione todos os nós.
3. Clique no menu suspenso Ações na parte superior da guia Nós protegidos, clique em **Remover nós** e depois selecione uma das opções descritas na tabela a seguir.

Tabela 102.

Opção	Descrição
Manter pontos de recuperação	Para manter todos os pontos de recuperação atualmente armazenados deste cluster.
Remover pontos de recuperação	Para remover do repositório todos os pontos de recuperação atualmente armazenados deste cluster.

Visualização de um relatório de cluster ou nó

É possível criar e visualizar relatórios de conformidade e erros sobre as atividades do AppAssure 5 para seu cluster e nós individuais. Os relatórios incluem informações de atividades do AppAssure 5 sobre o cluster, nó e volumes compartilhados.

Para obter mais informações sobre relatórios no AppAssure 5, 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 Relatórios.

Para visualizar um relatório de cluster ou nó

1. No AppAssure 5 Core Console, navegue até o cluster do qual deseja criar um relatório.
2. Se quiser criar um relatório de um nó sob um cluster, selecione o nó.
3. Clique na guia Ferramentas e, no menu Relatórios, selecione uma das seguintes opções:
   - Relatório de conformidade
   - Relatório de falhas
4. No calendário suspenso Hora inicial, selecione a data inicial e depois insira um horário inicial para o relatório.

   NOTA: Não há dados disponíveis anteriores ao horário em que o AppAssure 5 Core ou Agent foi implementado.

5. No calendário suspenso Hora final, selecione a data final e depois insira um horário final para o relatório.
6. Clique em **Gerar relatório**. Os resultados do relatório aparecem na página.

   Se o relatório ocupar diversas páginas, você clicar nos números de página ou nos botões de seta no alto dos resultados do relatório para mudar de página.
7. Para exportar os resultados do relatório em 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, faça um dos seguintes:
   - Clique no primeiro ícone Salvar para exportar um relatório e salvá-lo no disco.

- Clique no segundo ícone Salvar para exportar um relatório e exibi-lo em uma nova janela de navegador da Web.

8 Para imprimir os resultados do relatório, use uma das seguintes opções:

- Clique no primeiro ícone de Impressora para imprimir todo o relatório.
- Clique no segundo ícone de Impressora para imprimir a página atual do relatório.

5

Relatórios

Este capítulo fornece uma visão geral dos relatórios disponíveis no Dell AppAssure 5. Ele consiste nos seguintes tópicos:

Sobre relatórios

O AppAssure 5 permite gerar e visualizar informações de conformidade, erro e resumo de várias máquinas core e agente.

Você pode optar por visualizar os relatórios on-line, imprimi-los ou exportá-los e salvá-los em um dos vários formatos suportados. Os formatos que podem ser selecionados são os seguintes:

- PDF
- XLS
- XLSX
- RTF
- MHT
- HTML
- TXT
- CSV
- Imagem

Nesta versão do AppAssure 5, os relatórios incluem agora as unidades de medida, o que torna mais fácil determinar se uma coluna é representada em GB, TB ou segundos.

Sobre a barra de ferramentas Relatórios

A barra de ferramentas disponível para todos os relatórios permite imprimir e salvar de duas maneiras diferentes. A tabela a seguir descreve as opções de imprimir e salvar.

Tabela 103.

Ícone	Descrição
	Imprimir o relatório
	Imprimir a página atual
	Exportar um relatório e salvá-lo no disco

Para obter informações sobre como gerar um relatório, consulte Geração de um relatório para um Core ou Agent. Para obter informações sobre como gerar um relatório para vários cores no Central Management Console, consulte Gerar um relatório no Central Management Console. Para obter informações sobre como gerar relatórios de cluster, consulte Visualização de um relatório de cluster ou nó.

Sobre relatórios de conformidade

Estão disponíveis relatórios de conformidade para o AppAssure 5 Core e o AppAssure 5 Agent. Eles fornecem uma maneira de visualizar o status dos trabalhos realizados por um core ou agente selecionado. Os trabalhos com falha aparecem em texto em vermelho. As informações do Relatório de conformidade do Core que não estão associadas a um agente aparecem em branco.

Os detalhes sobre os trabalhos são apresentados em uma visualização de coluna que inclui as seguintes categorias:

- Core
- Agente protegido
- Tipo
- Resumo
- Status
- Erro
- Hora inicial
- Hora final
- Hora
- Trabalho total

Para obter informações sobre como gerar um relatório, consulte Geração de um relatório para um Core ou Agent.

Sobre relatórios de falha

Os relatórios de falha são subconjuntos dos Relatórios de conformidade e estão disponíveis para AppAssure 5 Cores e AppAssure 5 Agents. Os Relatórios de falha incluem apenas os trabalhos com falha relacionados em Relatórios de conformidade e que são compilados em um único relatório que pode ser impresso e exportado.

Os detalhes sobre os erros são apresentados em uma visualização de coluna com as seguintes categorias:

- Core
- Agente
- Tipo
- Resumo
- Erro
- Hora inicial
- Hora final
- Tempo decorrido
- Trabalho total

Para obter informações sobre como gerar um relatório, consulte Geração de um relatório para um Core ou Agent.

Sobre o relatório resumido

O Relatório resumido inclui informações sobre os repositórios no AppAssure 5 Core selecionado e sobre os agentes protegidos por esse core. As informações aparecem como dois resumos dentro de um relatório. Para obter informações sobre como gerar um Relatório resumido, consulte Geração de um relatório para um Core ou Agent.

Resumo de repositórios

A parte Repositórios do Relatório resumido inclui dados dos repositórios localizados no AppAssure 5 Core selecionado. Os 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
- Taxa de compressão/deduplicação

NOTA: Os espaços alocado, usado e livre são representados em unidades de medida. As medidas são em GB, TB ou segundos.

Resumo de agentes

A parte Agentes do Relatório resumido inclui dados de todos os agentes protegidos pelo AppAssure 5 Core selecionado.

Os 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 alteração por dia (Média | Mediana)
- Estatística dos trabalhos (Aprovada | Com falha | Cancelada)

Geração de um relatório para um Core ou Agent

Execute as etapas do procedimento a seguir para gerar um relatório para um AppAssure 5 Core ou AppAssure 5 Agent.

Para gerar um relatório para um core ou agente

1 Navegue até o AppAssure 5 Core Console e selecione o Core ou o Agent para o qual deseja executar o relatório.

2 Clique na guia Ferramentas.

3 Na guia Ferramentas, expanda **Relatórios** na área de navegação à esquerda.

4 Na área de navegação à esquerda, selecione o relatório que deseja executar. Os relatórios disponíveis dependem da seleção feita na Etapa 1 e estão descritos na tabela a seguir.

Tabela 104.

Máquina	Relatórios disponíveis
Core	Relatório de conformidade
	Relatório resumido
	Relatório de falhas
Agente	Relatório de conformidade
	Relatório de falhas

5 No calendário suspenso Hora inicial, selecione a data inicial e depois insira um horário inicial para o relatório.

NOTA: Não há dados disponíveis anteriores ao horário em que o Core ou o Agent foi implementado.

6 No calendário suspenso Hora final, selecione a data final e depois insira um horário final para o relatório.

7 Para um Relatório resumido, marque a caixa de seleção **A todo o momento** se quiser que a Hora inicial e a Hora final se estendam pela duração do Core.

8 Para um Relatório de conformidade ou de falha, use a lista suspensa Cores de destino para selecionar o Core do qual deseja visualizar dados.

9 Clique em **Gerar relatório**.

Após a geração do relatório, você pode usar a barra de ferramentas para imprimir ou exportar o relatório. Para obter mais informações sobre a barra de ferramentas, consulte Sobre a barra de ferramentas Relatórios.

Sobre relatórios de Core do Central Management Console

O AppAssure 5 permite gerar e visualizar informações de conformidade, erro e resumo de vários AppAssure 5 Cores. Os detalhes sobre os Cores são apresentados em visualizações de coluna com as mesmas categorias descritas nas seções Sobre relatórios de conformidade, Sobre relatórios de falha e Sobre o relatório resumido.

Para obter informações sobre como gerar um relatório de vários cores, consulte Gerar um relatório no Central Management Console.

Gerar um relatório no Central Management Console

Execute o procedimento a seguir para gerar um relatório para vários AppAssure 5 Cores no Central Management Console.

Para gerar um relatório no Central Management Console

1. Na tela Bem-Vindo do Central Management Console, clique no menu suspenso no canto superior direito.
2. No menu suspenso, clique em **Relatórios** e selecione uma das seguintes opções:
   - Relatório de conformidade
   - Relatório resumido
   - Relatório de falhas
3. Na área de navegação à esquerda, selecione o AppAssure 5 Core ou Cores para o(s) qual(is) deseja executar o relatório.
4. No calendário suspenso Hora inicial, selecione a data inicial e depois insira um horário inicial para o relatório.

   NOTA: Não há dados disponíveis anteriores ao horário em que os Cores foram implementados.

5. No calendário suspenso Hora final, selecione a data final e depois insira um horário final para o relatório.
6. Clique em **Gerar relatório**.

   Após a geração do relatório, você pode usar a barra de ferramentas para imprimir ou exportar o relatório. Para obter mais informações sobre a barra de ferramentas, consulte Sobre a barra de ferramentas Relatórios.

A

Scripts

O AppAssure 5 permite aos administradores automatizar a administração e o gerenciamento de recursos em determinadas ocorrências pela execução de comandos e scripts. O software AppAssure 5 suporta o uso de script de PowerShell para Windows e script de Bourne Shell para Linux.

△ **CUIDADO: Os scripts PowerShell e Bourne da amostra, oferecidos neste documento, irão funcionar quando executados conforme o que foi projetado pelos administradores qualificados. Tome cuidado ao modificar scripts de funcionamento para manter versões de trabalho. Quaisquer modificações nas amostras do script incluídas aqui, ou quaisquer scripts personalizados que você criar, são consideradas personalização, que normalmente não é coberta pelo Atendimento ao Cliente.**

Este apêndice descreve os scripts que podem ser usados por administradores em ocorrências designadas do AppAssure 5 para Windows e Linux. Os seguintes tópicos estão incluídos:

- PowerShell Scripting em AppAssure 5
- Parâmetros de entrada do PowerShell Scripting
- Scripts do PowerShell de amostra
- Sobre scripts Bourne Shell no AppAssure 5
- Parâmetros de entrada de scripts do Bourne Shell
- Scripts do Bourne Shell de amostra

PowerShell Scripting em AppAssure 5

O Windows PowerShell é um ambiente conectado ao Microsoft .NET Framework projetado visando a automação administrativa. O AppAssure 5 inclui kits abrangentes de desenvolvimento de software cliente (SDKs) para PowerShell scripting que permitem aos usuários administrativos executar scripts do PowerShell fornecidos pelo usuário em ocorrências designadas, por exemplo, antes ou depois de um snapshot, de verificações da capacidade de anexação e da montabilidade, e assim por diante. Os administradores podem executar scripts no AppAssure 5 Core e Agent. Os scripts podem aceitar parâmetros, e a saída de um script é escrita nos arquivos de log do core e do agente.

ⓘ **NOTA:** Para trabalhos noturnos, preserve um arquivo de script e o parâmetro de entrada *JobType* para distinguir entre trabalhos noturnos.

Os arquivos de script estão localizados na pasta %ALLUSERSPROFILE%\AppRecovery\Scripts.

- No Windows 7, o caminho para localizar a pasta %ALLUSERSPROFILE% é: C:\ProgramData.
- No Windows 2003, o caminho para localizar a pasta é: Documents and Settings\All Users\Application Data\.

ⓘ **NOTA:** É necessário que o Windows PowerShell esteja instalado e configurado antes de usar e executar os scripts do AppAssure 5.

Para obter mais informações sobre como usar os scripts do PowerShell consulte Scripts do PowerShell de amostra, Parâmetros de entrada do PowerShell Scripting e Scripts do Bourne Shell de amostra

Pré-requisitos do PowerShell Scripting

Antes de usar e executar scripts do PowerShell no AppAssure 5, é preciso instalar o Windows PowerShell 3.0.

NOTA: Certifique-se de colocar o arquivo powershell.exe.config no diretório base 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>
```

Teste dos scripts do PowerShell

Se desejar testar os scripts que pretende executar, poderá fazê-lo usando o editor gráfico do PowerShell, o *powershell_is*. Também é preciso adicionar o arquivo de configuração, *powershell_ise.exe.config* na mesma pasta do arquivo de configuração, *powershell.exe.config*.

NOTA: O arquivo de configuração, *powershell_ise.exe.config* deve ter o mesmo conteúdo do arquivo *powershell.exe.config*.

CUIDADO: **Se o script pré-PowerShell ou pós-PowerShell falhar, o trabalho também falhará.**

Parâmetros de entrada do PowerShell Scripting

Todos os parâmetros de entrada disponíveis são usados em scripts de exemplo. Os parâmetros estão descritos nas tabelas a seguir.

NOTA: Os arquivos de script devem possuir o mesmo nome dos arquivos de script de exemplo.

AgentProtectionStorageConfiguration (espaço de nomes Replay.Common.Contracts.Agents)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro AgentProtectionStorageConfiguration.

Tabela 105.

Método	Descrição
public Guid RepositoryId { get; set; }	Obtém ou define o ID do repositório onde os pontos de recuperação do Agent estão armazenados.
public string EncryptionKeyId { get; set; }	Obtém ou define o ID da chave de criptografia dos pontos de recuperação do Agent. Uma cadeia de caracteres vazia significa nenhuma criptografia.

AgentTransferConfiguration (espaço de nomes Replay.Common.Contracts.Transfer)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro AgentTransferConfiguration.

Tabela 106.

Método	Descrição
public uint MaxConcurrentStreams { get; set; }	Obtém ou define o número máximo de conexões TCP simultâneas que o Core estabelece com o Agent para transferência de dados.
public uint MaxTransferQueueDepth { get; set; }	Quando um intervalo de blocos é lido de um fluxo de transferência, esse intervalo é colocado em uma fila de produtor ou consumidor, onde um thread de consumidor o lê e grava no objeto epoch. Se o repositório grava mais lentamente do que a rede lê, essa fila fica cheia. O ponto em que a fila está cheia e a leitura é interrompida é a extensão máxima da fila de transferência.
public uint MaxConcurrentWrites { get; set; }	Obtém ou define o número máximo de operações de gravação de blocos pendentes em um epoch em qualquer momento. Se blocos adicionais forem recebidos quando essa quantidade de gravações de blocos estiver pendente, esses 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 que serão transferidos em uma única solicitação. Dependendo do teste, valores mais altos ou mais baixos podem ser ideais.
public Priority Priority { get; set; }	Obtém ou define a prioridade da solicitação de transferência.
public int MaxRetries { get; set; }	Obtém ou define o número máximo de vezes que uma transferência com falha deve ser tentada novamente antes de ser considerada como falha.
public Guid ProviderId{ get; set; }	Obtém ou define o GUID do provedor de VSS que será usado para snapshots neste host. Os administradores em geral aceitam o padrão.
public Collection<ExcludedWriter> ExcludedWriterIds { get; set; }	Obtém ou define o conjunto de IDs de gravação do VSS, os quais devem ser excluídos desse snapshot. O ID do gravador é determinado pelo nome do gravador. Esse nome é apenas para fins de documentação e não precisa corresponder exatamente ao nome do gravador.
public ushort TransferDataServerPort { get; set; }	Obtém ou define um valor que contém a porta TCP através da qual as conexões serão aceitas do Core para a transferência real de dados do Agent para o Core. O Agent tenta escutar essa porta, mas se ela estiver em uso, ele poderá usar uma porta diferente. O Core deve usar o número de porta especificado nas propriedades BlockHashesUri e BlockDataUri do objeto VolumeSnapshotInfo para cada volume expandido.
public TimeSpan SnapshotTimeout { get; set; }	Obtém ou define o tempo de espera para que uma operação de snapshot do VSS seja concluída antes que ela seja abandonada e expire.

Tabela 106.

Método	Descrição
public TimeSpan TransferTimeout { get; set; }	Obtém ou define o tempo de espera para contatos adicionais do Core antes de abandonar o snapshot.
public TimeSpan NetworkReadTimeout { get; set; }	Obtém ou define o tempo limite para operações de leitura de rede relacionadas a essa transferência.
public TimeSpan NetworkWriteTimeout { get; set; }	Obtém ou define o tempo limite para operações de gravação de rede relacionadas a essa transferência.

BackgroundJobRequest (espaço de nomes Replay.Core.Contracts.BackgroundJobs)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro BackgroundJobRequest.

Tabela 107.

Método	Descrição
public Guid AgentId { get; set; }	Obtém ou define o ID do Agent.
public bool IsNightlyJob { get; set; }	Obtém ou define o valor que indica se o trabalho em segundo plano é um trabalho noturno.
public virtual bool InvolvesAgentId(Guid agentId)	Determina o valor que indica se o Agent concreto está envolvido no trabalho.

ChecksumCheckJobRequest (espaço de nomes Replay.Core.Contracts.Exchange.ChecksumChecks)

Herda seus valores do parâmetro DatabaseCheckJobRequestBase.

DatabaseCheckJobRequestBase (espaço de nomes Replay.Core.Contracts.Exchange)

Herda seus valores do parâmetro, BackgroundJobRequest.

ExportJobRequest (espaço de nomes Replay.Core.Contracts.Export)

Herda seus valores do parâmetro, BackgroundJobRequest.

A tabela a seguir apresenta os objetos disponíveis para o parâmetro ExportJobRequest.

Tabela 108.

Método	Descrição
public uint RamInMegabytes { get; set; }	Obtém ou define o tamanho da memória para a VM exportada. Defina como zero (0) para usar o tamanho da memória da máquina de origem.
public VirtualMachineLocation Location { get; set; }	Obtém ou define o local de destino dessa exportação. Trata-se de uma classe de base abstrata.

Tabela 108.

Método	Descrição
public VolumeImageIdsCollection VolumeImageIds { get; private set; }	Obtém ou define as imagens de volume a incluir na exportação da VM.
public ExportJobPriority Priority { get; set; }	Obtém ou define a prioridade da solicitação de exportação.

NightlyAttachabilityJobRequest (espaço de nomes Replay.Core.Contracts.Sql)

Herda seus valores do parâmetro, BackgroundJobRequest.

RollupJobRequest (espaço de nomes Replay.Core.Contracts.Rollup)

Herda seus valores do parâmetro, BackgroundJobRequest.

TakeSnapshotResponse (espaço de nomes Replay.Agent.Contracts.Transfer)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro TakeSnapshotResponse.

Tabela 109.

Método	Descrição
public Guid SnapshotSetId { get; set; }	Obtém ou define o GUID atribuído pelo VSS a este snapshot.
public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }	Obtém ou define o conjunto de informações do snapshot para cada volume incluído no snapshot.

TransferJobRequest (espaço de nomes Replay.Core.Contracts.Transfer)

Herda seus valores do parâmetro, BackgroundJobRequest.

A tabela a seguir apresenta os objetos disponíveis para o parâmetro TransferJobRequest.

Tabela 110.

Método	Descrição
public VolumeNameCollection VolumeNames { get; set; }	Obtém ou define o conjunto de nomes para transferência. VolumeNames é uma estrutura de dados que contém os seguintes dados: • GuidName - O GUID associado ao volume, usado como o nome, caso DisplayName não esteja definido. • DisplayName - O nome de exibição do volume.
public ShadowCopyType ShadowCopyType { get; set; }	Obtém ou define o tipo de cópia da transferência. Os valores disponíveis são: • Unknown • Copy • Full

Tabela 110.

Método	Descrição
public AgentTransferConfiguration TransferConfiguration { get; set; }	Obtém ou define a configuração da transferência.
public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }	Obtém ou define a configuração do armazenamento.
public string Key { get; set; }	Gera uma chave pseudoaleatória (mas não criptograficamente segura), que pode ser usada como senha única para autenticar solicitações de transferência.
public bool ForceBaseImage { get; set; }	Obtém ou define o valor que indica se a imagem de base foi forçada ou não.
public bool IsLogTruncation { get; set; }	Obtém ou define o valor que indica se o trabalho é truncamento de log ou não.

TransferPrescriptParameter (espaço de nomes Replay.Common.Contracts.PowerShellExecution)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro TransferPrescript.

Tabela 111.

Método	Descrição
public VolumeNameCollection VolumeNames (get; set;)	Obtém ou define o conjunto de nomes de volume para transferência. VolumeNames é uma estrutura de dados que contém os seguintes dados: • GuidName - O GUID associado ao volume, usado como o nome, caso DisplayName não esteja definido. • DisplayName - O nome de exibição do volume.
public ShadowCopyType ShadowCopyType { get; set; }	Obtém ou define o tipo de cópia da transferência. ShadowCopyType é uma enumeração com valores. Os valores disponíveis são: • Unknown • Copy • Full

Tabela 111.

Método	Descrição

public AgentTransferConfiguration TransferConfiguration { get; set; }	Obtém ou define a configuração da transferência.
	AgentTransferConfiguration é um objeto que terá os seguintes dados:
	• MaxConcurrentStreams: o número máximo de conexões TCP simultâneas que o core estabelecerá com o Agent para transferir dados
	• MaxTransferQueueDepth: o número máximo de extensões de blocos que podem ser enfileiradas para gravação
	• MaxConcurrentWrites: o número máximo de operação de gravação de blocos pendentes em um epoch a qualquer momento. Se blocos adicionais forem recebidos quando essa quantidade de gravações de blocos estiver pendente, esses blocos adicionais serão ignorados até que um dos blocos pendentes seja gravado.
	• MaxSegmentSize: o número máximo de blocos contíguos que serão transferidos em uma única solicitação.
	• Priority: um objeto que terá os seguintes dados:
	  • Undefined
	  • One
	  • Two
	  • Three
	  • Four
	  • Five
	  • Six
	  • Seven
	  • Eight
	  • Nine
	  • Ten
	  • Highest (which is equal to One)
	  • Lowest (which is equal to Ten)
	  • Default (which is equal to Five)
	• MaxRetries: o número máximo de vezes que uma transferência deve ser tentada novamente antes de ser considerada como falha
	• UseDefaultMaxRetries: um valor que indica que o número máximo de tentativas é o valor padrão
	• ProviderId: o GUID do provedor de VSS que será usado para snapshots neste host. Quase todo mundo aceitará o padrão.

Tabela 111.

Método	Descrição
public AgentTransferConfiguration TransferConfiguration { get; set; } (cont.)	• ExcludedWriterIds: conjunto de IDs de gravação do VSS que devem ser excluídos do snapshot. O ID do gravador é determinado pelo nome do gravador. Esse nome é apenas para fins de documentação e não precisa corresponder exatamente ao nome real do gravador. • TransferDataServerPort: um valor contendo a porta TCP através da qual as conexões serão aceitas a partir do core para a transferência de dados do agente para o core. • SnapshotTimeout: tempo de espera para que uma operação de snapshot do VSS seja concluída antes que ela seja abandonada e expire. • TransferTimeout: tempo de espera para contatos adicionais do core antes de abandonar o snapshot. • NetworkReadTimeout: o tempo limite para operações de leitura de rede relacionadas à transferência. • NetworkWriteTimeout: o tempo limite para operações de gravação de rede relacionadas à transferência. • InitialQueueSize: o tamanho da fila inicial de solicitações. • MinVolumeFreeSpacePercents: quantidade mínima de espaço livre em um volume expressa em porcentagem. • MaxChangeLogsSizePercents: tamanho máximo dos registros de alterações no driver como parte da capacidade do volume medida em porcentagem. • EnableVerification: um valor que indica se a confirmação de diagnóstico para cada bloco enviado ao Core deve ser realizada.
public string Key { get; set; }	O método Key gera uma chave pseudoaleatória (mas não criptograficamente segura), que pode ser usada como senha única para autenticar solicitações de transferência.
public bool ForceBaseImage { get; set; }	Obtém ou define o valor que indica se a transferência foi uma captura de imagem de base forçada.
public bool IsLogTruncation { get; set; }	Obtém ou define o valor que indica se o registro está sendo truncado.
public uint LatestEpochSeenByCore { get; set; }	Obtém ou define o valor de epoch mais recente. O método LatestEpochSeenByCore é o número original do snapshot mais recentemente capturado pelo Core. Esse é o “número de epoch” atribuído pelo driver do filtro a este snapshot específico no momento em que ele foi capturado com o VSS.

TransferPostscriptParameter (espaço de nomes Replay.Common.Contracts.PowerShellExecution)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro TransferPostscript.

Tabela 112.

Método	Descrição
public VolumeNameCollection VolumeNames (get; set;)	Obtém ou define o conjunto de nomes de volume para transferência. VolumeNames é uma estrutura de dados que contém os seguintes dados: • GuidName - O GUID associado ao volume, usado como o nome, caso DisplayName não esteja definido. • DisplayName - O nome de exibição do volume.
public ShadowCopyType ShadowCopyType { get; set; }	Obtém ou define o tipo de cópia da transferência. ShadowCopyType é uma enumeração com valores. Os valores disponíveis são: • Unknown • Copy • Full

Tabela 112.

Método	Descrição

public AgentTransferConfiguration TransferConfiguration { get; set; }	Obtém ou define a configuração da transferência.
	AgentTransferConfiguration é um objeto que terá os seguintes dados:
	• MaxConcurrentStreams: o número máximo de conexões TCP simultâneas que o core estabelecerá com o Agent para transferir dados
	• MaxTransferQueueDepth: o número máximo de extensões de blocos que podem ser enfileiradas para gravação
	• MaxConcurrentWrites: o número máximo de operação de gravação de blocos pendentes em um epoch a qualquer momento. Se blocos adicionais forem recebidos quando essa quantidade de gravações de blocos estiver pendente, esses blocos adicionais serão ignorados até que um dos blocos pendentes seja gravado.
	• MaxSegmentSize: o número máximo de blocos contíguos que serão transferidos em uma única solicitação
	• Priority: um objeto que terá os seguintes dados:
	  • “Indefinido
	  • “Um
	  • “Dois
	  • “Três
	  • “Quatro
	  • “Cinco
	  • “Seis
	  • “Sete
	  • “Oito
	  • “Nove
	  • “Dez
	  • “Mais alto (é igual a Um)
	  • “Mais baixo (igual a Dez)
	  • “Padrão (igual a Cinco)
	• MaxRetries: o número máximo de vezes que uma transferência deve ser tentada novamente antes de ser considerada como falha
	• UseDefaultMaxRetries: um valor que indica que o número máximo de tentativas é o valor padrão
	• ProviderId: o GUID do provedor de VSS que será usado para snapshots neste host. Quase todo mundo aceitará o padrão

Tabela 112.

Método	Descrição
public AgentTransferConfiguration TransferConfiguration { get; set; } (cont.)	• ExcludedWriterIds: conjunto de IDs de gravação do VSS que devem ser excluídos do snapshot. O ID do gravador é determinado pelo nome do gravador. Esse nome é apenas para fins de documentação e não precisa corresponder exatamente ao nome real do gravador. • TransferDataServerPort: um valor contendo a porta TCP através da qual as conexões serão aceitas a partir do core para a transferência de dados do agente para o core. • SnapshotTimeout: tempo de espera para que uma operação de snapshot do VSS seja concluída antes que ela seja abandonada e expire. • TransferTimeout: tempo de espera para contatos adicionais do core antes de abandonar o snapshot. • NetworkReadTimeout: o tempo limite para operações de leitura de rede relacionadas à transferência. • NetworkWriteTimeout: o tempo limite para operações de gravação de rede relacionadas à transferência. • InitialQueueSize: o tamanho da fila inicial de solicitações. • MinVolumeFreeSpacePercents: quantidade mínima de espaço livre em um volume expressa em porcentagem. • MaxChangeLogsSizePercents: tamanho máximo dos registros de alterações no driver como parte da capacidade do volume medida em porcentagem. • EnableVerification: um valor que indica se a confirmação de diagnóstico para cada bloco enviado ao Core deve ser realizada.
public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }	Obtém ou define a configuração do armazenamento O objeto AgentProtectionStorageConfiguration contém os seguintes dados: • RepositoryId - nome do repositório onde os pontos de recuperação do Agent serão armazenados • EncryptionKeyId - o ID da chave de criptografia dos pontos de recuperação desse Agent. Uma cadeia de caracteres vazia significa nenhuma criptografia
public string Key { get; set; }	O método Key gera uma chave pseudoaleatória (mas não criptograficamente segura), que pode ser usada como senha única para autenticar solicitações de transferência.
public bool ForceBaseImage { get; set; }	Obtém ou define o valor que indica se a transferência foi uma captura de imagem de base forçada.

Tabela 112.

Método	Descrição
public bool IsLogTruncation { get; set; }	Obtém ou define o valor que indica se o registro está sendo truncado.
public uint LatestEpochSeenByCore { get; set; }	Obtém ou define o valor de epoch mais recente. O método LatestEpochSeenByCore é o número original do snapshot mais recentemente capturado pelo Core. Esse é o “número de epoch” atribuído pelo driver do filtro a este snapshot específico no momento em que ele foi capturado com o VSS.
public Guid SnapshotSetId { get; set; }	Obtém ou define o GUID atribuído pelo VSS a este snapshot.
public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }	Obtém ou define o conjunto de informações do snapshot para cada volume incluído no snapshot.

VirtualMachineLocation (espaço de nomes Replay.Common.Contracts.Virtualization)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro VirtualMachineLocation.

Tabela 113.

Método	Descrição
public string Description { get; set;}	Obtém ou define uma descrição desse local legível para humanos.
public string Method { get; set;}	Obtém ou define o nome da VM.

VolumeImageIdsCollection (espaço de nomes Replay.Core.Contracts.RecoveryPoints)

Herda seus valores do parâmetro System.Collections.ObjectModel.Collection<string>.

VolumeName (espaço de nomes Replay.Common.Contracts.Metadata.Storage)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro VolumeName.

Tabela 114.

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.

Tabela 114.

Método	Descrição
public string UrlEncode()	Obtém uma versão do nome codificada como URL que pode ser passada adequadamente em uma URL. **NOTA:** Existe um problema conhecido no .NET 4.0 WCF (https://connect.microsoft.com/VisualStudio/feedback/ViewFeedback.aspx?FeedbackID=413312) que impede os caracteres de escape de caminho de funcionar corretamente em um modelo de URI. Visto que o nome do volume contém '\' e '?', substitua os caracteres especiais '\' e '?' por outros caracteres especiais.
public string GetMountName()	Retorna um nome para esse volume que é válido para a imagem do volume de montagem em alguma pasta.

VolumeNameCollection (espaço de nomes eplay.Common.Contracts.Metadata.Storage)

Herda seus valores do parâmetro System.Collections.ObjectModel.Collection<VolumeName>.

A tabela a seguir apresenta os objetos disponíveis para o parâmetro VolumeNameCollection.

Tabela 115.

Método	Descrição
public override bool Equals(object obj)	Determina se essa instância e um objeto especificado, que também deve ser um objeto VolumeNameCollection, têm o mesmo valor. (Substitui Object.Equals(Object).)
public override int GetHashCode()	Retorna o código hash de VolumeNameCollection. (Substitui Object.GetHashCode().)

VolumeSnapshotInfo (espaço de nomes Replay.Common.Contracts.Transfer)

A tabela a seguir apresenta os objetos disponíveis para o parâmetro VolumeSnapshotInfo.

Tabela 116.

Método	Descrição
public Uri BlockHashesUri { get; set;}	Obtém ou define o URI em que os hashes MD5 dos blocos de volume podem ser lidos.
public Uri BlockDataUri { get; set;}	Obtém ou define o URI em que os blocos de dados de volume podem ser lidos.

VolumeSnapshotInfoDictionary (espaço de nomes Replay.Common.Contracts.Transfer)

Herda seus valores do parâmetro System.Collections.Generic.Dictionary<VolumeName, VolumeSnapshotInfo>.

Scripts do PowerShell de amostra

Os seguintes scripts de amostra são fornecidos para auxiliar os usuários administrativos na execução de scripts do PowerShell. Os scripts de amostra incluem:

- PreTransferScript.ps1
- PostTransferScript.ps1
- PreExportScript.ps1
- PostExportScript.ps1
- PreNightlyJobScript.ps1
- PostNightlyJobScript.ps1

PreTransferScript.ps1

O PreTransferScript é executado no lado do Agent antes da transferência de um snapshot.

Amostra de PreTransferScript

```
# receiving parameter from transfer job
param([object]$TransferPrescriptParameter)

# building path to Agent's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM =
$regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null

# Converting input parameter into specific object
$TransferPrescriptParameterObject = $TransferPrescriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPrescriptParameter];

# Working with input object. All echo's are logged
if($TransferPrescriptParameterObject -eq $null) {

     echo 'TransferPrescriptParameterObject parameter is null'
}
else {

     echo
     'TransferConfiguration:'$TransferPrescriptParameterObject.TransferConfiguratio
     n

     echo 'StorageConfiguration:'
     $TransferPrescriptParameterObject.StorageConfiguration
}
```

PostTransferScript.ps1

O PostTransferScript é executado no lado do Agent após a transferência de um snapshot.

Amostra de PostTransferScript

```
# receiving parameter from transfer job
param([object] $TransferPostscriptParameter)

# building path to Agent's Common.Contracts.dll and loading this assembly

$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM =
$regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null

# Converting input parameter into specific object
$TransferPostscriptParameterObject = $TransferPostscriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPostscriptParameter];

# Working with input object. All echo's are logged
if($TransferPostscriptParameterObject -eq $null) {

     echo 'TransferPostscriptParameterObject parameter is null'
}
else {
echo 'VolumeNames:' $TransferPostscriptParameterObject.VolumeNames

          echo 'ShadowCopyType:' $TransferPostscriptParameterObject.ShadowCopyType

     echo 'ForceBaseImage:' $TransferPostscriptParameterObject.ForceBaseImage

     echo 'IsLogTruncation:' $TransferPostscriptParameterObject.IsLogTruncation

}
```

PreExportScript.ps1

O PreExportScript é executado no lado do Core antes de qualquer trabalho de exportação.

Amostra de PreExportScript

```
# receiving parameter from export job
param([object]$ExportJobRequest)

# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM =
$regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null

# Converting input parameter into specific object
$ExportJobRequestObject = $ExportJobRequest -as
[Replay.Core.Contracts.Export.ExportJobRequest]

# Working with input object. All echo's are logged
```

```
if($ExportJobRequestObject -eq $null) {
     echo 'ExportJobRequestObject parameter is null'
}
else {
     echo 'Location:' $ExportJobRequestObject.Location
     echo 'Priority:' $ExportJobRequestObject.StorageConfiguration
}
```

PostExportScript.ps1

O PostExportScript é executado no lado do Core após qualquer trabalho de exportação.

NOTA: Não há parâmetros de entrada para o PostExportScript quando usado para executar uma vez no Agent exportado após a inicialização inicial. O Agent regular deve conter esse script na pasta de scripts do PowerShell como PostExportScript.ps1.

Amostra de PostExportScript

```
# receiving parameter from export job
param([object]$ExportJobRequest)

# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM =
$regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2 = $regVal2 + 'CoreService\Common.Contracts.dll'

# Converting input parameter into specific object
$ExportJobRequestObject = $ExportJobRequest -as
[Replay.Core.Contracts.Export.ExportJobRequest]

# Working with input object. All echo's are logged
if($ExportJobRequestObject -eq $null) {
     echo 'ExportJobRequestObject parameter is null'
}
else {
     echo 'VolumeImageIds:' $ExportJobRequestObject.VolumeImageIds
     echo 'RamInMegabytes:' $ExportJobRequestObject.RamInMegabytes
}
```

PreNightlyJobScript.ps1

O PreNightlyJobScript é executado antes de todo trabalho noturno no lado do Core. Ele contém o parâmetro $JobClassName, que ajuda a lidar com os trabalhos subordinados separadamente.

Amostra de PreNightlyJobScript

```
# receiving parameters from Nightlyjob
param([System.String]$JobClassMethod , [object]$NightlyAttachabilityJobRequest,
[object]$RollupJobRequest, [object]$Agents, [object]$ChecksumCheckJobRequest,
[object]$TransferJobRequest, [int]$LatestEpochSeenByCore)

# building path to Core's Common.Contracts.dll and loading this assembly
```

```
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM =
$regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null

# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job, Checksum
Check Job and Log Truncation Job. All of them are triggering the script, and
$JobClassMethod (contain job name that calls the script) helps to handle those child
jobs separately
switch ($JobClassMethod) {

# working with NightlyAttachability Job
   NightlyAttachabilityJob {

      $NightlyAttachabilityJobRequestObject = $NightlyAttachabilityJobRequest -as
      [Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];

      echo 'Nightly Attachability job results:';

            if($NightlyAttachabilityJobRequestObject -eq $null) {

                  echo 'NightlyAttachabilityJobRequestObject parameter is null';

            }

            else {

                  echo '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 após todo trabalho noturno no lado do Core. Ele contém o parâmetro $JobClassName, que ajuda a lidar com os trabalhos subordinados separadamente.

Amostra de PostNightlyJobScript

```
# receiving parameters from Nightlyjob
param([System.String]$JobClassMethod , [object]$NightlyAttachabilityJobRequest,
[object]$RollupJobRequest, [object]$Agents, [object]$ChecksumCheckJobRequest,
[object]$TransferJobRequest, [int]$LatestEpochSeenByCore,
[object]$TakeSnapshotResponse)

# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM =
$regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2= $regVal2 + 'CoreService\Core.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal2) | out-null

# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job, Checksum
Check Job and Log Truncation Job. All of them are triggering the script, and
$JobClassMethod (contain job name that calls the script) helps to handle those child
jobs separately
switch ($JobClassMethod) {

# working with NightlyAttachability Job
   NightlyAttachabilityJob {

      $NightlyAttachabilityJobRequestObject = $NightlyAttachabilityJobRequest -as
      [Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];

      echo 'Nightly Attachability job results:';

      if($NightlyAttachabilityJobRequestObject -eq $null) {

            echo 'NightlyAttachabilityJobRequestObject parameter is null';

      }

      else {

            echo '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;
    }
}
```

Sobre scripts Bourne Shell no AppAssure 5

Bourne shell (sh) ou Bourne Again Shell (BASH) é uma linguagem de shell ou intérprete de linha de comando para sistemas operacionais baseados em Unix e é usado no AppAssure 5 com Linux para personalizar ambientes e especificar que certas operações ocorram em uma sequência predeterminada. .sh é a extensão de arquivo e convenção de nomenclatura para arquivos Bourne shell.

Usando os ganchos de pré e pós-transferência e de script de exportação, é possível executar operações do sistema antes e depois de uma transferência ou exportação. Por exemplo, você talvez queira desativar certo cronjob enquanto a transferência está ocorrendo e ativá-lo assim que ela for concluída. Outro exemplo incluiria a necessidade de executar comandos para liberar dados específicos de aplicativos em disco. O conteúdo é gravado em um arquivo temporário e executado usando exec. Isso fará o script ser executado usando o intérprete definido na primeira linha do script, por exemplo, (#!/usr/bin/env bash) ou o shell padrão definido pela variável de ambiente $SHELL, se aquela não estiver presente. Dependendo de sua preferência, é possível substituir e usar qualquer intérprete, por exemplo, zsh, tcsh, e assim por diante, na linha #! do script para usar sua preferência, se ela for diferente do shell padrão.

É possível adicionar objetos disponíveis do parâmetro TransferPrescript ou adicionar seus próprios comandos aos scripts PreTransferScript.sh e PostTransfer.sh para personalizá-los.

Pré-requisitos para scripts do Bourne Shell

Todos os scripts devem ter o nome PreTransferScript.sh, PostTransfer.sh e PostExportScript.sh e precisam residir no diretório /opt/appassure/scripts/.

Teste dos scripts do Bourne Shell

É possível testar os scripts que deseja executar usando o editor de arquivos de script (.sh).

NOTA: Se os scripts pré-Bourne Shell ou pós-Bourne Shell falharem, o trabalho também falhará. Há informações sobre o trabalho disponíveis no arquivo /var/log/appassure/appassure.log.

Os scripts bem-sucedidos retornarão o código de saída 0.

Parâmetros de entrada de scripts do Bourne Shell

Os parâmetros dos scripts do Bourne Shell no AppAssure 5 são descritos nas tabelas a seguir.

TransferPrescriptParameters_VolumeNames

A tabela a seguir apresenta os objetos disponíveis para o parâmetro TransferPrescript.

Tabela 117.

Método	Descrição
public VolumeNameCollection VolumeNames (get; set;)	Obtém ou define o conjunto de nomes de volume para transferência. VolumeNames é uma estrutura de dados que contém os seguintes dados: • GuidName - O GUID associado ao volume, usado como o nome, caso DisplayName não esteja definido. • DisplayName - O nome de exibição do volume.
public ShadowCopyType ShadowCopyType { get; set; }	Obtém ou define o tipo de cópia da transferência. ShadowCopyType é uma enumeração com valores. Os valores disponíveis são: • Unknown • Copy • Full
public string Key { get; set; }	O método Key gera uma chave pseudoaleatória (mas não criptograficamente segura), que pode ser usada como senha única para autenticar solicitações de transferência.
public bool ForceBaseImage { get; set; }	Obtém ou define o valor que indica se a transferência foi uma captura de imagem de base forçada.
public bool IsLogTruncation { get; set; }	Obtém ou define o valor que indica se o registro está sendo truncado.
public uint LatestEpochSeenByCore { get; set; }	Obtém ou define o valor de epoch mais recente. O método LatestEpochSeenByCore é o número original do snapshot mais recentemente capturado pelo Core. Esse é o “número de epoch” atribuído pelo driver do filtro a este snapshot específico no momento em que ele foi capturado com o VSS.

TransferPostscriptParameter

A tabela a seguir apresenta os objetos disponíveis para o parâmetro TransferPostscript.

Tabela 118.

Método	Descrição
public VolumeNameCollection VolumeNames (get; set;)	Obtém ou define o conjunto de nomes de volume para transferência. VolumeNames é uma estrutura de dados que contém os seguintes dados: • GuidName - O GUID associado ao volume, usado como o nome, caso DisplayName não esteja definido. • DisplayName - O nome de exibição do volume.
public ShadowCopyType ShadowCopyType { get; set; }	Obtém ou define o tipo de cópia da transferência. ShadowCopyType é uma enumeração com valores. Os valores disponíveis são: • Unknown • Copy • Full
public string Key { get; set; }	O método Key gera uma chave pseudoaleatória (mas não criptograficamente segura), que pode ser usada como senha única para autenticar solicitações de transferência.
public bool ForceBaseImage { get; set; }	Obtém ou define o valor que indica se a transferência foi uma captura de imagem de base forçada.
public bool IsLogTruncation { get; set; }	Obtém ou define o valor que indica se o registro está sendo truncado.
public uint LatestEpochSeenByCore { get; set; }	Obtém ou define o valor de epoch mais recente. O método LatestEpochSeenByCore é o número original do snapshot mais recentemente capturado pelo Core. Esse é o “número de epoch” atribuído pelo driver do filtro a este snapshot específico no momento em que ele foi capturado com o VSS.

Scripts do Bourne Shell de amostra

Os seguintes scripts de amostra são fornecidos para auxiliar os usuários administrativos na execução de scripts do Bourne Shell para Agents. É possível usar os scripts de amostra e personalizá-los conforme necessário. Os scripts de amostra para Agents incluem:

- PreTransferScript.sh
- PostTransferScript.sh
- PostExportScript.sh

NOTA: O Agent usa o comando de shell 'exec' para iniciar o script. Você pode indicar que intérprete deve executar o script definindo essa informação na primeira linha do script, semelhante ao modo de definir para qualquer script normal executado na linha de comando. Se o intérprete não for especificado, o shell padrão interpretará o script. Se você optar por outra coisa que não seja o shell padrão, precisará garantir que o intérprete especificado esteja disponível em todas as máquinas protegidas.

PreTransferScript.sh

O PreTransferScript é executado no lado do Agent antes da transferência de um snapshot.

O seguinte script armazena os valores de parâmetros de entrada no arquivo Pre(Post)TransferScriptResult.txt, que está localizado e armazenado no diretório base raiz.

Amostra de PreTransferScript

```
#!/bin/bash
echo
"TransferPrescriptParameter_VolumeNames=$TransferPrescriptParameter_VolumeNames
TransferPrescriptParameter_ShadowCopyType=$TransferPrescriptParameter_ShadowCopyTyp
e
TransferPrescriptParameter_Key=$TransferPrescriptParameter_Key
TransferPrescriptParameter_ForceBaseImage=$TransferPrescriptParameter_ForceBaseImag
e
TransferPrescriptParameter_IsLogTruncation=$TransferPrescriptParameter_IsLogTruncat
ion
TransferPrescriptParameter_LatestEpochSeenByCore=$TransferPrescriptParameter_Latest
EpochSeenByCore" > ~/PreTransferScriptResult.txt
exit 0
```

PostTransferScript.sh

O PostTransferScript é executado no lado do Agent após a transferência de um snapshot.

O seguinte script armazena os valores de parâmetros de entrada no arquivo Pre(Post)TransferScriptResult.txt, que está localizado e armazenado no diretório base raiz.

Amostra de PostTransferScript

```
#!/bin/bash
echo "TransferPostscriptParameter_VolumeNames=$TransferPostscriptParameter_VolumeNames
TransferPostscriptParameter_ShadowCopyType=$TransferPostscriptParameter_ShadowCopyType
TransferPostscriptParameter_Key=$TransferPostscriptParameter_Key
TransferPostscriptParameter_ForceBaseImage=$TransferPostscriptParameter_ForceBaseImage
TransferPostscriptParameter_IsLogTruncation=$TransferPostscriptParameter_IsLogTruncati
on
TransferPostscriptParameter_LatestEpochSeenByCore=$TransferPostscriptParameter_LatestE
pochSeenByCore" > ~/PostTransferScriptResult.txt
exit 0
```

PostExportScript.sh

O PostExportScript é executado no lado do Agent após a transferência.

O seguinte script armazena os valores de parâmetros de entrada no arquivo Pre(Post)ExportScriptResult.txt, que está localizado e armazenado no diretório base raiz.

Amostra de PostExportScript

```
#!/bin/bash
echo
"$curr_name-exported" > /etc/hostname
exit 0
```

Glossário

A

Agente

Agente é uma máquina ou server protegido ou a ser protegido pelo AppAssure 5.

AppAssure 5

O AppAssure 5 estabelece um novo padrão de proteção de dados unificada, combinando cópia de segurança, replicação e recuperação em uma única solução, projetada para ser a cópia de segurança mais rápida e confiável para a proteção de máquinas virtuais (VM) e de ambientes físicos e de nuvem.

Atribuição de marca branca

O AppAssure 5 fornece a capacidade de os provedores de serviços de cópia de segurança e de recuperação após desastres colocarem um rótulo branco ou uma nova marca no AppAssure 5 com sua própria identidade e, depois, vendê-lo ou distribuí-lo como seu próprio produto ou serviço.

C

Capacidade de anexação do SQL

A capacidade de anexação do SQL é uma execução de teste dentro do AppAssure 5 Core para garantir que todos os pontos de recuperação do SQL estejam sem erro e disponíveis para cópia de segurança no caso de falha.

Central Management Console

O AppAssure 5 Central Management Console é um portal de gerenciamento de vários cores. Ele simplifica o processo de gerenciamento de diversas implementações do AppAssure 5 Core. Usando o Central Management Console, é possível agrupar e gerenciar as implementações usando uma única interface baseada na Web.

Chave de licença

A chave de licença obtida ao se registrar no Portal de licenças de software da Dell para uma conta é usada para acessar o Portal de licenças de software da Dell. Do Portal de licenças de software da Dell, é possível baixar AppAssure 5 Core e Agents, gerenciar licenças e grupos, monitorar a atividade de grupos, registrar máquinas, criar contas, convidar usuários e gerar relatórios.

Cluster

Consulte T.

Cluster Continuous Replication (CCR)

Uma solução não compartilhada de cluster de ativação pós-falha de armazenamento que usa a tecnologia integrada de envio de log assíncrono para criar e manter uma cópia de cada grupo de armazenamento em um segundo server de um cluster de ativação pós-falha. A CCR foi projetada para ser uma solução de um ou dois data centers, para fornecer alta disponibilidade e resiliência local. É um dos dois tipos de implementação de server de caixa de correio em cluster (CMS) disponíveis no Exchange 2007.

Cluster de ativação pós-falha do Windows

Um grupo de computadores independentes que funcionam juntos para aumentar a disponibilidade de aplicativos e serviços. Os servers em cluster (chamados de nós) são conectados por cabos físicos e por software. Se um dos nós do cluster falhar, outro nó começará a prestar o serviço (um processo conhecido como ativação pós-falha). Os usuários têm interrupções mínimas no serviço. O AppAssure 5 oferece suporte à proteção de vários tipos de cluster de SQL Server e Exchange Server.

Cluster de servers

Consulte T.

Compressão

A Storage Networking Industry Association (SNIA) define a compressão como o processo de codificação de dados que visa reduzir seu tamanho.

Core

O AppAssure 5 Core é o componente central da arquitetura do AppAssure. O Core fornece os serviços essenciais de backup, recuperação, retenção, replicação, arquivamento e gerenciamento. No contexto da replicação, o Core também é chamado de *core de origem*. O core de origem é o core originador; o core de destino é o destino.

Core de destino

Também chamado de *core de réplica*, é o AppAssure 5 Core que recebe os dados replicados do core de origem.

core remoto

Um core remoto representa um AppAssure 5 Core acessado por uma máquina que não é core por meio do Local Mount Utility.

Criptografia

Os dados são criptografados com a intenção de que estejam acessíveis apenas aos usuários autorizados que têm a chave de descriptografia apropriada. Os dados são criptografados usando AES de 256 bits no modo Cipher Block Chaining (CBC). No CBC, XOR é aplicado a cada bloco de dados com o bloco de texto cifrado anterior, antes de ser criptografado. Dessa forma, cada novo bloco de texto cifrado depende de todos os blocos anteriores de texto simples. Uma frase de acesso é usada como vetor de inicialização.

D

Deduplicação global

A Storage Networking Industry Association (SNIA) define a deduplicação de dados como a substituição de várias cópias dos dados, com níveis variados de granularidade, por referências a uma cópia compartilhada, para economizar espaço de armazenamento ou largura de banda. O AppAssure 5 Volume Manager realiza a deduplicação global de dados dentro de um volume lógico. O nível de granularidade da deduplicação é 8 KB. O escopo da deduplicação no AppAssure 5 é limitado às máquinas protegidas que usam o mesmo repositório e a mesma chave de criptografia.

F

Frase de acesso

A frase de acesso é uma chave usada na criptografia de dados. Se a frase de acesso for perdida, os dados não poderão ser recuperados.

Funções de gerenciamento

O AppAssure 5 Central Management Console introduz um novo conceito de funções de gerenciamento que permite dividir a responsabilidade administrativa entre administradores confiáveis de dados e serviços, além de acessar o controle de forma a oferecer suporte à delegação segura e eficiente da administração.

G

Grupo de disponibilidade de banco de dados (DAG)

Um conjunto de até 16 servers de caixa de correio do Microsoft Exchange Server 2010 que fornece recuperação automática em nível de banco de dados após uma falha de banco de dados, server ou rede. Os DAGs usam a replicação contínua e um subconjunto de tecnologias de cluster de ativação pós-falha do Windows para fornecer alta disponibilidade e resiliência local. Os servers de caixa de correio em um DAG monitoram uns aos outros em busca de falhas. Quando um server de caixa de correio é adicionado a um DAG, ele funciona com os outros servers no DAG para fornecer recuperação automática ao nível de banco de dados após falhas de banco de dados.

L

Live Recovery

O AppAssure Live Recovery é uma tecnologia de recuperação instantânea para VMs e servers. Fornece um acesso quase contínuo a volumes de dados em um servidor virtual ou físico, que permite recuperar um volume inteiro com RTO próximo de zero e RPO de minutos.

Local Console

O Local Console é uma interface baseada na Web que permite gerenciar totalmente o AppAssure 5 Core.

Local Mount Utility

O Local Mount Utility (LMU) é um aplicativo que pode ser adquirido via download, que permite a montagem de um ponto de recuperação em um AppAssure 5 Core remoto a partir de qualquer máquina.

M

Máquina

Uma máquina, também conhecida como agente, é uma máquina ou um server físico ou virtual protegido pelo AppAssure 5 Core. No contexto da replicação, um core também pode ser designado como *core de origem*.

Máquina de réplica de destino

A instância de uma máquina protegida em um core de destino é conhecida como agente de destino ou agente de réplica.

Montabilidade

A montabilidade do Exchange é um recurso de detecção de corrupção que informa os administradores sobre possíveis falhas e garante que todos os dados nos servidores do Exchange sejam recuperados com êxito em caso de falha.

N

Nó de cluster

Máquina individual que faz parte de um cluster de ativação pós-falha do Windows.

P

Pontos de recuperação

Os pontos de recuperação são uma coleção de Snapshots de vários volumes de disco. Por exemplo, C:, D: e E.

Portal de licenças

O Portal de licenças de software da Dell é uma interface da Web na qual os usuários e parceiros registram, baixam, ativam e gerenciam licenças do AppAssure 5.

PowerShell Scripting

O Windows PowerShell é um ambiente conectado ao Microsoft .NET Framework projetado visando a automação administrativa. O AppAssure 5 inclui SDKs de cliente abrangentes para PowerShell scripting que permitem aos administradores automatizar a administração e o gerenciamento dos recursos do AppAssure 5 pela execução de comandos diretos ou por meio de scripts.

Propagação

Na replicação, a transferência inicial de imagens de base de deduplicação e snapshots incrementais dos agentes protegidos, que pode acrescentar centenas ou milhares de gigabytes de dados. A replicação inicial pode ser propagada para o core de destino usando mídias externas, o que é útil para grandes conjuntos de dados ou locais com links lentos.

Q

Quórum

Para um cluster de ativação pós-falha, o número de elementos que devem estar on-line para determinado cluster continuar em execução. Os elementos relevantes nesse contexto são os nós do cluster. Esse termo também pode se referir ao recurso com capacidade de quórum selecionado para manter os dados de configuração necessários para a recuperação do cluster. Esses dados contém detalhes de todas as alterações aplicadas ao banco de dados de cluster. O recurso de quórum geralmente é acessível a outros recursos de cluster de modo que qualquer nó de cluster tem acesso às mais recentes alterações do banco de dados. Por padrão há apenas um recurso de quórum por cluster de server. A configuração de quórum especial (definições de cluster de ativação pós-falha) determina o ponto em que muitas falhas interrompem a execução do cluster.

R

Replicação

A replicação se otimiza com um algoritmo exclusivo de leitura-correspondência-gravação (RMW) acoplado fortemente à deduplicação. Ela representa o relacionamento entre os cores de origem e de destino no mesmo local ou em dois locais com link lento, em que o core de origem transmite de forma assíncrona os dados ao core de destino ou de origem em base por agente.

Repositório

O repositório, gerenciado pelo AppAssure 5 Core, é uma pasta usada para armazenar os snapshots capturados dos servers e máquinas protegidos. O repositório pode residir em tecnologias de armazenamento diferentes, como rede de área de armazenamento (SAN), armazenamento por conexão direta (DAS) ou armazenamento conectado à rede (NAS).

Retenção

A retenção define o período pelo qual os snapshots de cópia de segurança de máquinas protegidas são armazenados no AppAssure 5 Core. A política de retenção é aplicada aos pontos de recuperação por meio do processo de rollup.

Reversão

É o processo de reversão dos volumes em uma máquina a partir de pontos de recuperação.

Rollup

Trata-se de um procedimento de manutenção noturna interna que reforça a política de retenção por meio de colapso e eliminação de pontos de recuperação datados. O AppAssure 5 reduz o rollup apenas a operações de metadados.

S

Single Copy Cluster

Uma solução compartilhada de cluster de ativação pós-falha de armazenamento, que usa uma única cópia de um grupo de armazenamento no armazenamento que é compartilhado entre os nós do cluster. É um dos dois tipos de implementação de server de caixa de correio em cluster disponíveis no Exchange 2007.

Sistema de arquivos de objeto

O armazenamento de objeto escalável do AppAssure é um componente de sistema de arquivos de objeto. Ele trata todos os blocos de dados, dos quais os snapshots são derivados, como objetos. Ele armazena, recupera, mantém e replica esses objetos. Foi projetado para oferecer desempenho de entrada e saída (I/O) escalável em conjunto com deduplicação global de dados, criptografia e gerenciamento de retenção. O sistema de arquivos de objeto faz interface direta com tecnologias de armazenamento padrão do setor.

Smart Agent

O AppAssure 5 Smart Agent é instalado nas máquinas protegidas pelo AppAssure 5 Core. O Smart Agent rastreia os blocos alterados no volume de disco e cria um snapshot dos blocos alterados em um intervalo de proteção predefinido.

Snapshot

Snapshot é um termo comum do setor que define a capacidade de capturar e armazenar o estado de um volume de disco em um determinado ponto, enquanto os aplicativos estão executando. O Snapshot é crítico em caso de necessidade de recuperação do sistema devido a uma interrupção ou falha do sistema. Os snapshots do AppAssure 5 reconhecem o aplicativo, ou seja, todas as transações abertas e os registros de transações contínuas são concluídos e os caches são limpos antes da criação do snapshot. O AppAssure 5 usa o Microsoft Volume Shadow Services (VSS) para facilitar snapshots consistentes de falhas de aplicativos.

Soma de verificação

A soma de verificação é uma função que cria blocos de dados que são usados para detectar erros acidentais ocorridos durante a transmissão ou o armazenamento.

Standby virtual

O Standby virtual é um processo físico para virtual (P2V) que cria uma máquina virtual clone de uma máquina protegida ou agente. O Standby virtual pode ser criado usando um processo de exportação *ad hoc* ou de *atualização contínua*. Um Standby virtual criado usando uma *atualização contínua* é atualizado de forma incremental depois de cada snapshot capturado do agente de origem.

T

Transport Layer Security

Transport Layer Security (TLS) é um protocolo moderno de rede de criptografia projetado para garantir a segurança da comunicação pela Internet. Esse protocolo, definido pela Força-Tarefa de Engenharia de Internet, é o sucessor do Secure Sockets Layer (SSL). O termo SSL ainda é geralmente usado, e os protocolos são interoperáveis (um cliente TLS pode fazer o downgrade para se comunicar com um server SSL).

True Scale

True Scale é a arquitetura escalável do AppAssure 5.

Truncamento de log

O truncamento de log é uma função que remove registros de log do log de transações. Para uma máquina do SQL Server, quando você forçar o truncamento dos registros do SQL Server, esse processo identifica espaço livre no server do SQL. Para uma máquina do Exchange Server, você força o truncamento dos logs do Exchange Server. Essa ação libera espaço no server do Exchange.

U

Universal Recovery

A tecnologia AppAssure 5 Universal Recovery oferece flexibilidade ilimitada de restauração de máquinas. Permite realizar uma recuperação monolítica de/para qualquer plataforma física ou virtual de sua escolha, bem como atualizações de recuperação incremental para máquinas virtuais a partir de qualquer origem física ou virtual. Também permite realizar a recuperação de arquivos individuais, pastas, email, itens de calendário, bancos de dados e aplicativos no nível de aplicativo, de item e de objeto.

V

Verified Recovery

A tecnologia Verified Recovery é usada para realizar testes de recuperação e confirmação de backups de forma automatizada. Suporta vários sistemas de arquivo e servidores.

Volume Manager

O AppAssure 5 Volume Manager gerencia objetos e, depois, os armazena e apresenta como um volume lógico. Ele aproveita a arquitetura de pipeline dinâmico para fornecer escalabilidade TruScale, paralelismo e modelo assíncrono de entrada e saída (I/O) para alta taxa de transferência com latência mínima de I/O.

Sobre a Dell

A Dell escuta os clientes e fornece tecnologia inovadora, soluções empresariais e serviços globais de confiança e valor. Para obter mais informações, visite www.software.dell.com.

Contatos da Dell

Suporte técnico:
Suporte online

Vendas e dúvidas sobre produtos:
(800) 306-9329

E-mail:
info@software.dell.com

Recursos do suporte técnico

O suporte técnico está disponível para clientes que compraram produtos de software da Dell com um contrato de manutenção válido e clientes que estão usando versões de teste. Para acessar o Portal de suporte, visite http://software.dell.com/support/.

O Portal de suporte fornece ferramentas de autoajuda, que você pode usar para resolver problemas de forma rápida e independente, 24 horas por dia, 365 dias por ano. Além disso, o Portal fornece acesso direto a engenheiros de suporte de produtos por meio de um sistema online de Solicitação de serviço.

O site permite que você:

- Crie, atualize e gerencie as Solicitações (casos) de serviço.
- Visualize artigos da Base de conhecimento.
- Obtenha notificações de produtos.
- Baixe o software. No caso de software de teste, acesse Downloads de teste.
- Assista a vídeos instrucionais.
- Participe de discussões da comunidade.
- Converse com um engenheiro do suporte.