Dispositivo Dell DL1000
Guia do usuário

Notas, avisos e advertências

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

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

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

2015 - 12

Rev. A01

Índice

1 Apresentando o seu Dell DL1000.....7

Tecnologias de núcleo do Dell DL1000.....7

Live Recovery.....7

Universal Recovery.....7

Eliminação de duplicação global verdadeira.....8

Encryption (Criptografia).....8

Recursos de proteção de dados do Dell DL1000.....8

Núcleo do Dell DL1000.....8

Smart Agent do Dell DL1000.....9

Processo de instantâneos.....9

Replicação — provedor de serviços ou site de recuperação de desastres.....9

Recuperação.....10

Recuperação como serviço.....10

Virtualização e nuvem.....10

Arquitetura de implementação do Dell DL1000.....11

Outras informações úteis.....12

2 Trabalhar com o DL1000.....14

Acessar do Core Console DL1000.....14

Atualizar sites confiáveis no Internet Explorer.....14

Configurar os navegadores para acessar remotamente o Core Console.....14

Gerenciar licenças.....15

Alterar uma chave de licença.....16

Entrar em contato com o servidor do portal de licenças.....16

Alterar o idioma do AppAssure manualmente.....16

Alterar o idioma do sistema operacional durante a instalação.....17

Gerenciar as configurações de núcleo.....17

Alterar o nome de exibição do núcleo.....18

Alterar o horário de trabalho noturno.....18

Modificar as configurações de fila de transferência.....18

Ajustar as configurações de tempo limite de cliente.....18

Definir configurações de cache de eliminação de duplicações.....19

Modificar configurações de mecanismo.....19

Modificar configurações de implantação.....20

Modificar configurações de conexão com banco de dados.....21

Gerenciar eventos.....21

Configurar grupos notificação.....22

Configurar um servidor de e-mail.....23

Configurar um modelo de notificação por e-mail 24
Configurar a redução de repetição 25
Configurar retenção de evento 25
Gerenciar repositórios 26
Ver detalhes de repositório 26
Verificar um repositório 26
Gerenciar a segurança 27
Adicionar uma chave de criptografia 27
Editar uma chave de criptografia 27
Alterar uma senha de chave de criptografia 28
Importar uma chave de criptografia 28
Exportar uma chave de criptografia 28
Remover uma chave de criptografia 29
Gerenciar contas na nuvem 29
Adicionar uma conta na nuvem 29
Editar uma conta na nuvem 30
Definir configurações de conta na nuvem 31
Remover uma conta na nuvem 31
Monitorar o DL1000 32
Fazer upgrade do DL1000 32
Reparar o DL1000 32
Autorecuperação de dispositivo rápido 32

3 Proteger estações de trabalho e servidores 34

Sobre proteção de estações de trabalho e servidores 34
Implantar um agente (instalação por push) 34
Como proteger uma máquina 35
Pausar e retomar a proteção 38
Implantar o software de agente ao proteger um agente 38
Entender os cronogramas de proteção 39
Criar cronogramas personalizados 40
Modificar os cronogramas de proteção 40
Definir as configurações da máquina protegida 42
Ver e modificar as definições de configuração 42
Ver informações do sistema para uma máquina 42
Ver informações de licença 43
Modificar configurações de transferência 43
Arquivar dados 46
Criar um arquivamento 46
Importar um arquivamento 48
Arquivamento em uma nuvem 50
Ver os diagnósticos do sistema 50

Ver logs de máquina 50
Upload de logs da máquina..... 50
Cancelar operações em uma máquina 50
Ver status da máquina e outros detalhes 51
Gerenciar múltiplas máquinas 52
Implantar em várias máquinas 52
Monitorar a implantação de várias máquinas 52
Proteger múltiplas máquinas..... 53
Monitorar a proteção de várias máquinas 55

4 Recuperar dados..... 56
Gerenciar a recuperação 56
Gerenciar instantâneos e pontos de recuperação 56
Ver pontos de recuperação 56
Ver um ponto de recuperação específico..... 57
Montar um ponto de recuperação para uma máquina Windows 58
Desmontar pontos de recuperação selecionados 59
Desmontar todos os pontos de recuperação 59
Montar um ponto de recuperação para uma máquina Linux 59
Remover pontos de recuperação 60
Apagar uma cadeia de ponto de recuperação órfã..... 60
Forçar um instantâneo 61
Restaurar dados 61
Sobre exportar dados protegidos de máquinas Windows para máquinas virtuais..... 62
Gerenciar exportações..... 63
Exportar informações de backup de uma máquina Windows para uma máquina virtual 64
Exportar dados do Windows usando a exportação ESXi 64
Exportar dados do Windows usando a exportação de estação de trabalho VMware 67
Exportar dados do Windows usando a exportação do Hyper-V 70
Exportar dados do Windows usando a exportação de Oracle VirtualBox 73
Restaurar volumes a partir de um ponto de recuperação 75
Restaurar volumes para uma máquina Linux usando a linha de comando 79
Iniciar a restauração sem sistema operacional para máquinas Windows 80
Roteiro para realizar uma restauração sem sistema operacional para uma máquina Windows 80
Iniciar uma restauração sem sistema operacional para uma máquina Linux 86
Instalar o utilitário Tela..... 87
Criar partições inicializáveis em uma máquina Linux..... 87

5 Replicar pontos de recuperação..... 89
Replicação..... 89
Roteiro para executar a replicação 90

Replicação para um núcleo autogerenciado....90
Replicar para um núcleo gerenciado por terceiros....94
Replicar um novo agente....94
Replicar dados do agente em uma máquina....96
Configurar a prioridade de replicação para um agente....96
Monitorar a replicação....96
Gerenciar configurações de replicação....98
Remover a replicação....98
Remover uma máquina protegida de replicação do núcleo de origem....99
Remover uma máquina protegida no núcleo de destino....99
Remover um núcleo de destino da replicação....99
Remover um núcleo de origem da replicação....99
Recuperar dados replicados....100
Entender failover e failback....100
Executar failover....101
Executar failback....101

6 Relatório....103
Sobre os relatórios....103
Sobre a barra de ferramentas de relatórios....103
Sobre relatórios de conformidade....103
Sobre relatórios de erros....104
Sobre o relatório resumido de núcleo....104
Resumo de repositórios....104
Resumo de agentes....105
Gerar relatório para um núcleo ou agente....105
Sobre os relatórios de núcleo de console de gestão central....106
Gerar um relatório a partir do console de gestão central....106

7 Obter ajuda....107
Encontrar a documentação e as atualizações de software....107
Documentação....107
Atualizações de software....107
Entrar em contato com a Dell....107
Feedback sobre a documentação....107

1

Apresentando o seu Dell DL1000

O Dell DL1000 combina replicação e backup em um produto de proteção de dados unificado. Ele fornece recuperação confiável de dados de aplicativo a partir de backups para proteger máquinas físicas e máquinas virtuais. O seu dispositivo é capaz de processar até terabytes de dados com recursos incorporados de desduplicação global, compressão, criptografia e replicação para infraestruturas específicas de nuvem pública ou particular. Aplicativos de servidor e dados podem ser recuperados em questão de minutos para fins retenção de dados (DR) e de conformidade.

O DL1000 oferece suporte para ambientes com múltiplos hipervisores em nuvens públicas e particulares Microsoft Hyper-V e VMware vSphere.

Tecnologias de núcleo do Dell DL1000

O seu dispositivo combina as seguintes tecnologias:

- Recuperação em tempo real
- Recuperação universal
- Eliminação de duplicação global real
- Criptografia

Live Recovery

O Live Recovery é uma tecnologia de recuperação instantânea para servidores ou máquinas virtuais. Ele oferece acesso quase contínuo aos volumes de dados em servidores virtuais ou físicos.

A tecnologia de backup e replicação do DL1000 registra instantâneos simultâneos de múltiplos servidores ou máquinas virtuais, oferecendo dados quase instantâneos e proteção do sistema. Você pode voltar a usar o servidor montando o ponto de recuperação sem aguardar uma restauração completa para o armazenamento de produção.

Universal Recovery

O Universal Recovery proporciona uma flexibilidade ilimitada para a restauração da máquina. Você pode restaurar seus backups de sistemas físicos para máquinas virtuais, de máquinas virtuais para máquinas virtuais, de máquinas virtuais para sistemas físicos ou de sistemas físicos para sistemas físicos, e executar restaurações bare-metal para hardwares diferentes.

A tecnologia do Universal Recovery também acelera as transferências entre diferentes plataformas de máquinas virtuais. Por exemplo, transferências de dados de VMware para Hyper-V ou de Hyper-V para VMware. Ela possibilita a recuperação no nível de aplicativo, no nível de item e no nível de objeto (arquivos individuais, pastas, e-mails, itens de calendário, bancos de dados e aplicativos).

Eliminação de duplicação global verdadeira

A Eliminação de duplicação global verdadeira elimina dados redundantes ou duplicados executando backups incrementais no nível do bloco das máquinas.

O layout típico de um disco em um servidor consiste em sistema operacional, aplicativos e dados. Na maioria dos ambientes, os administradores frequentemente usam uma versão comum do sistema operacional de servidor e desktop em múltiplos sistemas para obter uma maior eficiência de implementação e gerenciamento. Quando o backup é feito no nível de bloco em múltiplas máquinas, ele proporciona uma visão mais detalhada do que está no backup e do que não está, independentemente da fonte. Esses dados contêm o sistema operacional, os aplicativos e os dados de aplicativos em todo o ambiente.

Figura 1. Diagrama da Eliminação de duplicação global verdadeira

Encryption (Criptografia)

O DL1000 fornece criptografia para proteger backups e dados em repouso contra o acesso e uso não autorizados, garantindo a privacidade dos dados. Os dados podem ser acessados e descriptografados usando a chave de criptografia. A criptografia é realizada de forma embutida nos dados do instantâneo, a velocidades de linha, sem afetar o desempenho.

Recursos de proteção de dados do Dell DL1000

Núcleo do Dell DL1000

O Núcleo é o componente central da arquitetura de implementação do DL1000. O Núcleo armazena e gerencia os backups da máquina e fornece serviços de backup, recuperação, retenção, replicação, arquivamento e gerenciamento. O Núcleo é uma rede independente, um computador endereçável que executa uma versão de 64 bits dos sistemas operacionais Microsoft Windows Server 2012 R2 Foundation e Standard. O dispositivo executa, em linha, compressão, criptografia e eliminação de duplicação de dados, baseado no destino, dos dados recebidos do agente. Em seguida, o Núcleo armazena os backups instantâneos no repositório, que reside no dispositivo. Os Núcleos são emparelhados para replicação.

O repositório reside no armazenamento interno do Núcleo. O Núcleo é gerenciado acessando a seguinte URL em um navegador da Web com JavaScript habilitado: **https://CORENAME:8006/apprecovery/admin**.

Smart Agent do Dell DL1000

O Smart Agent é instalado na máquina protegida pelo núcleo. O Smart Agent rastreia os blocos alterados no volume de disco e depois cria uma imagem dos blocos alterados em um intervalo de proteção predefinido. A abordagem infinita de instantâneos incrementais no nível do bloco impede a cópia repetida dos mesmos dados da máquina protegida no Núcleo.

Após sua configuração, o agente usa a tecnologia inteligente para rastrear os blocos alterados nos volumes de disco protegidos. Quando o instantâneo está pronto, ele é rapidamente transferido para o Núcleo por meio de conexões inteligentes baseadas em soquete e com multithread.

Processo de instantâneos

O processo de proteção do DL1000 começa quando uma imagem base é transferida de uma máquina protegida para o Núcleo. Nessa fase, uma cópia completa da máquina é transportada através da rede em operação normal, seguida de infinitos instantâneos incrementais. O agente do DL1000 para Windows usa o Serviço de cópias de sombra de volume da Microsoft (VSS) para congelar e fechar para novas sessões os dados de aplicativo no disco, a fim de capturar um backup consistente com o sistema de arquivos e um consistente com o aplicativo. Quando um instantâneo é criado, o gravador VSS no servidor de destino impede que novos conteúdos sejam gravados no disco. Durante o processo de interrupção de gravação de conteúdo em disco, todas as operações de E/S do disco são colocadas em fila e retomam apenas depois da conclusão do instantâneo, enquanto as operações em andamento serão concluídas e todos os arquivos abertos serão fechados. O processo de criação de uma cópia de sombra não afeta significativamente o desempenho do sistema de produção.

O DL1000 usa o VSS da Microsoft porque ele possui suporte integrado para todas as tecnologias internas do Windows, como NTFS, Registro e Active Directory, para liberar os dados no disco antes de obter o instantâneo. Além disso, outros aplicativos corporativos, como o Microsoft Exchange e o SQL, usam os plug-ins do gravador VSS para serem notificados quando um instantâneo estiver sendo preparado e quando devem liberar suas páginas de banco de dados usadas no disco para colocar o banco de dados em um estado transacional consistente. Os dados capturados são rapidamente transferidos e armazenados no Núcleo.

Replicação — provedor de serviços ou site de recuperação de desastres

A replicação é o processo de copiar pontos de recuperação de um AppAssure Core e transmiti-los para um outro AppAssure Core em um local secundário com a finalidade de recuperação de desastres. O processo exige uma relação origem/destino emparelhada entre dois ou mais núcleos.

O núcleo de origem copia os pontos de recuperação das máquinas protegidas selecionadas e, em seguida, transmite assíncrona e continuamente os dados de instantâneos incrementais para o núcleo de destino em um local de recuperação de desastres remoto. Você pode configurar a replicação de saída para um data center da sua própria empresa ou para um local de recuperação de desastres remoto (ou seja, um núcleo de destino "autogerenciado"). Ou, você pode configurar uma replicação de saída para um fornecedor de serviço gerenciado (MSP - Managed Service Provider) ou para um provedor de nuvem que hospeda serviços de backup e de recuperação de desastres fora do local. Quando for replicar para um núcleo de destino de terceiros, você pode usar os fluxos de trabalho incorporados que permitem que você solicite conexões e receba notificações de feedback automáticas.

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

A replicação apresenta auto-otimização com um algoritmo RMW (Read-Match-Write - Leitura/correspondência/gravação) único, fortemente ligado à Eliminação de duplicação. Com a replicação de RMW, o serviço de replicação de origem e de destino faz a correspondência das chaves antes de transferir os dados e, em seguida, replica pela WAN apenas os dados compactados, criptografados e com as duplicações eliminadas, resultando em uma redução de 10x nos requisitos de largura de banda.

A replicação começa com a propagação: a transferência inicial de imagens base com duplicações eliminadas e posteriormente de instantâneos incrementais das máquinas protegidas, o que pode totalizar centenas ou milhares de gigabytes de dados. A replicação inicial pode ser propagada para o núcleo de destino usando uma mídia externa. Isso normalmente é útil para grandes conjuntos de dados ou em locais com links lentos. Os dados no arquivo de propagação são compactados, criptografados e as duplicações são eliminadas. Se o tamanho total do arquivo for maior do que o espaço disponível na mídia removível, ele poderá englobar múltiplos dispositivos dependendo do espaço disponível na mídia. Durante o processo de propagação, os pontos de recuperação incrementais são replicados para o local de destino. Depois de o núcleo de destino consumir o arquivo de propagação, os pontos de recuperação incrementais recém-replicados são sincronizados automaticamente.

Recuperação

A recuperação pode ser realizada no site local ou no site remoto replicado. Depois que a implementação estiver em estado estável com proteção local e replicação opcional, o Núcleo do DL1000 permite que você execute uma recuperação usando o Verified Recovery, o Universal Recovery ou o Live Recovery.

Recuperação como serviço

Os fornecedores de serviço gerenciado (MSPs - Managed Service Provider) podem utilizar-se do DL1000 como plataforma para oferecer a recuperação como serviço (RaaS - Recovery As A Service). A RaaS facilita a recuperação completa na nuvem através da replicação dos servidores físicos e virtuais dos clientes. A nuvem do fornecedor de serviço é usada como máquinas virtuais para suportar as operações de teste de recuperação ou de recuperação de fato. Clientes que quiserem executar a recuperação na nuvem podem configurar a replicação em suas máquinas protegidas nos núcleos locais para um fornecedor de serviço do AppAssure. Na eventualidade de um desastre, os MSPs podem realizar instantaneamente o provisionamento das máquinas virtuais para o cliente.

O DL1000 não possui infraestrutura para multilocatários. Os MSPs podem usar o DL1000 em múltiplos sites e por fim criar um ambiente de multilocatários.

Virtualização e nuvem

O Núcleo do DL1000 é compatível com nuvem, o que permite que você utilize-se da capacidade de computação da nuvem para recuperação e arquivamento.

O DL1000 pode exportar qualquer máquina protegida ou replicada para versões licenciadas do VMware ou Hyper-V. Com as exportações contínuas, a máquina virtual é atualizada de forma incremental após cada instantâneo. As atualizações incrementais são rápidas e fornecem clones de espera prontos para serem acionados com um clique de um botão. Os tipos de exportação de máquina virtual suportados são:

- VMware Workstation ou Server em uma pasta

- Exportação direta para um host Vsphere ou VMware ESXi
- Exportação para Oracle VirtualBox
- Microsoft Hyper-V Server no Windows Server 2008 (x64)
- Microsoft Hyper-V Server no Windows Server 2008 R2
- Microsoft Hyper-V Server no Windows Server 2012 R2

Você agora pode arquivar os dados do seu repositório na nuvem usando plataformas como Microsoft Azure, Amazon S3, Rackspace Cloud Block Storage ou outros serviços de nuvem baseados em OpenStack.

Arquitetura de implementação do Dell DL1000

A arquitetura de implementação do DL1000 consiste em componentes locais e remotos. Os componentes remotos podem ser opcionais para aqueles ambientes que não exigem um site de recuperação de desastres ou um fornecedor de serviço gerenciado para recuperação fora do local. Uma implementação local básica consiste em um servidor de backup, chamado de Núcleo, e uma ou mais máquinas protegidas, conhecidas como agentes. O componente fora do local é ativado por meio de replicação, o que fornece recursos de recuperação total no site de recuperação de desastres. O Núcleo do DL1000 usa imagens base e instantâneos incrementais para compilar pontos de recuperação de agentes protegidos.

Além disso, o DL1000 é sensível à aplicação, pois ele pode detectar a presença do Microsoft Exchange e SQL, e de seus respectivos bancos de dados e arquivos de log. Os backups são executados com o uso de instantâneos em nível de bloco sensíveis à aplicação. O DL1000 faz o truncamento do log do servidor protegido do Microsoft Exchange.

O diagrama a seguir mostra uma simples implementação do DL1000. Os agentes do DL1000 são instalados em máquinas, como, por exemplo, um servidor de arquivos, um servidor de e-mail, um servidor de banco de dados; ou máquinas virtuais são conectadas e protegidas por um único Núcleo do DL1000, o qual consiste no repositório central. O Portal de licenças de software da Dell gerencia as assinaturas de licenças, os grupos e os usuários dos agentes e núcleos no ambiente. O Portal de licenças permite aos usuários fazer login, ativar contas, fazer download de software e implementar agentes e núcleos conforme a licença para o ambiente.

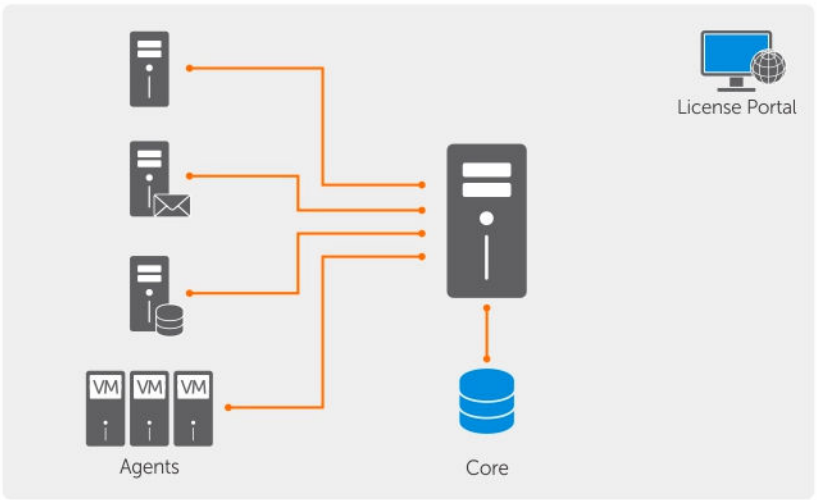

Figura 2. Arquitetura de implementação do Dell DL1000

Você pode também implementar múltiplos Núcleos do DL1000, conforme mostrado no diagrama abaixo. Um console central gerencia múltiplos núcleos.

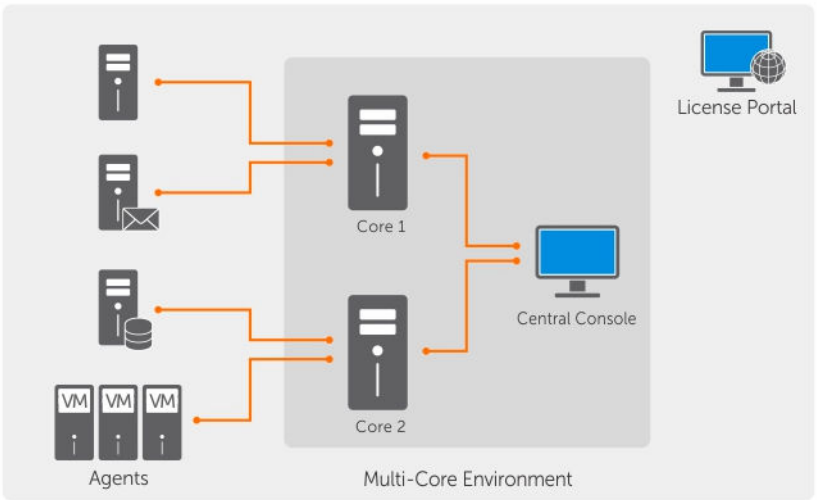

Figura 3. Arquitetura de implementação multinúcleos do DL1000

Outras informações úteis

NOTA: Para obter toda a documentação do Dell OpenManage, vá para **dell.com/openmanagemanuals**.

NOTA: Verifique sempre se há atualizações disponíveis no site **dell.com/support/home** e leia-as primeiro, pois elas geralmente substituem informações contidas em outros documentos.

NOTA: Para obter qualquer documentação relacionada ao Dell OpenManage Server Administrator, consulte **dell.com/openmanage/manuals**.

A documentação do produto inclui:

Guia de Noções Básicas	Fornece uma visão geral dos recursos do sistema, a configuração do seu sistema e as especificações técnicas. Este documento também é fornecido com o sistema.
Guia rápido do sistema	Fornece informações sobre como configurar o hardware e instalar o software na solução AppAssure.
Manual do proprietário	Fornece informações sobre os recursos do sistema e descreve como solucionar problemas do sistema e como instalar ou substituir componentes.
Guia de implementação	Fornece informações sobre a implementação do hardware e a implementação inicial do dispositivo.
Guia do usuário	Fornece informações sobre a configuração e o gerenciamento do sistema.
Notas de versão	Fornece informações sobre o produto e informações adicionais sobre o dispositivo Dell DL1000.
Guia de Interoperabilidade	Fornece informações sobre hardwares e softwares suportados pelo dispositivo DL1000, bem como considerações, recomendações e regras de uso.
Guia do Usuário do OpenManage Server Administrator	Fornece informações sobre o uso do Dell OpenManage Server Administrator para gerenciar o sistema.
Mídia de recursos	As mídias fornecidas com o sistema, as quais contêm a documentação e as ferramentas para a configuração e o gerenciamento do sistema. Inclui aquelas relativas ao sistema operacional, ao software de gerenciamento do sistema, a atualizações do sistema e aos componentes adquiridos com o sistema.

2

Trabalhar com o DL1000

Acessar do Core Console DL1000

Para acessar o Core Console DL1000:

1. Atualize os sites confiáveis em seu navegador.
2. Configure o navegador para acessar remotamente o console do núcleo DL1000. Consulte Configurar navegadores para acesso remoto ao Core Console.
3. Execute um dos seguintes procedimentos para acessar o Core Console DL1000:
   - Faça login localmente em seu servidor de núcleo DL1000 e depois clique duas vezes no ícone **Core Console**.
   - Digite um dos seguintes URLs em seu navegador:
     - **https://<nomedoseuservidordenucleo>:8006/apprecovery/admin/core**
     - **https://<endereçoIPdoseuservidordenucleo>:8006/apprecovery/admin/core**

Atualizar sites confiáveis no Internet Explorer

Para atualizar os sites confiáveis no Internet Explorer:

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

Configurar os navegadores para acessar remotamente o Core Console

Para acessar o console do núcleo através de uma máquina remota, você precisa modificar as configurações do seu navegador.

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

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

NOTA: Certifique-se de que a opção **Internet Explorer Enhanced Security Configuration** (Configuração de segurança aprimorada do Internet Explorer) esteja ativada quando você acessar o console da web do núcleo, seja local ou remotamente. Para ativar a opção **Internet Explorer Enhanced Security Configuration** (Configuração de segurança aprimorada do Internet Explorer):

1. Abra o **Server Manager** (Gerenciador de servidores).
2. Selecione a opção **Local Server IE Enhanced Security Configuration** (Configuração de segurança aprimorada do IE para servidor local) mostrada à direita. Certifique-se de que a opção esteja marcada como **On** (Ativada).

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

1. Abra o Internet Explorer.
2. No menu **Ferramentas**, selecione **Opções de Internet**, seguido pela guia **Segurança**.
3. Clique em **Sites confiáveis** e depois clique em **Sites**.
4. Desmarque a opção **Exigir verificação do servidor (https:) para todos os sites na zona** e depois adicione http://<*nome de host ou endereço IP do servidor de dispositivo que hospeda o núcleo AppAssure*> para **Sites confiáveis**.
5. Clique em **Fechar**, selecione **Sites confiáveis** e depois clique em **Nível personalizado**.
6. Navegue até **Diversos → Mostrar conteúdo misto** e selecione **Ativar**.
7. Desça até o final da tela, em **Autenticação de usuário → Logon** e selecione **Logon automático com o nome de usuário e a senha atuais**.
8. Clique em **OK** e depois selecione a guia **Avançado**.
9. Navegue até **Multimídia** e selecione **Reproduzir animações em páginas da Web**.
10. Navegue até **Segurança**, marque a opção **Habilitar a Autenticação Integrada do Windows** e depois clique em **OK**.

Para modificar as configurações do navegador Mozilla Firefox:

1. Na barra de endereços do Firefox, digite **about:config** e depois clique em **I'll be careful, I promise** (Eu vou ser cuidadoso, prometo) caso seja solicitado.
2. Pesquise pelo termo **ntlm**.

   A pesquisa deve encontrar no mínimo três resultados.
3. Clique duas vezes em **network.automatic-ntlm-auth.trusted-uris** e digite a seguinte configuração conforme apropriado para a máquina:
   - Para máquinas locais, digite o nome do host.
   - Para máquinas remotas, digite o nome do host ou o endereço IP separado por uma vírgula do sistema de dispositivo que hospeda o AppAssure Core; por exemplo, *endereço IP*,*nome do host*.
4. Reinicie o Firefox.

Gerenciar licenças

Você pode gerenciar as licenças do DL1000 diretamente através do Core Console. No console, você pode alterar a chave de licença e entrar em contato com o servidor de licença. Você pode também acessar o portal de licenças Dell AppAssure na página **Licensing** (Licenças) no Core Console.

A página **Licensing** (Licenças) inclui as seguintes informações:

- Tipo de licença

- Status de licença
- Número de máquinas protegidas
- Status de última resposta do servidor de licença
- Horário de último contato com o servidor de licença
- Próxima tentativa agendada de contato com o servidor de licença
- Limitações de licença

Alterar uma chave de licença

Para alterar uma chave de licença:

1. Navegue até o Core Console e selecione **Configuration (Configuração)** → **Licensing (Licenças)**.
   A página **Licensing** (Licenças) é mostrada.
2. Na página **License Details** (Detalhes de licença), clique em **Change** (Alterar).
   A caixa de diálogo **Change License Key** (Alterar chave de licença) é mostrada.
3. Na caixa de diálogo **Change License Key** (Alterar chave de licença), digite a nova chave de licença e depois clique em **OK**.

Entrar em contato com o servidor do portal de licenças

O Core Console entra em contato com o servidor do portal para atualizar as alterações feitas no portal de licenças. A comunicação com o servidor do portal ocorre automaticamente em intervalos designados; no entanto, você pode iniciar a comunicação sob demanda.

Para entrar em contato com o servidor do portal:

1. Navegue até o Core Console e clique em **Configuration (Configuração)** → **Licensing (Licenças)**.
   A página **Licensing** (Licenças) é mostrada.
2. Na opção **License Server** (Servidor de licenças), clique em **Contact Now** (Entrar em contato agora).

Alterar o idioma do AppAssure manualmente

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

1. Abra o editor de registro usando o comando `regdit`.
2. Navegue até **HKEY_LOCAL_MACHINE** → **SOFTWARE** → **AppRecovery** → **Core** → **Localization** (Localização).
3. Abra **Lcid**.
4. Selecione **decimal**.
5. Digite o valor do idioma necessário na caixa `Value data` (Dados de valor), os valores de idiomas compatíveis são:
   a. Inglês: 1033
   b. Português brasileiro: 1046
   c. Espanhol: 1034
   d. Francês: 1036
   e. Alemão: 1031
   f. Chinês simplificado: 2052

g. Japonês: 1041
h. Coreano: 1042

6. Clique com o botão direito e reinicie os serviços na ordem apresentada:
   a. Windows Management Instrumentation
   b. SRM Web Service
   c. AppAssure Core
7. Limpe o cache do navegador.
8. Feche o navegador e reinicie o console do núcleo pelo ícone na área de trabalho.

Alterar o idioma do sistema operacional durante a instalação

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

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

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

1. Na página **Start** (Iniciar), digite `language` (idioma) e certifique-se de que o escopo de busca esteja definido para Settings (Configurações).
2. No painel **Results** (Resultados), selecione **Language** (Idioma).
3. No painel **Change your language preferences** (Alterar suas preferências de idioma), selecione **Add a language** (Adicionar um idioma).
4. Procure ou pesquise pelo idioma que você deseja instalar.
   Por exemplo, selecione Catalan (Catalão) e, em seguida, selecione Add (Adicionar). O idioma catalão é agora adicionado como um dos idiomas.
5. No painel Change your language preferences (Alterar suas preferências de idioma), selecione **Options** (Opções) ao lado do idioma que você adicionou.
6. Se um pacote de idioma estiver disponível para o seu idioma, selecione `Download and install language pack` (Fazer download e instalar pacote de idiomas).
7. Quando o pacote de idiomas é instalado, o idioma é mostrado como disponível para uso como idioma de exibição do Windows.
8. Para tornar este o idioma de exibição, mova-o para o topo de sua lista de idiomas.
9. Faça logout e depois faça o login novamente no Windows para que a alteração seja aplicada.

Gerenciar as configurações de núcleo

As configurações de núcleo são usadas para definir diversas definições de desempenho e configuração. A maioria das configurações é definida para o melhor uso, mas você pode alterar as configurações a seguir conforme for necessário:

- Geral
- Trabalhos noturnos
- Fila de transferência
- Configurações de tempo-limite de cliente
- Configuração de cache de eliminação de duplicações

- Configurações de conexão com banco de dados

Alterar o nome de exibição do núcleo

NOTA: É recomendável que você selecione um nome de exibição da permanente durante a configuração inicial do seu dispositivo. Se você alterá-lo mais tarde, você precisa executar várias etapas manualmente para garantir que o novo nome do host entre em vigor e o aparelho funcione corretamente.

Para alterar o nome de exibição do núcleo:

1. Navegue até o Core Console e clique em **Configuration (Configuração)** → **Settings (Definições)**.
2. Na seção **General** (Geral), clique em **Change** (Alterar).
   A caixa de diálogo **Display Name** (Nome de exibição) é mostrada.
3. Na caixa de texto **Display Name** (Nome de exibição), digite um novo nome de exibição do núcleo.
4. Clique em **OK**.

Alterar o horário de trabalho noturno

A opção Nightly Job (Trabalho noturno) agenda trabalhos como acúmulo, conectividade e truncamento para agentes protegidos pelo núcleo.

Para ajustar o horário de trabalho noturno:

1. Navegue até o Core Console e selecione **Configuration (Configuração)** → **Settings (Definições)**.
2. Na seção **Nightly Jobs** (Trabalhos noturnos), clique em **Change** (Alterar).
   A caixa de diálogo **Nightly Jobs** (Trabalhos noturnos) é mostrada.
3. Na caixa de texto **Nightly Jobs Time** (Horário de trabalhos noturnos), digite um novo horário inicial.
4. Clique em **OK**.

Modificar as configurações de fila de transferência

As configurações de fila de transferência são definições a nível de núcleo que estabelecem o número máximo de transferências simultâneas e novas tentativas para transferência de dados.

Para modificar as configurações de fila de transferência:

1. Navegue até o Core Console e clique em **Configuration (Configuração)** → **Settings (Definições)**.
2. Na seção **Transfer Queue** (Fila de transferência), clique em **Change** (Alterar).
   A caixa de diálogo **Transfer Queue** (Fila de transferência) é mostrada.
3. Na caixa de texto **Maximum Concurrent Transfers** (Máximo de transferências simultâneas), digite um valor para atualizar o número de transferências simultâneas.
   Defina um número de 1 a 60. Quanto menor o número, menor a carga sobre a rede e outros recursos do sistema. A medida em que a capacidade que está sendo processada aumenta, a carga no sistema também sobe.
4. Na caixa de texto **Maximum Retries** (Máximo de novas tentativas), digite um valor para atualizar o número máximo de novas tentativas.
5. Clique em **OK**.

Ajustar as configurações de tempo limite de cliente

As configurações de tempo limite do cliente especificam o número de segundos ou minutos que o servidor aguardará antes de atingir seu limite ao se conectar a um cliente.

Para ajustar as configurações de tempo limite de cliente:

1. Navegue até o Core Console e clique em **Configuration (Configuração)** → **Settings (Definições)**.
2. Na seção **Client Timeout Settings** (Configurações de tempo limite de cliente), clique em **Change** (Alterar).

   A caixa de diálogo **Client Timeout Settings** (Configurações de tempo limite de cliente) é mostrada.
3. Na caixa de texto **Connection Timeout** (Tempo limite de conexão), digite o número de minutos e segundos até que ocorra um tempo limite de conexão.
4. Na caixa de texto **Read/Write Timeout** (Tempo limite de leitura/gravação), digite o número de minutos e segundos que você deseja que decorram antes que ocorra um tempo limite durante um evento de leitura/gravação.
5. Clique em **OK**.

Definir configurações de cache de eliminação de duplicações

A eliminação de duplicações global reduz a quantidade de espaço de armazenamento em disco necessária para seus dados em backup. O gerenciador de volume de eliminação de duplicações (DVM) combina um conjunto de locais de armazenamento em um único repositório. O cache de eliminação de duplicações mantém referências a blocos únicos. Por padrão, o cache de eliminação de duplicações é de 1,5 GB. Se a quantidade de informações redundantes for tão alta que o cache de eliminação de duplicações ficar cheio, o repositório não pode mais aproveitar completamente a eliminação de duplicações no repositório para dados recém-adicionados. Você pode então aumentar o tamanho do cache de eliminação de duplicações alterando a configuração de cache de eliminação de duplicações no console do núcleo.

Para configurar as configurações de cache de eliminação de duplicações:

1. Navegue até o Core Console e clique em **Configuration (Configuração)** → **Settings (Definições)**.
2. Na seção **Replay Deduplication Cache Configuration** (Configuração de cache de eliminação de duplicações), clique em **Change** (Alterar).

   A caixa de diálogo **Deduplication Cache Configuration** (Configuração de cache de eliminação de duplicações) é mostrada.
3. Na caixa de texto **Primary Cache Location** (Local de cache principal), digite o local de cache principal atualizado.
4. Na caixa de texto **Secondary Cache Location** (Local de cache secundário), digite o local de cache secundário atualizado.
5. Na caixa de texto **Metadata Cache Location** (Local de cache de metadados), digite o local de cache de metadados atualizado.
6. Clique em **OK**.

   NOTA: Você precisa reiniciar o serviço do núcleo para que as modificações tenham efeito.

Modificar configurações de mecanismo

Para modificar as configurações de mecanismo:

1. Navegue até o Core Console e clique em **Configuration (Configuração)** → **Settings (Definições)**.
2. Na seção **Replay Engine Configuration** (Configuração de mecanismo de reprodução), clique em **Change** (Alterar).

   A caixa de diálogo **Replay Engine Configuration** (Configuração de mecanismo de reprodução) é mostrada.

3. Na caixa de diálogo **Replay Engine Configuration** (Configuração de mecanismo de reprodução), especifique o **IP address** (Endereço IP). Selecione uma das opções a seguir:
   - Para usar o endereço IP preferido de seu TCP/IP, clique em **Automatically Determined** (Determinado automaticamente).
   - Para inserir um endereço IP manualmente, clique em **Use a specific IP Address** (Usar um endereço IP específico).
4. Digite as informações de configuração descritas da seguinte forma:

Caixa de texto	Descrição
Preferable Port (Porta preferida)	Digite um número de porta ou aceite a configuração padrão (8007 é a porta padrão). A porta é usada para especificar o canal de comunicação para o mecanismo.
Admin Group (Grupo de administração)	Digite um novo nome para o grupo de administração. O nome padrão é BUILTIN\Administrators.
Minimum Async I/O Length (Comprimento mínimo de E/S assíncrona)	Digite um valor ou escolha uma configuração padrão. A configuração descreve o comprimento mínimo de E/S assíncrona. A configuração padrão é 65536.
Receive Buffer Size (Tamanho de buffer de recebimento)	Digite um tamanho de buffer de entrada ou aceite a configuração padrão. A configuração padrão é 8192.
Send Buffer Size (Tamanho de buffer de envio)	Digite um tamanho de buffer de envio ou aceite a configuração padrão. A configuração padrão é 8192.
Read Timeout (Tempo limite de leitura)	Digite um valor de tempo limite de leitura ou escolha a configuração padrão. A configuração padrão é 00:00:30.
Write Timeout (Tempo limite de gravação)	Digite um valor de tempo limite de gravação ou escolha a configuração padrão. A configuração padrão é 00:00:30.

5. Selecione **No Delay** (Sem atraso).
6. Clique em **OK**.

Modificar configurações de implantação

Para modificar configurações de implantação:

1. Navegue até o Core Console e clique na guia **Configuration** (Máquinas) e depois em **Settings** (Configurações).
2. No painel **Deploy Settings** (Configurações de implantação), clique em **Change** (Alterar).

   A caixa de diálogo **Deploy Settings** (Configurações de implantação) é mostrada.
3. Na caixa de texto **Agent Installer Name** (Nome do instalador do agente), digite o nome do arquivo executável do agente. O padrão é Agentweb.exe.
4. Na caixa de texto **Core Address** (Endereço do núcleo), digite o endereço do núcleo.

5. Na caixa de texto **Failed Receive Timeout** (Falha de tempo limite de recebimento), digite o número de minutos sem atividade até o tempo limite expirar.
6. Na caixa de texto **Max Parallel Installs** (Número máximo de instalações paralelas), digite um número para o máximo de instalações que podem ser feitas em paralelo.
7. Selecione qualquer uma ou ambas as configurações opcionais a seguir:
   - Automatic reboot after install (Inicialização automática após instalação)
   - Protect After Deploy (Proteger após a implantação)
8. Clique em **OK**.

Modificar configurações de conexão com banco de dados

Para modificar as configurações de conexão com banco de dados:

1. Navegue até o Core Console e clique em **Configuration (Configuração) → Settings (Definições)**.
2. Na seção **Database Connection Settings** (Configurações de conexão de banco de dados), realize uma das seguintes ações:
   - Para restaurar a configuração padrão, clique em **Restore Default** (Restaurar padrão).
   - Para modificar as configurações de conexão com o banco de dados, clique em **Change** (Alterar).

   Ao clicar em Change (Alterar), a caixa de diálogo **Database Connection Settings** (Configurações de conexão de banco de dados) é mostrada.
3. Digite as configurações para modificar a conexão de banco de dados descritas da seguinte maneira:

Caixa de texto	Descrição
Host name (Nome do host)	Digite um nome de host para a conexão de banco de dados.
Port (Porta)	Digite um número de porta para a conexão de banco de dados.
User Name (Nome de usuário; opcional)	Digite um nome de usuário para acessar e gerenciar as configurações de conexão do banco. Ele é usado para especificar as credenciais de login para acessar a conexão com o banco de dados.
Password (Senha; opcional)	Digite uma senha para acessar e gerenciar as configurações de conexão com o banco de dados.
Retain event and job history for, days (Reter histórico de trabalho e eventos por, dias)	Insira o número de dias para reter o histórico de eventos e trabalhos para a conexão com o banco de dados.

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

Gerenciar eventos

O núcleo inclui conjuntos pré-definidos de eventos, que podem ser usados para notificar os administradores sobre problemas críticos no núcleo ou nos trabalhos de backup.

Na guia **Events** (Eventos), você pode gerenciar grupos de notificação, configurações de SMTP de e-mail, configurações de servidor, logs de rastreamento ativados, configuração da nuvem, redução de repetição e retenção de eventos.

A opção Notification Groups (Grupos de notificação) permite que você gerencie grupos notificação, a partir dos quais você pode:

- Especificar um evento para o qual você deseja gerar um alerta para o seguinte:
  - Clusters
  - Capacidade de conectividade
  - Trabalhos
  - Licenças
  - Truncamento de log
  - Arquivamento
  - Serviço de núcleo
  - Exportar
  - Proteção
  - Replicação
  - Reversão
- Especificar o tipo de alerta (de erro, de advertências e informativos).
- Especificar para quem e onde o os alertas são enviados. Entre as opções, estão:
  - Endereço de e-mail
  - Logs de eventos do Windows
  - Servidor de log do sistema
- Especificar um limite de tempo para repetição.
- Especificar o período de retenção para todos os eventos.

Configurar grupos notificação

Para configurar grupos de notificação:

1. No Core Console, selecione **Configuration (Configuração)** → **Events (Eventos)**.
2. Clique em **Add Group** (Adicionar grupo).

   A caixa de diálogo **Add Notification Group** (Adicionar grupo de notificação) é aberta e mostra dois painéis:
   - **Enable Alerts (Ativar alertas)**
   - **Notification Options (Opções de notificação)**

Ativar alertas

Ativar alertas permite a você definir o conjunto de eventos do sistema que você deseja fazer login, criar relatórios e definir alertas.

NOTA: Para criar alertas para todos os eventos, selecione **All Alertas** (Todos os alertas).

- Para criar alertas específicos para erros, avisos, mensagens informativas ou uma combinação destes, selecione uma das seguintes opções:
  - Ícone de triângulo vermelho (erro)

- Ícone de triângulo amarelo (aviso)
- Círculo azul (informações)
- Seta curva (restaura o padrão)

• Para criar alertas para eventos específicos, clique no símbolo **>** ao lado do grupo relevante e marque a caixa de seleção para ativar o alerta.

Configurar opções de notificação

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

   As opções de notificação são:

Caixa de texto	Descrição
Notify by e-mail (Notificar por e-mail)	Indique os destinatários da notificação por e-mail. Você pode digitar múltiplos endereços de e-mail separados, além de cópias e cópias ocultas conforme mostrado abaixo: • **Para:** • **CC:** • **BCC:**
Notify by Windows Event Log (Notificar por log de eventos do Windows)	Selecione essa opção se você deseja que a notificação de alertas seja relatada através do log de eventos do Windows.
Notify by sys logd (Notificar por logs de sistema)	Selecione essa opção se você deseja que alertas sejam relatados através de logs de sistema. Digite os detalhes do log de sistema nas caixas de texto a seguir: • **Hostname (Nome de host):** • **Port (Porta):1**
Notify by Toast alerts (Notificar por alertas do sistema)	Selecione essa opção se você deseja que o alerta apareça como uma janela pop-up no canto inferior direito da tela.

2. Clique em **OK**.

   A seguinte mensagem é mostrada: **The Group name cannot be changed after the creation of the Notification Group. are you sure you want to use this name?** (O nome do grupo não pode ser alterado após a criação do grupo de notificação. Tem certeza de que deseja usar esse nome?).

   - Para salvar o nome do grupo, clique em **Yes** (Sim).
   - Para alterar o nome do grupo, clique em **No** (Não). Retorne para a janela **Notification Options** (Opções de notificação), atualize o nome do grupo e outras configurações do grupo de notificação e salve o trabalho.

Configurar um servidor de e-mail

NOTA: Você precisa definir configurações de grupo de notificação, incluindo ativar a opção **Notifiy by email** (Notificar por e-mail) antes de enviar mensagens de alerta por e-mail.

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

1. No Core Console, clique em **Configuration (Configuração)** → **Events (Eventos)**.
2. No painel **Email Settings** (Configurações de e-mail), clique em **SMPT server** (Servidor SMPT).
   A caixa de diálogo **SMTP Server Settings** (Configurações de servidor SMTP) é mostrada.
3. Digite os detalhes do servidor de e-mail da seguinte maneira:

Caixa de texto	Descrição
SMTP Server (Servidor SMTP)	Digite o nome do servidor de e-mail que será usado pelo modelo de notificação por e-mail. A convenção de nomenclatura inclui o nome do host, domínio e sufixo; por exemplo **smtp.gmail.com**.
From (De)	Digite um endereço de e-mail de retorno. Ele é usado para especificar o endereço de e-mail de retorno do modelo de notificação de e-mail; por exemplo, **noreply@localhost.com**.
Username (Nome de usuário)	Digite um nome de usuário para o servidor de e-mail.
Password (Senha)	Digite uma senha para acessar o servidor de e-mail.
Port (Porta)	Digite um número de porta. Ele é usado para identificar a porta para o servidor de e-mail; por exemplo, a porta 587 para o Gmail. O padrão é 25.
Timeout (seconds) (Tempo limite (segundos))	Para especificar por quanto tempo será tentado realizar uma conexão antes do tempo limite expirar, digite um valor inteiro. Ele é usado para estabelecer o tempo, em segundos, ao tentar se conectar ao servidor de e-mail antes que o tempo limite expire. O padrão é 30 segundos.
TLS	Selecione essa opção se o servidor de e-mail usa uma conexão segura como TLS (Transport Layer Security, segurança da camada de transporte) ou SSL (Secure Sockets Layer, camada de soquete seguro).

4. Clique em **Send Test Email** (Enviar e-mail de teste) e realize o seguinte:
   a. Na caixa de diálogo Send Test Email (Enviar e-mail de teste), digite um endereço de e-mail de destino para a mensagem de teste e clique em **Send** (Enviar).
   b. Se a mensagem de teste falhar, feche a caixa de diálogo de erro e a caixa de diálogo **Send Test Email** (Enviar e-mail de teste) e verifique novamente as definições de configuração do seu servidor de e-mail. Repita a etapa 4.
   c. Clique em **OK** para confirmar.
   d. Verifique se a mensagem de e-mail de teste foi enviada.
   e. Volte à caixa de diálogo SMTP Server Settings (Configurações de servidor SMTP), clique em **Save** (Salvar) para fechar a caixa de diálogo e salve suas configurações.

Configurar um modelo de notificação por e-mail

Para receber notificações por e-mail sobre eventos, você precisa configurar um servidor de e-mail e um modelo de notificação por e-mail.

NOTA: Para receber mensagens de alerta por e-mail, defina as configurações de grupo de notificação e ative a opção **Notify by email** (Notificar por e-mail).

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

1. No Core Console, clique em **Configuration (Configuração)** → **Events (Eventos)**.
2. No painel **Email Settings** (Configurações de e-mail), clique em **Change** (Alterar).

   A caixa de diálogo **Edit Email Notification Configuration** (Editar configuração de notificação por e-mail) é mostrada.
3. Selecione **Enable email notifications** (Ativar notificações por e-mail) e, em seguida, digite os detalhes para o servidor de e-mail da seguinte maneira:

Caixa de texto	Descrição
Email Subject (Assunto do e-mail)	Digite o assunto para o modelo de e-mail. Ele é usado para definir o assunto do modelo de notificação por e-mail; por exemplo, `<hostname> - <level> <name>`.
E-mail	Digite as informações do corpo do modelo que descrevem o evento, quando ele ocorreu e a gravidade.

4. Clique em **Send Test Email** (Enviar e-mail de teste) e realize o seguinte:
   a. Na caixa de diálogo Send Test Email (Enviar e-mail de teste), digite um endereço de e-mail de destino para a mensagem de teste e clique em **Send** (Enviar).
   b. Se a mensagem de teste falhar, saia da caixa de diálogo de erro e da caixa de diálogo Send Test Email (Enviar e-mail de teste), clique em **OK** para salvar as configurações do modelo atual de e-mail e modificar as configurações de servidor de e-mail; consulte Configurar um servidor de e-mail e um modelo de notificação por e-mail. Lembre-se de digitar novamente a senha dessa conta de e-mail. Salve as configurações e, em seguida, retorne à etapa 4.
   c. Clique em **OK** para confirmar.
   d. Verifique se a mensagem de e-mail de teste foi enviada.
   e. Retorne para a caixa de diálogo **Edit Email Notification Configuration** (Editar configuração de notificação por e-mail), clique em **OK** para fechar a caixa de diálogo e salve suas configurações.

Configurar a redução de repetição

Para configurar a redução de repetição:

1. No Core Console, clique em **Configuration (Configuração)** → **Events (Eventos)**.
2. Na seção **Repetition Reduction** (Redução de repetição), clique em **Change** (Alterar).

   A caixa de diálogo **Enable Repetition Reduction** (Ativar redução de repetição) é mostrada.
3. Selecione **Enable Repetition Reduction** (Ativar redução de repetição).
4. Na caixa de texto **Store events for** (Armazenar eventos para), digite o número de minutos para armazenar os eventos para redução de repetição.
5. Clique em **OK**.

Configurar retenção de evento

Para configurar a retenção evento:

1. No Core Console, clique em **Configuration (Configuração)** → **Settings (Configurações)**.
2. Em **Database Connection Settings** (Configurações de conexão de banco de dados), clique em **change** (Alterar).

   A caixa de diálogo **Database Connection Settings** (Configurações de conexão de banco de dados) é mostrada.
3. Na caixa de texto **Retain event and job history for** (Reter evento e histórico de trabalho por), digite o número de dias pelo qual você deseja reter as informações sobre eventos.

Por exemplo, você pode selecionar 30 dias (padrão).

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

Gerenciar repositórios

Um repositório armazena instantâneos que são capturados de estações de trabalho e servidores protegidos. O repositório para o DL1000 é pré-configurado. O repositório está no armazenamento interno do sistema.

Entre os principais conceitos e considerações de repositório, estão:

- O repositório é baseado no sistema de arquivos de objeto escalonável do AppAssure.
- Todas as duplicações de dados armazenados dentro de um repositório são eliminadas globalmente.
- O sistema de arquivos de objeto escalonável pode fornecer desempenho de E/S escalonável em conjunto com desduplicação global de dados, criptografia e gerenciamento de retenção.

Ver detalhes de repositório

Para ver detalhes de repositório:

1. No Core Console, clique em **Configuration (Configuração)** → **Repositories (Repositório)**.
2. Clique em **>** ao lado da coluna **Status** do repositório cujos detalhes você quer ver.
3. Os detalhes do repositório incluem os locais e as estatísticas de armazenamento. Os detalhes de local de armazenamento incluem: caminho de metadados, caminho de dados e tamanho. As informações estatísticas incluem:
   - **Deduplication** (Eliminação de duplicações) — Informada como o número de resultados de desduplicação de blocos, erros de desduplicação de blocos e taxa de compressão de blocos.
   - **Record I/O** (E/S de registro) — Composta da taxa (MB/s), taxa de leitura (MB/s) e taxa de gravação (MB/s).
   - **Storage Engine** (Mecanismo de armazenamento) — Inclui a taxa (MB/s), taxa de leitura (MB/s) e taxa de gravação (MB/s).

Verificar um repositório

O Core Console pode executar uma verificação de diagnóstico de um volume de repositório quando ocorrerem erros . Os erros de núcleo podem ser o resultado de um desligamento incorreto ou de uma falha de hardware.

NOTA: Este procedimento deve ser executado somente para fins de diagnóstico.

Para verificar um repositório:

1. Clique em **Configuration (Configuração)** → **Repositories (Repositórios)**.
2. Clique no ícone Settings (Configurações) ao lado da coluna Compression Ratio (Razão de compressão) abaixo do botão **Actions** (Ações).
3. Clique em **Check** (Verificar).

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

NOTA: Quando você faz uma verificação, todas as tarefas ativas associadas a esse repositório serão canceladas. Antes da verificação ser iniciada, será mostrada uma mensagem solicitando que você confirme antes de prosseguir com a verificação. É recomendável redesenvolver o cache dos pontos de recuperação. A falha de uma verificação resultará em você tendo que restaurar o repositório de um arquivo.

Gerenciar a segurança

O DL1000 proporciona uma sólida criptografia. Ao aplicá-la, backups de máquinas protegidas ficam inacessíveis. Somente o usuário com a chave de criptografia pode acessá-los e decodificar os dados. A criptografia não afeta o desempenho. Entre os principais conceitos e considerações de segurança, estão:

- A criptografia é realizada usando AES de 256 bits no modo de sequenciamento de blocos de cifras (CBC) que está em conformidade com o SHA-3.
- A desduplicação funciona dentro de um domínio de criptografia para garantir a privacidade.
- A criptografia é executada sem afetar o desempenho.
- Você pode adicionar, remover, importar, exportar, modificar e apagar uma chave de criptografia configurada no núcleo.

Adicionar uma chave de criptografia

Para adicionar uma chave de criptografia:

1. No Core Console, clique em **Configuration (Configuração)** → **Security (Segurança)**.
2. No menu suspenso **Actions** (Ações), clique em **Add Encryption Key** (Adicionar chave de criptografia).
   A caixa de diálogo **Create Encryption Key** (Criar chave de criptografia) é mostrada.
3. Na caixa de diálogo **Create Encryption Key** (Criar chave de criptografia), digite os detalhes para a chave descritos da seguinte forma:

Caixa de texto	Descrição
Name (Nome)	Digite um nome para a chave de criptografia.
Description (Descrição)	Digite uma descrição da chave de criptografia. Ela é usada para fornecer mais detalhes sobre a chave de criptografia.
Passphrase (Senha)	Digite uma senha. Ela é utilizada para controlar o acesso.
Confirm Passphrase (Confirmar senha)	Digite novamente a senha. Ela é usada para confirmar a senha inserida.

4. Clique em **OK**.

   CUIDADO: É recomendável que você proteja a senha. Se você perder a senha, não é possível recuperar os dados.

Editar uma chave de criptografia

Para editar uma chave de criptografia:

1. No Core Console, clique em **Configuration (Configuração)** → **Security (Segurança)**.

A tela **Encryption Keys** (Chaves de criptografia) é mostrada.

2. Clique em **>** ao lado do nome da chave de criptografia que você deseja editar e, em seguida, clique em **Edit** (Editar).

   A caixa de diálogo **Edit Encryption Key** (Editar chave de criptografia) é mostrada.

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

Alterar uma senha de chave de criptografia

Para alterar uma senha de chave de criptografia:

1. No Core Console, clique em **Configuration (Configuração) → Security (Segurança)**.
2. Clique em **>** ao lado do nome da chave de criptografia que você deseja editar e, em seguida, clique em **Change Passphrase** (Alterar senha).

   A caixa de diálogo **Change Passphrase** (Alterar senha) é mostrada.

3. Na caixa de diálogo **Change Passphrase** (Alterar senha), digite a nova senha para a criptografia e, em seguida, digite novamente a senha para confirmar o que você inseriu.
4. Clique em **OK**.

   CUIDADO: É recomendável que você proteja a senha. Se você perder a senha, não é possível acessar os dados no sistema.

Importar uma chave de criptografia

Para importar uma chave de criptografia:

1. No Core Console, clique em **Configuration (Configuração) → Security (Segurança)**.
2. No menu suspenso **Actions** (Ações), clique em **Import** (Importar).

   A caixa de diálogo **Import Key** (Importar chave) é mostrada.

3. Na caixa de diálogo **Import Key** (Importar chave), clique em **Browse** (Procurar) para localizar a chave de criptografia que você deseja importar e depois clique em **Open** (Abrir).
4. Clique em **OK**.

Exportar uma chave de criptografia

Para exportar uma chave de criptografia:

1. No Core Console, clique em **Configuration (Configuração) → Security (Segurança)**.
2. No menu suspenso Configuration (Configuração) da chave de criptografia que você deseja exportar, selecione **Export** (Exportar).

   A caixa de diálogo **Export Key** (Exportar chave) é mostrada.

3. Na caixa de diálogo **Export Key** (Exportar chave), clique em **Save File** (Salvar arquivo) para salvar e armazene as chaves de criptografia em um local seguro.
4. Clique em **OK**.

Remover uma chave de criptografia

Para remover uma chave de criptografia:

1. No Core Console, clique em **Configuration (Configuração)** → **Security (Segurança)**.
2. No menu suspenso Configuration (Configuração) da chave de criptografia que você deseja remover, selecione **Remove** (Remover).

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

   NOTA: Remover uma chave de criptografia não descriptografa os dados.

Gerenciar contas na nuvem

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

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

Adicionar uma conta na nuvem

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

Para adicionar uma conta na nuvem:

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

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

Tabela 1. Adicionar uma conta na nuvem

Tipo de nuvem	Caixa de texto	Descrição
Microsoft Azure	Storage Account Name (Nome da conta de armazenamento)	Digite o nome da conta de armazenamento do Microsoft Azure.
	Access Key (Chave de acesso)	Digite a chave de acesso para sua conta.

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

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

Editar uma conta na nuvem

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

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

NOTA: Você não pode editar o tipo de nuvem.

Definir configurações de conta na nuvem

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

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

     1. Use as setas subir e descer para editar um das opções a seguir:
        - **Request Timeout** (Tempo limite de solicitação): mostrado em minutos e segundos, determina a quantidade de tempo que o AppAssure deve gastar em uma tentativa única para se conectar à conta na nuvem quando houver um atraso. As tentativas de conexão vão terminar após a quantidade de tempo informada.
        - **Retry Count** (Contagem de novas tentativas): determina o número de tentativas que o AppAssure deve realizar antes de determinar que não é possível se comunicar com a nuvem.
        - **Write Buffer Size** (Tamanho do buffer de gravação): determina o tamanho de buffer reservado para gravação de dados arquivados na nuvem.
        - **Read Buffer Size** (Tamanho do buffer de leitura): determina o tamanho de buffer reservado para leitura de dados arquivados na nuvem.
     2. Clique em **Next** (Avançar).
   - Clique em **Reset** (Redefinir). Isso retorna a configuração para as seguintes definições padrão:
     - **Tempo limite de solicitação:** 01:30 (minutos e segundos)
     - **Contagem de novas tentativas:** 3 (tentativas)

Remover uma conta na nuvem

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

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

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

Monitorar o DL1000

Você pode monitorar o status dos subsistemas do dispositivo DL1000 usando a guia **Appliance** (Dispositivo) na página **Overall Status** (Status geral). A página **Overall Status** (Status geral) mostra uma luz de status ao lado de cada subsistema, juntamente com uma descrição do status indicando a integridade do subsistema.

A página Overall Status (Status geral) também fornece links para ferramentas que exploram os detalhes de cada subsistema, algo que pode ser útil para solucionar avisos ou erros. O link **System Administrator** (Administrador de sistema), disponível para subsistemas de hardware de armazenamento e hardware de dispositivo, solicita você a fazer login no aplicativo System Administrador usado para gerenciar o hardware. Para obter mais informações sobre o aplicativo System Administrador, consulte o *Guia do usuário do OpenManage Server Administrador* na página **dell.com/support/manuals**.

Fazer upgrade do DL1000

NOTA: A Dell recomenda que você baixe a versão mais recente disponível do AppAssure no portal de ativação de licenças da Dell usando o instalador.

NOTA: Para outros upgrades de software, você receberá uma notificação para fazer upgrade para a versão mais recente.

Reparar o DL1000

NOTA: Antes de começar o processo de reparo, lembre-se de interromper os serviços de núcleo.

Autorecuperação de dispositivo rápido

A autorecuperação de dispositivo rápido (RASR) é um processo de restauração sem sistema operacional no qual as unidades de sistema operacional são recompiladas para a imagem de fábrica padrão.
Para executar a RASR:

NOTA: A Dell recomenda que você crie uma chave USB RASR depois de configurar o dispositivo. Para criar uma chave USB RASR, consulte a seção Criar a chave USB RASR.

1. Insira a chave USB RASR criada.
2. Reinicialize o dispositivo através da chave USB RASR.
3. Clique em **Rapid Appliance Self Recovery** (Autorecuperação de dispositivo rápido).
   Uma tela de boas-vindas é mostrada.
4. Clique em **Next** (Avançar).
   A tela **Prerequisites** check (Verificação de pré-requisitos) é mostrada.

   NOTA: Certifique-se de que todo o hardware, e outros pré-requisitos sejam verificadas antes de executar a RASR.
5. Clique em **Next** (Avançar).
   A tela **Recovery Mode Selection** (Seleção de modo de recuperação) tela é mostrada com três opções:

- **System Recovery (Recuperação do sistema)**
- **Windows Recovery Wizard (Assistente de recuperação do Windows)**
- **Factory Reset (Redefinição de fábrica)**

6. Selecione a opção **Factory Reset** (Redefinição de fábrica).

   Esta opção irá recuperar o disco do sistema operacional a partir da imagem de fábrica.
7. Clique em **Next** (Avançar).

   A tela **Storage Configuration** (Configuração de armazenamento) é mostrada.
8. Na tela **OS Recovery** (Recuperação de sistema operacional), a seguinte mensagem de aviso é mostrada em uma caixa de diálogo: `This operation will recover the operating system. All OS disk data will be overwritten.` (Essa operação vai recuperar o sistema operacional. Todos os dados serão substituídos).
9. Clique em **Yes** (Sim).

   O disco do sistema operacional começa a ser restaurado de volta à redefinição de fábrica.
10. Clique em **Finish** (Concluir).

Criar o pen drive USB RASR

NOTA: Após a configuração inicial do software, o assistente **AppAssure Appliance Configuration** (Configuração do AppAssure Appliance) é iniciado automaticamente. O ícone de status da guia **Appliance** (Dispositivo) é mostrado na cor amarela.

Para criar um pen drive USB RASR:

1. Navegue até a guia **Appliance** (Dispositivo).
2. Usando a navegação no painel esquerdo, selecione **Appliance (Dispositivo)** → **Backup**.

   A janela **Create RASR USB Drive** (Criar unidade USB RASR) é mostrada.

   NOTA: Insira um pen drive USB de 16 ou mais GB antes de tentar criar a chave RASR.
3. Após inserir um pen drive USB de 16 GB ou mais, clique em **Create RASR USB Drive now** (Criar unidade USB RASR agora).

   A mensagem **Prerequisite Check** (Verificação de pré-requisitos) é mostrada.

   Depois dos pré-requisitos serem verificados, a janela **Create the RASR USB Drive** (Criar a unidade USB RASR) mostra o tamanho mínimo necessário para criar a unidade USB e uma **Lista de possíveis caminhos de destino**.
4. Selecione o destino e clique em **Create** (Criar).

   Uma caixa de diálogo de aviso é mostrada.
5. Clique em **Yes** (Sim).

   A chave da unidade USB RASR é criada.
6. NOTA: Certifique-se de que utiliza a função Safely Remove USB Drive (Remoção segura da unidade USB) ou Windows Eject Drive (Unidade de ejeção do Windows). Caso contrário, o conteúdo do pen drive USB pode ser danificado e o pen drive USB não irá funcionar como o previsto.

   Retire o pen drive e a etiqueta e guarde-os para uso futuro.

3

Proteger estações de trabalho e servidores

Sobre proteção de estações de trabalho e servidores

Para proteger seus dados usando o DL1000, adicione as estações de trabalho e servidores que você deseja proteger no Core Console; por exemplo, o Exchange Server, SQL Server ou o servidor Linux.

NOTA: Neste capítulo, a palavra *máquina* também se refere ao software do AppAssure Agent instalado na máquina.

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

Implantar um agente (instalação por push)

O DL1000 permite que você implante o instalador do AppAssure Agente em máquinas Windows individuais para proteção. Conclua as etapas para transmitir o instalador para um agente. Para implantar agentes em múltiplas máquinas ao mesmo tempo, consulte Implantar em múltiplas máquinas.

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

Para implantar um agente:

1. Na área de navegação esquerda do Core Console, clique em **Protected Machines** (Máquinas protegidas).
2. Clique em **Actions (Ações)** → **Deploy Agent (Implantar agente)**.

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

Caixa de texto	Descrição
Machine (Máquina)	Digite o nome do host ou endereço IP da máquina que você deseja implantar.
Username (Nome de usuário)	Digite o nome de usuário para conectar-se a essa máquina (por exemplo, Administrador).
Password (Senha)	Digite a senha para conectar-se a esta máquina.

Caixa de texto	Descrição
Automatic reboot after install (Inicialização automática após instalação)	Selecione para especificar se o núcleo é inicializado após a conclusão da implantação e instalação do instalador do AppAssure Agent.

4. Clique em **Verify** (Verificar) para validar as credenciais inseridas.

   A caixa de diálogo **Deploy Agent** (Implantar agente) mostra uma mensagem indicando que a validação está em andamento.
5. Clique em **Abort** (Cancelar) se quiser cancelar o processo de verificação.

   Após o processo de verificação ser concluído, é mostrada uma mensagem indicando que a verificação está concluída.
6. Clique em **Deploy** (Implantar).

   É mostrada uma mensagem indicando que a implantação foi iniciada. Você pode ver o andamento na guia **Events** (Eventos).
7. Clique em **Show details** (Mostrar detalhes) para ver mais informações sobre o status da implantação do agente.
8. Clique em **OK**.

Como proteger uma máquina

Este tópico descreve como começar a proteger os dados em uma máquina especificada por você.

NOTA: A máquina precisa ter o software do AppAssure Agent instalado para ser protegida. Você pode optar por instalar o software do AppAssure Agent antes desse procedimento ou pode implantar o software para o agente quando você definir a proteção na caixa de diálogo **Connection** (Conexão). Para instalar o software do AppAssure Agent durante o processo de proteção de uma máquina, consulte Como implantar o software do agente ao proteger um agente.

Ao adicionar proteção, você precisa especificar o nome ou o endereço IP da máquina a ser protegida e os volumes na máquina a serem protegidos, além de definir o cronograma de proteção para cada volume.

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

Para proteger uma máquina:

1. Reinicie a máquina na qual o software do AppAssure Agent está instalado, se ainda não tiver feito isso.
2. No Core Console da máquina do núcleo, clique em **Protect (Proteger)** → **Protect Machine (Proteger máquina)** na barra de menu.

   O assistente **Protect Machine** (Proteger máquina) é mostrado.
3. Na página **Welcome** (Boas-vindas), selecione as opções de instalação apropriadas.
   - Se você não precisa definir um repositório ou estabelecer a criptografia, selecione **Typical** (Típica).
   - Caso não queira ver a página **Welcome** (Boas-vindas) do assistente **Protect Machine** (Proteger máquina) no futuro, selecione a opção **Skip this Welcome page the next time the wizard opens** (Ignorar essa página de boas-vindas na próxima vez que o assistente for aberto).
4. Clique em **Next** (Avançar).

5. Na página **Connection** (Conexão), digite as informações sobre a máquina à qual você deseja se conectar, como descrito na tabela a seguir.

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

6. Clique em **Next** (Avançar). Se a página **Protection** (Proteção) aparecer ao lado do assistente **Protect Machine** (Proteger máquina), pule para a etapa 7.

   NOTA: Se a página **Install Agent** (Instalar agente) aparecer ao lado do assistente **Protect Machine** (Proteger máquina), isso indica que o software do agente ainda não está instalado na máquina designada. Clique em **Next** (Avançar) para instalar o software do agente. O software precisa ser instalado na máquina que você deseja proteger e ela precisa ser reiniciada antes que você possa fazer o backup para o núcleo. Para que o instalador reinicialize a máquina do agente, selecione a opção **After installation, restart the machine automatically (recommended)** (Após a instalação, reiniciar a máquina automaticamente (recomendado)) antes de clicar em **Next** (Avançar).

7. O nome do host ou o endereço IP que você especificou na caixa de diálogo **Connect** (Conectar) é mostrado neste campo de texto. Opcionalmente, digite um novo nome para a máquina, o qual será mostrado no Core Console.
8. Selecione o cronograma de proteção adequado:
   - Para usar o cronograma de proteção padrão, na opção **Schedule Settings** (Configurações de cronograma), selecione **Default protection (3 hour snapshots of all volumes)** (Proteção padrão (instantâneos de todos os volumes a cada 3 horas)). Com um cronograma de proteção padrão, o núcleo salvará instantâneos da máquina do agente uma vez a cada 3 horas. Os instantâneos da máquina podem ser salvos uma vez por hora (mínimo). Para alterar as configurações de proteção a qualquer momento após fechar o assistente, incluindo escolher quais volumes você deseja proteger, acesse a guia Summary (Resumo) para a máquina do agente específica.
   - Para definir outro cronograma de proteção, na opção **Schedule Settings** (Configurações de cronograma), selecione **Custom protection** (Proteção personalizada).
9. Selecione uma das seguintes opções:
   - Se tiver selecionado uma configuração Típica no assistente **Protect Machine** (Proteger máquina) e especificado a proteção padrão, clique em **Finish** (Concluir) para confirmar suas escolhas, feche o assistente e proteja a máquina que você especificou.
   - Na primeira vez que a proteção é adicionada a uma máquina, uma imagem de base (isso é, um instantâneo de todos os dados nos volumes protegidos) será transferida para o repositório no AppAssure Core seguindo o cronograma definido, exceto caso você tenha especificado para pausar a proteção inicialmente.
   - Se você tiver selecionado uma configuração Típica para o assistente **Protect Machine** (Proteger máquina) e especificado uma proteção personalizada, clique em **Next** (Avançar) para configurar um cronograma de proteção personalizado. Para obter detalhes sobre como definir um cronograma de proteção personalizado, consulte Criar cronogramas de proteção personalizados.
   - Se você tiver selecionado a configuração Avançada no assistente **Protect Machine** (Proteger máquina) e a proteção padrão, clique em **Next** (Avançar) e prossiga para a etapa 12 para as opções de criptografia e repositório.

- Se você tiver selecionado a configuração Avançada para o assistente **Protect Machine** (Proteger máquina) e especificado a proteção personalizada, clique em **Next** (Avançar) e prossiga para a etapa 10 para selecionar quais volumes serão protegidos.

10. Na página **Protection Volumes** (Volumes de proteção), selecione os volumes na máquina do agente que você deseja proteger. Se estiver listado algum volume que você não deseja incluir na proteção, clique na coluna Check (Marcar) para apagar a seleção. Em seguida, clique em **Next** (Avançar).

    NOTA: É recomendado proteger o volume reservado ao sistema e o volume com o sistema operacional (normalmente, a unidade C).

11. Na página **Protection Schedule** (Cronograma de proteção), defina um cronograma de proteção personalizado.
12. Na página **Repository** (Repositório), selecione **Use an existing repository** (Usar um repositório existente).
13. Clique em **Next** (Avançar).

    A página **Encryption** (Criptografia) é mostrada.

14. Opcionalmente, para ativar a criptografia, na página **Encryption** (Criptografia), selecione **Enable Encryption** (Ativar criptografia).

    Os campos **Encryption key** (Chave de criptografia) são mostrados na página **Encryption** (Criptografia).

    NOTA: Se você ativar a criptografia, ela será aplicada aos dados para todos os volumes protegidos para essa máquina do agente. Você pode alterar as configurações posteriormente na guia **Configuration** (Configuração) no Core Console.

    CUIDADO: O AppAssure usa criptografia AES de 256 bits no modo de sequenciamento de blocos de cifra (CBC) com chaves de 256 bits. Embora o uso da criptografia seja opcional, a Dell recomenda expressamente que você defina uma chave de criptografia e que você proteja a senha definida. Armazene a senha em um local seguro uma vez que ela é essencial para a recuperação de dados. Sem uma senha, não é possível realizar a recuperação de dados.

15. Insira as informações conforme descrito na tabela a seguir para adicionar uma chave de criptografia ao núcleo.

Caixa de texto	Descrição
Name (Nome)	Digite um nome para a chave de criptografia.
Description (Descrição)	Digite uma descrição para fornecer detalhes adicionais para a chave de criptografia.
Passphrase (Senha)	Digite a senha utilizada para controlar o acesso.
Confirm Passphrase (Confirmar senha)	Digite novamente a senha que você acabou de digitar.

16. Clique em **Finish** (Concluir) para salvar e aplicar suas configurações.

    Na primeira vez que a proteção é adicionada a uma máquina, uma imagem de base (isso é, um instantâneo de todos os dados nos volumes protegidos) será transferida para o repositório no núcleo seguindo o cronograma definido, exceto caso você tenha especificado para pausar a proteção inicialmente.

Pausar e retomar a proteção

Quando pausa a proteção, você para temporariamente todas as transferências de dados da máquina atual.

Para pausar a proteção:

1. No Core Console, clique no menu suspenso **Protected Machines** (Máquinas protegidas) na área de navegação esquerda.
2. Selecione **Pause Protection** (Pausar proteção) para a máquina na qual você deseja pausar a proteção.

   A caixa de diálogo **Pause Protection** (Pausar proteção) é mostrada.
3. Selecione uma das seguintes opções e clique em **OK**.
   - Se você quiser pausar a proteção até explicitamente reativá-la, selecione **Pause until resumed** (Pausar até reativação).
   - Se você quiser pausar a proteção por um período especificado, selecione **Pause for** (Pausar por) e, em seguida nos controles Days (Dias), Hours (Horas) e Minutes (Minutos), digite ou selecione o período apropriado de pausa conforme for necessário.

NOTA: Para reativar a proteção, selecione **Resume Protection** (Reativar proteção) no menu suspenso the **Protected Machines** (Máquinas protegidas).

Implantar o software de agente ao proteger um agente

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

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

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

1. Clique em **Protected Machines** (Máquinas protegidas) no painel de navegação esquerdo.
2. Clique em **Actions (Ações)** → **Deploy Agent (Implantar agente)**.

   A caixa de diálogo **Deploy Agent** (Implantar agente) aparece.
3. Digite as configurações de proteção e logon da seguinte forma:
   - **Host name** (Nome de host) — Especifica o nome de host ou o endereço IP da máquina que você quer proteger.
   - **User name** (Nome de usuário) — Especifica o nome de usuário usado para se conectar a esta máquina; por exemplo, administrador.
   - **Password** (Senha) — Especifica a senha usada para se conectar a esta máquina.
   - **Protect machine after install** (Proteger máquina após a instalação) — A seleção dessa opção permite que o AppAssure salve um instantâneo dos dados após você adicionar a máquina para proteção. Essa opção é selecionada por padrão. Se você desmarcá-la, você precisa forçar um instantâneo manualmente quando estiver pronto para iniciar a proteção de dados.
   - **Display name** (Nome de exibição) — Especifica um nome para a máquina que aparece no Core Console. O nome de exibição pode ser igual ao nome de host.
   - **Port** (Porta) — Especifica o número da porta na qual o AppAssure Core se comunica com o agente na máquina. O valor padrão é 8006.

- **Repository** (Repositório) — Selecione o repositório no qual deseja armazenar dados desse agente.

  NOTA: Você pode armazenar dados de múltiplos agentes em um único repositório.

- **Encryption Key** (Chave de criptografia) — Especifica se a criptografia é aplicada aos dados de cada volume nessa máquina a serem armazenados no repositório.

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

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

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

Entender os cronogramas de proteção

Um cronograma de proteção define quando backups são transferidos de máquinas agente protegidas para o AppAssure Core.

Os cronogramas de proteção são inicialmente definidos usando o assistente **Protect Machine** (Proteger máquinas) ou o assistente **Protect Multiple Machines** (Proteger várias máquinas). Você pode então modificar o cronograma existente a qualquer momento usando a guia Summary (Resumo) para uma máquina do agente específica.

O AppAssure oferece um cronograma de proteção padrão, com dois períodos de proteção definidos. O primeiro período é para dias úteis (segunda a sexta-feira), com um período de tempo único definido (de 00:00 a 23:59). O intervalo padrão (o tempo entre os instantâneos) é de 3 horas. O segundo período é para fins de semana (sábado e domingo). O intervalo padrão para o segundo período é de 3 horas.

Quando a proteção é ativada pela primeira vez, o cronograma é ativado. Dessa forma, usando as configurações padrão, independentemente do horário do dia, o primeiro backup ocorrerá a cada 3 horas.

A primeira transferência de backup salva para o núcleo é chamada de um instantâneo de imagem de base. Todos os dados nos volumes especificados (incluindo o sistema operacional, aplicativos e configurações) são salvos para o núcleo. Posteriormente, instantâneos incrementais (backups menores, compostos apenas de dados alterados no agente desde o último backup) são salvos para o núcleo regularmente com base no intervalo definido.

Você pode criar um cronograma personalizado para alterar a frequência dos backups. Por exemplo, você pode alterar o intervalo do período de dias úteis para 60 minutos, resultando em instantâneos a cada hora. Ou você pode aumentar o intervalo em fins de semana de 60 para 180 minutos, resultando em instantâneos a cada três horas quando o tráfego está baixo.

Entre as outras opções na página do assistente **Protection Schedule** (Cronograma de proteção) estão a definição de um horário de proteção diário. Isso resulta em um backup único diariamente no período definido (a configuração padrão é para as 12:00).

A opção para pausar inicialmente a proteção impede que uma imagem ocorra (e, na verdade, impede todos os backups) até você continuar explicitamente com a proteção. Quando você estiver pronto para começar a proteger as máquinas com base no cronograma de proteção estabelecido, você precisa retomar a proteção explicitamente.

Criar cronogramas personalizados

1. Na página **Protection Schedule** (Cronograma de proteção) dos assistentes **Protect Machine** (Proteger máquina) ou **Protect Multiple Machines** (Proteger múltiplas máquinas), para alterar o cronograma de intervalo de qualquer período, faça o seguinte:
   a. Selecione **Periods** (Períodos).

      Os períodos existentes são mostrados e podem ser modificados. Entre os campos editáveis, estão horário inicial, horário final e intervalo (em minutos) para cada período.
   b. Clique no campo de intervalo e digite um intervalo apropriado em minutos.

      Por exemplo: selecione o intervalo atual e substitua-o pelo valor **60** para salvar instantâneos a cada 60 minutos nesse período.
2. Para criar um período de pico e fora de pico para dias úteis, altere o intervalo de tempo do período de dia útil para que ele não inclua um período de 24 horas, defina o intervalo ideal para o pico, selecione **Take snapshots for the remaining time** (Salvar instantâneos para o tempo restante) e defina um intervalo fora de pico fazendo o seguinte:
   a. Selecione **Periods** (Períodos).

      Os períodos atuais são mostrados e podem ser modificados.
   b. Clique na caixa **From** (De) para alterar a hora inicial desse período.

      A caixa de diálogo **Choose Time** (Escolher horário) é mostrada.
   c. Arraste os controles deslizantes de horas e minutos conforme apropriado para ajustar a hora inicial desejada e depois clique em **Done** (Concluído). Para especificar o horário atual, clique em **Now** (Agora).
   d. Clique na caixa **To** (Até) para alterar a hora final desse período.

      A caixa de diálogo **Choose Time** (Escolher horário) é mostrada.
   e. Arraste os controles deslizantes de horas e minutos conforme apropriado para ajustar a hora inicial desejada e depois clique em **Done** (Concluído). Para especificar o horário atual, clique em **Now** (Agora).
3. Para definir um horário único do dia para um backup único ocorrer diariamente, selecione **Daily protection time** (Hora de proteção diária) e depois defina um horário no formato HH:MM AM.
4. Para definir o cronograma sem começar backups, selecione **Initially pause protection** (Pausar proteção inicialmente).

   Depois de pausar a proteção do assistente, ela permanece parada até que você a retome explicitamente. Depois de retomar a proteção, os backups ocorrerão com base no cronograma estabelecido.
5. Clique em **Finish** (Concluir) ou **Next** (Avançar).

Modificar os cronogramas de proteção

Você pode modificar os cronogramas de proteção para volumes específicos em uma máquina.

Para modificar os cronogramas de proteção:

1. No Core Console, selecione a máquina com um cronograma de proteção definido que você deseja alterar.

   A guia Summary (Resumo) mostra a máquina.
2. Selecione os volumes para a máquina protegida que você deseja alterar e clique em **Set a schedule** (Definir um cronograma). Para selecionar todos os volumes de uma vez, clique na caixa de seleção na linha do cabeçalho.

Inicialmente, todos os volumes compartilham o mesmo cronograma de proteção. Normalmente é uma prática recomendada proteger, no mínimo, o volume reservado para o sistema e o volume com o sistema operacional (geralmente, a unidade C).

A caixa de diálogo **Protection Schedule** (Cronograma de proteção) é mostrada.

3. Na caixa de diálogo **Protection Schedule** (Cronograma de proteção), se você tiver criado um modelo de cronograma de proteção anteriormente e quiser aplicá-lo a esse agente, selecione o modelo na lista suspensa e depois prossiga para a etapa 9.
4. Se você quiser salvar esse novo cronograma de proteção como modelo, digite um nome para o modelo na caixa de texto.
5. Se você quiser remover um período de tempo existente do cronograma, desmarque as caixas de seleção ao lado de cada opção de período de tempo. As opções incluem:
   - **Mon - Fri** (Seg a sex). Esse intervalo de tempo indica uma semana útil típica com cinco dias.
   - **Sat - Sun** (Sáb e dom). Esse intervalo de tempo indica um fim de semana típico.
6. Se os horários de início e fim de dia útil forem 00:00 a 23:59, então há um único período. Para alterar os horários inicial ou final de um período definido, faça o seguinte:
   a. Selecione o período de tempo apropriado.
   b. Clique na caixa **Start Time** (Horário inicial) para alterar a hora inicial desse período.
   c. Arraste os controles deslizantes de horas e minutos conforme apropriado para ajustar a hora inicial desejada e depois clique em **Done** (Concluído). Para especificar o horário atual, clique em **Now** (Agora).
   d. Clique na caixa **End Time** (Horário final) para alterar a hora final desse período.

      A caixa de diálogo **Choose Time** (Escolher horário) é mostrada.
   e. Arraste os controles deslizantes de horas e minutos conforme apropriado para ajustar a hora inicial desejada e depois clique em **Done** (Concluído). Para especificar o horário atual, clique em **Now** (Agora).
   f. Altere o intervalo de acordo com as suas necessidades. Por exemplo, para definir um período de pico, altere o intervalo de 60 minutos para 20 minutos para obter instantâneos três vezes por hora.
7. Se você tiver definido um período diferente de 00:00 a 23:59 na etapa 6, você deseja que os backups sejam realizados nos intervalos de tempo restantes e precisa adicionar períodos adicionais para definir a proteção fazendo o seguinte:
   a. Clique em **+ Add period** (+ Adicionar período).

      Na categoria adequada (dias úteis ou fins de semana), é mostrado um novo período de tempo. Se o primeiro período começou após 00:00, o AppAssure inicia esse período automaticamente às 00:00. Seguindo o exemplo acima, esse segundo período começa às 00:00. Você pode precisar ajustar as horas ou minutos dos horários inicial e final.
   b. Arraste os controles deslizantes de horas e minutos conforme adequado para definir os horários inicial e final desejados conforme apropriado.
   c. Altere o intervalo de acordo com as suas necessidades. Por exemplo, para definir um período fora de pico, altere o intervalo de 60 minutos para 120 minutos para obter instantâneos a cada duas horas.
8. Se necessário, continue para criar períodos adicionais, configurando horários inicial e final e intervalos conforme apropriado.

   NOTA: Se você quiser remover um período adicionado, clique no **X** à extrema direita do período. Se remover um período acidentalmente, você pode clicar em **Cancel** (Cancelar).
9. Quando seu cronograma de proteção atender às suas necessidades, clique em **Apply** (Aplicar).

   A caixa de diálogo **Protection Schedule** (Cronograma de proteção) é fechada.

Definir as configurações da máquina protegida

Depois de adicionar proteção para máquinas no AppAssure, você pode modificar as definições de configuração básica da máquina (como nome e nome do host), configurações de proteção (Alterar o cronograma de proteção para volumes na máquina, adicionar ou remover volumes ou pausar a proteção) e muito mais.

Ver e modificar as definições de configuração

Para ver e modificar as definições de configuração:

1. No Core Console, navegue até a máquina que você deseja modificar.
2. Clique em **Configuration (Configuração)** → **Settings (Definições)**.
3. Clique em **Change** (Alterar) para modificar as definições da máquina, conforme descrito na tabela a seguir.

Caixa de texto	Descrição
Display Name (Nome de exibição)	Digite um nome de exibição para a máquina. Um nome para essa máquina a ser mostrado no Core Console. Por padrão, esse é o nome de host da máquina. Você pode alterar o nome de exibição para algo que facilite mais a referência caso seja necessário.
Host Name (Nome de host)	Digite um nome de host para a máquina.
Port (Porta)	Digite um número de porta para a máquina. O núcleo usa a porta padrão 8006 para se comunicar com essa máquina.
Encryption Key (Chave de criptografia)	Edite a chave de criptografia se necessário. Especifica se a criptografia é aplicada aos dados em cada volume na máquina que está armazenada no repositório.
Repository (Repositório)	Selecione um repositório para os pontos de recuperação. Exibe o repositório no núcleo no qual serão armazenados dados dessa máquina. **NOTA:** Esta definição só pode ser alteradas e não houver pontos de recuperação ou se o repositório anterior não estiver presente.

Ver informações do sistema para uma máquina

O Core Console mostra todas as máquinas que estão sendo protegidas.

Para ver as informações do sistema para uma máquina:

1. Na área de navegação esquerda do Core Console, em **Protected Machines** (Máquinas protegidas), selecione a máquina para ver as informações detalhadas do sistema.
2. Clique na guia **Tools** (Ferramentas).

   A guia System Information (Informações do sistema) é mostrada, incluindo:

   - Nome do host

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

As informações detalhadas sobre os volumes contidos neste computador incluem:

- Nome
- ID do dispositivo
- Sistema de arquivos
- Capacidade (incluindo bruta, formatada e usada)

Outras informações de máquina mostradas, incluindo:

- Processadores
- Adaptadores de rede
- Endereços IP associados a esta máquina

Ver informações de licença

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

Para ver as informações de licença:

1. No painel de navegação, selecione a máquina que você deseja ver.
2. Clique em **Configuration (Configuração)** → **Licensing (Licenças)**.

   A tela **Status** mostra os detalhes da licença do produto.

Modificar configurações de transferência

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

CUIDADO: Alterar as configurações de transferência pode ter efeitos significativos no seu ambiente AppAssure. Antes de modificar os valores de configurações de transferência, consulte o Guia de ajuste de desempenho de transferência no banco de conhecimento do Dell AppAssure.

Há três tipos de transferências no DL1000:

Instantâneos	A transferência que faz um backup dos dados na sua máquina protegida.
Exportação de MV	Um tipo de transferência que cria uma máquina virtual com todos os parâmetros e informações de backup conforme especificado pelo cronograma definido para proteger a máquina.
Restaurar	Um processo que restaura as informações de backup em uma máquina protegida.

A transferência de dados no DL1000 envolve a transmissão de um volume de dados em uma rede a partir de máquinas do AppAssure Agent para o núcleo. No caso da replicação, a transferência também ocorre do núcleo de origem ou para o núcleo de destino.

A transferência de dados pode ser otimizada para o seu sistema por meio de certas configurações de opção de desempenho. Essas configurações controlam o uso de largura de banda de dados durante o

processo de backup das máquinas do agente, de exportação de MV ou de reversão. Alguns fatores que influenciam o desempenho da transferência de dados são:

- Número de transferências simultâneas de dados de agentes
- Número de fluxos de dados simultâneos
- Quantidade de mudança de dados em disco
- Largura de banda de rede disponível
- Desempenho do subsistema do disco de repositório
- Quantidade de memória disponível para buffer de dados

Você pode alterar as opções de desempenho de forma a atender melhor suas necessidades de negócios e ajustar o desempenho com base no seu ambiente.

Para modificar configurações de transferência:

1. No Core Console, navegue até a máquina que você deseja modificar.
2. Clique na guia **Configuration** (Configuração) e, em seguida, clique em **Transfer Settings** (Configurações de transferência).

   A página **Transfer Settings** (Configurações de transferência) atual é mostrada.
3. Na página **Transfer Settings** (Configurações de transferência), clique em **Change** (Alterar).

   A caixa de diálogo **Transfer Settings** (Configurações de transferência) é mostrada.
4. Acesse as opções de **configurações de transferência** para a máquina conforme descrito na tabela a seguir.

Caixa de texto	Descrição
Prioridade	Define a prioridade de transferência entre máquinas protegidas. Permite que você atribua a prioridade em comparação com outras máquinas protegidas. Selecione um número de 1 a 10, onde 1 é a prioridade mais alta. A configuração padrão define uma prioridade igual a 5. NOTA: A prioridade é aplicada às transferências que estão na fila.
Máximo de fluxos simultâneos	Define o número máximo de ligações TCP que são enviadas para o núcleo para serem processadas em paralelo por agente. NOTA: A Dell recomenda definir esse valor como 8. Em caso de pacotes perdidos, tente aumentar essa configuração.
Máximo de gravações simultâneas	Define o número máximo de ações simultâneas de gravação em disco por conexão de agente. NOTA: A Dell recomenda definir esse valor como o mesmo valor selecionado para o número máximo de fluxos simultâneos. Em caso de perda de pacotes, defina esse valor um pouco abaixo. Por exemplo, se o número máximo de fluxos atuais estiver definido como 8, defina essa opção como 7.
Número máximo de tentativas	Define o número máximo de novas tentativas para cada máquina protegida, se algumas das operações não forem concluídas.

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 configuração padrão é 4194304. **CUIDADO: Não altere a configuração padrão dessa opção.**
Profundidade máxima de fila de transferência	Especifica o número de comandos que podem ser enviados simultaneamente. Você pode ajustar esta opção para um número mais alto se o seu sistema possui um número alto de operações simultâneas de entrada/saída.
Leituras pendentes por fluxo	Especifica como operações de leitura em fila serão armazenadas no backend. Essa configuração ajuda a controlar o processo de enfileiramento de agentes. **NOTA:** A Dell recomenda definir esse valor como 24.
Gravadores excluídos	Selecione um gravador se você deseja excluí-lo. Uma vez que os gravadores que aparecem na lista são específicos para a máquina que você está configurando, você pode não ver todos os gravadores listados. Entre os gravadores que você pode ver, estão: • Gravador ASR • Gravador BITS • Gravador COM+ REGDB • Gravador de contadores de desempenho • Gravador de registro • Gravador de otimização de cópia de sombra • SQLServerWriter • Gravador de sistema • Gravador de agendador de tarefas • Gravador de armazenamento de metadados VSS • Gravador WMI
Porta de servidor de dados de transferência	Define a porta para transferências. A configuração padrão é 8009.
Tempo limite de transferência	Especifica em minutos e segundos a quantidade de tempo para permitir que um pacote fique estático sem transferência.
Tempo limite do instantâneo	Especifica em minutos e segundos o tempo máximo para aguardar a gravação de um instantâneo.
Tempo limite de leitura de rede	Especifica o tempo máximo em minutos e segundos para aguardar uma conexão de leitura. Se a leitura de rede não for realizada nesse tempo, a operação é repetida.
Tempo limite de gravação de rede	Especifica o tempo máximo em segundos para aguardar uma conexão de gravação. Se a gravação de rede não for realizada nesse tempo, a operação é repetida.

5. Clique em **OK**.

Arquivar dados

As políticas de retenção reforçam períodos nos quais backups são armazenados em mídias de curto prazo (rápidas e caras). Às vezes, certos requisitos técnicos e comerciais exigem a retenção ampliada desses backups, mas o uso de armazenamento rápido não é financeiramente viável. Dessa forma, esse requisito cria uma necessidade por armazenamento de longo prazo (lento e barato). As empresas muitas vezes usam armazenamento de longo prazo para arquivar ambos dados de com ou sem exigências de conformidade. O recurso de arquivamento no AppAssure é usado para oferecer suporte à retenção ampliada para dados com ou sem exigências de conformidade. Ele também é usado para propagar dados de replicação para um núcleo replicado remoto.

Criar um arquivamento

Para criar um arquivamento:

1. No Core Console, clique em **Tools (Ferramentas)** → **Archive (Arquivamento)** → **Create (Criar)**.
   A caixa de diálogo **Add Archive Wizard** (Assistente de inclusão de arquivamento) é mostrada.
2. Na página **Create** (Criar) do assistente **Add Archive** (Adicionar arquivo), selecione uma das opções a seguir na lista suspensa **Location Type** (Tipo de local):
   - Local
   - Network (Rede)
   - Cloud (Nuvem)
3. Digite os detalhes para o arquivamento conforme descrito na tabela a seguir com base no tipo de local selecionado na Etapa 3.

Tabela 2. Criar um arquivamento

Opção	Caixa de texto	Descrição
Local	Output location (Local de saída)	Digite o local para a saída. É usado para definir o caminho do local onde você quer salvar o arquivamento; por exemplo, d:\trabalho\arquivamento.
Network (Rede)	Output location (Local de saída)	Digite o local para a saída. É usado para definir o caminho do local onde você quer salvar o arquivamento; por exemplo, \ \nome_do_servidor \nome_de_compartilhamento.
	User Name (Nome de usuário)	Digite um nome de usuário. Ele será usado para determinar as credenciais de login para o compartilhamento de rede.
	Password (Senha)	Digite uma senha para o caminho de rede. Ela será usada para determinar as credenciais

Opção	Caixa de texto	Descrição
		de login para o compartilhamento de rede.
Cloud (Nuvem)	Account (Conta)	Selecione uma conta na lista suspensa. **NOTA:** Para selecionar uma conta na nuvem, você primeiro deve adicioná-la ao Core Console. Consulte Adicionar uma conta na nuvem.
	Container (Contêiner)	Selecione no menu suspenso um contêiner associado à sua conta.
	Folder Name (Nome da pasta)	Digite um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é AppAssure-5-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

4. Clique em **Next** (Avançar).
5. Na página **Machines** (Máquinas) do assistente, selecione quais máquinas protegidas contêm os pontos de recuperação que você deseja arquivar.
6. Clique em **Next** (Avançar).
7. Na página **Options** (Opções), digite as informações descritas na tabela a seguir.

Caixa de texto	Descrição
Maximum Size (Tamanho máximo)	Arquivamentos grandes podem ser divididos em múltiplos segmentos. Selecione o espaço máximo que você quer reservar para a criação do arquivamento de uma das formas a seguir: • Selecione Entire Target (Destino inteiro) para reservar todo o espaço disponível no caminho fornecido como destino na Etapa 4 (por exemplo, se o local for D:\trabalho\arquivamento, todo o espaço disponível na unidade D: será reservada). • Selecione a caixa de texto em branco, use as setas para cima e para baixo para definir uma quantidade e, em seguida, selecione uma unidade de medida na lista suspensa para personalizar o espaço máximo que você quer reservar. **NOTA:** Os arquivamentos em nuvem da Amazon são automaticamente divididos em segmentos de 50 GB. Os arquivamentos em nuvem da Windows Azure são automaticamente divididos em segmentos de 200 GB.

Caixa de texto	Descrição
Recycle action (Ação de reciclagem)	Selecione uma das seguintes opções para a ação de reciclagem: • **Do not reuse** (Não reutilizar): Não sobrescreve nem apaga os dados arquivados existentes do local. Se o local não estiver vazio, a gravação do arquivamento falhará. • **Replace this Core** (Substituir este núcleo): Sobrescreve todos os dados arquivados preexistentes pertencentes a este núcleo, mas deixa intactos os dados de outros núcleos. • **Erase Completely** (Apagar por completo): Apaga todos os dados arquivados do diretório antes de gravar o novo arquivamento. • **Incremental**: Permite adicionar pontos de recuperação a um arquivamento existente. Compara os pontos de recuperação para evitar a duplicação de dados já existentes no arquivamento.
Comment (Comentário)	Digite quaisquer informações adicionais necessárias para a identificação do arquivamento. Os comentários serão mostrados se você importar o arquivamento posteriormente.
Use compatible format (Usar formato compatível)	Selecione esta opção para arquivar seus dados em um formato compatível com versões anteriores de núcleos. NOTA: O novo formato oferece maior desempenho; entretanto, não é compatível com núcleos mais antigos.

8. Clique em **Next** (Avançar).
9. Na página Date Range (Intervalo de datas), digite a Start Date (Data de início) e a Expiration Date (Data de vencimento) dos pontos de recuperação a serem arquivados.
   - Para incluir um horário, clique no horário mostrado (padrão, 08:00) para mostrar as barras deslizantes de seleção de horas e minutos.
   - Para incluir uma data, clique na caixa de texto para mostrar o calendário e, em seguida, clique no dia preferencial.
10. Clique em **Finish** (Concluir).

Importar um arquivamento

Para importar um arquivamento:

1. No Core Console, clique em **Tools (Ferramentas)** → **Archive (Arquivo)** → **Import (Importar)**.
2. Em **Location type** (Tipo de local), selecione uma das opções a seguir na lista suspensa:
   - Local
   - Rede
   - Cloud (Nuvem)
3. Digite os detalhes para o arquivamento conforme descrito na tabela a seguir com base no tipo de local selecionado na Etapa 3.

Tabela 3. Importar um arquivamento

Opção	Caixa de texto	Descrição
Local	Output location (Local de saída)	Digite o local para a saída. É usado para definir o caminho

Opção	Caixa de texto	Descrição
		do local onde você quer salvar o arquivamento; por exemplo, `d:\work\archive`ea.
Rede	Output location (Local de saída)	Digite o local para a saída. É usado para definir o caminho do local onde você quer salvar o arquivamento; por exemplo, \ \nome_do_servidor \nome_de_compartilhamento.
	User Name (Nome de usuário)	Digite um nome de usuário. Ele será usado para determinar as credenciais de login para o compartilhamento de rede.
	Password (Senha)	Digite uma senha para o caminho de rede. Ela será usada para determinar as credenciais de login para o compartilhamento de rede.
Cloud (Nuvem)	Account (Conta)	Selecione uma conta na lista suspensa. **NOTA:** Para selecionar uma conta na nuvem, você primeiro deve adicioná-la ao Core Console. Consulte Adicionar uma conta na nuvem.
	Container (Contêiner)	Selecione no menu suspenso um contêiner associado à sua conta.
	Folder Name (Nome da pasta)	Digite um nome para a pasta na qual os dados arquivados devem ser salvos. O nome padrão é AppAssure-5-Archive-[DATA DE CRIAÇÃO]-[HORA DE CRIAÇÃO]

4. Clique em **Check File** (Verificar arquivo) para validar a existência do arquivo para importação.
   A caixa de diálogo **Restore** (Restaurar) é exibida.
5. Na caixa de diálogo **Restore** (Restaurar), verifique o nome do núcleo de origem.
6. Selecione os agentes para importar do arquivo.
7. Selecione o repositório.
8. Clique em **Restore** (Restaurar) para importar o arquivamento.

Arquivamento em uma nuvem

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

Para exportar um arquivamento para uma nuvem:

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

Ver os diagnósticos do sistema

No AppAssure, informações de diagnóstico estão disponíveis para visualização dos dados de log de máquina de qualquer máquina protegida. Além disso, você pode ver e enviar informações de diagnóstico para o núcleo.

Ver logs de máquina

Se você encontrar quaisquer erros ou problemas com a máquina, pode ser útil consultar os logs para fins de solução de problemas.

Para ver os logs da máquina:

1. No Core Console, clique em **Tools (Ferramentas)** → **Diagnostics (Diagnósticos)** → **View Log (Ver log)**.

   A página **Download Core Log** (Baixar log do núcleo) é mostrada.
2. Selecione **Click here to begin the download** (Clique aqui para iniciar o download).

   Será mostrada uma mensagem alertando você a abrir ou salvar o arquivo.
3. Escolha o método preferido para processar o arquivo do log.

Upload de logs da máquina

1. Navegue até o Core Console, clique em **Tools (Ferramentas)** → **Diagnostics (Diagnósticos)** → **Upload Log (Upload de log)**.

   A página **Upload Log** (Upload de log) é mostrada.
2. Selecione **Click here to begin the upload** (Clique aqui para iniciar o upload).

   A guia Events (Eventos) mostra o andamento do upload das informações de log do núcleo e todas as máquinas protegidas.

Cancelar operações em uma máquina

Você pode cancelar operações em execução para uma máquina. Você pode cancelar um instantâneo atual ou cancelar todas as operações atuais, incluindo exportações e replicações.

Para cancelar operações em uma máquina:

1. No Core Console, selecione a máquina para a qual você deseja cancelar as operações.
2. Em **Events** (Eventos), amplie os detalhes do evento ou operação que você deseja cancelar.

3. Clique em **Cancel** (Cancelar).

Ver status da máquina e outros detalhes

Para ver o status da máquina e outros detalhes:

1. No Core Console, navegue até a máquina protegida que você deseja ver.

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

- Nome do host
- Último instantâneo salvo
- Próximo instantâneo agendado
- Status da criptografia
- Número da versão
- Status de verificação de capacidade de montagem
- Status de verificação de soma de verificação
- Último truncamento de log realizado

Informações detalhadas sobre os volumes contidos neste computador também são mostradas e incluem:

- Nome
- Tipo de sistema de arquivos
- Uso de espaço
- Cronograma atual
- Próximo instantâneo
- Tamanho total
- Espaço usado
- Espaço livre

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

- Status on-line
- Nome
- Caminho de instalação
- Versão

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

- Versão
- Caminho de instalação
- Caminho de dados
- Caminho de bancos de dados de troca de nome
- Caminho do arquivo de log
- Prefixo de log

- Caminho do sistema
- Tipo de armazenamento de e-mail

Gerenciar múltiplas máquinas

Este tópico descreve as tarefas que os administradores executam para implantar o software do AppAssure Agent simultaneamente em várias máquinas Windows.

Para implantar e proteger vários agentes, execute as seguintes tarefas:

1. Implantar o AppAssure em várias máquinas
   Consulte Implantar em várias máquinas.
2. Monitorar a atividade da implantação em lote.
   Consulte Monitorar a implantação de várias máquinas.
3. Proteger várias máquinas.
   Consulte Proteger várias máquinas.

   NOTA: Esta etapa pode ser ignorada se você selecionou a opção Protect Machine After Install (Proteger máquina após a instalação) durante a implantação.
4. Monitorar a atividade de proteção em lote.
   Consulte Monitorar a proteção de várias máquinas.

Implantar em várias máquinas

Você pode simplificar a tarefa de implantação do software do AppAssure Agent em várias máquinas Windows usando o recurso Implantar em lote do AppAssure. Você pode realizar uma implantação em lote para:

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

O recurso Implantar em massa detecta automaticamente máquinas em um host e permite que você selecione aquelas nas quais você deseja implantar. Opcionalmente, você pode inserir manualmente as informações de máquina e host.

NOTA: As máquinas que você está implantando precisam ter acesso à Internet para baixar e instalar bits uma vez que o AppAssure usa a versão da web do instalador do AppAssure Agent para implantar os componentes de instalação. Se o acesso à Internet não estiver disponível, você realizar a instalação do programa do AppAssure Agent por push a partir da máquina do núcleo. Você pode baixar atualizações de agente e núcleo através do portal de licenças.

Monitorar a implantação de várias máquinas

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

Para monitorar a implantação de várias máquinas:

1. No Core Console, clique em **Events (Eventos)** → **Alerts (Alertas)**.
2. Navegue até a guia inicial do AppAssure Core e clique na guia **Events** (Eventos).

Alertas e eventos são mostrados na lista, indicando o horário que o evento foi iniciado e uma mensagem. Para cada implantação correta do software do agente, você verá um alerta indicando que a máquina protegida foi adicionada.

3. Opcionalmente, clique em qualquer link de uma máquina protegida.

   A guia Summary (Resumo) da máquina selecionada é mostrada, indicando informações pertinentes que incluem:

   - O nome do host da máquina protegida
   - O último instantâneo, se aplicável
   - O horário programado do próximo instantâneo, com base no cronograma de proteção selecionado
   - Time Remaining (Tempo restante)
   - A chave de criptografia, se houver, usada para esse agente protegido
   - A versão do software do agente

Proteger múltiplas máquinas

Depois de implantar o software do AppAssure Agent em massa nas máquinas Windows, você precisa proteger as máquinas para proteger os dados. Se você selecionou **Protect Machine After Install** (Proteger máquinas após a instalação) ao implantar o agente, você pode pular esse procedimento.

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

Para proteger múltiplas máquinas:

1. No Core Console, clique em **Protect (Proteger)** → **Bulk Protect (Proteger em lote)**.

   A janela do assistente **Protect Multiple Machines** (Proteger múltiplas máquinas) é mostrada.

2. Selecione a opção de instalação apropriada:

   - Se você não precisa definir um repositório ou estabelecer a criptografia, selecione **Typical** (Típica).
   - Caso não queira ver a página Welcome (Boas-vindas) do assistente Protect Machine (Proteger máquina) no futuro, selecione a opção **Skip this Welcome page the next time the wizard opens** (Ignorar essa página de boas-vindas na próxima vez que o assistente for aberto).

3. Clique em **Next** (Avançar).

   A página **Connection** (Conexão) é mostrada.

4. Adicione as máquinas que você deseja proteger clicando em uma das opções a seguir.

   - Clique em **Active Directory** para especificar as máquinas em um domínio Active Directory. Digite as credenciais conforme descrito na tabela abaixo e clique em **Next** (Avançar).
   - Clique em **vCenter/ESXi** para especificar máquinas virtuais em um host virtual vCenter/ESXi. Digite as credenciais conforme descrito na tabela abaixo e clique em **Next** (Avançar).

Caixa de texto	Descrição
Host	O nome do host ou o endereço IP do domínio do Active Directory ou do host virtual do VMware vCenter Server/ESX(i).
Username (Nome de usuário)	Digite o nome de usuário usado para conectar-se a essa máquina; por exemplo, Administrador.
Password (Senha)	Digite a senha protegida usada para conectar-se a esta máquina.

   - Para adicionar as máquinas manualmente, selecione **Add the machines manually** (Adicionar máquinas manualmente). Clique em **Next** (Avançar).

5. Na página **Machines** (Máquinas), para especificar as máquinas manualmente, digite os seguintes detalhes de conexão para cada máquina em uma linha separada e depois clique em **Next** (Avançar).`hostname::username::password::port`
6. Na página **Machines** (Máquinas), para especificar as máquinas identificadas de um domínio Active Directory ou de um host virtual do VMware vCenter/ESX(i), selecione na lista cada máquina apropriada que você deseja proteger e depois clique em **Next** (Avançar).

   O sistema verifica cada máquina que você adicionou automaticamente e a página **Protection** (Proteção) é mostrada.
7. Na página **Protection** (Proteção), selecione o cronograma de proteção adequado.
   - Para usar o cronograma de proteção padrão, selecione **Default protection (hourly snapshots of all volumes)** (Proteção padrão (instantâneos de todos os volumes a cada hora)) na opção **Schedule Settings** (Configurações de cronograma).
   - Se quiser definir outro cronograma de proteção, selecione **Custom protection** (Proteção personalizada) na opção Schedule Settings (Configurações de cronograma) e depois clique em **Next** (Avançar).
8. Prossiga com a configuração da seguinte forma:
   - Se tiver selecionado uma configuração Típica para o assistente **Protect Multiple Machines** (Proteger múltiplas máquinas) e proteção padrão, clique em **Finish** (Concluir) para confirmar suas escolhas, feche o assistente e proteja as máquinas especificadas.
   - Se você tiver selecionado uma configuração Típica para o assistente **Protect Multiple Machines** (Proteger múltiplas máquinas) e especificado proteção personalizada, clique em **Next** (Avançar) e configure um cronograma personalizado.
   - Se você tiver selecionado a configuração Avançada para o assistente Protect Machine (Proteger máquina), clique em **Next** (Avançar) e prossiga para a etapa 9 para ver as opções de criptografia e repositório.
9. Na página **Repository** (Repositório), selecione **Use an existing repository** (Usar um repositório atual).
10. Clique em **Next** (Avançar).

    A página **Encryption** (Criptografia) é mostrada.
11. Para ativar a criptografia, na página **Encryption** (Criptografia), selecione **Enable Encryption** (Ativar criptografia).

    Os campos Encryption key (Chave de criptografia) são mostrados na página **Encryption** (Criptografia).

    NOTA: Se você ativar a criptografia, ela será aplicada aos dados para todos os volumes protegidos para as máquinas especificadas para proteção. Você pode alterar as configurações posteriormente na guia **Configuration** (Configuração) no Core Console. Para obter mais informações sobre a criptografia, consulte Managing Security (Gerenciar segurança).
12. Insira as informações conforme descrito na tabela a seguir para adicionar uma chave de criptografia ao núcleo.

Caixa de texto	Descrição
Name (Nome)	Digite um nome para a chave de criptografia.
Description (Descrição)	Digite uma descrição para fornecer detalhes adicionais para a chave de criptografia.
Passphrase (Senha)	Digite a senha utilizada para controlar o acesso.

Caixa de texto	Descrição
Confirm Passphrase (Confirmar senha)	Digite novamente a senha que você acabou de digitar.

13. Clique em **Finish** (Concluir) para salvar e aplicar suas configurações.

Monitorar a proteção de várias máquinas

Você pode monitorar o andamento conforme o AppAssure aplica as políticas e cronogramas de proteção às máquinas.

Para monitorar a proteção de várias máquinas, navegue até a guia Home (Início) do Core Console **Events** (Eventos).

A guia Events (Eventos) mostra tarefas, alertas e eventos. Quando volumes são transferidos, o status, horários iniciais e horários finais são mostrados no painel Tasks (Tarefas). Você também pode filtrar as tarefas por status (ativa, aguardando, concluída e falha).

A medida em que cada máquina protegida é adicionado, um alerta é registrado, indicando se a operação foi bem-sucedida ou se foram registrados erros.

4

Recuperar dados

Gerenciar a recuperação

O AppAssure Core pode restaurar ou recuperar instantaneamente máquinas físicas ou virtuais a partir de pontos de recuperação. Os pontos de recuperação contêm os instantâneos de volume de agente capturados a nível de bloco. Esses instantâneos possuem reconhecimento de aplicativos, o que significa que todos os logs de transação em andamento e transações em aberto são concluídos e caches são liberados do disco antes de criar o instantâneo. Usar instantâneos com reconhecimento de aplicativos em conjunto com a recuperação verificada permite que o núcleo realize diversos tipos de recuperações, incluindo:

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

Gerenciar instantâneos e pontos de recuperação

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

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

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

Ver pontos de recuperação

Para ver pontos de recuperação:

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

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

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

Ver um ponto de recuperação específico

Para ver um ponto de recuperação específico:

1. Na área de navegação esquerda do Core Console, selecione a máquina para a qual você deseja ver os pontos de recuperação e selecione a opção **Recovery Points** (Pontos de recuperação).
2. Clique em **>** ao lado de um ponto de recuperação na lista para ampliar a visualização.
   Você pode ver informações mais detalhadas sobre o conteúdo do ponto de recuperação para a máquina selecionada, bem como acessar uma variedade de operações que podem ser realizadas no ponto de recuperação, descritas na tabela a seguir:

Informações	Descrição
Ações	O menu **Actions** (Ações) inclui as seguintes operações que você pode realizar no ponto de recuperação selecionado: **Mount** (Montar) - Selecione essa opção para montar o ponto de recuperação selecionado. Para obter mais informações sobre a montagem de um ponto de recuperação selecionado, consulte Montar um ponto de recuperação para uma máquina Windows. **Export** (Exportar) — Na opção Exportar, você pode exportar o ponto de recuperação selecionado para o ESXi, para a estação de trabalho VMware ou para o HyperV. **Restore** (Restaurar) — Selecione essa opção para realizar uma restauração a partir do ponto de recuperação para um volume que você especificar.
Contents (Conteúdo)	A área Contents (Conteúdo) inclui uma linha para cada volume no ponto de recuperação ampliado que lista as seguintes informações para cada volume: A opção **Status** indica o status atual do ponto de recuperação. A opção **Title** (Título) lista o volume específico no ponto de recuperação.

A opção **Size** (Tamanho) mostra o espaço que o ponto de recuperação consome no repositório.

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

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

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

Montar um ponto de recuperação para uma máquina Windows

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

Para montar um ponto de recuperação para uma máquina Windows:

1. No Core Console, selecione a máquina que você deseja montar para um sistema local de arquivos.

   A guia **Summary** (Resumo) para a máquina selecionada é mostrada.
2. Selecione a guia **Recovery Points** (Pontos de recuperação).
3. Na lista de opções de recuperação, clique em **>** para ampliar o ponto de recuperação que você deseja montar.
4. Nos detalhes ampliados do ponto de recuperação, clique em **Mount** (Montar).

   A caixa de diálogo **Mount Recovery Points** (Montar pontos de recuperação) é mostrada.
5. Na caixa de diálogo **Mount** (Montar), edite as caixas de texto para montar um ponto de recuperação como descrito na tabela a seguir:

Caixa de texto	Descrição
Mount Location: Local Folder (Local de montagem: pasta local)	Especifique o caminho usado para acessar o ponto de recuperação montado.

Caixa de texto	Descrição
Volume Images (Imagens de volume)	Especifique as imagens de volume que você deseja montar.
Mount Type (Tipo de montagem)	Especifique a maneira para acessar os dados para o ponto de recuperação montado: • Mount Read-only (Montagem somente-leitura). • Montagem somente-leitura com gravações anteriores • Mount Writable (Montagem gravável).
Criar um compartilhamento do Windows para essa montagem	Opcionalmente, marque a caixa de seleção para especificar se o ponto de recuperação montado pode ser compartilhado e depois defina os direitos de acesso para ele incluindo o nome do compartilhamento e os grupos de acesso.

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

Desmontar pontos de recuperação selecionados

Para desmontar os pontos de recuperação selecionados:

1. Navegue até o Core Console, clique em **Tools (Ferramentas)** → **Mounts (Montagens)**.
2. Na página **Local Mounts** (Montagens locais), ao lado do ponto de montagem para o ponto de recuperação que você deseja desmontar, clique em **Dismount** (Desmontar).
3. Na janela Dismounting the Recovery Point (Desmontar o ponto de recuperação), clique em **Yes** (Sim) para confirmar.

Desmontar todos os pontos de recuperação

Para desmontar todos os pontos de recuperação:

1. Navegue até o Core Console, clique em **Tools (Ferramentas)** → **Mounts (Montagens)**.
2. Na página **Local Mounts** (Montagens locais), clique em **Dismount All** (Desmontar tudo).
3. Na janela **Dismounting the Recovery Point** (Desmontar o ponto de recuperação), clique em **Yes** (Sim) para confirmar.

Montar um ponto de recuperação para uma máquina Linux

Usando o utilitário **aamount** no AppAssure, você pode montar um volume remotamente de um ponto de recuperação como um volume local em uma máquina Linux.

1. Crie um novo diretório para montar o ponto de recuperação (por exemplo, você pode usar o comando **mkdir**).
2. Verifique se o diretório existe (por exemplo, usando o comando **ls**).
3. Execute o utilitário AppAssure **aamount** como raiz, ou como super usuário; por exemplo: **sudo aamount**
4. No prompt de montagem do AppAssure, digite o comando a seguir para listar as máquinas desprotegidas: **lm**
5. Quando solicitado, digite o endereço IP ou nome do host do servidor de núcleo.
6. Digite as credenciais de login do servidor de núcleo, isso é, o nome de usuário e a senha.

Será mostrada uma lista das máquinas protegidas pelo servidor AppAssure. Cada máquina é identificada pelas seguintes informações: número de item de linha, endereço IP/host e número de ID da máquina. Por exemplo: 293cc667-44b4-48ab-91d8-44bc74252a4f

7. Digite o seguinte comando para listar os pontos de recuperação que estão disponíveis para uma máquina especificada: **lr <número_de_linha_da_máquina>**
8. Digite o seguinte comando para selecionar e montar o ponto de recuperação especificado no caminho/ponto de montagem especificado. **m <número_de_ID_de_recuperação_de_volume> <caminho>**
9. Para verificar se a montagem foi realizada corretamente, digite o seguinte comando, o qual deve listar o volume remoto anexado: **l**

Remover pontos de recuperação

Você pode remover pontos de recuperação de uma determinada máquina do repositório facilmente. Ao apagar os pontos de recuperação no AppAssure, você pode especificar uma das seguintes opções:

Caixa de texto	Descrição
Delete All Recovery Points (Apagar todos os pontos de recuperação)	Remove todos os pontos de recuperação da máquina do agente selecionada do repositório.
Delete a Range of Recovery Points (Apagar 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, que são todos os dados da máquina, além dos pontos de recuperação após o atual até a próxima imagem de base.

NOTA: Você não pode recuperar os pontos de recuperação apagados.

Para remover pontos de recuperação:

1. Na área de navegação esquerda do Core Console, selecione a máquina para a qual você deseja ver os pontos de recuperação e depois clique na guia **Recovery Points** (Pontos de recuperação).
2. Clique no menu **Actions** (Ações).
3. Selecione uma das seguintes opções:
   - Para apagar todos os pontos de recuperação atualmente armazenados, clique em **Delete All** (Apagar tudo).
   - Para apagar um conjunto de pontos de recuperação em um intervalo de dados específico, clique em **Delete Range** (Apagar intervalo). A caixa de diálogo **Delete** (Apagar) é mostrada. Na caixa de diálogo **Delete Range** (Apagar intervalo), especifique o intervalo de pontos de recuperação que você deseja apagar usando datas e horas inicial e final e depois clique em **Delete** (Apagar).

Apagar uma cadeia de ponto de recuperação órfã

Um ponto de recuperação órfã é um instantâneo incremental que não está associado a uma imagem de base. Instantâneos subsequentes continuam a compilar a partir desse ponto de recuperação. Sem a imagem de base, os pontos de recuperação resultantes são incompletos e provavelmente não vão conter os dados necessários para concluir uma recuperação. Esses pontos de recuperação são considerados parte da cadeia de ponto de recuperação órfã. Se essa situação ocorrer, a melhor solução é apagar a cadeia e criar uma nova imagem de base. Para obter mais informações sobre como forçar uma imagem de base, consulte Forçar um instantâneo.

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

Para apagar uma cadeia de ponto de recuperação órfã:

1. No Core Console, selecione a máquina protegida para a qual você deseja apagar a cadeia de ponto de recuperação órfã.
2. Clique na guia **Recovery Points** (Pontos de recuperação).
3. Em **Recovery Points** (Pontos de recuperação), amplie o ponto de recuperação órfã.

   O ponto de recuperação é marcado na coluna **Type** (Tipo) como **Incremental Orphaned** (Órfão incremental).
4. Ao lado de **Actions** (Ações), clique em **Delete** (Apagar).

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

   CUIDADO: Apaga esse ponto de recuperação exclui toda a cadeia de pontos de recuperação, incluindo quaisquer pontos de recuperação incremental que ocorreram antes ou depois dela, até a próxima imagem de base. Essa operação não pode ser desfeita.

Forçar um instantâneo

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

Para forçar um instantâneo:

1. No Core Console, selecione a máquina ou o cluster com o ponto de recuperação para o qual você deseja forçar um instantâneo.
2. Clique na guia **Summary** (Resumo) na seção **Volumes** e depois selecione uma das opções descritas da seguinte forma:
   - **Force Snapshot** (Forçar instantâneo) - Salva um instantâneo incremental dos dados atualizados desde que o último instantâneo foi salvo.
   - **Force Base Image** (Forçar imagem de base) - Salva um instantâneo de todos os dados nos volumes da máquina.
3. Quando a notificação for mostrada na caixa de diálogo **Transfer Status** (Status de transferência) informando que o instantâneo foi colocado na fila, , clique em **OK**.

   Uma barra de andamento aparece ao lado da guia **Machines** (Máquinas) e mostra o andamento do instantâneo.

Restaurar dados

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

Se você tiver a replicação configurada entre dois núcleos (de origem e de destino), você só pode exportar os dados do núcleo de destino após a replicação inicial estar concluída.

Sobre exportar dados protegidos de máquinas Windows para máquinas virtuais

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

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

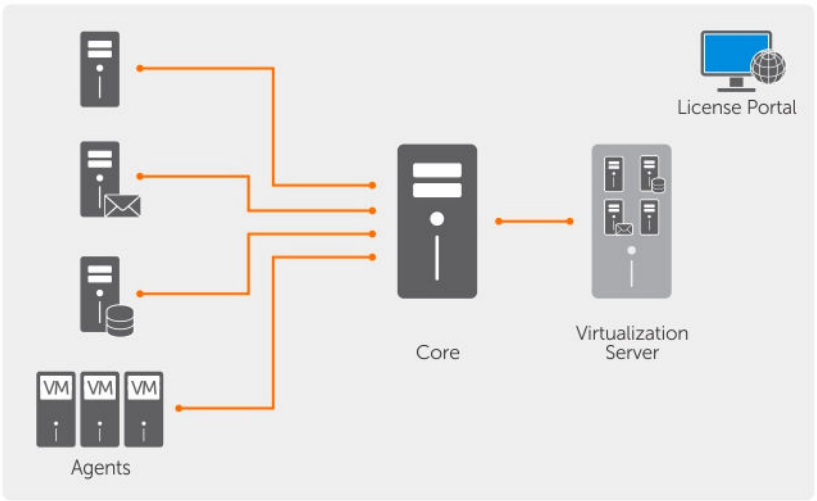

Figura 4. Exportar dados para uma máquina virtual

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

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

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

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

Limitações de suporte a volumes básicos e dinâmicos

O Dell AppAssure oferece suporte para salvar instantâneos de todos os volumes básicos e dinâmicos. O AppAssure também suporta exportar volumes dinâmicos simples que estão em um disco físico único. Volumes dinâmicos simples não são distribuídos, espelhados ou estendidos.

Discos dinâmicos (exceto discos dinâmicos simples, como descrito anteriormente) não estão disponíveis para seção no assistente Export (Exportar). Volumes dinâmicos que não sejam simples possuem geometrias de disco arbitrárias que não podem ser totalmente interpretadas. Dessa forma, o AppAssure não oferece suporte para a exportação de volumes dinâmicos que não sejam simples.

Gerenciar exportações

Na guia **Virtual Standby** (Espera virtual) do Core Console, você pode ver o status das exportações que você configurou, incluindo exportações únicas e exportações contínuas para espera virtual. Nessa guia, você pode gerenciar exportações ao pausar, parar, remover exportações ou ver uma fila das próximas exportações.

NOTA: Apenas o Dell DL1000 de 3TB com configuração de 2 máquinas virtuais oferece suporte para recursos de exportação única e contínua(espera virtual).

1. No Core Console, navegue até a guia **Virtual Standby** (Espera virtual).
   Na guia **Virtual Standby** (Espera virtual), você pode ver uma tabela das configurações de exportação salvas, incluindo as informações descritas na tabela a seguir.

Menu	Descrição
Status	**NOTA:** O status da configuração de espera virtual é definido pela cor do ícone. Verde – A espera virtual está configurada corretamente e está ativa, não pausada. A próxima exportação de espera virtual será realizada após o próximo instantâneo. Amarelo – A espera virtual está pausada e ainda está salva pelo núcleo. No entanto, após uma nova transferência, o trabalho de exportação não começará automaticamente e não haverá novas exportações de espera virtual para esse agente.
Machine Name (Nome da máquina)	O nome da máquina de origem.
Destination (Destination)	A máquina virtual e caminho para os quais os dados estão sendo exportados.
Export Type (Tipo de exportação)	O tipo de plataforma de máquina virtual para exportação, como ESXi, VMware, Hyper-V ou VirtualBox.
Last Export (Última exportação)	A data e a hora da última exportação. Se uma exportação acabou de ser adicionada mas não foi concluída, uma mensagem será mostrada informando que a exportação ainda não foi realizada. Se uma exportação tiver falhado ou tiver sido cancelada, uma mensagem correspondente também será mostrada.

2. Para gerenciar as configurações de exportação salvas, selecione uma exportação e depois clique em uma das opções a seguir:
   - **Pause** (Pausar): pausar a exportação.
   - **Resume** (Continuar): para reiniciar uma exportação pausada.
   - **Force** (Forçar): para forçar uma nova exportação. Essa opção pode ser útil quando a espera virtual está pausada e depois é retomada, o que significa que o trabalho será reiniciado somente

após uma nova transferência. Se você não quiser aguardar pela nova transferência, você pode forçar uma exportação.

3. Para remover uma exportação do sistema, clique em **Remove** (Remover). Ao remover uma exportação, ela é removida permanentemente do sistema e você não poderá reiniciá-la.
4. Para ver detalhes sobre as exportações ativas atualmente na fila para serem concluídas, clique em **Show Export Queue** (Mostrar fila de exportação).

   A tabela a seguir será mostrada:

Menu	Descrição
Machine Name (Nome da máquina)	O nome da máquina de origem.
Destination (Destination)	A espera virtual está configurada corretamente e está ativa, não pausada. A próxima exportação de espera virtual será realizada após o próximo instantâneo.
Export Type (Tipo de exportação)	A espera virtual está pausada e ainda está salva pelo núcleo. No entanto, após uma nova transferência, o trabalho de exportação não começará automaticamente e não haverá novas exportações de espera virtual para esse agente.
Schedule Type (Tipo de cronograma)	O tipo de exportação, seja única ou contínua.
Status	O andamento da exportação, mostrado como uma porcentagem na barra de progresso.

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

Você pode exportar dados de suas máquinas Windows para uma máquina virtual (VMware, ESXi, e Hyper-V) ao exportar todas as informações de backup de um ponto de recuperação além dos parâmetros definidos para o cronograma de proteção da máquina.

NOTA: Apenas o Dell DL1000 de 3TB com configuração de 2 máquinas virtuais oferece suporte para recursos de exportação única e contínua(espera virtual).

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

1. No Core Console, clique na guia **Protected Machines** (Máquinas protegidas).
2. Na lista de máquinas protegidas, selecione a máquina ou o cluster com o ponto de recuperação que você deseja exportar.
3. No menu suspenso **Actions** (Ações) da máquina, clique em **Export** (Exportar) e depois selecione o tipo de exportação que você deseja realizar. Você pode escolher entre as seguintes opções:
   - One-time (Única)
   - Virtual Standby (Espera virtual)

   A caixa de diálogo do assistente **Export** (Exportar) é mostrada.

Exportar dados do Windows usando a exportação ESXi

No AppAssure, você pode optar por exportar dados usando a exportação ESXi executando uma exportação contínua ou única.

Realizar uma exportação ESXi única

Para realizar uma exportação ESXi única:

1. No Core Console, navegue até a máquina que você deseja exportar.
2. Na guia **Summary** (Resumo), clique em **Actions (Ações)** → **Export** → **One-time (Exportação única)**.
   O assistente **Export** (Exportar) é mostrado na página **Protected Machines** (Máquinas protegidas).
3. Selecione uma máquina para exportação e clique em **Next** (Avançar).
4. Na página **Recovery Points** (Pontos de recuperação), selecione o ponto de recuperação que você deseja exportar e depois clique em **Next** (Avançar).

Definir informações de máquina virtual para realizar uma exportação ESXi

Para definir informações de máquina virtual para realizar uma exportação ESXi:

1. Na página **Destination** (Destino) no assistente **Export** (Exportar), no menu suspenso **Recover to a Virtual Machine** (Recuperar para uma máquina virtual), selecione **ESXi(i)**.
2. Digite os parâmetros para acessar a máquina virtual descritos da seguinte maneira:

Caixa de texto	Descrição
Host Name (Nome de host)	Digite um nome para a máquina do host.
Port (Porta)	Digite a porta da máquina host. A porta padrão é 443.
User name (Nome de usuário)	Digite as credenciais de login da máquina do host.
Password (Senha)	Digite as credenciais de login da máquina do host.

3. Na página **Virtual Machine Options** (Opções de máquina virtual), digite as informações conforme descrito na tabela a seguir.

Caixa de texto	Descrição
Resource Pool (Pool de recursos)	Selecione um pool de recursos na lista suspensa.
Data Store (Armazenamento de dados)	Selecione um armazenamento de dados na lista suspensa.
Virtual Machine Name (Nome da máquina virtual)	Digite um nome para a máquina virtual.
Memory (Memória)	Especifique o uso de memória.
Disk Provisioning (Provisionamento de disco)	Selecione o tipo de provisionamento de disco, dinâmico ou tradicional.

Caixa de texto	Descrição
Disk Mapping (Mapeamento de disco)	Especifique o tipo de mapeamento de disco, automático ou manual.
Version (Versão)	Selecione a versão da máquina virtual.

4. Clique em **Next** (Avançar).
5. Na página **Volumes**, selecione os volumes que você deseja exportar e depois clique em **Next** (Avançar).
6. Na página **Summary** (Resumo), clique em **Finish** (Concluir) para concluir o assistente e iniciar a exportação.

   NOTA: Você pode monitorar o status e o andamento da exportação na guia **Virtual Standby** (Espera virtual) ou **Events** (Eventos).

Realizar uma exportação ESXi contínua (espera virtual)

Para realizar uma exportação ESXi contínua (espera virtual):

1. No Core Console, realize uma das seguintes ações:
   - Na guia Virtual Standby (Espera virtual), clique em **Add** (Adicionar) para abrir o assistente **Export** (Exportar). Na página **Protected Machines** (Máquinas protegidas) do assistente **Export Wizard** (Exportar), selecione a máquina protegida que você deseja exportar e clique em **Next** (Avançar).
   - Navegue até a máquina que você deseja exportar e clique em **Actions (Ações) → Export (Exportar) → Virtual Standby (Espera virtual)**.
2. Na página **Destination** (Destino) do assistente **Export** (Exportar), no menu suspenso **Recover to a Virtual Machine** (Recuperar para uma máquina virtual), selecione **ESXi**.
3. Digite as informações para acessar a máquina virtual conforme descrito na tabela a seguir e clique em **Next** (Avançar).

Caixa de texto	Descrição
Host name (Nome do host)	Digite um nome para a máquina do host.
Port (Porta)	Digite a porta da máquina do host. O padrão é 443.
User Name (Nome de usuário)	Digite as credenciais de login da máquina do host.
Password (Senha)	Digite as credenciais de login da máquina do host.

4. Na página **Virtual Machine Options** (Opções de máquina virtual), digite as informações conforme descrito na tabela a seguir.

Caixa de texto	Descrição
Resource Pool (Pool de recursos)	Selecione um pool de recursos na lista suspensa.
Data Store (Armazenamento de dados)	Selecione um armazenamento de dados na lista suspensa.

Caixa de texto	Descrição
Virtual Machine Name (Nome da máquina virtual)	Digite um nome para a máquina virtual.
Memory (Memória)	Clique em Use a specific amount of RAM (Usar uma quantidade específica de memória RAM) para especificar quanta memória RAM será usada. Por exemplo, 4096 megabytes (MB). A quantidade mínima permitida é 512 MB e a quantidade máxima é determinada pela capacidade e pelas limitações da máquina de host (recomendado).
Disk Provisioning (Provisionamento de disco)	Selecione o tipo de provisionamento de disco, dinâmico ou tradicional.
Disk Mapping (Mapeamento de disco)	Especifique o tipo de mapeamento de disco, automático ou manual.
Version (Versão)	Selecione a versão da máquina virtual.

5. Clique em **Next** (Avançar).
6. Na página **Volumes**, selecione os volumes que você deseja exportar e depois clique em **Next** (Avançar).
7. Na página **Summary** (Resumo), clique em **Finish** (Concluir) para concluir o assistente e iniciar a exportação.

   NOTA: Você pode monitorar o status e o andamento da exportação verificando as guias **Virtual Standby** (Espera virtual) ou **Events** (Eventos).

Exportar dados do Windows usando a exportação de estação de trabalho VMware

No AppAssure, você pode optar por exportar dados usando a exportação de estação de trabalho VMware ao realizar uma exportação única ou contínua. Realize as etapas nos procedimentos a seguir para exportar usando a exportação de estação de trabalho VMware para o tipo de exportação apropriado.

Realizar uma exportação de estação de trabalho VMware única

Para realizar uma exportação de estação de trabalho VMware única:

1. No Core Console, navegue até a máquina que você deseja exportar.
2. Na página **Summary** (Resumo), clique em **Actions (Ações)** → **Export** → **One-time (Exportação única)**.

   O assistente **Export** (Exportar) é mostrado na página **Protected Machines** (Máquinas protegidas).
3. Selecione uma máquina para exportação e, em seguida, clique em **Next** (Avançar).
4. Na página **Recovery Points** (Pontos de recuperação), selecione o ponto de recuperação que você deseja exportar e depois clique em **Next** (Avançar).

Definir as configurações únicas para realizar uma exportação de estação de trabalho VMware

Para definir as configurações únicas para realizar uma exportação de estação de trabalho VMware:

1. Na página **Destination** (Destino) do assistente **Export** (Exportar), no menu suspenso **Recover to Virtual machine** (Recuperar para uma máquina virtual), selecione **VMware Workstation** (Estação de trabalho VMware) e depois clique em **Next** (Avançar).
2. Na página **Virtual Machine Options** (Opções de máquina virtual), digite os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir.

Caixa de texto	Descrição
Local	Especifique o caminho da pasta local ou do compartilhamento de rede no qual você deseja criar a máquina virtual. **NOTA:** Se você especificou um caminho de compartilhamento de rede, você vai precisar inserir as credenciais válidas de login para uma conta que esteja registrada na máquina de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.
User Name (Nome de usuário)	Digite as credenciais de login da máquina virtual. • Se você especificou um caminho de compartilhamento de rede, você precisa digitar um nome de usuário válido para a conta que está registrada na máquina de destino. • Se você digitou um caminho local, não é necessário informar um nome de usuário.
Password (Senha)	Digite as credenciais de login da máquina virtual. • Se você especificou um caminho de compartilhamento de rede, você precisa digitar uma senha válida da conta que está registrada na máquina de destino. • Se você digitou um caminho local, não é necessário informar uma senha.
Virtual Machine Name (Nome da máquina virtual)	Digite um nome para a máquina virtual que está sendo criada; por exemplo, VM-0A1B2C3D4. **NOTA:** O nome padrão é o nome da máquina de origem.
Version (Versão)	Especifique a versão da estação de trabalho VMware para a máquina virtual. Você pode escolher entre as seguintes opções: • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0
Memory (Memória)	Especifique o uso de memória da máquina virtual clicando em uma das opções a seguir: • Use the same amount of RAM as the source machine (Usar a mesma quantidade de memória RAM que a máquina de origem) - Para especificar que a configuração de memória RAM é a mesma da máquina virtual de origem.

Caixa de texto	Descrição
	• Use a specific amount of RAM (Usar uma quantidade específica de memória RAM) - Para especificar quanta memória RAM será usada; por exemplo, 4096 megabytes (MB). A quantidade mínima permitida é 512 MB e a quantidade máxima é determinada pela capacidade e pelas limitações da máquina de host (recomendado).

3. Clique em **Next** (Avançar).
4. Na página **Summary** (Resumo), clique em **Finish** (Concluir) para concluir o assistente e iniciar a exportação.

   NOTA: Você pode monitorar o status e o andamento da exportação verificando as guias **Virtual Standby** (Espera virtual) ou **Events** (Eventos).

Realizar uma exportação de estação de trabalho VMware contínua (espera virtual)

Para realizar uma exportação de estação de trabalho VMware contínua (espera virtual):

1. No Core Console, realize uma das seguintes ações:
   - Na guia Virtual Standby (Espera virtual), clique em **Add** (Adicionar) para abrir o assistente **Export** (Exportar). Na página **Protected Machines** (Máquinas protegidas) do assistente **Export Wizard** (Exportar), selecione a máquina protegida que você deseja exportar e clique em **Next** (Avançar).
   - Navegue até a máquina que você deseja exportar e, na guia **Summary** (Resumo) no menu suspenso **Actions** (Ações) da máquina, clique em **Export (Exportar) → Virtual Standby (Espera virtual)**.
2. Na página **Destination** (Destino) do assistente **Export** (Exportar), clique em **Recover to a Virtual Machine → VMware Workstation** (Recuperar para uma máquina virtual, Estação de trabalho VMware).
3. Clique em **Next** (Avançar).
4. Na página **Virtual Machine Options** (Opções de máquina virtual), digite os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir.

Caixa de texto	Descrição
Target Path (Caminho de destino)	Especifique o caminho da pasta local ou do compartilhamento de rede no qual você deseja criar a máquina virtual. NOTA: Se você especificou um caminho de compartilhamento de rede, digite as credenciais válidas de login para uma conta que esteja registrada na máquina de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.
User Name (Nome de usuário)	Digite as credenciais de login da máquina virtual. • Se você especificou um caminho de compartilhamento de rede, você precisa digitar um nome de usuário válido para a conta que está registrada na máquina de destino. • Se você digitou um caminho local, não é necessário informar um nome de usuário.
Password (Senha)	Digite as credenciais de login da máquina virtual. • Se você especificou um caminho de compartilhamento de rede, você precisa digitar uma senha válida da conta que está registrada na máquina de destino.

Caixa de texto	Descrição
	• Se você digitou um caminho local, não é necessário informar uma senha.
Virtual Machine (Máquina virtual)	Digite um nome para a máquina virtual que está sendo criada; por exemplo, VM-0A1B2C3D4. **NOTA:** O nome padrão é o nome da máquina de origem.
Version (Versão)	Especifique a versão da estação de trabalho VMware para a máquina virtual. Você pode escolher entre as seguintes opções: • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0
Memory (Memória)	Especifique a memória para a máquina virtual clicando em uma das opções a seguir: • Use the same amount of RAM as the source machine (Usar a mesma quantidade de memória RAM que a máquina de origem) - Para especificar que a configuração de memória RAM é a mesma da máquina virtual de origem. • Use a specific amount of RAM (Usar uma quantidade específica de memória RAM) - Para especificar quanta memória RAM será usada; por exemplo, 4096 megabytes (MB). A quantidade mínima permitida é 512 MB e a quantidade máxima é determinada pela capacidade e pelas limitações da máquina de host.

5. Selecione **Perform initial ad-hoc export** (Realizar exportação ad-hoc inicial) para realizar a exportação virtual imediatamente em vez ou após o próximo instantâneo agendado.
6. Clique em **Next** (Avançar).
7. Na página **Volumes**, selecione os volumes para exportação; por exemplo, C:\ e D:\, e clique em **Next** (Avançar).
8. Na página **Summary** (Resumo), clique em **Finish** (Concluir) para concluir o assistente e iniciar a exportação.

   NOTA: Você pode monitorar o status e o andamento da exportação verificando as guias **Virtual Standby** (Espera virtual) ou **Events** (Eventos).

Exportar dados do Windows usando a exportação do Hyper-V

No AppAssure, você pode optar por exportar dados usando a exportação do Hyper-V ao realizar uma exportação única ou contínua. Realize as etapas nos procedimentos a seguir para exportar usando a exportação do Hyper-V para o tipo de exportação apropriado.

Realizar uma exportação do Hyper-V única

Para realizar uma exportação do Hyper-V única:

1. No Core Console, navegue até a máquina que você deseja exportar.
2. Na guia Summary (Resumo), clique em **Actions (Ações)** → **Export** → **One-time (Exportação única)**.
   O assistente **Export** (Exportar) é mostrado na página **Protected Machines** (Máquinas protegidas).
3. Selecione uma máquina para exportação e, em seguida, clique em **Next** (Avançar).

4. Na página **Recovery Points** (Pontos de recuperação), selecione o ponto de recuperação que você deseja exportar e depois clique em **Next** (Avançar).

Definir as configurações únicas para realizar uma exportação do Hyper-V

Para definir as configurações únicas para realizar uma exportação do Hyper-V:

1. Na caixa de diálogo do Hyper-V, clique em **Use local machine** (Usar máquina local) para realizar a exportação em Hyper-V para uma máquina local com a função de Hyper-V atribuída.
2. Clique na opção **Remote host** (Host remoto) para indicar que o servidor Hyper-V está situado em uma máquina remota. Se você selecionou a opção Host remoto, digite os parâmetros para o host remoto conforme descrito a seguir:

Caixa de texto	Descrição
Host Name (Nome do host)	Digite um endereço IP ou nome de host para o servidor Hyper-V. Ele representa o endereço IP ou nome de host do servidor Hyper-V remoto.
Port (Porta)	Digite um número de porta para a máquina. Ele representa a porta através da qual o núcleo se comunica com essa máquina.
User Name (Nome de usuário)	Digite o nome de usuário do usuário com privilégios administrativos para a estação de trabalho com o servidor Hyper-V. Ele é usado para especificar as credenciais de login da máquina virtual.
Password (Senha)	Digite a senha do usuário com privilégios administrativos na estação de trabalho com o servidor Hyper-V. Ela é usada para especificar as credenciais de login da máquina virtual.

3. Clique em **Next** (Avançar).
4. Na página **Virtual Machines Options** (Opções de máquinas virtuais), digite o caminho ou o local da máquina virtual na caixa de texto **VM Machine Location** (Local da máquina virtual). Por exemplo, **D:\export**. O local da máquina virtual precisa ter espaço suficiente para armazenar os metadados da MV e as unidades virtuais necessárias para a máquina virtual.
5. Digite um nome para a máquina virtual na caixa de texto **Virtual Machine Name** (Nome da máquina virtual).

   O nome que você digitar será mostrado na lista de máquinas virtuais do console do gerenciador do Hyper-V.
6. Clique em uma das seguintes opções:
   - **Use the same amount of RAM as the source machine** (Usar a mesma quantidade de memória RAM que a máquina de origem) - para identificar que o uso da memória RAM é idêntico entre máquinas virtuais e de origem.
   - **Use a specific amount of RAM** (Usar uma quantidade de memória RAM específica) - para especificar quanta memória a máquina virtual tem após a exportação; por exemplo, 4096 MB (recomendado).
7. Para especificar o formato de disco, ao lado de **Disk Format** (Formato do disco), clique em uma das seguintes opções:
   - **VHDX**
   - **VHD (Disco rígido virtual)**

   NOTA: A exportação do Hyper-V Export oferece suporte para formatos de disco em VHDX se a máquina de destino estiver executando o Windows 8 (Windows Server 2012) ou mais recente. Se o VHDX não for compatível com o seu ambiente, a opção está desativada.
8. Na página **Volumes**, selecione os volumes a serem exportados. Para que a máquina virtual seja um backup efetivo da máquina protegida, inclua a unidade de inicialização da máquina protegida. Por exemplo, C:\.

Seus volumes selecionados não devem ser superiores a 2040 GB para o VHD. Se os volumes selecionados forem superiores a 2040 GB e o formato VHD for selecionado, será indicado um erro.

9. Na página **Summary** (Resumo), clique em **Finish** (Concluir) para concluir o assistente e iniciar a exportação.

Executar uma exportação contínua para Hyper-V (espera virtual)

NOTA: Apenas a configuração de 3 TB com 2 MVs do DL1000 oferece suporte para os recursos de exportação única e de exportação contínua (espera virtual).

Para executar uma exportação contínua para Hyper-V (espera virtual):

1. Na guia **Virtual Standby** (Espera virtual) do Core Console, clique em **Add** (Adicionar) para abrir o **Assistente de exportação**. Na página **Protected Machines** (Máquinas protegidas) do **Assistente de exportação**,
2. selecione a máquina que você quer exportar e clique em **Next** (Avançar).
3. Na guia **Summary** (Resumo), clique em **Export (Exportar) → Virtual Standby (Espera virtual)**.
4. Na caixa de diálogo Hyper-V, clique em **Use local machine** (Usar máquina local) para executar a exportação para Hyper-V para uma máquina local com a função Hyper-V atribuída.
5. Clique na opção **Remote host** (Host remoto) para indicar que o servidor Hyper-V está localizado em uma máquina remota. Se você selecionou a opção Remote host (Host remoto), digite os parâmetros do host remoto, conforme descrito a seguir:

Caixa de texto	Descrição
Host Name (Nome de host)	Digite um endereço IP ou um nome de host para o servidor Hyper-V. Ele representa o endereço IP ou o nome de host do servidor Hyper-V remoto.
Porta	Digite um número de porta para a máquina. Ele representa a porta através da qual o Núcleo se comunica com esta máquina.
Nome de Usuário	Digite o nome de usuário para o usuário com privilégios administrativos na estação de trabalho com o servidor Hyper-V. Ele é usado para especificar as credenciais de login da máquina virtual.
Senha	Digite a senha da conta de usuário com privilégios administrativos na estação de trabalho com o servidor Hyper-V. Ela é usada para especificar as credenciais de login da máquina virtual.

6. Na caixa de texto **VM Machine Location** (Local da máquina virtual) da página **Virtual Machines Options** (Opções de máquinas virtuais), digite o caminho ou o local da máquina virtual. Por exemplo, D:\export. O local da MV precisa ter espaço suficiente para guardar os metadados da MV e as unidades virtuais necessárias para a máquina virtual.
7. Digite um nome para a máquina virtual na caixa de texto **Virtual Machine Name** (Nome da máquina virtual).

   O nome que você digitar será mostrado na lista de máquinas virtuais do console do Gerenciador do Hyper-V.
8. Clique em uma das opções a seguir:
   - **Use the same amount of RAM** (Usar a mesma quantidade de RAM) que a máquina de origem para identificar que o uso de RAM é idêntico na máquina virtual e na máquina de origem.
   - **Use a specific amount of RAM** (Usar uma quantidade específica de RAM) para especificar a quantidade de memória que a máquina virtual deve ter após a exportação; por exemplo, 4.096 MB (recomendado).
9. Para especificar a Geração, clique em uma das opções a seguir:
   - Generation 1 (Geração 1) (recomendada)

- Generation 2 (Geração 2)

10. Para especificar o formato do disco, clique em uma das seguintes opções ao lado de **Disk Format** (Formado do disco):
    - **VHDX** (Padrão)
    - **VHD**

    NOTA: A exportação para Hyper-V suporta os formatos de disco VHDX apenas se a máquina de destino estiver rodando o Windows 8 (Windows Server 2012) ou posterior. Se o VHDX não for suportado em seu ambiente, a opção estará desabilitada. Na página Network Adapters (Adaptadores de rede), selecione o adaptador virtual que será conectado a um comutador.
11. Na página **Volumes**, selecione os volumes que você quer exportar. Para que a máquina virtual seja um backup efetivo da máquina protegida, adicione a unidade de inicialização da máquina protegida. Por exemplo, C:\.

    Os volumes selecionados não devem ser maiores do que 2.040 GB para VHD. Se os volumes selecionados forem maiores que 2.040 GB e o formato VHD estiver selecionado, você receberá uma mensagem de erro.
12. Na página **Summary** (Resumo), clique em **Finish** (Concluir) para concluir o assistente e iniciar a exportação.

    NOTA: Você pode monitorar o status e o andamento da exportação na guia **Virtual Standby** (Espera virtual) ou **Events** (Eventos)

Exportar dados do Windows usando a exportação de Oracle VirtualBox

No da AppAssure, você pode optar por exportar dos dados usando a exportação VirtualBox ao executar uma exportação contínua ou única ou ao estabelecer uma exportação contínua (para espera virtual).

Conclua as etapas nos procedimentos a seguir para o tipo apropriado de exportação.

NOTA: Para executar este tipo de exportação, que você já deve ter o Oracle VirtualBox instalado na máquina do núcleo. Há suporte para o VirtualBox versão 4.2.18 ou superior em hosts Windows.

Realizar uma exportação única do Oracle VirtualBox

Para realizar uma exportação única do Oracle VirtualBox:

1. No Core Console, navegue até a máquina Linux que você deseja exportar.
2. Na guia **Summary** (Resumo), clique em **Actions (Ações)** → **Export** → **One-time (Exportação única)**.

   O assistente **Export** (Exportar) é mostrado na página **Protected Machines** (Máquinas protegidas).
3. Selecione uma máquina para exportação e, em seguida, clique em **Next** (Avançar).
4. Na página **Recovery Points** (Pontos de recuperação), selecione o ponto de recuperação que você deseja exportar e depois clique em **Next** (Avançar).
5. Na página **Destination** (Destino) do assistente **Export** (Exportar), no menu suspenso **Recover to Virtual machine** (Recuperar para uma máquina virtual),selecione **Virtualbox** e clique em **Next** (Avançar).
6. Na página **Virtual Machine Options** (Opções de máquina virtual), selecione **Remote Linux Machine** (Máquina Linux remota).
7. Digite os parâmetros para acessar a máquina virtual da seguinte maneira:

Caixa de texto	Descrição
VirtualBox Host Name (Nome do host VirtualBox)	Digite um endereço IP ou nome de host para o servidor VirtualBox. Este campo representa o endereço IP ou o nome de host do servidor remoto VirtualBox.
Port (Porta)	Digite um número de porta para a máquina. Esse número representa a porta através da qual o núcleo se comunica com essa máquina.
Virtual Machine Name (Nome da máquina virtual)	Especifique um caminho de destino para criar a máquina virtual.
User Name (Nome de usuário)	Nome de usuário da conta na máquina de destino; por exemplo, raiz.
Password (Senha)	Digite as credenciais de login da máquina do host.
Memória	Especifique a memória para a máquina virtual.

8. Na página **Volumes**, selecione os volumes de dados para exportar e depois clique em **Next** (Avançar).
9. Na página **Summary** (Resumo), clique em **Finish** (Concluir) para concluir o assistente e iniciar a exportação.

   NOTA: Você pode monitorar o status e o andamento da exportação na guia Virtual Standby (Espera virtual) ou Events (Eventos).

Realizar uma exportação de Oracle VirtualBox contínua (espera virtual)

Para realizar uma exportação de Oracle VirtualBox contínua (espera virtual):

1. No Core Console, faça uma das seguintes ações:
   - Na guia **Virtual Standby** (Espera virtual), clique em **Add** (Adicionar) para abrir o assistente **Export** (Exportar). Na página **Protected Machines** (Máquinas protegidas) do assistente **Export Wizard** (Exportar), selecione a máquina protegida que você deseja exportar e clique em **Next** (Avançar).
   - Navegue até a máquina que você deseja exportar e, na guia **Summary** (Resumo) no menu suspenso **Actions** (Ações) da máquina, clique em **Export (Exportar) → Virtual Standby (Espera virtual)**.
2. Na página **Destination** (Destino) do assistente **Export** (Exportar), no menu suspenso **Recover to Virtual machine** (Recuperar para uma máquina virtual), selecione **Virtualbox** e depois clique em **Next** (Avançar).
3. Na página **Virtual Machine Options** (Opções de máquina virtual), selecione **Use Windows machine** (Usar máquina Windows).
4. Digite os parâmetros para acessar a máquina virtual conforme descrito na tabela a seguir.

Caixa de texto	Descrição
Virtual Machine Name (Nome da máquina virtual)	Digite um nome para a máquina virtual que está sendo criada. NOTA: O nome padrão é o nome da máquina de origem.
Target Path (Caminho de destino)	Especifique um local ou um caminho de destino para criar a máquina virtual. NOTA: O caminho de destino não deve ser um diretório raiz.

Caixa de texto	Descrição
	Se você especificar um caminho de compartilhamento de rede, você vai precisar inserir credenciais válidas de login (nome de usuário e senha) para uma conta que esteja registrada na máquina de destino. A conta precisa ter permissões de leitura e gravação para o compartilhamento de rede.
Memory (Memória)	Especifique a memória para a máquina virtual. • Clique em **Use the same amount of RAM as the source machine** (Usar a mesma quantidade de memória RAM que a máquina de origem) para especificar que a configuração de memória RAM é a mesma da máquina virtual de origem. • Clique em **Use a specific amount of RAM** (Usar uma quantidade específica de memória RAM) para especificar quanta memória RAM será usada; por exemplo, 4096 megabytes (MB). A quantidade mínima permitida é 512 MB e a quantidade máxima é determinada pela capacidade e pelas limitações da máquina de host.

5. Para especificar uma conta de usuário para a máquina virtual, selecione **Specify the user account for the exported virtual machine** (Especificar a conta de usuário para a máquina virtual exportada) e depois digite as informações a seguir. Isso se refere a uma conta de usuário específica para a qual a máquina virtual será registrada no caso de haver múltiplas contas de usuário na máquina virtual. Quando essa conta de usuário é conectada, somente esse usuário verá essa máquina virtual no gerenciador do VirtualBox. Se uma conta não for especificada, então a máquina virtual será registrada para todos os usuários atuais na máquina Windows com VirtualBox.
   - Nome de usuário - Digite o nome de usuário para o qual a máquina virtual está registrada.
   - Senha - Digite a senha para essa conta de usuário.
6. Selecione **Perform initial ad-hoc export** (Realizar exportação ad-hoc inicial) para realizar a exportação virtual imediatamente em vez ou após o próximo instantâneo agendado.
7. Clique em **Next** (Avançar).
8. Na página **Volumes**, selecione os volumes para exportação; por exemplo, C:\ e D:\, e depois clique em **Next** (Avançar).
9. Na página **Summary** (Resumo), clique em **Finish** (Concluir) para concluir o assistente e iniciar a exportação.

   NOTA: Você pode monitorar o status e o andamento da exportação verificando as guias **Virtual Standby** (Espera virtual) ou **Events** (Eventos).

Restaurar volumes a partir de um ponto de recuperação

Você pode restaurar os volumes em uma máquina protegida a partir dos pontos de recuperação armazenados no AppAssure Core. Para restaurar volumes a partir de um ponto de recuperação:

1. No Core Console, clique na guia **Restore** (Restaurar).

   O assistente **Restore Machine** (Restaurar máquina) é mostrado.
2. Na página **Protected Machines** (Máquinas protegidas), selecione a máquina protegida para a qual você deseja restaurar os dados e depois clique em **Next** (Avançar).

   NOTA: A máquina protegida precisa ter o software do agente instalado e deve possuir pontos de recuperação a partir dos quais você realizará a operação de restauração.

   A página **Recovery Points** (Pontos de recuperação) é mostrada.

3. A partir da lista de pontos de recuperação, procure o instantâneo que você deseja restaurar para a máquina do agente.

   NOTA: Se necessário, use os botões de navegação na parte inferior da página para mostrar outros pontos de recuperação. Ou, se você quiser limitar a quantidade de pontos de recuperação mostrada na página de pontos de recuperação do assistente, é possível filtrar por volumes (se definido) ou por data de criação do ponto de recuperação.

4. Clique em qualquer ponto de recuperação para selecioná-lo e depois clique em **Next** (Avançar).

   A página **Destination** (Destino) é mostrada.

5. Na página **Destination** (Destino), escolha a máquina para a qual você deseja restaurar os dados da seguinte forma:

   - Se quiser restaurar dados do ponto de recuperação selecionado para a mesma máquina do agente (por exemplo, Maquina1), e se os volumes que você deseja restaurar não incluírem o volume de sistema, selecione a opção **Recover to a protected machine (only non-system volumes)** (Recuperar para uma máquina protegida (apenas volumes que não sejam de sistema)), verifique se a máquina de destino (Maquina1) está selecionada e depois clique em **Next** (Avançar). A página **Volume Mapping** (Mapeamento de volume) é mostrada. Prossiga para a etapa 7.
   - Se você quiser restaurar dados a partir do ponto de recuperação para outra máquina protegida (por exemplo, para substituir o conteúdo da Maquina2 com dados da Maquina1), selecione **Recover to a protected machine (only non-system volumes)** (Recuperar para uma máquina protegida (apenas volumes que não sejam de sistema)), selecione a máquina de destino (por exemplo, Maquina2) na lista e depois clique em **Next** (Avançar). A página **Volume Mapping** (Mapeamento de volume) é mostrada. Prossiga para a etapa 7.
   - Se você quiser restaurar a partir do ponto de restauração selecionado para a mesma máquina ou uma máquina diferente usando um CD de inicialização e se os volumes que você deseja restaurar não incluírem o volume de sistema, selecione **Recover to any target machine using a boot CD** (Recuperar para qualquer máquina de destino usando um CD de inicialização).
   - Para continuar e criar o CD de inicialização com informações do ponto de recuperação selecionado, clique em **Next** (Avançar) e prossiga para a etapa 10.
   - Se você já tiver criado o CD de inicialização e a máquina de destino tiver sido iniciada usando o CD de inicialização, prossiga para a etapa 17.
   - Se quiser restaurar a partir de um ponto de recuperação para um volume de sistema (por exemplo, a unidade C da máquina de agente nomeada como Maquina1), você precisa realizar uma recuperação sem sistema operacional (BMR). Para obter mais informações sobre como realizar uma BMR no Windows, consulte Launching Bare Metal Restore For Windows Machines (Iniciar a restauração sem sistema operacional para máquinas Windows).
   - Para obter informações sobre como realizar uma BMR para Linux, consulte Roteiro para realizar uma restauração sem sistema operacional em máquinas LinuxIniciar uma restauração sem sistema operacional para uma máquina Linux.

6. Para conectar-se ao console de recuperação universal (URC) na máquina de destino, faça o seguinte:

   a. Selecione **I already have a boot CD running on the target machine** (Já tenho um CD de inicialização em execução na máquina de destino).
   b. Na caixa de texto endereço IP, digite o endereço IP da máquina de destino com o CD de inicialização.
   c. Na caixa de texto Authentication Key (Chave de autenticação), digite a chave de autenticação do URC na máquina de destino e depois clique em **Next** (Avançar).

   A página **Disk Mapping** (Mapeamento de disco) é mostrada. Prossiga para a etapa 20.

7. Na página **Volume Mapping** (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, selecione **Do not restore** (Não restaurar) na coluna Destination Volumes (Volumes de destino).

8. Selecione **Show advanced options** (Mostrar opções avançadas) e, em seguida, faça o seguinte:
   - Se quiser usar a recuperação em tempo real para restaurar para máquinas Windows, selecione **Live Recovery** (Recuperação em tempo real).

     Usando a tecnologia de recuperação instantânea em tempo real no AppAssure, você pode recuperar ou restaurar dados instantaneamente para suas máquinas físicas ou virtuais a partir dos pontos de recuperação armazenados de máquinas Windows, incluindo Microsoft Windows Storage Spaces. O recurso de recuperação em tempo real não está disponível para máquinas Linux.
   - Se você deseja forçar a desmontagem, selecione **Force Dismount** (Forçar desmontagem).

     Se você não forçar uma desmontagem antes de restaurar os dados, a restauração pode falhar com um erro de volume em uso.
9. Prossiga para a etapa 20.
10. Na página Boot CD (CD de inicialização), faça o seguinte:
    a. No campo de texto **Output path** (Caminho de saída), digite o caminho no qual a imagem de ISO do CD de inicialização deve ser armazenada,
    b. Em **Environment** (Ambiente), selecione a arquitetura mais adequada para o hardware que você está restaurando:
       - Para restaurar em qualquer máquina Windows com uma arquitetura de 64 bits, selecione **Windows 8 64-bit** (Windows 8 64 bits).
       - Para restaurar em qualquer máquina com uma arquitetura de 32 bits (x86), selecione **Windows 7 32-bit** (Windows 7 32 bits).
11. Opcionalmente, para configurar parâmetros de rede para o agente restaurado , ou para usar o UltraVNC, selecione **Show advanced options** (Mostrar opções avançadas) e selecione uma das opções a seguir:
    - Para estabelecer uma conexão de rede para a máquina restaurada, selecione **Use the following IP address** (Usar o seguinte endereço IP), conforme descrito na tabela a seguir.

Opção	Descrição
Endereço IP	Especifique o endereço IP ou o 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.
Servidor DNS	Especifique o servidor de nome de domínio da máquina restaurada.

    - Para definir as informações de UltraVNC, selecione **Add UltraVNC** (Adicionar UltraVNC) conforme descrito na tabela a seguir. Use essa opção se você precisar de acesso remoto ao console de recuperação. Você não pode fazer login nos Serviços de terminal da Microsoft enquanto usa o CD de inicialização.

Opção	Descrição
Password (Senha)	Especifique uma senha para essa conexão UltraVNC.
Port (Porta)	Especifique uma porta para essa conexão UltraVNC. A porta padrão é 5900.

12. Clique em **Next** (Avançar).
13. Para injetar um driver, faça o seguinte:
    a. Selecione **Add an archive of drivers** (Adicionar um arquivo de drivers).
    b. Navegue até um arquivo ZIP que contenha o arquivo, selecione o arquivo ZIP e clique em **Open** (Abrir). O arquivo é enviado e aparece na página Driver Injection (Injeção de driver).

c. Em seguida, clique em **Next** (Avançar).

14. Na página da imagem ISO, você pode ver o status conforme a imagem ISO do CD de inicialização é criada. Quando o CD de inicialização for criado com sucesso, clique em **Next** (Avançar).

    A página **Connection** (Conexão) é mostrada.

15. Inicie a máquina do agente para a qual você deseja restaurar os dados a partir do CD de inicialização.
    - Se possível, inicialize a máquina do agente a partir da imagem ISO.
    - Caso não seja possível, copie a imagem ISO para uma mídia física (um CD ou um DVD), carregue o disco na máquina do agente, configure a máquina para carregar a partir do CD de inicialização e reinicie a partir do CD de inicialização.

    NOTA: Pode ser necessário alterar as configurações do BIOS da máquina do agente para garantir que o primeiro volume a ser carregado seja o CD de inicialização.

    A máquina do agente, quando iniciada a partir do CD de inicialização, mostra a interface do console de recuperação universal (URC). Esse ambiente é usado para restaurar a unidade do sistema ou volumes selecionados diretamente a partir do AppAssure Core. Observe que o endereço IP e as credenciais de chave de autenticação no URC são atualizados toda vez que você inicia a partir do CD de inicialização.

16. No Core Console na página **Connection** (Conexão), digite as informações de autenticação da instância URC da máquina que você deseja restaurar da seguinte maneira:
    a. Na caixa de texto IP Address (Endereço IP), digite o endereço IP da máquina para a qual você está restaurando a partir de um ponto de recuperação.
    b. Na caixa de texto Authentication Key (Chave de autenticação), digite as informações do URC.
    c. Clique em **Next** (Avançar).

    A página **Disk Mapping** (Mapeamento de disco) é mostrada.

17. Para mapear os volumes manualmente, prossiga para a etapa 18. Para mapear os volumes automaticamente, faça o seguinte:
    a. Selecione **Automatic volume mapping** (Mapeamento automático de volume).
    b. Na área **Automatic volume mapping** (Mapeamento automático de volume), selecione os volumes que você deseja restaurar. Se você não deseja restaurar um volume listado, desmarque a opção.

       NOTA: No mínimo um volume precisa ser selecionado para realizar a restauração.
    c. Selecione o disco de destino para a restauração.
    d. Clique em **Next** (Avançar) e depois prossiga para a etapa 19.

18. Se você quiser mapear os volumes manualmente, faça o seguinte:
    a. Selecione **Manual volume mapping** (Mapeamento manual de volume).
    b. Na área **Manual volume mapping** (Mapeamento manual de volume), na lista suspensa **Destination Volumes** (Volumes de destino) de cada volume, selecione o volume que você deseja restaurar. Se você não desejar restaurar um volume listado, desmarque a opção.

       NOTA: No mínimo um volume precisa ser selecionado para realizar a restauração.
    c. Clique em **Finish** (Concluir).

    CUIDADO: Se você selecionar Finish (Concluir), todas as partições e dados atuais na unidade de destino serão removidas permanentemente e substituídas pelo conteúdo do ponto de recuperação selecionado, incluindo o sistema operacional e todos os dados.

    O assistente **Restore Machine** (Restaurar máquina) é fechado e os dados são restaurados dos volumes selecionados do ponto de recuperação para a máquina de destino. Prossiga para a etapa 22.

19. Na página **Disk Mapping Preview** (Pré-visualização de mapeamento de disco), confira os parâmetros das ações de restauração selecionadas. Para realizar a restauração, clique em **Finish** (Concluir).

CUIDADO: Se você selecionar Finish (Concluir), todas as partições e dados atuais na unidade de destino serão removidas permanentemente e substituídas pelo conteúdo do ponto de recuperação selecionado, incluindo o sistema operacional e todos os dados.

O assistente **Restore Machine** (Restaurar máquina) é fechado e os dados são restaurados dos volumes selecionados do ponto de recuperação para a máquina de destino. Prossiga para a etapa 22.

20. Se os volumes que você deseja restaurar contiverem bancos de dados SQL ou Microsoft Exchange, na página **Dismount Databases** (Desmontar bancos de dados), você é solicitado a desmontá-los. Opcionalmente, se você quiser remontar esses bancos de dados após a restauração ser concluída, selecione **Automatically remount all databases after the recovery point is restored** (Remontar automaticamente todos os bancos de dados após o ponto de recuperação ser restaurado). Clique em **Finish** (Concluir).
21. Clique em **OK** para confirmar a mensagem de status informando que o processo de restauração foi iniciado.
22. Para monitorar o andamento da ação de restauração, no Core Console, clique em **Events** (Eventos).

Restaurar volumes para uma máquina Linux usando a linha de comando

No AppAssure, você pode restaurar os volumes em suas máquinas Linux protegidas usando o utilitário de linha de comando `aamount`. Para restaurar os volumes para uma máquina Linux usando a linha de comando:

CUIDADO: Você não deve tentar restaurar o sistema ou o volume raiz (/).

1. Execute o utilitário AppAssure `aamount` como raiz, por exemplo:

   ```
   sudo aamount
   ```

2. No prompt de montagem do AppAssure, digite o comando a seguir para listar as máquinas protegidas:

   ```
   lm
   ```

3. Quando solicitado, digite o endereço IP ou nome do host do servidor do AppAssure Core.
4. Digite as credenciais de login, ou seja, o nome de usuário e a senha, desse servidor.

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

   ```
   lr <machine_line_item_number>
   ```

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

   Uma lista mostra os pontos de recuperação básicos e incrementais da máquina. A lista inclui um número de item, marcação de data/hora,local do volume, tamanho do ponto de recuperação e um número de ID do volume que inclui um número de sequência no final (por exemplo, `"293cc667-44b4-48ab-91d8-44bc74252a4f:2"`), que identifica o ponto de recuperação.
6. Para selecionar um ponto de recuperação para reversão, digite o comando a seguir:

   ```
   r [volume_recovery_point_ID_number] [path]
   ```

   Esse número reverte a imagem do volume especificada pela ID do núcleo ao caminho especificado. O caminho para a reversão é o caminho para o descritor do arquivo do dispositivo e não é o diretório ao qual ele está montado.

NOTA: Para identificar o ponto de recuperação, você pode também especificar um número de linha no comando, em vez do número de ID do ponto de recuperação. Nesse caso, use o número de linha do agente/máquina (da saída `lm`), seguido do número de linha do ponto de recuperação e a letra do volume, seguido pelo caminho, como `r [machine_line_item_number] [recovery_point_line_number] [volume_letter] [path]`. Nesse comando, [caminho] é o descritor de arquivo para o volume real.

Por exemplo, se o comando `lm` mostra três máquinas de agente, e você digitar o comando `lr` para a máquina número 2 e quiser reverter o volume b do ponto de recuperação 23 para o volume que estava montado no diretório `/mnt/data`, o comando é: `r2 23 b /mnt/data`.

7. Quando solicitado para continuar, digite `y` (yes) para indicar Sim.

   após a reversão, uma série de mensagens é mostrada para notificar você sobre o status.

8. Após a reversão, o utilitário `aamount` monta e reanexa automaticamente o módulo kernel ao volume revertido se o destino estiver previamente protegido e montado. Caso contrário, monte o volume de reversão no disco local e depois verifique se os arquivos são restaurados.

   Por exemplo, você pode usar o comando `sudo mount` e, em seguida, o comando `ls`.

Iniciar a restauração sem sistema operacional para máquinas Windows

O AppAssure oferece o recurso de executar uma restauração sem sistema operacional (BMR) para máquinas Windows independentemente do hardware ser similar ou diferente. Este processo engloba a criação de uma imagem de CD de inicialização, gravar a imagem em disco, inicializar o servidor de destino a partir do disco, conectar-se à instância do console de recuperação, mapear volumes, iniciar o recuperação e monitorar o processo. Depois que a restauração sem sistema operacional estiver concluída, você pode continuar a tarefa de carregar o sistema operacional e os aplicativos de software no servidor restaurado, seguido por suas configurações e definições únicas.

Outras circunstâncias nas quais você pode optar por executar uma restauração sem sistema operacional incluem upgrade de hardware ou substituição do servidor.

O recurso de BMR também é suportado para máquinas Linux protegidas usando o utilitário de linha de comando `aamount`. Para obter mais informações, consulte Iniciar uma restauração sem sistema operacional para uma máquina Linux.

Roteiro para realizar uma restauração sem sistema operacional para uma máquina Windows

Para realizar uma BMR em uma máquina Windows:

1. Crie um CD de inicialização.
2. Grave a imagem no disco.
3. Inicialize o servidor de destino pelo CD de inicialização.
4. Conecte-se ao disco de recuperação.
5. Mapeie os volumes.
6. Inicie a recuperação.
7. Monitore o andamento.

Criar uma imagem ISO em CD inicializável

Para realizar uma BMR para uma máquina Windows, você precisa criar uma imagem ISO/CD inicialização no Core Console, o qual contém a interface do console de recuperação universal do AppAssure. O console de recuperação universal do AppAssure é um ambiente usado para restaurar a unidade do sistema ou todo o servidor diretamente do AppAssure Core.

A imagem ISO que você cria é personalizada para a máquina que está sendo restaurada; dessa forma, ela precisa conter os drivers corretos de armazenamento em massa e rede. Se você prever que vai realizar restaurações para um hardware diferente da máquina na qual está criando o CD inicializável, você precisa incluir os drivers do controlador de armazenamento e outros no CD inicializável; consulte Injetar drivers em um CD inicializável.

NOTA: A Organização Internacional para Padronização (ISO) é um órgão internacional de representantes de diversas organizações nacionais que determina e define os padrões de sistema de arquivos. O ISO 9660 é um padrão de sistema de arquivos usado em mídias de disco ótico para troca de dados. Ele oferece suporte para diversos sistemas operacionais, como o Windows. Uma imagem ISO é o arquivo dos dados arquivados ou imagem em disco que contém dados de todos os setores do disco, além do sistema de arquivos do disco.

Para criar uma imagem ISO em CD inicializável:

1. No Core Console onde o servidor que você deseja restaurar está localizado, selecione **Core** (Núcleo) e depois clique na guia **Tools** (Ferramentas).
2. Clique em **Boot CDs** (CDs inicializáveis).
3. Selecione **Actions** (Ações) e depois clique em **Create Boot ISO** (Criar ISO inicializável).

   A caixa de diálogos **Create Boot CD** (Criar ISO inicializável) é mostrada. Para preencher a caixa de diálogo, use os procedimentos a seguir.

Nomear o arquivo de CD de inicialização e definição do caminho

Para nomear o arquivo de CD de inicialização e definir o caminho:

Na caixa de diálogo **Create Boot CD** (Criar CD de inicialização), digite o caminho ISO onde deve ser armazenado a imagem de inicialização no servidor do núcleo.

Se o compartilhamento no qual você deseja armazenar a imagem estiver com pouco espaço em disco, você pode definir o caminho conforme for necessário; por exemplo, D:\nomedoarquivo.iso.

NOTA: A extensão do arquivo deve ser .iso. Ao especificar o caminho, use somente caracteres alfanuméricos , o hífen e o ponto final (apenas para separar os nomes de host e domínios). As letras A a Z fazem distinção entre maiúsculas e minúsculas. Não use espaços. Nenhum caractere de símbolo ou de pontuação é permitido.

Criar conexões

Para criar conexões:

1. Em **Connection Options** (Opções de conexão), faça o seguinte:
   - Para obter o endereço IP dinamicamente usando o protocolo de configuração de host dinâmico (DHCP), selecione **Obtain IP address automatically** (Obter endereço IP automaticamente).
   - Opcionalmente, para especificar um endereço IP estático para o console de recuperação, selecione **Use the following IP address** (Usar o seguinte endereço IP) e digite o endereço IP, a

máscara de sub-rede, o gateway padrão e o servidor DNS nos campos apropriados. Você precisa especificar todos esses campos.

2. Caso seja necessário, em **UltraVNC Options** (Opções de UltraVNC), selecione **Add UltraVNC** (Adicionar UltraVNC) e depois digite as opções de UltraVNC. As configurações de UltraVNC permitem que você gerencie remotamente o console de recuperação enquanto ele está em uso.

   NOTA: Essa etapa é opcional. Se você precisar de acesso remoto para o console de recuperação, você precisa configurar e usar o UltraVNC. Você não pode fazer login usando os serviços de terminal da Microsoft enquanto usa o CD de inicialização.

Injetar drivers em um CD de inicialização

A injeção de drivers é usada para facilitar a operabilidade entre o console de recuperação, o adaptador de rede e o armazenamento no servidor de destino.

Se estiver restaurando para um hardware diferente, você precisa injetar os drivers de controlador de armazenamento, RAID, AHCI, chipset e outros drivers no CD de inicialização. Esses drivers possibilitam que o sistema operacional detecte e opere todos os dispositivos corretamente.

NOTA: Tenha em mente que o CD de inicialização vai conter automaticamente drivers do Windows 7PE de 32 bits.

Para injetar drivers em um CD de inicialização:

1. Baixe os drivers do site do fabricante para o servidor e descompacte-os.
2. Compacte a pasta que contém os drivers usando um utilitário de compactação, como, por exemplo, o WinZip.
3. Na caixa de diálogo **Create Boot CD** (Criar CD de inicialização), in no painel **Drivers**, clique em **Add a Driver** (Adicionar um driver).
4. Para localizar o arquivo de driver compactado, navegue pelo sistema de arquivamento. Selecione o arquivo e clique em **Open** (Abrir).

   Os drivers inseridos aparecem realçados no painel **Drivers**.

Criar o CD de inicialização

Para criar um CD de inicialização após você ter nomeado o CD de inicialização e especificado o caminho, criado uma conexão e, opcionalmente, injetado os drivers na tela **Create Boot CD** (Criar CD de inicialização), clique em **Create Boot CD** (Criar CD de inicialização). A imagem ISO é então criada.

Ver o andamento da criação de imagem ISO

Para ver o andamento da criação de imagem ISO, selecione a guia **Events** (Eventos) e, em seguida, em **Tasks** (Tarefas), você pode monitorar o andamento da criação da imagem ISO.

NOTA: Você também pode ver o andamento da criação da imagem ISO na caixa de diálogo **Monitor Active Task** (Monitorar tarefa ativa).

Quando a criação da imagem ISO estiver concluída, ela estará disponível na página **Boot CDs** (CDs de inicialização), acessível através do menu **Tools** (Ferramentas).

Acessar a imagem ISO

Para acessar a imagem ISO, navegue até o caminho de saída que você especificou, ou clique no link para baixar a imagem para um local no qual você possa então carregá-la no novo sistema. Por exemplo, na unidade de rede.

Carregar um CD de inicialização

Depois de criar a imagem do CD de inicialização, inicie o servidor de destino com o CD de inicialização recém-criado.

NOTA: Se você criou o CD de inicialização usando o DHCP; anote o endereço IP e a senha.

Para carregar um CD de inicialização:

1. Navegue até o novo servidor, carregar o CD de inicialização e depois inicie a máquina.
2. Especifique para **Boot from CD-ROM** (Inicializar do CD-ROM), que carrega o seguinte::
   - Windows 7 PE
   - Software do AppAssure Agent

   O console de recuperação universal do AppAssure inicia e mostra o endereço IP e a senha de autenticação da máquina.
3. Registre o endereço IP mostrado no painel Network Adapters Settings (Configurações de adaptadores de rede) e a autenticação e a senha mostradas no painel Authentication (Autenticação). Você vai usar essas informações posteriormente no processo de recuperação de dados para registrar de volta no console.
4. Se quiser alterar o endereço IP, selecione-o e clique em **Change** (Alterar).

   NOTA: Se você especificou um endereço IP na caixa de diálogo Create Boot CD (Criar CD de inicialização), o console de recuperação universal utiliza e o mostra na tela **Network Adapter settings** (Configurações de adaptador de rede).

Injetar drivers no servidor de destino

Se estiver restaurando para um hardware diferente, você precisa injetar os drivers de controlador de armazenamento, RAID, AHCI, chipset e se já não estiverem no CD de inicialização. Esses drivers possibilitam que o SO opere todos os dispositivos em seu servidor de destino corretamente.

Se não tiver certeza sobre quais drivers seu servidor de destino exige, clique na guia System Info (Informações de sistema) no console de recuperação universal. Essa guia mostra todos os tipos de dispositivos e hardware de sistema para o servidor de destino para o qual você deseja restaurar.

NOTA: Tenha em mente que seu servidor de destino contém automaticamente drivers do Windows 7PE de 32 bits.

Para injetar drivers no servidor de destino:

1. Baixe os drivers do site do fabricante para o servidor e descompacte-os.
2. Compacte a pasta que contém os drivers usando um utilitário de compactação de arquivos (por exemplo, o Winzip) e copie-a para o servidor de destino.
3. No console de recuperação universal, clique em **Driver Injection** (Injeção de driver).
4. Para localizar o arquivo de driver compactado, navegue pelo sistema de arquivamento e selecione o arquivo.
5. Se você clicou em **Driver Injection** (Injeção de driver) na etapa 3, clique em **Add Driver** (Adicionar driver). Se você clicou em **Load driver** (Carregar driver) na etapa 3, clique em **Open** (Abrir).

   Os drivers selecionados são injetados e serão carregados no sistema operacional após você reinicializar o servidor de destino.

Iniciar uma restauração a partir do núcleo

Para iniciar uma restauração a partir do núcleo:

1. Se os NICs em qualquer sistema que está sendo restaurado forem agrupados (ligados), remova todos exceto um dos cabos de rede.

   NOTA: A restauração do AppAssure não reconhece NICs agrupados. O processo não é capaz de resolver qual NIC usar se detectar mais de uma conexão ativa.
2. Navegue de volta para o servidor de núcleo e abra o Core Console.
3. Na guia **Machines** (Máquinas), selecione a máquina a partir da qual você deseja restaurar dados.
4. Clique no menu **Actions** (Ações) da máquina, clique em **Recovery Points** (Pontos de recuperação) para ver uma lista de todos os pontos de recuperação da máquina.
5. Amplie o ponto de recuperação a partir do qual você deseja restaurar e, em seguida, clique em **Rollback** (Reverter).
6. Na caixa de diálogo **Rollback** (Reverter), em Choose **Destination** (Escolher destino), selecione **Recovery Console Instance** (Instância de console de recuperação).
7. Nas caixas de texto **Host** e **Password** (Senha), digite o endereço IP e a senha de autenticação do novo servidor para o qual você deseja restaurar dados.

   NOTA: Os valores de host e senha são as credenciais que você registrou na tarefa anterior. Para obter mais informações, consulte Carregar um CD de inicialização.
8. Clique em **Load Volumes** (Carregar volumes) para carregar os volumes de destino para a nova máquina.

Mapear volumes

Você pode optar por mapear volumes para os discos no servidor de destino automática ou manualmente. Para o alinhamento automático de disco, o disco é apagado e reparticionado e todos os dados são apagados. O alinhamento é realizado na ordem em que os volumes estão listados e os volumes são alocados para os discos apropriadamente segundo o tamanho e assim por diante. Um disco pode ser usado por vários volumes. Se você mapear as unidades manualmente, você não pode usar o mesmo disco duas vezes.

Para o mapeamento manual, você precisa já ter formatado a nova máquina corretamente antes de restaurá-la.

Para mapear os volumes:

1. Para mapear volumes automaticamente, faça o seguinte:
   a. Na página **Disk Mapping** (Mapeamento de disco) do assistente **Restore Machine** (Restaurar máquina), selecione a guia **Automatically Map Volumes** (Mapear volumes automaticamente).
   b. Na área **Disk Mapping** (Mapeamento de disco), em **Source Volume** (Volume de origem), verifique se o volume de origem está selecionado e se os volumes apropriados estão não somente listados , mas também selecionados.
   c. Se o disco de destino que está mapeado automaticamente for o volume de destino correto, selecione a opção **Destination Disk** (Disco de destino).
   d. Clique em **Restore** (Restaurar) e depois prossiga para a etapa 3.
2. Para mapear volumes manualmente, faça o seguinte:
   a. Na página **Disk Mapping** (Mapeamento de disco) do assistente **Restore Machine** (Restaurar máquina), selecione a guia **Manually Map Volumes** (Mapear volumes manualmente).
   b. Na área **Volume Mapping** (Mapeamento de volume), em **Source Volume** (Volume de origem), verifique se o volume de origem está selecionado e se os volumes apropriados estão não somente listados , mas também selecionados.

c. Em **Destination** (Destino), no menu suspenso, selecione o destino correto que é o volume de destino para realizar a restauração do ponto de recuperação sem sistema operacional e depois clique em **Rollback** (Reverter).

3. Na caixa de diálogo de confirmação **RollbackURC** (Reverter URC), confira o mapeamento de origem do ponto de recuperação e o volume de destino da reversão. Para realizar a reversão, clique em **Restore** (Restaurar).

   CUIDADO: Se você selecionar Begin Rollback (Iniciar reversão), todas as partições e dados atuais na unidade de destino serão removidos permanentemente e substituídos pelo conteúdo do ponto de recuperação selecionado, incluindo o sistema operacional e todos os dados.

Ver o andamento da recuperação

Para ver o andamento da recuperação:

1. Após iniciar o processo de reversão, a caixa de diálogo **Active Task** (Tarefa ativa) é mostrada, indicando que a ação de reversão foi iniciada.

   NOTA: Esta aparência da caixa de diálogo **Active Task** (Tarefa ativa) não indica a conclusão bem-sucedida da tarefa.

2. Opcionalmente, para monitorar o andamento da tarefa de reversão, na caixa de diálogo Active Task (Tarefa ativa), clique em **Open Monitor** (Abrir monitor). Você pode ver o andamento da recuperação, além dos horários inicial e final, através da janela **Monitor Open Task** (Monitorar tarefa em aberto).

   NOTA: Para retornar aos pontos de recuperação para a máquina de origem a partir da caixa de diálogo **Active Task** (Tarefa ativa), clique em **Close** (Fechar).

Iniciar o servidor de destino restaurado

Para iniciar o servidor de destino restaurado:

1. Navegue de volta ao servidor de destino e, na interface **AppAssure Universal Recovery Console** (Console de recuperação universal do AppAssure), clique em **Reboot** (Reinicializar) para iniciar a máquina.
2. Especifique para iniciar o Windows normalmente.
3. Faça login na máquina.

   O sistema é restaurado para seu estado antes da restauração sem sistema operacional.

Reparar problemas de inicialização

Tenha em mente que, você tiver restaurado para um hardware diferente, você precisa ter injetado os drivers de controlador de armazenamento, RAID, AHCI, chipset e outros se já não estiverem no CD de inicialização. Esses drivers possibilitam que o SO opere todos os dispositivos em seu servidor de destino corretamente.

Para reparar problemas de inicialização:

1. Se você passar por problemas ao iniciar o servidor de destino restaurado, abra o console de recuperação universal recarregando o CD de inicialização.
2. No console de recuperação universal, clique em **Driver Injection** (Injeção de driver).
3. Na caixa de diálogo Driver Injection (Injeção de driver), clique em **Reparar Boot Problems** (Problemas de inicialização).

   Os parâmetros de inicialização no registro de inicialização de servidor de destino são reparados automaticamente.
4. No console de recuperação universal, clique em **Reboot** (Reinicializar).

Iniciar uma restauração sem sistema operacional para uma máquina Linux

O DL1000 pode realizar uma restauração sem sistema operacional (BMR) em uma máquina Linux, incluindo uma reversão do volume do sistema. Usando o utilitário de linha de comando do AppAssure `aamount`, reverta para a imagem de base do volume de inicialização. Antes de poder realizar uma BMR em uma máquina Linux, você precisa fazer o seguinte:

- Obtenha um arquivo do CD Live para BMR com o suporte do AppAssure, o qual inclui uma versão inicialização do Linux.

  NOTA: Você também pode baixar o CD Live para Linux no portal de licenças na página **https://licenseportal.com**.
- Certifique-se de que haja espaço suficiente no disco rígido para criar partições de destino na máquina de destino que vai conter os volumes de origem. Qualquer partição de destino deve no mínimo ter a mesma capacidade da partição de origem.
- Identifique o caminho da reversão, que é o caminho do descritor do arquivo do dispositivo. Para identificar o caminho do descritor do arquivo do dispositivo, use o comando `fdisk` em uma janela do terminal.

  NOTA: Antes de começar a usar os comandos do AppAssure, você pode instalar o utilitário Tela. O utilitário permite que você role a tela para ver uma quantidade maior de dados, como uma lista de pontos de recuperação.

Para iniciar uma restauração sem sistema operacional para uma máquina Linux:

1. Usando o CD Live que você recebeu do AppAssure, inicialize a máquina Linux e abra uma janela de terminal.
2. Caso seja necessário, crie uma nova partição de disco (por exemplo, ao executar o comando `fdisk` como raiz) e torne essa partição inicializável ao usar o comando `a`.
3. Execute o utilitário AppAssure `aamount` como raiz, por exemplo:

   ```
   sudo aamount
   ```
4. No prompt de montagem do AppAssure, digite o comando a seguir para listar as máquinas protegidas:

   ```
   lm
   ```
5. Quando solicitado, digite o endereço IP ou nome do host do servidor do AppAssure Core.
6. Digite as credenciais de login, ou seja, o nome de usuário e a senha, desse servidor.

   Uma lista mostra as máquinas protegidas por esse servidor do AppAssure Core. Ela mostra as máquinas encontradas por número de item de linha, endereço de host/IP e um número de identificação para a máquina (por exemplo: `293cc667-44b4-48ab-91d8-44bc74252a4f`).
7. Para listar os pontos de recuperação atualmente montados para a máquina que você deseja restaurar, digite o comando a seguir:

   ```
   lr <machine_line_item_number>
   ```

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

   É mostrada uma lista que indica os pontos de recuperação incrementais e de base para a máquina. Essa lista inclui um número de item de linha, carimbo de data/hora, local do volume, tamanho do ponto de recuperação e um número de identificação para o volume que inclui um número de sequência no final(por exemplo, "`293cc667-44b4-48ab-91d8-44bc74252a4f:2`"), o qual identifica o ponto de recuperação.

8. Para selecionar um ponto de recuperação de imagem de base para reversão, digite o comando a seguir:

   `r <volume_base_image_recovery_point_ID_number> <path>`

   CUIDADO: Você precisa garantir que o volume do sistema não esteja montado.

   Esse número reverte a imagem do volume especificada pela ID do núcleo ao caminho especificado. O caminho para a reversão é o caminho para o descritor do arquivo do dispositivo e não é o diretório ao qual ele está montado.

   NOTA: Você também pode especificar um número de linha no comando, em vez do número de ID de ponto de recuperação para identificar o ponto de recuperação. Use o número de linha de agente/máquina (do comando lm), seguido do número de linha de ponto de recuperação e letra do volume, seguidos pelo caminho, como, **r <machine_line_item_number> <base_image_recovery_point_line_number> <volume_letter> <path>**. Nesse comando, `<path>` é o descritor de arquivo para o volume real.

9. Quando solicitado para continuar, digite `y` (yes) para indicar Sim.

   Após a reversão, uma série de mensagens é mostrada para notificar você sobre o status.

10. Após a reversão correta, caso seja necessário, atualize o registro de inicialização principal com o carregador de inicialização restaurado.

    NOTA: Reparar ou configurar o carregador de inicialização só é necessário se esse disco for novo. Se essa é uma simples reversão para o mesmo disco, não é necessário configurar o carregador de inicialização.

    CUIDADO: Não desmonte um volume Linux protegido manualmente. Caso você precise desmontar manualmente um volume Linux protegido, você precisa executar o seguinte comando antes de desmontar o volume: bsctl -d <caminho para o volume>

    Nesse comando, o`<path to volume>` não se refere ao ponto de montagem do volume, mas sim ao descritor de arquivo do volume; ele deve estar no mesmo formato desse exemplo: **/dev/sda1**.

Instalar o utilitário Tela

Antes de começar a usar os comandos do AppAssure, você pode instalar o utilitário Tela. O utilitário permite que você role a tela para ver uma quantidade maior de dados, como uma lista de pontos de recuperação.

Para instalar o utilitário Tela:

1. Usando o arquivo do CD Live, inicie a máquina Linux.

   Uma janela de terminal é mostrada.

2. Digite o seguinte comando: `sudo apt-get install screen`.
3. Para iniciar o utilitário Tela, digite `screen` no prompt de comando.

Criar partições inicializáveis em uma máquina Linux

Para criar partições inicializáveis em uma máquina Linux usando a linha de comando:

1. Anexe todos os dispositivos usando o utilitário **bsctl** com o seguinte comando como raiz: `sudo bsctl --attach-to-device /dev/<restored volume>`

   NOTA: Repita essa etapa para cada volume restaurado.

2. Monte cada volume restaurado usando os seguintes comandos:

```
mount /dev/<restored volume> /mnt

mount /dev/<restored volume> /mnt
```

NOTA: Algumas configurações do sistema podem incluir o diretório de inicialização como parte do volume raiz.

3. Monte metadados de instantâneo para cada volume restaurado usando os seguintes comandos:

```
sudo bsctl --reset-bitmap-store /dev/<restored volume>

sudo bsctl --reset-bitmap-store /dev/<restored volume>
```

4. Verifique se o identificador universal único (UUID) contém os novos volumes usando os comandos `blkid` ou `ll /dev/disk/by-uuid`.
5. Verifique se `/etc/fstab` contém os UUIDs corretos dos volumes de inicialização e rais.
6. Instale o carregador de inicialização GRUB usando os seguintes comandos:

```
mount --bind /dev/ /mnt/dev

mount --bind /proc/ /mnt/proc

chroot/mnt/bin/bash

grub-install/dev/sda
```

7. Verifique se o arquivo **/boot/grub/grub .conf**o arquivo o UUID correto para o volume raiz ou atualize-o conforme necessário usando um editor de texto.
8. Remova o CD Live da unidade de CD-ROM e reinicie a máquina Linux.

5

Replicar pontos de recuperação

Replicação

A replicação é o processo de copiar pontos de recuperação e transmiti-los para um local secundário para fins de recuperação de desastre. O processo exige uma relação emparelhada de origem-destino entre dois núcleos. A replicação é gerenciada de acordo com cada máquina protegida; isso significa que instantâneos de backup de uma máquina protegida são replicados para o núcleo de replicação de destino. Quando a replicação é configurada, o núcleo de origem transmite, de forma assíncrona e contínua, os dados de instantâneo incremental para o núcleo de destino. Você pode configurar essa replicação de saída para o centro de dados de sua empresa ou para uma unidade de recuperação de desastres remota (isso é, um núcleo de destino "autogerenciado") ou para um provedor de serviços gerenciados (MSP) que ofereça serviços de recuperação de desastres e backup externos. Ao replicar para um MSP, você pode usar os fluxos de trabalho incorporados que permitem que você solicite conexões e receba notificações de feedback automáticas.

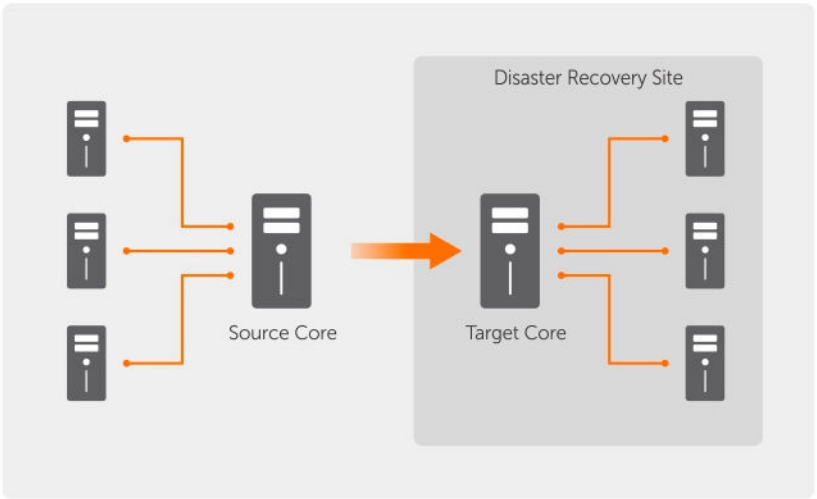

Figura 5. Arquitetura básica de replicação

A replicação começa com a propagação: a transferência inicial de imagens de base sem duplicações e instantâneos incrementais dos agentes protegidos, que podem chegar a centenas de milhares de gigabytes de dados. A replicação inicial pode ser propagada para o núcleo de destino usando uma mídia externa. Isso normalmente é útil para grandes conjuntos de dados ou unidades com conexões lentas. Os dados no arquivo de propagação são compactados, criptografados e as duplicações são eliminadas. Se o tamanho total do arquivo for superior ao espaço disponível na mídia removível, o arquivo pode ocupar diversos dispositivos com base no espaço disponível na mídia. Durante o processo de propagação, os pontos de recuperação incremental são replicados à unidade de destino. Após o núcleo de destino

consumir o arquivo de propagação, os pontos de recuperação incremental recém-replicados são sincronizados automaticamente.

Roteiro para executar a replicação

Para replicar dados usando o AppAssure, você precisa configurar os núcleos de origem e destino para replicação. Depois de configurar a replicação, você pode replicar os dados da máquina protegida, monitorar e gerenciar a replicação e realizar a recuperação.

A replicação no AppAssure envolve as seguintes operações:

- Configurar a replicação autogerenciada. Para obter mais informações sobre como replicar em um núcleo de destino autogerenciado, consulte Replicar em um núcleo autogerenciado.
- Configurar a replicação terceirizada. Para obter mais informações sobre como replicar em um núcleo de destino terceirizado, consulte Replicar em um núcleo gerenciado por um terceiro.
- Replicar em uma nova máquina protegida anexada ao núcleo de origem. Para obter mais informações sobre como replicar uma máquina protegida, consulte Replicar uma nova máquina protegida.
- Replicar em uma máquina protegida atual. Para obter mais informações sobre como configurar um agente para replicação, consulte Replicar dados de agente em uma máquina.
- Definir a prioridade de replicação para um agente. Para obter mais informações sobre como priorizar a replicação dos agentes, consulte Definir a prioridade de replicação para um agente.
- Monitorar a replicação conforme for necessário. Para obter mais informações sobre como monitorar a replicação, consulte Monitorar a replicação.
- Gerenciar configurações de replicação conforme necessário. Para obter mais informações sobre como gerenciar configurações de replicação, consulte Gerenciar configurações de replicação.
- Recuperar dados replicados no caso de desastre ou perda de dados. Para obter mais informações sobre como recuperar dados replicados, consulte Recuperar dados replicados.

Replicação para um núcleo autogerenciado

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

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

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

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

1. No núcleo, clique na guia **Replication** (Replicação).
2. Clique em **Add Target Core** (Adicionar núcleo de destino).

   O assistente **Replication** (Replicação) é mostrado.
3. Selecione **I have my own Target Core** (Tenho meu próprio núcleo de destino) e, em seguida, digite as informações conforme descrito na tabela a seguir.

Caixa de texto	Descrição
Host Name (Nome de host)	Digite o nome do host ou o endereço IP da máquina de núcleo à qual você está replicando.
Port (Porta)	Digite o número da porta na qual o AppAssure Core se comunica com a máquina. O número de porta padrão é 8006.
User Name (Nome de usuário)	Digite o nome do usuário para acessar a máquina. Por exemplo, **Administrador**.
Password (Senha)	Digite a senha para acessar a máquina.

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

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

4. Clique em **Next** (Avançar).
5. Na página **Details** (Detalhes), digite um nome para essa configuração de replicação; por exemplo, NucleoOrigem1. Se você estiver reiniciando ou reparando uma configuração de replicação anterior, selecione a replicação **My Core has been migrated and I would like to repair** (Meu núcleo foi migrado e eu gostaria de reparar)
6. Clique em **Next** (Avançar).
7. Na página **Agents** (Agentes), selecione os agentes que você deseja replicar e, em seguida, use as listas suspensas na coluna **Repository** (Repositório) para selecionar um repositório para cada agente.
8. Se você planeja executar o processo de propagação para a transferência de dados da base, execute as seguintes etapas:

   NOTA: Devido às enormes quantidades de dados que precisam ser copiadas para o dispositivo de armazenamento portátil,é recomendado uma conexão eSATA, USB 3.0 ou outra conexão de alta velocidade ao dispositivo portátil de armazenamento.

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

9. Na caixa de diálogo **Seed Drive Option** (Opção de unidade de propagação), digite as informações descritas abaixo:

Caixa de texto	Descrição
Maximum Size (Tamanho máximo)	Arquivos de dados grandes podem ser divididos em múltiplos segmentos. Selecione o tamanho máximo do segmento que você deseja reservar para criar a unidade de propagação executando uma das opções a seguir: • Selecione **Entire Target** (Todo o destino) para reservar todo o espaço disponível no caminho fornecido na página de local de unidade de propagação para uso futuro (por exemplo, se o local for D:\trabalho \arquivo, todo o espaço disponível na unidade D: é reservado caso seja necessário para copiar a unidade de propagação, mas não é reservado imediatamente após iniciar o processo de cópia). • Selecione a caixa de texto em branco, digite o valor e, em seguida, selecione uma unidade de medida na lista suspensa para personalizar o espaço máximo que você deseja reservar.
Customer ID (ID de cliente) (opcional)	Opcionalmente, digite a ID de cliente que foi atribuída a você pelo prestador de serviços.
Recycle action (Ação de reciclagem)	Caso o caminho já contenha uma unidade de propagação, selecione uma das opções a seguir: • **Do not reuse** (Não reutilizar) - Não substitui nem apaga os dados existentes do local. Se o local não estiver vazio, agravação da unidade de propagação falha. • **Replace this core** (Substituir esse núcleo) - Substitui quaisquer dados pré-existentes que pertençam a esse núcleo, mas deixa os dados de outros núcleos intactos. • **Erase completely** (Apagar completamente) - Apaga todos os dados do diretório antes de gravar na unidade de propagação.
Comment (Comentário)	Digite um comentário ou descrição do arquivo.
Adicionar todos os agentes à unidade de propagação	Selecione os agentes que você deseja replicar usando a unidade de propagação.
Build RP chains (fix orphans) (Construir cadeias de ponto de recuperação (corrigir órfãos))	Selecione esta opção para replicar toda cadeia de ponto de recuperação para a unidade de propagação. Essa opção é selecionada por padrão. A propagação típica no AppAssure replica apenas o ponto de recuperação mais recente para a unidade de propagação, reduzindo a quantidade de tempo e espaço necessária para criara unidade de propagação. Optar por desenvolver cadeias de ponto de recuperação (RP) para a unidade de propagação exige espaço suficiente na unidade de propagação para armazenar os pontos de recuperação mais recentes dos agentes especificados e pode levar tempo adicional para concluir a tarefa.
Use compatible format (Usar	Selecione esta opção para criar a unidade de propagação em um formato que é compatível com as versões novas e mais antigas do AppAssure Core.

Caixa de texto	Descrição
formato compatível)	

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

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

Consumir a unidade de propagação em um núcleo de destino

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

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

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

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

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

   Depois de o núcleo verificar o arquivo, ele preenche automaticamente a opção **Date Range** (Intervalo de datas) com as datas dos pontos de recuperação mais antigos e mais recentes contidos

na unidade de propagação. Ele também importa quaisquer comentários inseridos ao configurar a replicação para um núcleo autogerenciado.

7. Em **Agent Names** (Nomes de agente) na janela **Consume** (Consumir), selecione as máquinas para as quais você deseja consumir dados e depois clique em **Consume** (Consumir).

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

Abandonar uma unidade de propagação pendente

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

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

Para abandonar uma unidade de propagação pendente:

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

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

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

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

Replicar para um núcleo gerenciado por terceiros

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

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

Replicar um novo agente

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

Para replicar um novo agente:

1. Navegue até o Core Console e clique na guia **Machines** (Máquinas).
2. No menu suspenso **Actions** (Ações), clique em **Protect Machine** (Proteger máquina).

3. Na caixa de diálogo **Protect Machine** (Proteger máquina), digite as informações conforme descrito na tabela a seguir.

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

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

Caixa de texto	Descrição
Display Name (Nome de exibição)	Digite um nome para a máquina a ser mostrado no Core Console.
Repository (Repositório)	Selecione o repositório no AppAssure Core onde os dados dessa máquina são armazenados.
Encryption Key (Chave de criptografia)	Especifique se a criptografia é aplicada aos dados para cada volume nessa máquina armazenado no repositório. NOTA: As configurações de criptografia para um repositório são definidas na guia **Configuration** (Configuração) no Core Console.
Remote Core (Núcleo remoto)	Especifique o núcleo de destino ao qual você deseja replicar o agente.
Remote Repository (Repositório remoto)	O nome do repositório desejado no núcleo de destino no qual serão armazenados os dados replicados dessa máquina.
Pause (Pausar)	Marque essa caixa de seleção se você deseja pausar a replicação; por exemplo, para pausá-la até depois que o AppAssure salvar uma imagem de base do novo agente.
Programação	Selecione uma das seguintes opções: • Proteger todos os volumes com o cronograma padrão • Proteger volumes específicos com o cronograma personalizado NOTA: O cronograma padrão é a cada 15 minutos.
Initially pause protection (Pausar proteção inicialmente)	Marque essa caixa de seleção se você deseja pausar a proteção; por exemplo, para evitar que o AppAssure salve a imagem de base até depois dos horários de pico de uso.

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

Replicar dados do agente em uma máquina

A replicação é a relação entre os núcleos de origem e destino na mesma unidade, ou entre duas unidades com conexão lenta por cada agente. Quando a replicação é configurada entre dois núcleos, o núcleo de origem transmite de forma assíncrona os dados de instantâneo incremental dos agentes selecionados para o núcleo de destino ou de origem. A replicação de saída pode ser configurada para um provedor de serviços gerenciados que ofereça serviço de recuperação de desastres e backup externo ou para um núcleo autogerenciado. Para replicar dados de agente em uma máquina:

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

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

Configurar a prioridade de replicação para um agente

Para configurar a prioridade de replicação para um agente:

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

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

Monitorar a replicação

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

Para monitorar a replicação:

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

Tabela 4. Monitorar a replicação

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

Section (Seção)	Descrição	Ações disponíveis
	núcleo remoto, estado, máquinas e andamento.	cliente, endereço de e-mail e comentários para o núcleo replicado. • **Consume** (Consumir) — Consome os dados iniciais da unidade de propagação e os salva no repositório local.

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

Gerenciar configurações de replicação

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

Para gerenciar as configurações de replicação:

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

Opção	Descrição
Cache lifetime (Vida útil do cache)	Especifique a quantidade de tempo entre cada solicitação de status de núcleo de destino feita pelo núcleo de origem.
Volume image session timeout (Tempo limite de imagem de volume)	Especifique a quantidade de tempo que o núcleo de origem gasta tentando transferir uma imagem de volume para o núcleo de destino.
Max. concurrent replication jobs (Número máximo de trabalhos de replicação simultâneos)	Especifique o número permitido de máquinas protegidas para replicar para o núcleo de destino por vez.
Max. parallel streams (Número máximo de fluxos paralelos)	Especifique o número permitido de conexões de rede a serem usadas por uma única máquina protegida para replicar os dados da máquina por vez.

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

Remover a replicação

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

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

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

Remover uma máquina protegida de replicação do núcleo de origem

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

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

Remover uma máquina protegida no núcleo de destino

Para remover uma máquina protegida no núcleo de destino:

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

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

Remover um núcleo de destino da replicação

Para remover um núcleo de destino da replicação:

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

Remover um núcleo de origem da replicação

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

Para remover um núcleo de origem da replicação:

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

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

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

Recuperar dados replicados

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

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

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

- Montar pontos de recuperação.
- Reverter para pontos de recuperação.
- Realizar uma exportação de máquina virtual (MV).
- Executar uma restauração sem sistema operacional (BMR).
- Executar o failback (caso você tenha um ambiente de failover/failback de replicação configurado).

Entender failover e failback

O AppAssure oferece suporte para failover e failback em ambientes replicados, no caso de uma interrupção grave na qual agentes e núcleo de origem falhem. O termo failover refere-se a alternar para um destino redundante ou em espera (AppAssure Core) após uma falha do sistema ou terminação anormal de um núcleo de origem e agentes associados. A meta principal do failover é iniciar um novo agente idêntico ao agente que falhou. A meta secundária é alternar o núcleo de destino para um novo modo para que o núcleo de destino proteja o agente de failover da mesma maneira que o núcleo de origem protegeu o agente inicial antes da falha. O núcleo de destino pode recuperar instâncias de agentes replicados e dar início imediato à proteção nas máquinas que passaram por failover.

Failback é o processo de restaurar um agente e um núcleo de volta aos seus estados originais (antes da falha). O objetivo principal do failback é restaurar um agente (na maioria dos casos, essa é uma nova máquina que substitui um agente que falhou) para um estado idêntico ao último do agente novo e temporário. Quando restaurado, ele é protegido por um núcleo de origem restaurado. A replicação também é restaurada e o núcleo de destino age como um destino de replicação novamente.

Executar failover

Ao se deparar com uma situação de desastre na qual seu núcleo de origem e agentes associados falharam, você pode ativar o failover no AppAssure para alternar a proteção para seu núcleo de failover (destino) idêntico. O núcleo de destino se torna o único núcleo a proteger os dados em seu ambiente e você então inicia um novo agente para substituir temporariamente o agente que falhou.

Para realizar o failover no núcleo de destino:

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

   A caixa de diálogo **Fail Over** é mostrada e lista as próximas etapas necessárias para concluir um failover.
4. Clique em **Continue** (Continuar).
5. Na área de navegação esquerda, abaixo de **Protected Machines** (Máquinas protegidas), selecione a máquina que possui o software do AppAssure Agent associado aos pontos de recuperação.
6. Exporte as informações de ponto de recuperação de backup nesse agente para uma máquina virtual.
7. Exporte as informações de ponto de recuperação de backup nesse agente para uma máquina virtual.
8. Inicie a máquina virtual que agora inclui as informações de backup exportadas.

   Você precisa aguardar até que o software do driver de dispositivo seja instalado.
9. Reinicie a máquina virtual e aguarde até o serviço de agente iniciar.
10. Volte ao núcleo do Core Console de destino e verifique se o novo agente é mostrado em **Protected Machines** (Máquinas protegidas) e na guia **Replication** (Replicação) em **Incoming Replication** (Replicação de entrada).
11. Force múltiplos instantâneos e verifique se eles são concluídos corretamente.

    Para obter mais informações consulte Forçar um instantâneo.
12. Você agora pode prosseguir com a realização do failback.

    Para obter mais informações consulte Realizar failback.

Executar failback

Depois que você reparar ou trocar os agentes e o núcleo de origem originais que apresentaram falhas, você precisa transferir os dados de suas máquinas com failover para restaurar as máquinas de origem.

Para executar o failback:

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

   A caixa de diálogo **Fail Back** (Failback) é mostrada para descrever as etapas que você precisa seguir antes de clicar no botão **Continue** (Continuar) para concluir o failback.
4. Clique em **Cancel** (Cancelar).
5. Se a máquina que passou por failover estiver executando um servidor Microsoft SQL ou Microsoft Exchange, pare esses serviços.
6. Force um instantâneo da máquina. Para obter mais informações, consulte Forcing a Snapshot (Forçar um instantâneo).

7. Desligue a máquina que passou por failover.
8. Crie um arquivo do agente que passou por failover e salve-o no disco ou em um local de compartilhamento de rede.

   Para obter mais informações sobre como criar arquivos, consulte Creating An Archive (Criar um arquivo).
9. Depois de criar o arquivo, navegue até o Core Console no núcleo de origem recém-reparado e clique na guia **Tools** (Ferramentas).
10. Importe o arquivo que você acabou de criar na etapa 8.

    Para obter mais informações consulte Importing An Archive (Importar um arquivo).
11. Volte ao Core Console no núcleo de destino e clique na guia **Replication** (Replicação).
12. Em **Incoming Replication** (Replicação de entrada), selecione o agente de failover e expanda os detalhes.
13. Na caixa de diálogo **Failback** (Failback), clique em **Continue** (Continuar).
14. Desligue a máquina que contém o agente exportado que foi criado durante o failover.
15. Realize uma BMR (Bare Metal Restore, restauração sem sistema operacional) para o agente e o núcleo de origem.

    NOTA: Ao iniciar a restauração, você precisa usar os pontos de recuperação que foram importados do núcleo de destino para o agente na máquina virtual.
16. Aguarde pela reinicialização da BMR e o serviço de agente ser reiniciado; depois, veja e registre os detalhes de rede da máquina.
17. Navegue até o Core Console no núcleo de origem e, na guia **Machines** (Máquinas), modifique as configurações de proteção da máquina para adicionar os detalhes da nova conexão de rede.

    Para obter mais informações, consulte Configuring Machine Settings (Definir configurações da máquina).
18. Navegue até o Core Console no núcleo de destino e apague o agente da guia **Replication** (Replicação).
19. No Core Console do núcleo de origem, configure a replicação novamente entre a origem e o destino clicando na guia **Replication** (Replicação) e depois adicione o núcleo de destino para replicação.

6

Relatório

Sobre os relatórios

O dispositivo DL permite que você gere e veja a informações de conformidade, erro e dados resumidos de múltiplas máquinas agente e núcleos.

Você pode optar por ver os relatórios on-line, imprimir relatórios ou exportar e salvá-los em um dos diversos formatos compatíveis. Os formatos à sua escolha são:

- PDF
- XLS
- XLSX
- RTF
- MHT
- HTML
- TXT
- CSV
- Imagem

Sobre a barra de ferramentas de relatórios

A barra de ferramentas disponível para todos os relatórios permite que você imprima e salve de duas formas diferentes. A tabela a seguir descreve as opções para imprimir e salvar.

Ícone	Descrição
	Imprimir o relatório
	Imprimir a página atual
	Exportar um relatório e salvá-lo no disco
	Exportar um relatório e mostrá-lo em uma nova janela Use esta opção para copiar, colar e enviar por e-mail a URL para que outros vejam o relatório em um navegador da Web.

Sobre relatórios de conformidade

Relatórios de conformidade estão disponíveis para o núcleo e o AppAssure Agent. Eles fornecem a você uma maneira de ver o status dos trabalhos executados por um determinado núcleo ou agente. Trabalhos com falhas são mostrados com texto vermelho. Informações no relatório de conformidade do núcleo que não estejam associados a um agente aparecem em branco.

Detalhes sobre os trabalhos são apresentados em um visualização de coluna que inclui as seguintes categorias:

- Núcleo
- Agente protegido
- Tipo
- Resumo
- Status
- Erro
- Horário de início
- Horário de término
- Horário
- Trabalho total

Sobre relatórios de erros

Relatórios de erros são subconjuntos de relatórios de conformidade e estão disponíveis para núcleos e agentes AppAssure. Os relatórios de erros incluem apenas os trabalhos que falharam e que estão listados nos relatórios de conformidade e os compilam em um único relatório que pode ser impresso e exportado.

Detalhes sobre erros são apresentados em um visualização de coluna com as seguintes categorias:

- Núcleo
- Agente
- Tipo
- Resumo
- Erro
- Horário de início
- Horário de término
- Tempo decorrido
- Trabalho total

.

Sobre o relatório resumido de núcleo

O **Relatório resumido de núcleo** inclui informações sobre os repositórios no núcleo selecionado e sobre os agentes protegidos por esse núcleo. A informação é mostrada como dois resumos dentro de um único relatório.

Resumo de repositórios

A parte **Repositories** (Repositórios) do **relatório resumido de núcleo** inclui dados dos repositórios situados no núcleo selecionado. Detalhes sobre os repositórios são apresentados em uma visualização de coluna com as seguintes categorias:

- Nome
- Caminho de dados

- Caminho de metadados
- Espaço alocado
- Espaço usado
- Espaço livre
- Razão de compressão/desduplicação

Resumo de agentes

A parte **Agents** (Agentes) do **relatório resumido de núcleo** inclui dados para todos os agentes protegidos pelo núcleo selecionado.

Mais detalhes sobre os agentes são apresentados em uma visualização de coluna com as seguintes categorias:

- Nome
- Volumes protegidos
- Espaço total protegido
- Espaço protegido atual
- Taxa de mudança por dia (**média**, **mediana**)
- Estatísticas de trabalho (**aprovados**, **reprovados**, **cancelados**)

Gerar relatório para um núcleo ou agente

Para gerar relatório para um núcleo ou agente:

1. Navegue até o Core Console e selecione o núcleo ou o agente para o qual você deseja executar o relatório.
2. Clique na guia **Tools** (Ferramentas).
3. Na guia **Tools** (Ferramentas), amplie a seção **Reports** (Relatórios) na área de navegação esquerda.
4. Na área de navegação esquerda, selecione o relatório que você deseja executar. Os relatórios disponíveis dependem da seleção feita na etapa 1 e são descritos abaixo.

Máquina	Relatórios disponíveis
Núcleo	Relatório de conformidade Relatório resumido Relatório de erros
Agente	Relatório de conformidade Relatório de erros

5. No calendário suspenso **Start Time** (Horário inicial), selecione uma data inicial e depois digite um horário inicial para o relatório.

   NOTA: Não há dados disponíveis antes de quando o núcleo ou o agente foram implantados.
6. No calendário suspenso **End Time** (Horário final), selecione uma data final e depois digite um horário final para o relatório.
7. Na opção **Core Summary Report** (Relatório resumido), marque a caixa de seleção **All Time** (Todo o tempo) se você quiser que **horário inicial** e **horário final** englobem a vida útil do núcleo..

8. Para os relatórios **Core Compliance Report** (Relatório de conformidade de núcleo), ou **Core Errors Report** (Relatório de erros de núcleo), use a lista suspensa **Target Cores** (Núcleos de destino) para selecionar o núcleo do qual você deseja ver os dados.
9. Clique em **Generate Report** (Gerar relatório).

   Depois do relatório ser gerado, você pode usar a barra de ferramentas para imprimir ou exportar o relatório.

Sobre os relatórios de núcleo de console de gestão central

O dispositivo DL permite que você gere e veja informações de conformidade, erro e dados resumidos de vários núcleos. Detalhes sobre os núcleos são apresentados em visualizações de coluna com as mesmas categorias descritas nessa seção.

Gerar um relatório a partir do console de gestão central

Para gerar um relatório a partir do console de gestão central:

1. Na tela **Central Management Console Welcome** (Bem-vindo ao console de gestão central), clique no menu suspenso no canto superior direito.
2. No menu suspenso, clique em **Reports** (Relatórios) e depois selecione uma das opções a seguir:
   - **Relatório de conformidade**
   - **Relatório resumido**
   - **Relatório de falhas**
3. Na área de navegação esquerda, selecione os núcleos para os quais você deseja executar o relatório.
4. No calendário suspenso **Start Time** (Horário inicial), selecione uma data inicial e depois digite um horário inicial para o relatório.

   NOTA: Não há dados disponíveis antes de quando os núcleos foram implantados.
5. No calendário suspenso **End Time** (Horário final), selecione uma data final e depois digite um horário final para o relatório.
6. Clique em **Generate Report** (Gerar relatório).

   Depois do relatório ser gerado, você pode usar a barra de ferramentas para imprimir ou exportar o relatório.

7

Obter ajuda

Encontrar a documentação e as atualizações de software

Links diretos para a documentação e atualizações de software do AppAssure e do dispositivo DL1000 estão disponíveis no Core Console.

Documentação

Para acessar o link da documentação:

1. No Core Console, clique na guia **Appliance** (Dispositivo).
2. No painel esquerdo, navegue até o link **Appliance (Dispositivo)** → **Documentation (Documentação)**.

Atualizações de software

Para acessar o link Atualizações de software:

1. No Core Console, clique na guia **Appliance** (Dispositivo).
2. No painel esquerdo, navegue até o link **Appliance (Dispositivo)** → **Software Updates (Atualizações de software)**.

Entrar em contato com a Dell

A Dell fornece várias opções de suporte e atendimento on-line ou por telefone. Se não tiver uma conexão de Internet ativa, você pode encontrar as informações de contato na sua fatura de compra, nota de expedição, nota fiscal ou catálogo de produtos Dell. A disponibilidade varia de acordo com o país e o produto, e alguns serviços podem não estar disponíveis na sua região.

Para entrar em contato com a Dell para tratar de assuntos de vendas, suporte técnico ou questões de atendimento ao cliente, visite **software.dell.com/support**.

Feedback sobre a documentação

Clique no link **Feedback** em qualquer uma das páginas de documentação da Dell, preencha o formulário e clique em **Submit** (Enviar) para enviar seu feedback.