




Dispositivo Dell DL4300

Guia de implementação



Notas, avisos e advertências

-  **NOTA:** Uma NOTA indica informações importantes que ajudam você a usar melhor os recursos do computador.
-  **CUIDADO:** Um AVISO indica possíveis danos ao hardware ou perda de dados e ensina como evitar o problema.
-  **ATENÇÃO:** Uma ADVERTÊNCIA indica possíveis danos à propriedade, risco de lesões corporais ou mesmo risco de vida.

© 2016 Dell Inc. Todos os direitos reservados. Este produto é protegido por leis de copyright e de propriedade intelectual dos EUA e internacionais. Dell e o logotipo Dell são marcas comerciais da Dell Inc. nos Estados Unidos e/ou em outras jurisdições. Todas as outras marcas e os nomes aqui mencionados podem ser marcas comerciais de suas respectivas empresas.

2016 - 05

Rev. A02

Índice

1 Configurar o dispositivo DL4300.....	5
Introdução.....	5
Termos usados neste documento.....	5
Configurações disponíveis.....	5
Pré-requisitos de instalação.....	6
Requisitos de rede.....	6
Infraestrutura de rede recomendada.....	6
Configurar o hardware.....	6
Instalar o dispositivo em um rack.....	7
Configurar o comutador de configuração do gabinete de armazenamento.....	7
Conectar o gabinete de armazenamento ao sistema.....	7
Conectar o braço de gerenciamento de cabos (opcional).....	9
Cabeamento do dispositivo.....	9
Ligar o dispositivo.....	9
Configurações de disco do DL4300.....	9
2 Configuração inicial do software.....	11
Assistente de configuração de dispositivo do AppAssure.....	11
Configurar a interface de rede.....	12
Definir o nome de host e as configurações de domínio.....	13
Definir as configurações do SNMP.....	13
Criar discos virtuais RASR e Windows.....	14
Utilitário de recuperação e atualização.....	15
Recuperação automática rápida do dispositivo.....	15
Criar o pen drive USB RASR.....	16
Executar a RASR.....	16
Executar a RASR através do módulo SD duplo interno.....	17
Provisionar o armazenamento.....	17
Provisionar o armazenamento selecionado.....	19
Configurar o DL4300 usando armazenamento Fibre Channel (opcional).....	20
3 Tarefas pós-instalação.....	21
Acessar o Core Console.....	21
Atualizar sites confiáveis no Internet Explorer.....	21
Configurar os navegadores para o acesso remoto ao Core Console.....	22
Configurar o navegador Internet Explorer e Chrome.....	22
Configurar o navegador Mozilla Firefox.....	22
Analisar períodos de retenção.....	23

Criptografar dados de instantâneo do agente.....	23
Configurar um servidor de e-mail e um modelo de notificação por e-mail	24
Ajustar o número de fluxos.....	25
Proteger as máquinas e verificar a conectividade com os clientes.....	25
Verificar a conectividade de rede.....	26
Verificar as configurações de firewall.....	26
Verificar a resolução de nomes (se aplicável).....	26
Agrupar adaptadores de rede.....	26
Reinstalar o Broadcom Advanced Configuration Suite	27
Criar o grupo de NICs.....	27
Configurar um comutador virtual Hyper-V.....	28
4 Instalar agentes nos clientes.....	29
Instalar agentes remotamente (instalação forçada).....	29
Implementar o software do agente ao proteger um agente.....	30
Instalar agentes do Microsoft Windows no cliente.....	31
Adicionar um agente usando o portal de licenças.....	31
Instalar agentes em máquinas Linux.....	32
Localização dos arquivos de um agente Linux.....	33
Dependências do agente.....	33
Instalar o agente no Ubuntu.....	34
Instalar o agente no Red Hat Enterprise Linux ou no CentOS.....	35
Instalar o agente no SUSE Linux Enterprise Server.....	35
5 Obter ajuda.....	37
Localizar a documentação e as atualizações de software.....	37
Encontrar atualizações de software.....	37
Como entrar em contato com a Dell.....	37
Feedback sobre a documentação.....	37

Configurar o dispositivo DL4300

Introdução

O Dell DL4300 é a última geração de dispositivo de backup em disco com a plataforma de software Dell AppAssure. O dispositivo permite:

- Recursos de armazenamento dimensionáveis, compatíveis com organizações de qualquer tamanho
- Backups mais rápidos, bem como cenários de recuperação mais rápidos do que com dispositivos de fita convencionais e outras metodologias de backup
- Capacidade opcional de eliminação de duplicações
- Proteção contínua de dados de servidores de data centers e escritórios remotos
- Implementação rápida e fácil, o que reduz o tempo necessário para começar a proteger dados críticos
- Opção de configuração de Fibre Channel

Termos usados neste documento

A tabela a seguir mostra os termos usados neste documento para fazer referência a vários componentes de hardware e de software do dispositivo DL4300.

Tabela 1. Componentes de hardware e software do dispositivo DL4300

Componente	Termo usado
Dispositivo DL4300	Dispositivo
Gabinete de armazenamento Dell Storage MD1400	Gabinete de armazenamento
Software Dell AppAssure	AppAssure

Configurações disponíveis


O dispositivo DL está disponível em duas configurações: Standard Edition e High Capacity Edition.

Tabela 2. Configurações de capacidade do DL4300 Standard Edition

Capacidade	Configuração de hardware
5 TB	12 unidades de 1 TB, 4 unidades internas de 1 TB
10-20 TB	12 unidades de 2 TB, 4 unidades internas de 2 TB
30-40 TB	12 unidades de 4 TB, 4 unidades internas de 4 TB
50-60 TB	12 unidades de 6 TB, 4 unidades internas de 6 TB


Tabela 3. Configurações de capacidade do DL4300 High Capacity Edition

Capacidade	Configuração de hardware
40 TB, 50 TB, 60 TB, 70 TB, 80 TB, 90 TB, 100 TB, 110 TB e 120 TB	12 unidades de 6 TB, 4 unidades internas de 6 TB

 **NOTA:** O armazenamento adicional pode ser adicionado por meio de prateleiras de expansão (Dell Storage MD1400). O armazenamento adicional pode ser adicionado a qualquer modelo. Entretanto, o Standard Edition tem uma capacidade máxima de 60 TB e o High Capacity Edition tem uma capacidade máxima de 120 TB. As duas edições suportam até quatro prateleiras de expansão.

Cada configuração contém os seguintes hardwares e softwares:

- Sistema Dell DL4300
- Controladores RAID Dell PowerEdge (PERC)
- Sistema operacional pré-instalado, sistema Dell OpenManage e software de gerenciamento de armazenamento
- Software AppAssure

 **NOTA:** Se a configuração do dispositivo não incluir gabinetes de armazenamento Dell Storage MD1400, ignore, neste documento, as referências a Dell Storage MD1400 e aos gabinetes de armazenamento.

Pré-requisitos de instalação

Requisitos de rede

Seu dispositivo precisa do seguinte ambiente de rede:


- Rede ativa com cabos e conexões Ethernet disponíveis
- Um endereço IP estático e endereço IP do servidor DNS, caso não seja fornecido pelo protocolo DHCP
- Nome de usuário e senha com privilégios de administrador

Infraestrutura de rede recomendada

A Dell recomenda que as organizações usem um comutador de 1 GbE junto com o AppAssure para obter um desempenho eficiente, e redes de 10 GbE para ambientes extremamente robustos.

Configurar o hardware

O dispositivo é fornecido com um único sistema DL4300. Antes de instalar o hardware do dispositivo, consulte o documento *Dell DL4300 Appliance Getting Started With Your System* fornecido com o dispositivo. Desembale e instale o hardware do dispositivo DL.

 **NOTA:** O software está pré-instalado no dispositivo. Qualquer mídia contida no sistema precisa ser usada apenas na eventualidade de uma recuperação do sistema.

Para instalar o hardware do dispositivo DL:

1. Instale o rack e os cabos do sistema DL4300 e do(s) compartimento(s) de armazenamento.
2. Ligue o(s) compartimento(s) de armazenamento(s) e, em seguida, o sistema DL4300.

Instalar o dispositivo em um rack

Se o seu sistema contém um kit de trilhos, localize as *Instruções de instalação em rack* fornecidas com o kit do rack. Siga as instruções descritas para instalar os trilhos na unidade de rack, bem como o sistema e o gabinete de armazenamento.

Configurar o comutador de configuração do gabinete de armazenamento

Configure o modo de armazenamento do gabinete de armazenamento para o modo unificado, conforme indicado na figura a seguir.

NOTA: O comutador de configuração precisa ser configurado antes de ligar o gabinete de armazenamento. Alterar o modo de configuração depois de ligar o gabinete de armazenamento não tem efeito sobre a configuração do gabinete até que o sistema seja reinicializado. Para obter mais informações, consulte o *Dell Storage MD1400 Enclosures Hardware Owner's Manual* (Manual do Proprietário de Hardware de Gabinetes Dell Storage MD1400) disponível em dell.com/support/home.

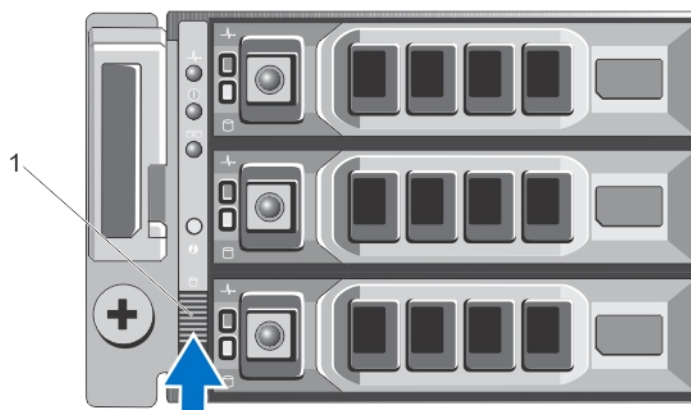


Figura 1. Configurar o comutador de configuração do gabinete de armazenamento PowerVault MD1400

1. comutador de configuração

Conectar o gabinete de armazenamento ao sistema

Conecte o cabo de dados do Controlador RAID PowerEdge (PERC - PowerEdge RAID Controller) instalado no sistema Dell DL4300 à porta SAS EMM (Enclosure Management Module — Módulo de gerenciamento do gabinete) principal do gabinete de armazenamento.

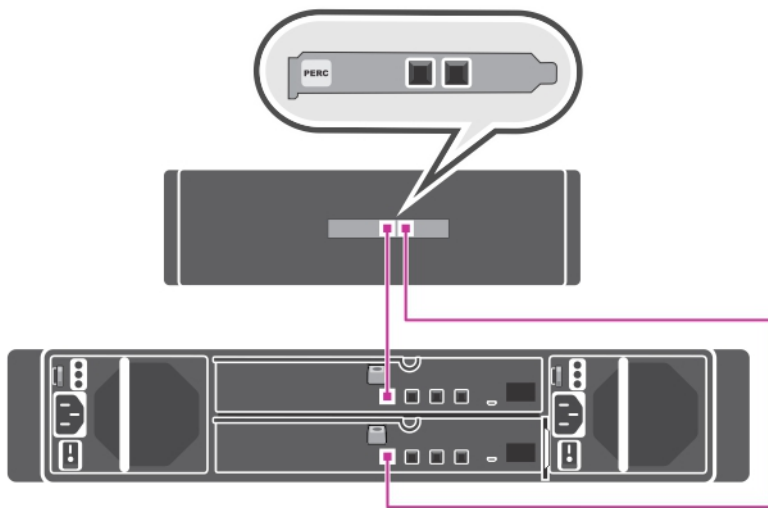


Figura 2. Conectar o sistema DL4300 ao gabinete de armazenamento MD1400

Configuração da porta redundante

Para obter uma configuração de porta redundante:

1. Conecte uma extremidade de cada cabo SAS à porta 0 e à porta 1 no controlador PERC do sistema DL4300.
2. Conecte a outra extremidade de cada cabo SAS à porta 1 de cada EMM no gabinete de armazenamento MD1400.

Configuração de porta única

Para obter uma configuração de porta única:

1. Conecte uma extremidade do cabo SAS à porta 0 no controlador PERC do sistema DL4300.
2. Conecte a outra extremidade do cabo SAS à porta 1 do EMM no gabinete de armazenamento MD1400.

Configuração multicadeia

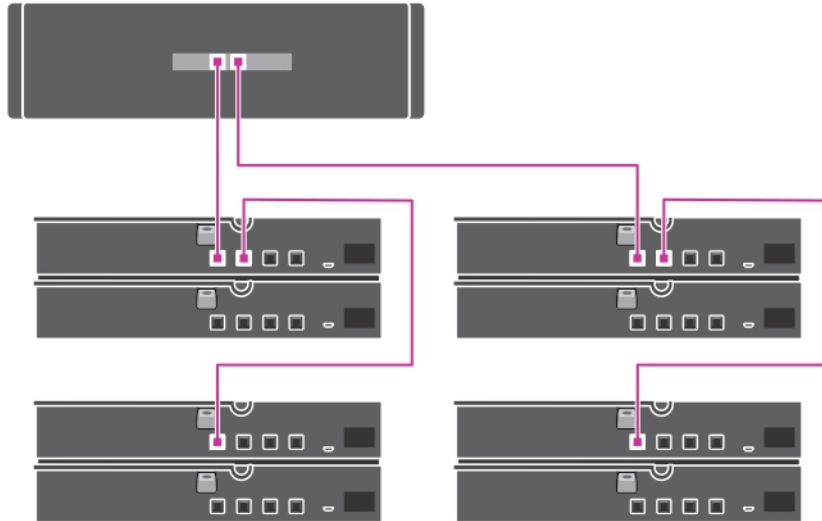


Figura 3. Configuração multicadeia

A configuração multicadeia suporta até quatro gabinetes. Os dois primeiros gabinetes são ligados em série com um dos gabinetes conectado a uma porta única na placa controladora. Os outros dois gabinetes são ligados em série com um dos gabinetes conectado à segunda porta na placa controladora.

Conectar o braço de gerenciamento de cabos (opcional)


Se o dispositivo tiver um CMA (Cable Management Arm – braço de gerenciamento de cabos), consulte as *Instruções de instalação* fornecidas com o kit do CMA e siga as instruções descritas para instalá-lo.

Cabeamento do dispositivo

Localize o documento *Getting Started With Your System* (Guia de Noções Básicas do Sistema) em Dell.com/support/home fornecido com o dispositivo. Siga as instruções para conectar os cabos de teclado, mouse, monitor, alimentação e rede ao dispositivo.

Ligar o dispositivo

Depois de conectar o cabeamento do dispositivo, ligue o gabinete de armazenamento MD1400 e, em seguida, o sistema DL4300.

 **NOTA:** Para o máximo de confiabilidade e disponibilidade, é recomendável que você conecte o dispositivo a uma fonte de alimentação ininterrupta (UPS).



Configurações de disco do DL4300

O DL4300 oferece suporte para unidades SATA e SAS nearline. O sistema operacional reside em um disco virtual RAID 1 (espelhado) localizado nos slots 12 e 13. Para obter informações sobre esses discos, consulte o *Dell DL4300 Appliance Owner's Manual* (Guia do Usuário do Dispositivo Dell DL4300), disponível em Dell.com/support/home. As unidades disponíveis nos slots 0 a 11 e 14 a 17 estão disponíveis para configuração automática pelo Assistente de configuração de dispositivo do AppAssure


(recomendado), mas configurações personalizadas podem ser feitas manualmente, se necessário. Os discos são provisionados automaticamente como RAID 6. A expansão de capacidade por meio de um gabinete de armazenamento MD1400 é opcional.

Configuração inicial do software

Quando você ligar o dispositivo pela primeira vez e alterar a senha do sistema, o **Assistente de configuração de dispositivo do AppAssure** será executado automaticamente.

1. Depois de ligar o sistema, escolha o idioma do sistema operacional entre as opções de idiomas do Windows.
O Contrato de licença do usuário final é mostrado na página **Settings** (Configurações).
 2. Para aceitar o Contrato de licença do usuário final, clique no botão **I accept** (Aceito).
O sistema mostra uma tela para alterar a senha do administrador.
 3. Clique em **OK** na mensagem que solicita a alteração da senha de administrador.
 4. Digite e confirme a nova senha.
Uma mensagem confirma que a senha foi alterada.
 5. Clique em **OK**.
 6. Na tela **Dell readme.htm**, role para baixo e clique em **Proceed** (Continuar).
 7. Faça login usando a senha de administrador alterada.
A tela **Select the language for AppAssure Appliance** (Selecionar o idioma do dispositivo AppAssure) é mostrada.
 8. Selecione o idioma do dispositivo na lista de idiomas suportados.
A tela de boas-vindas do **Assistente de configuração do dispositivo AppAssure** é mostrada.
-  **NOTA:** O **Assistente de configuração de dispositivo do AppAssure** pode demorar até 30 segundos para ser mostrado no console do sistema.
-  **NOTA:** Não feche o **Assistente de configuração de dispositivo do AppAssure** antes que todas as tarefas tenham sido concluídas.

Assistente de configuração de dispositivo do AppAssure

 **CUIDADO:** Certifique-se de executar todas as etapas do **Assistente de configuração de dispositivo do AppAssure** antes de executar qualquer outra tarefa ou alterar qualquer configuração no dispositivo. Até concluir o assistente, não faça nenhuma alteração através do Painel de controle, não use o Microsoft Windows Update, não atualize o software AppAssure nem instale licenças.

O **Assistente de configuração de dispositivo do AppAssure** guia você através das seguintes etapas para configurar o software no dispositivo:

- [Definir a interface de rede](#)
- [Definir o nome de host e as configurações de domínio](#)
- [Definir as configurações do SNMP](#)
- [Criar discos virtuais RASR e Windows](#)

Quando a instalação usando o assistente terminar, o Core Console será iniciado automaticamente.

Configurar a interface de rede

Para configurar as interfaces de rede disponíveis:

1. Na tela **AppAssure Appliance Configuration Wizard Welcome** (Bem-vindo ao assistente de configuração de dispositivo do AppAssure), clique em **Next** (Avançar).

A página **network interfaces** (interfaces de rede) mostra as interfaces de rede conectadas disponíveis.

2. Selecione as interfaces de rede que você quer configurar.



NOTA: O **Assistente de configuração de dispositivo do AppAssure** configura as interfaces de rede como portas individuais (não agrupadas). Para aumentar o desempenho do tráfego de entrada, você pode criar um canal maior para o tráfego de entrada agrupando as NICs. Entretanto, é preciso que essa configuração seja feita apenas depois da configuração inicial do dispositivo.

3. Se necessário, conecte interfaces de rede adicionais e clique em **Refresh** (Atualizar).

As interfaces de rede conectadas adicionais serão mostradas.

4. Clique em **Next** (Avançar).

A página **Configure selected network interface** (Configurar a interface de rede selecionada) é mostrada.

5. Selecione o protocolo de internet adequado para a interface selecionada.

Você pode escolher **IPv4** ou **IPv6**.

Os detalhes de rede que serão mostrados dependem do protocolo de internet selecionado.

6. Para atribuir os detalhes do protocolo de internet, escolha uma destas duas opções:

- Para atribuir os detalhes do protocolo de internet selecionado automaticamente, selecione **Obtain an IPv4 address automatically** (Obter um endereço IPv4 automaticamente).
- Para atribuir a conexão de rede manualmente, selecione **Use the following IPv4 address** (Usar o seguinte endereço IPv4) e digite as informações a seguir:
 - **IPv4 Address** (Endereço IPv4) ou **IPv6 Address** (Endereço IPv6)
 - **Subnet mask** (Máscara de sub-rede) para IPv4 e **Subnet prefix length** (Comprimento do prefixo da sub-rede) para IPv6
 - **Default Gateway (Gateway padrão)**

7. Para atribuir os detalhes do servidor DNS, escolha uma destas duas opções:

- Para atribuir o endereço do servidor DNS automaticamente, selecione **Obtain DNS server address automatically** (Obter o endereço do servidor DNS automaticamente).
- Para atribuir o servidor DNS manualmente, selecione **Use the following DNS server address** (Usar o seguinte endereço do servidor DNS) e digite os detalhes a seguir:
 - **Preferred DNS server (Servidor DNS preferencial)**
 - **Alternate DNS Server (Servidor DNS alternativo)**


8. Clique em **Next** (Avançar).

A página **Configure hostname and domain setting** (Definir o nome de host e as configurações de domínio) é mostrada.

Para obter informações sobre agrupamento de NICs, consulte [Agrupar adaptadores de rede](#).


Definir o nome de host e as configurações de domínio

Você precisa atribuir um nome de host para o utilitário. É recomendável que você altere o nome de host antes de iniciar os backups. Por padrão, o nome de host é o nome do sistema que o sistema operacional atribui.


 **NOTA:** Se você quiser alterar o nome de host, é recomendável que você o altere neste momento. Alterar o nome de host após a conclusão do **Assistente de configuração de dispositivo do AppAssure** exige a execução manual de várias etapas.

Para definir o nome de host e as configurações de domínio:

1. Na página **Configure host name and domain setting** (Definir o nome de host e as configurações de domínio), para alterar o nome de host do dispositivo, digite um nome de host adequado na caixa de texto **New Host name** (Novo nome de host).
2. Se você não quiser que o dispositivo seja associado a um domínio, selecione **No** (Não) como resposta à pergunta **Do you want this appliance to join a domain?** (Você quer que esse dispositivo seja associado a um domínio?)
Por padrão, **Yes** (Sim) é selecionado.
3. Para associar o dispositivo a um domínio, digite as informações a seguir:
 - **Domain name (Nome do domínio)**
 - **Nome do usuário do domínio**
4. Clique em **Next** (Avançar).

 **NOTA:** O usuário do domínio precisa ter direitos administrativos locais.

- **Domain user password (Senha do usuário do domínio)**


 **NOTA:** Alterar o nome de host ou o domínio exige a reinicialização da máquina. Depois de reiniciar a máquina, o **Assistente de configuração de dispositivo do AppAssure** será iniciado automaticamente. Se o dispositivo estiver conectado a um domínio, depois de reiniciar a máquina, você precisará fazer login no dispositivo como um usuário do domínio com privilégios de administrador.

A página **Configure SNMP Settings** (Definir as configurações do SNMP) é mostrada.

Definir as configurações do SNMP

O SNMP (Simple Network Management Protocol - protocolo de gerenciamento de rede simplificada) é um protocolo de gerenciamento de rede normalmente usado que permite o uso de funções de gerenciamento compatíveis com o SNMP, como descoberta de dispositivo, monitoramento e geração de eventos. O SNMP fornece o gerenciamento de rede do protocolo TCP/IP.

Para configurar os alertas de SNMP para o dispositivo:

1. Na página **Configure SNMP Settings** (Definir as configurações do SNMP), selecione **Configure SNMP on this appliance** (Configurar o SNMP neste dispositivo).
 -  **NOTA:** Desmarque **Configure SNMP on this appliance** (Configurar o SNMP neste dispositivo) caso você não queira configurar os detalhes e os alertas de SNMP no dispositivo, e vá para a etapa 6.
2. Em **Communities** (Comunidades), digite um ou mais nomes de comunidades SNMP.
Use vírgulas para separar vários nomes de comunidades.
3. Em **Accept SNMP packets from these hosts** (Aceitar pacotes SNMP destes hosts), digite os nomes dos hosts com os quais o dispositivo pode se comunicar.

Separe os nomes dos hosts com vírgulas ou deixe em branco para permitir a comunicação com todos os hosts.

4. Para configurar os alertas de SNMP, digite o **Community Name** (Nome da comunidade) e os **Trap destinations** (Destinos das interceptações) para os alertas de SNMP, e clique em **Add** (Adicionar). Repita essa etapa para adicionar mais endereços SNMP.
5. Para remover um endereço SNMP configurado, em **Configured SNMP addresses** (Endereços SNMP configurados), selecione o endereço SNMP adequado e clique em **Remove** (Remover).
6. Clique em **Next** (Avançar).
A página **Create Windows and RASR virtual disk(s)** (Criar discos virtuais RASR e Windows) é mostrada.


Criar discos virtuais RASR e Windows

O sistema DL4300 oferece suporte para:

- Duas unidades de sistema operacional, doze unidades de dados e quatro discos rígidos internos
- Opção para criar LUNs (Logical Unit Number – Número de unidade lógica) para o armazenamento de informações de restauração bare-metal (BMR)
- Opção para criar um espaço separado para o arquivo de RASR de backup do Windows.

Para criar discos virtuais opcionais:

1. Selecione os seguintes discos virtuais:
 - a. Disco virtual de backup do Windows

 **CUIDADO: Se você ignorou esta opção no Assistente de configuração de dispositivo do AppAssure, você não será capaz de criar um backup do Windows Server e configurar uma política de backup.**

O disco virtual de backup do Windows fornece espaço onde criar backups do Windows Server. Por padrão, são alocados 75 GB de espaço para o disco virtual de backup do Windows e você não pode aumentar o tamanho do disco virtual de backup do Windows. Com o tempo, os dados salvos em backups podem exceder 75 GB e, se isso ocorrer, não será possível efetuar o backup nem configurar a política de backup na página de **Backup**, e um erro de capacidade excedida será exibido. Neste caso, o backup do Windows pode ser reconfigurado para um compartilhamento de rede ou para outro volume de disco no dispositivo DI. Para obter mais informações, consulte a seção Configure a Scheduled Shared Network Drive Backup Policy (Configurar uma política de backup programado de unidade de rede compartilhada) em *Recovering a Dell™ DL Backup and Recovery Appliance using Rapid Appliance Self Recovery (RASR)* (Recuperação de um dispositivo de backup e recuperação Dell™ DL usando a recuperação automática rápida do dispositivo (RASR)) em Dell.com/supportmanuals.

- b. Disco virtual inicializável RASR

O disco virtual inicializável RASR fornece um volume de recuperação redundante para realizar uma recuperação RASR. Para reinicializar por meio do volume de recuperação redundante, pressione <F8> durante o POST (Power-on self test – Teste automático de ativação). Depois da reinicialização, siga o procedimento descrito em [Executar a RASR através de um pen drive USB RASR](#).

2. Clique em **Avançar**.

Durante a configuração, o sistema mostrará uma tela de agradecimento e, ao final, uma mensagem de conclusão da configuração.

3. Clique em **Exit** (Sair).
O Core Console será iniciado automaticamente.
4. Continue o processo de configuração em [Provisionar o armazenamento](#)


Utilitário de recuperação e atualização


O Utilitário de recuperação e atualização (RUU - Recovery and Update Utility) é um instalador do tipo "tudo em um" para recuperar e atualizar softwares de Aparelhos DL (DL1000, DL1300, DL4000 e DL4300). Ele contém o software AppAssure Core e componentes específicos do aparelho.


O RUU é composto de versões atualizadas das Funções e recursos do Windows Server, ASP .NET MVC3, LSI Provider, DL Applications, OpenManage Server Administrator e do software AppAssure Core. Além disso, o Utilitário de recuperação e atualização também atualiza o conteúdo da Recuperação automática rápida do aparelho (RASR - Rapid Appliance Self Recovery).

Para fazer download da versão mais recente do RUU:

1. Acesse a seção Downloads no portal de licenças e faça download do instalador do RUU ou acesse support.dell.com.
2. Execute o instalador do RUU.

 **NOTA:** O sistema pode ser reiniciado durante o processo de atualização do RUU.

 **NOTA:** Se você usar o RUU 184 e a versão do AppAssure Core no seu aparelho DL for inferior à versão 5.4.3.106, o núcleo será atualizado para o AppAssure Core 5.4.3.106.

 **NOTA:** Se atualizar para o RUU 184, você poderá começar a ver algumas inconsistências nas execuções futuras de backups já agendados do Windows (através da RASR) ou talvez não consiga criar uma política do Backup do Windows. Essas inconsistências ocorrem devido a limitações de espaço no seu local de armazenamento do Backup do Windows.

Outras causas possíveis dessas falhas incluem:

1. Upgrade para o Rapid Recovery, principalmente se mais do que o cache mínimo de eliminação de duplicação for usado.
2. Instalação ou atualização de qualquer software (por exemplo, o Outlook) no aparelho.
3. Instalações de atualizações do Windows.
4. Inclusão/aumento de arquivos de dados (como o cache de eliminação de duplicação).
5. Combinações das situações anteriores.

Recuperação automática rápida do dispositivo

A RASR (Rapid Appliance Self Recovery – Recuperação automática rápida do dispositivo) é um processo de recuperação bare-metal em que as unidades de sistema operacional e as unidades de dados são usadas para:

- Restaurar as configurações de fábrica
- Recuperar o seu dispositivo para um estado anterior à falha


Criar o pen drive USB RASR

Para criar um pen drive USB RASR:

1. Navegue até a guia **Appliance** (Dispositivo).
2. Usando a navegação no painel esquerdo, selecione **Appliance (Dispositivo)** → **Backup**.
A janela **Create RASR USB Drive** (Criar unidade USB RASR) é mostrada.
 **NOTA:** Insira um pen drive USB de 16 ou mais GB antes de tentar criar a chave RASR.
3. Após inserir um pen drive USB de 16 GB ou mais, clique em **Create RASR USB Drive now** (Criar unidade USB RASR agora).
A mensagem **Prerequisite Check** (Verificação de pré-requisitos) é mostrada.
Depois dos pré-requisitos serem verificados, a janela **Create the RASR USB Drive** (Criar a unidade USB RASR) mostra o tamanho mínimo necessário para criar a unidade USB e uma **Lista de possíveis caminhos de destino**.
4. Selecione o destino e clique em **Create** (Criar).
Uma caixa de diálogo de aviso é mostrada.
5. Clique em **Yes** (Sim).
A chave da unidade USB RASR é criada.
6.  **NOTA:** Certifique-se de utilizar a função Windows Eject Drive (Unidade de ejeção do Windows) para preparar o pen drive USB para remoção. Caso contrário, o conteúdo do pen drive USB pode ser danificado e o pen drive USB não irá funcionar como o previsto.

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

Executar a RASR

-  **NOTA:** A Dell recomenda que você crie um pen drive USB RASR depois de configurar o dispositivo. Para criar um pen drive USB RASR, consulte a seção [Criar o pen drive USB RASR](#)

Essas etapas ajudam você a executar a redefinição de fábrica.

Para recuperar o seu dispositivo para um estado anterior à falha e recuperar repositórios, pontos de recuperação e configurações, consulte o documento *Recovering a Dell™ DL Backup and Recovery Appliance using Rapid Appliance Self Recovery (RASR)* (Recuperar um dispositivo DL de backup e recuperação da Dell™ usando Recuperação automática rápida do dispositivo) disponível em **Dell.com/support/home**

Para executar a RASR:

1. Insira a chave USB RASR criada.
2. Reinicie o dispositivo e selecione **Boot Manager (F11)** (Gerenciador de Inicialização (F11)).
3. No **Boot Manager Main Menu** (Menu principal do Gerenciador de Inicialização), selecione **One-shot BIOS Boot Menu** (Menu de inicialização única do BIOS).
4. No **Boot Manager Boot Menu** (Menu de inicialização do Gerenciador de Inicialização), selecione a unidade USB conectada.
5. Selecione o layout de teclado.
6. Clique em **Troubleshoot (Solucionar problemas)** → **Rapid Appliance Self Recovery (Recuperação automática rápida do dispositivo)**.
7. Selecione o sistema operacional (SO) de destino.

A RASR é aberta e a tela de boas-vindas é mostrada.

8. Clique em **Avançar**.

A tela de verificação **Prerequisites** (Pré-requisitos) é mostrada.



NOTA: Confirme que todo o hardware e os outros pré-requisitos foram verificados antes de executar a RASR.

9. Clique em **Avançar**.

A tela **Recovery Mode Selection** (Seleção do modo de recuperação) é mostrada com três opções:

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

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

Esta opção irá recuperar o disco do sistema operacional a partir da imagem de fábrica.

11. Clique em **Avançar**.

A seguinte mensagem de advertência é mostrada em uma caixa de diálogo: `This operation will recover the operating system. All OS disk data will be overwritten.` (Esta operação irá recuperar o sistema operacional. Todos os dados de disco do SO serão substituídos.)

12. Clique em **Yes** (Sim).

O disco do sistema operacional começa a ser restaurado de volta à redefinição de fábrica.

13. Após a conclusão do processo de recuperação da redefinição de fábrica, na tela **RASR Completed** (RASR concluída), clique em **Finish** (Concluir).

Executar a RASR através do módulo SD duplo interno

O seu sistema é fornecido com um IDSDM (Internal Dual SD Module – Módulo SD duplo interno) e um cartão SD com 16 GB de capacidade.

Para executar a RASR usando o IDSDM:

1. Reinicialize o dispositivo pelo IDSDM.



CUIDADO: Confirme que o cartão SD está inserido no slot 1.

A mensagem a seguir será mostrada.

`The secondary SD card is missing, not responding, or in write-protected mode. Do one of the following: 1) Install a SD card media in the secondary SD card reader. 2) Reseat or replace the SD card media.3) If write-protected mode is expected, then no respose action is required.`


Ignore a mensagem acima.

2. Para continuar executando a RASR pelo módulo SD interno, execute as etapas 5 a 13 da seção [Executar a RASR através do pen drive USB RASR](#).


Provisionar o armazenamento


O dispositivo configura o armazenamento interno disponível do DL4300 e todos os gabinetes de armazenamento externo conectados para:

- Repositórios do AppAssure

 **NOTA:** Se o HBA Fibre Channel estiver configurado, o processo de criação dos repositórios será manual. O AppAssure não criará automaticamente um repositório no diretório raiz. Para obter mais informações, consulte o *Dell DL4300 Appliance Deployment Guide* (Guia de Implementação do Dispositivo Dell DL4300).

- Espera virtual das máquinas protegidas

 **NOTA:** São compatíveis os dispositivos MD1400 com unidades de 1 TB, 2 TB, 4 TB ou 6 TB (para alta capacidade) conectadas ao controlador H830. Até quatro dispositivos MD1400 são suportados.

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

Antes de começar a provisionar o armazenamento no disco, determine o quanto de armazenamento você quer alocar para as máquinas virtuais em espera. Você pode alocar qualquer porcentagem da capacidade disponível restante após a criação do repositório do AppAssure para hospedar máquinas virtuais em espera. Por exemplo, se você estiver usando o SRM (Storage Resource Management - Gerenciamento de recursos de armazenamento), você poderá alocar até 100% da capacidade do armazenamento restante após a criação do repositório do AppAssure. É possível alocar espaço para máquinas virtuais em espera apenas nos dispositivos que são provisionados para hospedar máquinas virtuais. Usando o recurso Live Recovery (Recuperação em tempo real) do AppAssure, você pode usar essas máquinas virtuais para substituir rapidamente um servidor com falha que o dispositivo protege.

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

Quando você seleciona a guia **Appliance** (Dispositivo), o software AppAssure Appliance localiza o espaço de armazenamento disponível de todos os controladores suportados no sistema e confirma que o hardware atende aos requisitos.

Para concluir o provisionamento de disco para todo o armazenamento disponível:

1. Na guia **Appliance** (Dispositivo), clique em **Tasks (Tarefas) → Provisioning (Provisionamento)**.

A tela **Provisioning** (Provisionamento) mostra a capacidade estimada para o provisionamento. Essa capacidade é usada para criar um novo repositório do AppAssure.

 **CUIDADO:** Antes de continuar, confirme se as Etapas 2 a 4 foram seguidas neste procedimento.

2.  **NOTA:** Provisione o controlador RAID interno para criar o repositório inicial em seu dispositivo.

Abra a janela **Provisioning Storage** (Provisionar armazenamento) clicando em **Provision** (Provisionar) na coluna Action (Ação) ao lado do armazenamento que você quer provisionar.

3. Na seção **Optional Storage Reserve** (Reserva de armazenamento opcional), marque a caixa ao lado de **Allocate a portion of the storage being provisioned for Standby Virtual Machines or other purposes** (Alocar uma parte do armazenamento que está sendo provisionado para as máquinas virtuais em espera ou outros fins) e indique uma porcentagem do armazenamento para alocar. Caso contrário, a porcentagem de armazenamento indicada na seção **Optional Storage Reserve** (Reserva de armazenamento opcional) será retirada de todos os discos conectados.

4. Clique em **Provision** (Provisionar).

Status	Task Name	State	Action
>	Provision MD1400 6VFXQ22 Full shelf 0	Verified: Ready for provisioning	Provision
>	Provision MD1400 6VFXQ22 Full shelf 0	Verified: Ready for provisioning	Provision
>	Provision PERC H730P Mini(3,0) Full shelf 0, Create repository	Provisioned	

Showing 1-3 of 3

Os discos virtuais para a hospedagem de repositórios e para as máquinas virtuais em espera são criados.

Provisionar o armazenamento selecionado

Para provisionar o armazenamento selecionado:

1. Na guia **Appliance** (Dispositivo), clique em **Tasks** (Tarefas).
A tela **Tasks** (Tarefas) mostra a capacidade de armazenamento interna e externa que está disponível para o dispositivo, se ela está disponível para provisionamento ou se já foi provisionada, ou se há uma condição impedindo que o armazenamento seja automaticamente provisionado. Essa capacidade é usada para criar um repositório do AppAssure.

2. **NOTA:** É recomendável provisionar o armazenamento interno disponível antes de expandir para o compartimento externo (MD1400).

Para provisionar somente uma parte do espaço disponível, clique em **Provision** (Provisionar) em **Action** (Ação) ao lado do espaço de armazenamento que você quer provisionar.

- Para criar novo repositório, selecione **Create a new repository** (Criar um novo repositório) e forneça um nome para o repositório.
Por padrão, Repositório 1 aparece como o nome do repositório. Você pode alterar esse nome.
- Para adicionar capacidade a um repositório existente, selecione **Expand the existing repository** (Expandir o repositório existente) e, em seguida, selecione o repositório na lista **Existing Repositories** (Repositórios existentes).

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

3. Em **Optional Storage Reserve** (Reserva de armazenamento opcional), você pode selecionar a opção para alocar uma parte do armazenamento para máquinas virtuais em espera e, em seguida, especificar o percentual de armazenamento para alocar para as MVs.
4. Você pode optar por desmarcar a caixa de seleção **Do this for only one provisioning task when more than one task is being provisioned at a time** (Fazer isso para apenas uma tarefa de provisionamento quando mais de uma tarefa estiver sendo provisionada por vez) (selecionada por padrão).

Ao desmarcar essa opção, a porcentagem do armazenamento selecionado é aplicada apenas para o dispositivo de armazenamento selecionado. Ao marcar essa opção, você pode aplicar a porcentagem do armazenamento selecionado para o armazenamento interno e para os compartimentos externos.

5. Clique em **Provision** (Provisionar).

O provisionamento de disco começa e o status da criação do repositório do AppAssure é mostrado na área de **Status** da tela **Tasks** (Tarefas). A **Status Description** (Descrição do status) é mostrada como **Provisioned** (Provisionado).

6. Para ver os detalhes após a conclusão do provisionamento, clique em > ao lado da luz de status.
A página **Tasks** (Tarefas) se expande e mostra o status, o repositório e os detalhes do disco virtual (se alocado).

Configurar o DL4300 usando armazenamento Fibre Channel (opcional)

A edição de alta capacidade do DL4300 oferece uma opção de armazenamento HBA Fibre Channel que permite a criação de repositórios usando matrizes de armazenamento Fibre Channel.



NOTA: Se a configuração de Fibre Channel for pedida, ela substituirá o adaptador SAS PERC H830 no slot.




NOTA: Para obter os pré-requisitos, as premissas e informações detalhadas sobre o procedimento a seguir, consulte o informativo técnico *DL4xxx - Fibre Channel Implementation* (DL4xxx - Implementação em Fibre Channel), disponível em dell.com/support/home.

Para integrar e configurar o DL4300 usando o armazenamento Fibre Channel:

1. Conecte o HBA Fibre Channel do DL4300 a um comutador SAN.
2. Instale o software de gerenciamento de HBAs Emulex ou Qlogic para os adaptadores pedidos com o sistema.
3. Instale o software de múltiplos caminhos da matriz de armazenamento.
4. Execute o zoneamento da malha Fibre Channel.
5. Crie um LUN (Logical Unit Number - Número de unidade lógica) de Fibre Channel para ser atribuído e usado como um repositório do DL4300.
6. Monte o LUN de armazenamento Fibre Channel.
7. Configure o armazenamento Fibre Channel do DL4300 como um repositório de backup.

Tarefas pós-instalação

Depois de concluir o **Assistente de configuração de dispositivo do AppAssure**, execute os seguintes procedimentos para garantir que o dispositivo de backup e os servidores cujo backup está sendo feito pelo dispositivo estão configurados corretamente.

-  **NOTA:** O dispositivo é configurado com uma licença de software temporária do AppAssure válida por 30 dias. Para obter uma chave de licença permanente, faça login no portal de licenças do Dell AppAssure, na página www.dell.com/DLActivation. Para conhecer detalhes sobre a alteração de uma chave de licença no software AppAssure, consulte o tópico "Changing A License Key" (Alterar uma chave de licença) no *Dell DL4300 Appliance User's Guide* (Guia do Usuário do Dispositivo Dell DL4000) disponível em dell.com/support/home.

Acessar o Core Console

Confirme que os sites confiáveis foram atualizados conforme descrito no tópico [Atualizar sites confiáveis no Internet Explorer](#) e configure o seu navegador como descrito no tópico [Configurar os navegadores para acessar remotamente o Core Console](#). Após atualizar os sites confiáveis no Internet Explorer e configurar os seus navegadores, execute um dos seguintes procedimentos para acessar o Core Console:

- Faça login localmente no servidor do núcleo do AppAssure e clique duas vezes no ícone do **Core Console**.
- Digite uma das seguintes URLs no navegador da Web:
 - <https://<yourCoreServerName>:8006/apprecovery/admin/core>
 - <https://<yourCoreServerIPaddress>: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://\[nome de exibição\]](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 o acesso remoto ao Core Console

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

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

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

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


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

Configurar o navegador Internet Explorer e Chrome

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

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

Configurar o navegador Mozilla Firefox

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

Para modificar as configurações do navegador Mozilla Firefox:

1. Na barra de endereços do Firefox, digite **about:config** e clique em **Serei cuidadoso, prometo!** se solicitado.
2. Procure o termo **ntlm**.
A pesquisa deve retornar pelo menos três resultados.

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

Analisar períodos de retenção

O dispositivo AppAssure define períodos de retenção que determinam com que frequência os instantâneos são obtidos e por quanto tempo são mantidos. Os períodos de retenção precisam ser baseados nas necessidades do seu ambiente. Por exemplo, se você estiver fazendo backup de servidores que executam dados essenciais à continuidade dos negócios e que mudam com frequência, os instantâneos precisam ser feitos com regularidade.

Para analisar e alterar os períodos de retenção:

1. Abra o Core Console.
2. Selecione a guia **Configuration** (Configuração) e clique em **Retention Policy** (Política de retenção).
3. Ajuste a política de retenção com base nas necessidades da sua organização.
4. Clique em **Apply** (Aplicar).

Criptografar dados de instantâneo do agente

O Núcleo pode criptografar dados de instantâneos do agente no repositório. Em vez de criptografar todo o repositório, ele permite que você especifique uma chave de criptografia durante a proteção de um agente em um repositório, o que permite que as chaves sejam reusadas para diferentes agentes.

Para criptografar dados de instantâneo do agente:

1. No AppAssure Core, clique em **Configuration** → **Manage** → **Security** (Configuração → Gerenciar → Segurança).
2. Clique em **Ações** (Actions) e, em seguida, clique em **Add Encryption Key** (Adicionar chave de criptografia).
A página **Create Encryption Key** (Criar chave de criptografia) é mostrada.
3. Preencha as seguintes informações:


Campo	Descrição
Name (Nome)	Digite um nome para a chave de criptografia.
Comment (Comentário)	Digite um comentário para a chave de criptografia, usado para fornecer mais detalhes sobre a chave de criptografia.
Passphrase (Senha)	Digite uma senha. Ela é usada para controlar o acesso.
Confirm Passphrase (Confirmar senha)	Digite novamente a senha. Este campo é usado para confirmar a senha.



NOTA: É recomendável que você anote a senha de criptografia, pois a perda da senha torna os dados inacessíveis.

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

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

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

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

1. No Core, selecione a guia **Configuration** (Configuração).
2. Na opção **Manage** (Gerenciar), clique em **Events** (Eventos).
3. No painel **Email SMTP Settings** (Configurações de SMTP do e-mail), clique em **Change** (Alterar). A caixa de diálogo de edição **Email Notification Configuration** (Configuração de notificação de e-mail) é exibida.
4. Selecione **Enable Email Notifications** (Ativar notificações de e-mail) e, em seguida, insira os detalhes para o servidor de e-mail descritos a seguir:

Caixa de texto Descrição

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

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.

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

Ajustar o número de fluxos

Por padrão, o AppAssure é configurado para permitir três fluxos simultâneos ao dispositivo. É recomendável que o número de fluxos seja um a mais do que o número de máquinas (agentes) que você está fazendo backup. Por exemplo, se você estiver fazendo backup de seis agentes, **Maximum Concurrent Transfers** (Número máximo de transferências simultâneas) precisa ser definido para sete.

Para alterar o número de fluxos simultâneos:

1. Selecione a guia **Configuration** (Configuração) e, em seguida, clique em **Settings** (Configurações).
2. Selecione alterar em **Transfer Queue** (Fila de transferência).
3. Altere **Maximum Concurrent Transfers** (Número máximo de transferências simultâneas) para um número que seja pelo menos um a mais do que o número de clientes que você está fazendo backup.

Proteger as máquinas e verificar a conectividade com os clientes

Após configurar o dispositivo DL e o Núcleo, verifique se é possível conectar-se às máquinas que você planeja fazer backup.

Para proteger uma máquina:

1. Navegue até o Core Console e selecione a guia **Machines** (Máquinas).
2. No menu suspenso **Ações** (Actions), clique em **Protect Machine** (Proteger máquina). A caixa de diálogo **Connect** (Conectar) é mostrada.
3. Na caixa de diálogo **Connect** (Conectar), digite as informações da máquina que você quer conectar, conforme descrito na tabela a seguir.

Host	O nome de host ou o endereço IP da máquina que você quer proteger.
Port (Porta)	O número da porta através da qual o AppAssure Core se comunica com o agente na máquina.
Username (Nome de usuário)	O nome de usuário usado para se conectar a esta máquina; por exemplo, administrador.
Password (Senha)	A senha usada para se conectar a essa máquina.

4. Clique em **Connect** (Conectar).
5. Se o dispositivo não conseguir se conectar à máquina para fazer backup, uma mensagem de erro será mostrada. Para resolver o problema:
 - a. Verifique a conectividade de rede.

- b. Verifique as configurações de firewall.
- c. Verifique se os serviços do AppAssure e o RPC estão em execução.
- d. Verifique a pesquisa ao serviço de nomes de domínio (se aplicável).

Verificar a conectividade de rede

Para verificar a conectividade de rede:

1. No sistema do cliente ao qual você está tentando se conectar, abra uma interface de linha de comando.
2. Execute o comando **ipconfig** e anote o endereço IP do cliente.
3. Abra uma interface de linha de comando no dispositivo.
4. Execute o comando **ping <IP address of client>**.
5. Dependendo do resultado, escolha uma destas opções:
 - Se o cliente não responder ao ping, verifique a conectividade e as configurações de rede do servidor.
 - Se o cliente responder, verifique se as configurações do firewall permitem a execução dos componentes do AppAssure.

Verificar as configurações de firewall

Se o cliente estiver conectado corretamente à rede, mas não puder ser visto pelo Core Console, verifique o firewall para garantir que há permissão para as comunicações de entrada e de saída necessárias.

Para verificar as configurações de firewall no AppAssure Core e em todos os clientes que ele faz backup:

1. No dispositivo, clique em **Iniciar** → **Painel de controle**.
2. No **Painel de controle**, clique em **Sistema e segurança**, em **Firewall do Windows** clique em **Verificar status do firewall**.
3. Clique em **Configurações avançadas**.
4. Na tela **Firewall do Windows com segurança avançada**, clique em **Regras de entrada**.
5. Confirme que o AppAssure Core e as portas mostrem **Sim** na coluna **Habilitado**.
6. Se a regra não estiver habilitada, clique com o botão direito em AppAssure Core e selecione **Habilitar regra**.
7. Clique em **Regras de saída** e faça a mesma verificação para AppAssure Core.

Verificar a resolução de nomes (se aplicável)

Se a máquina que você está tentando fazer backup usa DNS, verifique se as pesquisas diretas e inversas de DNS estão corretas.

Para confirmar que as pesquisas inversas estão corretas:

1. No dispositivo do AppAssure, vá até **C:\Windows\system32\drivers\etc** hosts.
2. Digite o endereço IP de cada cliente que faz backup usando o DL4300.

Agrupar adaptadores de rede

Por padrão, os adaptadores de rede (NICs) no dispositivo DL4300 não estão vinculados, o que afeta o desempenho do sistema. É recomendável agrupá-los em uma única interface. O agrupamento de NICs exigirá:

- Reinstalar o Broadcom Advanced Control Suite
- Criar o grupo de NICs
- Configurar um comutador virtual Hyper-V

Reinstalar o Broadcom Advanced Configuration Suite

Para reinstalar o Broadcom Advanced Configuration Suite (BACS):

1. Identifique os NICs em seu sistema. Para identificar os NICs:
 - a. Acesse o Dell Open Manage Server Administrator (OMSA).
 - b. Na página principal, clique em **System** → **Main System Chassis** → **Slots** (Sistema → Chassi do sistema principal → Slots).
2. Desinstale as versões anteriores dos drivers da Broadcom e dos aplicativos de gerenciamento.
3. Faça download do BACS e dos drivers da Broadcom adequados para o seu dispositivo.


Os seguintes drivers estão disponíveis no site dell.com/support.

 - Driver QLogic

Clique em **Servers, storage, & Networking** → **Dell Software DL 4300** → **Drivers & downloads** → **Category** → **Network** → **QLogic BCM57xx and BCM57xxx** (Servidores, armazenamento e rede → Software Dell DL4300 → Drivers e downloads → Categoria → Rede → QLogic BCM57xx e BCM57xxx).
 - Driver Broadcom


Clique em **Servers, storage, & Networking** → **Dell Software DL 4300** → **Drivers & downloads** → **Category** → **Network** → **Broadcom Windows 64bit driver update for NetXtrene Ethernet adapters** (Servidores, armazenamento e rede → Software Dell DL4300 → Drivers e downloads → Categoria → Rede → Atualização de driver Broadcom Windows 64bit para adaptadores NetXtrene Ethernet).
4. Conclua a instalação utilizando o assistente de instalação.

Criar o grupo de NICs

 **NOTA:** É recomendável não usar a interface de agrupamento nativa no Windows 2012 Server. O algoritmo de agrupamento é otimizado para tráfego de saída, não para tráfego de entrada. O desempenho em uma carga de trabalho de backup é baixo, mesmo com mais portas de rede no grupo.


Para criar um agrupamento de NICs:

1. Vá para **Iniciar** → **Pesquisar** → **Broadcom Advanced Control Suite**.

 **NOTA:** Quando usar o Broadcom Advanced Control Suite, selecione apenas as placas de rede da Broadcom.
2. No **Broadcom Advanced Control Suite**, selecione **Teams (Grupos)** → **Go to Team View (Ir para a exibição do grupo)**.
3. Na **lista Hosts** à esquerda, clique com o botão direito no nome de host do dispositivo DL4300 e selecione **Create Team** (Criar grupo).

A janela **Broadcom Teaming Wizard** (Assistente de agrupamento da Broadcom) é mostrada.
4. Clique em **Avançar**.
5. Digite um nome para o grupo e clique em **Next** (Avançar).
6. Selecione **Team Type** (Tipo de grupo) e clique em **Next** (Avançar).
7. Selecione o adaptador que você quer que faça parte do grupo e clique em **Add** (Adicionar).

8. Repita esse procedimento para todos os outros adaptadores que fazem parte do grupo.
9. Depois de selecionar todos os adaptadores do grupo, clique em **Next** (Avançar).
10. Selecione um NIC reserva se você quiser que um NIC possa ser usado como o NIC padrão em caso de falha do grupo.
11. Selecione se quer configurar o **LiveLink** e clique em **Next** (Avançar).
12. Selecione **Skip Manage VLAN** (Ignorar o gerenciamento de VLAN) e clique em **Next** (Avançar).
13. Selecione **Commit changes to system** (Confirmar as alterações no sistema) e clique em **Finish** (Concluir).
14. Clique em **Yes** (Sim) ao ser avisado de que a conexão de rede será interrompida.

 **NOTA:** A criação do grupo pode levar cerca de cinco minutos.

Configurar um comutador virtual Hyper-V

Para as máquinas de espera virtual se comunicarem dentro de um ambiente de produção, crie um comutador virtual. Para criar um comutador virtual externo, consulte a seção *Configurar redes virtuais* no site www.technet.microsoft.com.

Instalar agentes nos clientes

Cada cliente com backup feito pelo dispositivo AppAssure precisa ter o agente do AppAssure instalado. O Core Console possibilita que você implemente os agentes nas máquinas. A implementação dos agentes nas máquinas exige a pré-configuração de parâmetros para selecionar um tipo único de agente a ser instalado nos clientes. Esse método funciona bem se todos os clientes estiverem rodando o mesmo sistema operacional. Entretanto, caso haja versões diferentes de sistemas operacionais, talvez seja mais fácil instalar os agentes diretamente nas máquinas.

Você pode também implementar o software do agente na máquina do agente durante o processo de proteção da máquina. Essa opção está disponível para máquinas que ainda estão sem o software do agente instalado. Para obter mais informações sobre a implementação do software do agente durante a proteção da máquina, consulte *Dell DL4300 Appliance User's Guide* (Guia do Usuário do Dispositivo Dell DL4300), disponível no site dell.com/support/home.

Instalar agentes remotamente (instalação forçada)

Para instalar os agentes remotamente (instalação forçada):

1. Se o cliente estiver rodando uma versão do sistema operacional mais antiga que o Windows Server 2012, verifique se o cliente tem o Microsoft .NET Framework 4 instalado:
 - a. No cliente, inicie o **Windows Server Manager**.
 - b. Clique em **Configuração** → **Serviços**.
 - c. Confirme que o Microsoft .NET Framework aparece na lista de serviços.
Se não estiver instalado, você pode obter uma cópia de instalação no site microsoft.com.
2. Confirme ou altere o caminho para os pacotes de instalação do agente:
 - a. No AppAssure Core Console, clique na guia **Configuration** (Configuração) e, em seguida, clique em **Settings** (Configurações) no painel esquerdo.
 - b. Na área **Deploy Settings** (Configurações de implementação), clique em **Change** (Alterar).
 - c. Preencha as seguintes informações sobre a localização do agente:

Campo	Descrição
Agent Installer Name (Nome do instalador do agente)	Especifica o caminho exato até a folder\file do agente.
Core Address (Endereço do núcleo)	Especifica o endereço IP do dispositivo onde o AppAssure Core está sendo executado.

Campo

Descrição



NOTA: Por padrão, o campo **Core Address** (Endereço do núcleo) está em branco. O campo **Core Address** (Endereço do núcleo) não precisa de um endereço IP, pois os arquivos de instalação estão instalados no dispositivo.

d. Clique em **OK**.

3. Clique na guia **Tools** (Ferramentas) e, em seguida, clique em **Bulk Deploy** (Implementação em massa) no painel esquerdo.



NOTA: Se o cliente já tiver um agente instalado, o programa de instalação verificará a versão do agente. Se o agente que você está tentando instalar for mais recente do que a versão instalada, o programa de instalação oferecerá fazer o upgrade do agente. Se a versão atual do agente estiver instalada no host, a implementação em lote iniciará a proteção entre o AppAssure Core e o agente.

4. Na lista de clientes, selecione todos os clientes e clique em **Verify** (Verificar) para confirmar que a máquina está ativa e o agente pode ser implementado.
5. Quando a coluna **Message** (Mensagem) confirmar que a máquina está pronta, clique em **Deploy** (Implementar).
6. Para monitorar o status da implementação, selecione a guia **Events** (Eventos).
Depois de o agente ser implementado, um backup do cliente será iniciado automaticamente.

Implementar o software do agente ao proteger um agente

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




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


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

1. Na caixa de diálogo **Protect Machine** (Proteger máquina) → **Connect** (Conectar), depois de digitar as configurações adequadas de conexão, clique em **Connect** (Conectar).
A caixa de diálogo **Deploy Agent** (Implementar agente) é mostrada.
2. Clique em **Yes** (Sim) para implementar remotamente o software do agente na máquina.
A caixa de diálogo **Deploy Agent** (Implementar agente) é mostrada.
3. Digite as configurações de proteção e logon da seguinte forma:
 - **Host name** (Nome de host) — Especifica o nome de host ou o endereço IP da máquina que você quer proteger.
 - **Port** (Porta) — Especifica o número da porta na qual o AppAssure Core se comunica com o agente na máquina. O valor padrão é 8006.
 - **User name** (Nome de usuário) — Especifica o nome de usuário usado para se conectar a esta máquina; por exemplo, administrador.
 - **Password** (Senha) — Especifica a senha usada para se conectar a esta máquina.
 - **Display name** (Nome de exibição) — Especifica um nome para a máquina que aparece no Core Console. O nome de exibição pode ser igual ao nome de host.

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

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

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

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

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

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

Instalar agentes do Microsoft Windows no cliente

Para instalar os agentes:

1. Verifique se o Microsoft .NET4 Framework está instalado no cliente:
 - a. No cliente, inicie o **Windows Server Manager**.
 - b. Clique em **Configuração** → **Serviços**.
 - c. Confirme que o Microsoft .NET Framework aparece na lista de serviços.
Se não estiver instalado, é possível obter uma cópia em **microsoft.com**.
2. Instalar o agente:
 - a. No dispositivo AppAssure, compartilhe o diretório **C: \install\AppAssure** com o(s) cliente(s) dos quais você planeja fazer backup.
 - b. No sistema do cliente, mapeie uma unidade para **C: \install\AppAssure** no dispositivo AppAssure.
 - c. No sistema do cliente, abra o diretório **C:\install\AppAssure** e clique duas vezes no agente correto para que o sistema do cliente inicie a instalação.

Adicionar um agente usando o portal de licenças

 **NOTA:** Você precisa ter privilégios de administrador para fazer download e adicionar agentes.


Para adicionar um agente:


1. Na página **inicial do Portal de licenças do AppAssure**, selecione um grupo e, em seguida, clique em **Download Agent** (Fazer download do agente).
A caixa de diálogo **Download Agent** (Fazer download do agente) é mostrada.
2. Clique no botão **Download** (Fazer download) que está ao lado da versão do instalador que você quer obter por download.

Você pode escolher entre:

- Instalador para Windows 32 bits


- Instalador para Windows 64 bits
- Instalador para Linux Red Hat Enterprise 6.3, 6.4 32 bits
- Instalador para Linux Red Hat Enterprise 6.3, 6.4 64 bits
- Instalador para CentOS 6.3, 6.4 32 bits
- Instalador para CentOS 6.3, 6.4 64 bits
- Instalador para Ubuntu LTS 12.04 13.04 32 bits
- Instalador para Ubuntu LTS 12.04 13.04 64 bits
- Instalador para SUSE Linux Enterprise Server 11 SP2, SP3 32 bits
- Instalador para SUSE Linux Enterprise Server 11 SP2, SP3 64 bits
- Microsoft Hyper-V Server 2012

 **NOTA:** Oferecemos suporte para essas distribuições do Linux e testamos na maioria das versões de kernel liberadas.

 **NOTA:** Os agentes instalados no Microsoft Hyper-V Server 2012 funcionam no modo Core Edition do Windows Server 2012.


O arquivo do **agente** é obtido por download.

3. Clique em **Run** (Executar) na caixa de diálogo **Installer** (Instalador).

 **NOTA:** Para obter mais informações sobre como adicionar agentes usando a máquina do Núcleo, consulte o tópico "Deploying An Agent (Push Install)" (Implementar um agente (Instalação forçada)) no *Dell DL4300 Appliance User's Guide* (Guia do Usuário do Dispositivo Dell DL4000) disponível em dell.com/support/home.

Instalar agentes em máquinas Linux

Faça o download do instalador de 32 bits ou 64 bits específico para a sua distribuição em todos os servidores Linux que você quer proteger usando o AppAssure Core. Você pode fazer o download dos instaladores a partir do Portal de licenças do AppAssure Core em <https://licenseportal.com>. Para obter mais informações, consulte [Adicionar um agente usando o portal de licenças](#).

 **NOTA:** No Linux, a segurança em torno da proteção de uma máquina é baseada no módulo de autenticação conectável (PAM - Pluggable Authentication Module). Após um usuário ser autenticado usando **libpam**, o usuário só será autorizado a proteger a máquina se ele estiver em um dos grupos a seguir:


- sudo
- admin
- appassure
- wheel


Para obter informações sobre como proteger uma máquina, consulte a seção "Protecting a Machine" (Proteger uma máquina) no *Dell DL4300 Appliance User's Guide* (Guia do Usuário do Dispositivo Dell DL4000) disponível em dell.com/support/home.

As instruções de instalação podem ser diferentes dependendo da distribuição do Linux que você está usando. Para obter mais informações sobre como instalar o agente para Linux em sua distribuição, consulte os tópicos a seguir:

- [Instalar o agente no Ubuntu](#)

- [Instalar o agente no Red Hat Enterprise Linux e CentOS](#)
- [Instalar o agente no SUSE Linux Enterprise Server](#)

 **NOTA:** Oferecemos suporte para essas distribuições do Linux e testamos na maioria das versões de kernel liberadas.

 **NOTA:** A instalação do agente para Linux substitui todas as regras de firewall aplicadas através de UFW, Yast2 ou **system-config-firewall**.

Caso você tenha adicionado regras de firewall manualmente, será necessário adicionar as portas do AppAssure manualmente após a instalação. Um backup das regras existentes será gravado em **/var/lib/appassure/backup.fwl**.

Para que o AppAssure Core consiga acessar os agentes, você precisará adicionar exceções de firewall em todos os servidores que estiverem executando o agente do AppAssure através das portas TCP 8006 e 8009.

Localização dos arquivos de um agente Linux

Os arquivos do agente Linux estão localizados nos seguintes diretórios para todas as distribuições:

Componente	Local/Caminho
mono	/opt/appassure/mono
agent	/opt/appassure/aagent
aamount	/opt/appassure/amount
aavdisk e aavdctl	/usr/bin
arquivos de configuração para aavdisk	/etc/appassure/aavdisk.conf
wrappers para aamount e agent	<ul style="list-style-type: none"> • /usr/bin/aamount • /usr/bin/aagent
scripts autorun para aavdisk e agent	<ul style="list-style-type: none"> • /etc/init.d/appassure-agent • /etc/init.d/appassure-avdisk

Dependências do agente

As dependências a seguir são obrigatórias e são instaladas como parte do pacote do instalador do agente:

Para Ubuntu	Dependência
O appassure-vss exige	dkms, gcc, make, linux-headers-`uname-r`
O appassure-aavdisk exige	libc6 (> = 2.7-18), libblkid1, libpam0g, libpcre3

Para Ubuntu Dependência

O `appassure-mono` exige `libc6 (> = 2.7-18)`

Para Red Hat Enterprise Linux e CentOS Dependência

O `nbd-dkms` exige `dkms, gcc, make, kernel-headers-`uname-r` kernel-devel-`uname-r``

O `appassure-vss` exige `dkms, gcc, make, kernel-headers-`uname-r` kernel-devel-`uname-r``

O `appassure-aavdisk` exige `nbd-dkms, libblkid, pam, pcre`

O `appassure-mono` exige `glibc >=2.11`

Para SUSE Linux Enterprise Server Dependência


O `nbd-dkms` exige `dkms, gcc, make, kernel-syms`

O `appassure-vss` exige `dkms, kernel-syms, gcc, make`

O `appassure-aavdisk` exige `libblkid1, pam, pcre`

O `appassure-mono` exige `glibc >= 2.11`


Instalar o agente no Ubuntu

 **NOTA:** Antes de executar este procedimento, confirme que você fez o download do pacote do instalador específico do Ubuntu para `/home/system directory`.

Para instalar o agente do AppAssure no Ubuntu:


1. Abra uma sessão de terminal com acesso à raiz.
2. Para tornar o instalador do AppAssure Agent executável, digite o seguinte comando:
`chmod +x appassure-installer_ubuntu_amd64_5.x.x.xxxxx.sh` e, em seguida, pressione <Enter>.

O arquivo se torna executável.

 **NOTA:** Para ambientes de 32 bits, o nome do instalador é `appassureinstaller_ubuntu_i386_5.x.x.xxxxx.sh`


3. Para extrair e instalar o AppAssure Agent, digite o seguinte comando:
`/appassure-installer_ubuntu_amd64_5.x.x.xxxxx.sh` e, em seguida, pressione <Enter>.

O agente para Linux inicia o processo de extração e instalação. Todos os pacotes ou arquivos ausentes que o agente precisar serão obtidos por download e instalados automaticamente como parte do script.

 **NOTA:** Para obter informações sobre os arquivos que o agente precisa, consulte [Dependências do agente](#).


Depois de o instalador terminar, o agente estará em execução na máquina. Para obter mais informações sobre como proteger esta máquina com o Núcleo, consulte a seção "Protecting Workstations and Servers" (Proteger estações de trabalho e servidores) no *Dell DL4300 Appliance User's Guide* (Guia do Usuário do Dispositivo Dell DL4000) disponível em dell.com/support/home.

Instalar o agente no Red Hat Enterprise Linux ou no CentOS

 **NOTA:** Antes de executar este procedimento, certifique-se de obter por download o pacote do instalador para Red Hat ou CentOS e de colocá-lo em `/home/system directory`. O procedimento a seguir é igual para ambientes de 32 bits e 64 bits.

Para instalar um agente no Red Hat Enterprise Linux ou no CentOS:

1. Abra uma sessão de terminal com acesso à raiz.
2. Para tornar o instalador do AppAssure Agent executável, digite o seguinte comando:
`chmod +x appassure-installer__rhel_amd64_5.x.x.xxxxx.sh` e, em seguida, pressione <Enter>.

 **NOTA:** Para ambientes de 32 bits, o nome do instalador é `appassureinstaller__rhel_i386_5.x.x.xxxxx.sh`.

O arquivo se torna executável.


3. Para extrair e instalar o AppAssure Agent, digite o seguinte comando:
`/appassure-installer__rhel_amd64_5.x.x.xxxxx.sh` e, em seguida, pressione <Enter>.

O agente para Linux inicia seu processo de extração e instalação. Todos os pacotes ou arquivos ausentes que o agente precisar serão obtidos por download e instalados automaticamente como parte do script.

Para obter informações sobre os arquivos que o agente precisa, consulte [Dependências do agente](#).

Após o instalador terminar, o agente estará em execução na máquina. Para obter mais informações sobre como proteger esta máquina com o Núcleo, consulte a seção "Protecting Workstations and Servers" (Proteger estações de trabalho e servidores) no *Dell DL4300 Appliance User's Guide* (Guia do Usuário do Dispositivo Dell DL4000) disponível em dell.com/support/home.

Instalar o agente no SUSE Linux Enterprise Server

 **NOTA:** Antes de executar este procedimento, certifique-se de obter por download o pacote do instalador para SUSE Linux Enterprise Server (SLES) e de colocá-lo em `/home/system directory`. O procedimento a seguir é igual para ambientes de 32 bits e 64 bits.

Para instalar o agente no SLES:

1. Abra uma sessão de terminal com acesso à raiz.
2. Para tornar o instalador do AppAssure Agent executável, digite o seguinte comando:

`chmod +x appassure-installer_sles_amd64_5.x.x.xxxxx.sh` e, em seguida, pressione <Enter>.



NOTA: Para ambientes de 32 bits, o nome do instalador é `appassureinstaller_sles_i386_5.x.x.xxxxx.sh`

O arquivo se torna executável.

3. Para extrair e instalar o AppAssure Agent, digite o seguinte comando:

`/appassure-installer_sles_amd64_5.x.x.xxxxx.sh` e, em seguida, pressione <Enter>.

O agente para Linux inicia seu processo de extração e instalação. Todos os pacotes ou arquivos ausentes que o agente precisar serão obtidos por download e instalados automaticamente como parte do script.

Para obter informações sobre os arquivos que o agente precisa, consulte [Dependências do agente](#).

4. Quando for solicitado instalar os novos pacotes, digite `y` e pressione <Enter>.

O sistema conclui o processo de instalação.

Depois de o instalador terminar, o agente estará em execução na máquina. Para obter mais informações sobre como proteger esta máquina com o Núcleo, consulte a seção "Protecting Workstations and Servers" (Proteger estações de trabalho e servidores) no *Dell DL4300 Appliance User's Guide* (Guia do Usuário do Dispositivo Dell DL4000) disponível em dell.com/support/home.

Obter ajuda


Localizar a documentação e as atualizações de software

No console do AppAssure Core, há links diretos para a documentação do Dispositivo AppAssure e as atualizações do software. Para acessar os links, clique na guia **Appliance** (Dispositivo) e, em seguida, clique em **Overall Status** (Status geral). Os links para as atualizações de software e a documentação estão localizados na seção **Documentação**.

Encontrar atualizações de software

Há links diretos para atualizações de software do AppAssure e do Dispositivo DL4300 disponíveis no AppAssure 5 Core Console. Para acessar os links de atualizações de software, selecione a guia **Appliance** (Dispositivo) e, em seguida, clique em **Overall Status** (Status geral). Os links para as atualizações de software estão localizados na seção **Documentation** (Documentação).

Como entrar em contato com a Dell

 **NOTA:** Se não tiver uma conexão Internet ativa, você pode encontrar as informações de contato na sua fatura, nota de expedição, nota de compra ou no catálogo de produtos Dell.

A Dell fornece várias opções de serviço e atendimento on-line e por telefone. Se não tiver uma conexão de Internet ativa, você pode encontrar as informações de contato na sua fatura, nota de expedição, nota fiscal ou catálogo de produtos Dell. A disponibilidade varia de acordo com o país e o produto, e alguns serviços podem não estar disponíveis na sua região. Para entrar em contato com a Dell para tratar de assuntos de vendas, suporte técnico ou serviço de atendimento ao cliente, acesse software.dell.com/support.

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.