



# **Instalar o plug-in SnapCenter para sistemas de arquivos Unix**

## SnapCenter software

NetApp

November 06, 2025

This PDF was generated from [https://docs.netapp.com/pt-br/snapcenter-61/protect-scu/reference\\_prerequisites\\_for\\_adding\\_hosts\\_and\\_installing\\_snapcenter\\_plug\\_ins\\_package\\_for\\_linux.html](https://docs.netapp.com/pt-br/snapcenter-61/protect-scu/reference_prerequisites_for_adding_hosts_and_installing_snapcenter_plug_ins_package_for_linux.html) on November 06, 2025. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Índice

Instalar o plug-in SnapCenter para sistemas de arquivos Unix .....	1
Pré-requisitos para adicionar hosts e instalar o pacote de plug-ins para Linux.....	1
Requisitos do host Linux .....	1
Adicionar hosts e instalar o pacote de plug-ins para Linux usando a GUI .....	2
Monitorar o status da instalação .....	4
Configurar o serviço SnapCenter Plug-in Loader .....	5
Configurar certificado CA com o serviço SnapCenter Plug-in Loader (SPL) no host Linux.....	8
Gerenciar senha para keystore SPL e alias do par de chaves assinadas pela CA em uso .....	8
Configurar certificados raiz ou intermediários para armazenamento confiável SPL .....	9
Configurar o par de chaves assinadas pela CA para o armazenamento confiável SPL .....	10
Configurar lista de revogação de certificados (CRL) para SPL .....	11
Habilitar certificados CA para plug-ins .....	11

# Instalar o plug-in SnapCenter para sistemas de arquivos Unix

## Pré-requisitos para adicionar hosts e instalar o pacote de plug-ins para Linux

Antes de adicionar um host e instalar o pacote de plug-ins para Linux, você deve atender a todos os requisitos.

- Se você estiver usando iSCSI, o serviço iSCSI deverá estar em execução.
- Você pode usar a autenticação baseada em senha para o usuário root ou não root ou a autenticação baseada em chave SSH.

O plug-in SnapCenter para sistemas de arquivos Unix pode ser instalado por um usuário não root. No entanto, você deve configurar os privilégios sudo para que o usuário não root instale e inicie o processo do plug-in. Após instalar o plug-in, os processos serão executados como um usuário não root.

- Crie credenciais com modo de autenticação como Linux para o usuário de instalação.
- Você deve ter instalado o Java 11 no seu host Linux.



Certifique-se de ter instalado apenas a edição certificada do JAVA 11 no host Linux.

Para obter informações sobre como baixar o JAVA, consulte: "[Downloads Java para todos os sistemas operacionais](#)"

- Você deve ter **bash** como o shell padrão para instalação de plug-ins.

## Requisitos do host Linux

Você deve garantir que o host atenda aos requisitos antes de instalar o Pacote de plug-ins do SnapCenter para Linux.

Item	Requisitos
Sistemas operacionais	<ul style="list-style-type: none"><li>• Red Hat Enterprise Linux</li><li>• Oracle Linux</li><li>• Servidor SUSE Linux Enterprise (SLES)</li></ul>
RAM mínima para o plug-in SnapCenter no host	2 GB

Item	Requisitos
Espaço mínimo de instalação e registro para o plug-in SnapCenter no host	<p>2 GB</p> <p></p> <p>Você deve alocar espaço em disco suficiente e monitorar o consumo de armazenamento pela pasta de logs. O espaço de log necessário varia dependendo do número de entidades a serem protegidas e da frequência das operações de proteção de dados. Se não houver espaço em disco suficiente, os logs não serão criados para as operações executadas recentemente.</p>
Pacotes de software necessários	<p>Java 11 Oracle Java e OpenJDK</p> <p></p> <p>Certifique-se de ter instalado apenas a edição certificada do JAVA 11 no host Linux.</p> <p>Se você atualizou o JAVA para a versão mais recente, certifique-se de que a opção JAVA_HOME localizada em /var/opt/snapcenter/spl/etc/spl.properties esteja definida para a versão correta do JAVA e o caminho correto.</p>

Para obter as informações mais recentes sobre as versões suportadas, consulte o ["Ferramenta de Matriz de Interoperabilidade da NetApp"](#).

## Adicionar hosts e instalar o pacote de plug-ins para Linux usando a GUI

Você pode usar a página Adicionar Host para adicionar hosts e, em seguida, instalar o Pacote de Plug-ins do SnapCenter para Linux. Os plug-ins são instalados automaticamente nos hosts remotos.

### Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Verifique se a aba **Hosts Gerenciados** está selecionada na parte superior.
3. Clique em **Adicionar**.
4. Na página Hosts, execute as seguintes ações:

Para este campo...	Faça isso...
Tipo de host	Selecte <b>Linux</b> como o tipo de host.
Nome do host	<p>Digite o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do host.</p> <p>O SnapCenter depende da configuração correta do DNS. Portanto, a melhor prática é inserir o FQDN.</p> <p>Se você estiver adicionando um host usando o SnapCenter e o host fizer parte de um subdomínio, você deverá fornecer o FQDN.</p>
Credenciais	<p>Selecte o nome da credencial que você criou ou crie novas credenciais.</p> <p>A credencial deve ter direitos administrativos no host remoto. Para obter detalhes, consulte as informações sobre como criar credenciais.</p> <p>Você pode visualizar detalhes sobre as credenciais posicionando o cursor sobre o nome da credencial que você especificou.</p> <p> O modo de autenticação de credenciais é determinado pelo tipo de host especificado no assistente Adicionar Host.</p>

5. Na seção Selecionar plug-ins para instalar, selecione **Sistemas de arquivos Unix**.

6. (Opcional) Clique em **Mais opções**.

Para este campo...	Faça isso...
Porta	<p>Mantenha o número da porta padrão ou especifique o número da porta.</p> <p>O número da porta padrão é 8145. Se o SnapCenter Server foi instalado em uma porta personalizada, esse número de porta será exibido como a porta padrão.</p> <p> Se você instalou manualmente os plug-ins e especificou uma porta personalizada, deverá especificar a mesma porta. Caso contrário, a operação falhará.</p>

Para este campo...	Faça isso...
Caminho de instalação	O caminho padrão é <code>/opt/NetApp/snapcenter</code> . Opcionalmente, você pode personalizar o caminho. Se você usar o caminho personalizado, certifique-se de que o conteúdo padrão dos sudoers seja atualizado com o caminho personalizado.
Ignorar verificações de pré-instalação opcionais	Marque esta caixa de seleção se você já instalou os plug-ins manualmente e não deseja validar se o host atende aos requisitos para instalar o plug-in.

#### 7. Clique em **Enviar**.

Se você não tiver marcado a caixa de seleção Ignorar pré-verificações, o host será validado para verificar se ele atende aos requisitos para instalar o plug-in.



O script de pré-verificação não valida o status do firewall da porta do plug-in se ele estiver especificado nas regras de rejeição do firewall.

Mensagens de erro ou aviso apropriadas serão exibidas se os requisitos mínimos não forem atendidos. Se o erro estiver relacionado ao espaço em disco ou à RAM, você pode atualizar o arquivo web.config localizado em `C:\Program Files\NetApp\ SnapCenter WebApp` para modificar os valores padrão. Se o erro estiver relacionado a outros parâmetros, você deverá corrigir o problema.



Em uma configuração de HA, se você estiver atualizando o arquivo web.config, deverá atualizar o arquivo em ambos os nós.

#### 8. Verifique a impressão digital e clique em **Confirmar e Enviar**.



O SnapCenter não suporta o algoritmo ECDSA.



A verificação de impressão digital é obrigatória mesmo que o mesmo host tenha sido adicionado anteriormente ao SnapCenter e a impressão digital tenha sido confirmada.

#### 9. Monitore o progresso da instalação.

Os arquivos de log específicos da instalação estão localizados em `/custom_location/snapcenter/logs`.

### Resultado

Todos os sistemas de arquivos montados no host são descobertos automaticamente e exibidos na Página de Recursos. Se nada for exibido, clique em **Atualizar recursos**.

### Monitorar o status da instalação

Você pode monitorar o progresso da instalação do pacote de plug-in SnapCenter usando a página Tarefas. Talvez você queira verificar o andamento da instalação para determinar quando ela foi concluída ou se há algum problema.

## Sobre esta tarefa

Os seguintes ícones aparecem na página Trabalhos e indicam o estado da operação:

- Em andamento
- Concluído com sucesso
- Fracassado
- Concluído com avisos ou não pôde ser iniciado devido a avisos
- Na fila

## Passos

1. No painel de navegação esquerdo, clique em **Monitor**.
2. Na página **Monitor**, clique em **Trabalhos**.
3. Na página **Trabalhos**, para filtrar a lista de modo que apenas as operações de instalação de plug-ins sejam listadas, faça o seguinte:
  - a. Clique em **Filtrar**.
  - b. Opcional: especifique a data de início e término.
  - c. No menu suspenso Tipo, selecione **Instalação de plug-in**.
  - d. No menu suspenso Status, selecione o status da instalação.
  - e. Clique em **Aplicar**.
4. Selecione o trabalho de instalação e clique em **Detalhes** para visualizar os detalhes do trabalho.
5. Na página **Detalhes do trabalho**, clique em **Exibir registros**.

## Configurar o serviço SnapCenter Plug-in Loader

O serviço SnapCenter Plug-in Loader carrega o pacote de plug-in para Linux interagir com o SnapCenter Server. O serviço SnapCenter Plug-in Loader é instalado quando você instala o SnapCenter Plug-ins Package para Linux.

## Sobre esta tarefa

Após instalar o pacote de plug-ins do SnapCenter para Linux, o serviço SnapCenter Plug-in Loader é iniciado automaticamente. Se o serviço SnapCenter Plug-in Loader não iniciar automaticamente, você deve:

- Certifique-se de que o diretório onde o plug-in está operando não seja excluído
- Aumentar o espaço de memória alocado à Máquina Virtual Java

O arquivo `spl.properties`, localizado em `/custom_location/NetApp/snapcenter/spl/etc/`, contém os seguintes parâmetros. Valores padrão são atribuídos a esses parâmetros.

Nome do parâmetro	Descrição
NÍVEL_LOG	<p>Exibe os níveis de log suportados.</p> <p>Os valores possíveis são TRACE, DEBUG, INFO, WARN, ERROR e FATAL.</p>
PROTÓCOLO_SPL	<p>Exibe o protocolo suportado pelo SnapCenter Plug-in Loader.</p> <p>Somente o protocolo HTTPS é suportado. Você pode adicionar o valor se o valor padrão estiver faltando.</p>
PROTÓCOLO_DO_SERVIDOR_SNAPCENTER	<p>Exibe o protocolo suportado pelo SnapCenter Server.</p> <p>Somente o protocolo HTTPS é suportado. Você pode adicionar o valor se o valor padrão estiver faltando.</p>
PULAR_ATUALIZAÇÃO_JAVAHOME	<p>Por padrão, o serviço SPL detecta o caminho Java e atualiza o parâmetro JAVA_HOME.</p> <p>Portanto, o valor padrão é definido como FALSE. Você pode definir como TRUE se quiser desabilitar o comportamento padrão e corrigir manualmente o caminho Java.</p>
SPL_KEYSTORE_SENHA	<p>Exibe a senha do arquivo keystore.</p> <p>Você só poderá alterar esse valor se alterar a senha ou criar um novo arquivo de keystore.</p>
PORTA_SPL	<p>Exibe o número da porta na qual o serviço SnapCenter Plug-in Loader está em execução.</p> <p>Você pode adicionar o valor se o valor padrão estiver faltando.</p> <div style="display: flex; align-items: center;"> <span data-bbox="856 1431 910 1501"></span> <span data-bbox="971 1431 1405 1501">Você não deve alterar o valor após instalar os plug-ins.</span> </div>
SNAPCENTER_SERVER_HOST	Exibe o endereço IP ou nome do host do SnapCenter Server.
Caminho_de_keystore_spl	Exibe o caminho absoluto do arquivo keystore.
PORTA_DO_SERVIDOR_SNAPCENTER	Exibe o número da porta na qual o SnapCenter Server está sendo executado.

Nome do parâmetro	Descrição
CONTAGEM_MÁXIMA_DE_LOGS	<p>Exibe o número de arquivos de log do SnapCenter Plug-in Loader que são retidos na pasta <code>/custom_location/snapcenter/spl/logs</code>.</p> <p>O valor padrão é definido como 5000. Se a contagem for maior que o valor especificado, os últimos 5000 arquivos modificados serão retidos. A verificação do número de arquivos é feita automaticamente a cada 24 horas a partir do momento em que o serviço SnapCenter Plug-in Loader é iniciado.</p> <p> Se você excluir manualmente o arquivo <code>spl.properties</code>, o número de arquivos a serem retidos será definido como 9999.</p>
JAVA_HOME	<p>Exibe o caminho absoluto do diretório do <code>JAVA_HOME</code> que é usado para iniciar o serviço SPL.</p> <p>Este caminho é determinado durante a instalação e como parte do início do SPL.</p>
TAMANHO_MÁXIMO_DE_LOG	<p>Exibe o tamanho máximo do arquivo de log do trabalho.</p> <p>Quando o tamanho máximo é atingido, o arquivo de log é compactado e os logs são gravados no novo arquivo daquele trabalho.</p>
RETER_REGISTROS_DOS_ÚLTIMOS_DIAS	<p>Exibe o número de dias até os quais os logs são retidos.</p>
HABILITAR_VALIDAÇÃO_DE_CERTIFICADO	<p>Exibe verdadeiro quando a validação do certificado CA está habilitada para o host.</p> <p>Você pode habilitar ou desabilitar esse parâmetro editando o <code>spl.properties</code> ou usando a GUI ou o cmdlet do SnapCenter .</p>

Se algum desses parâmetros não estiver atribuído ao valor padrão ou se você quiser atribuir ou alterar o valor, você poderá modificar o arquivo `spl.properties`. Você também pode verificar o arquivo `spl.properties` e editá-lo para solucionar quaisquer problemas relacionados aos valores atribuídos aos parâmetros. Depois de modificar o arquivo `spl.properties`, você deve reiniciar o serviço SnapCenter Plug-in Loader .

## Passos

- Execute uma das seguintes ações, conforme necessário:

- Inicie o serviço SnapCenter Plug-in Loader :
  - Como usuário root, execute: `/custom_location/NetApp/snapcenter/spl/bin/spl`

start

- Como usuário não root, execute: sudo  
/custom\_location/NetApp/snapcenter/spl/bin/spl start
- Pare o serviço SnapCenter Plug-in Loader :
  - Como usuário root, execute: /custom\_location/NetApp/snapcenter/spl/bin/spl stop
  - Como usuário não root, execute: sudo  
/custom\_location/NetApp/snapcenter/spl/bin/spl stop



Você pode usar a opção -force com o comando stop para interromper o serviço SnapCenter Plug-in Loader à força. No entanto, você deve ter cuidado antes de fazer isso, pois isso também encerra as operações existentes.

- Reinicie o serviço SnapCenter Plug-in Loader :

- Como usuário root, execute: /custom\_location/NetApp/snapcenter/spl/bin/spl restart
  - Como usuário não root, execute: sudo  
/custom\_location/NetApp/snapcenter/spl/bin/spl restart

- Encontre o status do serviço SnapCenter Plug-in Loader :

- Como usuário root, execute: /custom\_location/NetApp/snapcenter/spl/bin/spl status
  - Como usuário não root, execute: sudo  
/custom\_location/NetApp/snapcenter/spl/bin/spl status

- Encontre a alteração no serviço SnapCenter Plug-in Loader :

- Como usuário root, execute: /custom\_location/NetApp/snapcenter/spl/bin/spl change
  - Como usuário não root, execute: sudo  
/custom\_location/NetApp/snapcenter/spl/bin/spl change

## Configurar certificado CA com o serviço SnapCenter Plug-in Loader (SPL) no host Linux

Você deve gerenciar a senha do keystore SPL e seu certificado, configurar o certificado CA, configurar certificados raiz ou intermediários para o trust-store SPL e configurar o par de chaves assinadas pela CA para o trust-store SPL com o serviço SnapCenter Plug-in Loader para ativar o certificado digital instalado.



O SPL usa o arquivo 'keystore.jks', que está localizado em '/var/opt/snapcenter/spl/etc' como seu armazenamento confiável e armazenamento de chaves.

### Gerenciar senha para keystore SPL e alias do par de chaves assinadas pela CA em uso

#### Passos

1. Você pode recuperar a senha padrão do keystore SPL a partir do arquivo de propriedades SPL.

É o valor correspondente à chave 'SPL\_KEYSTORE\_PASS'.

2. Alterar a senha do keystore:

```
keytool -storepasswd -keystore keystore.jks
```

. Altere a senha de todos os aliases de entradas de chave privada no keystore para a mesma senha usada para o keystore:

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

Atualize o mesmo para a chave SPL\_KEYSTORE\_PASS no arquivo spl.properties.

3. Reinicie o serviço após alterar a senha.



A senha para o keystore SPL e para todas as senhas de alias associadas da chave privada deve ser a mesma.

## Configurar certificados raiz ou intermediários para armazenamento confiável SPL

Você deve configurar os certificados raiz ou intermediários sem a chave privada para o armazenamento confiável SPL.

### Passos

1. Navegue até a pasta que contém o keystore SPL: /var/opt/snapcenter/spl/etc.

2. Localize o arquivo 'keystore.jks'.

3. Listar os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
```

. Adicione um certificado raiz ou intermediário:

```
keytool -import -trustcacerts -alias
<AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. Reinicie o serviço após configurar os certificados raiz ou
intermediários para o armazenamento confiável SPL.
```



Você deve adicionar o certificado da CA raiz e depois os certificados da CA intermediária.

## Configurar o par de chaves assinadas pela CA para o armazenamento confiável SPL

Você deve configurar o par de chaves assinadas pela CA para o armazenamento confiável SPL.

### Passos

1. Navegue até a pasta que contém o keystore do SPL /var/opt/snapcenter/spl/etc.
2. Localize o arquivo 'keystore.jks'.
3. Listar os certificados adicionados no keystore:

```
keytool -list -v -keystore keystore.jks
. Adicione o certificado da CA com chave privada e pública.
```

```
keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Listar os certificados adicionados no keystore.
```

```
keytool -list -v -keystore keystore.jks
. Verifique se o keystore contém o alias correspondente ao novo
certificado CA, que foi adicionado ao keystore.
. Altere a senha da chave privada adicionada para o certificado CA para
a senha do keystore.
```

A senha padrão do keystore SPL é o valor da chave SPL\_KEYSTORE\_PASS no arquivo spl.properties.

```
keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks
. Se o nome do alias no certificado da CA for longo e contiver espaços
ou caracteres especiais ("*, ", "), altere o nome do alias para um nome
simples:
```

```
keytool -changealias -alias "<OriginalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Configure o nome do alias do keystore localizado no arquivo
spl.properties.
```

Atualize este valor em relação à chave SPL\_CERTIFICATE\_ALIAS.

4. Reinicie o serviço após configurar o par de chaves assinadas pela CA para o armazenamento confiável SPL.

## Configurar lista de revogação de certificados (CRL) para SPL

Você deve configurar o CRL para SPL

### Sobre esta tarefa

- O SPL procurará os arquivos CRL em um diretório pré-configurado.
- O diretório padrão para os arquivos CRL do SPL é `/var/opt/snapcenter/spl/etc/crl`.

### Passos

1. Você pode modificar e atualizar o diretório padrão no arquivo `spl.properties` com a chave `SPL_CRL_PATH`.
2. Você pode colocar mais de um arquivo CRL neste diretório.

Os certificados recebidos serão verificados em relação a cada CRL.

## Habilitar certificados CA para plug-ins

Você deve configurar os certificados CA e implantá-los no SnapCenter Server e nos hosts de plug-in correspondentes. Você deve habilitar a validação do certificado CA para os plug-ins.

### Antes de começar

- Você pode habilitar ou desabilitar os certificados da CA usando o cmdlet `run Set-SmCertificateSettings`.
- Você pode exibir o status do certificado para os plug-ins usando `Get-SmCertificateSettings`.

As informações sobre os parâmetros que podem ser usados com o cmdlet e suas descrições podem ser obtidas executando `Get-Help command_name`. Alternativamente, você também pode consultar o "[Guia de referência do cmdlet do software SnapCenter](#)" .

### Passos

1. No painel de navegação esquerdo, clique em **Hosts**.
2. Na página Hosts, clique em **Hosts gerenciados**.
3. Selecione hosts de plug-in únicos ou múltiplos.
4. Clique em **Mais opções**.
5. Selecione **Ativar validação de certificado**.

### Depois que você terminar

A guia Hosts gerenciados exibe um cadeado e a cor do cadeado indica o status da conexão entre o SnapCenter Server e o host do plug-in.

- \* \* indica que o certificado CA não está habilitado nem atribuído ao host do plug-in.
- \* \* indica que o certificado CA foi validado com sucesso.
- \* \* indica que o certificado CA não pôde ser validado.
- \* \* indica que as informações de conexão não puderam ser recuperadas.



Quando o status é amarelo ou verde, as operações de proteção de dados foram concluídas com sucesso.

## **Informações sobre direitos autorais**

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

**ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTE DOCUMENTO. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTE SOFTWARE, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.**

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

**LEGENDA DE DIREITOS LIMITADOS:** o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

## **Informações sobre marcas comerciais**

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.