



# Configurar o gerenciamento de chaves externas

ONTAP 9

NetApp  
January 17, 2025

# Índice

- Configurar o gerenciamento de chaves externas ..... 1
  - Configurar uma visão geral do gerenciamento de chaves externas ..... 1
  - Gerencie gerenciadores de chaves externos com o System Manager ..... 1
  - Instale certificados SSL no cluster ..... 3
  - Habilite o gerenciamento de chaves externas no ONTAP 9.6 e versões posteriores (NVE)..... 4
  - Habilite o gerenciamento de chaves externas no ONTAP 9.5 e versões anteriores ..... 7
  - Gerencie chaves com um provedor de nuvem ..... 9

# Configurar o gerenciamento de chaves externas

## Configurar uma visão geral do gerenciamento de chaves externas

Você pode usar um ou mais servidores de gerenciamento de chaves externos para proteger as chaves que o cluster usa para acessar dados criptografados. Um servidor de gerenciamento de chaves externo é um sistema de terceiros em seu ambiente de storage que serve chaves para nós que usam o Key Management Interoperability Protocol (KMIP).



Para o ONTAP 9.1 e versões anteriores, as LIFs de gerenciamento de nós devem ser atribuídas a portas configuradas com a função de gerenciamento de nó antes de usar o gerenciador de chaves externo.

O NetApp volume Encryption (NVE) é compatível com o Gerenciador de chaves integrado no ONTAP 9.1 e posterior. A partir do ONTAP 9.3, o NVE é compatível com gerenciamento de chaves externas (KMIP) e Gerenciador de chaves integrado. A partir do ONTAP 9.10,1, você pode usar [Serviço do Azure Key Vault ou do Google Cloud Key Manager](#) para proteger suas chaves NVE. A partir do ONTAP 9.11,1, você pode configurar vários gerenciadores de chaves externos em um cluster. Consulte [Configurar servidores de chaves em cluster](#).

## Gerencie gerenciadores de chaves externos com o System Manager

A partir do ONTAP 9.7, você pode armazenar e gerenciar chaves de autenticação e criptografia com o Gerenciador de chaves integrado. A partir do ONTAP 9.13,1, você também pode usar gerenciadores de chaves externos para armazenar e gerenciar essas chaves.

O Gerenciador de chaves integrado armazena e gerencia chaves em um banco de dados seguro interno ao cluster. Seu escopo é o cluster. Um gerenciador de chaves externo armazena e gerencia chaves fora do cluster. Seu escopo pode ser o cluster ou a VM de storage. Um ou mais gerenciadores de chaves externos podem ser usados. Aplicam-se as seguintes condições:

- Se o Gerenciador de chaves integrado estiver habilitado, um gerenciador de chaves externo não poderá ser habilitado no nível do cluster, mas poderá ser habilitado no nível da VM de armazenamento.
- Se um gerenciador de chaves externo estiver habilitado no nível do cluster, o Gerenciador de chaves integrado não poderá ser habilitado.

Ao usar gerenciadores de chaves externos, você pode Registrar até quatro servidores de chaves primárias por VM de armazenamento e cluster. Cada servidor de chave primária pode ser agrupado com até três servidores de chaves secundárias.

## Configurar um gerenciador de chaves externo



Para adicionar um gerenciador de chaves externo para uma VM de armazenamento, você deve adicionar um gateway opcional ao configurar a interface de rede para a VM de armazenamento. Se a VM de



armazenamento foi criada sem a rota de rede, você terá que criar a rota explicitamente para o gerenciador de chaves externo. "[Criar um LIF \(interface de rede\)](#)" Consulte .

## Passos

Você pode configurar um gerenciador de chaves externo a partir de diferentes locais no System Manager.

1. Para configurar um gerenciador de chaves externo, execute um dos seguintes passos iniciais.

Fluxo de trabalho	Navegação	Etapa inicial
Configure o Gerenciador de chaves	<b>Cluster &gt; Settings</b>	Role até a seção <b>Segurança</b> . Em <b>criptação</b> ,  selecione . Selecione <b>External Key Manager</b> .
Adicionar nível local	<b>Armazenamento &gt; camadas</b>	Selecione * Adicionar nível local*. Marque a caixa de seleção "Configurar Gerenciador de chaves". Selecione <b>External Key Manager</b> .
Prepare o armazenamento	<b>Painel</b>	Na seção <b>capacidade</b> , selecione <b>preparar armazenamento</b> . Em seguida, selecione "Configure Key Manager". Selecione <b>External Key Manager</b> .
Configurar a criptografia (gerenciador de chaves somente no escopo da VM de storage)	<b>Storage &gt; Storage VMs</b>	Selecione a VM de armazenamento. Selecione a guia <b>Configurações</b> . Na seção <b>criptografia</b> em <b>Segurança</b> ,  selecione .



2. Para adicionar um servidor de chave primária, selecione **+ Add** e preencha os campos **Endereço IP ou Nome do host** e **porta**.
3. Os certificados instalados existentes são listados nos campos **certificados KMIP Server CA** e **KMIP Client Certificate**. Você pode executar qualquer uma das seguintes ações:
  -  Selecione para selecionar os certificados instalados que pretende mapear para o gestor de chaves. (Podem ser selecionados vários certificados de CA de serviço, mas apenas um certificado de cliente pode ser selecionado.)
  - Selecione **Adicionar novo certificado** para adicionar um certificado que ainda não tenha sido instalado e mapeie-o para o gerenciador de chaves externo.
  -  Selecione ao lado do nome do certificado para excluir os certificados instalados que você não deseja mapear para o gerenciador de chaves externo.
4. Para adicionar um servidor de chaves secundário, selecione **Add** na coluna **Secondary Key Servers** e forneça seus detalhes.
5. Selecione **Save** para concluir a configuração.


## Editar um gerenciador de chaves externo existente

Se você já tiver configurado um gerenciador de chaves externo, poderá modificar suas configurações.

## Passos

1. Para editar a configuração de um gerenciador de chaves externo, execute um dos seguintes passos iniciais.

Âmbito de aplicação	Navegação	Etapa inicial
Gerenciador de chaves externo do escopo do cluster	<b>Cluster &gt; Settings</b>	Role até a seção <b>Segurança</b> . Em <b>Encryption</b> ,  selecione e, em seguida, selecione <b>Edit External Key Manager</b> .
Gerenciador de chaves externo de escopo da VM de storage	<b>Storage &gt; Storage VMs</b>	Selecione a VM de armazenamento. Selecione a guia <b>Configurações</b> . Na seção <b>criptografia</b> em <b>Segurança</b> ,  selecione e selecione <b>Editar Gerenciador de chaves externas</b> .



- Os servidores de chave existentes estão listados na tabela **Key Servers**. Você pode executar as seguintes operações:
  - Adicione um novo servidor de chaves selecionando **+ Add**.
  - Exclua um servidor de chaves selecionando  no final da célula da tabela que contém o nome do servidor de chaves. Os servidores de chave secundária associados a esse servidor de chave primária também são removidos da configuração.

## Excluir um gerenciador de chaves externo

Um gerenciador de chaves externo pode ser excluído se os volumes não forem criptografados.

### Passos

- Para excluir um gerenciador de chaves externo, execute uma das etapas a seguir.

Âmbito de aplicação	Navegação	Etapa inicial
Gerenciador de chaves externo do escopo do cluster	<b>Cluster &gt; Settings</b>	Role até a seção <b>Segurança</b> . Em <b>Encryption</b> , selecione  e, em seguida, selecione <b>Delete External Key Manager</b> .
Gerenciador de chaves externo de escopo da VM de storage	<b>Storage &gt; Storage VMs</b>	Selecione a VM de armazenamento. Selecione a guia <b>Configurações</b> . Na seção <b>criptografia</b> em <b>Segurança</b> ,  selecione e selecione <b>Excluir Gerenciador de chaves externas</b> .

## Instale certificados SSL no cluster

O cluster e o servidor KMIP usam certificados SSL KMIP para verificar a identidade uns dos outros e estabelecer uma conexão SSL. Antes de configurar a conexão SSL com o servidor KMIP, você deve instalar os certificados SSL do cliente KMIP para o cluster e o certificado público SSL para a autoridade de certificação raiz (CA) do servidor KMIP.

### Sobre esta tarefa

Em um par de HA, ambos os nós precisam usar os mesmos certificados KMIP SSL públicos e privados. Se você conectar vários pares de HA ao mesmo servidor KMIP, todos os nós dos pares de HA precisarão usar os mesmos certificados KMIP SSL públicos e privados.

## Antes de começar

- O tempo deve ser sincronizado no servidor criando os certificados, o servidor KMIP e o cluster.
- Você deve ter obtido o certificado de cliente KMIP SSL público para o cluster.
- Você deve ter obtido a chave privada associada ao certificado de cliente SSL KMIP para o cluster.
- O certificado de cliente SSL KMIP não deve ser protegido por senha.
- Você deve ter obtido o certificado público SSL para a autoridade de certificação raiz (CA) do servidor KMIP.
- Em um ambiente MetroCluster, é necessário instalar os mesmos certificados SSL KMIP em ambos os clusters.



Você pode instalar os certificados de cliente e servidor no servidor KMIP antes ou depois de instalar os certificados no cluster.

## Passos

1. Instale os certificados de cliente SSL KMIP para o cluster:

```
security certificate install -vserver admin_svm_name -type client
```

Você será solicitado a inserir os certificados SSL KMIP público e privado.

```
cluster1::> security certificate install -vserver cluster1 -type client
```

2. Instale o certificado público SSL para a autoridade de certificação raiz (CA) do servidor KMIP:

```
security certificate install -vserver admin_svm_name -type server-ca
```

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
```

## Habilite o gerenciamento de chaves externas no ONTAP 9.6 e versões posteriores (NVE)

Você pode usar um ou mais servidores KMIP para proteger as chaves que o cluster usa para acessar dados criptografados. A partir do ONTAP 9.6, você tem a opção de configurar um gerenciador de chaves externo separado para proteger as chaves que um SVM de dados usa para acessar dados criptografados.

A partir do ONTAP 9.11,1, você pode adicionar até 3 servidores de chaves secundárias por servidor de chaves primárias para criar um servidor de chaves em cluster. Para obter mais informações, [Configurar servidores de chaves externas em cluster](#) consulte .

### Sobre esta tarefa

É possível conectar até quatro servidores KMIP a um cluster ou SVM. Recomenda-se um mínimo de dois servidores para redundância e recuperação de desastres.

O escopo do gerenciamento de chaves externas determina se os servidores de gerenciamento de chaves protegem todos os SVMs no cluster ou somente SVMs selecionadas:

- Você pode usar um *cluster scope* para configurar o gerenciamento de chaves externas para todos os

SVMs no cluster. O administrador do cluster tem acesso a todas as chaves armazenadas nos servidores.

- A partir do ONTAP 9.6, você pode usar um *escopo SVM* para configurar o gerenciamento de chaves externas para um SVM de dados no cluster. Isso é melhor para ambientes com alocação a vários clientes nos quais cada locatário usa um SVM diferente (ou conjunto de SVMs) para fornecer dados. Somente o administrador do SVM de um determinado locatário tem acesso às chaves desse locatário.
- Para ambientes multitenant, instale uma licença para *MT\_EK\_MGMT* usando o seguinte comando:

```
system license add -license-code <MT_EK_MGMT license code>
```

Para obter a sintaxe de comando completa, consulte a página man para o comando.

Você pode usar ambos os escopos no mesmo cluster. Se os servidores de gerenciamento de chaves tiverem sido configurados para um SVM, o ONTAP usará apenas esses servidores para proteger chaves. Caso contrário, o ONTAP protege as chaves com os servidores de gerenciamento de chaves configurados para o cluster.

Você pode configurar o gerenciamento de chaves integradas no escopo do cluster e o gerenciamento de chaves externas no escopo da SVM. Você pode usar o `security key-manager key migrate` comando para migrar chaves do gerenciamento de chaves integradas no escopo do cluster para gerenciadores de chaves externos no escopo da SVM.

### Antes de começar

- Os certificados de cliente e servidor KMIP SSL devem ter sido instalados.
- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.
- Para habilitar o gerenciamento de chaves externas para um ambiente MetroCluster, o MetroCluster deve estar totalmente configurado antes de habilitar o gerenciamento de chaves externas.
- Em um ambiente MetroCluster, é necessário instalar o mesmo certificado KMIP SSL em ambos os clusters.

### Passos

1. Configurar a conectividade do gerenciador de chaves para o cluster:

```
security key-manager external enable -vserver admin_SVM -key-servers  
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert  
server_CA_certificates
```



- O `security key-manager external enable` comando substitui o `security key-manager setup` comando. Se você executar o comando no prompt de login do cluster, *admin\_SVM* o padrão será o administrador SVM do cluster atual. Você deve ser o administrador do cluster para configurar o escopo do cluster. Você pode executar o `security key-manager external modify` comando para alterar a configuração de gerenciamento de chaves externas.
- Em um ambiente MetroCluster, se você estiver configurando o gerenciamento de chaves externas para o SVM de administrador, repita o `security key-manager external enable` comando no cluster de parceiros.

O comando a seguir habilita o gerenciamento de chaves externas para `cluster1` com três servidores de chaves externas. O primeiro servidor de chaves é especificado usando seu nome de host e porta, o segundo é especificado usando um endereço IP e a porta padrão, e o terceiro é especificado usando um endereço IPv6 e porta:

```
cluster1::> security key-manager external enable -vserver cluster1 -key
-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

## 2. Configurar um gerenciador de chaves e uma SVM:

```
security key-manager external enable -vserver SVM -key-servers
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
server_CA_certificates
```



- Se você executar o comando no prompt de login SVM, SVM o padrão será SVM atual. Você precisa ser um administrador de cluster ou SVM para configurar o escopo do SVM. Você pode executar o `security key-manager external modify` comando para alterar a configuração de gerenciamento de chaves externas.
- Em um ambiente MetroCluster, se você estiver configurando o gerenciamento de chaves externas para um SVM de dados, não será necessário repetir o `security key-manager external enable` comando no cluster de parceiros.

O comando a seguir habilita o gerenciamento de chaves externas para `svm1` que um servidor de chave única esteja escutando na porta padrão 5696:

```
svm11::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

## 3. Repita a última etapa para quaisquer SVMs adicionais.



Você também pode usar o `security key-manager external add-servers` comando para configurar SVMs adicionais. O `security key-manager external add-servers` comando substitui o `security key-manager add` comando. Para obter a sintaxe completa do comando, consulte a página man.

## 4. Verifique se todos os servidores KMIP configurados estão conectados:

```
security key-manager external show-status -node node_name
```



O `security key-manager external show-status` comando substitui o `security key-manager show -status` comando. Para obter a sintaxe completa do comando, consulte a página man.



```

cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                     Status
----  -
-----
node1
  svm1
    keyserver.svm1.com:5696                     available
  cluster1
    10.0.0.10:5696                               available
    fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234 available
    ks1.local:15696                              available
node2
  svm1
    keyserver.svm1.com:5696                     available
  cluster1
    10.0.0.10:5696                               available
    fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234 available
    ks1.local:15696                              available

8 entries were displayed.

```

5. Opcionalmente, converta volumes de texto simples em volumes criptografados.

```
volume encryption conversion start
```

Um gerenciador de chaves externo deve estar totalmente configurado antes de converter os volumes. Em um ambiente MetroCluster, um gerenciador de chaves externo deve ser configurado em ambos os locais.

## Habilite o gerenciamento de chaves externas no ONTAP 9.5 e versões anteriores

Você pode usar um ou mais servidores KMIP para proteger as chaves que o cluster usa para acessar dados criptografados. É possível conectar até quatro servidores KMIP a um nó. Recomenda-se um mínimo de dois servidores para redundância e recuperação de desastres.

### Sobre esta tarefa

O ONTAP configura a conectividade do servidor KMIP para todos os nós no cluster.

### Antes de começar

- Os certificados de cliente e servidor KMIP SSL devem ter sido instalados.
- Você deve ser um administrador de cluster para executar esta tarefa.
- Você deve configurar o ambiente MetroCluster antes de configurar um gerenciador de chaves externo.

- Em um ambiente MetroCluster, é necessário instalar o mesmo certificado KMIP SSL em ambos os clusters.

## Passos

1. Configurar a conectividade do gerenciador de chaves para nós de cluster:

```
security key-manager setup
```

A configuração do gerenciador de chaves é iniciada.



Em um ambiente MetroCluster, você deve executar esse comando nos dois clusters.

2. Insira a resposta apropriada em cada prompt.
3. Adicionar um servidor KMIP:

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.1
```



Em um ambiente MetroCluster, você deve executar esse comando nos dois clusters.

4. Adicione um servidor KMIP adicional para redundância:

```
security key-manager add -address key_management_server_ipaddress
```

```
cluster1::> security key-manager add -address 20.1.1.2
```



Em um ambiente MetroCluster, você deve executar esse comando nos dois clusters.

5. Verifique se todos os servidores KMIP configurados estão conectados:

```
security key-manager show -status
```

Para obter a sintaxe completa do comando, consulte a página man.

```
cluster1::> security key-manager show -status
```

Node	Port	Registered Key Manager	Status
-----	----	-----	-----
cluster1-01	5696	20.1.1.1	available
cluster1-01	5696	20.1.1.2	available
cluster1-02	5696	20.1.1.1	available
cluster1-02	5696	20.1.1.2	available

6. Opcionalmente, converta volumes de texto simples em volumes criptografados.

```
volume encryption conversion start
```

Um gerenciador de chaves externo deve estar totalmente configurado antes de converter os volumes. Em um ambiente MetroCluster, um gerenciador de chaves externo deve ser configurado em ambos os locais.

## Gerencie chaves com um provedor de nuvem

A partir do ONTAP 9.10,1, você pode usar ["Azure Key Vault \(AKV\)"](#) e ["Serviço de gerenciamento de chaves do Google Cloud Platform \(Cloud KMS\)"](#) proteger suas chaves de criptografia ONTAP em um aplicativo hospedado na nuvem. A partir do ONTAP 9.12,0, também é possível proteger as chaves NVE com ["KMS DA AWS"](#)o .

O AWS KMS, AKV e o Cloud KMS podem ser usados para proteger ["Chaves de criptografia de volume NetApp \(NVE\)"](#) somente SVMs de dados.

### Sobre esta tarefa

O gerenciamento de chaves com um fornecedor de nuvem pode ser habilitado com a CLI ou a API REST do ONTAP.

Ao usar um provedor de nuvem para proteger suas chaves, esteja ciente de que, por padrão, um data SVM LIF é usado para se comunicar com o endpoint de gerenciamento de chaves na nuvem. Uma rede de gerenciamento de nós é usada para se comunicar com os serviços de autenticação do provedor de nuvem (login.microsoftonline.com para Azure; oauth2.googleapis.com para Cloud KMS). Se a rede do cluster não estiver configurada corretamente, o cluster não utilizará adequadamente o serviço de gerenciamento de chaves.

Ao utilizar um serviço de gerenciamento de chaves do provedor de nuvem, você deve estar ciente das seguintes limitações:

- O gerenciamento de chaves do fornecedor de nuvem não está disponível para criptografia de storage NetApp (NSE) e criptografia agregada NetApp (NAE). ["KMIPs externos"](#) pode ser usado em vez disso.
- O gerenciamento de chaves do fornecedor de nuvem não está disponível para configurações do MetroCluster.
- O gerenciamento de chaves do fornecedor de nuvem só pode ser configurado em um data SVM.

### Antes de começar

- Você deve ter configurado o KMS no provedor de nuvem apropriado.
- Os nós do cluster do ONTAP devem ser compatíveis com NVE.
- ["Você deve ter instalado as licenças de criptografia de volume \(VE\) e gerenciamento de chaves de criptografia de vários locatários \(MTEKM\)"](#). Estas licenças estão incluídas no ["ONTAP One"](#).
- Você precisa ser um administrador de cluster ou SVM.
- O SVM não deve incluir volumes criptografados nem empregar um gerenciador de chaves. Se o SVM de dados incluir volumes criptografados, você precisará migrá-los antes de configurar o KMS.

## Ativar o gerenciamento de chaves externas

A ativação do gerenciamento de chaves externas depende do gerenciador de chaves específico que você usa. Escolha a guia do gerenciador de chaves e do ambiente apropriados.

## AWS

### Antes de começar

- Você deve criar uma subvenção para a chave AWS KMS que será usada pela função de gerenciamento de criptografia do IAM. A função IAM deve incluir uma política que permita as seguintes operações:
  - DescribeKey
  - Encrypt
  - Decrypt Para obter mais informações, consulte a documentação da AWS para "[subvenções](#)".

### Habilite o AWS KMS em um SVM do ONTAP

1. Antes de começar, obtenha o ID da chave de acesso e a chave secreta do seu AWS KMS.
2. Defina o nível de privilégio como avançado:  
`set -priv advanced`
3. Habilite o AWS KMS:  
`security key-manager external aws enable -vserver svm_name -region AWS_region -key-id key_ID -encryption-context encryption_context`
4. Quando solicitado, insira a chave secreta.
5. Confirme se o AWS KMS foi configurado corretamente:  
`security key-manager external aws show -vserver svm_name`

## Azure

### Habilite o cofre de chaves do Azure em um SVM do ONTAP

1. Antes de começar, você precisa obter as credenciais de autenticação apropriadas da sua conta Azure, seja um segredo de cliente ou certificado. Você também precisa garantir que todos os nós no cluster estejam íntegros. Você pode verificar isso com o comando `cluster show`.
2. Defina o nível privilegiado como avançado  
`set -priv advanced`
3. Ativar AKV no SVM  
`security key-manager external azure enable -client-id client_id -tenant-id tenant_id -name -key-id key_id -authentication-method {certificate|client-secret}` quando solicitado, insira o certificado de cliente ou o segredo do cliente na sua conta Azure.
4. Verifique se o AKV está ativado corretamente:  
`security key-manager external azure show vserver svm_name` Se a acessibilidade do serviço não estiver OK, estabeleça a conectividade com o serviço de gerenciamento de chaves AKV através dos dados SVM LIF.

## Google Cloud

### Habilite o KMS da nuvem em um SVM do ONTAP

1. Antes de começar, obtenha a chave privada para o arquivo de chave de conta KMS do Google Cloud em um formato JSON. Isso pode ser encontrado na sua conta do GCP. Você também precisa garantir que todos os nós no cluster estejam íntegros. Você pode verificar isso com o comando `cluster show`.
2. Defina o nível privilegiado como avançado:  
`set -priv advanced`

### 3. Ative o Cloud KMS no SVM

```
security key-manager external gcp enable -vserver svm_name -project-id  
project_id-key-ring-name key_ring_name -key-ring-location key_ring_location  
-key-name key_name
```

 quando solicitado, insira o conteúdo do arquivo JSON com a chave privada da conta de serviço

### 4. Verifique se o Cloud KMS está configurado com os parâmetros corretos:

```
security key-manager external gcp show vserver svm_name
```

 O status do `kms_wrapped_key_status` será "UNKNOWN" se nenhum volume criptografado tiver sido criado. Se a acessibilidade do serviço não estiver OK, estabeleça a conectividade com o serviço de gerenciamento de chaves do GCP por meio do data SVM LIF.

Se um ou mais volumes criptografados já estiverem configurados para um SVM de dados e as chaves NVE correspondentes forem gerenciadas pelo gerenciador de chaves integrado SVM de administrador, essas chaves deverão ser migradas para o serviço de gerenciamento de chaves externo. Para fazer isso com a CLI, execute o comando:

```
security key-manager key migrate -from-Vserver admin_SVM -to-Vserver data_SVM
```

Novos volumes criptografados não podem ser criados para o SVM de dados do locatário até que todas as chaves NVE do SVM de dados sejam migradas com sucesso.

### Informações relacionadas

- ["Criptografia de volumes com soluções de criptografia NetApp para Cloud Volumes ONTAP"](#)

## 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 DESTES DOCUMENTOS. 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 SOBRESSALIENTES; 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 DESTES SOFTWARES, 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.