



Configurar o NVE

ONTAP 9

NetApp
January 08, 2026

Índice

Configurar o NVE	1
Determine se a versão do seu cluster ONTAP oferece suporte a NVE	1
Instalar a licença de criptografia de volume em um cluster ONTAP	1
Configurar o gerenciamento de chaves externas	1
Saiba mais sobre como configurar o gerenciamento de chaves externas com o ONTAP NetApp	
Volume Encryption	2
Gerencie gerenciadores de chaves externas com o ONTAP System Manager	2
Instalar certificados SSL no cluster ONTAP	4
Habilitar gerenciamento de chaves externas para NVE no ONTAP 9.6 e posterior	5
Habilitar gerenciamento de chaves externas para NVE no ONTAP 9.5 e versões anteriores	8
Gerenciar chaves NVE para SVMs de dados ONTAP com um provedor de nuvem	10
Gerenciar chaves ONTAP com Barbican KMS	13
Habilitar o gerenciamento de chaves integrado para NVE no ONTAP 9.6 e posterior	18
Habilitar o gerenciamento de chaves integrado para NVE no ONTAP 9.5 e versões anteriores	20
Habilitar o gerenciamento de chaves integrado em nós ONTAP recém-adicionados	23

Configurar o NVE

Determine se a versão do seu cluster ONTAP oferece suporte a NVE

Você deve determinar se a versão do cluster é compatível com NVE antes de instalar a licença. Você pode usar o `version` comando para determinar a versão do cluster.

Sobre esta tarefa

A versão do cluster é a versão mais baixa do ONTAP em execução em qualquer nó no cluster.

Passos

1. Determine se a versão do cluster é compatível com NVE:

```
version -v
```

O NVE não é suportado se o comando output exibir o texto `1Ono-DARE` (para "criptografia sem dados em repouso") ou se você estiver usando uma plataforma que não está listada no ["Detalhes do suporte"](#).

Instalar a licença de criptografia de volume em um cluster ONTAP

Uma licença VE permite que você use o recurso em todos os nós do cluster. Essa licença é necessária para que você possa criptografar dados com NVE. Está incluído com ["ONTAP One"](#).

Antes do ONTAP One, a licença VE foi incluída com o pacote de encriptação. O pacote de criptografia não é mais oferecido, mas ainda é válido. Embora não seja necessário atualmente, os clientes existentes podem optar por ["Atualize para o ONTAP One"](#).

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- Tem de ter recebido a chave de licença VE do seu representante de vendas ou ter o ONTAP One instalado.

Passos

1. ["Verifique se a licença VE está instalada"](#).

O nome do pacote de licença VE é `VE`.

2. Se a licença não estiver instalada, ["Use o Gerenciador do sistema ou a CLI do ONTAP para instalá-lo"](#).

Configurar o gerenciamento de chaves externas

Saiba mais sobre como configurar o gerenciamento de chaves externas com o ONTAP NetApp Volume Encryption

Você pode usar um ou mais servidores externos de gerenciamento de chaves para proteger as chaves que o cluster usa para acessar dados criptografados. Um servidor externo de gerenciamento de chaves é um sistema de terceiros em seu ambiente de armazenamento que fornece chaves para nós usando o Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP). Além do Gerenciador de Chaves Onboard, o ONTAP oferece suporte a vários servidores externos de gerenciamento de chaves.

A partir do ONTAP 9.10.1, você pode usar [Azure Key Vault](#) ou [serviço Google Cloud Key Manager](#) para proteger suas chaves NVE para SVMs de dados. A partir do ONTAP 9.11.1, é possível configurar vários gerenciadores de chaves externos em um cluster. Ver [Configure servidores de chave em cluster](#). A partir do ONTAP 9.12.0, você pode usar ["KMS DA AWS"](#) para proteger suas chaves NVE para SVMs de dados. A partir do ONTAP 9.17.1, você pode usar o OpenStack. [Barbican KMS](#) para proteger suas chaves NVE para SVMs de dados.

Gerencie gerenciadores de chaves externas com o ONTAP 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	Cluster > Settings	Role até a seção Segurança . Em encriptação ,  selecione . Selecione External Key Manager .
Adicionar nível local	Armazenamento > camadas	Selecione * Adicionar nível local*. Marque a caixa de seleção "Configurar Gerenciador de chaves". Selecione External Key Manager .
Prepare o armazenamento	Painel	Na seção capacidade , selecione preparar armazenamento . Em seguida, selecione "Configure Key Manager". Selecione External Key Manager .
Configurar a criptografia (gerenciador de chaves somente no escopo da VM de storage)	Storage > Storage VMs	Selecione a VM de armazenamento. Selecione a guia Configurações . Na seção criptografia em Segurança ,  selecione .


- Para adicionar um servidor de chave primária, selecione  **Add** e preencha os campos **Endereço IP ou Nome do host** e **porta**.
- 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.
- Para adicionar um servidor de chaves secundário, selecione **Add** na coluna **Secondary Key Servers** e forneça seus detalhes.
- 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

- 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	Cluster > Settings	Role até a seção Segurança . Em Encryption ,  selecione e, em seguida, selecione Edit External Key Manager .

Gerenciador de chaves externo de escopo da VM de storage	Storage > Storage VMs	Selecione a VM de armazenamento. Selecione a guia Configurações . Na seção criptografia em Segurança ,  selecione e selecione Editar Gerenciador de chaves externas .
--	---------------------------------	--



- 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	Cluster > Settings	Role até a seção Segurança . Em Encryption , selecione  e, em seguida, selecione Delete External Key Manager .
Gerenciador de chaves externo de escopo da VM de storage	Storage > Storage VMs	Selecione a VM de armazenamento. Selecione a guia Configurações . Na seção criptografia em Segurança ,  selecione e selecione Excluir Gerenciador de chaves externas .

Migrar chaves entre os gerenciadores-chave

Quando vários gerenciadores de chaves estão habilitados em um cluster, as chaves devem ser migradas de um gerenciador de chaves para outro. Este processo é concluído automaticamente com o System Manager.

- Se o Gerenciador de chaves integrado ou um gerenciador de chaves externo estiver habilitado em um nível de cluster e alguns volumes estiverem criptografados, então, quando você configurar um gerenciador de chaves externo no nível de VM de armazenamento, as chaves devem ser migradas do Gerenciador de chaves integrado ou do gerenciador de chaves externo no nível do cluster para o gerenciador de chaves externo no nível de VM de armazenamento. Este processo é concluído automaticamente pelo System Manager.
- Se os volumes tiverem sido criados sem criptografia em uma VM de armazenamento, as chaves não precisarão ser migradas.

Instalar certificados SSL no cluster ONTAP

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
```

Informações relacionadas

- ["instalação do certificado de segurança"](#)

Habilitar gerenciamento de chaves externas para NVE no ONTAP 9.6 e posterior

Use 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

Você pode conectar até quatro servidores KMIP a um cluster ou SVM. Use pelo menos 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>
```

Saiba mais sobre `system license add` o ["Referência do comando ONTAP"](#) na .

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.

Saiba mais sobre `security key-manager key migrate` o ["Referência do comando ONTAP"](#) na .

Antes de começar

- Os certificados de cliente e servidor KMIP SSL devem ter sido instalados.
- O servidor KMIP deve ser acessível a partir da LIF de gerenciamento de nós de cada nó.
- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.
- Em um ambiente MetroCluster :
 - O MetroCluster deve ser totalmente configurado antes de habilitar o gerenciamento de chaves externas.
 - Você deve instalar o mesmo certificado SSL KMIP em ambos os clusters.
 - Um gerenciador de chaves externo deve ser configurado 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 é o SVM de administração do cluster atual. Você pode executar o `security key-manager external modify` comando para alterar a configuração de gerenciamento de chaves externas.

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 do SVM, SVM o padrão é o SVM atual. 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. Saiba mais sobre `security key-manager external add-servers` o ["Referência do comando ONTAP"](#) na .

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. Saiba mais sobre `security key-manager external show-status` o ["Referência do comando ONTAP"](#) na .

```
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 ser totalmente configurado antes de converter os volumes.

Informações relacionadas

- [Configurar servidores de chaves externas em cluster](#)
- ["adicionar licença do sistema"](#)
- ["gerenciador de chaves de segurança migração de chaves"](#)
- ["gerenciador de chaves de segurança servidores externos adicionais"](#)
- ["gerenciador de chaves de segurança externo show-status"](#)

Habilitar gerenciamento de chaves externas para NVE 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 este comando em ambos os clusters. Saiba mais sobre `security key-manager setup` no ["Referência do comando ONTAP"](#).

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
```

Saiba mais sobre os comandos descritos neste procedimento no ["Referência do comando ONTAP"](#).

```
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.

Gerenciar chaves NVE para SVMs de dados ONTAP 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 usará 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`

Saiba mais sobre `security key-manager external aws` o ["Referência do comando ONTAP"](#) na .

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`. Saiba mais sobre `cluster show` o ["Referência do comando ONTAP"](#) na .
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.

Saiba mais sobre `security key-manager external azure` o ["Referência do comando ONTAP"](#) na .

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. Saiba mais sobre cluster show o ["Referência do comando ONTAP"](#) na .

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 de `kms_wrapped_key_status` vai ser "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 SVM LIF de dados.

Saiba mais sobre `security key-manager external gcp` o ["Referência do comando ONTAP"](#) na .

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"](#)
- ["gerenciador de chaves de segurança externo"](#)

Gerenciar chaves ONTAP com Barbican KMS

A partir do ONTAP 9.17.1, você pode usar o OpenStack ["Barbican KMS"](#) para proteger chaves de criptografia ONTAP . O Barbican KMS é um serviço para armazenamento e acesso seguro a chaves. O Barbican KMS pode ser usado para proteger chaves de Criptografia de Volume NetApp (NVE) para SVMs de dados. O Barbican conta com ["OpenStack Keystone"](#) , serviço de identidade do OpenStack, para autenticação.

Sobre esta tarefa

Você pode configurar o gerenciamento de chaves com o Barbican KMS usando a CLI ou a API REST do ONTAP . Com a versão 9.17.1, o suporte ao Barbican KMS apresenta as seguintes limitações:

- O Barbican KMS não é compatível com NetApp Storage Encryption (NSE) e NetApp Aggregate Encryption (NAE). Como alternativa, você pode usar ["KMIPs externos"](#) ou o ["Gerenciador de Chaves de Bordo \(OKM\)"](#) para chaves NSE e NVE.
- O Barbican KMS não é compatível com configurações do MetroCluster .
- O Barbican KMS só pode ser configurado para uma SVM de dados. Não está disponível para a SVM de administrador.

Salvo indicação em contrário, os administradores da `admin` nível de privilégio pode executar os seguintes procedimentos.

Antes de começar

- O Barbican KMS e o OpenStack Keystone devem ser configurados. A SVM que você está usando com o Barbican deve ter acesso à rede dos servidores Barbican e OpenStack Keystone .
- Se você estiver usando uma Autoridade de Certificação (CA) personalizada para os servidores Barbican e OpenStack Keystone , você deve instalar o certificado da CA com `security certificate install -type server-ca -vserver <admin_svm>` .

Criar e ativar uma configuração do Barbican KMS

Você pode criar uma nova configuração do Barbican KMS para uma SVM e ativá-la. Uma SVM pode ter várias configurações inativas do Barbican KMS, mas apenas uma pode estar ativa por vez.

Passos

1. Crie uma nova configuração inativa do Barbican KMS para um SVM:

```
security key-manager external barbican create-config -vserver <svm_name>
-config-name <unique_config_name> -key-id <key_id> -keystone-url
<keystone_url> -application-cred-id
<keystone_applications_credentials_id>
```

- `-key-id` é o identificador da chave de criptografia da chave Barbican (KEK). Insira um URL completo, incluindo `https://` .



Algumas URLs incluem o caractere de ponto de interrogação (?). O ponto de interrogação ativa a ajuda ativa da linha de comando do ONTAP . Para inserir uma URL com um ponto de interrogação, você precisa primeiro desativar a ajuda ativa com o comando `set -active-help false` . A ajuda ativa pode ser reativada posteriormente com o comando `set -active-help true` . Saiba mais em ["Referência do comando ONTAP"](#) .

- `-keystone-url` é a URL do host de autorização do OpenStack Keystone . Insira uma URL completa, incluindo `https://` .
- `-application-cred-id` é o ID das credenciais do aplicativo.

Após inserir este comando, você será solicitado a inserir a chave secreta das credenciais do aplicativo. Este comando cria uma configuração inativa do Barbican KMS.

O exemplo a seguir cria uma nova configuração inativa do Barbican KMS chamada `config1` para o SVM `svm1` :

```
cluster1:> security key-manager external barbican create-config
-vserver svm1 -config-name config1 -keystone-url
https://172.21.76.152:5000/v3 -application-cred-id app123 -key-id
https://172.21.76.153:9311/v1/secrets/<id_value>
```

```
Enter the Application Credentials Secret for authentication with
Keystone: <key_value>
```


2. Ative a nova configuração do Barbican KMS:

```
security key-manager keystore enable -vserver <svm_name> -config-name  
<unique_config_name> -keystore barbican
```

Você pode usar este comando para alternar entre as configurações do Barbican KMS. Se já houver uma configuração ativa do Barbican KMS no SVM, ela será desativada e a nova configuração será ativada.

3. Verifique se a nova configuração do Barbican KMS está ativa:

```
security key-manager external barbican check -vserver <svm_name> -node  
<node_name>
```

Este comando fornecerá o status da configuração ativa do Barbican KMS no SVM ou nó. Por exemplo, se o SVM `svm1` no nó `node1` tem uma configuração ativa do Barbican KMS, o comando a seguir retornará o status dessa configuração:

```
cluster1::> security key-manager external barbican check -node node1  
  
Vserver: svm1  
Node: node1  
  
Category: service_reachability  
          Status: OK  
  
Category: kms_wrapped_key_status  
          Status: OK
```

Atualizar as credenciais e configurações de uma configuração do Barbican KMS

Você pode visualizar e atualizar as configurações atuais de uma configuração ativa ou inativa do Barbican KMS.

Passos

1. Veja as configurações atuais do Barbican KMS para um SVM:

```
security key-manager external barbican show -vserver <svm_name>
```

O ID da chave, o URL do OpenStack Keystone e o ID das credenciais do aplicativo são exibidos para cada configuração do Barbican KMS no SVM.

2. Atualizar as configurações de uma configuração do Barbican KMS:

```
security key-manager external barbican update-config -vserver <svm_name>
-config-name <unique_config_name> -timeout <timeout> -verify
<true|false> -verify-host <true|false>
```

Este comando atualiza as configurações de tempo limite e verificação da configuração especificada do Barbican KMS. `timeout` determina o tempo em segundos que o ONTAP aguardará a resposta do Barbican antes que a conexão falhe. O padrão `timeout` são dez segundos. `verify` e `verify-host` determinar se a identidade e o nome do host do host Barbican devem ser verificados antes da conexão. Por padrão, esses parâmetros são definidos como `true`. O `vserver` e `config-name` parâmetros são obrigatórios. Os demais parâmetros são opcionais.

3. Se necessário, atualize as credenciais de uma configuração ativa ou inativa do Barbican KMS:

```
security key-manager external barbican update-credentials -vserver
<svm_name> -config-name <unique_config_name> -application-cred-id
<keystone_applications_credentials_id>
```

Após digitar este comando, você será solicitado a informar a nova chave secreta de credenciais do aplicativo.

4. Se necessário, restaure uma chave de criptografia de chave SVM ausente (KEK) para uma configuração ativa do Barbican KMS:
 - a. Restaurar uma SVM KEK ausente com `security key-manager external barbican restore` :

```
security key-manager external barbican restore -vserver <svm_name>
```

Este comando restaurará a SVM KEK para a configuração ativa do Barbican KMS comunicando-se com o servidor Barbican.

5. Se necessário, troque a chave SVM KEK para uma configuração Barbican KMS:
 - a. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

- b. Redigite o SVM KEK com `security key-manager external barbican rekey-internal` :

```
security key-manager external barbican rekey-internal -vserver
<svm_name>
```

Este comando gera uma nova KEK SVM para a SVM especificada e reempacota as chaves de criptografia do volume com a nova KEK SVM. A nova KEK SVM será protegida pela configuração ativa do Barbican KMS.

Migrar chaves entre o Barbican KMS e o Onboard Key Manager

Você pode migrar chaves do Barbican KMS para o Gerenciador de Chaves Onboard (OKM) e vice-versa. Para saber mais sobre o OKM, consulte ["Habilite o gerenciamento de chaves integradas no ONTAP 9.6 e posterior"](#).

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Se necessário, migre as chaves do Barbican KMS para o OKM:

```
security key-manager key migrate -from-vserver <svm_name> -to-vserver  
<admin_svm_name>
```

`svm_name` é o nome do SVM com a configuração do Barbican KMS.

3. Se necessário, migre as chaves do OKM para o Barbican KMS:

```
security key-manager key migrate -from-vserver <admin_svm_name> -to  
-vserver <svm_name>
```

Desabilitar e excluir uma configuração do Barbican KMS

Você pode desabilitar uma configuração ativa do Barbican KMS sem volumes criptografados e pode excluir uma configuração inativa do Barbican KMS.

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Desabilitar uma configuração ativa do Barbican KMS:

```
security key-manager keystore disable -vserver <svm_name>
```

Se existirem volumes criptografados NVE no SVM, você deverá descriptografá-los ou [migrar as chaves](#) antes de desabilitar a configuração do Barbican KMS. A ativação de uma nova configuração do Barbican KMS não exige a descriptografia de volumes NVE nem a migração de chaves, e desabilitará a configuração ativa do Barbican KMS.

3. Excluir uma configuração inativa do Barbican KMS:

```
security key-manager keystore delete -vserver <svm_name> -config-name  
<unique_config_name> -type barbican
```

Habilitar o gerenciamento de chaves integrado para NVE no ONTAP 9.6 e posterior

Você pode usar o Gerenciador de chaves integrado para proteger as chaves que o cluster usa para acessar dados criptografados. É necessário ativar o Gerenciador de chaves integrado em cada cluster que acessa um volume criptografado ou um disco com autcriptografia.

Sobre esta tarefa

Você deve executar o `security key-manager onboard sync` comando sempre que adicionar um nó ao cluster.

Se você tiver uma configuração do MetroCluster, deverá executar primeiro o `security key-manager onboard enable` comando no cluster local e, em seguida, executar o `security key-manager onboard sync` comando no cluster remoto, usando a mesma senha em cada um. Ao executar o `security key-manager onboard enable` comando a partir do cluster local e depois sincronizar no cluster remoto, não é necessário executar o `enable` comando novamente a partir do cluster remoto.

Saiba mais sobre `security key-manager onboard enable` e `security key-manager onboard sync` no ["Referência do comando ONTAP"](#).

Por padrão, você não é obrigado a inserir a senha do gerenciador de chaves quando um nó é reinicializado. Pode utilizar a `cc-mode-enabled=yes` opção para exigir que os utilizadores introduzam a frase-passe após uma reinicialização.

Para NVE, se você definir `cc-mode-enabled=yes`, os volumes criados com os `volume create` comandos e `volume move start` serão criptografados automaticamente. Para `volume create`, não é necessário especificar `-encrypt true`. Para `volume move start`, não é necessário especificar `-encrypt-destination true`.

Ao configurar a criptografia de dados em repouso do ONTAP, para atender aos requisitos de Soluções Comerciais para Classificados (CSfC), você deve usar o NSE com o NVE e garantir que o Onboard Key Manager esteja habilitado no modo Common Criteria. Ver ["Resumo da solução CSfC"](#).

Quando o Gerenciador de chaves integrado está habilitado no modo Common Criteria (`cc-mode-enabled=yes`), o comportamento do sistema é alterado das seguintes maneiras:

- O sistema monitoriza as tentativas consecutivas de frase-passe do cluster falhadas ao funcionar no modo Common Criteria (critérios comuns).

Se você não digitar a senha do cluster 5 vezes, aguarde 24 horas ou reinicie o nó para redefinir o limite.



- As atualizações de imagem do sistema usam o certificado de assinatura de código NetApp RSA-3072 juntamente com os digests assinados por código SHA-384 para verificar a integridade da imagem em vez do certificado de assinatura de código NetApp RSA-2048 usual e os digests assinados por código SHA-256.

O comando de atualização verifica se o conteúdo da imagem não foi alterado ou corrompido, verificando várias assinaturas digitais. O sistema prossegue para a próxima etapa no processo de atualização da imagem se a validação for bem-sucedida; caso contrário, a atualização da imagem falha. Saiba mais sobre `cluster image` no ["Referência do comando ONTAP"](#).



O Onboard Key Manager armazena chaves na memória volátil. O conteúdo da memória volátil é limpo quando o sistema é reinicializado ou interrompido. O sistema limpa a memória volátil em 30 segundos quando é interrompido.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- Você deve configurar o ambiente MetroCluster antes de configurar o Gerenciador de chaves integrado.

Passos

1. Inicie a configuração do gerenciador de chaves:

```
security key-manager onboard enable -cc-mode-enabled yes|no
```



Defina `cc-mode-enabled=yes` para exigir que os usuários inseram a senha do gerenciador de chaves após uma reinicialização. Para NVE, se você definir `cc-mode-enabled=yes`o``, os volumes criados com os ``volume create` comandos e `volume move start` serão criptografados automaticamente. A `- cc-mode-enabled` opção não é suportada nas configurações do MetroCluster. O `security key-manager onboard enable` comando substitui o `security key-manager setup` comando.

2. Digite uma senha entre 32 e 256 caracteres ou, para "cc-mode", uma senha entre 64 e 256 caracteres.



Se a senha "cc-mode" especificada for inferior a 64 caracteres, haverá um atraso de cinco segundos antes que a operação de configuração do gerenciador de chaves exiba o prompt de senha novamente.

3. No prompt de confirmação da senha, redigite a senha.
4. Verifique se as chaves de autenticação foram criadas:

```
security key-manager key query -key-type NSE-AK
```



O `security key-manager key query` comando substitui o `security key-manager query key` comando.

Saiba mais sobre `security key-manager key query` o ["Referência do comando ONTAP"](#) na .

5. Opcionalmente, você pode converter volumes de texto simples em volumes criptografados.

```
volume encryption conversion start
```

O Gerenciador de chaves integrado deve estar totalmente configurado antes de converter os volumes. Em um ambiente MetroCluster, o Gerenciador de chaves integrado deve ser configurado em ambos os sites.

Depois de terminar

Copie a senha para um local seguro fora do sistema de armazenamento para uso futuro.

Depois de configurar a senha do Onboard Key Manager, faça backup manualmente das informações em um local seguro fora do sistema de armazenamento. Ver ["Faça backup manual das informações de gerenciamento de chaves integradas"](#) .

Informações relacionadas

- ["comandos de imagem de cluster"](#)
- ["gerenciador de chaves de segurança externo habilitado"](#)
- ["consulta de chave do gerenciador de chaves de segurança"](#)
- ["habilitar gerenciador de chaves de segurança integrado"](#)

Habilitar o gerenciamento de chaves integrado para NVE no ONTAP 9.5 e versões anteriores

Você pode usar o Gerenciador de chaves integrado para proteger as chaves que o cluster usa para acessar dados criptografados. É necessário habilitar o Gerenciador de chaves integrado em cada cluster que acessa um volume criptografado ou um disco com autcriptografia.

Sobre esta tarefa

Você deve executar o `security key-manager setup` comando sempre que adicionar um nó ao cluster.

Se você tiver uma configuração do MetroCluster, revise estas diretrizes:

- No ONTAP 9.5, você deve executar `security key-manager setup` no cluster local e `security key-manager setup -sync-metrocluster-config yes` no cluster remoto, usando a mesma senha em cada um.
- Antes do ONTAP 9.5, você deve executar `security key-manager setup` no cluster local, esperar aproximadamente 20 segundos e, em seguida, executar `security key-manager setup` no cluster remoto, usando a mesma senha em cada um.

Por padrão, você não é obrigado a inserir a senha do gerenciador de chaves quando um nó é reinicializado. A partir do ONTAP 9.4, pode utilizar a `-enable-cc-mode yes` opção para exigir que os utilizadores introduzam a frase-passe após uma reinicialização.

Para NVE, se você definir `-enable-cc-mode yes`o` , os volumes criados com os ``volume create` comandos e `volume move start` serão criptografados automaticamente. Para `volume create`, não é necessário especificar `-encrypt true`. Para `volume move start`, não é necessário especificar `-encrypt-destination true`.



Depois de uma tentativa de frase-passe com falha, tem de reiniciar o nó novamente.

Antes de começar

- Se você usar NSE ou NVE com um servidor de gerenciamento de chaves externas (KMIP), exclua o banco de dados do gerenciador de chaves externas.

["Transição para o gerenciamento de chaves integrado do gerenciamento de chaves externas"](#)

- Você deve ser um administrador de cluster para executar esta tarefa.
- Configure o ambiente MetroCluster antes de configurar o Onboard Key Manager.

Passos

1. Inicie a configuração do gerenciador de chaves:

```
security key-manager setup -enable-cc-mode yes|no
```



A partir do ONTAP 9.4, pode utilizar a `-enable-cc-mode yes` opção para exigir que os utilizadores introduzam a frase-passe do gestor de chaves após uma reinicialização. Para NVE, se você definir `-enable-cc-mode yes`o` , os volumes criados com os ``volume create` comandos e `volume move start` serão criptografados automaticamente.

O exemplo a seguir inicia a configuração do gerenciador de chaves no `cluster1` sem exigir que a senha seja inserida após cada reinicialização:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:  <32..256 ASCII characters long
text>
```

2. Digite `yes` no prompt para configurar o gerenciamento de chaves integradas.
3. No prompt de frase-passe, insira uma frase-passe entre 32 e 256 caracteres ou, para "cc-mode", uma frase-passe entre 64 e 256 caracteres.



Se a senha "cc-mode" especificada for inferior a 64 caracteres, haverá um atraso de cinco segundos antes que a operação de configuração do gerenciador de chaves exiba o prompt de senha novamente.

4. No prompt de confirmação da senha, redigite a senha.
5. Verifique se as chaves estão configuradas para todos os nós:

```
security key-manager show-key-store
```

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

Node: node1
Key Store: onboard
Key ID                                     Used By
-----
-----
<id_value> NSE-AK
<id_value> NSE-AK

Node: node2
Key Store: onboard
Key ID                                     Used By
-----
-----
<id_value> NSE-AK
<id_value> NSE-AK
```

Saiba mais sobre `security key-manager show-key-store` no ["Referência do comando ONTAP"](#).

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

```
volume encryption conversion start
```

Configure o Onboard Key Manager antes de converter volumes. Em ambientes MetroCluster, configure-o em ambos os sites.

Depois de terminar

Copie a senha para um local seguro fora do sistema de armazenamento para uso futuro.

Ao configurar a senha do Onboard Key Manager, faça backup das informações em um local seguro fora do sistema de armazenamento, em caso de desastre. Ver ["Faça backup manual das informações de gerenciamento de chaves integradas"](#).

Informações relacionadas

- ["Faça backup manual das informações de gerenciamento de chaves integradas"](#)
- ["Transição para o gerenciamento de chaves integrado do gerenciamento de chaves externas"](#)
- ["gerenciador de chaves de segurança mostrar-armazenamento-de-chaves"](#)

Habilitar o gerenciamento de chaves integrado em nós ONTAP recém-adicionados

Você pode usar o Gerenciador de chaves integrado para proteger as chaves que o cluster usa para acessar dados criptografados. É necessário habilitar o Gerenciador de chaves integrado em cada cluster que acessa um volume criptografado ou um disco com autcriptografia.



Para o ONTAP 9.6 e versões posteriores, você deve executar o `security key-manager onboard sync` comando a cada vez que você adiciona um nó ao cluster.

Para o ONTAP 9.5 e versões anteriores, você deve executar o `security key-manager setup` comando sempre que adicionar um nó ao cluster.

Se você adicionar um nó a um cluster com gerenciamento de chaves integrado, execute este comando para atualizar as chaves ausentes.

Se você tiver uma configuração do MetroCluster, revise estas diretrizes:

- A partir do ONTAP 9.6, é necessário executar `security key-manager onboard enable` primeiro no cluster local e, em seguida, executar `security key-manager onboard sync` no cluster remoto, usando a mesma frase-passe em cada um.

Saiba mais sobre `security key-manager onboard enable` e `security key-manager onboard sync` no ["Referência do comando ONTAP"](#).

- No ONTAP 9.5, você deve executar `security key-manager setup` no cluster local e `security key-manager setup -sync-metrocluster-config yes` no cluster remoto, usando a mesma senha em cada um.
- Antes do ONTAP 9.5, você deve executar `security key-manager setup` no cluster local, esperar aproximadamente 20 segundos e, em seguida, executar `security key-manager setup` no cluster remoto, usando a mesma senha em cada um.

Por padrão, você não é obrigado a inserir a senha do gerenciador de chaves quando um nó é reinicializado. A partir do ONTAP 9.4, pode utilizar a `-enable-cc-mode yes` opção para exigir que os utilizadores introduzam a frase-passe após uma reinicialização.

Para NVE, se você definir `-enable-cc-mode yes`o` , os volumes criados com os ``volume create` comandos e `volume move start` serão criptografados automaticamente. Para `volume create`, não é necessário especificar `-encrypt true`. Para `volume move start`, não é necessário especificar `-encrypt-destination true`.



Se a tentativa de senha falhar, reinicie o nó. Após a reinicialização, você pode tentar inserir a senha novamente.

Informações relacionadas

- ["comandos de imagem de cluster"](#)
- ["gerenciador de chaves de segurança externo habilitado"](#)
- ["habilitar gerenciador de chaves de segurança integrado"](#)

Informações sobre direitos autorais

Copyright © 2026 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 SOBRESSALENTE; 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 DOCUMENTOS, 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.