



# Configurar a criptografia baseada em hardware do NetApp

ONTAP 9

NetApp  
January 17, 2025

# Índice

- Configurar a criptografia baseada em hardware do NetApp ..... 1
  - Configure a visão geral da criptografia baseada em hardware do NetApp ..... 1
  - Configurar o gerenciamento de chaves externas ..... 3
  - Configurar o gerenciamento de chaves integradas ..... 16
  - Atribuir uma chave de autenticação FIPS 140-2-2 a uma unidade FIPS ..... 23
  - Habilite o modo compatível com FIPS em todo o cluster para conexões de servidor KMIP ..... 24

# Configurar a criptografia baseada em hardware do NetApp

## Configure a visão geral da criptografia baseada em hardware do NetApp

A criptografia baseada em hardware da NetApp oferece suporte à criptografia de disco completo (FDE) dos dados conforme eles são gravados. Os dados não podem ser lidos sem uma chave de criptografia armazenada no firmware. A chave de criptografia, por sua vez, é acessível apenas para um nó autenticado.

### Compreensão da criptografia baseada em hardware do NetApp

Um nó se autentica em uma unidade de autcriptografia usando uma chave de autenticação recuperada de um servidor de gerenciamento de chaves externo ou Gerenciador de chaves integrado:

- O 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). É uma prática recomendada configurar servidores de gerenciamento de chaves externos em um sistema de armazenamento diferente dos seus dados.
- O Gerenciador de chaves integrado é uma ferramenta integrada que serve chaves de autenticação para nós do mesmo sistema de storage que seus dados.

Você pode usar a criptografia de volume do NetApp com criptografia baseada em hardware para "criptografar dados" em unidades com autcriptografia.

Quando as unidades de autcriptografia estão ativadas, o despejo de memória também é criptografado.



Se um par de HA estiver usando a criptografia de unidades SAS ou NVMe (SED, NSE, FIPS), siga as instruções no [Retornar uma unidade FIPS ou SED para o modo desprotegido](#) tópico para todas as unidades do par de HA antes de inicializar o sistema (opções de inicialização 4 ou 9). Se não fizer isso, poderá resultar em perda de dados futura se as unidades forem reaproveitadas.

### Tipos de unidade com autcriptografia compatíveis

Dois tipos de unidades com autcriptografia são compatíveis:

- As unidades SAS ou NVMe com certificação FIPS são compatíveis com todos os sistemas FAS e AFF. Essas unidades, chamadas unidades *FIPS*, estão em conformidade com os requisitos da publicação padrão Federal de processamento de informações 140-2, nível 2. Os recursos certificados habilitam proteções além da criptografia, como impedir ataques de negação de serviço na unidade. As unidades FIPS não podem ser combinadas com outros tipos de unidades no mesmo nó ou par de HA.
- A partir do ONTAP 9.6, as unidades NVMe com autcriptografia que não foram submetidas ao teste FIPS são compatíveis com sistemas AFF A800, A320 e posteriores. Essas unidades, chamadas *SEDs*, oferecem os mesmos recursos de criptografia que as unidades FIPS, mas podem ser combinadas com unidades sem criptografia no mesmo nó ou par de HA.
- Todas as unidades validadas FIPS usam um módulo criptográfico de firmware que passou pela validação FIPS. O módulo criptográfico da unidade FIPS não usa nenhuma chave gerada fora da unidade (a senha

de autenticação que é inserida na unidade é usada pelo módulo criptográfico de firmware da unidade para obter uma chave de criptografia de chave).



Unidades com autcriptografia são unidades que não são unidades FIPS ou SEDs.



Se você estiver usando o NSE em um sistema com um módulo Flash Cache, também deverá ativar o NVE ou NAE. O NSE não criptografa dados que residem no módulo Flash Cache.

## Quando usar o gerenciamento de chaves externas

Embora seja mais barato e normalmente mais conveniente usar o gerenciador de chaves integrado, você deve usar o gerenciamento de chaves externas se alguma das seguintes opções for verdadeira:

- A política da sua organização requer uma solução de gerenciamento de chaves que use um módulo criptográfico FIPS 140-2 nível 2 (ou superior).
- Você precisa de uma solução de vários clusters, com gerenciamento centralizado de chaves de criptografia.
- Sua empresa requer a segurança adicional de armazenar chaves de autenticação em um sistema ou em um local diferente dos dados.

## Detalhes do suporte

A tabela a seguir mostra detalhes importantes do suporte à criptografia de hardware. Consulte a Matriz de interoperabilidade para obter as informações mais recentes sobre servidores KMIP, sistemas de storage e compartimentos de disco compatíveis.

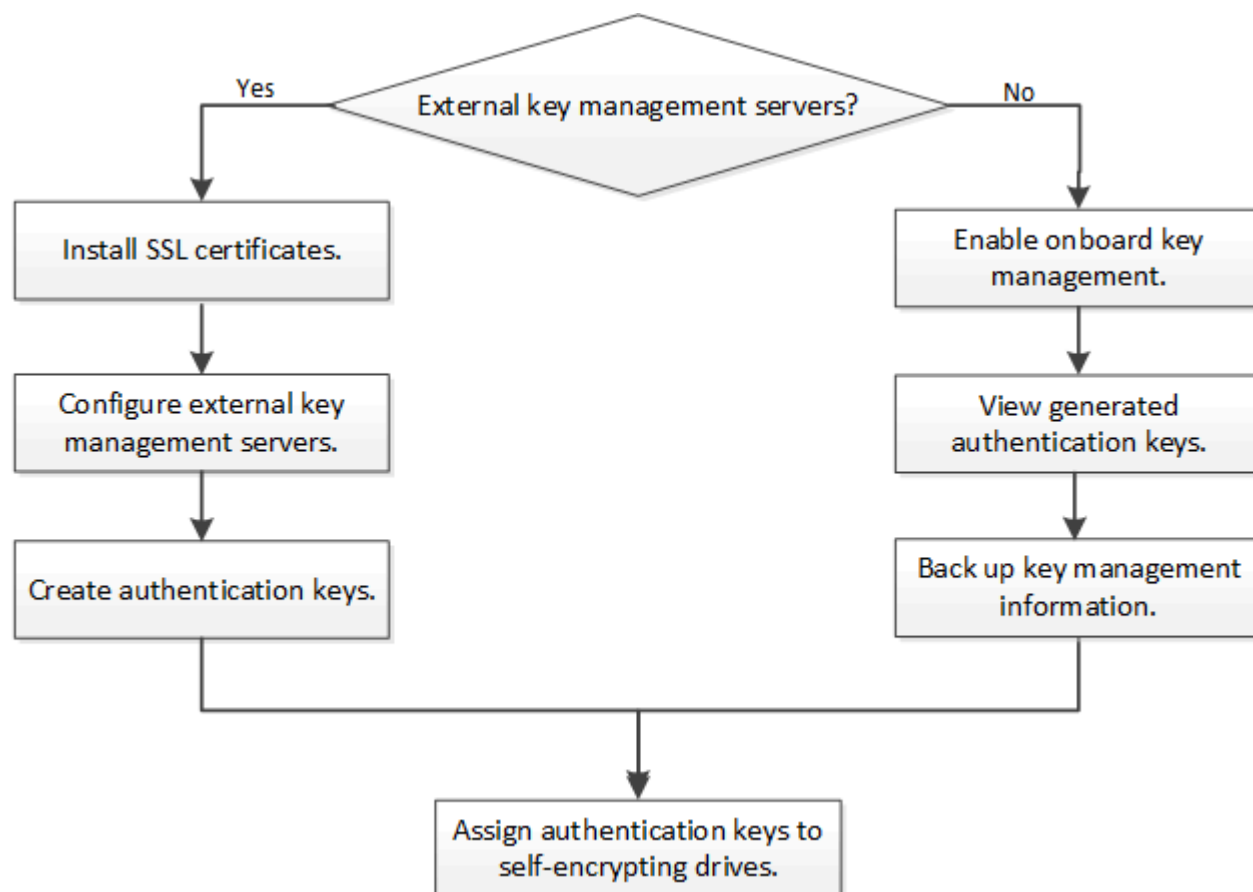
Recurso ou recurso	Detalhes do suporte
Conjuntos de discos não homogêneos	<ul style="list-style-type: none"><li>• As unidades FIPS não podem ser combinadas com outros tipos de unidades no mesmo nó ou par de HA. Pares de HA em conformidade podem coexistir com pares de HA não conformes no mesmo cluster.</li><li>• As SEDs podem ser combinadas com unidades sem criptografia no mesmo nó ou par de HA.</li></ul>
Tipo de unidade	<ul style="list-style-type: none"><li>• As unidades FIPS podem ser unidades SAS ou NVMe.</li><li>• As SEDs devem ser unidades NVMe.</li></ul>
Interfaces de rede de 10 GB	A partir do ONTAP 9.3, as configurações de gerenciamento de chaves KMIP suportam interfaces de rede de 10 GB para comunicações com servidores de gerenciamento de chaves externas.
Portas para comunicação com o servidor de gerenciamento de chaves	A partir do ONTAP 9.3, você pode usar qualquer porta de controlador de armazenamento para comunicação com o servidor de gerenciamento de chaves. Caso contrário, você deve usar a porta e0M para comunicação com servidores de gerenciamento de chaves. Dependendo do modelo do controlador de storage, algumas interfaces de rede podem não estar disponíveis durante o processo de inicialização para comunicação com servidores de gerenciamento de chaves.

## MetroCluster (MCC)

- As unidades NVMe são compatíveis com MCC.
- As unidades SAS não suportam MCC.

## Fluxo de trabalho de criptografia baseado em hardware

Você deve configurar os serviços de gerenciamento de chaves antes que o cluster possa se autenticar na unidade de autocriptografia. Você pode usar um servidor de gerenciamento de chaves externo ou um gerenciador de chaves integrado.



### Informações relacionadas

- ["NetApp Hardware Universe"](#)
- ["Criptografia de volumes do NetApp e criptografia agregada do NetApp"](#)

## 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) pode ser implementado com o Gerenciador de chaves integrado no ONTAP 9.1 e posterior. No ONTAP 9.3 e posterior, o NVE pode ser implementado com gerenciamento de chaves externas (KMIP) e Gerenciador de chaves integrado. 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](#).

## Colete informações de rede no ONTAP 9.2 e anteriores

Se você estiver usando o ONTAP 9.2 ou anterior, você deve preencher a Planilha de configuração de rede antes de ativar o gerenciamento de chaves externas.



A partir do ONTAP 9.3, o sistema detecta automaticamente todas as informações de rede necessárias.

Item	Notas	Valor
Nome da interface de rede de gerenciamento de chaves		
Endereço IP da interface de rede de gerenciamento de chaves	Endereço IP do LIF de gerenciamento de nós, no formato IPv4 ou IPv6	
Comprimento do prefixo da rede IPv6 da interface de rede de gerenciamento de chaves	Se você estiver usando IPv6, o comprimento do prefixo de rede IPv6	
Máscara de sub-rede da interface de rede de gerenciamento de chaves		
Endereço IP do gateway de interface de rede de gerenciamento de chaves		
Endereço IPv6 para a interface de rede do cluster	Necessário somente se você estiver usando IPv6 para a interface de rede de gerenciamento de chaves	
Número da porta para cada servidor KMIP	Opcional. O número da porta deve ser o mesmo para todos os servidores KMIP. Se você não fornecer um número de porta, o padrão será a porta 5696, que é a porta atribuída pela IANA (Internet Assigned Numbers Authority) para KMIP.	

Nome da etiqueta da chave	Opcional. O nome da tag chave é usado para identificar todas as chaves pertencentes a um nó. O nome da etiqueta de chave padrão é o nome do nó.	
---------------------------	---	--

### Informações relacionadas

["Relatório técnico da NetApp 3954: Requisitos e procedimentos de pré-instalação de criptografia de armazenamento da NetApp para o Gerenciador de chaves vitalício"](#)

["Relatório técnico da NetApp 4074: Requisitos e procedimentos de pré-instalação da criptografia de armazenamento NetApp para o KeySecure"](#)

## 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 posterior (baseado em hardware)

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.

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 .

### 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 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. Você pode executar o `security key-manager external modify` comando para alterar a configuração de gerenciamento de chaves externas. Para obter a sintaxe completa do comando, consulte as páginas man.
- 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 -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. Verifique se todos os servidores KMIP configurados estão conectados:

```
security key-manager external show-status -node node_name -vserver SVM -key
-server host_name|IP_address:port -key-server-status available|not-
responding|unknown
```



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
  cluster1
    10.0.0.10:5696                             available
    fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234 available
    ks1.local:15696                             available
node2
  cluster1
    10.0.0.10:5696                             available
    fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234 available
    ks1.local:15696                             available

6 entries were displayed.
```

## Habilite o gerenciamento de chaves externas no ONTAP 9.5 e versões anteriores (baseado em hardware)

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.

## Configurar servidores de chaves externas em cluster no ONTAP

A partir do ONTAP 9.11,1, é possível configurar a conectividade com servidores de gerenciamento de chaves externos em cluster em um SVM. Com servidores de chaves em cluster, você pode designar servidores de chaves primárias e secundárias em um SVM. Ao Registrar chaves, o ONTAP tentará primeiro acessar um servidor de chaves primárias antes de tentar acessar sequencialmente servidores secundários até que a operação seja concluída com êxito, evitando a duplicação de chaves.

Os servidores de chaves externas podem ser usados para chaves NSE, NVE, NAE e SED. Um SVM pode dar suporte a até quatro servidores KMIP primários externos. Cada servidor principal pode suportar até três servidores de chaves secundárias.

### Antes de começar

- ["O gerenciamento de chaves KMIP deve estar habilitado para SVM"](#).
- Esse processo só suporta servidores-chave que usam KMIP. Para obter uma lista de servidores de chaves suportados, verifique o ["Ferramenta de Matriz de interoperabilidade do NetApp"](#).
- Todos os nós no cluster devem estar executando o ONTAP 9.11,1 ou posterior.
- A ordem dos argumentos da lista de servidores no `-secondary-key-servers` parâmetro reflete a ordem de acesso dos servidores de gerenciamento de chaves externas (KMIP).
- Saiba mais sobre os comandos descritos neste procedimento no ["Referência do comando ONTAP"](#).

### Crie um servidor de chaves em cluster

O procedimento de configuração depende se você configurou ou não um servidor de chave primária.

### Adicionar servidores de chaves primárias e secundárias a uma SVM

1. Confirme se nenhum gerenciamento de chaves foi habilitado para o cluster:  
`security key-manager external show -vserver svm_name` Se o SVM já tiver o máximo de quatro servidores de chaves primárias ativados, você deverá remover um dos servidores de chaves primárias existentes antes de adicionar um novo.
2. Ative o gerenciador de chaves principal:  
`security key-manager external enable -vserver svm_name -key-servers server_ip -client-cert client_cert_name -server-ca-certs server_ca_cert_names`
3. Modifique o servidor de chaves primárias para adicionar servidores de chaves secundárias. O `-secondary-key-servers` parâmetro aceita uma lista separada por vírgulas de até três servidores-chave.  
`security key-manager external modify-server -vserver svm_name -key-servers primary_key_server -secondary-key-servers list_of_key_servers`

### Adicione servidores de chave secundária a um servidor de chave primária existente

1. Modifique o servidor de chaves primárias para adicionar servidores de chaves secundárias. O `-secondary-key-servers` parâmetro aceita uma lista separada por vírgulas de até três servidores-chave.  
`security key-manager external modify-server -vserver svm_name -key-servers primary_key_server -secondary-key-servers list_of_key_servers` Para obter mais informações sobre servidores de chaves secundárias, [\[mod-secondary\]](#) consulte .

### Modificar servidores de chaves em cluster

Você pode modificar clusters de servidores de chave externos alterando o status (primário ou secundário) de servidores de chave específicos, adicionando e removendo servidores de chave secundária ou alterando a ordem de acesso de servidores de chave secundária.

### Converta servidores de chaves primárias e secundárias

Para converter um servidor de chave primária em um servidor de chave secundário, primeiro remova-o do SVM com o `security key-manager external remove-servers` comando.

Para converter um servidor de chave secundária em um servidor de chave primária, primeiro você deve remover o servidor de chave secundária de seu servidor de chave primária existente. [\[mod-secondary\]](#) Consulte . Se você converter um servidor de chaves secundário para um servidor primário ao remover uma chave existente, tentar adicionar um novo servidor antes de concluir a remoção e conversão pode resultar na duplicação de chaves.

### Modificar servidores de chaves secundárias

Os servidores de chaves secundárias são gerenciados com o `-secondary-key-servers` parâmetro `security key-manager external modify-server` do comando. O `-secondary-key-servers` parâmetro aceita uma lista separada por vírgulas. A ordem especificada dos servidores de chaves secundárias na lista determina a sequência de acesso para os servidores de chaves secundárias. A ordem de acesso pode ser modificada executando o comando `security key-manager external modify-server` com os servidores de chaves secundárias inseridos em uma sequência diferente.

Para remover um servidor de chave secundário, os `-secondary-key-servers` argumentos devem incluir

os servidores de chave que você deseja manter ao omitir o que deve ser removido. Para remover todos os servidores de chaves secundárias, use o argumento `-`, significando nenhum.

Saiba mais sobre o comando link:[https://docs.NetApp.com/US-en/ONTAP-cli/\[security key-manager external ONTAP](https://docs.NetApp.com/US-en/ONTAP-cli/[security key-manager external ONTAP)

## Crie chaves de autenticação no ONTAP 9.6 e posterior

Você pode usar o `security key-manager key create` comando para criar as chaves de autenticação para um nó e armazená-las nos servidores KMIP configurados.

### Sobre esta tarefa

Se a configuração de segurança exigir que você use chaves diferentes para autenticação de dados e autenticação FIPS 140-2-2, você deve criar uma chave separada para cada uma. Se esse não for o caso, você poderá usar a mesma chave de autenticação para conformidade com FIPS usada para acesso aos dados.

O ONTAP cria chaves de autenticação para todos os nós no cluster.

- Este comando não é suportado quando o Onboard Key Manager está ativado. No entanto, duas chaves de autenticação são criadas automaticamente quando o Onboard Key Manager está ativado. As teclas podem ser visualizadas com o seguinte comando:

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

- Você receberá um aviso se os servidores de gerenciamento de chaves configurados já estiverem armazenando mais de 128 chaves de autenticação.
- Você pode usar o `security key-manager key delete` comando para excluir quaisquer chaves não utilizadas. O `security key-manager key delete` comando falha se a chave dada estiver atualmente em uso pelo ONTAP. (Você deve ter Privileges maior que "admin" para usar este comando.)



Em um ambiente MetroCluster, antes de excluir uma chave, certifique-se de que a chave não está em uso no cluster de parceiros. Você pode usar os seguintes comandos no cluster de parceiros para verificar se a chave não está em uso:

- `storage encryption disk show -data-key-id key-id`
- `storage encryption disk show -fips-key-id key-id`

### Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

### Passos

1. Crie as chaves de autenticação para nós de cluster:

```
security key-manager key create -key-tag passphrase_label -prompt-for-key true|false
```



A configuração `prompt-for-key=true` faz com que o sistema solicite ao administrador do cluster a senha a ser usada ao autenticar unidades criptografadas. Caso contrário, o sistema gera automaticamente uma frase-passe de 32 bytes. O `security key-manager key create` comando substitui o `security key-manager create-key` comando. Para obter a sintaxe completa do comando, consulte a página `man`.

O exemplo a seguir cria as chaves de autenticação para `cluster1`o` , gerando automaticamente uma senha de 32 bytes:

```
cluster1::> security key-manager key create
Key ID:
000000000000000000002000000000001006268333f870860128fbe17d393e5083b00000000
00000000
```

2. Verifique se as chaves de autenticação foram criadas:

```
security key-manager key query -node node
```



O `security key-manager key query` comando substitui o `security key-manager query key` comando. Para obter a sintaxe completa do comando, consulte a página `man`. O ID da chave exibido na saída é um identificador usado para se referir à chave de autenticação. Não é a chave de autenticação real ou a chave de criptografia de dados.

O exemplo a seguir verifica se as chaves de autenticação foram criadas para `cluster1:`

```

cluster1::> security key-manager key query
      Vserver: cluster1
      Key Manager: external
      Node: node1

Key Tag                                Key Type  Restored
-----                                -
node1                                  NSE-AK    yes
      Key ID:
000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                  NSE-AK    yes
      Key ID:
000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

      Vserver: cluster1
      Key Manager: external
      Node: node2

Key Tag                                Key Type  Restored
-----                                -
node2                                  NSE-AK    yes
      Key ID:
000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                  NSE-AK    yes
      Key ID:
000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

```

## Crie chaves de autenticação no ONTAP 9.5 e anteriores

Você pode usar o `security key-manager create-key` comando para criar as chaves de autenticação para um nó e armazená-las nos servidores KMIP configurados.

### Sobre esta tarefa

Se a configuração de segurança exigir que você use chaves diferentes para autenticação de dados e autenticação FIPS 140-2-2, você deve criar uma chave separada para cada uma. Se esse não for o caso, você poderá usar a mesma chave de autenticação para conformidade com o FIPS usada para acesso aos dados.

O ONTAP cria chaves de autenticação para todos os nós no cluster.

- Este comando não é suportado quando o gerenciamento de chaves integradas está habilitado.

- Você receberá um aviso se os servidores de gerenciamento de chaves configurados já estiverem armazenando mais de 128 chaves de autenticação.

Você pode usar o software do servidor de gerenciamento de chaves para excluir quaisquer chaves não utilizadas e, em seguida, executar o comando novamente.

### Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

### Passos

1. Crie as chaves de autenticação para nós de cluster:

```
security key-manager create-key
```

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



O ID da chave exibido na saída é um identificador usado para se referir à chave de autenticação. Não é a chave de autenticação real ou a chave de criptografia de dados.

O exemplo a seguir cria as chaves de autenticação para `cluster1`:

```
cluster1::> security key-manager create-key
  (security key-manager create-key)
Verifying requirements...

Node: cluster1-01
Creating authentication key...
Authentication key creation successful.
Key ID: F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C

Node: cluster1-01
Key manager restore operation initialized.
Successfully restored key information.

Node: cluster1-02
Key manager restore operation initialized.
Successfully restored key information.
```

2. Verifique se as chaves de autenticação foram criadas:

```
security key-manager query
```

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

O exemplo a seguir verifica se as chaves de autenticação foram criadas para `cluster1`:



```

cluster1::> security key-manager query

(security key-manager query)

      Node: cluster1-01
    Key Manager: 20.1.1.1
  Server Status: available

Key Tag          Key Type  Restored
-----          -
cluster1-01     NSE-AK   yes
      Key ID:
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C

      Node: cluster1-02
    Key Manager: 20.1.1.1
  Server Status: available

Key Tag          Key Type  Restored
-----          -
cluster1-02     NSE-AK   yes
      Key ID:
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C

```

## Atribuir uma chave de autenticação de dados a uma unidade FIPS ou SED (gerenciamento de chaves externas)

Você pode usar o `storage encryption disk modify` comando para atribuir uma chave de autenticação de dados a uma unidade FIPS ou SED. Os nós de cluster usam essa chave para bloquear ou desbloquear dados criptografados na unidade.

### Sobre esta tarefa

Uma unidade com autocriptografia é protegida contra acesso não autorizado somente se o ID da chave de autenticação estiver definido como um valor não padrão. O ID seguro do fabricante (MSID), que tem ID de chave 0x0, é o valor padrão para unidades SAS. Para unidades NVMe, o valor padrão é uma chave nula, representada como um ID de chave em branco. Quando você atribui o ID da chave a uma unidade de autocriptografia, o sistema altera o ID da chave de autenticação para um valor não padrão.

Este procedimento não causa interrupções.

### Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

### Passos

1. Atribuir uma chave de autenticação de dados a uma unidade FIPS ou SED:

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```

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



Você pode usar o `security key-manager query -key-type NSE-AK` comando para exibir IDs de chave.

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id  
F1CB30AFF1CB30B0010100000000000A68B167F92DD54196297159B5968923C
```

```
Info: Starting modify on 14 disks.  
View the status of the operation by using the  
storage encryption disk show-status command.
```

## 2. Verifique se as chaves de autenticação foram atribuídas:

```
storage encryption disk show
```

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

```
cluster1::> storage encryption disk show  
Disk      Mode Data Key ID  
-----  
-----  
0.0.0     data  
F1CB30AFF1CB30B001010000000000A68B167F92DD54196297159B5968923C  
0.0.1     data  
F1CB30AFF1CB30B001010000000000A68B167F92DD54196297159B5968923C  
[...]
```

# Configurar o gerenciamento de chaves integradas

## Habilite o gerenciamento de chaves integradas no ONTAP 9.6 e posterior

Você pode usar o Gerenciador de chaves integrado para autenticar nós de cluster em uma unidade FIPS ou SED. O Gerenciador de chaves integrado é uma ferramenta integrada que serve chaves de autenticação para nós do mesmo sistema de storage que seus dados. O Gerenciador de chaves integrado é compatível com FIPS-140-2 nível 1.

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 onboard enable` comando sempre que adicionar um nó

ao cluster. Nas configurações do MetroCluster, você deve 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 senha em cada um.

Por padrão, você não é obrigado a inserir a senha do gerenciador de chaves quando um nó é reinicializado. Exceto no MetroCluster, você pode usar a `cc-mode-enabled=yes` opção para exigir que os usuários digitem a senha após uma reinicialização.

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 a criptação de armazenamento NetApp (NSE) estiver ativada e não conseguir introduzir a frase-passe correta do cluster no arranque, o sistema não pode autenticar-se nas suas unidades e reinicia automaticamente. Para corrigir isso, você deve inserir a senha correta do cluster no prompt de inicialização. Uma vez iniciado, o sistema permite até 5 tentativas consecutivas para inserir corretamente a senha do cluster em um período de 24 horas para qualquer comando que exija a senha do cluster como um parâmetro. Se o limite for atingido (por exemplo, você não conseguiu inserir corretamente a senha do cluster 5 vezes em uma linha), então você deve esperar o período de tempo limite de 24 horas para decorrer, ou você deve reiniciar o nó, a fim de 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 `upgrade` verifica se o conteúdo da imagem não foi alterado ou corrompido verificando várias assinaturas digitais. O processo de atualização da imagem prossegue para o próximo passo se a validação for bem-sucedida; caso contrário, a atualização da imagem falhará. Consulte a página de manual `""imagem de cluster""` para obter informações sobre atualizações do sistema.

O Gerenciador de chaves integrado armazena as chaves na memória volátil. O conteúdo da memória volátil é apagado quando o sistema é reinicializado ou interrompido. Em condições normais de funcionamento, o conteúdo da memória volátil será apagado dentro de 30sMB quando um sistema for interrompido.

### Antes de começar

- Se você estiver usando o NSE com um servidor de gerenciamento de chaves externas (KMIP), exclua o banco de dados do gerenciador de chaves externo.

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

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

### Passos

1. Inicie o comando de 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. 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.

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

```
cluster1::> security key-manager onboard enable

Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1":<  <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase:  <32..256 ASCII characters long
text>
```

2. 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.

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

```
security key-manager key query -node node
```



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

O exemplo a seguir verifica se as chaves de autenticação foram criadas para `cluster1`:

```

cluster1::> security key-manager key query
      Vserver: cluster1
      Key Manager: onboard
      Node: node1

Key Tag                                Key Type  Restored
-----                                -
node1                                  NSE-AK    yes
      Key ID:
000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                  NSE-AK    yes
      Key ID:
000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

      Vserver: cluster1
      Key Manager: onboard
      Node: node2

Key Tag                                Key Type  Restored
-----                                -
node1                                  NSE-AK    yes
      Key ID:
000000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                  NSE-AK    yes
      Key ID:
000000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

```

### Depois de terminar

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

Todas as informações de gerenciamento de chaves são automaticamente armazenadas no banco de dados replicado (RDB) para o cluster. Você também deve fazer backup das informações manualmente para uso em caso de desastre.

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

Você pode usar o Gerenciador de chaves integrado para autenticar nós de cluster em uma unidade FIPS ou SED. O Gerenciador de chaves integrado é uma ferramenta integrada que serve chaves de autenticação para nós do mesmo sistema de storage que seus dados. O Gerenciador de chaves integrado é compatível com FIPS-140-2 nível 1.

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 estiver usando o NSE com um servidor de gerenciamento de chaves externas (KMIP), exclua o banco de dados do gerenciador de chaves externo.

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

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

### 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 key show
```

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

```

cluster1::> security key-manager key show

Node: node1
Key Store: onboard
Key ID                                     Used By
-----
0000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                     Used By
-----
0000000000000000020000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

```

## Depois de terminar

Todas as informações de gerenciamento de chaves são automaticamente armazenadas no banco de dados replicado (RDB) para o cluster.

Sempre que você configurar a senha do Gerenciador de chaves integrado, você também deve fazer backup das informações manualmente para um local seguro fora do sistema de armazenamento para uso em caso de desastre. "[Faça backup manual das informações de gerenciamento de chaves integradas](#)" Consulte .

## Atribuir uma chave de autenticação de dados a uma unidade FIPS ou SED (gerenciamento de chaves integradas)

Você pode usar o `storage encryption disk modify` comando para atribuir uma chave de autenticação de dados a uma unidade FIPS ou SED. Os nós de cluster usam essa chave para acessar dados na unidade.

### Sobre esta tarefa

Uma unidade com autocriptografia é protegida contra acesso não autorizado somente se o ID da chave de autenticação estiver definido como um valor não padrão. O ID seguro do fabricante (MSID), que tem ID de chave 0x0, é o valor padrão para unidades SAS. Para unidades NVMe, o valor padrão é uma chave nula, representada como um ID de chave em branco. Quando você atribui o ID da chave a uma unidade de autocriptografia, o sistema altera o ID da chave de autenticação para um valor não padrão.

### Antes de começar

Você deve ser um administrador de cluster para executar esta tarefa.

### Passos

1. Atribuir uma chave de autenticação de dados a uma unidade FIPS ou SED:

```
storage encryption disk modify -disk disk_ID -data-key-id key_ID
```

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



Você pode usar o `security key-manager key query -key-type NSE-AK` comando para exibir IDs de chave.

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id  
0000000000000000000020000000000010019215b9738bc7b43d4698c80246db1f4
```

```
Info: Starting modify on 14 disks.  
View the status of the operation by using the  
storage encryption disk show-status command.
```

2. Verifique se as chaves de autenticação foram atribuídas:

```
storage encryption disk show
```

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



```

cluster1::> storage encryption disk show
Disk      Mode Data Key ID
-----  ----
-----
0.0.0    data
0000000000000000000020000000000010019215b9738bc7b43d4698c80246db1f4
0.0.1    data
0000000000000000000020000000000010059851742AF2703FC91369B7DB47C4722
[...]

```

## Atribuir uma chave de autenticação FIPS 140-2-2 a uma unidade FIPS

Você pode usar o `storage encryption disk modify` comando com a `-fips-key-id` opção para atribuir uma chave de autenticação FIPS 140-2 a uma unidade FIPS. Os nós de cluster usam essa chave para operações de unidade que não sejam o acesso a dados, como impedir ataques de negação de serviço na unidade.

### Sobre esta tarefa

Sua configuração de segurança pode exigir que você use chaves diferentes para autenticação de dados e autenticação FIPS 140-2. Se esse não for o caso, você poderá usar a mesma chave de autenticação para conformidade com o FIPS usada para acesso aos dados.

Este procedimento não causa interrupções.

### Antes de começar

O firmware da unidade deve ser compatível com a conformidade FIPS 140-2-2. O "[Ferramenta de Matriz de interoperabilidade do NetApp](#)" contém informações sobre as versões de firmware da unidade suportadas.

### Passos

1. Primeiro, você deve garantir que atribuiu uma chave de autenticação de dados. Isso pode ser feito com o uso de um [gerenciador de chaves externo](#) ou um [gerenciador de chaves integrado](#). Verifique se a chave está atribuída com o comando `storage encryption disk show`.
2. Atribuir uma chave de autenticação FIPS 140-2 a SEDs:

```

storage encryption disk modify -disk disk_id -fips-key-id
fips_authentication_key_id

```

Você pode usar o `security key-manager query` comando para exibir IDs de chave.

```
cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
```

```
Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

### 3. Verifique se a chave de autenticação foi atribuída:

```
storage encryption disk show -fips
```

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

```
cluster1::> storage encryption disk show -fips
Disk      Mode FIPS-Compliance Key ID
-----  ----
-----
2.10.0    full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
2.10.1    full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
[...]
```

## Habilite o modo compatível com FIPS em todo o cluster para conexões de servidor KMIP

Você pode usar o `security config modify` comando com a `-is-fips-enabled` opção de ativar o modo compatível com FIPS em todo o cluster para dados em trânsito. Isso força o cluster a usar o OpenSSL no modo FIPS ao se conectar a servidores KMIP.

### Sobre esta tarefa

Quando você ativa o modo compatível com FIPS em todo o cluster, o cluster usará automaticamente somente pacotes de codificação validados por FIPS e TLS1,2. O modo compatível com FIPS em todo o cluster está desativado por padrão.

Você deve reinicializar os nós de cluster manualmente após modificar a configuração de segurança em todo o cluster.

### Antes de começar

- O controlador de storage deve ser configurado no modo compatível com FIPS.
- Todos os servidores KMIP precisam oferecer suporte a TLSv1,2. O sistema requer o TLSv1,2 para concluir a conexão com o servidor KMIP quando o modo compatível com FIPS em todo o cluster estiver ativado.

### Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Verifique se o TLSv1,2 é suportado:

```
security config show -supported-protocols
```

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

```
cluster1::> security config show
      Cluster
Security
Interface FIPS Mode  Supported Protocols  Supported Ciphers  Config
Ready
-----
-----
SSL        false          TLSv1.2, TLSv1.1, TLSv1  ALL:!LOW:
!aNULL:!EXP:
!eNULL          yes
```

3. Ativar o modo compatível com FIPS em todo o cluster:

```
security config modify -is-fips-enabled true -interface SSL
```

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

4. Reinicializar os nós de cluster manualmente.

5. Verifique se o modo compatível com FIPS em todo o cluster está ativado:

```
security config show
```

```
cluster1::> security config show
      Cluster
Security
Interface FIPS Mode  Supported Protocols  Supported Ciphers  Config
Ready
-----
-----
SSL        true           TLSv1.2, TLSv1.1      ALL:!LOW:
!aNULL:!EXP:
!eNULL:!RC4      yes
```

## 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.