Configurar a criptografia baseada em hardware do NetApp

ONTAP 9

NetApp
January 08, 2026

Índice

Configurar a criptografia baseada em hardware do NetApp

Saiba mais sobre a criptografia baseada em hardware ONTAP

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 autocriptografia 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 autocriptografia.

Quando as unidades de autocriptografia 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 autocriptografia compatíveis

Dois tipos de unidades com autocriptografia 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 autocriptografia 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 autocriptografia 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

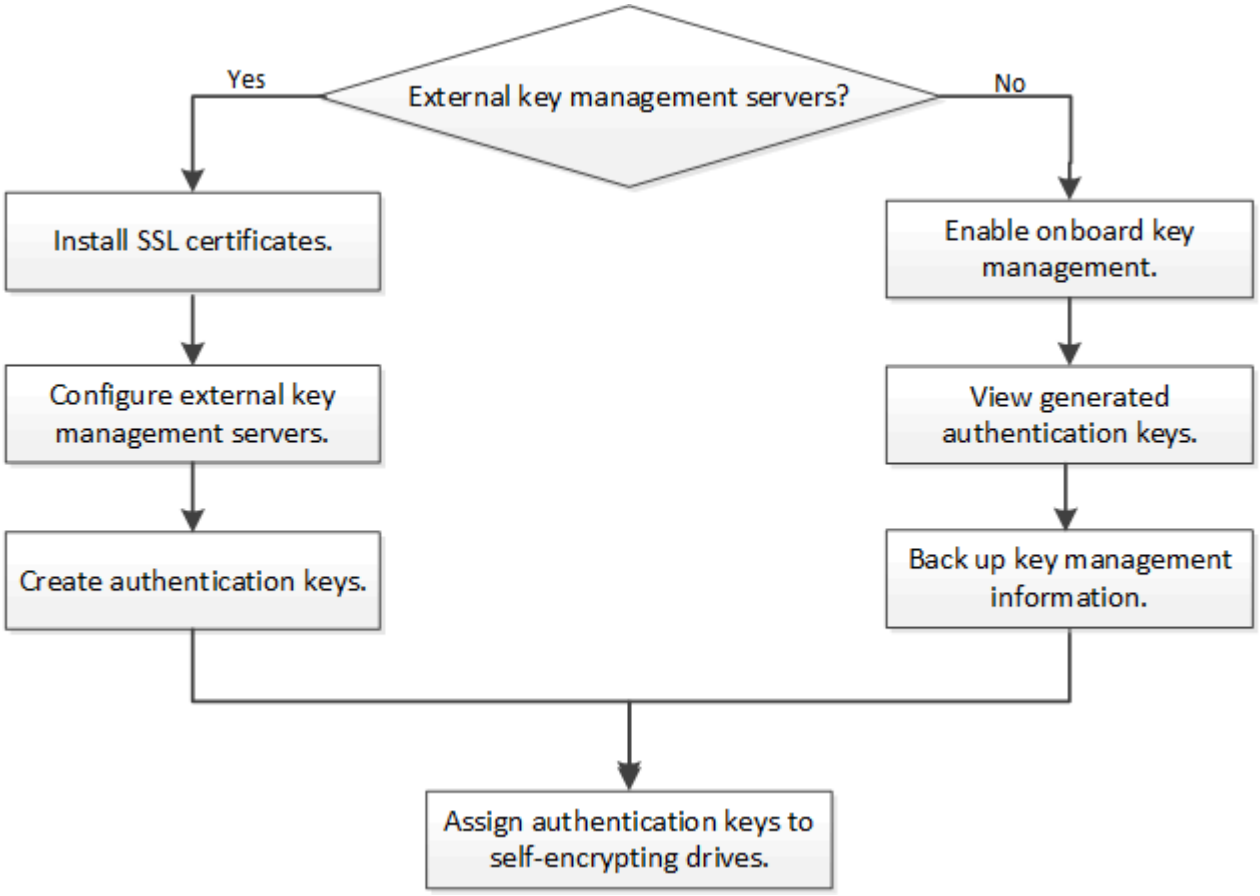
A tabela a seguir mostra detalhes importantes do suporte à criptografia de hardware. Consulte a Matriz de interoperabilidade para obter as informações mais recentes sobre servidores KMIP, sistemas de storage e compartimentos de disco compatíveis.

Recurso ou recurso	Detalhes do suporte
Conjuntos de discos não homogéneos	• 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. • As SEDs podem ser combinadas com unidades sem criptografia no mesmo nó ou par de HA.
Tipo de unidade	• As unidades FIPS podem ser unidades SAS ou NVMe. • As SEDs devem ser unidades NVMe.
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

Saiba mais sobre como configurar o gerenciamento de chaves externas ONTAP

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).

A criptografia de volume NetApp (NVE) pode ser implementada com o Gerenciador de chaves integrado. 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.

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 criptografia baseada em hardware no ONTAP 9.6 e posterior

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 clusterconsulte .

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.
- Em um ambiente MetroCluster :
  - Você deve configurar o ambiente MetroCluster antes de configurar um gerenciador de chaves externo.
  - Você deve instalar o mesmo certificado SSL KMIP em ambos os clusters.

Passos

1. Configurar a conetividade 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. Saiba mais sobre `security key-manager external enable` o "Referência do comando ONTAP"na .
   - 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:

   ```
   clusterl::> 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 conetados:

```
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. 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
      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.
```

Informações relacionadas

- Configurar servidores de chaves externas em cluster
- "gerenciador de chaves de segurança-habilitação externa"
- "gerenciador de chaves de segurança externo mostrar status"

Habilitar gerenciamento de chaves externas para criptografia baseada em hardware 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`

   ```
   clusterl::> 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`

   ```
   clusterl::> 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 conetados:

   `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.

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 externas em cluster em uma SVM. Com servidores de chaves em cluster, você pode designar servidores de chaves primários e secundários em uma SVM. Ao registrar ou recuperar chaves, o ONTAP primeiro tenta acessar o servidor de chaves primário antes de tentar acessar sequencialmente os servidores secundários até que a operação seja concluída com sucesso.

Você pode usar servidores de chaves externos para as chaves do NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE) e NetApp Aggregate Encryption (NAE). Uma SVM pode suportar até quatro servidores KMIP externos primários. Cada servidor primário pode suportar até três servidores de chave secundários.

Sobre esta tarefa

- 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".

Antes de começar

- "O gerenciamento de chaves KMIP deve estar habilitado para SVM".
- Todos os nós no cluster devem estar executando o ONTAP 9.11,1 ou posterior.
- A ordem dos servidores listados no `-secondary-key-servers` O parâmetro reflete a ordem de acesso dos servidores externos de gerenciamento de chaves (KMIP).

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

Passos

1. Confirme se nenhum gerenciamento de chaves foi habilitado para o cluster (SVM de administrador):

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

   Se a SVM já tiver o máximo de quatro servidores de chave primária ativados, você deverá remover um dos servidores de chave primária existentes antes de adicionar um novo.

2. Ative o gerenciador de chaves primárias:

   ```
   security key-manager external enable -vserver <svm_name> -key-servers
   <primary_key_server_ip> -client-cert <client_cert_name> -server-ca-certs
   <server_ca_cert_names>
   ```

   - Se você não especificar uma porta no `-key-servers` Para esse parâmetro, é utilizada a porta padrão 5696.

   > Se você estiver executando o `security key-manager external enable` Para executar o comando no SVM de administração em uma configuração MetroCluster , você deve executar o comando em ambos os clusters. Se você estiver executando o comando para um SVM de dados individual, não precisa executá-lo em ambos os clusters. A NetApp recomenda enfaticamente o uso dos mesmos servidores de chave em ambos os clusters.

3. Modifique o servidor de chave primária para adicionar servidores de chave secundária. O `-secondary-key-servers` O parâmetro aceita uma lista de até três servidores-chave, separados por vírgula:

   ```
   security key-manager external modify-server -vserver <svm_name> -key
   -servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
   ```

   - Não inclua um número de porta para servidores de chave secundários no `-secondary-key -servers` parâmetro. Ele usa o mesmo número de porta que o servidor de chave primária.

   > Se você estiver executando o `security key-manager external` Para executar o comando no SVM de administração em uma configuração MetroCluster , você deve executar o comando em ambos os clusters. Se você estiver executando o comando para um SVM de dados individual, não precisa executá-lo em ambos os clusters. A NetApp recomenda enfaticamente o uso dos mesmos servidores de chave em ambos os clusters.

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

Passos

1. Modifique o servidor de chave primária para adicionar servidores de chave secundária. O `-secondary-key-servers` O parâmetro aceita uma lista de até três servidores-chave, separados por vírgula:

   ```
   security key-manager external modify-server -vserver <svm_name> -key
   -servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
   ```

- Não inclua um número de porta para servidores de chave secundários no `-secondary-key-servers` parâmetro. Ele usa o mesmo número de porta que os servidores de chave primária.

> Se você estiver executando o `security key-manager external modify-server` Para executar o comando no SVM de administração em uma configuração MetroCluster , você deve executar o comando em ambos os clusters. Se você estiver executando o comando para um SVM de dados individual, não precisa executá-lo em ambos os clusters. A NetApp recomenda enfaticamente o uso dos mesmos servidores de chave em ambos os clusters.

Para obter mais informações sobre servidores de chaves secundários, consulte [mod-secondary].

Modificar servidores de chaves em cluster

É possível modificar servidores de chaves externas em cluster adicionando e removendo servidores de chaves secundários, alterando a ordem de acesso dos servidores de chaves secundários ou alterando a designação (primária ou secundária) de servidores de chaves específicos. Se você modificar servidores de chaves externas em cluster em uma configuração MetroCluster , a NetApp recomenda enfaticamente o uso dos mesmos servidores de chaves em ambos os clusters.

Modificar servidores de chaves secundárias

Use o parâmetro `-secondary-key-servers` do comando `security key-manager external modify-server` para gerenciar servidores de chaves secundários. O `-secondary-key-servers` O parâmetro aceita uma lista separada por vírgulas. A ordem especificada dos servidores de chaves secundárias na lista determina a sequência de acesso para esses servidores. É possível modificar a ordem de acesso executando o comando `security key-manager external modify-server` com os servidores de chaves secundários inseridos em uma sequência diferente. Não inclua um número de porta para servidores de chave secundários.

> Se você estiver executando o `security key-manager external modify-server` Para executar o comando no SVM de administração em uma configuração MetroCluster , você deve executar o comando em ambos os clusters. Se você estiver executando o comando para um SVM de dados individual, não precisa executá-lo em ambos os clusters.

Para remover um servidor de chaves secundário, inclua os servidores de chaves que deseja manter na lista. `-secondary-key-servers` parâmetro e omita aquele que deseja remover. Para remover todos os servidores de chave secundários, use o argumento. `-` , que significa nenhum.

Converta servidores de chaves primárias e secundárias

Você pode seguir os passos abaixo para alterar a designação (primária ou secundária) de servidores de chave específicos.

Converter um servidor de chave primária em um servidor de chave secundária.

Passos

1. Remova o servidor de chave primária da SVM:

   `security key-manager external remove-servers`

   > Se você estiver executando o `security key-manager external remove-servers` Para executar o comando no SVM de administração em uma configuração MetroCluster , você deve executar o comando em ambos os clusters. Se você estiver executando o comando para um SVM de dados individual, não precisa executá-lo em ambos os clusters.

2. Realize oCrie um servidor de chaves em cluster Procedimento que utiliza o antigo servidor de chaves primárias como servidor de chaves secundárias.

Converter um servidor de chaves secundário em um servidor de chaves primário.

Passos

1. Remova o servidor de chaves secundário do seu servidor de chaves primário existente:

   `security key-manager external modify-server -secondary-key-servers`

- Se você estiver executando o `security key-manager external modify-server -secondary -key-servers` Para executar o comando no SVM de administração em uma configuração MetroCluster , você deve executar o comando em ambos os clusters. Se você estiver executando o comando para um SVM de dados individual, não precisa executá-lo em ambos os clusters.
- Se você converter um servidor de chaves secundário em um servidor de chaves primário enquanto remove um servidor de chaves existente, tentar adicionar um novo servidor de chaves antes de concluir a remoção e a conversão pode resultar na duplicação de chaves.

1. Realize oCrie um servidor de chaves em cluster Procedimento que utiliza o antigo servidor de chaves secundário como servidor de chaves primário do novo servidor de chaves em cluster.

Consulte[mod-secondary] para mais informações.

Informações relacionadas

- Saiba mais sobre `security key-manager external` no"Referência do comando 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 do 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. Saiba mais sobre `security key-manager key create` o "Referência do comando ONTAP"na .

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: <id_value>
```

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.
>
> 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: <id_value>
node1                                   NSE-AK    yes
    Key ID: <id_value>

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                 Key Type  Restored
--------------------------------------  --------  --------
node2                                   NSE-AK    yes
    Key ID: <id_value>
node2                                   NSE-AK    yes
    Key ID: <id_value>
```

Saiba mais sobre `security key-manager key query` o "Referência do comando ONTAP"na .

Informações relacionadas

- "exibição de disco de criptografia de armazenamento"

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`

   Saiba mais sobre `security key-manager create-key` o "Referência do comando ONTAP"na .

   > 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: <id_value>

   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`

Saiba mais sobre `security key-manager query` o "Referência do comando ONTAP"na .

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: <id_value>


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

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-02     NSE-AK    yes
       Key ID: <id_value>
```

Atribuir uma chave de autenticação de dados a uma unidade FIPS ou SED com gerenciamento de chaves externas ONTAP

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`

   Saiba mais sobre `storage encryption disk modify` o "Referência do comando ONTAP"na .

   > 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
   <id_value>

   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`

   Saiba mais sobre `storage encryption disk show` o "Referência do comando ONTAP"na .

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

Informações relacionadas

- "exibição de disco de criptografia de armazenamento"
- "disco de criptografia de armazenamento mostrar-status"

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 autocriptografia.

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.

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. 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 encriptação 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 de atualização verifica se o conteúdo da imagem não foi alterado ou corrompido, verificando várias assinaturas digitais. Se a validação funcionar, a atualização da imagem vai para a próxima etapa. Se a validação não funcionar, a atualização da imagem falhará. Saiba mais sobre `cluster image` no"Referência do comando ONTAP" .

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 de configurar o Gerenciador de chaves integrado.

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:

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 carateres, 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 o sistema cria as chaves de autenticação:

   `security key-manager key query -node node`

   > 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 .

Depois de terminar

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

O sistema faz backup automaticamente das principais informações de gerenciamento no banco de dados replicado (RDB) do cluster. Você também deve fazer backup dessas informações manualmente para recuperação de desastres.

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"
- "Transição para o gerenciamento de chaves integrado do gerenciamento de chaves externas"

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 Onboard Key Manager para proteger as chaves que o cluster usa para acessar dados criptografados. Habilite o Onboard Key Manager em cada cluster que acessa volumes criptografados ou discos autocriptografados.

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 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 carateres ou, para "cc-mode", uma frase-passe entre 64 e 256 carateres.

Se a senha "'cc-mode'" especificada for inferior a 64 carateres, 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`

   Saiba mais sobre `security key-manager show-key-store` no"Referência do comando ONTAP" .

```
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
```

Depois de terminar

O ONTAP faz backup automático das informações de gerenciamento de chaves no banco de dados replicado (RDB) do cluster.

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

- "Faça backup manual das informações de gerenciamento de chaves integradas"
- "configuração do gerenciador de chaves de segurança"
- "gerenciador de chaves de segurança mostrar-armazenamento-de-chaves"
- "Transição para o gerenciamento de chaves integrado do gerenciamento de chaves externas"

Atribua uma chave de autenticação de dados a uma unidade FIPS ou SED com gerenciamento de chaves integrado ONTAP

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`

   Saiba mais sobre `storage encryption disk modify` o "Referência do comando ONTAP"na .

   > 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
   <id_value>

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

   Saiba mais sobre `security key-manager key query` o "Referência do comando ONTAP"na .

2. Verifique se as chaves de autenticação foram atribuídas:

   `storage encryption disk show`

   Saiba mais sobre `storage encryption disk show` o "Referência do comando ONTAP"na .

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

Informações relacionadas

- "exibição de disco de criptografia de armazenamento"
- "disco de criptografia de armazenamento mostrar-status"

Atribuir uma chave de autenticação FIPS 140-2 a uma unidade ONTAP 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 140-2-2. 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
   <id_value>

   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`

   Saiba mais sobre `storage encryption disk show` o "Referência do comando ONTAP"na .

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

Informações relacionadas

- "modificação de disco de criptografia de armazenamento"
- "exibição de disco de criptografia de armazenamento"
- "disco de criptografia de armazenamento mostrar-status"

Habilite o modo compatível com FIPS em todo o cluster para conexões de servidor KMIP no ONTAP

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 conetar 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
   ```

   Saiba mais sobre `security config show` o "Referência do comando ONTAP"na .

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

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

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

Saiba mais sobre `security config modify` o "Referência do comando ONTAP"na .

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

Informações sobre direitos autorais

Informações sobre marcas comerciais