



Configurar o gerenciamento de chaves externas

ONTAP 9

NetApp
February 12, 2026

Índice

Configurar o gerenciamento de chaves externas	1
Saiba mais sobre como configurar o gerenciamento de chaves externas ONTAP	1
Instalar certificados SSL no cluster ONTAP	1
Habilitar gerenciamento de chaves externas para criptografia baseada em hardware no ONTAP 9.6 e posterior	2
Habilitar gerenciamento de chaves externas para criptografia baseada em hardware no ONTAP 9.5 e versões anteriores	4
Configurar servidores de chaves externas em cluster no ONTAP	5
Crie um servidor de chaves em cluster	6
Modificar servidores de chaves em cluster	8
Crie chaves de autenticação no ONTAP 9.6 e posterior	9
Crie chaves de autenticação no ONTAP 9.5 e anteriores	11
Atribuir uma chave de autenticação de dados a uma unidade FIPS ou SED com gerenciamento de chaves externas ONTAP	13

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 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.
- 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 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. 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:

```
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. Saiba mais sobre `security key-manager external show-status` no ["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
```

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



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

4. Adicione um servidor KMIP adicional para redundância:

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

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



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

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

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

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

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

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

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

```
volume encryption conversion start
```

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

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 o [Crie 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 o [Crie 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

- 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` no ["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"](#)

Informações sobre direitos autorais

Copyright © 2026 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

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

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

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

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

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

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

Informações sobre marcas comerciais

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