



# Configurar o gerenciamento de chaves integradas

ONTAP 9

NetApp  
February 12, 2026

# Índice

- Configurar o gerenciamento de chaves integradas ..... 1
  - Habilite o gerenciamento de chaves integradas no ONTAP 9.6 e posterior ..... 1
  - Habilite o gerenciamento de chaves integradas no ONTAP 9.5 e versões anteriores ..... 3
  - Atribua uma chave de autenticação de dados a uma unidade FIPS ou SED com gerenciamento de chaves integrado ONTAP ..... 6

# 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.

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 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 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 autcriptografados.

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



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

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

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

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 autcriptografia 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 autcriptografia, 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"](#)

## Informações sobre direitos autorais

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

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

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS 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.