



Gerenciar a criptografia NetApp

ONTAP 9

NetApp
January 08, 2026

Índice

Gerenciar a criptografia NetApp	1
Descriptografe dados de volume no ONTAP	1
Mova um volume criptografado no ONTAP	1
Altere a chave de criptografia de um volume com o comando de início de rechavear de criptografia de volume no ONTAP	2
Alterar a chave de criptografia de um volume com o comando ONTAP volume move start	4
Gire as chaves de autenticação para criptografia de armazenamento ONTAP NetApp	5
Excluir um volume criptografado no ONTAP	5
Limpe os dados com segurança em um volume criptografado	6
Saiba mais sobre como limpar dados com segurança de um volume ONTAP criptografado	6
Limpar dados de um volume ONTAP criptografado sem um relacionamento SnapMirror	7
Limpar dados de um volume ONTAP criptografado com um relacionamento assíncrono SnapMirror	8
Limpar dados de um volume ONTAP criptografado com um relacionamento síncrono SnapMirror	10
Alterar a senha de gerenciamento de chaves onboard do ONTAP	12
Faça backup manualmente das informações de gerenciamento de chaves de bordo do ONTAP	13
Restaurar chaves de criptografia integradas de gerenciamento de chaves no ONTAP	15
ONTAP 9 F.6 e mais tarde	15
ONTAP 9.8 ou posterior com volume de raiz criptografado	15
ONTAP 9 F.5 e anteriores	16
Restaurar chaves de criptografia de gerenciamento de chaves externas ONTAP	16
Substituir certificados SSL KMIP no cluster ONTAP	17
Substitua uma unidade FIPS ou SED no ONTAP	18
Tornar os dados em uma unidade FIPS ou SED inacessíveis	20
Aprenda a tornar os dados ONTAP em uma unidade FIPS ou SED inacessíveis	20
Higienize uma unidade FIPS ou SED em ONTAP	21
Destrua uma unidade FIPS ou SED no ONTAP	23
Dados de emergência cortados em uma unidade FIPS ou SED no ONTAP	24
Retorne uma unidade FIPS ou SED ao serviço quando as chaves de autenticação forem perdidas no ONTAP	28
Retornar uma unidade FIPS ou SED ao modo desprotegido no ONTAP	30
Modo de manutenção	32
Remova uma conexão externa do gerenciador de chaves no ONTAP	33
Modificar propriedades do servidor de gerenciamento de chaves externas ONTAP	34
Transição para o gerenciamento de chaves externas do gerenciamento de chaves integrado no ONTAP	35
Mude do gerenciamento de chaves externas para o gerenciamento de chaves integrado ONTAP	36
O que acontece quando os servidores de gerenciamento de chaves não estão acessíveis durante o processo de inicialização do ONTAP	37
Desabilitar criptografia ONTAP por padrão	39

Gerenciar a criptografia NetApp

Descriptografe dados de volume no ONTAP

Você pode usar o `volume move start` comando para mover e descriptografar dados de volume.

Antes de começar

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

Passos

1. Mova um volume criptografado existente e descriptografe os dados no volume:

```
volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false
```

Saiba mais sobre `volume move start` o ["Referência do comando ONTAP"](#) na .

O comando a seguir move um volume existente nomeado `vol1` para o agregado de destino `aggr3` e descriptografa os dados no volume:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination-aggregate aggr3 -encrypt-destination false
```

O sistema exclui a chave de criptografia do volume. Os dados no volume não são criptografados.

2. Verifique se o volume está desativado para criptografia:

```
volume show -encryption
```

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

O comando a seguir exibe se os volumes em `cluster1` são criptografados:

```
cluster1::> volume show -encryption
```

Vserver	Volume	Aggregate	State	Encryption State
-----	-----	-----	-----	-----
vs1	vol1	aggr1	online	none

Mova um volume criptografado no ONTAP

Você pode usar o `volume move start` comando para mover um volume criptografado. O volume movido pode residir no mesmo agregado ou em um agregado diferente.

Sobre esta tarefa

A movimentação falhará se o nó de destino ou o volume de destino não suportar criptografia de volume.

A `-encrypt-destination` opção para `volume move start` o padrão é verdadeiro para volumes criptografados. O requisito para especificar que não deseja que o volume de destino seja criptografado garante que você não descriptografe inadvertidamente os dados no volume.

Antes de começar

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

Passos

1. Mova um volume criptografado existente e deixe os dados no volume criptografados:

```
volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name
```

Saiba mais sobre `volume move start` o ["Referência do comando ONTAP"](#) na .

O comando a seguir move um volume existente nomeado `vol1` para o agregado de destino `aggr3` e deixa os dados no volume criptografados:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination -aggregate aggr3
```

2. Verifique se o volume está ativado para criptografia:

```
volume show -is-encrypted true
```

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

O comando a seguir exibe os volumes criptografados em `cluster1`:

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
-----	-----	-----	-----	-----	-----	-----	-----
vs1	vol1	aggr3	online	RW	200GB	160.0GB	20%

Altere a chave de criptografia de um volume com o comando de início de rechavear de criptografia de volume no ONTAP

É uma prática recomendada de segurança alterar a chave de criptografia para um volume periodicamente. A partir do ONTAP 9.3, você pode usar o `volume encryption rekey start` comando para alterar a chave de criptografia.

Sobre esta tarefa

Depois de iniciar uma operação de rechavear, ela deve ser concluída. Não há retorno à chave antiga. Se você encontrar um problema de desempenho durante a operação, você pode executar o `volume encryption rekey pause` comando para pausar a operação e o `volume encryption rekey resume` comando para retomar a operação.

Até que a operação de rechavear termine, o volume terá duas teclas. Novas gravações e suas leituras correspondentes usarão a nova chave. Caso contrário, as leituras usarão a chave antiga.



Você não pode usar `volume encryption rekey start` para rechavear um volume SnapLock.

Passos

1. Alterar uma chave de encriptação:

```
volume encryption rekey start -vserver SVM_name -volume volume_name
```

O comando a seguir altera a chave de criptografia `vol1` no `SVMvs1`:

```
cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
```

2. Verifique o estado da operação de rechavear:

```
volume encryption rekey show
```

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

O seguinte comando apresenta o estado da operação de rechavear:

```
cluster1::> volume encryption rekey show
```

Vserver	Volume	Start Time	Status
-----	-----	-----	-----
vs1	vol1	9/18/2017 17:51:41	Phase 2 of 2 is in progress.

3. Quando a operação de rechavear estiver concluída, verifique se o volume está ativado para encriptação:

```
volume show -is-encrypted true
```

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

O comando a seguir exibe os volumes criptografados em `cluster1`:

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
-----	-----	-----	-----	-----	-----	-----	-----
vs1	vol1	aggr2	online	RW	200GB	160.0GB	20%

Alterar a chave de criptografia de um volume com o comando ONTAP volume move start

É uma prática recomendada de segurança alterar a chave de criptografia para um volume periodicamente. Você pode usar o `volume move start` comando para alterar a chave de criptografia. O volume movido pode residir no mesmo agregado ou em um agregado diferente.

Sobre esta tarefa

Você não pode usar `volume move start` para rechavear um volume SnapLock ou FlexGroup.

Antes de começar

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

Passos

1. Mova um volume existente e altere a chave de criptografia:

```
volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -generate-destination-key true
```

Saiba mais sobre `volume move start` o ["Referência do comando ONTAP"](#) na .

O comando a seguir move um volume existente nomeado **vol1** para o agregado de destino **aggr2** e altera a chave de criptografia:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination -aggregate aggr2 -generate-destination-key true
```

Uma nova chave de criptografia é criada para o volume. Os dados no volume permanecem criptografados.

2. Verifique se o volume está ativado para criptografia:

```
volume show -is-encrypted true
```

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

O comando a seguir exibe os volumes criptografados em `cluster1`:

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
-----	-----	-----	-----	-----	-----	-----	-----
vs1	vol1	aggr2	online	RW	200GB	160.0GB	20%

Gire as chaves de autenticação para criptografia de armazenamento ONTAP NetApp

Você pode girar as chaves de autenticação ao usar a criptografia de armazenamento NetApp (NSE).

Sobre esta tarefa

A rotação de chaves de autenticação em um ambiente NSE é suportada se você estiver usando o KMIP (External Key Manager).



A rotação de chaves de autenticação em um ambiente NSE não é compatível com OKM (Onboard Key Manager).

Passos

1. Use o `security key-manager create-key` comando para gerar novas chaves de autenticação.

É necessário gerar novas chaves de autenticação antes de poder alterar as chaves de autenticação.

2. Use o `storage encryption disk modify -disk * -data-key-id` comando para alterar as chaves de autenticação.

Informações relacionadas

- ["modificação de disco de criptografia de armazenamento"](#)

Excluir um volume criptografado no ONTAP

Você pode usar o `volume delete` comando para excluir um volume criptografado.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- O volume deve estar offline.

Passo

1. Eliminar um volume encriptado:

```
volume delete -vserver SVM_name -volume volume_name
```

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

O comando a seguir exclui um volume criptografado chamado `vol1`:

```
cluster1::> volume delete -vserver vs1 -volume vol1
```

Digite `yes` quando for solicitado que você confirme a exclusão.

O sistema exclui a chave de criptografia do volume após 24 horas.

Use `volume delete` com a `-force true` opção para excluir um volume e destruir a chave de criptografia correspondente imediatamente. Este comando requer Privileges avançado. Saiba mais sobre `volume delete` no ["Referência do comando ONTAP"](#) na .

Depois de terminar

Você pode usar o `volume recovery-queue` comando para recuperar um volume excluído durante o período de retenção após a emissão do `volume delete` comando:

```
volume recovery-queue SVM_name -volume volume_name
```

["Como usar o recurso recuperação de volume"](#)

Limpe os dados com segurança em um volume criptografado

Saiba mais sobre como limpar dados com segurança de um volume ONTAP criptografado

A partir do ONTAP 9.4, você usa a limpeza segura para limpeza de dados em volumes habilitados para NVE sem interrupções. A análise de dados em um volume criptografado garante que ele não possa ser recuperado da Mídia física, por exemplo, em casos de "spillage", onde os rastreamentos de dados podem ter sido deixados para trás quando os blocos foram substituídos, ou para excluir com segurança os dados de um local em vazio.

A limpeza segura funciona apenas para arquivos excluídos anteriormente em volumes habilitados para NVE. Não é possível limpar um volume não criptografado. Você precisa usar servidores KMIP para fornecer chaves, não o gerenciador de chaves integrado.

Considerações sobre a utilização de uma purga segura

- Os volumes criados em um agregado habilitado para NetApp Aggregate Encryption (NAE) não oferecem suporte à limpeza segura.
- A limpeza segura funciona apenas para arquivos excluídos anteriormente em volumes habilitados para NVE.
- Não é possível limpar um volume não criptografado.
- Você precisa usar servidores KMIP para fornecer chaves, não o gerenciador de chaves integrado.

A limpeza segura funciona de forma diferente, dependendo da sua versão do ONTAP.

ONTAP 9 F.8 e mais tarde

- A purga segura é suportada pelo MetroCluster e pelo FlexGroup.
- Se o volume a ser purgado for a origem de uma relação SnapMirror, não é necessário interromper a relação SnapMirror para executar uma limpeza segura.
- O método de recryptografia é diferente para volumes que usam a proteção de dados do SnapMirror em vez de volumes que não usam a proteção de dados do SnapMirror (DP) ou aqueles que usam a proteção de dados estendida do SnapMirror.
 - Por padrão, os volumes que usam o modo de proteção de dados SnapMirror (DP) recryptografam os dados usando o método de recryptografia de movimentação de volume.
 - Por padrão, os volumes que não usam a proteção de dados SnapMirror ou volumes que usam o modo SnapMirror Extended Data Protection (XDP) usam o método de recryptografia no local.
 - Esses padrões podem ser alterados usando o `secure purge re-encryption-method [volume-move|in-place-rekey]` comando.
- Por padrão, todos os snapshots em volumes FlexVol são excluídos automaticamente durante a operação de limpeza segura. Por padrão, os snapshots em volumes e volumes do FlexGroup que usam a proteção de dados do SnapMirror não são excluídos automaticamente durante a operação de limpeza segura. Esses padrões podem ser alterados usando o `secure purge delete-all-snapshots [true|false]` comando.

ONTAP 9.7 e anteriores:

- A purga segura não suporta o seguinte:
 - FlexClone
 - SnapVault
 - FabricPool
- Se o volume que está sendo purgado for a origem de uma relação do SnapMirror, você deve quebrar a relação do SnapMirror antes de poder limpar o volume.

Se houver snapshots ocupados no volume, você deverá liberar os snapshots antes de limpar o volume. Por exemplo, talvez seja necessário dividir um volume FlexClone de seu pai.

- Chamar com êxito o recurso de limpeza segura aciona uma movimentação de volume que recryptografa os dados restantes e não limpos com uma nova chave.

O volume movido permanece no agregado atual. A chave antiga é destruída automaticamente, garantindo que os dados purgados não possam ser recuperados da Mídia de armazenamento.

Limpar dados de um volume ONTAP criptografado sem um relacionamento SnapMirror

A partir do ONTAP 9.4, você pode usar a limpeza segura para dados "crostas" sem interrupções em volumes habilitados para NVE.

Sobre esta tarefa

A limpeza segura pode levar de vários minutos a muitas horas para ser concluída, dependendo da quantidade de dados nos arquivos excluídos. Pode utilizar o `volume encryption secure-purge show` comando para visualizar o estado da operação. Você pode usar o `volume encryption secure-purge abort`

comando para encerrar a operação.



Para fazer uma limpeza segura em um host SAN, você deve excluir todo o LUN que contém os arquivos que deseja limpar, ou você deve ser capaz de perfurar buracos no LUN para os blocos que pertencem aos arquivos que deseja limpar. Se você não puder excluir o LUN ou o sistema operacional do host não suportar furos no LUN, não será possível executar uma limpeza segura.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- São necessários Privileges avançados para esta tarefa.

Passos

1. Exclua os arquivos ou o LUN que você deseja limpar com segurança.
 - Em um cliente nas, exclua os arquivos que você deseja limpar com segurança.
 - Em um host SAN, exclua o LUN que você deseja limpar com segurança ou perfurar buracos no LUN para os blocos que pertencem aos arquivos que deseja limpar.
2. No sistema de armazenamento, altere para nível de privilégio avançado:

```
set -privilege advanced
```

3. Se os arquivos que você deseja limpar com segurança estiverem em snapshots, exclua os snapshots:

```
snapshot delete -vserver SVM_name -volume volume_name -snapshot
```

4. Limpe com segurança os arquivos excluídos:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name
```

O comando a seguir limpa com segurança os arquivos excluídos vol1 no SVMvs1:

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume  
vol1
```

5. Verifique o estado da operação de purga segura:

```
volume encryption secure-purge show
```

Limpar dados de um volume ONTAP criptografado com um relacionamento assíncrono SnapMirror

A partir do ONTAP 9.8, você pode usar uma limpeza segura para dados "cruzadores" sem interrupções em volumes habilitados para NVE com uma relação assíncrona do SnapMirror.

Antes de começar

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

- São necessários Privileges avançados para esta tarefa.

Sobre esta tarefa

A limpeza segura pode levar de vários minutos a muitas horas para ser concluída, dependendo da quantidade de dados nos arquivos excluídos. Pode utilizar o `volume encryption secure-purge show` comando para visualizar o estado da operação. Você pode usar o `volume encryption secure-purge abort` comando para encerrar a operação.



Para fazer uma limpeza segura em um host SAN, você deve excluir todo o LUN que contém os arquivos que deseja limpar, ou você deve ser capaz de perfurar buracos no LUN para os blocos que pertencem aos arquivos que deseja limpar. Se você não puder excluir o LUN ou o sistema operacional do host não suportar furos no LUN, não será possível executar uma limpeza segura.

Passos

1. No sistema de armazenamento, mude para o nível de privilégio avançado:

```
set -privilege advanced
```

2. Exclua os arquivos ou o LUN que você deseja limpar com segurança.

- Em um cliente nas, exclua os arquivos que você deseja limpar com segurança.
- Em um host SAN, exclua o LUN que você deseja limpar com segurança ou perfurar buracos no LUN para os blocos que pertencem aos arquivos que deseja limpar.

3. Prepare o volume de destino na relação assíncrona para ser purgado com segurança:

```
volume encryption secure-purge start -vserver SVM_name -volume volume_name  
-prepare true
```

Repita esta etapa em cada volume em sua relação assíncrona do SnapMirror.

4. Se os arquivos que você deseja limpar com segurança estiverem em snapshots, exclua os snapshots:

```
snapshot delete -vserver SVM_name -volume volume_name -snapshot
```

5. Se os arquivos que você deseja limpar com segurança estiverem nos snapshots base, faça o seguinte:

- a. Crie um instantâneo no volume de destino na relação assíncrona do SnapMirror:

```
volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume  
volume_name
```

- b. Atualize o SnapMirror para mover o instantâneo base para a frente:

```
snapmirror update -source-snapshot snapshot_name -destination-path  
destination_path
```

Repita esta etapa para cada volume na relação assíncrona do SnapMirror.

- a. Repita as etapas (a) e (b) iguais ao número de instantâneos base mais um.

Por exemplo, se você tiver dois snapshots base, repita as etapas (a) e (b) três vezes.

- b. Verifique se o instantâneo base está presente `snapshot show -vserver SVM_name -volume volume_name`
- c. Eliminar o instantâneo base `snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot`

6. Limpe com segurança os arquivos excluídos:

```
volume encryption secure-purge start -vserver svm_name -volume volume_name
```

Repita esta etapa em cada volume na relação assíncrona do SnapMirror.

O seguinte comando limpa com segurança os arquivos excluídos no "vol1" na SVM "VS1":

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume vol1
```

7. Verifique o estado da operação de purga segura:

```
volume encryption secure-purge show
```

Informações relacionadas

- ["atualização do snapmirror"](#)

Limpar dados de um volume ONTAP criptografado com um relacionamento síncrono SnapMirror

A partir do ONTAP 9.8, você pode usar uma limpeza segura para "limpar" dados em volumes habilitados para NVE sem interrupções, com uma relação síncrona SnapMirror.

Sobre esta tarefa

Uma limpeza segura pode levar de vários minutos a muitas horas para ser concluída, dependendo da quantidade de dados nos arquivos excluídos. Pode utilizar o `volume encryption secure-purge show` comando para visualizar o estado da operação. Você pode usar o `volume encryption secure-purge abort` comando para encerrar a operação.



Para fazer uma limpeza segura em um host SAN, você deve excluir todo o LUN que contém os arquivos que deseja limpar, ou você deve ser capaz de perfurar buracos no LUN para os blocos que pertencem aos arquivos que deseja limpar. Se você não puder excluir o LUN ou o sistema operacional do host não suportar furos no LUN, não será possível executar uma limpeza segura.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- São necessários Privileges avançados para esta tarefa.

Passos

1. No sistema de armazenamento, altere para nível de privilégio avançado:

```
set -privilege advanced
```

2. Exclua os arquivos ou o LUN que você deseja limpar com segurança.

- Em um cliente nas, exclua os arquivos que você deseja limpar com segurança.
- Em um host SAN, exclua o LUN que você deseja limpar com segurança ou perfurar buracos no LUN para os blocos que pertencem aos arquivos que deseja limpar.

3. Prepare o volume de destino na relação assíncrona para ser purgado com segurança:

```
volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
-prepare true
```

Repita esta etapa para o outro volume em sua relação síncrona do SnapMirror.

4. Se os arquivos que você deseja limpar com segurança estiverem em snapshots, exclua os snapshots:

```
snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
```

5. Se o arquivo de limpeza segura estiver na base ou em snapshots comuns, atualize o SnapMirror para mover o snapshot comum para frente:

```
snapmirror update -source-snapshot <snapshot_name> -destination-path
<destination_path>
```

Há dois snapshots comuns, portanto, esse comando deve ser emitido duas vezes.

6. Se o arquivo de limpeza segura estiver no snapshot consistente com o aplicativo, exclua o snapshot em ambos os volumes na relação síncrona do SnapMirror:

```
snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
```

Execute esta etapa em ambos os volumes.

7. Limpe com segurança os arquivos excluídos:

```
volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
```

Repita esta etapa em cada volume na relação síncrona do SnapMirror.

O comando a seguir limpa com segurança os arquivos excluídos no "vol1" no SVM "VS1".

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

8. Verifique o estado da operação de purga segura:

```
volume encryption secure-purge show
```

Informações relacionadas

- ["atualização do snapmirror"](#)

Alterar a senha de gerenciamento de chaves onboard do ONTAP

A NetApp recomenda que você altere regularmente a senha de gerenciamento de chaves integradas. Você deve armazenar a nova senha em um local seguro fora do sistema de armazenamento.

Antes de começar

- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.
- São necessários Privileges avançados para esta tarefa.
- Em um ambiente MetroCluster , após atualizar a senha no cluster local, sincronize a atualização da senha no cluster parceiro.

Passos

1. Alterar para nível de privilégio avançado:

```
set -privilege advanced
```

2. Alterar a senha de gerenciamento da chave integrada. O comando que você usa depende da versão do ONTAP que você está executando.

ONTAP 9 F.6 e mais tarde

```
security key-manager onboard update-passphrase
```

ONTAP 9 F.5 e anteriores

```
security key-manager update-passphrase
```

3. 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.

4. No prompt de confirmação da senha, redigite a senha.
5. Se você estiver em uma configuração MetroCluster , sincronize a senha atualizada no cluster parceiro.
 - a. Sincronize a senha no cluster parceiro selecionando o comando correto para a sua versão do ONTAP :

ONTAP 9 F.6 e mais tarde

```
security key-manager onboard sync
```

ONTAP 9 F.5 e anteriores

- No ONTAP 9.5, execute:

```
security key-manager setup -sync-metrocluster-config
```

- No ONTAP 9.4 e versões anteriores, após atualizar a senha no cluster local, aguarde 20 segundos e execute o seguinte comando no cluster parceiro:

```
security key-manager setup
```

- b. Digite a nova senha quando solicitado.

A mesma senha deve ser usada em ambos os clusters.

Depois de terminar

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

Faça backup manual das informações de gerenciamento de chaves sempre que alterar a senha de gerenciamento de chaves integrada.

Informações relacionadas

- ["Faça backup manual das informações de gerenciamento de chaves integradas"](#)
- ["gerenciador de chaves de segurança integrado atualização de frase-senha"](#)

Faça backup manualmente das informações de gerenciamento de chaves de bordo do ONTAP

Você deve copiar as informações de gerenciamento de chaves integradas para um local seguro fora do sistema de armazenamento sempre que configurar a senha do Gerenciador de chaves integrado.

Antes de começar

- Você deve ser um administrador de cluster para executar esta tarefa.
- São necessários Privileges avançados para esta tarefa.

Sobre esta tarefa

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

Passos

1. Alterar para nível de privilégio avançado:

```
set -privilege advanced
```

2. Apresentar as informações de cópia de segurança da gestão de chaves para o cluster:

Para esta versão ONTAP...	Use este comando...
ONTAP 9 F.6 e mais tarde	<code>security key-manager onboard show-backup</code>
ONTAP 9 F.5 e anteriores	<code>security key-manager backup show</code>

O comando 9.6 a seguir exibe as informações de backup do gerenciamento de chaves para `cluster1` :

```
cluster1::> security key-manager onboard show-backup
```

[illegible]

3. Copie as informações de backup para um local seguro fora do sistema de armazenamento para uso em caso de desastre.

Informações relacionadas

- ["gerenciador de chaves de segurança a bordo show-backup"](#)
- ["exibição de backup do gerenciador de chaves de segurança"](#)

Restaurar chaves de criptografia integradas de gerenciamento de chaves no ONTAP

Ocasionalmente, pode ser necessário restaurar uma chave de criptografia de gerenciamento de chaves integrada. Depois de verificar se uma chave precisa ser restaurada, você pode configurar o Onboard Key Manager para restaurá-la. O procedimento a ser seguido para restaurar suas chaves de criptografia de gerenciamento de chaves onboard varia de acordo com sua versão do ONTAP.

Antes de começar

- Exclua o banco de dados do gerenciador de chaves externo se você usar o NSE com um servidor KMIP externo. Para mais detalhes, veja ["Transição do gerenciamento de chaves externas para o gerenciamento de chaves onboard do ONTAP"](#).
- Você deve ser um administrador de cluster para executar esta tarefa.



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.

ONTAP 9 F.6 e mais tarde



Se você estiver executando o ONTAP 9.8 ou posterior e o volume raiz estiver criptografado, siga o procedimento para [\[ontap-9-8\]](#).

1. Verifique se a chave precisa ser restaurada `security key-manager key query -node node`

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

2. Restaurar a chave `security key-manager onboard sync`

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

3. No prompt de frase-passe, insira a senha de gerenciamento de chave integrada para o cluster.

ONTAP 9.8 ou posterior com volume de raiz criptografado

Se você estiver executando o ONTAP 9.8 e posterior e seu volume raiz estiver criptografado, defina uma senha de recuperação de gerenciamento de chaves integrado com o menu de inicialização. Este processo também é necessário se você fizer uma substituição de Mídia de inicialização.

1. Inicialize o nó no menu de inicialização e selecione a opção (10) `Set onboard key management recovery secrets`.

2. Enter `y` para utilizar esta opção.
3. No prompt, insira a senha de gerenciamento de chaves integradas para o cluster.
4. No prompt, insira os dados da chave de backup.

Após inserir os dados da chave de backup, o nó retorna ao menu de inicialização.

5. No menu de inicialização, selecione a opção (1) `Normal Boot`.

ONTAP 9 F.5 e anteriores

1. Verifique se a chave precisa ser restaurada `security key-manager key show`
2. Restaurar a chave `security key-manager setup -node node`

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

3. No prompt de frase-passe, insira a senha de gerenciamento de chave integrada para o cluster.

Restaurar chaves de criptografia de gerenciamento de chaves externas ONTAP

Você pode restaurar manualmente as chaves de criptografia de gerenciamento de chaves externas e enviá-las para um nó diferente. Você pode querer fazer isso se estiver reiniciando um nó que estava inativo temporariamente quando criou as chaves para o cluster.

Sobre esta tarefa

No ONTAP 9.6 e posterior, você pode usar o `security key-manager key query -node node_name` comando para verificar se sua chave precisa ser restaurada.

No ONTAP 9.5 e anteriores, você pode usar o `security key-manager key show` comando para verificar se sua chave precisa ser restaurada.



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.

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

Antes de começar

Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passos

1. Se você estiver executando o ONTAP 9.8 ou posterior e o volume raiz estiver criptografado, faça o seguinte:

Se você estiver executando o ONTAP 9.7 ou anterior, ou se estiver executando o ONTAP 9.8 ou posterior e o volume raiz não estiver criptografado, pule esta etapa.

- a. Defina os bototargs `setenv kmip.init.ipaddr <ip-address> setenv kmip.init.netmask <netmask> setenv kmip.init.gateway <gateway> setenv kmip.init.interface e0M`

boot_ontap

- b. Inicialize o nó no menu de inicialização e selecione a opção (11) `Configure node for external key management`.
- c. Siga as instruções para inserir o certificado de gerenciamento.

Depois que todas as informações do certificado de gerenciamento forem inseridas, o sistema retornará ao menu de inicialização.

- d. No menu de inicialização, selecione a opção (1) `Normal Boot`.

2. Restaure a chave:

Para esta versão ONTAP...	Use este comando...
ONTAP 9 F.6 e mais tarde	<code>`security key-manager external restore -vserver SVM -node node -key-server host_name`</code>
<code>IP_address:port -key-id key_id -key -tag key_tag`</code>	ONTAP 9 F.5 e anteriores



`node` o padrão é todos os nós.

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

O seguinte comando ONTAP 9.6 restaura chaves de autenticação de gerenciamento de chaves externas para todos os nós no `cluster1`:

```
cluster1::> security key-manager external restore
```

Informações relacionadas

- ["restauração externa do gerenciador de chaves de segurança"](#)

Substituir certificados SSL KMIP no cluster ONTAP

Todos os certificados SSL têm uma data de validade. Você deve atualizar seus certificados antes que eles expirem para evitar a perda de acesso às chaves de autenticação.

Antes de começar

- Você precisa ter obtido o certificado público de substituição e a chave privada do cluster (certificado de cliente KMIP).
- Você deve ter obtido o certificado público de substituição para o servidor KMIP (certificado KMIP Server-CA).
- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.
- Se você estiver substituindo os certificados SSL KMIP em um ambiente MetroCluster, instale o mesmo certificado SSL KMIP de substituição em ambos os clusters.



Você pode instalar os certificados de cliente e servidor de substituição no servidor KMIP antes ou depois de instalar os certificados no cluster.

Passos

1. Instale o novo certificado KMIP Server-CA:

```
security certificate install -type server-ca -vserver <>
```

2. Instale o novo certificado de cliente KMIP:

```
security certificate install -type client -vserver <>
```

3. Atualize a configuração do gerenciador de chaves para usar os certificados recém-instalados:

```
security key-manager external modify -vserver <> -client-cert <> -server-ca  
-certs <>
```

Se você estiver executando o ONTAP 9.6 ou posterior em um ambiente MetroCluster e quiser modificar a configuração do gerenciador de chaves no SVM admin, execute o comando nos dois clusters na configuração.



Atualizar a configuração do gerenciador de chaves para usar os certificados recém-instalados retornará um erro se as chaves públicas/privadas do novo certificado do cliente forem diferentes das chaves instaladas anteriormente. Veja o "[Base de conhecimento da NetApp : As novas chaves públicas ou privadas do certificado do cliente são diferentes do certificado do cliente existente](#)" para obter instruções sobre como substituir esse erro.

Informações relacionadas

- "[instalação do certificado de segurança](#)"
- "[modificação externa do gerenciador de chaves de segurança](#)"

Substitua uma unidade FIPS ou SED no ONTAP

Você pode substituir uma unidade FIPS ou SED da mesma forma que substitui um disco comum. Certifique-se de atribuir novas chaves de autenticação de dados à unidade de substituição. Para uma unidade FIPS, você também pode querer atribuir uma nova chave de autenticação FIPS 140-2-2.



Se um par de HA estiver usando "[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.

Antes de começar

- Você deve saber o ID da chave para a chave de autenticação usada pela unidade.
- Você deve ser um administrador de cluster para executar esta tarefa.

Passos

1. Certifique-se de que o disco foi marcado como com falha:

```
storage disk show -broken
```

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

```
cluster1::> storage disk show -broken
Original Owner: cluster1-01
Checksum Compatibility: block
```

Physical											Usable
Disk	Outage	Reason	HA	Shelf	Bay	Chan	Pool	Type	RPM	Size	
Size											
-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----
0.0.0	admin	failed	0b	1	0	A	Pool0	FCAL	10000	132.8GB	
133.9GB											
0.0.7	admin	removed	0b	2	6	A	Pool1	FCAL	10000	132.8GB	
134.2GB											
[...]											

2. Remova o disco com falha e substitua-o por uma nova unidade FIPS ou SED, seguindo as instruções no guia de hardware do modelo de compartimento de disco.

3. Atribua a propriedade do disco recém-substituído:

```
storage disk assign -disk disk_name -owner node
```

Saiba mais sobre `storage disk assign` o ["Referência do comando ONTAP"](#) na .

```
cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
```

4. Confirme se o novo disco foi atribuído:

```
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>		
-------	------	------------	--	--

1.10.0	data	<id_value>		
--------	------	------------	--	--

1.10.1	data	<id_value>		
--------	------	------------	--	--

2.1.1	open	0x0		
-------	------	-----	--	--

[...]				
-------	--	--	--	--

5. Atribua as chaves de autenticação de dados à unidade FIPS ou SED.

["Atribuição de uma chave de autenticação de dados a uma unidade FIPS ou SED \(gerenciamento de chaves externas\)"](#)

6. Se necessário, atribua uma chave de autenticação FIPS 140-2-2 à unidade FIPS.

["Atribuição de uma chave de autenticação FIPS 140-2-2 a uma unidade FIPS"](#)

Informações relacionadas

- ["atribuição de disco de armazenamento"](#)
- ["exibição do disco de armazenamento"](#)
- ["exibição de disco de criptografia de armazenamento"](#)

Tornar os dados em uma unidade FIPS ou SED inacessíveis

Aprenda a tornar os dados ONTAP em uma unidade FIPS ou SED inacessíveis

Se você quiser tornar os dados em uma unidade FIPS ou SED permanentemente inacessíveis, mas manter o espaço não utilizado da unidade disponível para novos dados, você pode higienizar o disco. Se você quiser tornar os dados permanentemente inacessíveis e você não precisa reutilizar a unidade, você pode destruí-la.

- Sanitização de disco

Quando você limpa uma unidade de autocriptografia, o sistema altera a chave de criptografia de disco para um novo valor aleatório, redefine o estado de bloqueio de inicialização para falso e define o ID da chave para um valor padrão, seja a ID segura do fabricante 0x0 (unidades SAS) ou uma chave nula (unidades NVMe). Isso torna os dados no disco inacessíveis e impossível de recuperar. Você pode reutilizar discos higienizados como discos sobressalentes não zerados.

- Destruição de disco

Quando você destrói uma unidade FIPS ou SED, o sistema define a chave de criptografia de disco para um valor aleatório desconhecido e bloqueia o disco irreversivelmente. Isso torna o disco permanentemente inutilizável e os dados nele permanentemente inacessíveis.

Você pode higienizar ou destruir unidades de autcriptografia individuais ou todas as unidades de autcriptografia de um nó.

Higienize uma unidade FIPS ou SED em ONTAP

Se você quiser tornar os dados em uma unidade FIPS ou SED permanentemente inacessíveis e usar a unidade para novos dados, use o `storage encryption disk sanitize` comando para higienizar a unidade.

Sobre esta tarefa

Quando você limpa uma unidade de autcriptografia, o sistema altera a chave de criptografia de disco para um novo valor aleatório, redefine o estado de bloqueio de inicialização para falso e define o ID da chave para um valor padrão, seja a ID segura do fabricante 0x0 (unidades SAS) ou uma chave nula (unidades NVMe). Isso torna os dados no disco inacessíveis e impossível de recuperar. Você pode reutilizar discos higienizados como discos sobressalentes não zerados.

Antes de começar

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

Passos

1. Migre qualquer dado que precise ser preservado para um agregado em outro disco.
2. Exclua o agregado na unidade FIPS ou SED para ser higienizado:

```
storage aggregate delete -aggregate aggregate_name
```

```
cluster1::> storage aggregate delete -aggregate aggr1
```

Saiba mais sobre `storage aggregate delete` o ["Referência do comando ONTAP"](#) na .

3. Identifique a ID do disco para a unidade FIPS ou SED a ser higienizada:

```
storage encryption disk show -fields data-key-id,fips-key-id,owner
```

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>
1.10.2    data <id_value>
[...]
```

4. Se uma unidade FIPS estiver em execução no modo de conformidade com FIPS, defina o ID da chave de autenticação FIPS para o nó novamente para o MSID padrão 0x0:

```
storage encryption disk modify -disk disk_id -fips-key-id 0x0
```

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

```
cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0
```

Info: Starting modify on 1 disk.

View the status of the operation by using the
storage encryption disk show-status command.

5. Higienize a unidade:

```
storage encryption disk sanitize -disk disk_id
```

Você pode usar este comando para higienizar discos hot spare ou quebrados somente. Para higienizar todos os discos independentemente do tipo, use a `-force-all-state` opção. Saiba mais sobre `storage encryption disk sanitize` o ["Referência do comando ONTAP"](#) na .



O ONTAP solicitará que você insira uma frase de confirmação antes de continuar. Insira a frase exatamente como mostrado na tela.

```
cluster1::> storage encryption disk sanitize -disk 1.10.2
```

Warning: This operation will cryptographically sanitize 1 spare or
broken self-encrypting disk on 1 node.

To continue, enter sanitize disk: sanitize disk

Info: Starting sanitize on 1 disk.

View the status of the operation using the
storage encryption disk show-status command.

6. Desfalhe o disco higienizado: `storage disk unfail -spare true -disk disk_id`

7. Verifique se o disco tem um proprietário: `storage disk show -disk disk_id` Se o disco não tem um proprietário, atribua um. `storage disk assign -owner node -disk disk_id`

8. Introduza o nodeshell para o nó que possui os discos que pretende higienizar:

```
system node run -node node_name
```

Executar o `disk sanitize release` comando.

9. Saia do nodeshell. Desfalhe o disco novamente: `storage disk unfail -spare true -disk disk_id`

10. Verifique se o disco agora está sobressalente e pronto para ser reutilizado em um agregado: `storage disk show -disk disk_id`

Informações relacionadas

- ["atribuição de disco de armazenamento"](#)
- ["exibição do disco de armazenamento"](#)
- ["disco de armazenamento infalível"](#)
- ["modificação de disco de criptografia de armazenamento"](#)
- ["criptografia de armazenamento e higienização de disco"](#)
- ["disco de criptografia de armazenamento mostrar-status"](#)

Destrua uma unidade FIPS ou SED no ONTAP

Se você quiser tornar os dados em uma unidade FIPS ou SED permanentemente inacessíveis e não precisar reutilizar a unidade, use o `storage encryption disk destroy` comando para destruir o disco.

Sobre esta tarefa

Quando você destrói uma unidade FIPS ou SED, o sistema define a chave de criptografia de disco para um valor aleatório desconhecido e bloqueia a unidade irreversivelmente. Isso torna o disco praticamente inutilizável e os dados nele permanentemente inacessíveis. No entanto, você pode redefinir o disco para suas configurações configuradas de fábrica usando a ID física segura (PSID) impressa na etiqueta do disco. Para obter mais informações, ["Retornar uma unidade FIPS ou SED ao serviço quando as chaves de autenticação são perdidas"](#) consulte .



Você não deve destruir uma unidade FIPS ou SED, a menos que tenha o serviço Non-Returnable Disk Plus (NRD Plus). Destruir um disco anula sua garantia.

Antes de começar

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

Passos

1. Migre qualquer dado que precise ser preservado para um agregado em outro disco diferente.
2. Exclua o agregado na unidade FIPS ou SED a ser destruído:

```
storage aggregate delete -aggregate aggregate_name
```

```
cluster1::> storage aggregate delete -aggregate aggr1
```

Saiba mais sobre `storage aggregate delete` o ["Referência do comando ONTAP"](#) na .

3. Identifique a ID do disco para a unidade FIPS ou SED a ser destruída:

```
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>
```

```
1.10.2   data <id_value>
```

```
[...]
```

4. Destrua o disco:

```
storage encryption disk destroy -disk disk_id
```

Saiba mais sobre `storage encryption disk destroy` o ["Referência do comando ONTAP"](#) na .



É-lhe pedido que introduza uma frase de confirmação antes de continuar. Insira a frase exatamente como mostrado na tela.

```
cluster1::> storage encryption disk destroy -disk 1.10.2
```

```
Warning: This operation will cryptographically destroy 1 spare or broken  
self-encrypting disks on 1 node.
```

```
You cannot reuse destroyed disks unless you revert  
them to their original state using the PSID value.
```

```
To continue, enter
```

```
destroy disk
```

```
:destroy disk
```

```
Info: Starting destroy on 1 disk.
```

```
View the status of the operation by using the  
"storage encryption disk show-status" command.
```

Informações relacionadas

- ["criptografia de armazenamento, destruição de disco"](#)
- ["exibição de disco de criptografia de armazenamento"](#)
- ["disco de criptografia de armazenamento mostrar-status"](#)

Dados de emergência cortados em uma unidade FIPS ou SED no ONTAP

Em caso de emergência de segurança, você pode impedir instantaneamente o acesso a uma unidade FIPS ou SED, mesmo que a energia não esteja disponível para o sistema de armazenamento ou para o servidor KMIP.

Antes de começar

- Se você estiver usando um servidor KMIP que não tem energia disponível, o servidor KMIP deve ser configurado com um item de autenticação facilmente destruído (por exemplo, um smart card ou unidade USB).
- Você deve ser um administrador de cluster para executar esta tarefa.

Passo

1. Execute a fragmentação de emergência de dados em uma unidade FIPS ou SED:

Se...	Então...
-------	----------

<p>A energia está disponível para o sistema de armazenamento e você tem tempo para colocar o sistema de armazenamento offline graciosamente</p>	<ol style="list-style-type: none"> Se o sistema de storage estiver configurado como um par de HA, desative o takeover. Tire todos os agregados off-line e exclua-os. Defina o nível de privilégio como avançado <code>set -privilege advanced</code> Se a unidade estiver no modo de conformidade FIPS, defina o ID da chave de autenticação FIPS para o nó de volta para o MSID padrão <code>storage encryption disk modify -disk * -fips-key-id 0x0</code> Parar o sistema de storage. Arranque no modo de manutenção. Sanitize ou destrua os discos: <ol style="list-style-type: none"> Se você quiser tornar os dados nos discos inacessíveis e ainda conseguir reutilizar os discos, limpe os discos <code>disk encrypt sanitize -all</code> Se você quiser tornar os dados nos discos inacessíveis e você não precisa salvar os discos, destrua os discos <code>disk encrypt destroy disk_id1 disk_id2 ...</code> 	<p>A energia está disponível para o sistema de armazenamento e você deve destruir os dados imediatamente</p>
---	---	--

<p>a. Se você quiser tornar os dados nos discos inacessíveis e ainda conseguir reutilizar os discos, higienize os discos:</p> <p>b. Se o sistema de storage estiver configurado como um par de HA, desative o takeover.</p> <p>c. Defina o nível de privilégio como avançado:</p> <pre>set -privilege advanced</pre> <p>d. Se a unidade estiver no modo de conformidade FIPS, defina o ID da chave de autenticação FIPS para o nó de volta para o MSID padrão:</p> <pre>storage encryption disk modify -disk * -fips-key-id 0x0</pre> <p>e. Higienizar o disco:</p> <pre>storage encryption disk sanitize -disk * -force-all-states true</pre>	<p>a. Se você quiser tornar os dados nos discos inacessíveis e não precisar salvar os discos, destrua os discos:</p> <p>b. Se o sistema de storage estiver configurado como um par de HA, desative o takeover.</p> <p>c. Defina o nível de privilégio como avançado:</p> <pre>set -privilege advanced</pre> <p>d. Destrua os discos: storage encryption disk destroy -disk * -force -all-states true</p>	<p>O sistema de armazenamento entra em pânico, deixando o sistema em um estado permanentemente desativado com todos os dados apagados. Para utilizar novamente o sistema, tem de o reconfigurar.</p>
<p>A energia está disponível para o servidor KMIP, mas não para o sistema de storage</p>	<p>a. Faça login no servidor KMIP.</p> <p>b. Destrua todas as chaves associadas às unidades FIPS ou SEDs que contenham os dados aos quais você deseja impedir o acesso. Isso impede o acesso a chaves de criptografia de disco pelo sistema de armazenamento.</p>	<p>A energia não está disponível para o servidor KMIP nem para o sistema de storage</p>

Informações relacionadas

- ["criptografia de armazenamento, destruição de disco"](#)
- ["modificação de disco de criptografia de armazenamento"](#)
- ["criptografia de armazenamento e higienização de disco"](#)

Retorne uma unidade FIPS ou SED ao serviço quando as chaves de autenticação forem perdidas no ONTAP

O sistema trata uma unidade FIPS ou SED como quebrado se você perder as chaves de autenticação permanentemente e não conseguir recuperá-las do servidor KMIP. Embora você não possa acessar ou recuperar os dados no disco, você pode tomar medidas para tornar o espaço não utilizado do SED disponível novamente para os dados.

Antes de começar

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

Sobre esta tarefa

Deve utilizar este processo apenas se tiver a certeza de que as chaves de autenticação para a unidade FIPS ou SED estão permanentemente perdidas e que não pode recuperá-las.

Se os discos forem particionados, eles devem primeiro ser desparticionados antes de iniciar esse processo.



O comando para desparticionar um disco está disponível somente no nível de diagnóstico e deve ser executado somente sob a supervisão do Suporte da NetApp . **É altamente recomendável que você entre em contato com o Suporte da NetApp antes de prosseguir.** Você também pode consultar o "[Base de conhecimento da NetApp : Como desparticionar uma unidade reserva no ONTAP](#)" .

Passos

1. Retornar uma unidade FIPS ou SED à manutenção:

Se os SEDS são...	Siga estes passos...
-------------------	----------------------

<p>Não está no modo de conformidade FIPS nem no modo de conformidade FIPS, e a chave FIPS está disponível</p>	<ol style="list-style-type: none"> a. Defina o nível de privilégio como avançado: <code>set -privilege advanced</code> b. Reponha a chave FIPS para a ID segura de fabricação padrão 0x0: <code>storage encryption disk modify -fips-key-id 0x0 -disk <i>disk_id</i></code> c. Verifique se a operação foi bem-sucedida: <code>storage encryption disk show-status</code> Se a operação falhou, use o processo PSID neste tópico. d. Sanitize o disco quebrado: <code>storage encryption disk sanitize -disk <i>disk_id</i></code> Verifique se a operação foi bem-sucedida com o comando <code>storage encryption disk show-status</code> antes de prosseguir para a próxima etapa. e. Desfalhe o disco higienizado: <code>storage disk unfail -spare true -disk <i>disk_id</i></code> f. Verifique se o disco tem um proprietário: <code>storage disk show -disk <i>disk_id</i></code> Se o disco não tem um proprietário, atribua um. <code>storage disk assign -owner node -disk <i>disk_id</i></code> <ol style="list-style-type: none"> i. Introduza o nodeshell para o nó que possui os discos que pretende higienizar: <code>system node run -node <i>node_name</i></code> <p>Executar o <code>disk sanitize release</code> comando.</p> g. Saia do nodeshell. Desfalhe o disco novamente: <code>storage disk unfail -spare true -disk <i>disk_id</i></code> h. Verifique se o disco agora está sobressalente e pronto para ser reutilizado em um agregado: <code>storage disk show -disk <i>disk_id</i></code>
---	--

<p>No modo de conformidade com o FIPS, a chave FIPS não está disponível e os SEDs têm um PSID impresso na etiqueta</p>	<ol style="list-style-type: none"> a. Obtenha o PSID do disco a partir da etiqueta do disco. b. Defina o nível de privilégio como avançado: <code>set -privilege advanced</code> c. Redefina o disco para suas configurações configuradas de fábrica: <code>storage encryption disk revert-to-original-state -disk <i>disk_id</i> -psid <i>disk_physical_secure_id</i></code> Verifique se a operação foi bem-sucedida com o comando <code>storage encryption disk show-status</code> antes de prosseguir para a próxima etapa. d. Se você estiver executando o ONTAP 9.8P5 ou anterior, vá para a próxima etapa. Se você estiver executando o ONTAP 9.8P6 ou posterior, desmarque o disco higienizado. <code>storage disk unfaill -disk <i>disk_id</i></code> e. Verifique se o disco tem um proprietário: <code>storage disk show -disk <i>disk_id</i></code> Se o disco não tem um proprietário, atribua um. <code>storage disk assign -owner node -disk <i>disk_id</i></code> <ol style="list-style-type: none"> i. Introduza o nodeshell para o nó que possui os discos que pretende higienizar: <code>system node run -node <i>node_name</i></code> <p>Executar o <code>disk sanitize release</code> comando.</p> f. Saia do nodeshell.. Desfalhe o disco novamente: <code>storage disk unfaill -spare true -disk <i>disk_id</i></code> g. Verifique se o disco agora está sobressalente e pronto para ser reutilizado em um agregado: <code>storage disk show -disk <i>disk_id</i></code>
--	---

Informações relacionadas

- ["modificação de disco de criptografia de armazenamento"](#)
- ["disco de criptografia de armazenamento reverte ao estado original"](#)
- ["criptografia de armazenamento e higienização de disco"](#)
- ["disco de criptografia de armazenamento mostrar-status"](#)

Retornar uma unidade FIPS ou SED ao modo desprotegido no ONTAP

Uma unidade FIPS ou SED é protegida contra acesso não autorizado somente se o ID da chave de autenticação para o nó estiver definido para um valor diferente do padrão. Você pode retornar uma unidade FIPS ou SED para o modo desprotegido usando o `storage encryption disk modify` comando para definir o ID da chave como padrão. Uma unidade FIPS ou SED no modo desprotegido usa as chaves de criptografia padrão, enquanto uma unidade FIPS ou SED no modo protegido usa chaves de

criptografia secretas fornecidas. Se houver dados criptografados na unidade e a unidade for redefinida para o modo desprotegido, os dados ainda serão criptografados e não serão expostos.



Siga este procedimento para garantir que quaisquer dados criptografados se tornem inacessíveis depois que a unidade FIPS ou o SED retornar ao modo desprotegido. Depois que os FIPS e os IDs das chaves de dados são redefinidos, os dados existentes não podem ser descriptografados e se tornam inacessíveis, a menos que as chaves originais sejam restauradas.

Se um par de HA estiver usando a criptografia de unidades SAS ou NVMe (SED, NSE, FIPS), siga este processo para todas as unidades dentro 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.

Antes de começar

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

Passos

1. Defina o nível de privilégio como avançado:

```
set -privilege advanced
```

2. Se uma unidade FIPS estiver em execução no modo de conformidade com FIPS, defina o ID da chave de autenticação FIPS para o nó novamente para o MSID padrão 0x0:

```
storage encryption disk modify -disk disk_id -fips-key-id 0x0
```

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

```
cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id 0x0
```

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

Confirme a operação com sucesso com o comando:

```
storage encryption disk show-status
```

Repita o comando `show-status` até que os números em "Disks Begun" e "Disks Done" sejam os mesmos.

```
cluster1:: storage encryption disk show-status
```

	FIPS	Latest	Start		Execution	Disks
Disks	Disks					
Node	Support	Request	Timestamp		Time (sec)	Begun
Done	Successful					
-----	-----	-----	-----	-----	-----	-----
-----	-----					
cluster1	true	modify	1/18/2022 15:29:38	3	14	5
5						

1 entry was displayed.

3. Defina o ID da chave de autenticação de dados para o nó de volta para o MSID padrão 0x0:

```
storage encryption disk modify -disk disk_id -data-key-id 0x0
```

O valor de `-data-key-id` deve ser definido como 0x0 se você estiver retornando uma unidade SAS ou NVMe para o modo desprotegido.

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

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id 0x0
```

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

Confirme a operação com sucesso com o comando:

```
storage encryption disk show-status
```

Repita o comando `show-status` até que os números sejam os mesmos. A operação estará concluída quando os números em "discos iniciados" e "discos concluídos" forem iguais.

Modo de manutenção

Começando com ONTAP 9.7, você pode rechavear uma unidade FIPS a partir do modo de manutenção. Você só deve usar o modo de manutenção se não puder usar as instruções da CLI do ONTAP na seção anterior.

Passos

1. Defina o ID da chave de autenticação FIPS para o nó de volta para o MSID padrão 0x0:

```
disk encrypt rekey_fips 0x0 disklist
```

2. Defina o ID da chave de autenticação de dados para o nó de volta para o MSID padrão 0x0:

```
disk encrypt rekey 0x0 disklist
```

3. Confirme se a chave de autenticação FIPS foi rekeyed com êxito:

```
disk encrypt show_fips
```

4. Confirmar chave de autenticação de dados foi rekeyed com sucesso com:

```
disk encrypt show
```

Sua saída provavelmente exibirá o ID de chave padrão MSID 0x0 ou o valor de 64 caracteres mantido pelo servidor de chaves. O `Locked?` campo refere-se ao bloqueio de dados.

Disk	FIPS Key ID	Locked?
0a.01.0	0x0	Yes

Informações relacionadas

- ["modificação de disco de criptografia de armazenamento"](#)
- ["disco de criptografia de armazenamento mostrar-status"](#)

Remova uma conexão externa do gerenciador de chaves no ONTAP

Você pode desconectar um servidor KMIP de um nó quando não precisar mais do servidor. Por exemplo, você pode desconectar um servidor KMIP quando estiver migrando para a criptografia de volume.

Sobre esta tarefa

Ao desconectar um servidor KMIP de um nó em um par de HA, o sistema desconecta automaticamente o servidor de todos os nós de cluster.



Se você pretende continuar usando o gerenciamento de chaves externas depois de desconectar um servidor KMIP, verifique se outro servidor KMIP está disponível para servir as chaves de autenticação.

Antes de começar

Você deve ser um administrador de cluster ou SVM para executar essa tarefa.

Passo

1. Desconecte um servidor KMIP do nó atual:

Para esta versão ONTAP...	Use este comando...
ONTAP 9 F.6 e mais tarde	<code>`security key-manager external remove-servers -vserver SVM -key -servers host_name`</code>

IP_address:port,...`	ONTAP 9 F.5 e anteriores
----------------------	--------------------------

Em um ambiente do MetroCluster, você deve repetir esses comandos nos dois clusters para o SVM de administrador.

O seguinte comando ONTAP 9.6 desativa as conexões a dois servidores de gerenciamento de chaves externas para `cluster1`, o primeiro chamado `ks1`, ouvindo na porta padrão 5696, o segundo com o endereço IP 10.0.0.20, ouvindo na porta 24482:

```
cluster1::> security key-manager external remove-servers -vserver  
cluster-1 -key-servers ks1,10.0.0.20:24482
```

Saiba mais sobre `security key-manager external remove-servers` e `security key-manager delete` no ["Referência do comando ONTAP"](#).

Modificar propriedades do servidor de gerenciamento de chaves externas ONTAP

A partir do ONTAP 9.6, você pode usar o `security key-manager external modify-server` comando para alterar o tempo limite de e/S e o nome de usuário de um servidor de gerenciamento de chaves externo.

Antes de começar

- Você deve ser um administrador de cluster ou SVM para executar essa tarefa.
- São necessários Privileges avançados para esta tarefa.
- Em um ambiente do MetroCluster, repita essas etapas nos dois clusters para o SVM de administrador.

Passos

1. No sistema de armazenamento, altere para nível de privilégio avançado:

```
set -privilege advanced
```

2. Modifique as propriedades do servidor do gerenciador de chaves externo para o cluster:

```
security key-manager external modify-server -vserver admin_SVM -key-server  
host_name|IP_address:port,... -timeout 1...60 -username user_name
```



O valor de tempo limite é expresso em segundos. Se você modificar o nome de usuário, será solicitado que você insira uma nova senha. Se você executar o comando no prompt de login do cluster, `admin_SVM` o padrão será o administrador SVM do cluster atual. Você deve ser o administrador do cluster para modificar as propriedades do servidor do gerenciador de chaves externo.

O comando a seguir altera o valor de tempo limite para 45 segundos para que o `cluster1` servidor de gerenciamento de chaves externo esteja escutando na porta padrão 5696:

```
cluster1::> security key-manager external modify-server -vserver  
cluster1 -key-server ks1.local -timeout 45
```

3. Modificar as propriedades do servidor do gerenciador de chaves externo para uma SVM (somente NVE):

```
security key-manager external modify-server -vserver SVM -key-server  
host_name|IP_address:port,... -timeout 1...60 -username user_name
```



O valor de tempo limite é expresso em segundos. Se você modificar o nome de usuário, será solicitado que você insira uma nova senha. Se você executar o comando no prompt de login SVM, *SVM* o padrão será SVM atual. Você deve ser o administrador do cluster ou SVM para modificar as propriedades do servidor do gerenciador de chaves externo.

O comando a seguir altera o nome de usuário e a senha do *svm1* servidor de gerenciamento de chaves externo ouvindo na porta padrão 5696:

```
svm1::> security key-manager external modify-server -vserver svm11 -key  
-server ks1.local -username svm1user  
Enter the password:  
Reenter the password:
```

4. Repita a última etapa para quaisquer SVMs adicionais.

Informações relacionadas

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

Transição para o gerenciamento de chaves externas do gerenciamento de chaves integrado no ONTAP

Se você quiser alternar para o gerenciamento de chaves externas do gerenciamento de chaves integradas, exclua a configuração de gerenciamento de chaves integradas antes de habilitar o gerenciamento de chaves externas.

Antes de começar

- Para criptografia baseada em hardware, é necessário redefinir as chaves de dados de todas as unidades FIPS ou SEDs para o valor padrão.

["Retornar uma unidade FIPS ou SED para o modo desprotegido"](#)

- Para criptografia baseada em software, você deve descriptografar todos os volumes.

["Uncryptografando dados de volume"](#)

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

Passo

1. Exclua a configuração de gerenciamento de chaves integradas para um cluster:

Para esta versão ONTAP...	Use este comando...
ONTAP 9 F.6 e mais tarde	<code>security key-manager onboard disable -vserver SVM</code>
ONTAP 9 F.5 e anteriores	<code>security key-manager delete-key-database</code>

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

Mude do gerenciamento de chaves externas para o gerenciamento de chaves integrado ONTAP

Para alternar para o gerenciamento de chaves integrado, exclua a configuração de gerenciamento de chaves externas antes de habilitar o gerenciamento de chaves integrado.

Antes de começar

- Para criptografia baseada em hardware, é necessário redefinir as chaves de dados de todas as unidades FIPS ou SEDs para o valor padrão.

["Retornar uma unidade FIPS ou SED para o modo desprotegido"](#)

- Você deve ter excluído todas as conexões externas do gerenciador de chaves.

["Excluindo uma conexão externa do gerenciador de chaves"](#)

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

Passos

As etapas para fazer a transição do gerenciamento de chaves dependem da versão do ONTAP que você está usando.

ONTAP 9 F.6 e mais tarde

1. Mude para o nível de privilégio avançado:

```
set -privilege advanced
```

2. Use o comando:

```
security key-manager external disable -vserver admin_SVM
```



Em um ambiente MetroCluster, você deve repetir o comando nos dois clusters para o SVM de administrador.

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

ONTAP 9 F.5 e anteriores

Use o comando:

```
security key-manager delete-knip-config
```

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

Informações relacionadas

- ["desabilitação externa do gerenciador de chaves de segurança"](#)

O que acontece quando os servidores de gerenciamento de chaves não estão acessíveis durante o processo de inicialização do ONTAP

O ONTAP toma certas precauções para evitar um comportamento indesejado caso um sistema de armazenamento configurado para NSE não alcance nenhum dos servidores de gerenciamento de chaves especificados durante o processo de inicialização.

Se o sistema de armazenamento estiver configurado para NSE, os SEDs são rekeyed e locked e os SEDs são ligados, o sistema de armazenamento deve recuperar as chaves de autenticação necessárias dos servidores de gerenciamento de chaves para se autenticar nos SEDs antes de poder acessar os dados.

O sistema de armazenamento tenta contactar os servidores de gestão de chaves especificados durante até três horas. Se o sistema de armazenamento não puder alcançar nenhum deles depois desse tempo, o processo de inicialização será interrompido e o sistema de armazenamento será interrompido.

Se o sistema de armazenamento entrar em Contato com qualquer servidor de gerenciamento de chaves especificado, ele tentará estabelecer uma conexão SSL por até 15 minutos. Se o sistema de armazenamento não puder estabelecer uma conexão SSL com qualquer servidor de gerenciamento de chaves especificado, o processo de inicialização será interrompido e o sistema de armazenamento será interrompido.

Enquanto o sistema de armazenamento tenta entrar em Contato e se conectar a servidores de gerenciamento de chaves, ele exibe informações detalhadas sobre as tentativas de Contato com falha na CLI. Você pode

interromper as tentativas de Contato a qualquer momento pressionando Ctrl-C.

Como medida de segurança, os SEDs permitem apenas um número limitado de tentativas de acesso não autorizado, após o qual desativam o acesso aos dados existentes. Se o sistema de armazenamento não puder contactar qualquer servidor de gestão de chaves especificado para obter as chaves de autenticação adequadas, só poderá tentar autenticar com a chave predefinida, o que leva a uma tentativa de falha e a um pânico. Se o sistema de armazenamento estiver configurado para reiniciar automaticamente em caso de pânico, ele entra em um loop de inicialização que resulta em tentativas de autenticação com falha contínua nos SEDs.

Parar o sistema de armazenamento nesses cenários é por projeto para impedir que o sistema de armazenamento entre em um loop de inicialização e possível perda não intencional de dados como resultado dos SEDs bloqueados permanentemente devido a exceder o limite de segurança de um certo número de tentativas consecutivas de autenticação falhadas. O limite e o tipo de proteção de bloqueio dependem das especificações de fabricação e do tipo de SED:

Tipo de SED	Número de tentativas consecutivas falhadas de autenticação, resultando em bloqueio	Tipo de proteção de bloqueio quando o limite de segurança é atingido
HDD	1024	Permanente. Os dados não podem ser recuperados, mesmo quando a chave de autenticação adequada se torna disponível novamente.
X440_PHM2800MCTO 800GB SSDs NSE com revisões de firmware NA00 ou NA01	5	Temporário. O bloqueio só está em vigor até que o disco seja ligado a um ciclo de energia.
X577_PHM2800MCTO 800GB SSDs NSE com revisões de firmware NA00 ou NA01	5	Temporário. O bloqueio só está em vigor até que o disco seja ligado a um ciclo de energia.
X440_PHM2800MCTO 800GB SSDs NSE com revisões de firmware mais altas	1024	Permanente. Os dados não podem ser recuperados, mesmo quando a chave de autenticação adequada se torna disponível novamente.
X577_PHM2800MCTO 800GB SSDs NSE com revisões de firmware mais altas	1024	Permanente. Os dados não podem ser recuperados, mesmo quando a chave de autenticação adequada se torna disponível novamente.
Todos os outros modelos de SSD	1024	Permanente. Os dados não podem ser recuperados, mesmo quando a chave de autenticação adequada se torna disponível novamente.

Para todos os tipos de SED, uma autenticação bem-sucedida redefine a contagem de tentativas para zero.

Se você encontrar este cenário em que o sistema de armazenamento é interrompido devido a falha em alcançar qualquer servidor de gerenciamento de chaves especificado, primeiro você deve identificar e corrigir

a causa da falha de comunicação antes de tentar continuar inicializando o sistema de armazenamento.

Desabilitar criptografia ONTAP por padrão

A partir do ONTAP 9.7, a criptografia de volume e agregado é ativada por padrão se você tiver uma licença de criptografia de volume (VE) e usar um gerenciador de chaves integrado ou externo. Se necessário, você pode desativar a criptografia por padrão para todo o cluster.

Antes de começar

Você deve ser um administrador de cluster para executar essa tarefa ou um administrador SVM a quem o administrador de cluster delegou autoridade.

Passo

1. Para desativar a criptografia por padrão para todo o cluster no ONTAP 9.7 ou posterior, execute o seguinte comando:

```
options -option-name encryption.data_at_rest_encryption.disable_by_default  
-option-value on
```

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 SOBRESSAIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES DOCUMENTOS, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

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

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

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

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

Informações sobre marcas comerciais

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