Limpe os dados com segurança em um volume criptografado

ONTAP 9

NetApp
January 17, 2025

Índice

Limpe os dados com segurança em um volume criptografado

Limpe os dados com segurança em uma visão geral de volume 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 locatário 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 recriptografia 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) recriptografam os dados usando o método de recriptografia 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 recriptografia no local.
  - Esses padrões podem ser alterados usando o `secure purge re-encryption-method [volume-move|in-place-rekey]` comando.
- Por padrão, todas as cópias Snapshot nos volumes FlexVol são automaticamente excluídas 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 cópias snapshot ocupadas no volume, você precisará liberar as cópias Snapshot para poder 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 recriptografa 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.

Limpe os dados com segurança em um volume criptografado sem uma relação com o 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 SVM`vs1`:

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

5. Verifique o estado da operação de purga segura:

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

Limpe com segurança os dados em um volume criptografado com uma relação assíncrona do 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 cópias Snapshot, exclua as cópias Snapshot:

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

5. Se os arquivos que você deseja limpar com segurança estiverem nas cópias Snapshot base, faça o seguinte:

   a. Crie uma cópia Snapshot 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 a cópia Snapshot base para 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 cópias Snapshot base mais uma.

   Por exemplo, se você tiver duas cópias Snapshot básicas, repita as etapas (a) e (b) três vezes.

b. Verifique se a cópia Snapshot base está presente `snapshot show -vserver *SVM_name* -volume *volume_name*`

c. Eliminar a cópia Snapshot 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`

Limpeza de dados em um volume criptografado com uma relação síncrona 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 cópias Snapshot, exclua as cópias Snapshot:

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

5. Se o arquivo de limpeza segura estiver na base ou nas cópias Snapshot comuns, atualize o SnapMirror para mover a cópia Snapshot comum para frente:

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

   Há duas cópias Snapshot comuns, portanto, esse comando deve ser emitido duas vezes.

6. Se o arquivo de limpeza segura estiver na cópia Snapshot consistente com o aplicativo, exclua a cópia 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 sobre direitos autorais

Informações sobre marcas comerciais