Löschen Sie Daten auf einem verschlüsselten Volume sicher

ONTAP 9

NetApp
April 24, 2024

Inhalt

Löschen Sie Daten auf einem verschlüsselten Volume sicher

Löschen Sie Daten sicher auf einer Übersicht über ein verschlüsseltes Volume

Ab ONTAP 9.4 können Sie Daten auf NVE-fähigen Volumes durch sicheres Löschen unterbrechungsfrei abspeichern. Das Scrubbing von Daten auf einem verschlüsselten Volume stellt sicher, dass sie nicht von physischen Medien wiederhergestellt werden können, beispielsweise bei „`s` pillage“, bei denen Spuren von Daten beim Überschreiben von Blöcken hinterlassen wurden oder zum sicheren Löschen der Daten eines Mandanten.

Secure Purge ist nur für zuvor gelöschte Dateien auf Volumes mit NVE geeignet. Sie können ein unverschlüsseltes Volume nicht abreiben. Sie müssen KMIP-Server für die Schlüsselverwendung verwenden, nicht für den integrierten Schlüsselmanager.

Überlegungen zur Verwendung einer sicheren Löschung

- Volumes, die in einem Aggregat erstellt wurden, das für NetApp Aggregate Encryption (NAE) aktiviert ist, unterstützen das sichere Löschen nicht.
- Secure Purge ist nur für zuvor gelöschte Dateien auf Volumes mit NVE geeignet.
- Sie können ein unverschlüsseltes Volume nicht abreiben.
- Sie müssen KMIP-Server für die Schlüsselverwendung verwenden, nicht für den integrierten Schlüsselmanager.

Sichere Spülfunktionen je nach Version von ONTAP unterschiedlich.

ONTAP 9.8 und höher

- Sicheres Löschen wird von MetroCluster und FlexGroup unterstützt.
- Wenn das zu löckige Volume die Quelle einer SnapMirror-Beziehung ist, müssen Sie die SnapMirror-Beziehung nicht unterbrechen, um eine sichere Löschung durchzuführen.
- Die Umverschlüsselungsmethode unterscheidet sich bei Volumes, die SnapMirror Datensicherung verwenden, im Gegensatz zu Volumes, die keine SnapMirror Datensicherung (DP) verwenden, oder solchen, die SnapMirror erweiterte Datensicherung nutzen.
  - Standardmäßig werden Daten bei Volumes im SnapMirror Data Protection (DP)-Modus mit der erneuten Verschlüsselungsmethode für Volume Move neu verschlüsselt.
  - Standardmäßig verwenden Volumes, die keine SnapMirror Datensicherung oder Volumes verwenden, die den XDP-Modus (Extended Data Protection) von SnapMirror verwenden, die in-Place-Reverschlüsselungsmethode.
  - Diese Standardeinstellungen können mit dem geändert werden `secure purge re-encryption-method [volume-move|in-place-rekey]` Befehl.
- Standardmäßig werden alle Snapshot-Kopien in FlexVol Volumes während des sicheren Löschvorgangs automatisch gelöscht. Standardmäßig werden Snapshots in FlexGroup Volumes und Volumes mit SnapMirror Datensicherung nicht automatisch während des sicheren Löschvorgangs gelöscht. Diese Standardeinstellungen können mit dem geändert werden `secure purge delete-all-snapshots [true|false]` Befehl.

ONTAP 9.7 und früher:

- Sicheres Löschen unterstützt Folgendes nicht:
  - FlexClone
  - SnapVault
  - FabricPool
- Wenn das zu löckige Volume die Quelle einer SnapMirror-Beziehung ist, müssen Sie die SnapMirror-Beziehung unterbrechen, bevor Sie das Volume löschen können.

  Falls im Volume bereits Snapshot-Kopien vorhanden sind, müssen Sie die Snapshot-Kopien freigeben, bevor Sie das Volume löschen können. Beispielsweise müssen Sie ein FlexClone Volume unter Umständen von seinem übergeordneten Volume trennen.

- Durch das erfolgreiche Aufrufen der Funktion zum sicheren Löschen wird eine Volume-Verschiebung ausgelöst, die die verbleibenden, nicht gelöschten Daten mit einem neuen Schlüssel erneut verschlüsselt.

  Das verschobene Volume bleibt im aktuellen Aggregat. Der alte Schlüssel wird automatisch zerstört und stellt sicher, dass die gelöschten Daten nicht von den Speichermedien wiederhergestellt werden können.

Löschen Sie Daten auf einem verschlüsselten Volume sicher ohne SnapMirror Beziehung

Ab ONTAP 9.4 können Sie auf NVE-fähigen Volumes sichere Datenlöschung auch für unterbrechungsfreie „`sCrub`“-Daten verwenden.

Über diese Aufgabe

Die sichere Löschung kann in Abhängigkeit von der Datenmenge in den gelöschten Dateien mehrere Minuten bis viele Stunden dauern. Sie können das verwenden `volume encryption secure-purge show` Befehl zum Anzeigen des Status des Vorgangs. Sie können das verwenden `volume encryption secure-purge abort` Befehl zum Beenden des Vorgangs.

> Um eine sichere Löschung auf einem SAN-Host durchzuführen, müssen Sie die gesamte LUN löschen, die die zu löschenden Dateien enthält. Alternativ können Sie Löcher in der LUN für die Blöcke lochen, die zu den Dateien gehören, die gelöscht werden sollen. Wenn Sie die LUN nicht löschen können oder Ihr Host-Betriebssystem keine Stanzlöcher in der LUN unterstützt, können Sie keine sichere Löschung durchführen.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

Schritte

1. Löschen Sie die Dateien oder die LUN, die Sie löschen möchten.
   - Löschen Sie auf einem NAS-Client die Dateien, die Sie sicher löschen möchten.
   - Löschen Sie auf einem SAN-Host die LUN, die Sie löschen oder Löcher in der LUN sicher löschen möchten, damit die Blöcke zu den Dateien gehören, die gelöscht werden sollen.
2. Ändern Sie im Storage-System die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

3. Wenn die Dateien, die Sie sicher löschen möchten, in Snapshots gespeichert sind, löschen Sie die Snapshots:

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

4. Löschen Sie gelöschte Dateien sicher:

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

   Mit dem folgenden Befehl werden die gelöschten Dateien auf sicher gelöscht `vol1` Auf SVM`vs1`:

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

5. Überprüfen Sie den Status des Secure-Purge-Vorgangs:

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

Löschen Sie Daten mit einer asynchronen SnapMirror-Beziehung sicher auf einem verschlüsselten Volume

Ab ONTAP 9.8 kann auf NVE-fähigen Volumes mit einer asynchronen SnapMirror-

Beziehung ein sicheres Löschen von Daten verwendet werden, die unterbrechungsfrei „`sCrub`“ Daten erzeugen.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

Über diese Aufgabe

Die sichere Löschung kann in Abhängigkeit von der Datenmenge in den gelöschten Dateien mehrere Minuten bis viele Stunden dauern. Sie können das verwenden `volume encryption secure-purge show` Befehl zum Anzeigen des Status des Vorgangs. Sie können das verwenden `volume encryption secure-purge abort` Befehl zum Beenden des Vorgangs.

> Um eine sichere Löschung auf einem SAN-Host durchzuführen, müssen Sie die gesamte LUN löschen, die die zu löschenden Dateien enthält. Alternativ können Sie Löcher in der LUN für die Blöcke lochen, die zu den Dateien gehören, die gelöscht werden sollen. Wenn Sie die LUN nicht löschen können oder Ihr Host-Betriebssystem keine Stanzlöcher in der LUN unterstützt, können Sie keine sichere Löschung durchführen.

Schritte

1. Wechseln Sie auf dem Speichersystem auf die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Löschen Sie die Dateien oder die LUN, die Sie löschen möchten.
   - Löschen Sie auf einem NAS-Client die Dateien, die Sie sicher löschen möchten.
   - Löschen Sie auf einem SAN-Host die LUN, die Sie löschen oder Löcher in der LUN sicher löschen möchten, damit die Blöcke zu den Dateien gehören, die gelöscht werden sollen.
3. Bereiten Sie das Zielvolumen in der asynchronen Beziehung vor, die sicher gelöscht werden soll:

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

   Wiederholen Sie diesen Schritt für jedes Volume in Ihrer asynchronen SnapMirror-Beziehung.

4. Wenn die Dateien, die Sie sicher löschen möchten, in Snapshot-Kopien gespeichert sind, löschen Sie die Snapshot-Kopien:

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

5. Wenn sich die Dateien, die Sie sicher löschen möchten, in den Basiskopien befinden, führen Sie folgende Schritte aus:

   a. Erstellung einer Snapshot Kopie auf dem Ziel-Volume in der asynchronen SnapMirror Beziehung:

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

   b. Aktualisieren Sie SnapMirror, um die Snapshot Basiskopie nach vorn zu verschieben:

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

destination_path

Wiederholen Sie diesen Schritt für jedes Volume in der asynchronen SnapMirror-Beziehung.

a. Wiederholen Sie die Schritte (A) und (b) entsprechend der Anzahl der Basis-Snapshot-Kopien plus einer.

   Wenn Sie beispielsweise zwei Basis-Snapshot-Kopien haben, sollten Sie die Schritte (A) und (b) dreimal wiederholen.

b. Überprüfen Sie, ob die Snapshot Basiskopie vorhanden ist:
   `snapshot show -vserver SVM_name -volume volume_name`

c. Löschen Sie die Snapshot Basiskopie:
   `snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot`

6. Löschen Sie gelöschte Dateien sicher:

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

   Wiederholen Sie diesen Schritt für jedes Volume in der asynchronen SnapMirror-Beziehung.

   Mit dem folgenden Befehl werden die gelöschten Dateien auf „`vol1`“ auf SVM „`vs1`“ sicher gelöscht:

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

7. Überprüfen Sie den Status des sicheren Löschvorgangs:

   `volume encryption secure-purge show`

Scrub die Daten auf einem verschlüsselten Volume mit einer synchronen SnapMirror-Beziehung ab

Ab ONTAP 9.8 können Sie ein sicheres Löschen verwenden, um Daten auf NVE-fähigen Volumes mit einer synchronen SnapMirror Beziehung unterbrechungsfrei „zu verschieben“.

Über diese Aufgabe

Eine sichere Löschung kann in Abhängigkeit von der Datenmenge in den gelöschten Dateien von mehreren Minuten bis zu vielen Stunden dauern. Sie können das verwenden `volume encryption secure-purge show` Befehl zum Anzeigen des Status des Vorgangs. Sie können das verwenden `volume encryption secure-purge abort` Befehl zum Beenden des Vorgangs.

> Um eine sichere Löschung auf einem SAN-Host durchzuführen, müssen Sie die gesamte LUN löschen, die die zu löschenden Dateien enthält. Alternativ können Sie Löcher in der LUN für die Blöcke lochen, die zu den Dateien gehören, die gelöscht werden sollen. Wenn Sie die LUN nicht löschen können oder Ihr Host-Betriebssystem keine Stanzlöcher in der LUN unterstützt, können Sie keine sichere Löschung durchführen.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

Schritte

1. Ändern Sie im Storage-System die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Löschen Sie die Dateien oder die LUN, die Sie löschen möchten.
   - Löschen Sie auf einem NAS-Client die Dateien, die Sie sicher löschen möchten.
   - Löschen Sie auf einem SAN-Host die LUN, die Sie löschen oder Löcher in der LUN sicher löschen möchten, damit die Blöcke zu den Dateien gehören, die gelöscht werden sollen.
3. Bereiten Sie das Zielvolumen in der asynchronen Beziehung vor, die sicher gelöscht werden soll:

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

   Wiederholen Sie diesen Schritt für das andere Volume in Ihrer synchronen SnapMirror Beziehung.

4. Wenn die Dateien, die Sie sicher löschen möchten, in Snapshot-Kopien gespeichert sind, löschen Sie die Snapshot-Kopien:

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

5. Falls sich die Datei für die sichere Löschung im Basistelefon oder allgemeinen Snapshot Kopien befindet, aktualisieren Sie das SnapMirror, um die allgemeine Snapshot Kopie vorwärts zu verschieben:

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

   Es gibt zwei gemeinsame Snapshot Kopien. Dieser Befehl muss also zweimal ausgeführt werden.

6. Falls sich die sichere Spüldatei in der applikationskonsistenten Snapshot Kopie befindet, löschen Sie die Snapshot Kopie auf beiden Volumes in der synchronen SnapMirror Beziehung:

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

   Führen Sie diesen Schritt auf beiden Volumes durch.

7. Löschen Sie gelöschte Dateien sicher:

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

   Wiederholen Sie diesen Schritt für jedes Volume in der synchronen SnapMirror-Beziehung.

   Mit dem folgenden Befehl werden die gelöschten Dateien auf „`vol1`“ auf SMV „`vs1`“ sicher gelöscht.

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

8. Überprüfen Sie den Status des sicheren Löschvorgangs:

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