Daten auf einem verschlüsselten Volume sicher löschen

ONTAP 9

NetApp
November 10, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/encryption-at-rest/secure-purge-data-encrypted-volume-concept.html on November 10, 2026. Always check docs.netapp.com for the latest.

Inhalt

Daten auf einem verschlüsselten Volume sicher löschen 1
Informationen zum sicheren Löschen von Daten aus einem verschlüsselten ONTAP Volume 1
Überlegungen zur Verwendung von Secure Purge 1
Verschlüsselte Daten aus einem ONTAP Volume ohne SnapMirror entfernen 2
Bereinigung verschlüsselter Daten aus einem ONTAP Volume mit asynchronem SnapMirror 3
Verschlüsselte Daten aus einem ONTAP Volume mit synchronem SnapMirror bereinigen 5

Daten auf einem verschlüsselten Volume sicher löschen

Informationen zum sicheren Löschen von Daten aus einem verschlüsselten ONTAP Volume

Ab ONTAP 9.4 kann die Funktion „Secure Purge“ verwendet werden, um Daten auf NVE-fähigen Volumes unterbrechungsfrei zu löschen. Das Löschen von Daten auf einem verschlüsselten Volume stellt sicher, dass diese nicht vom physischen Medium wiederhergestellt werden können, zum Beispiel in Fällen von „Spillage“, bei denen Datenspuren beim Überschreiben von Blöcken zurückgeblieben sein könnten, oder um die Daten eines ausscheidenden Mandanten sicher zu löschen.

Die sichere Löschung funktioniert nur für zuvor gelöschte Dateien auf NVE-fähigen Volumes. Ein unverschlüsseltes Volume kann nicht bereinigt werden. Es sind KMIP-Server zur Bereitstellung der Schlüssel zu verwenden, nicht der integrierte Schlüsselmanager.

Überlegungen zur Verwendung von Secure Purge

- Volumes, die in einem für NetApp Aggregate Encryption (NAE) aktivierten Aggregat erstellt wurden, unterstützen kein sicheres Löschen.
- Die sichere Löschung funktioniert nur für zuvor gelöschte Dateien auf NVE-fähigen Volumes.
- Ein unverschlüsseltes Volume kann nicht bereinigt werden.
- Es sind KMIP-Server zur Bereitstellung der Schlüssel zu verwenden, nicht der integrierte Schlüsselmanager.

Die Secure Purge Funktion arbeitet je nach Ihrer ONTAP Version unterschiedlich.

ONTAP 9.8 und höher

- Secure Purge wird von MetroCluster und FlexGroup unterstützt.
- Wenn das zu löschende Volume die Quelle einer SnapMirror Beziehung ist, muss die SnapMirror Beziehung nicht getrennt werden, um eine sichere Löschung durchzuführen.
- Die Methode zur erneuten Verschlüsselung unterscheidet sich für Volumes mit SnapMirror Datenschutz im Vergleich zu Volumes ohne SnapMirror Datenschutz (DP) oder solchen mit SnapMirror erweiterter Datenschutzfunktion.
  - Standardmäßig werden Daten auf Volumes, die den SnapMirror Datenschutzmodus (DP) verwenden, mithilfe der Volume Move Re-Verschlüsselungsmethode erneut verschlüsselt.
  - Standardmäßig verwenden Volumes, die keinen SnapMirror Datenschutz verwenden, oder Volumes, die den SnapMirror erweiterten Datenschutzmodus (XDP) verwenden, die Methode der direkten Neuverschlüsselung.
  - Diese Standardeinstellungen können mit dem `secure purge re-encryption-method [volume-move|in-place-rekey]` Befehl geändert werden.
- Standardmäßig werden alle Snapshots in FlexVol Volumes während der sicheren Bereinigung automatisch gelöscht. Standardmäßig werden Snapshots in FlexGroup Volumes und Volumes, die SnapMirror Datenschutz verwenden, während der sicheren Bereinigung nicht automatisch gelöscht.

Diese Standardeinstellungen können mit dem `secure purge delete-all-snapshots [true|false]` Befehl geändert werden.

ONTAP 9.7 und früher:

- Die sichere Bereinigung unterstützt die folgenden Funktionen nicht:
  - FlexClone
  - SnapVault
  - FabricPool
- Wenn das zu löschende Volumen die Quelle einer SnapMirror Beziehung ist, muss die SnapMirror Beziehung getrennt werden, bevor das Volumen gelöscht werden kann.

  Wenn sich im Volume belegte Snapshots befinden, müssen die Snapshots freigegeben werden, bevor das Volume gelöscht werden kann. Beispielsweise kann es erforderlich sein, ein FlexClone Volume von seinem übergeordneten Volume zu trennen.

- Das erfolgreiche Aufrufen der Funktion „secure-purge“ löst eine Volume-Verschiebung aus, bei der die verbleibenden, nicht gelöschten Daten mit einem neuen Schlüssel neu verschlüsselt werden.

  Das verschobene Volume verbleibt auf dem aktuellen Aggregat. Der alte Schlüssel wird automatisch gelöscht, wodurch sichergestellt wird, dass gelöschte Daten nicht vom Speichermedium wiederhergestellt werden können.

Verschlüsselte Daten aus einem ONTAP Volume ohne SnapMirror entfernen

Ab ONTAP 9.4 kann secure-purge verwendet werden, um Daten auf NVE-fähigen Volumes unterbrechungsfrei zu „scrubben“.

Über diese Aufgabe

Die sichere Löschung kann je nach Datenmenge in den gelöschten Dateien einige Minuten bis mehrere Stunden dauern. Der Status des Vorgangs kann mit dem `volume encryption secure-purge show` Befehl angezeigt werden. Der Vorgang kann mit dem `volume encryption secure-purge abort` Befehl beendet werden.

> Um eine sichere Bereinigung auf einem SAN-Host durchzuführen, müssen Sie entweder die gesamte LUN löschen, die die Dateien enthält, die Sie bereinigen möchten, oder Sie müssen in der Lage sein, in der LUN für die Blöcke, die zu den Dateien gehören, die Sie bereinigen möchten, Löcher zu schlagen. Wenn Sie die LUN nicht löschen können oder Ihr Host-Betriebssystem das Schlagen von Löchern in der LUN nicht unterstützt, kann eine sichere Bereinigung nicht durchgeführt werden.

Bevor Sie beginnen

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

Schritte

1. Die Dateien oder die LUN, die sicher gelöscht werden sollen, löschen.

- Auf einem NAS-Client die Dateien löschen, die Sie sicher entfernen möchten.
- Auf einem SAN-Host die LUN löschen, die Sie sicher bereinigen möchten, oder Löcher in die LUN für die Blöcke stanzen, die zu den Dateien gehören, die Sie bereinigen möchten.

2. Im Speichersystem zur erweiterten Berechtigungsstufe wechseln:

   ```
   set -privilege advanced
   ```

3. Wenn sich die Dateien, die Sie sicher löschen möchten, in Snapshots befinden, löschen Sie die Snapshots:

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

4. Gelöschte Dateien sicher löschen:

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

   Der folgende Befehl entfernt die gelöschten Dateien sicher von `vol1` auf SVM `vs1`:

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

5. Status des Secure-Purge-Vorgangs überprüfen:

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

Bereinigung verschlüsselter Daten aus einem ONTAP Volume mit asynchronem SnapMirror

Ab ONTAP 9.8 kann ein sicherer Bereinigungsvorgang verwendet werden, um Daten auf NVE-fähigen Volumes mit einer SnapMirror asynchronen Beziehung unterbrechungsfrei zu „scrubben“.

Bevor Sie beginnen

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

Über diese Aufgabe

Die sichere Löschung kann je nach Datenmenge in den gelöschten Dateien einige Minuten bis mehrere Stunden dauern. Der Status des Vorgangs kann mit dem `volume encryption secure-purge show` Befehl angezeigt werden. Der Vorgang kann mit dem `volume encryption secure-purge abort` Befehl beendet werden.

> Um eine sichere Bereinigung auf einem SAN-Host durchzuführen, müssen Sie entweder die gesamte LUN löschen, die die Dateien enthält, die Sie bereinigen möchten, oder Sie müssen in der Lage sein, in der LUN für die Blöcke, die zu den Dateien gehören, die Sie bereinigen möchten, Löcher zu schlagen. Wenn Sie die LUN nicht löschen können oder Ihr Host-Betriebssystem das Schlagen von Löchern in der LUN nicht unterstützt, kann eine sichere Bereinigung nicht durchgeführt werden.

Schritte

1. Im Speichersystem zur erweiterten Berechtigungsstufe wechseln:

   ```
   set -privilege advanced
   ```

2. Die Dateien oder die LUN, die sicher gelöscht werden sollen, löschen.
   - Auf einem NAS-Client die Dateien löschen, die Sie sicher entfernen möchten.
   - Auf einem SAN-Host die LUN löschen, die Sie sicher bereinigen möchten, oder Löcher in die LUN für die Blöcke stanzen, die zu den Dateien gehören, die Sie bereinigen möchten.
3. Das Zielvolume in der asynchronen Beziehung wird für die sichere Löschung vorbereitet:

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

   Diesen Schritt bei jedem Volume in Ihrer SnapMirror asynchronen Beziehung wiederholen.

4. Wenn sich die Dateien, die Sie sicher löschen möchten, in Snapshots befinden, löschen Sie die Snapshots:

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

5. Wenn sich die Dateien, die Sie sicher löschen möchten, in den Basis-Snapshots befinden, ist Folgendes zu tun:

   a. Einen Snapshot auf dem Quellvolume in der SnapMirror asynchronen Beziehung erstellen:

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

   b. Die SnapMirror Beziehung wird aktualisiert, um den Basissnapshot auf das Ziel zu verschieben:

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

   Diesen Schritt für jedes Volume in der SnapMirror asynchronen Beziehung wiederholen.

   a. Die Schritte (a) und (b) werden so oft wiederholt, wie es Basis-Snapshots plus eins gibt.

      Wenn Sie beispielsweise zwei Basis-Snapshots haben, sollten die Schritte (a) und (b) dreimal wiederholt werden.

   b. Es sollte überprüft werden, ob der Basis-Snapshot vorhanden ist:
      `snapshot show -vserver SVM_name -volume volume_name`
   c. Den Basis-Snapshot löschen:
      `snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot`
6. Gelöschte Dateien sicher löschen:

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

   Dieser Schritt ist für jedes Volume in der SnapMirror asynchronen Beziehung zu wiederholen.

   Der folgende Befehl entfernt die gelöschten Dateien auf “vol1” auf SVM “vs1” sicher:

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

7. Status des sicheren Löschvorgangs überprüfen:

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

Verwandte Informationen

- "SnapMirror update"

Verschlüsselte Daten aus einem ONTAP Volume mit synchronem SnapMirror bereinigen

Ab ONTAP 9.8 ist es möglich, mit einer sicheren Bereinigung Daten auf NVE-fähigen Volumes mit einer SnapMirror synchronen Beziehung unterbrechungsfrei zu „bereinigen“.

Über diese Aufgabe

Eine sichere Datenlöschung kann je nach Datenmenge in den gelöschten Dateien einige Minuten bis mehrere Stunden dauern. Der Status des Vorgangs kann mit dem `volume encryption secure-purge show` Befehl angezeigt werden. Der Vorgang kann mit dem `volume encryption secure-purge abort` Befehl beendet werden.

> Um eine sichere Bereinigung auf einem SAN-Host durchzuführen, müssen Sie entweder die gesamte LUN löschen, die die Dateien enthält, die Sie bereinigen möchten, oder Sie müssen in der Lage sein, in der LUN für die Blöcke, die zu den Dateien gehören, die Sie bereinigen möchten, Löcher zu schlagen. Wenn Sie die LUN nicht löschen können oder Ihr Host-Betriebssystem das Schlagen von Löchern in der LUN nicht unterstützt, kann eine sichere Bereinigung nicht durchgeführt werden.

Bevor Sie beginnen

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

Schritte

1. Im Speichersystem zur erweiterten Berechtigungsstufe wechseln:

```
set -privilege advanced
```

2. Die Dateien oder die LUN, die sicher gelöscht werden sollen, löschen.
   - Auf einem NAS-Client die Dateien löschen, die Sie sicher entfernen möchten.
   - Auf einem SAN-Host die LUN löschen, die Sie sicher bereinigen möchten, oder Löcher in die LUN für die Blöcke stanzen, die zu den Dateien gehören, die Sie bereinigen möchten.
3. Das Zielvolume in der asynchronen Beziehung wird für die sichere Löschung vorbereitet:

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

Diesen Schritt für das andere Volume in Ihrer SnapMirror synchronen Beziehung wiederholen.

4. Wenn sich die Dateien, die Sie sicher löschen möchten, in Snapshots befinden, löschen Sie die Snapshots:

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

5. Befindet sich die sichere Löschdatei im Basis- oder gemeinsamen Snapshot, wird die SnapMirror Beziehung aktualisiert, um den gemeinsamen Snapshot voranzubewegen:

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

   Es gibt zwei gemeinsame Snapshots, daher muss dieser Befehl zweimal ausgeführt werden.

6. Befindet sich die sichere Löschdatei im applikationskonsistenten Snapshot, wird der Snapshot auf beiden Volumes in der SnapMirror synchronen Beziehung gelöscht:

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

   Führen Sie diesen Schritt auf beiden Volumes durch.

7. Gelöschte Dateien sicher löschen:

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

   Dieser Schritt ist für jedes Volume in der SnapMirror synchronen Beziehung zu wiederholen.

   Der folgende Befehl entfernt die gelöschten Dateien auf “vol1” auf SVM “vs1” sicher und unwiderruflich.

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

8. Status des sicheren Löschvorgangs überprüfen:

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

Verwandte Informationen

- "SnapMirror update"

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.