Löschen Sie Daten auf einem verschlüsselten Volume sicher

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/encryption-at-rest/secure-purge-data-encrypted-volume-concept.html on February 12, 2026. Always check docs.netapp.com for the latest.

Inhalt

Löschen Sie Daten auf einem verschlüsselten Volume sicher . . . 1
Erfahren Sie mehr über das sichere Löschen von Daten aus einem verschlüsselten ONTAP -Volume . . . 1
Überlegungen zur Verwendung einer sicheren Löschung . . . 1
Daten von einem verschlüsselten ONTAP Volume ohne SnapMirror -Beziehung bereinigen . . . 2
Daten von einem verschlüsselten ONTAP Volume mit einer asynchronen SnapMirror -Beziehung bereinigen . . . 3
Daten von einem verschlüsselten ONTAP Volume mit einer synchronen SnapMirror -Beziehung bereinigen . . . 5

Löschen Sie Daten auf einem verschlüsselten Volume sicher

Erfahren Sie mehr über das sichere Löschen von Daten aus einem verschlüsselten ONTAP -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 `secure purge re-encryption-method [volume-move|in-place-rekey]` Befehl geändert werden.
- Standardmäßig werden alle Snapshots 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 `secure purge delete-all-snapshots [true|false]` Befehl geändert werden.

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.

  Wenn im Volume überlastete Snapshots vorhanden sind, müssen Sie die Snapshots 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.

Daten von einem verschlüsselten ONTAP Volume ohne SnapMirror -Beziehung bereinigen

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 den `volume encryption secure-purge show` Status des Vorgangs mit dem Befehl anzeigen. Sie können den `volume encryption secure-purge abort` Vorgang mit dem Befehl beenden.

> 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 `vol1` SVM sicher gelöscht`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
   ```

Daten von einem verschlüsselten ONTAP Volume mit einer asynchronen SnapMirror -Beziehung bereinigen

Ab ONTAP 9.8 können Sie zum unterbrechungsfreien Löschen von „`sCrub`“-Daten auf

NVE-fähigen Volumes mit asynchroner SnapMirror Beziehung verwenden.

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 den `volume encryption secure-purge show` Status des Vorgangs mit dem Befehl anzeigen. Sie können den `volume encryption secure-purge abort` Vorgang mit dem Befehl beenden.

> 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 Snapshots gespeichert sind, 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, gehen Sie wie folgt vor:

   a. Erstellen Sie einen Snapshot auf dem Ziel-Volume in der asynchronen SnapMirror Beziehung:

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

   b. SnapMirror aktualisieren, um den Basis-Snapshot vorwärts 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) gleich der Anzahl der Basis-Snapshots plus eins.

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

b. Überprüfen Sie, ob der Basis-Snapshot vorhanden ist:
   `snapshot show -vserver *SVM_name* -volume *volume_name*`

c. Löschen Sie den Basis-Snapshot:
   `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`

Verwandte Informationen

- "Snapmirror-Update"

Daten von einem verschlüsselten ONTAP Volume mit einer synchronen SnapMirror -Beziehung bereinigen

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

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 den `volume encryption secure-purge show` Status des Vorgangs mit dem Befehl anzeigen. Sie können den `volume encryption secure-purge abort` Vorgang mit dem Befehl beenden.

> 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 Snapshots gespeichert sind, löschen Sie die Snapshots:

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

5. Wenn sich die sichere Löschdatei in der Basis oder in allgemeinen Snapshots befindet, aktualisieren Sie die SnapMirror, um den gemeinsamen Snapshot vorwärts zu verschieben:

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

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

6. Wenn sich die Datei für das sichere Löschen im anwendungskonsistenten Snapshot befindet, löschen Sie den Snapshot 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 SVM „`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
```

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.