Verwaltung der NetApp Verschlüsselung

ONTAP 9

NetApp
November 10, 2026

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

Inhalt

Verwaltung der NetApp Verschlüsselung . . . 1
- Volumendaten in ONTAP entschlüsseln . . . 1
- Verschieben eines verschlüsselten Volumes in ONTAP . . . 1
- Änderung des Verschlüsselungsschlüssels für ein ONTAP Volume . . . 2
- Änderung des Verschlüsselungsschlüssels für ein ONTAP Volume . . . 4
- Rotation von Authentifizierungsschlüsseln für NetApp Storage Encryption in ONTAP . . . 5
- Löschen eines verschlüsselten Volumes in ONTAP . . . 5
- Daten auf einem verschlüsselten Volume sicher löschen . . . 6
  - Informationen zum sicheren Löschen von Daten aus einem verschlüsselten ONTAP Volume . . . 6
  - Verschlüsselte Daten aus einem ONTAP Volume ohne SnapMirror entfernen . . . 7
  - Bereinigung verschlüsselter Daten aus einem ONTAP Volume mit asynchronem SnapMirror . . . 8
  - Verschlüsselte Daten aus einem ONTAP Volume mit synchronem SnapMirror bereinigen . . . 10
- Die Passphrase für die ONTAP Onboard-Schlüsselverwaltung ändern . . . 12
- ONTAP Onboard-Schlüsselverwaltungsinformationen manuell sichern . . . 13
- Onboard Key Management-Verschlüsselungsschlüssel in ONTAP wiederherstellen . . . 15
  - ONTAP 9.6 und höher . . . 15
  - ONTAP 9.8 oder höher mit verschlüsseltem Root-Volume . . . 15
  - ONTAP 9.5 und früher . . . 16
- Wiederherstellung der ONTAP externen Schlüsselverwaltungs-Verschlüsselungsschlüssel . . . 16
- KMIP SSL-Zertifikate auf dem ONTAP Cluster ersetzen . . . 17
- Austausch eines FIPS-Laufwerks oder SED in ONTAP . . . 18
- Daten auf einem FIPS-Laufwerk oder SED unzugänglich machen . . . 20
  - Datenträgerbereinigung und -vernichtung in ONTAP . . . 20
  - Ein FIPS-Laufwerk oder SED in ONTAP bereinigen . . . 21
  - Ein FIPS-Laufwerk oder eine SED in ONTAP zerstören . . . 23
  - Daten auf einem FIPS-Laufwerk oder SED im Notfall in ONTAP vernichten . . . 25
- Wiederherstellung des Betriebs eines FIPS-Laufwerks oder einer ONTAP SED bei verlorenen Schlüsseln . . . 28
- Ein FIPS-Laufwerk oder SED in ONTAP in den ungeschützten Modus zurückversetzen . . . 30
  - Wartungsmodus . . . 32
- Eine externe Schlüsselverwaltungsverbindung in ONTAP entfernen . . . 33
- Eigenschaften des externen Schlüsselverwaltungsservers von ONTAP ändern . . . 34
- Übergang von der internen zur externen Schlüsselverwaltung in ONTAP . . . 35
- Wechsel von externer Schlüsselverwaltung zu ONTAP interner Schlüsselverwaltung . . . 36
- Wie ONTAP mit nicht erreichbaren Schlüsselverwaltungsservern während des Systemstarts umgeht . . . 37
- ONTAP Verschlüsselung standardmäßig deaktiviert . . . 39

Verwaltung der NetApp Verschlüsselung

Volumendaten in ONTAP entschlüsseln

Der `volume move start` Befehl kann verwendet werden, um Volumendaten zu verschieben und zu entschlüsseln.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Ein vorhandenes verschlüsseltes Volume verschieben und die Daten auf dem Volume entschlüsseln:

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

   Weitere Informationen zu `volume move start` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl verschiebt ein vorhandenes Volume mit dem Namen `vol1` in das Zielaggregat `aggr3` und entschlüsselt die Daten auf dem Volume:

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

   Das System löscht den Verschlüsselungsschlüssel für das Volume. Die Daten auf dem Volume sind unverschlüsselt.

2. Es sollte überprüft werden, ob die Verschlüsselung des Volumes deaktiviert ist:

   `volume show -encryption`

   Weitere Informationen zu `volume show` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl zeigt an, ob Volumes auf `cluster1`verschlüsselt sind:

   ```
   cluster1::> volume show -encryption

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

Verschieben eines verschlüsselten Volumes in ONTAP

Sie können den `volume move start` Befehl verwenden, um ein verschlüsseltes Volume zu verschieben. Das verschobene Volume kann sich auf demselben Aggregat oder auf einem anderen Aggregat befinden.

Über diese Aufgabe

Der Vorgang schlägt fehl, wenn der Zielknoten oder das Zielvolume die Volume-Verschlüsselung nicht unterstützt.

Die `-encrypt-destination`Option für `volume move start` ist bei verschlüsselten Volumes standardmäßig aktiviert. Die Anforderung, explizit anzugeben, dass das Zielvolume nicht verschlüsselt werden soll, stellt sicher, dass die Daten auf dem Volume nicht versehentlich entschlüsselt werden.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Ein vorhandenes verschlüsseltes Volume kann verschoben werden, wobei die Daten auf dem Volume verschlüsselt bleiben:

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

   Weitere Informationen zu `volume move start` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl verschiebt ein vorhandenes Volume mit dem Namen `vol1` in das Zielaggregat `aggr3` und lässt die Daten auf dem Volume verschlüsselt:

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

2. Es sollte überprüft werden, ob das Volume für die Verschlüsselung aktiviert ist:

   `volume show -is-encrypted true`

   Weitere Informationen zu `volume show` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl zeigt die verschlüsselten Volumes auf `cluster1` an:

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

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

Änderung des Verschlüsselungsschlüssels für ein ONTAP Volume

Es gilt als bewährte Sicherheitsmaßnahme, den Verschlüsselungsschlüssel eines Volumes regelmäßig zu ändern. Ab ONTAP 9.3 kann der Verschlüsselungsschlüssel mit dem `volume encryption rekey start` Befehl geändert werden.

Über diese Aufgabe

Sobald Sie einen Schlüsselerneuerungsvorgang starten, muss dieser abgeschlossen werden. Eine Rückkehr zum alten Schlüssel ist nicht möglich. Wenn während des Vorgangs Leistungsprobleme auftreten, kann der Vorgang mit dem `volume encryption rekey pause` Befehl angehalten und mit dem `volume encryption rekey resume` Befehl fortgesetzt werden.

Bis zum Abschluss der Neuverschlüsselung verfügt das Volume über zwei Schlüssel. Neue Schreibvorgänge und die zugehörigen Lesevorgänge verwenden den neuen Schlüssel. Andernfalls verwenden Lesevorgänge den alten Schlüssel.

Es ist nicht möglich, mit `volume encryption rekey start` ein SnapLock Volume neu zu verschlüsseln.

Schritte

1. Ändern eines Verschlüsselungsschlüssels:

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

   Der folgende Befehl ändert den Verschlüsselungsschlüssel für `vol1` auf SVM `vs1`:

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

2. Status des Schlüsselerneuerungsvorgangs überprüfen:

   `volume encryption rekey show`

   Weitere Informationen zu `volume encryption rekey show` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl zeigt den Status des Rekey-Vorgangs an:

   ```
   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. Nach Abschluss der Schlüsselerneuerung kann überprüft werden, ob das Volume für die Verschlüsselung aktiviert ist:

   `volume show -is-encrypted true`

   Weitere Informationen zu `volume show` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl zeigt die verschlüsselten Volumes auf `cluster1` an:

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

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

Änderung des Verschlüsselungsschlüssels für ein ONTAP Volume

Es gilt als bewährte Sicherheitsmaßnahme, den Verschlüsselungsschlüssel eines Volumes regelmäßig zu ändern. Der `volume move start` Befehl kann zum Ändern des Verschlüsselungsschlüssels verwendet werden. Das verschobene Volume kann sich auf demselben Aggregat oder auf einem anderen Aggregat befinden.

Über diese Aufgabe

Sie können `volume move start`nicht verwenden, um ein SnapLock- oder FlexGroup-Volumen neu zu verschlüsseln.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Ein vorhandenes Volume verschieben und den Verschlüsselungsschlüssel ändern:

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

   Weitere Informationen zu `volume move start` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl verschiebt ein vorhandenes Volume mit dem Namen **`vol1`** in das Zielaggregat **`aggr2`** und ändert den Verschlüsselungsschlüssel:

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

   Für das Volume wird ein neuer Verschlüsselungsschlüssel erstellt. Die Daten auf dem Volume bleiben verschlüsselt.

2. Es sollte überprüft werden, ob das Volume für die Verschlüsselung aktiviert ist:

   `volume show -is-encrypted true`

   Weitere Informationen zu `volume show` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl zeigt die verschlüsselten Volumes auf `cluster1` an:

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

   Vserver  Volume  Aggregate  State  Type  Size  Available  Used
   ```

```
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2      online    RW  200GB    160.0GB  20%
```

Rotation von Authentifizierungsschlüsseln für NetApp Storage Encryption in ONTAP

Die Authentifizierungsschlüssel können bei Verwendung von NetApp Storage Encryption (NSE) rotiert werden.

Über diese Aufgabe

Die Rotation von Authentifizierungsschlüsseln in einer NSE-Umgebung wird unterstützt, wenn der External Key Manager (KMIP) verwendet wird.

> Die Rotation von Authentifizierungsschlüsseln in einer NSE-Umgebung wird für Onboard Key Manager (OKM) nicht unterstützt.

Schritte

1. Mit dem `security key-manager create-key` Befehl werden neue Authentifizierungsschlüssel generiert.

   Sie müssen neue Authentifizierungsschlüssel generieren, bevor Sie die Authentifizierungsschlüssel ändern können.

2. Mit dem `storage encryption disk modify -disk * -data-key-id`Befehl lassen sich die Authentifizierungsschlüssel ändern.

Verwandte Informationen

- "Speicherverschlüsselung Festplatte ändern"

Löschen eines verschlüsselten Volumes in ONTAP

Mit dem `volume delete` Befehl lässt sich ein verschlüsseltes Volume löschen.

Bevor Sie beginnen

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Das Volume muss offline sein.

Schritt

1. Löschen eines verschlüsselten Volumes:

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

   Weitere Informationen zu `volume delete` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl löscht ein verschlüsseltes Volume mit dem Namen `vol1`:

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

Geben Sie `yes` ein, wenn Sie zur Bestätigung der Löschung aufgefordert werden.

Das System löscht den Verschlüsselungsschlüssel für das Volume nach 24 Stunden.

Verwenden Sie `volume delete` mit der `-force true` Option, um ein Volume zu löschen und den entsprechenden Verschlüsselungsschlüssel sofort zu zerstören. Dieser Befehl erfordert erweiterte Berechtigungen. Weitere Informationen zu `volume delete` finden sich in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

Mit dem `volume recovery-queue` Befehl kann ein gelöschtes Volume während der Aufbewahrungsfrist nach Ausführung des `volume delete` Befehls wiederhergestellt werden:

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

"Verwendung der Volume Recovery Funktion"

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"

Die Passphrase für die ONTAP Onboard-Schlüsselverwaltung ändern

NetApp empfiehlt, die Passphrase für die integrierte Schlüsselverwaltung regelmäßig zu ändern. Die neue Passphrase muss an einem sicheren Ort außerhalb des Speichersystems aufbewahrt werden.

Bevor Sie beginnen

- Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.
- Sie müssen die aktuelle Passphrase für die Onboard Schlüsselverwaltung eingeben, bevor Sie eine neue Passphrase festlegen können.
- In einer MetroCluster Umgebung wird nach der Aktualisierung der Passphrase auf dem lokalen Cluster die Passphrase-Aktualisierung auf dem Partnercluster synchronisiert.

Schritte

1. Wechsel zum erweiterten Berechtigungslevel:

   ```
   set -privilege advanced
   ```

2. Ändern der Passphrase für die integrierte Schlüsselverwaltung. Der verwendete Befehl hängt von der ONTAP-Version ab, die ausgeführt wird.

   Nachdem Sie den Befehl eingegeben haben, antworten Sie auf die Aufforderungen, um die aktuelle Passphrase, die neue Passphrase und zur Bestätigung erneut die neue Passphrase einzugeben.

   ONTAP 9.6 und höher

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

   ONTAP 9.5 und früher

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

3. Wenn Sie dazu aufgefordert werden, geben Sie die aktuelle Passphrase ein.
4. Geben Sie eine neue Passphrase mit 32 bis 256 Zeichen ein oder für “cc-mode” eine Passphrase mit 64 bis 256 Zeichen.

   Ist die angegebene Passphrase für den “cc-mode” kürzer als 64 Zeichen, tritt eine Verzögerung von fünf Sekunden auf, bevor die Passphrase-Aufforderung im Rahmen der Schlüsselmanager-Einrichtung erneut angezeigt wird.

5. An der Aufforderung zur Bestätigung der Passphrase ist die neue Passphrase erneut einzugeben.
6. Wenn Sie sich in einer MetroCluster Konfiguration befinden, sollte die aktualisierte Passphrase auf dem Partnercluster synchronisiert werden.
   a. Die Passphrase auf dem Partnercluster wird synchronisiert, indem der richtige Befehl für die jeweilige ONTAP Version ausgewählt wird:

ONTAP 9.6 und höher

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

ONTAP 9.5 und früher

- In ONTAP 9.5 führen Sie Folgendes aus:

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

- In ONTAP 9.4 und früheren Versionen sollte nach der Aktualisierung der Passphrase auf dem lokalen Cluster 20 Sekunden gewartet werden, bevor der folgende Befehl auf dem Partnercluster ausgeführt wird:

  ```
  security key-manager setup
  ```

b. Geben Sie die neue Passphrase ein, wenn Sie dazu aufgefordert werden.

   Für beide Cluster muss dieselbe Passphrase verwendet werden.

Nachdem Sie fertig sind

Die Passphrase für die integrierte Schlüsselverwaltung sollte an einem sicheren Ort außerhalb des Speichersystems für die zukünftige Verwendung aufbewahrt werden.

Schlüsselverwaltungsinformationen sollten manuell gesichert werden, sobald die Passphrase für die integrierte Schlüsselverwaltung geändert wird.

Verwandte Informationen

- "Onboard-Schlüsselverwaltungsinformationen manuell sichern"
- "security key-manager onboard update-passphrase"

ONTAP Onboard-Schlüsselverwaltungsinformationen manuell sichern

Sie sollten die Onboard Key Management-Informationen immer dann an einem sicheren Ort außerhalb des Speichersystems speichern, wenn Sie die Passphrase des Onboard Key Manager konfigurieren.

Bevor Sie beginnen

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

Über diese Aufgabe

Alle Schlüsselverwaltungsinformationen werden automatisch in der replizierten Datenbank (RDB) des Clusters gesichert. Schlüsselverwaltungsinformationen sollten zusätzlich manuell gesichert werden, um sie im Katastrophenfall verwenden zu können.

Schritte

1. Wechsel zum erweiterten Berechtigungslevel:

```
set -privilege advanced
```

2. Die Sicherungsinformationen für die Schlüsselverwaltung des Clusters anzeigen:

Für diese ONTAP Version…	Verwenden Sie diesen Befehl…
ONTAP 9.6 und höher	`security key-manager onboard show-backup`
ONTAP 9.5 und früher	`security key-manager backup show`

Der folgende 9.6-Befehl zeigt die Sicherungsinformationen für die Schlüsselverwaltung für `cluster1` an:

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

     ------------------------BEGIN BACKUP-------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAADuD+byAAAAACEAAAAAAAAA
     QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
     IgAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AQAAAAMAAAAYAQAAAAAAADA5/ccAAAAAIgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAA
     AAAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAACIAAAAAAAAA
     KAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
     AAAAAAAAAAAkAAAAAAAAAIAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
     LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA
     1cNLLwAAAAiAAAAAAAAACgAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAIAAAAAAAkA
     ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAIgAAAAAAAAoAAAAAAAAJ4/cQsAAAAA
     AAAAAAAAAACAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAACQAAAAAAAA
     gAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
     rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     ------------------------END BACKUP--------------------------
```

3. Die Sicherungsdaten sollten an einen sicheren Ort außerhalb des Speichersystems kopiert werden, damit sie im Katastrophenfall zur Verfügung stehen.

Verwandte Informationen

- "security key-manager onboard show-backup"
- "security key-manager backup show"

Onboard Key Management-Verschlüsselungsschlüssel in ONTAP wiederherstellen

Gelegentlich kann es erforderlich sein, einen Onboard Key Management Verschlüsselungsschlüssel wiederherzustellen. Nachdem überprüft wurde, dass ein Schlüssel wiederhergestellt werden muss, kann der Onboard Key Manager eingerichtet werden, um den Schlüssel wiederherzustellen. Das Verfahren zur Wiederherstellung der Onboard Key Management Verschlüsselungsschlüssel variiert je nach Ihrer ONTAP Version.

Bevor Sie beginnen

- Löschen Sie die externe Key-Manager-Datenbank, wenn Sie NSE mit einem externen KMIP-Server verwenden. Weitere Details finden sich unter "Übergang von externer Schlüsselverwaltung zur ONTAP internen Schlüsselverwaltung".
- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

> Wenn Sie NSE auf einem System mit Flash Cache Modul verwenden, sollten Sie auch NVE oder NAE aktivieren. NSE verschlüsselt keine Daten, die sich auf dem Flash Cache Modul befinden.

ONTAP 9.6 und höher

> Wenn ONTAP 9.8 oder höher verwendet wird und das Root-Volume verschlüsselt ist, ist die Vorgehensweise für ONTAP 9.8 oder höher mit verschlüsseltem Root-Volume zu befolgen.

1. Überprüfen, ob der Schlüssel wiederhergestellt werden muss:
   `security key-manager key query -node node`

   Weitere Informationen zu `security key-manager key query` finden sich in der "ONTAP-Befehlsreferenz".

2. Schlüssel wiederherstellen:
   `security key-manager onboard sync`

   Weitere Informationen zu `security key-manager onboard sync` finden sich in der "ONTAP-Befehlsreferenz".

3. An der Passphrase-Aufforderung die Passphrase für die integrierte Schlüsselverwaltung des Clusters eingeben.

ONTAP 9.8 oder höher mit verschlüsseltem Root-Volume

Wenn Sie ONTAP 9.8 oder höher verwenden und Ihr Root-Volume verschlüsselt ist, muss über das Bootmenü eine Wiederherstellungs-Passphrase für die Onboard-Schlüsselverwaltung festgelegt werden. Dieser Vorgang ist auch erforderlich, wenn ein Bootmedium ersetzt wird.

1. Den Knoten zum Bootmenü starten und Option `(10) Set onboard key management recovery secrets` auswählen.
2. Geben Sie `y` ein, um diese Option zu verwenden.
3. An der Eingabeaufforderung ist die Passphrase für die Onboard-Schlüsselverwaltung des Clusters einzugeben.
4. An der Eingabeaufforderung die Sicherungsschlüsseldaten eingeben.

   Nach Eingabe der Sicherungsschlüsseldaten kehrt der Knoten zum Bootmenü zurück.

5. Im Bootmenü die Option `(1) Normal Boot` auswählen.

ONTAP 9.5 und früher

1. Überprüfen, ob der Schlüssel wiederhergestellt werden muss:
   `security key-manager key show`
2. Schlüssel wiederherstellen:
   `security key-manager setup -node` *node*

   Weitere Informationen zu `security key-manager setup` finden sich in der "ONTAP-Befehlsreferenz".

3. An der Passphrase-Aufforderung die Passphrase für die integrierte Schlüsselverwaltung des Clusters eingeben.

Wiederherstellung der ONTAP externen Schlüsselverwaltungs-Verschlüsselungsschlüssel

Sie können Verschlüsselungsschlüssel für die externe Schlüsselverwaltung manuell wiederherstellen und auf einen anderen Knoten übertragen. Dies kann sinnvoll sein, wenn ein Knoten neu gestartet wird, der zum Zeitpunkt der Erstellung der Schlüssel für den Cluster vorübergehend ausgefallen war.

Über diese Aufgabe

In ONTAP 9.6 und höher kann mit dem `security key-manager key query -node node_name` Befehl überprüft werden, ob Ihr Schlüssel wiederhergestellt werden muss.

In ONTAP 9.5 und früher können Sie den `security key-manager key show` Befehl verwenden, um zu überprüfen, ob Ihr Schlüssel wiederhergestellt werden muss.

> Wenn Sie NSE auf einem System mit Flash Cache Modul verwenden, sollten Sie auch NVE oder NAE aktivieren. NSE verschlüsselt keine Daten, die sich auf dem Flash Cache Modul befinden.

Weitere Informationen zu `security key-manager key query` finden sich in der "ONTAP-Befehlsreferenz".

Bevor Sie beginnen

Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Wenn Sie ONTAP 9.8 oder höher verwenden und Ihr Root-Volume verschlüsselt ist, führen Sie Folgendes aus:

   Wenn ONTAP 9.7 oder eine frühere Version verwendet wird oder wenn ONTAP 9.8 oder eine neuere Version verwendet wird und das Root-Volume nicht verschlüsselt ist, kann dieser Schritt übersprungen werden.

   a. Bootargumente festlegen:
   ```
   setenv kmip.init.ipaddr <ip-address>
   setenv kmip.init.netmask <netmask>
   setenv kmip.init.gateway <gateway>
   setenv kmip.init.interface e0M
   boot_ontap
   ```
   b. Den Knoten zum Bootmenü starten und Option `(11) Configure node for external key management` auswählen.
   c. Den Anweisungen zum Eingeben des Managementzertifikats folgen.

      Nach Eingabe aller Managementzertifikatsinformationen kehrt das System zum Bootmenü zurück.

   d. Im Bootmenü die Option `(1) Normal Boot` auswählen.
2. Stellen Sie den Schlüssel wieder her:

Für diese ONTAP Version…	Verwenden Sie diesen Befehl…
ONTAP 9.6 und höher	`security key-manager external restore -vserver SVM -node node -key-server host_name
IP_address:port -key-id key_id -key -tag key_tag`	ONTAP 9.5 und früher

> `node`Standardmäßig gilt dies für alle Knoten.
>
> Dieser Befehl wird nicht unterstützt, wenn die Onboard-Schlüsselverwaltung aktiviert ist.

Der folgende ONTAP 9.6 Befehl stellt die Authentifizierungsschlüssel für das externe Schlüsselmanagement auf allen Knoten in `cluster1`wieder her:

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

Verwandte Informationen

- "security key-manager external restore"

KMIP SSL-Zertifikate auf dem ONTAP Cluster ersetzen

Alle SSL-Zertifikate haben ein Ablaufdatum. Die Zertifikate müssen vor ihrem Ablauf aktualisiert werden, um den Verlust des Zugriffs auf Authentifizierungsschlüssel zu verhindern.

Bevor Sie beginnen

- Das Ersatz-Public-Zertifikat und der Ersatz-Private-Key für den Cluster (KMIP-Client-Zertifikat) müssen vorliegen.
- Sie müssen das Ersatzzertifikat für den KMIP-Server (KMIP-Server-CA-Zertifikat) erhalten haben.
- Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.
- Wenn Sie die KMIP-SSL-Zertifikate in einer MetroCluster Umgebung ersetzen, müssen Sie auf beiden Clustern dasselbe Ersatz-KMIP-SSL-Zertifikat installieren.

Sie können die Ersatz-Client- und Serverzertifikate auf dem KMIP-Server vor oder nach der Installation der Zertifikate auf dem Cluster installieren.

Schritte

1. Das neue KMIP Server-CA-Zertifikat installieren:

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

2. Das neue KMIP Clientzertifikat installieren:

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

3. Die Konfiguration des Schlüsselmanagers wird aktualisiert, sodass die neu installierten Zertifikate verwendet werden:

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

   Wenn Sie ONTAP 9.6 oder höher in einer MetroCluster Umgebung verwenden und die Key-Manager-Konfiguration auf der Admin-SVM ändern möchten, muss der Befehl auf beiden Clustern in der Konfiguration ausgeführt werden.

Die Aktualisierung der Schlüsselverwaltungskonfiguration zur Verwendung der neu installierten Zertifikate führt zu einem Fehler, wenn sich die öffentlichen/privaten Schlüssel des neuen Clientzertifikats von den zuvor installierten Schlüsseln unterscheiden. Siehe die "NetApp Knowledge Base: Die öffentlichen oder privaten Schlüssel des neuen Clientzertifikats unterscheiden sich von den bestehenden Clientzertifikaten." für Anweisungen zum Überschreiben dieses Fehlers.

Verwandte Informationen

- "Sicherheitszertifikat installieren"
- "security key-manager external modify"

Austausch eines FIPS-Laufwerks oder SED in ONTAP

Ein FIPS-Laufwerk oder eine SED kann genauso ausgetauscht werden wie eine herkömmliche Festplatte. Es ist sicherzustellen, dass dem Ersatzlaufwerk neue Datenauthentifizierungsschlüssel zugewiesen werden. Bei einem FIPS-Laufwerk kann außerdem die Zuweisung eines neuen FIPS 140-2 Authentifizierungsschlüssels sinnvoll sein.

Wenn ein HA-Paar "Verschlüsselung von SAS- oder NVMe-Laufwerken (SED, NSE, FIPS)" verwendet wird, müssen Sie die Anweisungen im Thema "Zurückstellen eines FIPS-Laufwerks oder SED in den ungeschützten Modus" für alle Laufwerke innerhalb des HA-Paares befolgen, bevor Sie das System initialisieren (Boot-Optionen 4 oder 9). Andernfalls kann es in Zukunft zu Datenverlust kommen, wenn die Laufwerke wiederverwendet werden.

Bevor Sie beginnen

- Sie müssen die Schlüssel-ID für den Authentifizierungsschlüssel kennen, der vom Laufwerk verwendet wird.
- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Stellen Sie sicher, dass die Festplatte als ausgefallen markiert wurde:

   `storage disk show -broken`

   Weitere Informationen zu `storage disk show` finden sich in der "ONTAP-Befehlsreferenz".

```
cluster1::> storage disk show -broken
Original Owner: node1
  Checksum Compatibility: block
                                                    Drawer
Usable Physical
    Disk            Outage Reason  HA Shelf Bay  /Slot Chan   Pool
Type    RPM     Size     Size Model
    --------------- ------------- --- ----- --- ------ ---- ------
------- ------ -------- -------- ----------------
    1.0.12          admin failed   0a     0  12   -/-     A FAILED SSD-
NVM      -   1.75TB   1.75TB X4024S173A1T9NTE

Original Owner: node2
  Checksum Compatibility: block
                                                    Drawer
Usable Physical
    Disk            Outage Reason  HA Shelf Bay  /Slot Chan   Pool
Type    RPM     Size     Size Model
    --------------- ------------- --- ----- --- ------ ---- ------
------- ------ -------- -------- ----------------
    1.0.13          admin failed   0b     0  13   -/-     B FAILED SSD-
NVM      -   1.75TB   1.75TB X4024S173A1T9NTF

2 entries were displayed.
[...]
```

2. Die defekte Festplatte ist durch ein neues FIPS-Laufwerk oder SED zu ersetzen, entsprechend den Anweisungen im Hardware-Handbuch für Ihr Festplattengehäusemodell.

3. Die Besitzrechte der neu ausgetauschten Festplatte zuweisen:

   `storage disk assign -disk disk_name -owner node`

   Weitere Informationen zu `storage disk assign` finden sich in der "ONTAP-Befehlsreferenz".

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

4. Bestätigen, dass die neue Festplatte zugewiesen wurde:

   `storage encryption disk show`

   Weitere Informationen zu `storage encryption disk show` finden sich in der "ONTAP-Befehlsreferenz".

   ```
   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. Die Authentifizierungsschlüssel für Daten dem FIPS-Laufwerk oder SED zuweisen.

   "Zuweisung eines Authentifizierungsschlüssels zu einem FIPS-Laufwerk oder SED (externes Schlüsselmanagement)"

6. Falls erforderlich, einen FIPS 140-2-Authentifizierungsschlüssel dem FIPS-Laufwerk zuweisen.

   "Zuweisung eines FIPS 140-2 Authentifizierungsschlüssels zu einem FIPS-Laufwerk"

Verwandte Informationen

- "Speicherdatenträger zuweisen"
- "Speicherdatenträger anzeigen"
- "storage encryption Disk anzeigen"

Daten auf einem FIPS-Laufwerk oder SED unzugänglich machen

Datenträgerbereinigung und -vernichtung in ONTAP

Wenn Sie Daten auf einem FIPS-Laufwerk oder Self-Encrypting Drive dauerhaft

unzugänglich machen möchten, der ungenutzte Speicherplatz jedoch für neue Daten verfügbar bleiben soll, kann das Laufwerk bereinigt werden. Wenn Daten dauerhaft unzugänglich gemacht werden sollen und eine Wiederverwendung des Laufwerks nicht erforderlich ist, kann es zerstört werden.

- Datenträgerbereinigung

  Beim Bereinigen eines Self-Encrypting Drives ändert das System den Verschlüsselungsschlüssel auf einen neuen Zufallswert, setzt den Sperrzustand beim Einschalten auf „false“ und setzt die Schlüssel-ID auf einen Standardwert, entweder die Hersteller Secure ID 0x0 (SAS-Laufwerke) oder einen Null-Schlüssel (NVMe-Laufwerke). Dadurch sind die Daten auf dem Laufwerk unzugänglich und können nicht wiederhergestellt werden. Bereinigte Laufwerke können als nicht mit Nullen überschriebene Ersatzlaufwerke wiederverwendet werden.

- Datenträger zerstören

  Wenn Sie ein FIPS-Laufwerk oder ein Self-Encrypting Drive zerstören, setzt das System den Festplattenverschlüsselungsschlüssel auf einen unbekannten Zufallswert und sperrt die Festplatte unwiderruflich. Dadurch wird die Festplatte dauerhaft unbrauchbar und die darauf befindlichen Daten sind dauerhaft unzugänglich.

Es besteht die Möglichkeit, einzelne Self-Encrypting Drives zu bereinigen oder zu zerstören oder alle Self-Encrypting Drives eines Knotens zu zerstören.

Ein FIPS-Laufwerk oder SED in ONTAP bereinigen

Wenn Daten auf einem FIPS-Laufwerk oder Self-Encrypting Drive dauerhaft unzugänglich gemacht werden sollen und das Laufwerk für neue Daten verwendet werden soll, kann der `storage encryption disk sanitize` Befehl zum Bereinigen des Laufwerks verwendet werden.

Über diese Aufgabe

Beim Bereinigen eines Self-Encrypting Drives ändert das System den Verschlüsselungsschlüssel auf einen neuen Zufallswert, setzt den Sperrzustand beim Einschalten auf „false“ und setzt die Schlüssel-ID auf einen Standardwert, entweder die Hersteller Secure ID 0x0 (SAS-Laufwerke) oder einen Null-Schlüssel (NVMe-Laufwerke). Dadurch sind die Daten auf dem Laufwerk unzugänglich und können nicht wiederhergestellt werden. Bereinigte Laufwerke können als nicht mit Nullen überschriebene Ersatzlaufwerke wiederverwendet werden.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Alle Daten, die erhalten bleiben müssen, zu einem Aggregat auf einer anderen Festplatte migrieren.
2. Das Aggregat auf dem FIPS-Laufwerk oder dem zu bereinigenden SED löschen:

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

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

Weitere Informationen zu `storage aggregate delete` finden sich in der "ONTAP-Befehlsreferenz".

3. Die Datenträger-ID für das zu bereinigende FIPS-Laufwerk oder die Self-Encrypting Drives (SED) identifizieren:

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

   Weitere Informationen zu `storage encryption disk show` finden sich in der "ONTAP-Befehlsreferenz".

   ```
   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. Wenn ein FIPS-Laufwerk im FIPS-Konformitätsmodus betrieben wird, wird die FIPS-Authentifizierungsschlüssel-ID für den Knoten wieder auf den Standardwert MSID 0x0 gesetzt:

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

   Mit dem `security key-manager query` Befehl lassen sich die Schlüssel-IDs anzeigen.

   ```
   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. Das Laufwerk bereinigen:

   `storage encryption disk sanitize -disk disk_id`

   Mit diesem Befehl können nur Hot Spare- oder defekte Festplatten bereinigt werden. Um alle Festplatten unabhängig vom Typ zu bereinigen, ist die Option `-force-all-state` zu verwenden. Weitere Informationen zu `storage encryption disk sanitize` finden sich in der "ONTAP-Befehlsreferenz".

   > ⓘ ONTAP fordert Sie auf, vor dem Fortfahren eine Bestätigungsphrase einzugeben. Die Phrase muss exakt so eingegeben werden, wie sie auf dem Bildschirm angezeigt wird.

   ```
   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. Die bereinigte Festplatte wiederherstellen: `storage disk unfail -spare true -disk disk_id`
7. Es ist zu prüfen, ob die Festplatte einen Besitzer hat: `storage disk show -disk disk_id` + Falls die Festplatte keinen Besitzer hat, ist einer zuzuweisen. `storage disk assign -owner node -disk disk_id`
8. Öffnen Sie die Nodeshell für den Node, dem die Festplatten gehören, die Sie bereinigen möchten:

   `system node run -node node_name`

   Führe den `disk sanitize release` Befehl aus.

9. Beenden Sie die Nodeshell. Die Festplatte wird erneut in den betriebsbereiten Zustand versetzt: `storage disk unfail -spare true -disk disk_id`
10. Es sollte überprüft werden, dass die Festplatte nun als Ersatzfestplatte verfügbar ist und zur Wiederverwendung in einem Aggregat bereitsteht: `storage disk show -disk disk_id`

Verwandte Informationen

- "Speicherdatenträger zuweisen"
- "Speicherdatenträger anzeigen"
- "Speicherfestplatte wiederherstellen"
- "Speicherverschlüsselung Festplatte ändern"
- "Speicherverschlüsselung Festplattenbereinigung"
- "storage encryption disk show-status"

Ein FIPS-Laufwerk oder eine SED in ONTAP zerstören

Wenn Daten auf einem FIPS-Laufwerk oder Self-Encrypting Drive dauerhaft unzugänglich gemacht werden sollen und das Laufwerk nicht wiederverwendet werden muss, kann der `storage encryption disk destroy` Befehl verwendet werden, um die Festplatte zu zerstören.

Über diese Aufgabe

Wenn Sie ein FIPS-Laufwerk oder eine Self-Encrypting Drive zerstören, setzt das System den Festplattenverschlüsselungsschlüssel auf einen unbekannten Zufallswert und sperrt das Laufwerk unwiderruflich. Dadurch wird die Festplatte praktisch unbrauchbar und die darauf befindlichen Daten dauerhaft unzugänglich. Es besteht jedoch die Möglichkeit, die Festplatte mithilfe der auf dem Etikett aufgedruckten physischen Secure ID (PSID) auf die werkseitig konfigurierten Einstellungen zurückzusetzen. Weitere Informationen finden sich unter "Wiederinbetriebnahme eines FIPS-Laufwerks oder SED, wenn Authentifizierungsschlüssel verloren gegangen sind".

Ein FIPS-Laufwerk oder Self-Encrypting Drive sollte nur zerstört werden, wenn der Non-Returnable Disk Plus Service (NRD Plus) vorhanden ist. Durch das Zerstören eines Datenträgers erlischt die Garantie.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Alle Daten, die erhalten bleiben müssen, werden in ein Aggregat auf einer anderen Festplatte migriert.
2. Das Aggregat auf dem FIPS-Laufwerk oder dem zu zerstörenden SED löschen:

   `storage aggregate delete -aggregate aggregate_name`

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

   Weitere Informationen zu `storage aggregate delete` finden sich in der "ONTAP-Befehlsreferenz".

3. Die Datenträger-ID für das FIPS-Laufwerk oder den zu zerstörenden Self-Encrypting Drive (SED) identifizieren:

   `storage encryption disk show`

   Weitere Informationen zu `storage encryption disk show` finden sich in der "ONTAP-Befehlsreferenz".

   ```
   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. Zerstören der Festplatte:

   `storage encryption disk destroy -disk disk_id`

   Weitere Informationen zu `storage encryption disk destroy` finden sich in der "ONTAP-Befehlsreferenz".

   Sie werden aufgefordert, vor dem Fortfahren eine Bestätigungsphrase einzugeben. Die Phrase muss exakt so eingegeben werden, wie sie auf dem Bildschirm angezeigt wird.

   ```
   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.
```

Verwandte Informationen

- "Speicherverschlüsselungsfestplatte zerstören"
- "storage encryption Disk anzeigen"
- "storage encryption disk show-status"

Daten auf einem FIPS-Laufwerk oder SED im Notfall in ONTAP vernichten

Im Falle eines Sicherheitsnotfalls kann der Zugriff auf ein FIPS-Laufwerk oder eine SED sofort verhindert werden, selbst wenn das Speichersystem oder der KMIP-Server nicht mit Strom versorgt wird.

Bevor Sie beginnen

- Wenn ein KMIP-Server ohne verfügbare Stromversorgung verwendet wird, muss der KMIP-Server mit einem leicht zu zerstörenden Authentifizierungsobjekt (zum Beispiel einer Smartcard oder einem USB-Laufwerk) konfiguriert werden.
- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritt

1. Notfallvernichtung von Daten auf einem FIPS-Laufwerk oder SED durchführen:

Wenn…	Dann…

Die Stromversorgung des Speichersystems ist gewährleistet und es besteht ausreichend Zeit, das Speichersystem ordnungsgemäß offline zu nehmen.	a. Wenn das Speichersystem als HA-Paar konfiguriert ist, sollte die Übernahme deaktiviert werden. b. Alle Aggregate offline nehmen und löschen. c. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced` d. Wenn sich das Laufwerk im FIPS-Konformitätsmodus befindet, wird die FIPS-Authentifizierungsschlüssel-ID für den Knoten wieder auf die Standard-MSID gesetzt: `storage encryption disk modify -disk * -fips-key-id 0x0` e. Das Speichersystem anhalten. f. Im Wartungsmodus starten. g. Datenträger bereinigen oder zerstören: ◦ Wenn die Daten auf den Festplatten unzugänglich gemacht werden sollen und die Festplatten dennoch wiederverwendet werden können, empfiehlt sich eine Bereinigung der Festplatten: `disk encrypt sanitize -all` ◦ Wenn die Daten auf den Datenträgern unzugänglich gemacht werden sollen und die Datenträger nicht aufbewahrt werden müssen, zerstören Sie die Datenträger: `disk encrypt destroy disk_id1 disk_id2 …` Die `disk encrypt sanitize` und	Die Stromversorgung des Speichersystems ist gewährleistet, und die Daten müssen sofort vernichtet werden.

a. **Wenn Sie die Daten auf den Festplatten unzugänglich machen und die Festplatten dennoch wiederverwenden möchten, bereinigen Sie die Festplatten:**
b. Wenn das Speichersystem als HA-Paar konfiguriert ist, sollte die Übernahme deaktiviert werden.
c. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:
`set -privilege advanced`
d. Wenn sich das Laufwerk im FIPS-Konformitätsmodus befindet, wird die FIPS-Authentifizierungsschlüssel-ID für den Knoten wieder auf die Standard-MSID gesetzt:
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. Festplatte bereinigen:
`storage encryption disk sanitize -disk * -force-all-states true`
	a. **Wenn die Daten auf den Datenträgern unzugänglich gemacht werden sollen und die Datenträger nicht aufbewahrt werden müssen, die Datenträger zerstören:**
	b. Wenn das Speichersystem als HA-Paar konfiguriert ist, sollte die Übernahme deaktiviert werden.
	c. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:
	`set -privilege advanced`
	d. Zerstören Sie die Festplatten:
	`storage encryption disk destroy -disk * -force-all-states true`
		Das Speichersystem stürzt ab und befindet sich dadurch in einem dauerhaft deaktivierten Zustand, wobei alle Daten gelöscht werden. Um das System erneut zu verwenden, ist eine Neukonfiguration erforderlich.

Strom ist für den KMIP-Server verfügbar, jedoch nicht für das Speichersystem.	a. Melden Sie sich beim KMIP Server an. b. Alle Schlüssel, die mit den FIPS-Laufwerken oder Self-Encrypting Drives verknüpft sind und die Daten enthalten, auf die kein Zugriff mehr möglich sein soll, werden zerstört. Dadurch wird der Zugriff des Speichersystems auf die Festplattenverschlüsselungsschlüssel verhindert.	Strom ist für den KMIP-Server oder das Speichersystem nicht verfügbar.

Verwandte Informationen

- "Speicherverschlüsselungsfestplatte zerstören"
- "Speicherverschlüsselung Festplatte ändern"

- "Speicherverschlüsselung Festplattenbereinigung"

Wiederherstellung des Betriebs eines FIPS-Laufwerks oder einer ONTAP SED bei verlorenen Schlüsseln

Das System behandelt ein FIPS-Laufwerk oder eine SED als defekt, wenn die Authentifizierungsschlüssel dafür dauerhaft verloren gehen und nicht vom KMIP-Server abgerufen werden können. Obwohl auf die Daten auf der Festplatte nicht zugegriffen oder sie wiederhergestellt werden können, besteht die Möglichkeit, den ungenutzten Speicherplatz der SED wieder für Daten verfügbar zu machen.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Über diese Aufgabe

Dieses Verfahren sollte nur verwendet werden, wenn Sie sicher sind, dass die Authentifizierungsschlüssel für das FIPS-Laufwerk oder SED dauerhaft verloren sind und nicht wiederhergestellt werden können.

Falls die Festplatten partitioniert sind, müssen sie zuerst entpartitioniert werden, bevor Sie mit diesem Vorgang beginnen können.

> Der Befehl zum Aufheben der Partitionierung einer Festplatte ist nur auf der Diagnoseebene verfügbar und sollte nur unter Aufsicht des NetApp Supports durchgeführt werden. **Es wird dringend empfohlen, vor dem weiteren Vorgehen den NetApp Support zu kontaktieren.** Es kann auch auf die "NetApp Knowledge Base: Wie eine Ersatzfestplatte in ONTAP entpartitioniert wird" verwiesen werden.

Schritte

1. Ein FIPS-Laufwerk oder SED wieder in Betrieb nehmen:

Wenn die SEDS…	Diese Schritte können verwendet werden…

Nicht im FIPS-Konformitätsmodus oder im FIPS-Konformitätsmodus und der FIPS-Schlüssel ist verfügbar	a. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt:
	`set -privilege advanced`
	b. Der FIPS-Schlüssel wird auf die standardmäßige sichere Hersteller-ID 0x0 zurückgesetzt:
	`storage encryption disk modify -fips-key-id 0x0 -disk disk_id`
	c. Es sollte überprüft werden, ob der Vorgang erfolgreich war:
	`storage encryption disk show-status` Falls der Vorgang fehlgeschlagen ist, kann der in diesem Thema beschriebene PSID-Prozess verwendet werden.
	d. Die defekte Festplatte bereinigen:
	`storage encryption disk sanitize -disk disk_id` Mit dem Befehl `storage encryption disk show-status` kann überprüft werden, ob der Vorgang erfolgreich war, bevor zum nächsten Schritt übergegangen wird.
	e. Die bereinigte Festplatte wiederherstellen:
	`storage disk unfail -spare true -disk disk_id`
	f. Es ist zu prüfen, ob die Festplatte einen Besitzer hat:
	`storage disk show -disk disk_id` + Falls die Festplatte keinen Besitzer hat, ist einer zuzuweisen.
	`storage disk assign -owner node -disk disk_id`
	i. Öffnen Sie die Nodeshell für den Node, dem die Festplatten gehören, die Sie bereinigen möchten:
	`system node run -node node_name`
	Führe den `disk sanitize release` Befehl aus.
	g. Beenden Sie die Nodeshell. Die Festplatte wird erneut in den betriebsbereiten Zustand versetzt:
	`storage disk unfail -spare true -disk disk_id`
	h. Es sollte überprüft werden, dass die Festplatte nun als Ersatzfestplatte verfügbar ist und zur Wiederverwendung in einem Aggregat bereitsteht:
	`storage disk show -disk disk_id`

Im FIPS-Konformitätsmodus ist der FIPS-Schlüssel nicht verfügbar und die SEDs haben eine PSID auf dem Etikett aufgedruckt	a. Die PSID der Festplatte lässt sich dem Festplattenetikett entnehmen. b. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced` c. Setzen Sie die Festplatte auf die werkseitigen Einstellungen zurück: `storage encryption disk revert-to-original-state -disk` *`disk_id`* `-psid` *`disk_physical_secure_id`* Mit dem Befehl `storage encryption disk show-status` lässt sich überprüfen, ob der Vorgang erfolgreich war, bevor zum nächsten Schritt übergegangen wird. d. Wenn Sie ONTAP 9.8P5 oder früher verwenden, zum nächsten Schritt wechseln. Wenn Sie ONTAP 9.8P6 oder später verwenden, die bereinigte Festplatte wiederherstellen. `storage disk unfail -disk` *`disk_id`* e. Es ist zu prüfen, ob die Festplatte einen Besitzer hat: `storage disk show -disk` *`disk_id`* + Falls die Festplatte keinen Besitzer hat, ist einer zuzuweisen. `storage disk assign -owner node -disk` *`disk_id`* i. Öffnen Sie die Nodeshell für den Node, dem die Festplatten gehören, die Sie bereinigen möchten: `system node run -node` *`node_name`* Führe den `disk sanitize release` Befehl aus. f. Die Nodeshell wird beendet. Die Festplatte wird erneut in den betriebsbereiten Zustand versetzt: `storage disk unfail -spare true -disk` *`disk_id`* g. Es sollte überprüft werden, dass die Festplatte nun als Ersatzfestplatte verfügbar ist und zur Wiederverwendung in einem Aggregat bereitsteht: `storage disk show -disk` *`disk_id`*

Verwandte Informationen

- "Speicherverschlüsselung Festplatte ändern"
- "Speicherverschlüsselungsfestplatte auf ursprünglichen Zustand zurücksetzen"
- "Speicherverschlüsselung Festplattenbereinigung"
- "storage encryption disk show-status"

Ein FIPS-Laufwerk oder SED in ONTAP in den ungeschützten Modus zurückversetzen

Ein FIPS-Laufwerk oder SED ist nur dann vor unberechtigtem Zugriff geschützt, wenn die Authentifizierungsschlüssel-ID des Knotens auf einen anderen Wert als den Standardwert gesetzt ist. Ein FIPS-Laufwerk oder SED kann in den ungeschützten Modus zurückgesetzt werden, indem mit dem `storage encryption disk modify` Befehl die Schlüssel-ID auf den Standardwert gesetzt wird. Ein FIPS-Laufwerk oder SED im

ungeschützten Modus verwendet die Standardverschlüsselungsschlüssel, während ein FIPS-Laufwerk oder SED im geschützten Modus bereitgestellte, geheime Verschlüsselungsschlüssel verwendet. Wenn sich verschlüsselte Daten auf dem Laufwerk befinden und das Laufwerk in den ungeschützten Modus zurückgesetzt wird, bleiben die Daten weiterhin verschlüsselt und werden nicht offengelegt.

> Dieses Verfahren stellt sicher, dass alle verschlüsselten Daten unzugänglich werden, nachdem das FIPS-Laufwerk oder SED in den ungeschützten Modus zurückgesetzt wurde. Sobald die FIPS- und Datenschlüssel-IDs zurückgesetzt sind, können vorhandene Daten nicht mehr entschlüsselt werden und bleiben unzugänglich, sofern die ursprünglichen Schlüssel nicht wiederhergestellt werden.

Wenn ein HA-Paar verschlüsselnde SAS- oder NVMe-Laufwerke (SED, NSE, FIPS) verwendet, muss dieser Prozess für alle Laufwerke innerhalb des HA-Paares vor der Initialisierung des Systems (Boot-Optionen 4 oder 9) durchgeführt werden. Andernfalls kann es in Zukunft zu Datenverlust kommen, wenn die Laufwerke wiederverwendet werden.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Wenn ein FIPS-Laufwerk im FIPS-Konformitätsmodus betrieben wird, wird die FIPS-Authentifizierungsschlüssel-ID für den Knoten wieder auf den Standardwert MSID 0x0 gesetzt:

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

   Mit dem `security key-manager query` Befehl lassen sich die Schlüssel-IDs anzeigen.

   ```
   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.
   ```

   Der erfolgreiche Abschluss des Vorgangs lässt sich mit folgendem Befehl bestätigen:

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

   Den Befehl show-status so oft ausführen, bis die Zahlen in "Disks Begun" und "Disks Done" identisch sind.

   ```
   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. Die Authentifizierungsschlüssel-ID für den Knoten wird wieder auf den Standardwert MSID 0x0 gesetzt:

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

   Der Wert `-data-key-id` sollte auf 0x0 gesetzt werden, unabhängig davon, ob Sie ein SAS- oder NVMe-Laufwerk in den ungeschützten Modus zurückversetzen.

   Mit dem `security key-manager query` Befehl lassen sich die Schlüssel-IDs anzeigen.

```
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.
```

   Der erfolgreiche Abschluss des Vorgangs lässt sich mit folgendem Befehl bestätigen:

   `storage encryption disk show-status`

   Wiederholen Sie den Befehl „show-status“, bis die Zahlen übereinstimmen. Der Vorgang ist abgeschlossen, wenn die Zahlen in „disks begun“ und „disks done“ übereinstimmen.

Wartungsmodus

Ab ONTAP 9.7 kann ein FIPS-Laufwerk im Wartungsmodus neu verschlüsselt werden. Der Wartungsmodus sollte nur verwendet werden, wenn die ONTAP CLI-Anweisungen im vorherigen Abschnitt nicht genutzt werden können.

Schritte

1. Die FIPS-Authentifizierungsschlüssel-ID für den Knoten wird wieder auf den Standardwert MSID 0x0 gesetzt:

   `disk encrypt rekey_fips 0x0 disklist`

2. Die Authentifizierungsschlüssel-ID für den Knoten wird wieder auf den Standardwert MSID 0x0 gesetzt:

   `disk encrypt rekey 0x0 disklist`

3. Bestätigen Sie, dass der FIPS Authentifizierungsschlüssel erfolgreich neu generiert wurde:

```
disk encrypt show_fips
```

4. Bestätigung, dass der Authentifizierungsschlüssel erfolgreich neu verschlüsselt wurde mit:

```
disk encrypt show
```

Ihre Ausgabe zeigt wahrscheinlich entweder die Standard-MSID 0x0-Schlüssel-ID oder den vom Schlüsselserver gespeicherten 64-stelligen Wert an. Das `Locked?` Feld bezieht sich auf die Datensperrung.

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

Verwandte Informationen

- "Speicherverschlüsselung Festplatte ändern"
- "storage encryption disk show-status"

Eine externe Schlüsselverwaltungsverbindung in ONTAP entfernen

Sie können einen KMIP-Server von einem Knoten trennen, wenn der Server nicht mehr benötigt wird. Beispielsweise kann ein KMIP-Server getrennt werden, wenn auf Volumenverschlüsselung umgestellt wird.

Über diese Aufgabe

Wenn ein KMIP-Server von einem Knoten in einem HA-Paar getrennt wird, trennt das System den Server automatisch von allen Cluster-Knoten.

> Wenn nach dem Trennen eines KMIP-Servers weiterhin die externe Schlüsselverwaltung verwendet werden soll, muss ein anderer KMIP-Server verfügbar sein, um Authentifizierungsschlüssel bereitzustellen.

Bevor Sie beginnen

Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritt

1. Einen KMIP-Server vom aktuellen Knoten trennen:

Für diese ONTAP Version…	Verwenden Sie diesen Befehl…
ONTAP 9.6 und höher	`security key-manager external remove-servers -vserver SVM -key-servers host_name
IP_address:port,…`	ONTAP 9.5 und früher

In einer MetroCluster Umgebung müssen diese Befehle auf beiden Clustern für die Admin-SVM wiederholt werden.

Der folgende ONTAP 9.6 Befehl deaktiviert die Verbindungen zu zwei externen Schlüsselverwaltungsservern für `cluster1`, der erste mit dem Namen `ks1`, der auf dem Standardport 5696 lauscht, der zweite mit der IP-Adresse 10.0.0.20, der auf Port 24482 lauscht:

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

Weitere Informationen zu `security key-manager external remove-servers` und `security key-manager delete` finden sich in der "ONTAP-Befehlsreferenz".

Eigenschaften des externen Schlüsselverwaltungsservers von ONTAP ändern

Ab ONTAP 9.6 kann mit dem `security key-manager external modify-server` Befehl die I/O-Zeitüberschreitung und der Benutzername eines externen Schlüsselverwaltungsservers geändert werden.

Bevor Sie beginnen

- Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.
- In einer MetroCluster Umgebung müssen diese Schritte auf beiden Clustern für die Admin-SVM wiederholt werden.

Schritte

1. Im Speichersystem zur erweiterten Berechtigungsstufe wechseln:

   ```
   set -privilege advanced
   ```

2. Eigenschaften des externen Schlüsselverwaltungsservers für den Cluster anpassen:

   ```
   security key-manager external modify-server -vserver admin_SVM -key-server
   host_name|IP_address:port,… -timeout 0…60 -username user_name
   ```

   - Der Zeitüberschreitungswert ist die Zeit in Sekunden, die zum Aufbau der Verbindung mit dem KMIP Server benötigt wird. Wenn 0 angegeben wird, gibt es keine Zeitüberschreitung und die Verbindungsanfrage kann unbegrenzt warten. Wenn ein Wert im Bereich von 1 bis 60 angegeben wird, tritt eine Zeitüberschreitung der Verbindungsanfrage ein, wenn innerhalb der angegebenen Sekunden keine Verbindung zum KMIP Key Server hergestellt werden kann.
   - Wenn der Benutzername geändert wird, erscheint eine Aufforderung zur Eingabe eines neuen Passworts.
   - Wenn der Befehl an der Cluster-Anmeldeaufforderung ausgeführt wird, *`admin_SVM`* ist standardmäßig die Admin-SVM des aktuellen Clusters voreingestellt. Um die Eigenschaften des externen Key Manager-Servers zu ändern, ist die Rolle des Cluster-Administrators erforderlich.

Der folgende Befehl ändert den Zeitüberschreitungswert auf 45 Sekunden für den `cluster1` externen

Schlüsselverwaltungsserver, der auf dem Standardport 5696 lauscht:

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

3. Eigenschaften des externen Schlüsselverwaltungsservers für eine SVM ändern:

   `security key-manager external modify-server -vserver SVM -key-server host_name|IP_address:port,… -timeout 0…60 -username user_name`

   - Der Zeitüberschreitungswert ist die Zeit in Sekunden, die zum Aufbau der Verbindung mit dem KMIP Server benötigt wird. Wenn 0 angegeben wird, gibt es keine Zeitüberschreitung und die Verbindungsanfrage kann unbegrenzt warten. Wenn ein Wert im Bereich von 1 bis 60 angegeben wird, tritt eine Zeitüberschreitung der Verbindungsanfrage ein, wenn innerhalb der angegebenen Sekunden keine Verbindung zum KMIP Key Server hergestellt werden kann.
   - Wenn der Benutzername geändert wird, erscheint eine Aufforderung zur Eingabe eines neuen Passworts.
   - Wenn der Befehl an der SVM-Anmeldeaufforderung ausgeführt wird, *SVM* gilt standardmäßig die aktuelle SVM. Zum Ändern der Eigenschaften des externen Schlüsselverwaltungsservers sind Cluster- oder SVM-Administratorrechte erforderlich.

   Der folgende Befehl ändert den Benutzernamen und das Passwort des `svm1` externen Schlüsselverwaltungsservers, der auf dem Standardport 5696 lauscht:

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

4. Den letzten Schritt für alle weiteren SVMs wiederholen.

Verwandte Informationen

- "security key-manager external modify-server"

Übergang von der internen zur externen Schlüsselverwaltung in ONTAP

Wenn Sie von der Onboard-Schlüsselverwaltung zur externen Schlüsselverwaltung wechseln möchten, hängen die erforderlichen Schritte vom Geltungsbereich des Schlüsselmanagers ab. Für die Admin SVM (Cluster-Geltungsbereich) müssen Sie die Konfiguration der Onboard-Schlüsselverwaltung deaktivieren, bevor Sie einen externen Schlüsselmanager aktivieren können. Ab ONTAP 9.20.1 können Daten-SVMs einen externen Schlüsselmanager direkt aktivieren, und ONTAP migriert die Volume-Verschlüsselungsschlüssel der SVM automatisch vom Schlüsselmanager mit Admin-

Geltungsbereich zum neuen Schlüsselmanager der Daten-SVM.

> Ab ONTAP 9.20.1 ist diese Aufgabe nur noch erforderlich, wenn Sie die admin SVM von der internen Schlüsselverwaltung auf die externe Schlüsselverwaltung umstellen. Wenn Sie einen externen Schlüsselmanager für eine data SVM konfigurieren, müssen Sie die interne Schlüsselverwaltung nicht zuerst deaktivieren.

Bevor Sie beginnen

- Für hardwarebasierte Verschlüsselung müssen die Datenschlüssel aller FIPS-Laufwerke oder Self-Encrypting Drives auf den Standardwert zurückgesetzt werden.

  "Zurückstellen eines FIPS-Laufwerks oder SED in den ungeschützten Modus"

- Bei softwarebasierter Verschlüsselung müssen alle Volumes entschlüsselt werden.

  "Entschlüsselung der Volumendaten"

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritt

1. Löschen der Konfiguration der integrierten Schlüsselverwaltung für die admin SVM:

Für diese ONTAP Version…	Verwenden Sie diesen Befehl…
ONTAP 9.6 und höher	`security key-manager onboard disable -vserver SVM`
ONTAP 9.5 und früher	`security key-manager delete-key-database`

   Weitere Informationen zu `security key-manager onboard disable` und `security key-manager delete-key-database` finden sich in der "ONTAP-Befehlsreferenz".

Wechsel von externer Schlüsselverwaltung zu ONTAP interner Schlüsselverwaltung

Um auf die integrierte Schlüsselverwaltung umzuschalten, muss die externe Schlüsselverwaltungskonfiguration gelöscht werden, bevor die integrierte Schlüsselverwaltung aktiviert wird.

Bevor Sie beginnen

- Für hardwarebasierte Verschlüsselung müssen die Datenschlüssel aller FIPS-Laufwerke oder Self-Encrypting Drives auf den Standardwert zurückgesetzt werden.

  "Zurückstellen eines FIPS-Laufwerks oder SED in den ungeschützten Modus"

- Alle externen Schlüsselverwaltungsverbindungen müssen gelöscht worden sein.

  "Löschen einer externen Schlüsselverwaltungsverbindung"

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

Die Schritte zur Umstellung Ihrer Schlüsselverwaltung hängen von der Version von ONTAP ab, die Sie

verwenden.

ONTAP 9.6 und höher

1. Wechsel zur erweiterten Berechtigungsstufe:

   ```
   set -privilege advanced
   ```

2. Verwenden Sie den Befehl:

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

   In einer MetroCluster Umgebung muss der Befehl für die Admin-SVM auf beiden Clustern wiederholt werden.

Weitere Informationen zu `security key-manager external disable` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP 9.5 und früher

Verwenden Sie den Befehl:
`security key-manager delete-kmip-config`

Weitere Informationen zu `security key-manager delete-kmip-config` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "security key-manager external disable"

Wie ONTAP mit nicht erreichbaren Schlüsselverwaltungsservern während des Systemstarts umgeht

ONTAP trifft bestimmte Vorkehrungen, um unerwünschtes Verhalten zu vermeiden, falls ein für NSE konfiguriertes Speichersystem während des Bootvorgangs keinen der angegebenen Schlüsselverwaltungsserver erreichen kann.

Wenn das Speichersystem für NSE konfiguriert ist, die SEDs neu verschlüsselt und gesperrt sind und die SEDs eingeschaltet sind, muss das Speichersystem die erforderlichen Authentifizierungsschlüssel von den Schlüsselverwaltungsservern abrufen, um sich gegenüber den SEDs zu authentifizieren, bevor auf die Daten zugegriffen werden kann.

Das Speichersystem versucht bis zu drei Stunden lang, die angegebenen Schlüsselverwaltungsserver zu kontaktieren. Wenn das Speichersystem nach dieser Zeit keinen von ihnen erreichen kann, stoppt der Startvorgang und das Speichersystem wird angehalten.

Wenn das Speichersystem erfolgreich Kontakt zu einem angegebenen Schlüsselverwaltungsserver aufnimmt, versucht es anschließend bis zu 15 Minuten lang, eine SSL-Verbindung herzustellen. Wenn das Speichersystem keine SSL-Verbindung zu einem angegebenen Schlüsselverwaltungsserver herstellen kann, wird der Startvorgang gestoppt und das Speichersystem angehalten.

Während das Speichersystem versucht, Kontakt zu den Schlüsselverwaltungsservern aufzunehmen und eine Verbindung herzustellen, werden in der Befehlszeile detaillierte Informationen über die fehlgeschlagenen Kontaktversuche angezeigt. Die Kontaktversuche lassen sich jederzeit durch Drücken von Strg+C unterbrechen.

Als Sicherheitsmaßnahme erlauben SEDs nur eine begrenzte Anzahl unautorisierter Zugriffsversuche, danach wird der Zugriff auf die vorhandenen Daten deaktiviert. Wenn das Speichersystem keinen der angegebenen Schlüsselverwaltungsserver kontaktieren kann, um die richtigen Authentifizierungsschlüssel zu erhalten, kann es nur versuchen, sich mit dem Standardschlüssel zu authentifizieren, was zu einem Fehlschlag und einem Systemabsturz führt. Wenn das Speichersystem so konfiguriert ist, dass es im Falle eines Systemabsturzes automatisch neu startet, gerät es in eine Boot-Schleife, was zu kontinuierlich fehlgeschlagenen Authentifizierungsversuchen auf den SEDs führt.

Das Anhalten des Speichersystems in diesen Szenarien ist beabsichtigt, um zu verhindern, dass das Speichersystem in eine Boot-Schleife gerät und möglicher unbeabsichtigter Datenverlust entsteht, wenn die SEDs dauerhaft gesperrt werden, weil das Sicherheitslimit für eine bestimmte Anzahl aufeinanderfolgender fehlgeschlagener Authentifizierungsversuche überschritten wurde. Das Limit und die Art des Sperrschutzes hängen von den Herstellerspezifikationen und dem jeweiligen SED-Typ ab.

SED-Typ	Anzahl aufeinanderfolgender fehlgeschlagener Authentifizierungsversuche, die zur Sperrung führen	Sperrschutzart bei Erreichen des Sicherheitsgrenzwerts
HDD	1024	Unwiderruflich. Die Daten können nicht wiederhergestellt werden, selbst wenn der korrekte Authentifizierungsschlüssel wieder verfügbar ist.
X440_PHM2800MCTO 800GB NSE SSDs mit Firmware-Revisionen NA00 oder NA01	5	Vorübergehend. Die Sperre ist nur bis zum Neustart der Festplatte aktiv.
X577_PHM2800MCTO 800GB NSE SSDs mit Firmware-Revisionen NA00 oder NA01	5	Vorübergehend. Die Sperre ist nur bis zum Neustart der Festplatte aktiv.
X440_PHM2800MCTO 800GB NSE SSDs mit höheren Firmware-Revisionen	1024	Unwiderruflich. Die Daten können nicht wiederhergestellt werden, selbst wenn der korrekte Authentifizierungsschlüssel wieder verfügbar ist.
X577_PHM2800MCTO 800GB NSE SSDs mit höheren Firmware-Revisionen	1024	Unwiderruflich. Die Daten können nicht wiederhergestellt werden, selbst wenn der korrekte Authentifizierungsschlüssel wieder verfügbar ist.
Alle anderen SSD Modelle	1024	Unwiderruflich. Die Daten können nicht wiederhergestellt werden, selbst wenn der korrekte Authentifizierungsschlüssel wieder verfügbar ist.

Für alle SED-Typen wird der Versuchszähler nach einer erfolgreichen Authentifizierung auf null zurückgesetzt.

Wenn Sie auf dieses Szenario stoßen, in dem das Speichersystem aufgrund des Nichterreichens eines der

angegebenen Schlüsselverwaltungsserver angehalten wird, muss zunächst die Ursache für den Kommunikationsfehler ermittelt und behoben werden, bevor versucht wird, das Speichersystem weiter zu starten.

ONTAP Verschlüsselung standardmäßig deaktiviert

Ab ONTAP 9.7 ist die Aggregat- und Volumenverschlüsselung standardmäßig aktiviert, sofern Sie über eine Volumenverschlüsselungslizenz (VE) verfügen und einen integrierten oder externen Schlüsselmanager verwenden. Falls erforderlich, kann die Verschlüsselung standardmäßig für den gesamten Cluster deaktiviert werden.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können, oder SVM-Administrator, dem der Cluster-Administrator die entsprechende Berechtigung delegiert hat.

Schritt

1. Um die Verschlüsselung für den gesamten Cluster in ONTAP 9.7 oder höher standardmäßig zu deaktivieren, ist folgender Befehl auszuführen:

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

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.