NetApp Verschlüsselung managen

ONTAP 9

NetApp
February 12, 2026

Inhalt

NetApp Verschlüsselung managen

Entschlüsselung von Volume-Daten in ONTAP

Sie können mit dem `volume move start` Befehl Volume-Daten verschieben und die Verschlüsselung aufheben.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritte

1. Verschieben eines vorhandenen verschlüsselten Volumes und Entschlüsseln der Daten auf dem Volume:

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

   Erfahren Sie mehr über `volume move start` in der "ONTAP-Befehlsreferenz".

   Mit dem folgenden Befehl wird ein vorhandenes Volume mit `vol1` dem Namen zum `aggr3` Zielaggregat verschoben und die Verschlüsselung der Daten auf dem Volume aufgehoben:

   ```
   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 werden unverschlüsselt.

2. Vergewissern Sie sich, dass das Volume zur Verschlüsselung deaktiviert ist:

   `volume show -encryption`

   Erfahren Sie mehr über `volume show` in der "ONTAP-Befehlsreferenz".

   Mit dem folgenden Befehl wird angezeigt, ob Volumes in `cluster1` verschlüsselt sind:

   ```
   cluster1::> volume show -encryption

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

Verschieben Sie ein verschlüsseltes Volume in ONTAP

Sie können `volume move start` ein verschlüsseltes Volume mit dem Befehl verschieben. Das verschobene Volume kann auf demselben Aggregat oder einem

anderen Aggregat residieren.

Über diese Aufgabe

Die Verschiebung schlägt fehl, wenn der Ziel-Node oder das Ziel-Volume die Volume-Verschlüsselung nicht unterstützt.

Die `-encrypt-destination` Option für `volume move start` die Standardeinstellung TRUE für verschlüsselte Volumes. Wenn Sie angeben müssen, dass das Ziel-Volume nicht verschlüsselt werden soll, wird sichergestellt, dass die Verschlüsselung der Daten auf dem Volume nicht versehentlich aufgehoben wird.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritte

1. Verschieben Sie ein vorhandenes verschlüsseltes Volume, und lassen Sie die Daten auf dem Volume verschlüsselt:

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

   Erfahren Sie mehr über `volume move start` in der "ONTAP-Befehlsreferenz".

   Mit dem folgenden Befehl wird ein vorhandenes Volume `vol1` mit dem Namen zum `aggr3` Zielaggregat verschoben und die Daten des Volumes bleiben verschlüsselt:

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

2. Vergewissern Sie sich, dass das Volume für die Verschlüsselung aktiviert ist:

   `volume show -is-encrypted true`

   Erfahren Sie mehr über `volume show` in der "ONTAP-Befehlsreferenz".

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

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

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

Ändern Sie den Verschlüsselungsschlüssel für ein Volume mit dem Befehl Volume Encryption Rekey Start in ONTAP

Es handelt sich hierbei um eine Best Practice für Sicherheit, den Verschlüsselungsschlüssel für ein Volume regelmäßig zu ändern. Ab ONTAP 9.3 können

Sie den `volume encryption rekey start` Befehl verwenden, um den Verschlüsselungsschlüssel zu ändern.

Über diese Aufgabe

Sobald Sie einen Rekeyvorgang starten, muss er abgeschlossen sein. Es gibt keine Rückkehr zum alten Schlüssel. Falls während des Vorgangs ein Performance-Problem auftritt, können Sie den `volume encryption rekey pause` Befehl ausführen, um den Vorgang anzuhalten, und den `volume encryption rekey resume` Befehl, um den Vorgang fortzusetzen.

Bis der Vorgang des Neuschlüssels abgeschlossen ist, verfügt das Volume über zwei Tasten. Neue Schreibzugriffe und die entsprechenden Lesezugriffe nutzen den neuen Schlüssel. Andernfalls wird der alte Schlüssel bei den Lesevorgängen verwendet.

Sie können kein `volume encryption rekey start` Rekekey für ein SnapLock-Volume verwenden.

Schritte

1. Ändern eines Verschlüsselungsschlüssels:

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

   Mit dem folgenden Befehl wird der Verschlüsselungsschlüssel für `vol1` auf SVM geändert`vs1`:

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

2. Überprüfen Sie den Status der Rekeybedienung:

   `volume encryption rekey show`

   Erfahren Sie mehr über `volume encryption rekey show` in der "ONTAP-Befehlsreferenz".

   Mit dem folgenden Befehl wird der Status der Rekeyoperation angezeigt:

   ```
   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. Vergewissern Sie sich nach Abschluss des Rekeyvorgangs, dass das Volume für die Verschlüsselung aktiviert ist:

   `volume show -is-encrypted true`

   Erfahren Sie mehr über `volume show` in der "ONTAP-Befehlsreferenz".

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

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

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

Ändern Sie den Verschlüsselungsschlüssel für ein Volume mit dem Befehl „ONTAP Volume Move Start“

Es handelt sich hierbei um eine Best Practice für Sicherheit, den Verschlüsselungsschlüssel für ein Volume regelmäßig zu ändern. Sie können den `volume move start` Befehl verwenden, um den Verschlüsselungsschlüssel zu ändern. Das verschobene Volume kann auf demselben Aggregat oder einem anderen Aggregat residieren.

Über diese Aufgabe

Sie können kein `volume move start` Rekekey für ein SnapLock- oder FlexGroup-Volume verwenden.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritte

1. Verschieben eines vorhandenen Volumes und Ändern des Verschlüsselungsschlüssels:

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

   Erfahren Sie mehr über `volume move start` in der "ONTAP-Befehlsreferenz".

   Mit dem folgenden Befehl wird ein vorhandenes Volume **`vol1`** mit dem Namen in das Zielaggregat verschoben **`aggr2`** und der Schlüssel geändert:

   ```
   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. Vergewissern Sie sich, dass das Volume für die Verschlüsselung aktiviert ist:

   `volume show -is-encrypted true`

   Erfahren Sie mehr über `volume show` in der "ONTAP-Befehlsreferenz".

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

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

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

Rotieren Sie die Authentifizierungsschlüssel für ONTAP NetApp Storage Encryption

Sie können die Authentifizierungsschlüssel mit der NetApp Storage Encryption (NSE) drehen.

Über diese Aufgabe

Die rotierenden Authentifizierungsschlüssel in einer NSE-Umgebung werden unterstützt, wenn Sie External Key Manager (KMIP) verwenden.

> Rotierende Authentifizierungsschlüssel in einer NSE-Umgebung werden von Onboard Key Manager (OKM) nicht unterstützt.

Schritte

1. `security key-manager create-key`Erstellen Sie mit dem Befehl neue Authentifizierungsschlüssel.

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

2. Verwenden Sie den `storage encryption disk modify -disk * -data-key-id` Befehl, um die Authentifizierungsschlüssel zu ändern.

Verwandte Informationen

- "Speicherverschlüsselung Datenträger ändern"

Löschen Sie ein verschlüsseltes Volume in ONTAP

Sie können das `volume delete` verschlüsselte Volume mit dem Befehl löschen.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Das Volume muss sich offline befinden.

Schritt

1. Verschlüsseltes Volume löschen:

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

   Erfahren Sie mehr über `volume delete` in der "ONTAP-Befehlsreferenz".

Mit dem folgenden Befehl wird ein verschlüsseltes Volume mit dem Namen gelöscht `vol1`:

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

Geben Sie ein `yes`, wenn Sie zur Bestätigung des Löschvorgangs 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 löschen. Dieser Befehl erfordert erweiterte Berechtigungen. Erfahren Sie mehr über `volume delete` in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

Sie können mit dem `volume recovery-queue` Befehl ein gelöschtes Volume während der Aufbewahrungsfrist wiederherstellen, nachdem Sie den `volume delete` Befehl ausgegeben haben:

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

"So verwenden Sie die Volume Recovery-Funktion"

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"

Ändern Sie die ONTAP Onboard-Schlüsselverwaltungspassphrase

NetApp empfiehlt, die Passphrase für die Onboard-Schlüsselverwaltung regelmäßig zu ändern. Sie müssen die neue Passphrase an einem sicheren Ort außerhalb des Speichersystems aufbewahren.

Bevor Sie beginnen

- Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.
- In einer MetroCluster Umgebung müssen Sie nach der Aktualisierung der Passphrase auf dem lokalen Cluster die Aktualisierung der Passphrase auf dem Partnercluster synchronisieren.

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Ändern Sie die Passphrase für die Onboard-Schlüsselverwaltung. Der zu verwendende Befehl hängt von der verwendeten ONTAP Version ab.

   ONTAP 9.6 und höher

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

   ONTAP 9.5 und frühere Versionen

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

3. Geben Sie eine Passphrase zwischen 32 und 256 Zeichen oder für „cc-mode“ eine Passphrase zwischen 64 und 256 Zeichen ein.

   Wenn die angegebene „`cc-Mode`“-Passphrase weniger als 64 Zeichen beträgt, liegt eine Verzögerung von fünf Sekunden vor, bevor die Eingabeaufforderung für das Setup des Schlüsselmanagers die Passphrase erneut anzeigt.

4. Geben Sie die Passphrase erneut an der Eingabeaufforderung zur Bestätigung der Passphrase ein.
5. Wenn Sie eine MetroCluster -Konfiguration verwenden, synchronisieren Sie die aktualisierte Passphrase mit dem Partnercluster.
   a. Synchronisieren Sie die Passphrase auf dem Partnercluster, indem Sie den richtigen Befehl für Ihre ONTAP Version auswählen:

ONTAP 9.6 und höher

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

ONTAP 9.5 und frühere Versionen

- Führen Sie in ONTAP 9.5 Folgendes aus:

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

- In ONTAP 9.4 und früheren Versionen warten Sie nach der Aktualisierung der Passphrase auf dem lokalen Cluster 20 Sekunden und führen dann den folgenden Befehl auf dem Partnercluster aus:

  ```
  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

Kopieren Sie die Passphrase für die interne Schlüsselverwaltung an einen sicheren Ort außerhalb des Speichersystems zur späteren Verwendung.

Sichern Sie die Schlüsselverwaltungsinformationen manuell, wann immer Sie die Passphrase für die integrierte Schlüsselverwaltung ändern.

Verwandte Informationen

- "Manuelles Backup der integrierten Informationen für das Verschlüsselungsmanagement"
- "Sicherheitsschlüssel-Manager, integriertes Update-Passwort"

Manuelles Sichern der ONTAP Onboard-Schlüsselverwaltungsinformationen

Wenn Sie die Onboard-Passphrase für das Verschlüsselungsmanagement an einen sicheren Ort außerhalb des Storage-Systems konfigurieren, sollten Sie die Onboard-Verschlüsselungsmanagement-Informationen an einen sicheren Ort kopieren.

Bevor Sie beginnen

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

Über diese Aufgabe

Alle Informationen zum Verschlüsselungsmanagement werden automatisch in der replizierten Datenbank (RDB) für den Cluster gesichert. Außerdem sollten Sie die Informationen zum Verschlüsselungsmanagement manuell für den Notfall sichern.

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

```
set -privilege advanced
```

2. Anzeigen der Backup-Informationen für das Verschlüsselungsmanagement für das Cluster:

Für diese ONTAP-Version…	Befehl
ONTAP 9.6 und höher	`security key-manager onboard show-backup`
ONTAP 9.5 und frühere Versionen	`security key-manager backup show`

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

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

     --------------------------BEGIN BACKUP--------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
     QAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
     IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAAACQAAAAAAAAAgAAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
     AQAAAAMAAAAYAQAAAAAAAADA5/ccAAAAAIgAAAAAAAAAoAAAAAAAAAAEOTcR0AAAAA
     AAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAACIAAAAAAAAA
     KAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAgAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
     AAAAAAAAAAkAAAAAAAAAAIAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
     LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA
     1cNLLwAAAAAiAAAAAAAAAACgAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAIAAAAAAAAkA
     ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAIgAAAAAAAAAoAAAAAAAAAAJ4/cQsAAAAA
     AAAAAAAAAACAAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAACQAAAAAAAAA
     gAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
     rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     ---------------------------END BACKUP---------------------------
```

3. Backup-Informationen sollten bei einem Notfall an einen sicheren Ort außerhalb des Storage-Systems kopiert werden.

Verwandte Informationen

- "Sicherheitsschlüssel-Manager Onboard Show-Backup"
- "Sicherheitsschlüssel-Manager-Backup anzeigen"

Wiederherstellung der integrierten Verschlüsselungsmanagement-Schlüssel in ONTAP

Gelegentlich müssen Sie möglicherweise einen integrierten Verschlüsselungsschlüssel für die Schlüsselverwaltung wiederherstellen. Nachdem Sie überprüft haben, dass ein Schlüssel wiederhergestellt werden muss, können Sie den Onboard Key Manager zum Wiederherstellen des Schlüssels einrichten. Das Verfahren zum Wiederherstellen Ihrer Verschlüsselungsschlüssel für die Onboard-Schlüsselverwaltung hängt von Ihrer ONTAP-Version ab.

Bevor Sie beginnen

- Löschen Sie die externe Schlüsselmanager-Datenbank, wenn Sie NSE mit einem externen KMIP-Server verwenden. Weitere Einzelheiten finden Sie unter"Übergang von der externen Schlüsselverwaltung zur integrierten ONTAP -Schlüsselverwaltung" .
- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

> Wenn Sie NSE in einem System mit einem Flash Cache Modul verwenden, sollten Sie auch NVE oder NAE aktivieren. NSE verschlüsselt keine Daten im Flash Cache Modul.

ONTAP 9.6 und höher

> Wenn Sie ONTAP 9.8 oder höher ausführen und Ihr Stammvolume verschlüsselt ist, befolgen Sie das Verfahren für [ontap-9-8].

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

   Erfahren Sie mehr über `security key-manager key query` in der "ONTAP-Befehlsreferenz".

2. Stellen Sie den Schlüssel wieder her:
   `security key-manager onboard sync`

   Erfahren Sie mehr über `security key-manager onboard sync` in der "ONTAP-Befehlsreferenz".

3. Geben Sie an der Eingabeaufforderung für die Passphrase die integrierte Passphrase für das Verschlüsselungsmanagement für das Cluster ein.

ONTAP 9.8 oder höher mit verschlüsseltem Root-Volume

Wenn Sie ONTAP 9.8 und höher verwenden und Ihr Root-Volume verschlüsselt ist, müssen Sie mit dem Boot-Menü eine integrierte Recovery-Passphrase für das Verschlüsselungsmanagement festlegen. Dieser Vorgang

ist auch erforderlich, wenn Sie einen Bootmedienaustausch durchführen.

1. Starten Sie den Knoten im Boot-Menü und wählen Sie Option `(10) Set onboard key management recovery secrets`.
2. Geben Sie ein, `y` um diese Option zu verwenden.
3. Geben Sie an der Eingabeaufforderung die integrierte Passphrase für das Verschlüsselungsmanagement für das Cluster ein.
4. Geben Sie an der Eingabeaufforderung die Backup-Schlüsseldaten ein.

   Nachdem Sie die Daten des Sicherungsschlüssels eingegeben haben, kehrt der Knoten zum Startmenü zurück.

5. Wählen Sie im Boot-Menü die Option `(1) Normal Boot`.

ONTAP 9.5 und frühere Versionen

1. Überprüfen Sie, ob der Schlüssel wiederhergestellt werden muss:
   `security key-manager key show`
2. Stellen Sie den Schlüssel wieder her:
   `security key-manager setup -node` *node*

   Erfahren Sie mehr über `security key-manager setup` im"ONTAP-Befehlsreferenz" .
3. Geben Sie an der Eingabeaufforderung für die Passphrase die integrierte Passphrase für das Verschlüsselungsmanagement für das Cluster ein.

Wiederherstellen der ONTAP External Key Management-Verschlüsselungsschlüssel

Sie können die externen Verschlüsselungsschlüssel zum Verschlüsselungsmanagement manuell wiederherstellen und sie auf einen anderen Node verschieben. Dies sollten Sie tun, wenn Sie einen Node neu starten, der während des Erstellungsens der Schlüssel für das Cluster vorübergehend nicht verfügbar war.

Über diese Aufgabe

In ONTAP 9.6 und später können Sie mit dem `security key-manager key query -node node_name` Befehl überprüfen, ob Ihr Schlüssel wiederhergestellt werden muss.

In ONTAP 9.5 und früher können Sie mit dem `security key-manager key show` Befehl überprüfen, ob Ihr Schlüssel wiederhergestellt werden muss.

> Wenn Sie NSE in einem System mit einem Flash Cache Modul verwenden, sollten Sie auch NVE oder NAE aktivieren. NSE verschlüsselt keine Daten im Flash Cache Modul.

Erfahren Sie mehr über `security key-manager key query` in der "ONTAP-Befehlsreferenz".

Bevor Sie beginnen

Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

Schritte

1. Wenn Sie ONTAP 9.8 oder höher verwenden und Ihr Root-Volume verschlüsselt ist, gehen Sie wie folgt vor:

   Wenn Sie ONTAP 9.7 oder früher oder ONTAP 9.8 oder höher verwenden und Ihr Root-Volume nicht verschlüsselt ist, überspringen Sie diesen Schritt.

   a. Stellen Sie die Bootargs:
   `setenv kmip.init.ipaddr <ip-address>` + +
   `setenv kmip.init.netmask <netmask>` `setenv kmip.init.gateway <gateway>` + ein
   `setenv kmip.init.interface e0M` `boot_ontap`

   b. Starten Sie den Knoten im Boot-Menü und wählen Sie Option `(11) Configure node for external key management.`

   c. Befolgen Sie die Anweisungen zum Eingeben des Managementzertifikats.

      Nachdem alle Informationen zum Managementzertifikat eingegeben wurden, kehrt das System zum Boot-Menü zurück.

   d. Wählen Sie im Boot-Menü die Option `(1) Normal Boot.`

2. Wiederherstellen des Schlüssels:

Für diese ONTAP-Version…	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 frühere Versionen

   `node` Standardmäßig werden alle Knoten angezeigt.

   Dieser Befehl wird nicht unterstützt, wenn das integrierte Verschlüsselungsmanagement aktiviert ist.

   Der folgende ONTAP 9.6-Befehl stellt externe Schlüssel zur Schlüsselverwaltung-Authentifizierung auf allen Knoten in wieder her `cluster1`:

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

Verwandte Informationen

- "Externe Wiederherstellung des Sicherheitsschlüsselmanagers"

Ersetzen Sie KMIP-SSL-Zertifikate auf dem ONTAP Cluster

Alle SSL-Zertifikate haben ein Ablaufdatum. Sie müssen Ihre Zertifikate aktualisieren, bevor sie ablaufen, um den Verlust des Zugriffs auf Authentifizierungsschlüssel zu verhindern.

Bevor Sie beginnen

- Sie müssen das öffentliche Ersatzzertifikat und den privaten Schlüssel für das Cluster (KMIP-Client-Zertifikat) erhalten haben.
- Sie müssen das öffentliche Ersatzzertifikat für den KMIP-Server (KMIP-Server-Ca-Zertifikat) erhalten haben.
- Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.
- Wenn Sie die KMIP-SSL-Zertifikate in einer MetroCluster-Umgebung ersetzen, müssen Sie auf beiden Clustern das gleiche KMIP-SSL-Ersatzzertifikat installieren.

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

Schritte

1. Installieren Sie das neue KMIP Server-Ca-Zertifikat:

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

2. Installieren Sie das neue KMIP-Client-Zertifikat:

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

3. Aktualisieren Sie die Konfiguration des Schlüsselmanagers, um die neu installierten Zertifikate zu verwenden:

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

   Wenn Sie ONTAP 9.6 oder höher in einer MetroCluster-Umgebung ausführen und die Schlüsselmanager-Konfiguration auf der Admin-SVM ändern möchten, müssen Sie den Befehl in der Konfiguration auf beiden Clustern ausführen.

Beim Aktualisieren der Schlüsselmanagerkonfiguration zur Verwendung der neu installierten Zertifikate wird ein Fehler zurückgegeben, 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 Client-Zertifikats unterscheiden sich vom vorhandenen Client-Zertifikat" Anweisungen zum Überschreiben dieses Fehlers finden Sie unter.

Verwandte Informationen

- "Sicherheitszertifikat installieren"
- "Sicherheitsschlüssel-Manager extern ändern"

Ersetzen Sie ein FIPS-Laufwerk oder SED in ONTAP

Sie können ein FIPS-Laufwerk oder SED auf dieselbe Weise ersetzen, wie Sie eine normale Festplatte ersetzen. Stellen Sie sicher, dass Sie dem Ersatzlaufwerk neue Datenauthentifizierungsschlüssel zuweisen. Bei einem FIPS-Laufwerk kann auch ein neuer FIPS 140-2-Authentifizierungsschlüssel zugewiesen werden.

Wenn ein HA-Paar verwendet"Verschlüsselung von SAS- oder NVMe-Laufwerken (SED, NSE, FIPS)", müssen Sie die Anweisungen im Thema "Ein FIPS-Laufwerk oder eine SED-Festplatte in den ungeschützten Modus zurückkehren" für alle Laufwerke innerhalb des HA-Paars befolgen, bevor Sie das System initialisieren (Startoptionen 4 oder 9). Andernfalls kann es zu künftigen Datenverlusten kommen, wenn die Laufwerke einer anderen Verwendung zugewiesen werden.

Bevor Sie beginnen

- Sie müssen die Schlüssel-ID für den vom Laufwerk verwendeten Authentifizierungsschlüssel kennen.
- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritte

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

   `storage disk show -broken`

   Erfahren Sie mehr über `storage disk show` in der "ONTAP-Befehlsreferenz".

   ```
   cluster1::> storage disk show -broken
   Original Owner: cluster1-01
     Checksum Compatibility: block
                                                                    Usable
   Physical
       Disk   Outage Reason HA Shelf Bay Chan   Pool  Type    RPM     Size
   Size
       ------ ---- ------------ ---- --- ---- ------ -----  -----  -------
   -------
       0.0.0  admin  failed  0b    1   0    A  Pool0  FCAL  10000  132.8GB
   133.9GB
       0.0.7  admin  removed 0b    2   6    A  Pool1  FCAL  10000  132.8GB
   134.2GB
   [...]
   ```

2. Entfernen Sie die ausgefallene Festplatte, und ersetzen Sie sie durch ein neues FIPS-Laufwerk oder eine neue SED. Befolgen Sie die Anweisungen im Hardware-Leitfaden für das Festplatten-Shelf-Modell.
3. Besitzer der neu ersetzten Festplatte zuweisen:

   `storage disk assign -disk disk_name -owner node`

   Erfahren Sie mehr über `storage disk assign` in der "ONTAP-Befehlsreferenz".

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

4. Vergewissern Sie sich, dass die neue Festplatte zugewiesen wurde:

   `storage encryption disk show`

Erfahren Sie mehr über `storage encryption disk show` 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. Weisen Sie den Datenauthentifizierungsschlüssel dem FIPS-Laufwerk oder der SED zu.

   "Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder einer SED (externes Verschlüsselungsmanagement)"

6. Weisen Sie bei Bedarf dem FIPS-Laufwerk einen FIPS 140-2-Authentifizierungsschlüssel zu.

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

Verwandte Informationen

- "Speicherdatenträger zuweisen"
- "Speicherdatenträger anzeigen"
- "Speicherverschlüsselung Datenträger anzeigen"

Daten auf einem FIPS-Laufwerk oder SED-Laufwerk können nicht darauf zugegriffen werden

Erfahren Sie, wie Sie ONTAP Daten auf einem FIPS-Laufwerk oder SED unzugänglich machen

Wenn Daten auf einem FIPS- oder SED-Laufwerk dauerhaft nicht zugänglich sind, aber den nicht genutzten Speicherplatz des Laufwerks für neue Daten beibehalten werden sollen, kann die Festplatte bereinigen. Wenn Sie Daten dauerhaft unzugänglich machen und Sie das Laufwerk nicht wiederverwenden müssen, können Sie es zerstören.

- Festplattenbereinigung

  Wenn Sie ein selbstverschlüsselndes Laufwerk desinfizieren, ändert das System den Verschlüsselungsschlüssel in einen neuen zufälligen Wert, setzt den Einschloß-Status auf false zurück und setzt die Schlüssel-ID auf einen Standardwert, entweder die Herstellersichere ID 0x0 (SAS-Laufwerke) oder einen Null-Schlüssel (NVMe-Laufwerke). Dadurch werden die Daten auf der Festplatte nicht mehr zugänglich und können nicht abgerufen werden. Sie können desinfizierte Festplatten als nicht auf Null bereinigte Ersatzfestplatten wiederverwenden.

- Festplatte zerstören

  Wenn Sie ein FIPS- oder SED-Laufwerk zerstören, setzt das System den Schlüssel für die Festplattenverschlüsselung auf einen unbekannten zufälligen Wert und sperrt die Festplatte unwiderruflich. Dadurch wird die Festplatte permanent nicht nutzbar und die Daten darauf dauerhaft zugänglich gemacht.

Es können einzelne Self-Encrypting Drives oder alle Self-Encrypting Drives eines Node bereinigen oder zerstört werden.

Bereinigen eines FIPS-Laufwerks oder SED in ONTAP

Wenn Sie Daten auf einem FIPS-Laufwerk oder einer SED dauerhaft unzugänglich machen möchten und das Laufwerk für neue Daten verwenden möchten, können Sie `storage encryption disk sanitize` das Laufwerk mit dem Befehl bereinigen.

Über diese Aufgabe

Wenn Sie ein selbstverschlüsselndes Laufwerk desinfizieren, ändert das System den Verschlüsselungsschlüssel in einen neuen zufälligen Wert, setzt den Einschloß-Status auf false zurück und setzt die Schlüssel-ID auf einen Standardwert, entweder die Herstellersichere ID 0x0 (SAS-Laufwerke) oder einen Null-Schlüssel (NVMe-Laufwerke). Dadurch werden die Daten auf der Festplatte nicht mehr zugänglich und können nicht abgerufen werden. Sie können desinfizierte Festplatten als nicht auf Null bereinigte Ersatzfestplatten wiederverwenden.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritte

1. Migrieren Sie alle Daten, die in einem Aggregat auf einer anderen Festplatte aufbewahrt werden müssen.
2. Löschen Sie das Aggregat auf dem FIPS-Laufwerk oder der SED, das bereinigt werden soll:

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

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

   Erfahren Sie mehr über `storage aggregate delete` in der "ONTAP-Befehlsreferenz".

3. Festplatten-ID für das zu desinfizierte FIPS-Laufwerk oder SED ermitteln:

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

   Erfahren Sie mehr über `storage encryption disk show` 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-Compliance-Modus ausgeführt wird, legen Sie die FIPS-Authentifizierungsschlüssel-ID für den Node wieder auf den Standard MSID 0x0:

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

   Sie können den `security key-manager query` Befehl verwenden, um Schlüssel-IDs anzuzeigen.

```
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. Antrieb desinfizieren:

   `storage encryption disk sanitize -disk disk_id`

   Mit diesem Befehl können Sie nur Hot-Spare- oder defekte Festplatten bereinigen. Um unabhängig vom Typ alle Festplatten bereinigen `-force-all-state` zu können, verwenden Sie die Option. Erfahren Sie mehr über `storage encryption disk sanitize` in der "ONTAP-Befehlsreferenz".

   ⓘ ONTAP fordert Sie auf, eine Bestätigungsaufforderung einzugeben, bevor Sie fortfahren. Geben Sie den Ausdruck genau so ein, wie er 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. Bereinigte Festplatte aufheben: `storage disk unfail -spare true -disk disk_id`

7. Überprüfen Sie, ob die Festplatte einen Besitzer hat: `storage disk show -disk disk_id` + Wenn die Platte keinen Besitzer hat, weisen Sie einen zu. `storage disk assign -owner node -disk disk_id`
8. Geben Sie den Knotenpunkt für den Knoten ein, der die Festplatten besitzt, die Sie desinfizieren möchten:

   `system node run -node node_name`

   Führen Sie den `disk sanitize release` Befehl aus.

9. Verlassen Sie die Nodeshell. Fehler der Festplatte erneut aufheben: `storage disk unfail -spare true -disk disk_id`
10. Überprüfen Sie, ob die Festplatte jetzt als Ersatzlaufwerk verwendet und in einem Aggregat wiederverwendet werden kann: `storage disk show -disk disk_id`

Verwandte Informationen

- "Speicherdatenträger zuweisen"
- "Speicherdatenträger anzeigen"
- "Speicherfestplatte nicht fehlgeschlagen"
- "Speicherverschlüsselung Datenträger ändern"
- "Speicherverschlüsselung Datenträgerbereinigung"
- "Speicherverschlüsselung Datenträger Status anzeigen"

Zerstören Sie ein FIPS-Laufwerk oder eine SED in ONTAP

Wenn Sie Daten auf einem FIPS-Laufwerk oder SED dauerhaft unzugänglich machen möchten und das Laufwerk nicht erneut verwenden müssen, können Sie den `storage encryption disk destroy` Befehl verwenden, um die Festplatte zu zerstören.

Über diese Aufgabe

Wenn Sie ein FIPS- oder SED-Laufwerk zerstören, setzt das System den Schlüssel für die Festplattenverschlüsselung auf einen unbekannten zufälligen Wert und sperrt das Laufwerk unwiderruflich. Dadurch wird die Festplatte praktisch nicht nutzbar und die Daten auf ihr dauerhaft zugänglich. Sie können die Festplatte jedoch mithilfe der physischen sicheren ID (PSID) auf dem Etikett des Datenträgers auf die werkseitig konfigurierten Einstellungen zurücksetzen. Weitere Informationen finden Sie unter "Ein FIPS-Laufwerk oder eine SED-Appliance wird zurückgegeben, wenn Authentifizierungsschlüssel verloren gehen".

> Ein FIPS- oder SED-Laufwerk darf nur zerstört werden, wenn Sie über den Non-Returnable Disk Plus-Service (NRD Plus) verfügen. Beim Zerstören einer Festplatte wird die Gewährleistung nicht mehr abgedeckt.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritte

1. Migrieren Sie alle Daten, die in einem Aggregat auf einer anderen, unterschiedlichen Festplatte aufbewahrt werden müssen.
2. Löschen Sie das Aggregat auf dem zu zerstörenden FIPS-Laufwerk oder SED:

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

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

Erfahren Sie mehr über `storage aggregate delete` in der "ONTAP-Befehlsreferenz".

3. Identifizieren Sie die Festplatten-ID für das zu zerstörenden FIPS-Laufwerk oder die SED:

```
storage encryption disk show
```

Erfahren Sie mehr über `storage encryption disk show` 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 Sie die Festplatte:

```
storage encryption disk destroy -disk disk_id
```

Erfahren Sie mehr über `storage encryption disk destroy` in der "ONTAP-Befehlsreferenz".

Sie werden aufgefordert, einen Bestätigungsphrase einzugeben, bevor Sie fortfahren. Geben Sie den Ausdruck genau so ein, wie er 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

- "Speicherverschlüsselung Festplatte zerstören"
- "Speicherverschlüsselung Datenträger anzeigen"
- "Speicherverschlüsselung Datenträger Status anzeigen"

Notfall shred Daten auf einem FIPS-Laufwerk oder SED in ONTAP

Im Falle eines Sicherheitsnotfalls können Sie den Zugriff auf ein FIPS-Laufwerk oder eine SED umgehend verhindern, auch wenn dem Storage-System oder dem KMIP-Server keine Stromversorgung zur Verfügung steht.

Bevor Sie beginnen

- Wenn Sie einen KMIP-Server ohne Stromversorgung verwenden, muss der KMIP-Server mit einem einfach zerstörten Authentifizierungselement (z. B. eine Smartcard oder ein USB-Laufwerk) konfiguriert werden.
- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritt

1. Daten im Notfall auf einem FIPS-Laufwerk oder SED sreddern:

Wenn…	Dann…

Das Storage-System verfügt über einen Stromanstieg, und Sie können das Storage-System normal offline schalten	a. Wenn das Storage-System als HA-Paar konfiguriert ist, deaktivieren Sie Takeover. b. Alle Aggregate offline schalten und löschen. c. Stellen Sie die Berechtigungsebene auf erweitert: + ein `set -privilege advanced` d. Wenn sich das Laufwerk im FIPS-Compliance-Modus befindet, setzen Sie die FIPS-Authentifizierungsschlüssel-ID für den Node auf die Standard-MSID: + zurück `storage encryption disk modify -disk * -fips-key-id 0x0` e. Stoppen Sie das Speichersystem. f. Booten Sie im Wartungsmodus. g. Desinfizieren oder zerstören Sie die Festplatten: ◦ Wenn Sie die Daten auf den Festplatten unzugänglich machen und die Festplatten weiterhin wiederverwenden können, bereinigen Sie die Festplatten: `disk encrypt sanitize -all` ◦ Wenn Sie die Daten auf den Festplatten unzugänglich machen möchten und Sie die Festplatten nicht speichern müssen, zerstören Sie die Festplatten: `disk encrypt destroy disk_id1 disk_id2 …`	Dem Storage-System steht Strom zur Verfügung, und Sie müssen die Daten sofort schüttelt haben

a. **Wenn Sie die Daten auf den Datenträgern unzugänglich machen und die Festplatten noch wiederverwenden können, desinfizieren Sie die Festplatten:**
b. Wenn das Storage-System als HA-Paar konfiguriert ist, deaktivieren Sie Takeover.
c. Legen Sie die Berechtigungsebene auf erweitert fest:
`set -privilege advanced`
d. Wenn sich das Laufwerk im FIPS-Compliance-Modus befindet, legen Sie die FIPS-Authentifizierungsschlüssel-ID für den Node wieder auf die Standard-MSID fest:
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. Festplatte bereinigen:
`storage encryption disk sanitize -disk * -force-all-states true`
	a. **Wenn Sie die Daten auf den Datenträgern unzugänglich machen und Sie nicht brauchen, um die Festplatten zu speichern, zerstören Sie die Festplatten:**
	b. Wenn das Storage-System als HA-Paar konfiguriert ist, deaktivieren Sie Takeover.
	c. Legen Sie die Berechtigungsebene auf erweitert fest:
	`set -privilege advanced`
	d. Zerstören Sie die Festplatten:
	`storage encryption disk destroy -disk * -force-all-states true`
		Das Speichersystem kommt zu einer Panik, sodass das System dauerhaft deaktiviert ist, während alle Daten gelöscht werden. Um das System erneut zu verwenden, müssen Sie es neu konfigurieren.

Der KMIP-Server mit Strom ist, nicht jedoch für das Storage-System verfügbar	a. Melden Sie sich beim KMIP-Server an. b. Vernichten Sie alle Schlüssel, die den FIPS-Laufwerken oder SEDs zugeordnet sind, die die Daten enthalten, auf die Sie Zugriff verhindern möchten. Dadurch wird der Zugriff auf die Festplattenverschlüsselung durch das Speichersystem verhindert.	Der KMIP-Server oder das Storage-System bieten keine Stromversorgung

Verwandte Informationen

- "Speicherverschlüsselung Festplatte zerstören"
- "Speicherverschlüsselung Datenträger ändern"

- "Speicherverschlüsselung Datenträgerbereinigung"

Geben Sie ein FIPS-Laufwerk oder SED wieder in Betrieb, wenn Authentifizierungsschlüssel in ONTAP verloren gehen

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 Sie nicht auf die Daten auf der Festplatte zugreifen oder diese wiederherstellen können, können Sie Schritte Unternehmen, um den nicht genutzten Speicherplatz der SED für Daten erneut verfügbar zu machen.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Über diese Aufgabe

Sie sollten diesen Prozess nur verwenden, wenn Sie sicher sind, dass die Authentifizierungsschlüssel für das FIPS-Laufwerk oder die SED dauerhaft verloren gehen und nicht wiederhergestellt werden können.

Wenn die Festplatten partitioniert werden, müssen sie zunächst nicht partitioniert werden, bevor Sie diesen Prozess starten können.

Der Befehl zum Aufheben der Partitionierung einer Festplatte ist nur auf Diagnoseebene verfügbar und sollte nur unter Aufsicht des NetApp Supports ausgeführt werden. **Es wird dringend empfohlen, dass Sie sich an den NetApp -Support wenden, bevor Sie fortfahren.** Sie können sich auch auf die"NetApp Knowledge Base: So trennen Sie die Partition eines Ersatzlaufwerks in ONTAP" .

Schritte

1. Rückgabe eines FIPS-Laufwerks oder SED an den Dienst:

Wenn die SEDS…	Verwenden Sie die folgenden Schritte…

Nicht im FIPS-Compliance-Modus oder im FIPS-Compliance-Modus und der FIPS-Schlüssel ist verfügbar	a. Legen Sie die Berechtigungsebene auf erweitert fest:
	`set -privilege advanced`
	b. Setzen Sie den FIPS-Schlüssel auf die standardmäßige gesicherte Herstellerkennung 0x0 zurück:
	`storage encryption disk modify -fips-key-id 0x0 -disk disk_id`
	c. Überprüfen Sie, ob `storage encryption disk show-status` der Vorgang erfolgreich war: Wenn der Vorgang fehlgeschlagen ist, verwenden Sie den PSID-Prozess in diesem Thema.
	d. Bereinigen Sie die beschädigte Festplatte:
	`storage encryption disk sanitize -disk disk_id` Überprüfen Sie mit dem Befehl `storage encryption disk show-status`, ob der Vorgang erfolgreich war, bevor Sie mit dem nächsten Schritt fortfahren.
	e. Bereinigte Festplatte aufheben:
	`storage disk unfail -spare true -disk disk_id`
	f. Überprüfen Sie, ob die Festplatte einen Besitzer hat:
	`storage disk show -disk disk_id` + Wenn die Platte keinen Besitzer hat, weisen Sie einen zu.
	`storage disk assign -owner node -disk disk_id`
	i. Geben Sie den Knotenpunkt für den Knoten ein, der die Festplatten besitzt, die Sie desinfizieren möchten:
	`system node run -node node_name`
	Führen Sie den `disk sanitize release` Befehl aus.
	g. Verlassen Sie die Nodeshell. Fehler der Festplatte erneut aufheben:
	`storage disk unfail -spare true -disk disk_id`
	h. Überprüfen Sie, ob die Festplatte jetzt als Ersatzlaufwerk verwendet und in einem Aggregat wiederverwendet werden kann:
	`storage disk show -disk disk_id`

Im FIPS-Compliance-Modus ist der FIPS-Schlüssel nicht verfügbar, und SEDs haben eine PSID auf dem Etikett	a. Beziehen Sie die PSID des Datenträgers von der Datenträgerbezeichnung. b. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced` c. Setzen Sie die Festplatte auf die werkseitig konfigurierten Einstellungen zurück: `storage encryption disk revert-to-original-state -disk` *`disk_id`* `-psid` *`disk_physical_secure_id`* Überprüfen Sie `storage encryption disk show-status`, ob der Vorgang mit dem Befehl erfolgreich war, bevor Sie mit dem nächsten Schritt fortfahren. d. Wenn Sie ONTAP 9.8P5 oder eine frühere Version verwenden, fahren Sie mit dem nächsten Schritt fort. Wenn Sie ONTAP 9.8P6 oder höher ausführen, nehmen Sie den Fehler auf der bereinigten Festplatte zurück. `storage disk unfail -disk` *`disk_id`* e. Überprüfen Sie, ob die Festplatte einen Besitzer hat: `storage disk show -disk` *`disk_id`* + Wenn die Platte keinen Besitzer hat, weisen Sie einen zu. `storage disk assign -owner node -disk` *`disk_id`* i. Geben Sie den Knotenpunkt für den Knoten ein, der die Festplatten besitzt, die Sie desinfizieren möchten: `system node run -node` *`node_name`* Führen Sie den `disk sanitize release` Befehl aus. f. Verlassen Sie die Nodeshell.. Fehler der Festplatte erneut aufheben: `storage disk unfail -spare true -disk` *`disk_id`* g. Überprüfen Sie, ob die Festplatte jetzt als Ersatzlaufwerk verwendet und in einem Aggregat wiederverwendet werden kann: `storage disk show -disk` *`disk_id`*

Verwandte Informationen

- "Speicherverschlüsselung Datenträger ändern"
- "Speicherverschlüsselung Datenträger in den ursprünglichen Zustand zurücksetzen"
- "Speicherverschlüsselung Datenträgerbereinigung"
- "Speicherverschlüsselung Datenträger Status anzeigen"

Setzen Sie ein FIPS-Laufwerk oder SED in ONTAP in den ungeschützten Modus zurück

Ein FIPS-Laufwerk oder SED ist nur dann vor unberechtigtem Zugriff geschützt, wenn die Authentifizierungsschlüssel-ID für den Knoten auf einen anderen Wert als den Standardwert gesetzt ist. Sie können ein FIPS-Laufwerk oder eine SED in den ungeschützten Modus zurücksetzen `storage encryption disk modify`, indem Sie mit dem Befehl die Schlüssel-ID auf den Standardwert setzen. Ein FIPS-Laufwerk oder

eine SED im ungeschützten Modus verwendet die standardmäßigen Verschlüsselungsschlüssel, während ein FIPS-Laufwerk oder eine SED im geschützten Modus die angegebenen geheimen Verschlüsselungsschlüssel verwendet. Wenn auf dem Laufwerk verschlüsselte Daten gespeichert sind und das Laufwerk in den ungeschützten Modus zurückgesetzt wird, werden die Daten weiterhin verschlüsselt und nicht offengelegt.

> Befolgen Sie dieses Verfahren, um sicherzustellen, dass auf alle verschlüsselten Daten nicht mehr zugegriffen werden kann, nachdem das FIPS-Laufwerk oder die SED wieder in den ungeschützten Modus versetzt wurde. Sobald die FIPS- und Datenschlüssel-IDs zurückgesetzt wurden, können vorhandene Daten nicht mehr entschlüsselt werden und sind nicht mehr zugänglich, es sei denn, die ursprünglichen Schlüssel werden wiederhergestellt.

Wenn ein HA-Paar SAS- oder NVMe-Laufwerke (SED, NSE, FIPS) verwendet, müssen Sie diesen Prozess für alle Laufwerke innerhalb des HA-Paars befolgen, bevor das System initialisiert wird (Boot-Optionen 4 oder 9). Andernfalls kann es zu künftigen Datenverlusten kommen, wenn die Laufwerke einer anderen Verwendung zugewiesen werden.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Wenn ein FIPS-Laufwerk im FIPS-Compliance-Modus ausgeführt wird, legen Sie die FIPS-Authentifizierungsschlüssel-ID für den Node wieder auf den Standard MSID 0x0:

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

   Sie können den `security key-manager query` Befehl verwenden, um Schlüssel-IDs anzuzeigen.

   ```
   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.
   ```

   Bestätigen Sie den Vorgang mit dem Befehl:

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

   Wiederholen Sie den Befehl „show-status“, bis die Zahlen in „Disks Begun“ und „Disks Done“ gleich 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. Legen Sie die Daten-Authentifizierungsschlüssel-ID für den Knoten wieder auf die Standard-MSID 0x0:

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

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

   Sie können den `security key-manager query` Befehl verwenden, um Schlüssel-IDs anzuzeigen.

```
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.
```

   Bestätigen Sie den Vorgang mit dem Befehl:

   `storage encryption disk show-status`

   Wiederholen Sie den Befehl „show-status“, bis die Zahlen gleich sind. Der Vorgang ist abgeschlossen, wenn die Zahlen in „Disks started“ und „Disks done“ gleich sind.

Wartungsmodus

Ab ONTAP 9.7 können Sie eine FIPS-Festplatte aus dem Wartungsmodus neu Schlüssel aktivieren. Sie sollten den Wartungsmodus nur verwenden, wenn Sie die ONTAP-CLI-Anweisungen im vorherigen Abschnitt nicht verwenden können.

Schritte

1. Legen Sie die FIPS-Authentifizierungsschlüssel-ID für den Knoten wieder auf die Standard-MSID 0x0:

   `disk encrypt rekey_fips 0x0 disklist`

2. Legen Sie die Daten-Authentifizierungsschlüssel-ID für den Knoten wieder auf die Standard-MSID 0x0:

```
disk encrypt rekey 0x0 disklist
```

3. Bestätigen Sie, dass der FIPS-Authentifizierungsschlüssel erfolgreich umcodiert wurde:

   ```
   disk encrypt show_fips
   ```

4. Bestätigung der erfolgreichen Verschlüsselung des Datenauthentifizierungsschlüssels mit:

   ```
   disk encrypt show
   ```

   In Ihrer Ausgabe wird wahrscheinlich entweder die Standard-MSID 0x0-Schlüssel-ID oder der 64-stellige Wert des Schlüsselservers angezeigt. Das `Locked?` Feld bezieht sich auf die Datensperrung.

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

Verwandte Informationen

- "Speicherverschlüsselung Datenträger ändern"
- "Speicherverschlüsselung Datenträger Status anzeigen"

Entfernen Sie eine externe Schlüsselmanager-Verbindung in ONTAP

Sie können einen KMIP-Server von einem Node trennen, wenn Sie den Server nicht mehr benötigen. Beispielsweise können Sie einen KMIP-Server trennen, wenn Sie die Volume-Verschlüsselung umstellen.

Über diese Aufgabe

Wenn Sie einen KMIP Server von einem Node in einem HA-Paar trennen, trennt das System die Verbindung zwischen dem Server automatisch und allen Cluster-Nodes.

> Wenn Sie nach der Trennung eines KMIP Servers weiterhin externes Verschlüsselungsmanagement nutzen möchten, stellen Sie sicher, dass ein anderer KMIP Server für die Authentifizierung von Schlüsseln zur Verfügung steht.

Bevor Sie beginnen

Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

Schritt

1. Trennen eines KMIP-Servers vom aktuellen Node:

Für diese ONTAP-Version…	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 frühere Versionen

In einer MetroCluster Umgebung müssen Sie die folgenden Befehle für beide Cluster für die Administrator-SVM wiederholen.

Der folgende ONTAP 9.6-Befehl deaktiviert die Verbindungen zu zwei externen Schlüsselverwaltungs-Servern für `cluster1`, den ersten genannten `ks1`, der auf dem Standardport 5696, den zweiten 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
```

Erfahren Sie mehr über `security key-manager external remove-servers` und `security key-manager delete` in der "ONTAP-Befehlsreferenz".

Ändern der Eigenschaften des externen ONTAP Schlüsselverwaltungsservers

Ab ONTAP 9.6 können Sie mit dem `security key-manager external modify-server` Befehl das I/O-Timeout und den Benutzernamen eines externen Schlüsselverwaltungs-Servers ändern.

Bevor Sie beginnen

- Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.
- In einer MetroCluster Umgebung müssen Sie die folgenden Schritte auf beiden Clustern für den Administrator-SVM wiederholen.

Schritte

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

   ```
   set -privilege advanced
   ```

2. Ändern der Eigenschaften eines externen Schlüsselmanagers-Servers für das Cluster:

   ```
   security key-manager external modify-server -vserver admin_SVM -key-server
   host_name|IP_address:port,… -timeout 1…60 -username user_name
   ```

   Der Timeout-Wert wird in Sekunden angegeben. Wenn Sie den Benutzernamen ändern, werden Sie aufgefordert, ein neues Passwort einzugeben. Wenn Sie den Befehl an der Anmeldeaufforderung für das Cluster ausführen, *`admin_SVM`* wird standardmäßig die Administrator-SVM des aktuellen Clusters verwendet. Sie müssen der Cluster-Administrator sein, um die Eigenschaften eines externen Schlüsselmanager-Servers zu ändern.

Mit dem folgenden Befehl wird der Timeout-Wert für den `cluster1` externen Schlüsselverwaltungsserver, der auf dem Standardport 5696 lauscht, auf 45 Sekunden geändert:

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

3. Ändern Sie die Server-Eigenschaften von externen Verschlüsselungsmanagement für eine SVM (nur NVE):

   `security key-manager external modify-server -vserver SVM -key-server host_name|IP_address:port,… -timeout 1…60 -username user_name`

   > Der Timeout-Wert wird in Sekunden angegeben. Wenn Sie den Benutzernamen ändern, werden Sie aufgefordert, ein neues Passwort einzugeben. Wenn Sie den Befehl an der Anmeldeaufforderung der SVM ausführen, *SVM* wird standardmäßig die aktuelle SVM verwendet. Zum Ändern der Eigenschaften des externen Schlüsselmanager-Servers müssen Sie der Cluster oder der SVM-Administrator sein.

   Mit dem folgenden Befehl ändern Sie den Benutzernamen und das Kennwort 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. Wiederholen Sie den letzten Schritt für alle weiteren SVMs.

Verwandte Informationen

- "Sicherheitsschlüssel-Manager, externer Änderungsserver"

Wechseln Sie zum externen Verschlüsselungsmanagement vom integrierten Verschlüsselungsmanagement in ONTAP

Wenn Sie von Onboard-Verschlüsselungsmanagement auf externes Verschlüsselungsmanagement wechseln möchten, müssen Sie die integrierte Verschlüsselungsmanagementkonfiguration löschen, bevor Sie externes Verschlüsselungsmanagement aktivieren können.

Bevor Sie beginnen

- Bei der hardwarebasierten Verschlüsselung müssen die Datenschlüssel aller FIPS-Laufwerke oder SEDs auf den Standardwert zurückgesetzt werden.

  "Ein FIPS-Laufwerk oder eine SED-Festplatte in den ungeschützten Modus zurückkehren"

- Bei softwarebasierter Verschlüsselung müssen Sie alle Volumes entschlüsseln.

  "Verschlüsselung von Volume-Daten aufheben"

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritt

1. Löschen der integrierten Verschlüsselungsmanagementkonfiguration für ein Cluster:

Für diese ONTAP-Version…	Befehl
ONTAP 9.6 und höher	`security key-manager onboard disable -vserver SVM`
ONTAP 9.5 und frühere Versionen	`security key-manager delete-key-database`

Erfahren Sie mehr über `security key-manager onboard disable` und `security key-manager delete-key-database` in der "ONTAP-Befehlsreferenz".

Wechseln Sie von der externen Schlüsselverwaltung zur integrierten ONTAP -Schlüsselverwaltung

Um zur integrierten Schlüsselverwaltung zu wechseln, löschen Sie die externe Schlüsselverwaltungskonfiguration, bevor Sie die integrierte Schlüsselverwaltung aktivieren.

Bevor Sie beginnen

- Bei der hardwarebasierten Verschlüsselung müssen die Datenschlüssel aller FIPS-Laufwerke oder SEDs auf den Standardwert zurückgesetzt werden.

  "Ein FIPS-Laufwerk oder eine SED-Festplatte in den ungeschützten Modus zurückkehren"

- Sie müssen alle externen Schlüsselmanager-Verbindungen gelöscht haben.

  "Löschen einer externen Schlüsselmanager-Verbindung"

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritte

Die Schritte zur Umstellung Ihres Schlüsselmanagements hängen von der verwendeten Version von ONTAP ab.

ONTAP 9.6 und höher

1. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Verwenden Sie den Befehl:

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

   In einer MetroCluster-Umgebung müssen Sie den Befehl für die Administrator-SVM auf beiden Clustern wiederholen.

Erfahren Sie mehr über `security key-manager external disable` im"ONTAP-Befehlsreferenz" .

ONTAP 9.5 und frühere Versionen

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

Erfahren Sie mehr über `security key-manager delete-kmip-config` im"ONTAP-Befehlsreferenz" .

Verwandte Informationen

- "Sicherheitsschlüssel-Manager extern deaktivieren"

Was passiert, wenn Schlüsselverwaltungsserver während des ONTAP Bootvorgangs nicht erreichbar sind?

ONTAP ergreift Maßnahmen, um unerwünschte Verhaltensweisen zu vermeiden, wenn ein mit NSE konfiguriertes Storage-System während des Bootens keinen der angegebenen Verschlüsselungsmanagementserver erreichen kann.

Wenn das Storage-System für NSE konfiguriert ist, werden die SEDs rekeyed und gesperrt und die SEDs eingeschaltet. Das Storage-System muss die erforderlichen Authentifizierungsschlüssel von den Verschlüsselungsmanagement-Servern abrufen, um sich bei SEDs zu authentifizieren, bevor es auf die Daten zugreifen kann.

Das Storage-System versucht, bis zu drei Stunden lang die angegebenen Schlüsselmanagementserver zu kontaktieren. Sollte das Storage-System zu diesem Zeitpunkt keinen Zugang haben, wird der Bootvorgang abgebrochen und das Storage-System stoppt.

Wenn das Speichersystem einen bestimmten Schlüsselverwaltungsserver erfolgreich kontaktiert, versucht es dann, eine SSL-Verbindung für bis zu 15 Minuten herzustellen. Wenn das Storage-System keine SSL-Verbindung zu einem angegebenen Schlüsselmanagementserver herstellen kann, wird der Bootvorgang angehalten und das Speichersystem wird angehalten.

Während das Speichersystem versucht, sich mit wichtigen Managementservern zu verbinden und eine Verbindung herzustellen, werden in der CLI detaillierte Informationen über fehlgeschlagene Kontaktversuche angezeigt. Sie können die Kontaktversuche jederzeit unterbrechen, indem Sie Strg-C drücken

Als Sicherheitsmaßnahme erlauben SEDs nur eine begrenzte Anzahl von unbefugten Zugriffsversuchen, wonach sie den Zugriff auf die vorhandenen Daten deaktivieren. Wenn das Speichersystem keine bestimmten Schlüsselverwaltungsserver kontaktieren kann, um die richtigen Authentifizierungsschlüssel zu erhalten, kann es nur versuchen, sich mit dem Standardschlüssel zu authentifizieren, der zu einem fehlgeschlagenen Versuch und einem Panikzustand führt. Wenn das Storage-System so konfiguriert ist, dass es im Falle eines Panikzustands automatisch neu gestartet wird, wird eine Boot-Schleife erzeugt, die zu kontinuierlichen fehlgeschlagenen Authentifizierungsversuchen von SEDs führt.

Das Anhalten des Storage-Systems in diesen Szenarien ist durch das Design zu verhindern, dass das Storage-System in einen Boot-Loop und möglichen unbeabsichtigten Datenverlust durch die dauerhaft gesperrten SEDs gelangt, da es die Sicherheitsgrenze einer bestimmten Anzahl aufeinander folgender fehlgeschlagener Authentifizierungsversuche überschreitet. Der Grenzwert und die Art des Sperrschutzes hängen von den Herstellungsspezifikationen und dem Typ der SED ab:

SED-Typ	Anzahl aufeinanderfolgender fehlgeschlagener Authentifizierungsversuche, die zu einer Sperrung führen	Sicherungstyp sperren, wenn die Sicherheitsgrenze erreicht ist
HDD	1024	Dauerhaft: Daten können nicht wiederhergestellt werden, selbst wenn der richtige Authentifizierungsschlüssel wieder verfügbar ist.
X440_PHM2800MCTO 800 GB NSE SSDs mit Firmware-Versionen NA00 oder NA01	5	Temporär. Die Sperrung wird nur wirksam, bis die Festplatte aus- und wieder eingeschaltet wird.
X577_PHM2800MCTO 800 GB NSE SSDs mit Firmware-Versionen NA00 oder NA01	5	Temporär. Die Sperrung wird nur wirksam, bis die Festplatte aus- und wieder eingeschaltet wird.
X440_PHM2800MCTO 800 GB NSE SSDs mit höherer Firmware-Version	1024	Dauerhaft: Daten können nicht wiederhergestellt werden, selbst wenn der richtige Authentifizierungsschlüssel wieder verfügbar ist.
X577_PHM2800MCTO 800 GB NSE SSDs mit höherer Firmware-Version	1024	Dauerhaft: Daten können nicht wiederhergestellt werden, selbst wenn der richtige Authentifizierungsschlüssel wieder verfügbar ist.
Alle anderen SSD-Modelle	1024	Dauerhaft: Daten können nicht wiederhergestellt werden, selbst wenn der richtige Authentifizierungsschlüssel wieder verfügbar ist.

Bei allen SED-Typen wird durch eine erfolgreiche Authentifizierung die Anzahl der Versuche auf Null zurückgesetzt.

Wenn dieses Szenario auftritt, bei dem das Speichersystem aufgrund eines Fehlers angehalten wird, um irgendwelche angegebenen Schlüsselverwaltungsserver zu erreichen, müssen Sie zuerst die Ursache für den Kommunikationsfehler identifizieren und korrigieren, bevor Sie versuchen, das Speichersystem weiterhin zu booten.

Deaktivieren Sie die ONTAP Verschlüsselung standardmäßig

Ab ONTAP 9.7 ist die Aggregat- und Volume-Verschlüsselung standardmäßig aktiviert, wenn Sie über eine VE-Lizenz (Volume Encryption) verfügen und einen integrierten oder externen Schlüsselmanager verwenden. Bei Bedarf können Sie die Verschlüsselung standardmäßig für den gesamten Cluster deaktivieren.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe durchzuführen, oder ein SVM-Administrator, an den der Cluster-Administrator die Berechtigungen delegiert hat.

Schritt

1. Führen Sie den folgenden Befehl aus, um die Verschlüsselung für das gesamte Cluster in ONTAP 9.7 oder höher standardmäßig zu deaktivieren:

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