Integriertes Verschlüsselungsmanagement

ONTAP 9

NetApp
February 12, 2026

Inhalt

Integriertes Verschlüsselungsmanagement

Ermöglichen Sie integriertes Verschlüsselungsmanagement in ONTAP 9.6 und höher

Mit dem Onboard Key Manager können Clusterknoten auf einem FIPS-Laufwerk oder SED authentifiziert werden. Der integrierte Onboard Key Manager ist ein Tool, das Authentifizierungsschlüssel für Nodes aus demselben Storage-System wie Ihre Daten bereitstellt. Der Onboard Key Manager ist nach FIPS-140-2 Level 1 zertifiziert.

Mit dem integrierten Key Manager werden die Schlüssel gesichert, die das Cluster für den Zugriff auf verschlüsselte Daten verwendet. Sie müssen Onboard Key Manager für jedes Cluster aktivieren, das auf ein verschlüsseltes Volume oder eine selbstverschlüsselnde Festplatte zugreift.

Über diese Aufgabe

Sie müssen den `security key-manager onboard enable` Befehl jedes Mal ausführen, wenn Sie dem Cluster einen Node hinzufügen. In MetroCluster-Konfigurationen müssen Sie `security key-manager onboard enable` zuerst auf dem lokalen Cluster ausführen und dann `security key-manager onboard sync` auf dem Remote-Cluster unter Verwendung derselben Passphrase auf beiden ausführen.

Erfahren Sie mehr über `security key-manager onboard enable` Und `security key-manager onboard sync` im"ONTAP-Befehlsreferenz" .

Standardmäßig müssen Sie beim Neustart eines Node nicht die Passphrase für das Schlüsselmanagement eingeben. Mit Ausnahme von MetroCluster können Sie die `cc-mode-enabled=yes` Option verwenden, um zu verlangen, dass Benutzer die Passphrase nach einem Neustart eingeben.

Wenn der Onboard Key Manager im Common Criteria-Modus aktiviert ist(`cc-mode-enabled=yes`, wird das Systemverhalten wie folgt geändert:

- Das System überwacht bei der Verwendung im Common Criteria-Modus auf aufeinanderfolgende fehlgeschlagene Cluster-Passphrase.

  Wenn NetApp Storage Encryption (NSE) aktiviert ist und Sie beim Booten nicht die richtige Cluster-Passphrase eingeben, kann sich das System nicht auf seinen Laufwerken authentifizieren und automatisch neu starten. Um dies zu korrigieren, müssen Sie an der Boot-Eingabeaufforderung die richtige Cluster-Passphrase eingeben. Sobald das System gebootet wurde, können bis zu 5 aufeinanderfolgende Versuche unternommen werden, um für jeden Befehl, für den die Cluster-Passphrase als Parameter erforderlich ist, in einem Zeitraum von 24 Stunden korrekt einzugeben. Wenn das Limit erreicht wird (beispielsweise konnten Sie den Cluster-Passphrase 5 Mal hintereinander nicht korrekt eingeben), müssen Sie entweder warten, bis der 24-Stunden-Timeout abgelaufen ist, oder Sie müssen den Node neu booten, um das Limit zurückzusetzen.

- Updates für das System-Image nutzen das Code-Signing-Zertifikat von NetApp RSA-3072 zusammen mit dem von SHA-384 signierten Code, um die Image-Integrität anstelle des üblichen NetApp RSA-2048-Code-Signaturzertifikats und den von SHA-256 signierten Digests zu überprüfen.

  Der Upgrade-Befehl überprüft durch die Überprüfung verschiedener digitaler Signaturen, ob der Bildinhalt verändert oder beschädigt wurde. Wenn die Validierung funktioniert, geht die Bildaktualisierung zum nächsten Schritt über. Wenn die Validierung nicht funktioniert, schlägt die Bildaktualisierung fehl. Erfahren Sie mehr über `cluster image` im"ONTAP-Befehlsreferenz" .

Der Onboard Key Manager speichert Schlüssel im volatilen Speicher. Der Inhalt von flüchtigem Speicher wird gelöscht, wenn das System neu gestartet oder angehalten wird. Unter normalen Betriebsbedingungen wird der Inhalt von flüchtigem Speicher innerhalb von 30 s gelöscht, wenn ein System angehalten wird.

Bevor Sie beginnen

- Wenn Sie NSE mit einem externen KMIP-Server (Key Management) verwenden, müssen Sie die externe Schlüsselmanager-Datenbank gelöscht haben.

  "Umstellung auf integriertes Verschlüsselungsmanagement von externem Verschlüsselungsmanagement"

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Sie müssen die MetroCluster-Umgebung konfigurieren, bevor Sie den Onboard Key Manager konfigurieren.

Schritte

1. Starten Sie den Key Manager Setup-Befehl:

   ```
   security key-manager onboard enable -cc-mode-enabled yes|no
   ```

Legen Sie fest `cc-mode-enabled=yes`, dass Benutzer nach einem Neustart die Passphrase für den Schlüsselmanager eingeben müssen. Die `- cc-mode-enabled` Option wird in MetroCluster-Konfigurationen nicht unterstützt. Der `security key-manager onboard enable` Befehl ersetzt den `security key-manager setup` Befehl.

Das folgende Beispiel startet den Befehl zum Einrichten des Schlüsselmanagers in cluster1, ohne dass nach jedem Neustart die Passphrase eingegeben werden muss:

2. 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.

3. Geben Sie die Passphrase erneut an der Eingabeaufforderung zur Bestätigung der Passphrase ein.
4. Überprüfen Sie, ob das System die Authentifizierungsschlüssel erstellt:

```
security key-manager key query -node node
```

Der `security key-manager key query` Befehl ersetzt den `security key-manager query key` Befehl.

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

Nachdem Sie fertig sind

Kopieren Sie die Passphrase zur späteren Verwendung an einen sicheren Ort außerhalb des Storage-Systems.

Das System sichert wichtige Verwaltungsinformationen automatisch in der replizierten Datenbank (RDB) für den Cluster. Sie sollten diese Informationen für die Notfallwiederherstellung auch manuell sichern.

Verwandte Informationen

- "Cluster-Image-Befehle"
- "Sicherheitsschlüsselmanager extern aktivieren"
- "Sicherheitsschlüssel-Manager-Schlüsselabfrage"
- "Sicherheitsschlüssel-Manager Onboard aktivieren"
- "Umstellung auf integriertes Verschlüsselungsmanagement von externem Verschlüsselungsmanagement"

Ermöglichen Sie integriertes Verschlüsselungsmanagement in ONTAP 9.5 und früher

Mit dem Onboard Key Manager können Clusterknoten auf einem FIPS-Laufwerk oder SED authentifiziert werden. Der integrierte Onboard Key Manager ist ein Tool, das Authentifizierungsschlüssel für Nodes aus demselben Storage-System wie Ihre Daten bereitstellt. Der Onboard Key Manager ist nach FIPS-140-2 Level 1 zertifiziert.

Mit dem Onboard Key Manager können Sie die Schlüssel sichern, die der Cluster für den Zugriff auf verschlüsselte Daten verwendet. Aktivieren Sie den Onboard Key Manager auf jedem Cluster, der auf verschlüsselte Volumes oder selbstverschlüsselnde Datenträger zugreift.

Über diese Aufgabe

Sie müssen den `security key-manager setup` Befehl jedes Mal ausführen, wenn Sie dem Cluster einen Node hinzufügen.

Wenn Sie über eine MetroCluster-Konfiguration verfügen, überprüfen Sie diese Richtlinien:

- In ONTAP 9.5 müssen Sie `security key-manager setup` auf dem lokalen Cluster und `security key-manager setup -sync-metrocluster-config yes` auf dem Remote-Cluster unter Verwendung derselben Passphrase ausgeführt werden.
- Vor ONTAP 9.5 müssen Sie `security key-manager setup` auf dem lokalen Cluster ausführen, etwa 20 Sekunden warten und dann `security key-manager setup` auf dem Remote-Cluster unter Verwendung derselben Passphrase auf jedem Cluster ausführen.

Standardmäßig müssen Sie beim Neustart eines Node nicht die Passphrase für das Schlüsselmanagement eingeben. Ab ONTAP 9.4 können Sie mit der `-enable-cc-mode yes` Option festlegen, dass Benutzer die Passphrase nach einem Neustart eingeben müssen.

Wenn Sie für NVE festlegen, `-enable-cc-mode yes` `volume create` `volume move start` werden Volumes, die Sie mit den Befehlen und erstellen, automatisch verschlüsselt. Für `volume create` müssen Sie nicht angeben `-encrypt true`. Für `volume move start` müssen Sie nicht angeben `-encrypt -destination true`.

Nach einem fehlgeschlagenen Passphrase-Versuch müssen Sie den Node erneut neu booten.

Bevor Sie beginnen

- Wenn Sie NSE mit einem externen Schlüsselverwaltungsserver (KMIP) verwenden, löschen Sie die externe Schlüsselverwaltungsdatenbank.

  "Umstellung auf integriertes Verschlüsselungsmanagement von externem Verschlüsselungsmanagement"

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Konfigurieren Sie die MetroCluster -Umgebung, bevor Sie den Onboard Key Manager konfigurieren.

Schritte

1. Starten Sie die Konfiguration des Schlüsselmanagers:

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   Ab ONTAP 9.4 können Sie mit der `-enable-cc-mode yes` Option festlegen, dass Benutzer nach einem Neustart die Passphrase für den Schlüsselmanager eingeben müssen. Wenn Sie für NVE festlegen, `-enable-cc-mode yes` `volume create` `volume move start` werden Volumes, die Sie mit den Befehlen und erstellen, automatisch verschlüsselt.

   Das folgende Beispiel beginnt mit dem Einrichten des Schlüsselmanagers auf Clustered 1, ohne dass die Passphrase nach jedem Neustart eingegeben werden muss:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

...

Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. Geben Sie `yes` an der Eingabeaufforderung ein, um die integrierte Schlüsselverwaltung zu konfigurieren.
3. Geben Sie an der Eingabeaufforderung für die Passphrase 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. Vergewissern Sie sich, dass die Schlüssel für alle Nodes konfiguriert sind:

   `security key-manager show-key-store`

   Erfahren Sie mehr über `security key-manager show-key-store` im"ONTAP-Befehlsreferenz" .

```
cluster1::> security key-manager show-key-store

Node: node1
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK

Node: node2
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK
```

Nachdem Sie fertig sind

ONTAP sichert wichtige Verwaltungsinformationen automatisch in der replizierten Datenbank (RDB) für den Cluster.

Nachdem Sie die Passphrase für den Onboard Key Manager konfiguriert haben, sichern Sie die Informationen manuell an einem sicheren Ort außerhalb des Speichersystems. Sehen"Manuelles Backup der integrierten Informationen für das Verschlüsselungsmanagement" .

Verwandte Informationen

- "Manuelles Backup der integrierten Informationen für das Verschlüsselungsmanagement"
- "Einrichtung des Sicherheitsschlüssel-Managers"
- "Sicherheitsschlüssel-Manager Show-Key-Store"
- "Umstellung auf integriertes Verschlüsselungsmanagement von externem Verschlüsselungsmanagement"

Weisen Sie einem FIPS-Laufwerk oder SED mit der integrierten Schlüsselverwaltung von ONTAP einen Datenauthentifizierungsschlüssel zu

Mit dem `storage encryption disk modify` Befehl können Sie einem FIPS-Laufwerk oder einer SED einen Datenauthentifizierungsschlüssel zuweisen. Cluster-Nodes verwenden diesen Schlüssel für den Zugriff auf die Daten auf dem Laufwerk.

Über diese Aufgabe

Ein selbstverschlüsselndes Laufwerk ist nur dann vor unberechtigtem Zugriff geschützt, wenn seine Authentifizierungsschlüssel-ID auf einen nicht standardmäßigen Wert eingestellt ist. Der Hersteller Secure ID (MSID), der die Schlüssel-ID 0x0 hat, ist der Standardvorgabewert für SAS-Laufwerke. Bei NVMe-Laufwerken ist der Standardwert ein Null-Schlüssel, der als leere Schlüssel-ID dargestellt wird. Wenn Sie einem selbstverschlüsselnden Laufwerk die Schlüssel-ID zuweisen, ändert das System seine Authentifizierungsschlüssel-ID in einen nicht standardmäßigen Wert.

Bevor Sie beginnen

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

Schritte

1. Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder einer SED:

   `storage encryption disk modify -disk` *`disk_ID`* `-data-key-id` *`key_ID`*

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

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

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
<id_value>

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

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

2. Vergewissern Sie sich, dass die Authentifizierungsschlüssel zugewiesen wurden:

   `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>
[...]
```

Verwandte Informationen

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