Konfigurieren Sie die hardwarebasierte NetApp Verschlüsselung

ONTAP 9

NetApp
February 12, 2026

Inhalt

Konfigurieren Sie die hardwarebasierte NetApp Verschlüsselung

Erfahren Sie mehr über die hardwarebasierte Verschlüsselung von ONTAP

Die hardwarebasierte Verschlüsselung von NetApp unterstützt die vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) von Daten beim Schreiben. Ohne einen auf der Firmware gespeicherten Verschlüsselungsschlüssel können die Daten nicht gelesen werden. Der Verschlüsselungsschlüssel wiederum ist nur für einen authentifizierten Knoten zugänglich.

Allgemeines zur hardwarebasierten Verschlüsselung von NetApp

Ein Node authentifiziert sich selbst auf einem Self-Encrypting Drive, wobei ein Authentifizierungsschlüssel von einem externen Verschlüsselungsmanagement-Server oder Onboard Key Manager abgerufen wird:

- Der externe Verschlüsselungsmanagement-Server ist ein Drittanbietersystem in der Storage-Umgebung, das mithilfe des Key Management Interoperability Protocol (KMIP) Schlüssel zu Nodes bereitstellt. Als Best Practice wird empfohlen, externe Verschlüsselungsmanagementserver auf einem anderen Storage-System zu Ihren Daten zu konfigurieren.
- Der integrierte Onboard Key Manager ist ein Tool, das Authentifizierungsschlüssel für Nodes aus demselben Storage-System wie Ihre Daten bereitstellt.

Mit NetApp Volume Encryption mit hardwarebasierter Verschlüsselung können Daten auf Self-Encrypting Drives `double Encryption` verschlüsselt werden.

Bei Aktivierung von Self-Encrypting Drives wird der Core Dump ebenfalls verschlüsselt.

> Wenn ein HA-Paar SAS- oder NVMe-Laufwerke (SED, NSE, FIPS) verschlüsselt, müssen Sie Ein FIPS-Laufwerk oder eine SED-Festplatte in den ungeschützten Modus zurückkehrenvor der Initialisierung des Systems die Anweisungen im Thema für alle Laufwerke innerhalb des HA-Paars befolgen (Boot-Optionen 4 oder 9). Andernfalls kann es zu künftigen Datenverlusten kommen, wenn die Laufwerke einer anderen Verwendung zugewiesen werden.

Unterstützte Self-Encrypting Drives

Es werden zwei Arten von Self-Encrypting Drives unterstützt:

- FIPS-zertifizierte Self-Encrypting-SAS- oder NVMe-Laufwerke werden auf allen FAS und AFF Systemen unterstützt. Diese Laufwerke, so genannte *FIPS-Laufwerke*, entsprechen den Anforderungen der Federal Information Processing Standard Publication 140-2, Level 2. Die zertifizierten Funktionen ermöglichen neben der Verschlüsselung auch Schutz, beispielsweise die Verhinderung von Denial-of-Service-Angriffen auf dem Laufwerk. FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden.
- Ab ONTAP 9.6 werden Self-Encrypting-NVMe-Laufwerke, die noch keine FIPS-Tests durchlaufen haben, auf AFF A800, A320 und neueren Systemen unterstützt. Diese Laufwerke, sogenannte *SEDs*, bieten dieselben Verschlüsselungsfunktionen wie FIPS-Laufwerke, können aber ohne Verschlüsselung von Laufwerken auf demselben Node oder HA-Paar kombiniert werden.

- Alle FIPS-validierten Laufwerke verwenden ein kryptografisches Firmware-Modul, das durch die FIPS-Validierung erfolgt. Das FIPS-Laufwerk-kryptografische Modul verwendet keine Schlüssel, die außerhalb des Laufwerks generiert werden (die Authentifizierungs-Passphrase, die an das Laufwerk eingegeben wird, wird vom Laufwerk-Firmware-kryptographic-Modul verwendet, um einen Schlüssel zu erhalten).

Laufwerke ohne Verschlüsselung sind Laufwerke, die keine SEDs oder FIPS-Laufwerke sind.

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.

Wann Sie externes Verschlüsselungsmanagement verwenden sollten

Obwohl es kostengünstiger und in der Regel bequemer ist, den Onboard-Schlüsselmanager zu verwenden, sollten Sie ein externes Verschlüsselungsmanagement nutzen, wenn eine der folgenden zutrifft:

- Die Richtlinie Ihres Unternehmens erfordert eine Verschlüsselungsmanagementlösung, die ein kryptografisches Modul nach FIPS 140-2 Level 2 (oder höher) verwendet.
- Sie benötigen eine Multi-Cluster-Lösung mit zentralem Management von Verschlüsselungen.
- Ihr Unternehmen erfordert die zusätzliche Sicherheit beim Speichern von Authentifizierungsschlüsseln auf einem System oder an einem anderen Speicherort als den Daten.

Support-Details

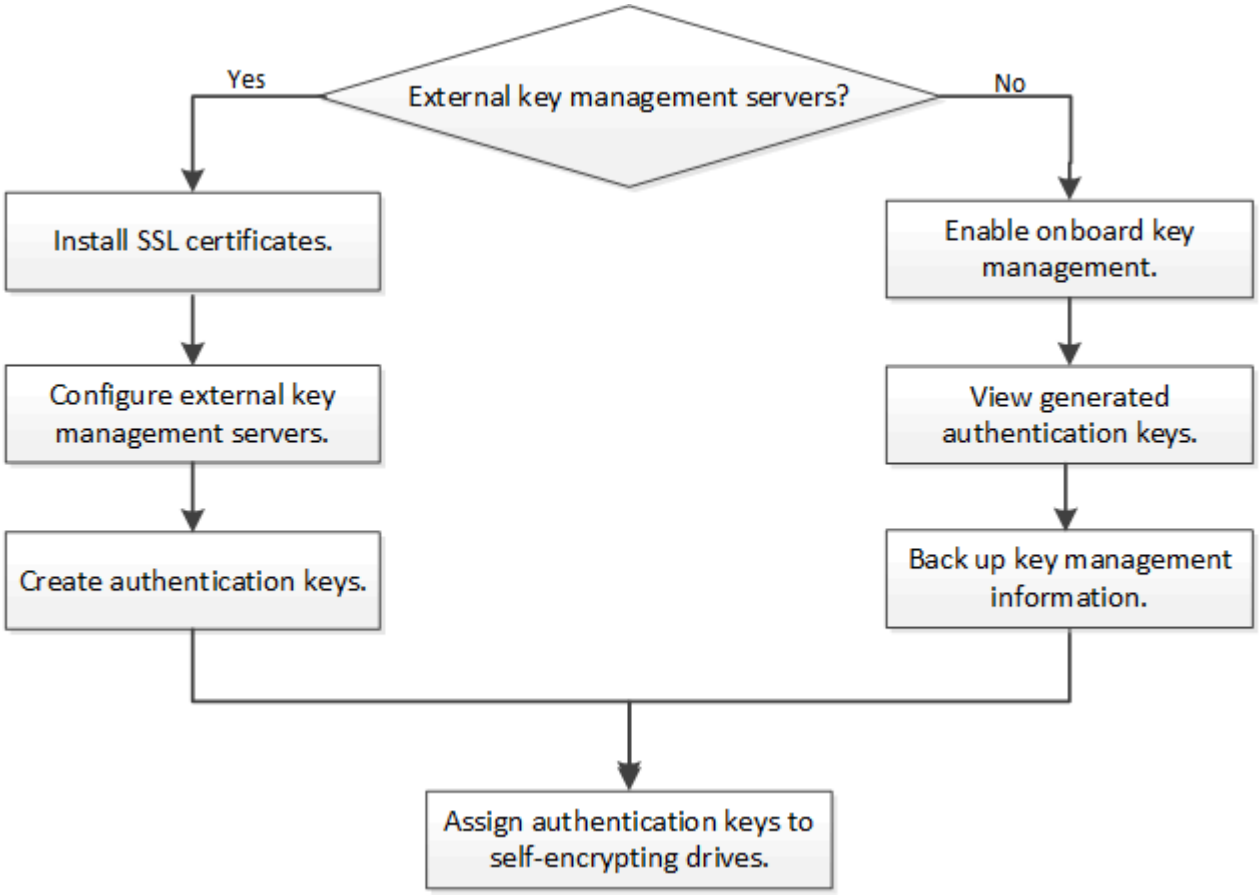
In der folgenden Tabelle sind wichtige Details zur Unterstützung der Hardwareverschlüsselung aufgeführt. In der Interoperabilitäts-Matrix finden Sie die neuesten Informationen zu unterstützten KMIP-Servern, Storage-Systemen und Festplatten-Shelfs.

Ressource oder Funktion	Support-Details
Nicht homogene Festplattengruppen	• FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden. Die Einhaltung der HA-Paare kann bei nicht übereinstimmenden HA-Paaren im selben Cluster vorhanden sein. • SEDs können mit Laufwerken ohne Verschlüsselung auf demselben Node oder HA-Paar kombiniert werden.
Laufwerkstyp	• FIPS-Laufwerke können SAS- oder NVMe-Laufwerke sein. • SEDs müssen NVMe-Laufwerke sein.
10-GB-Netzwerkschnittstellen	Ab ONTAP 9.3 unterstützen die KMIP-Verschlüsselungsmanagementkonfigurationen 10 GB-Netzwerkschnittstellen für die Kommunikation mit externen Verschlüsselungsmanagement-Servern.

Ports für die Kommunikation mit dem Schlüsselverwaltungsserver	Ab ONTAP 9.3 können Sie jeden beliebigen Storage Controller Port zur Kommunikation mit dem Schlüsselmanagement-Server verwenden. Andernfalls sollten Sie Port E0M für die Kommunikation mit Schlüsselmanagement-Servern verwenden. Je nach Storage-Controller-Modell sind während des Bootvorgangs möglicherweise bestimmte Netzwerkschnittstellen zur Kommunikation mit wichtigen Management-Servern nicht verfügbar.
MetroCluster (MCC)	• NVMe-Laufwerke unterstützen MCC. • SAS-Laufwerke unterstützen MCC nicht.

Hardwarebasierter Verschlüsselungs-Workflow

Sie müssen Verschlüsselungsmanagementdienste konfigurieren, bevor sich das Cluster auf dem Self-Encrypting Drive authentifizieren kann. Sie können einen externen Verschlüsselungsmanagementserver oder einen integrierten Schlüsselmanager verwenden.



Verwandte Informationen

- "NetApp Hardware Universe"
- "NetApp Volume Encryption und NetApp Aggregate Encryption"

Externes Verschlüsselungsmanagement konfigurieren

Erfahren Sie mehr über die Konfiguration der externen Schlüsselverwaltung von ONTAP

Sie können einen oder mehrere externe Verschlüsselungsmanagementserver verwenden, um die Schlüssel zu sichern, die das Cluster zum Zugriff auf verschlüsselte Daten verwendet. Ein externer Verschlüsselungsmanagement-Server ist ein Drittanbietersystem in Ihrer Storage-Umgebung, der mithilfe des Key Management Interoperability Protocol (KMIP) Schlüssel zu Nodes bereitstellt.

NetApp Volume Encryption (NVE) kann mit Onboard Key Manager implementiert werden. NVE kann in ONTAP 9.3 oder höher mit externem Verschlüsselungsmanagement (KMIP) und Onboard Key Manager implementiert werden. Ab ONTAP 9.11.1 können Sie mehrere externe Schlüsselmanager in einem Cluster konfigurieren. Siehe Konfigurieren Sie Cluster-Key-Server.

Installieren Sie SSL-Zertifikate auf dem ONTAP -Cluster

Das Cluster und der KMIP-Server verwenden KMIP SSL-Zertifikate, um die Identität des jeweils anderen zu überprüfen und eine SSL-Verbindung herzustellen. Vor dem Konfigurieren der SSL-Verbindung mit dem KMIP-Server müssen die KMIP-Client-SSL-Zertifikate für das Cluster und das öffentliche SSL-Zertifikat für die Root-Zertifizierungsstelle des KMIP-Servers installiert werden.

Über diese Aufgabe

In einem HA-Paar müssen beide Nodes dieselben öffentlichen und privaten KMIP-SSL-Zertifikate verwenden. Wenn Sie mehrere HA-Paare mit demselben KMIP-Server verbinden, müssen alle Nodes der HA-Paare dieselben öffentlichen und privaten KMIP-SSL-Zertifikate verwenden.

Bevor Sie beginnen

- Die Zeit muss auf dem Server synchronisiert werden, der die Zertifikate, den KMIP-Server und das Cluster erstellt.
- Sie müssen das öffentliche SSL KMIP-Client-Zertifikat für den Cluster erhalten haben.
- Sie müssen den privaten Schlüssel für das SSL KMIP Client-Zertifikat für das Cluster erhalten haben.
- Das SSL KMIP-Client-Zertifikat darf nicht durch ein Passwort geschützt sein.
- Sie müssen das öffentliche SSL-Zertifikat für die Root-Zertifizierungsstelle (CA) des KMIP-Servers erhalten haben.
- In einer MetroCluster-Umgebung müssen Sie auf beiden Clustern dieselben KMIP-SSL-Zertifikate installieren.

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

Schritte

1. Installieren Sie die SSL KMIP-Client-Zertifikate für das Cluster:

```
security certificate install -vserver admin_svm_name -type client
```

Sie werden aufgefordert, die öffentlichen und privaten SSL KMIP-Zertifikate einzugeben.

```
cluster1::> security certificate install -vserver cluster1 -type client
```

2. Installieren Sie das öffentliche SSL-Zertifikat für die Root-Zertifizierungsstelle (CA) des KMIP-Servers:

```
security certificate install -vserver admin_svm_name -type server-ca
```

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
```

Verwandte Informationen

- "Sicherheitszertifikat installieren"

Aktivieren Sie die externe Schlüsselverwaltung für die hardwarebasierte Verschlüsselung in ONTAP 9.6 und höher

Ein oder mehrere KMIP-Server dienen zur Sicherung der Schlüssel, die das Cluster für den Zugriff auf verschlüsselte Daten verwendet. Mit einem Node können bis zu vier KMIP-Server verbunden werden. Für Redundanz und Disaster Recovery werden mindestens zwei Server empfohlen.

Ab ONTAP 9.11.1 können Sie bis zu 3 sekundäre Schlüsselserver pro primären Schlüsselserver hinzufügen, um einen geclusterten Schlüsselserver zu erstellen. Weitere Informationen finden Sie unter Konfigurieren Sie externe geclusterte Schlüsselserver.

Bevor Sie beginnen

- Die KMIP SSL-Client- und Serverzertifikate müssen installiert sein.
- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- In einer MetroCluster -Umgebung:
  - Sie müssen die MetroCluster Umgebung konfigurieren, bevor Sie einen externen Schlüsselmanager konfigurieren.
  - Sie müssen auf beiden Clustern dasselbe KMIP-SSL-Zertifikat installieren.

Schritte

1. Konfigurieren Sie die Schlüsselmanager-Konnektivität für das Cluster:

```
security key-manager external enable -vserver admin_SVM -key-servers
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
server_CA_certificates
```

> - Der `security key-manager external enable` Befehl ersetzt den `security key-manager setup` Befehl. Sie können den `security key-manager external modify` Befehl ausführen, um die Konfiguration der externen Schlüsselverwaltung zu ändern. Erfahren Sie mehr über `security key-manager external enable` in der "ONTAP-Befehlsreferenz".
> - Wenn Sie in einer MetroCluster-Umgebung externes Verschlüsselungsmanagement für die Admin-SVM konfigurieren, müssen Sie den `security key-manager external enable` Befehl im Partner-Cluster wiederholen.

Mit dem folgenden Befehl wird die externe Schlüsselverwaltung für `cluster1` mit drei externen Schlüsselservern aktiviert. Der erste Schlüsselserver wird mit seinem Hostnamen und Port angegeben, der zweite mit einer IP-Adresse und dem Standardport und der dritte mit einer IPv6-Adresse und einem IPv6-Port:

```
cluster1::> security key-manager external enable -key-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. Vergewissern Sie sich, dass alle konfigurierten KMIP-Server verbunden sind:

`security key-manager external show-status -node node_name -vserver SVM -key -server host_name|IP_address:port -key-server-status available|not-responding|unknown`

> Der `security key-manager external show-status` Befehl ersetzt den `security key-manager show -status` Befehl. Erfahren Sie mehr über `security key-manager external show-status` in der "ONTAP-Befehlsreferenz".

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  --------------------------------------
-------------
node1
      cluster1
               10.0.0.10:5696                                  available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234    available
               ks1.local:15696                                 available
node2
      cluster1
               10.0.0.10:5696                                  available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234    available
               ks1.local:15696                                 available

6 entries were displayed.
```

Verwandte Informationen

- Konfigurieren Sie externe geclusterte Schlüsselserver
- "Sicherheitsschlüssel-Manager-extern-aktivieren"
- "Sicherheitsschlüssel-Manager-externer-Status anzeigen"

Aktivieren Sie die externe Schlüsselverwaltung für die hardwarebasierte Verschlüsselung in ONTAP 9.5 und früher

Ein oder mehrere KMIP-Server dienen zur Sicherung der Schlüssel, die das Cluster für den Zugriff auf verschlüsselte Daten verwendet. Mit einem Node können bis zu vier KMIP-Server verbunden werden. Für Redundanz und Disaster Recovery werden mindestens zwei Server empfohlen.

Über diese Aufgabe

ONTAP konfiguriert die KMIP-Serverkonnektivität für alle Nodes im Cluster.

Bevor Sie beginnen

- Die KMIP SSL-Client- und Serverzertifikate müssen installiert sein.
- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Sie müssen die MetroCluster Umgebung konfigurieren, bevor Sie einen externen Schlüsselmanager konfigurieren.
- In einer MetroCluster-Umgebung müssen Sie dasselbe KMIP-SSL-Zertifikat auf beiden Clustern installieren.

Schritte

1. Konfigurieren Sie die Schlüsselmanager-Konnektivität für Cluster-Nodes:

   `security key-manager setup`

   Die Konfiguration des Schlüsselmanagers wird gestartet.

   In einer MetroCluster -Umgebung müssen Sie diesen Befehl auf beiden Clustern ausführen. Erfahren Sie mehr über `security key-manager setup` im"ONTAP-Befehlsreferenz" .

2. Geben Sie an jeder Eingabeaufforderung die entsprechende Antwort ein.
3. Hinzufügen eines KMIP-Servers:

   `security key-manager add -address key_management_server_ipaddress`

   ```
   clusterl::> security key-manager add -address 20.1.1.1
   ```

   In einer MetroCluster-Umgebung müssen Sie den folgenden Befehl auf beiden Clustern ausführen.

4. Fügen Sie aus Redundanzgründen einen zusätzlichen KMIP-Server hinzu:

   `security key-manager add -address key_management_server_ipaddress`

   ```
   clusterl::> security key-manager add -address 20.1.1.2
   ```

In einer MetroCluster-Umgebung müssen Sie den folgenden Befehl auf beiden Clustern ausführen.

5. Vergewissern Sie sich, dass alle konfigurierten KMIP-Server verbunden sind:

   `security key-manager show -status`

   Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen finden Sie im"ONTAP-Befehlsreferenz" .

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

Node            Port      Registered Key Manager  Status
--------------  ----      ----------------------  ---------------
cluster1-01     5696      20.1.1.1                available
cluster1-01     5696      20.1.1.2                available
cluster1-02     5696      20.1.1.1                available
cluster1-02     5696      20.1.1.2                available
```

6. Konvertieren Sie optional Klartextvolumes in verschlüsselte Volumes.

   `volume encryption conversion start`

   Ein externer Schlüsselmanager muss vollständig konfiguriert sein, bevor Sie die Volumes konvertieren. In einer MetroCluster-Umgebung muss auf beiden Seiten ein externer Schlüsselmanager konfiguriert werden.

Konfiguration von geclusterten externen Schlüsselservern in ONTAP

Ab ONTAP 9.11.1 können Sie die Konnektivität zu geclusterten externen Schlüsselverwaltungsservern auf einer SVM konfigurieren. Mit geclusterten Schlüsselservern können Sie primäre und sekundäre Schlüsselserver auf einer SVM festlegen. Beim Registrieren oder Abrufen von Schlüsseln versucht ONTAP zunächst, auf den primären Schlüsselserver zuzugreifen, bevor es nacheinander versucht, auf sekundäre Server zuzugreifen, bis der Vorgang erfolgreich abgeschlossen ist.

Sie können externe Schlüsselserver für NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE) und NetApp Aggregate Encryption (NAE) Schlüssel verwenden. Ein SVM kann bis zu vier primäre externe KMIP-Server unterstützen. Jeder primäre Server kann bis zu drei sekundäre Schlüsselserver unterstützen.

Über diese Aufgabe

- Dieser Prozess unterstützt nur wichtige Server, die KMIP verwenden. Eine Liste der unterstützten Schlüsselserver finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

Bevor Sie beginnen

- "KMIP-Verschlüsselungsmanagement muss für die SVM aktiviert sein".
- Alle Nodes im Cluster müssen ONTAP 9.11.1 oder höher ausführen.
- Die Reihenfolge der in der `-secondary-key-servers` Der Parameter spiegelt die Zugriffsreihenfolge

der externen Schlüsselverwaltungsserver (KMIP) wider.

Erstellen Sie einen Cluster-Schlüsselserver

Das Konfigurationsverfahren hängt davon ab, ob Sie einen primären Schlüsselserver konfiguriert haben oder nicht.

Hinzufügen von primären und sekundären Schlüsselservern zu einer SVM

Schritte

1. Vergewissern Sie sich, dass für den Cluster (Admin-SVM) keine Schlüsselverwaltung aktiviert ist:

   ```
   security key-manager external show -vserver <svm_name>
   ```

   Wenn auf der SVM bereits die maximale Anzahl von vier primären Schlüsselservern aktiviert ist, müssen Sie einen der vorhandenen primären Schlüsselserver entfernen, bevor Sie einen neuen hinzufügen können.

2. Aktivieren Sie den Primärschlüsselmanager:

   ```
   security key-manager external enable -vserver <svm_name> -key-servers
   <primary_key_server_ip> -client-cert <client_cert_name> -server-ca-certs
   <server_ca_cert_names>
   ```

   - Wenn Sie keinen Port angeben in der `-key-servers` Bei diesem Parameter wird standardmäßig der Port 5696 verwendet.

   > Wenn Sie die `security key-manager external enable` Für den Befehl auf der Admin-SVM in einer MetroCluster -Konfiguration muss der Befehl auf beiden Clustern ausgeführt werden. Wenn Sie den Befehl für eine einzelne Daten-SVM ausführen, müssen Sie den Befehl nicht auf beiden Clustern ausführen. NetApp empfiehlt dringend, auf beiden Clustern die gleichen Key-Server zu verwenden.

3. Ändern Sie den primären Schlüsselserver, um sekundäre Schlüsselserver hinzuzufügen. Der `-secondary-key-servers` Der Parameter akzeptiert eine durch Kommas getrennte Liste von bis zu drei Schlüsselservern:

   ```
   security key-manager external modify-server -vserver <svm_name> -key
   -servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
   ```

   - Geben Sie keine Portnummer für sekundäre Schlüsselserver an. `-secondary-key-servers` Parameter. Es verwendet dieselbe Portnummer wie der primäre Schlüsselserver.

   > Wenn Sie die `security key-manager external` Für den Befehl auf der Admin-SVM in einer MetroCluster -Konfiguration muss der Befehl auf beiden Clustern ausgeführt werden. Wenn Sie den Befehl für eine einzelne Daten-SVM ausführen, müssen Sie den Befehl nicht auf beiden Clustern ausführen. NetApp empfiehlt dringend, auf beiden Clustern die gleichen Key-Server zu verwenden.

Fügen Sie einem vorhandenen primären Schlüsselserver sekundäre Schlüsselserver hinzu

Schritte

1. Ändern Sie den primären Schlüsselserver, um sekundäre Schlüsselserver hinzuzufügen. Der `-secondary-key-servers` Der Parameter akzeptiert eine durch Kommas getrennte Liste von bis zu drei Schlüsselservern:

   ```
   security key-manager external modify-server -vserver <svm_name> -key
   -servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
   ```

- Geben Sie keine Portnummer für sekundäre Schlüsselserver an. `-secondary-key-servers` Parameter. Es verwendet dieselbe Portnummer wie die primären Schlüsselserver.

> Wenn Sie die `security key-manager external modify-server` Für den Befehl auf der Admin-SVM in einer MetroCluster -Konfiguration muss der Befehl auf beiden Clustern ausgeführt werden. Wenn Sie den Befehl für eine einzelne Daten-SVM ausführen, müssen Sie den Befehl nicht auf beiden Clustern ausführen. NetApp empfiehlt dringend, auf beiden Clustern die gleichen Key-Server zu verwenden.

Weitere Informationen zu sekundären Schlüsselservern finden Sie unter [mod-secondary]Die

Cluster-Key-Server ändern

Sie können gruppierte externe Schlüsselserver modifizieren, indem Sie sekundäre Schlüsselserver hinzufügen und entfernen, die Zugriffsreihenfolge der sekundären Schlüsselserver ändern oder die Bezeichnung (primär oder sekundär) bestimmter Schlüsselserver ändern. Wenn Sie geclusterte externe Schlüsselserver in einer MetroCluster -Konfiguration ändern, empfiehlt NetApp dringend, auf beiden Clustern die gleichen Schlüsselserver zu verwenden.

Ändern Sie sekundäre Schlüsselserver

Verwenden Sie den `-secondary-key-servers`-Parameter des Befehls `security key-manager external modify-server`, um Server mit sekundärem Schlüssel zu verwalten. Der `-secondary-key -servers` Der Parameter akzeptiert eine durch Kommas getrennte Liste. Die in der Liste angegebene Reihenfolge der sekundären Schlüsselserver bestimmt die Zugriffsreihenfolge für die sekundären Schlüsselserver. Sie können die Zugriffsreihenfolge ändern, indem Sie den Befehl `security key-manager external modify-server`mit den sekundären Schlüsselservern in einer anderen Reihenfolge ausführen. Geben Sie für sekundäre Schlüsselserver keine Portnummer an.

> Wenn Sie die `security key-manager external modify-server` Für den Befehl auf der Admin-SVM in einer MetroCluster -Konfiguration muss der Befehl auf beiden Clustern ausgeführt werden. Wenn Sie den Befehl für eine einzelne Daten-SVM ausführen, müssen Sie den Befehl nicht auf beiden Clustern ausführen.

Um einen sekundären Schlüsselserver zu entfernen, fügen Sie die Schlüsselserver, die Sie behalten möchten, in die Liste ein. `-secondary-key-servers` Parameter und lassen Sie denjenigen weg, den Sie entfernen möchten. Um alle sekundären Schlüsselserver zu entfernen, verwenden Sie das Argument `-` , was bedeutet, dass es keine gibt.

Konvertieren Sie primäre und sekundäre Schlüsselserver

Mit den folgenden Schritten können Sie die Bezeichnung (primär oder sekundär) bestimmter Schlüsselserver ändern.

Konvertierung eines primären Schlüsselservers in einen sekundären Schlüsselserver

Schritte

1. Entfernen Sie den primären Schlüsselserver aus der SVM:

   ```
   security key-manager external remove-servers
   ```

   Wenn Sie die `security key-manager external remove-servers` Für den Befehl auf der Admin-SVM in einer MetroCluster -Konfiguration muss der Befehl auf beiden Clustern ausgeführt werden. Wenn Sie den Befehl für eine einzelne Daten-SVM ausführen, müssen Sie den Befehl nicht auf beiden Clustern ausführen.

2. Führe dieErstellen Sie einen Cluster-Schlüsselserver Verfahren, bei dem der frühere primäre Schlüsselserver als sekundärer Schlüsselserver verwendet wird.

Konvertierung eines sekundären Schlüsselservers in einen primären Schlüsselserver

Schritte

1. Entfernen Sie den sekundären Schlüsselserver von seinem bestehenden primären Schlüsselserver:

   ```
   security key-manager external modify-server -secondary-key-servers
   ```

- Wenn Sie die `security key-manager external modify-server -secondary-key-servers` Für den Befehl auf der Admin-SVM in einer MetroCluster -Konfiguration muss der Befehl auf beiden Clustern ausgeführt werden. Wenn Sie den Befehl für eine einzelne Daten-SVM ausführen, müssen Sie den Befehl nicht auf beiden Clustern ausführen.
- Wenn Sie einen sekundären Schlüsselserver in einen primären Schlüsselserver umwandeln, während Sie einen vorhandenen Schlüsselserver entfernen, kann der Versuch, einen neuen Schlüsselserver hinzuzufügen, bevor die Entfernung und Umwandlung abgeschlossen ist, zu einer Duplizierung der Schlüssel führen.

1. Führe dieErstellen Sie einen Cluster-Schlüsselserver Verfahren, bei dem der frühere sekundäre Schlüsselserver als primärer Schlüsselserver des neuen Cluster-Schlüsselservers verwendet wird.

Siehe[mod-secondary] für weitere Informationen.

Verwandte Informationen

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

Erstellen Sie Authentifizierungsschlüssel in ONTAP 9.6 und höher

Mit dem `security key-manager key create` Befehl können Sie die Authentifizierungsschlüssel für einen Node erstellen und auf den konfigurierten KMIP-Servern speichern.

Über diese Aufgabe

Wenn Sie in Ihrer Sicherheitseinrichtung unterschiedliche Schlüssel für die Datenauthentifizierung und die FIPS 140-2-Authentifizierung verwenden müssen, sollten Sie jeweils einen separaten Schlüssel erstellen. Ist dies nicht der Fall, können Sie denselben Authentifizierungsschlüssel für die FIPS-Compliance verwenden wie

für den Datenzugriff.

ONTAP erstellt Authentifizierungsschlüssel für alle Nodes im Cluster.

- Dieser Befehl wird nicht unterstützt, wenn Onboard Key Manager aktiviert ist. Es werden jedoch automatisch zwei Authentifizierungsschlüssel erstellt, wenn der Onboard Key Manager aktiviert ist. Die Tasten können mit dem folgenden Befehl angezeigt werden:

```
security key-manager key query -key-type NSE-AK
```

- Sie erhalten eine Warnung, wenn auf den konfigurierten Schlüsselverwaltungsservern bereits mehr als 128 Authentifizierungsschlüssel gespeichert werden.
- Sie können den `security key-manager key delete` Befehl verwenden, um alle nicht verwendeten Schlüssel zu löschen. Der `security key-manager key delete` Befehl schlägt fehl, wenn der angegebene Schlüssel derzeit von ONTAP verwendet wird. (Privileges muss größer sein als `admin` für die Verwendung dieses Befehls.)

> Bevor Sie einen Schlüssel in einer MetroCluster-Umgebung löschen, müssen Sie sicherstellen, dass der Schlüssel nicht im Partner-Cluster verwendet wird. Sie können auf dem Partner-Cluster folgende Befehle verwenden, um zu überprüfen, ob der Schlüssel nicht verwendet wird:
>
> - `storage encryption disk show -data-key-id <key-id>`
> - `storage encryption disk show -fips-key-id <key-id>`

Bevor Sie beginnen

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

Schritte

1. Authentifizierungsschlüssel für Cluster-Nodes erstellen:

```
security key-manager key create -key-tag <passphrase_label> -prompt-for
-key true|false
```

> `prompt-for-key=true`Durch die Einstellung fordert das System den Clusteradministrator auf, die Passphrase bei der Authentifizierung verschlüsselter Laufwerke zu verwenden. Andernfalls generiert das System automatisch eine 32-Byte-Passphrase. Der `security key-manager key create` Befehl ersetzt den `security key-manager create-key` Befehl. Erfahren Sie mehr über `security key-manager key create` in der link:https://docs.netapp.com/us-en/ontap-cli/security-key-manager-key-create.html?q=security+key-manager+key+create["ONTAP-Befehlsreferenz"^].

Im folgenden Beispiel werden die Authentifizierungsschlüssel für erstellt `cluster1`, die automatisch eine 32-Byte-Passphrase erzeugen:

```
cluster1::> security key-manager key create
Key ID: <id_value>
```

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

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

> Der `security key-manager key query` Befehl ersetzt den `security key-manager query key` Befehl.
>
> Die in der Ausgabe angezeigte Schlüssel-ID ist eine Kennung, die auf den Authentifizierungsschlüssel verweist. Es handelt sich nicht um den tatsächlichen Authentifizierungsschlüssel oder den Datenverschlüsselung.

Im folgenden Beispiel wird überprüft, ob Authentifizierungsschlüssel für erstellt `cluster1` wurden:

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: external
          Node: node1

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID: <id_value>
node1                                    NSE-AK    yes
    Key ID: <id_value>

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID: <id_value>
node2                                    NSE-AK    yes
    Key ID: <id_value>
```

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

Verwandte Informationen

- "Speicherverschlüsselung Datenträger anzeigen"

Erstellen Sie Authentifizierungsschlüssel in ONTAP 9.5 und früher

Mit dem `security key-manager create-key` Befehl können Sie die Authentifizierungsschlüssel für einen Node erstellen und auf den konfigurierten KMIP-Servern speichern.

Über diese Aufgabe

Wenn Sie in Ihrer Sicherheitseinrichtung unterschiedliche Schlüssel für die Datenauthentifizierung und die FIPS 140-2-Authentifizierung verwenden müssen, sollten Sie jeweils einen separaten Schlüssel erstellen. Falls dies nicht der Fall ist, können Sie denselben Authentifizierungsschlüssel für die FIPS-Compliance verwenden, den Sie für den Datenzugriff verwenden.

ONTAP erstellt Authentifizierungsschlüssel für alle Nodes im Cluster.

- Dieser Befehl wird nicht unterstützt, wenn das integrierte Verschlüsselungsmanagement aktiviert ist.
- Sie erhalten eine Warnung, wenn auf den konfigurierten Schlüsselverwaltungsservern bereits mehr als 128 Authentifizierungsschlüssel gespeichert werden.

  Sie können die Verschlüsselungsmanagement-Server-Software verwenden, um alle nicht verwendeten Schlüssel zu löschen, und führen den Befehl erneut aus.

Bevor Sie beginnen

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

Schritte

1. Authentifizierungsschlüssel für Cluster-Nodes erstellen:

   ```
   security key-manager create-key
   ```

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

   > ⓘ Die in der Ausgabe angezeigte Schlüssel-ID ist eine Kennung, die auf den Authentifizierungsschlüssel verweist. Es handelt sich nicht um den tatsächlichen Authentifizierungsschlüssel oder den Datenverschlüsselung.

   Im folgenden Beispiel werden die Authentifizierungsschlüssel für erstellt `cluster1`:

```
cluster1::> security key-manager create-key
   (security key-manager create-key)
Verifying requirements...

Node: cluster1-01
Creating authentication key...
Authentication key creation successful.
Key ID: <id_value>

Node: cluster1-01
Key manager restore operation initialized.
Successfully restored key information.

Node: cluster1-02
Key manager restore operation initialized.
Successfully restored key information.
```

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

   `security key-manager query`

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

   Im folgenden Beispiel wird überprüft, ob Authentifizierungsschlüssel für erstellt `cluster1` wurden:

```
cluster1::> security key-manager query

  (security key-manager query)

          Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-01     NSE-AK    yes
       Key ID: <id_value>


          Node: cluster1-02
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-02     NSE-AK    yes
       Key ID: <id_value>
```

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

Mit dem `storage encryption disk modify` Befehl können Sie einem FIPS-Laufwerk oder einer SED einen Datenauthentifizierungsschlüssel zuweisen. Clusterknoten verwenden diesen Schlüssel zum Sperren oder Entsperren verschlüsselter 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.

Dieses Verfahren ist nicht störend.

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 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.
```

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"

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"

Weisen Sie einem ONTAP FIPS-Laufwerk einen FIPS 140-2-Authentifizierungsschlüssel zu

Sie können den `storage encryption disk modify` Befehl mit der `-fips-key-id` Option verwenden, um einem FIPS-Laufwerk einen FIPS-140-2-

Authentifizierungsschlüssel zuzuweisen. Cluster-Nodes verwenden diesen Schlüssel für andere Laufwerksvorgänge als Datenzugriff, z. B. zur Verhinderung von Denial-of-Service-Angriffen auf das Laufwerk.

Über diese Aufgabe

In Ihrer Sicherheitseinrichtung müssen Sie unter Umständen unterschiedliche Schlüssel zur Datenauthentifizierung und zur FIPS 140-2-2-Authentifizierung verwenden. Falls dies nicht der Fall ist, können Sie denselben Authentifizierungsschlüssel für die FIPS-Compliance verwenden, den Sie für den Datenzugriff verwenden.

Dieses Verfahren ist nicht störend.

Bevor Sie beginnen

Die Laufwerk-Firmware muss FIPS 140-2-2-konform unterstützen. Das "NetApp Interoperabilitäts-Matrix-Tool" enthält Informationen zu unterstützten Festplatten-Firmware-Versionen.

Schritte

1. Sie müssen zunächst sicherstellen, dass Sie einen Datenauthentifizierungsschlüssel zugewiesen haben. Dies kann mit einem Externer Schlüsselmanager oder einem durchgeführt werdenIntegriertes Verschlüsselungsmanagement. Überprüfen Sie, ob der Schlüssel mit dem Befehl zugewiesen `storage encryption disk show` ist.
2. SEDs einen FIPS 140-2-Authentifizierungsschlüssel zuweisen:

   `storage encryption disk modify -disk` *`disk_id`* `-fips-key-id` *`fips_authentication_key_id`*

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

   ```
   cluster1::> storage encryption disk modify -disk 2.10.* -fips-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.
   ```

3. Vergewissern Sie sich, dass der Authentifizierungsschlüssel zugewiesen wurde:

   `storage encryption disk show -fips`

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

```
cluster1::> storage encryption disk show -fips
Disk    Mode FIPS-Compliance Key ID
------  ----
--------------------------------------------------------------------
2.10.0  full <id_value>
2.10.1  full <id_value>
[...]
```

Verwandte Informationen

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

Ermöglichen Sie den Cluster-weiten FIPS-konformen Modus für KMIP-Serververbindungen in ONTAP

Sie können den `security config modify` Befehl mit der `-is-fips-enabled` Option verwenden, um Cluster-weiten FIPS-konformen Modus für genutzte Daten zu aktivieren. Dadurch wird die Verwendung von OpenSSL im FIPS-Modus erzwingt, wenn eine Verbindung zu KMIP-Servern hergestellt wird.

Über diese Aufgabe

Wenn Sie den FIPS-konformen Cluster-Modus aktivieren, verwendet das Cluster automatisch nur TLS1.2 und FIPS-validierte Chiffre Suites. Der clusterweite FIPS-konforme Modus ist standardmäßig deaktiviert.

Sie müssen die Cluster-Nodes manuell neu booten, nachdem Sie die Cluster-weite Sicherheitskonfiguration geändert haben.

Bevor Sie beginnen

- Der Storage Controller muss im FIPS-konformen Modus konfiguriert sein.
- Alle KMIP-Server müssen TLSv1.2 unterstützen. Das System benötigt TLSv1.2, um die Verbindung zum KMIP-Server abzuschließen, wenn der clusterweite FIPS-konforme Modus aktiviert ist.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Vergewissern Sie sich, dass TLSv1.2 unterstützt wird:

   ```
   security config show -supported-protocols
   ```

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

```
cluster1::> security config show
          Cluster                                                  Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ---------------------- -----------------
----------------
SSL       false      TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL
```

3. Cluster-weiten, FIPS-konformen Modus aktivieren:

   `security config modify -is-fips-enabled true -interface SSL`

   Erfahren Sie mehr über `security config modify` in der "ONTAP-Befehlsreferenz".

4. Manuelles Neubooten der Cluster-Nodes
5. Vergewissern Sie sich, dass der FIPS-konforme Cluster-weite Modus aktiviert ist:

   `security config show`

```
cluster1::> security config show
          Cluster                                                  Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ---------------------- -----------------
----------------
SSL       true       TLSv1.2, TLSv1.1       ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL:!RC4
```