Hardwarebasierte Verschlüsselung von NetApp konfigurieren

ONTAP 9

NetApp
November 10, 2026

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

Inhalt

Hardwarebasierte Verschlüsselung von NetApp konfigurieren . . . 1
Informationen zu ONTAP hardwarebasierter Verschlüsselung . . . 1
Verständnis der NetApp hardwarebasierten Verschlüsselung . . . 1
Unterstützte Self-Encrypting Drives Typen . . . 1
Wann wird externes Schlüsselmanagement verwendet? . . . 2
Supportdetails . . . 2
Hardwarebasierter Verschlüsselungsworkflow . . . 3
Externe Schlüsselverwaltung konfigurieren . . . 3
Informationen zur externen Schlüsselverwaltung in ONTAP . . . 3
SSL-Zertifikate auf dem ONTAP Cluster installieren . . . 4
Externe Schlüsselverwaltung für die Hardwareverschlüsselung in ONTAP 9.6 und höheren Versionen aktivieren . . . 5
Aktivierung der externen Schlüsselverwaltung für die Hardwareverschlüsselung in ONTAP 9.5 und früheren Versionen . . . 6
Konfiguration von gruppierten externen Schlüsselservern in ONTAP . . . 8
Authentifizierungsschlüssel in ONTAP 9.6 und höher erstellen . . . 11
Authentifizierungsschlüssel in ONTAP 9.5 und früher erstellen . . . 13
Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder ONTAP SED . . . 15
Onboard-Schlüsselverwaltung konfigurieren . . . 16
Integrierte Schlüsselverwaltung in ONTAP 9.6 und höher aktivieren . . . 16
Integrierte Schlüsselverwaltung in ONTAP 9.5 und früher aktivieren . . . 19
Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder ONTAP SED . . . 21
Einem ONTAP FIPS-Laufwerk einen FIPS 140-2-Authentifizierungsschlüssel zuweisen . . . 22
Clusterweiten FIPS-konformen Modus für KMIP-Verbindungen in ONTAP aktivieren . . . 24

Hardwarebasierte Verschlüsselung von NetApp konfigurieren

Informationen zu ONTAP hardwarebasierter Verschlüsselung

NetApp hardwarebasierte Verschlüsselung unterstützt die vollständige Festplattenverschlüsselung (FDE) von Daten während des Schreibvorgangs. Die Daten können ohne einen auf der Firmware gespeicherten Verschlüsselungsschlüssel nicht gelesen werden. Der Verschlüsselungsschlüssel ist wiederum nur für einen authentifizierten Knoten zugänglich.

Verständnis der NetApp hardwarebasierten Verschlüsselung

Ein Knoten authentifiziert sich gegenüber einem Self-Encrypting Drive mithilfe eines Authentifizierungsschlüssels, der von einem externen Schlüsselverwaltungsserver oder dem Onboard Key Manager abgerufen wird:

- Der externe Schlüsselverwaltungsserver ist ein Drittanbietersystem in Ihrer Speicherumgebung, das Schlüssel für Knoten mithilfe des Key Management Interoperability Protocol (KMIP) bereitstellt. Es gilt als Best Practice, externe Schlüsselverwaltungsserver auf einem anderen Speichersystem als Ihren Daten zu konfigurieren.
- Der Onboard Key Manager ist ein integriertes Tool, das Authentifizierungsschlüssel für Knoten aus demselben Speichersystem bereitstellt wie Ihre Daten.

Sie können NetApp Volume Encryption mit hardwarebasierter Verschlüsselung verwenden, um Daten auf Self-Encrypting Drives „doppelt zu verschlüsseln“.

Wenn Self-Encrypting Drives aktiviert sind, wird auch der Core Dump verschlüsselt.

> Wenn ein HA-Paar verschlüsselnde SAS- oder NVMe-Laufwerke (SED, NSE, FIPS) verwendet, sind die Anweisungen im Thema Zurückstellen eines FIPS-Laufwerks oder SED in den ungeschützten Modus für alle Laufwerke innerhalb des HA-Paares vor der Initialisierung des Systems (Boot-Optionen 4 oder 9) zu beachten. Andernfalls kann es in Zukunft zu Datenverlust kommen, wenn die Laufwerke wiederverwendet werden.

Unterstützte Self-Encrypting Drives Typen

Es werden zwei Arten von Self-Encrypting Drives unterstützt:

- Self-Encrypting Drives (FIPS-zertifizierte SAS- oder NVMe-Laufwerke) werden auf allen FAS und AFF Systemen unterstützt. Diese Laufwerke, sogenannte FIPS Drives, erfüllen die Anforderungen der Federal Information Processing Standard Publication 140-2, Level 2. Die zertifizierten Funktionen ermöglichen neben der Verschlüsselung weitere Schutzmechanismen, wie beispielsweise die Abwehr von Denial-of-Service-Angriffen. FIPS-Laufwerke dürfen nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden.
- Ab ONTAP 9.6 werden Self-Encrypting NVMe Drives, die nicht dem FIPS-Test unterzogen wurden, auf AFF A800, A320 und späteren Systemen unterstützt. Diese Laufwerke, sogenannte SEDs, bieten dieselben Verschlüsselungsfunktionen wie FIPS Drives, können aber zusammen mit nicht

verschlüsselnden Laufwerken auf demselben Node oder HA-Paar eingesetzt werden.

- Alle FIPS-validierten Laufwerke verwenden ein Firmware-Kryptografiemodul, das die FIPS-Validierung durchlaufen hat. Das FIPS-Kryptografiemodul des Laufwerks verwendet keine Schlüssel, die außerhalb des Laufwerks generiert werden (die Authentifizierungs-Passphrase, die für das Laufwerk eingegeben wird, wird vom Firmware-Kryptografiemodul des Laufwerks verwendet, um einen Schlüssel zur Verschlüsselung zu erhalten).

Nicht verschlüsselnde Laufwerke sind Laufwerke, die weder SEDs noch FIPS-Laufwerke sind.

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

Wann wird externes Schlüsselmanagement verwendet?

Auch wenn die Verwendung des integrierten Schlüsselmanagers kostengünstiger und in der Regel bequemer ist, empfiehlt sich die Nutzung einer externen Schlüsselverwaltung, wenn einer der folgenden Punkte zutrifft:

- Die Richtlinie Ihrer Organisation erfordert eine Schlüsselverwaltungslösung, die ein kryptografisches Modul gemäß FIPS 140-2 Level 2 (oder höher) verwendet.
- Sie benötigen eine Multi-Cluster-Lösung mit zentralisierter Verwaltung der Verschlüsselungsschlüssel.
- Ihr Unternehmen benötigt die zusätzliche Sicherheit, Authentifizierungsschlüssel auf einem System oder an einem anderen Ort als die Daten zu speichern.

Supportdetails

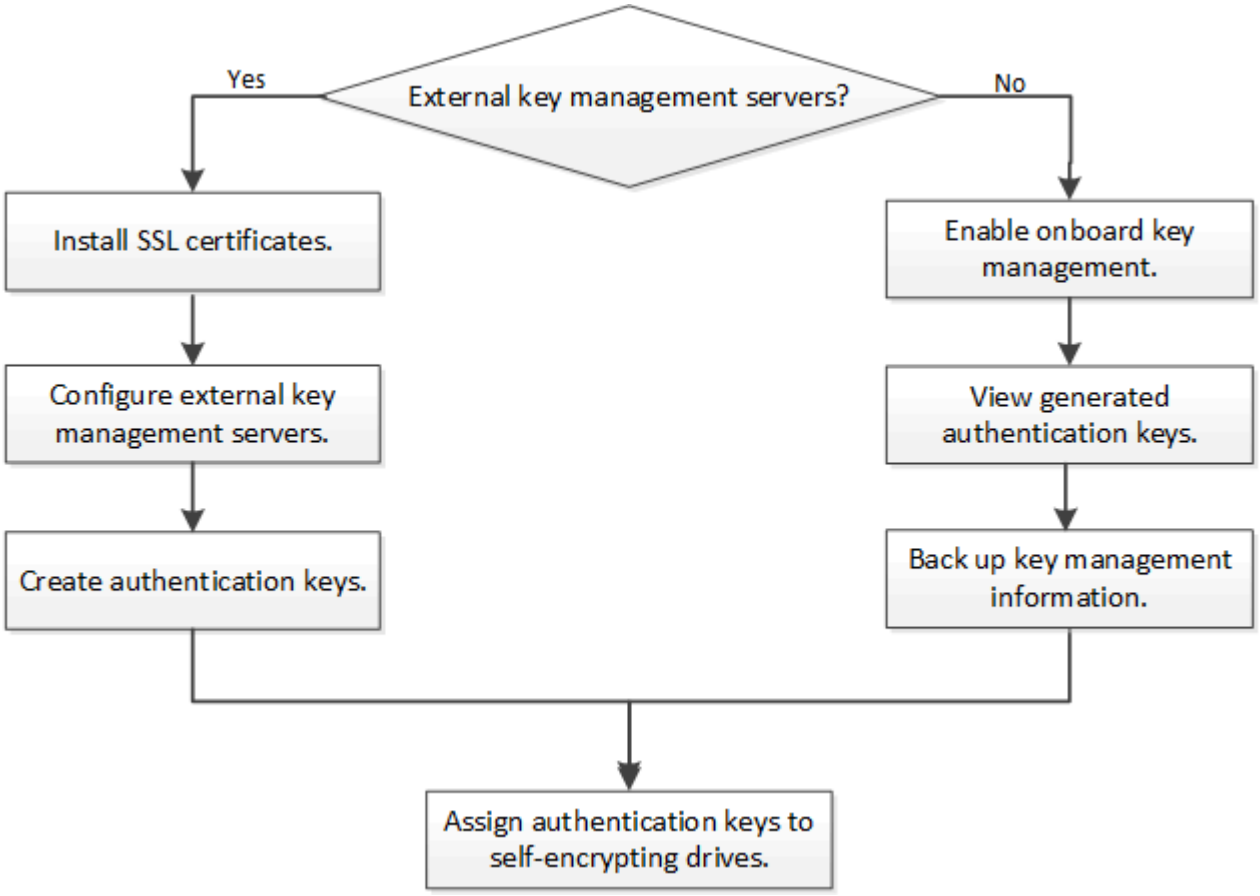
Die folgende Tabelle enthält wichtige Details zur Hardware-Verschlüsselungsunterstützung. Die Interoperabilitätsmatrix enthält aktuelle Informationen zu unterstützten KMIP-Servern, Speichersystemen und Festplattengehäusen.

Ressource oder Funktion	Supportdetails
Nicht-homogene Festplattensätze	• FIPS-Laufwerke dürfen nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden. Konforme HA-Paare können im selben Cluster neben nicht-konformen HA-Paaren existieren. • SEDs können mit nicht verschlüsselnden Laufwerken auf demselben Node oder HA Pair gemischt werden.
Laufwerkstyp	• FIPS-Laufwerke können SAS- oder NVMe-Laufwerke sein. • SEDs müssen NVMe-Laufwerke sein.
10 Gb Netzwerkschnittstellen	Ab ONTAP 9.3 unterstützen KMIP-Schlüsselverwaltungskonfigurationen 10 Gb Netzwerkschnittstellen für die Kommunikation mit externen Schlüsselverwaltungsservern.
Ports für die Kommunikation mit dem Schlüsselverwaltungsserver	Ab ONTAP 9.3 kann jeder beliebige Port des Storage Controllers für die Kommunikation mit dem Key Management Server verwendet werden. Andernfalls sollte Port e0M für die Kommunikation mit Key Management Servern verwendet werden. Je nach Storage Controller Modell sind bestimmte Netzwerkschnittstellen während des Bootvorgangs möglicherweise nicht für die Kommunikation mit Key Management Servern verfügbar.

MetroCluster (MCC)	• NVMe-Laufwerke unterstützen MCC. • SAS-Laufwerke unterstützen MCC nicht.

Hardwarebasierter Verschlüsselungsworkflow

Die Schlüsselverwaltungsdienste müssen konfiguriert werden, bevor sich der Cluster gegenüber den Self-Encrypting Drives authentifizieren kann. Es kann ein externer Schlüsselverwaltungsserver oder ein integrierter Schlüsselmanager verwendet werden.



Verwandte Informationen

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

Externe Schlüsselverwaltung konfigurieren

Informationen zur externen Schlüsselverwaltung in ONTAP

Sie können einen oder mehrere externe Schlüsselverwaltungsserver verwenden, um die Schlüssel zu sichern, die der Cluster für den Zugriff auf verschlüsselte Daten verwendet. Ein externer Schlüsselverwaltungsserver ist ein Drittanbietersystem in Ihrer Speicherumgebung, das Schlüssel an Nodes mithilfe des Key Management Interoperability Protocol (KMIP) bereitstellt.

NetApp Volume Encryption (NVE) kann mit dem Onboard Key Manager implementiert werden. In ONTAP 9.3 und höher kann NVE mit externem Key Management (KMIP) und dem Onboard Key Manager implementiert werden. Ab ONTAP 9.11.1 ist die Konfiguration mehrerer externer Schlüsselmanager in einem Cluster möglich. Siehe Clustered Key-Server konfigurieren.

SSL-Zertifikate auf dem ONTAP Cluster installieren

Der Cluster und der KMIP-Server verwenden KMIP-SSL-Zertifikate, um gegenseitig die Identität zu verifizieren und eine SSL-Verbindung herzustellen. Vor der Konfiguration der SSL-Verbindung mit dem KMIP-Server müssen die KMIP-Client-SSL-Zertifikate für den Cluster sowie das öffentliche SSL-Zertifikat für die Root-Zertifizierungsstelle (CA) des KMIP-Servers installiert werden.

Über diese Aufgabe

In einem HA-Paar müssen beide Knoten dieselben öffentlichen und privaten KMIP-SSL-Zertifikate verwenden. Wenn mehrere HA-Paare mit demselben KMIP-Server verbunden sind, müssen alle Knoten in den HA-Paaren dieselben öffentlichen und privaten KMIP-SSL-Zertifikate verwenden.

Bevor Sie beginnen

- Die Zeit muss auf dem Server, der die Zertifikate erstellt, dem KMIP Server und dem Cluster synchronisiert sein.
- Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.
- Das öffentliche SSL KMIP-Clientzertifikat für den Cluster muss vorliegen.
- Der private Schlüssel, der dem SSL KMIP Clientzertifikat für den Cluster zugeordnet ist, muss vorliegen.
- Das SSL KMIP-Clientzertifikat darf nicht passwortgeschützt sein.
- Das öffentliche SSL-Zertifikat für die Stammzertifizierungsstelle (CA) des KMIP-Servers muss vorliegen.
- In einer MetroCluster Umgebung müssen auf beiden Clustern die gleichen KMIP SSL-Zertifikate installiert werden.

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

`admin_SVM` ist die Admin-SVM für den Cluster. In den folgenden Beispielen heißt die Admin-SVM `cluster1`, daher erscheint `cluster1` sowohl in der Eingabeaufforderung (`cluster1::>`) als auch als Wert für `-vserver`.

Schritte

1. Die SSL-KMIP-Clientzertifikate für den Cluster installieren:

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

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

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

2. Das öffentliche SSL-Zertifikat für die Root-Zertifizierungsstelle (CA) des KMIP-Servers installieren:

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

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

Verwandte Informationen

- "Sicherheitszertifikat installieren"

Externe Schlüsselverwaltung für die Hardwareverschlüsselung in ONTAP 9.6 und höheren Versionen aktivieren

Sie können einen oder mehrere KMIP-Server verwenden, um die Schlüssel zu sichern, die der Cluster für den Zugriff auf verschlüsselte Daten verwendet. Sie können bis zu vier KMIP-Server mit einem Knoten verbinden. Für Redundanz und Notfallwiederherstellung werden mindestens zwei Server empfohlen.

Ab ONTAP 9.11.1 können bis zu 3 sekundäre Schlüsselserver pro primärem Schlüsselserver hinzugefügt werden, um einen gruppierten Schlüsselserver zu erstellen. Weitere Informationen finden sich unter Clustered externe Schlüsselserver konfigurieren.

Bevor Sie beginnen

- Die KMIP SSL-Client- und Serverzertifikate müssen installiert sein.
- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- In einer MetroCluster Umgebung:
  - Die MetroCluster Umgebung muss konfiguriert werden, bevor ein externer Schlüsselmanager konfiguriert wird.
  - Auf beiden Clustern ist dasselbe KMIP SSL-Zertifikat zu installieren.

Schritte

1. Die Key-Manager-Konnektivität für den Cluster konfigurieren:

   ```
   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. Der `security key-manager external modify` Befehl kann verwendet werden, um die Konfiguration der externen Schlüsselverwaltung zu ändern. Weitere Informationen zu `security key-manager external enable` finden sich in der "ONTAP-Befehlsreferenz".
   - In einer MetroCluster Umgebung muss bei der Konfiguration der externen Schlüsselverwaltung für die Admin-SVM der `security key-manager external enable` Befehl auf dem Partnercluster wiederholt werden.

   Der folgende Befehl aktiviert die externe Schlüsselverwaltung für `cluster1` mit drei externen Schlüsselservern. Der erste Schlüsselserver wird über seinen Hostnamen und Port angegeben, der zweite über eine IP-Adresse und den Standardport, und der dritte über eine IPv6-Adresse und den 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. Es wird überprüft, ob 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. Weitere Informationen zu `security key-manager external show-status` finden sich 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

- Clustered externe Schlüsselserver konfigurieren
- "security-key-manager-external-enable"
- "security-key-manager-external-show-status"

Aktivierung der externen Schlüsselverwaltung für die Hardwareverschlüsselung in ONTAP 9.5 und früheren Versionen

Sie können einen oder mehrere KMIP-Server verwenden, um die Schlüssel zu sichern, die der Cluster für den Zugriff auf verschlüsselte Daten verwendet. Sie können bis zu vier KMIP-Server mit einem Knoten verbinden. Für Redundanz und Notfallwiederherstellung werden mindestens zwei Server empfohlen.

Über diese Aufgabe

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

Bevor Sie beginnen

- Die KMIP SSL-Client- und Serverzertifikate müssen installiert sein.
- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Die MetroCluster Umgebung muss konfiguriert werden, bevor ein externer Schlüsselmanager konfiguriert wird.
- In einer MetroCluster Umgebung muss auf beiden Clustern dasselbe KMIP SSL-Zertifikat installiert werden.

Schritte

1. Konfiguration der Key-Manager-Konnektivität für Clusterknoten:

   `security key-manager setup`

   Die Einrichtung des Schlüsselmanagers beginnt.

   In einer MetroCluster Umgebung muss dieser Befehl auf beiden Clustern ausgeführt werden. Weitere Informationen zu `security key-manager setup` finden sich in der "ONTAP-Befehlsreferenz".

2. Geben Sie bei jeder Eingabeaufforderung die entsprechende Antwort ein.
3. Einen KMIP-Server hinzufügen:

   `security key-manager add -address key_management_server_ipaddress`

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

   In einer MetroCluster Umgebung muss dieser Befehl auf beiden Clustern ausgeführt werden.

4. Einen zusätzlichen KMIP Server für Redundanz hinzufügen:

   `security key-manager add -address key_management_server_ipaddress`

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

   In einer MetroCluster Umgebung muss dieser Befehl auf beiden Clustern ausgeführt werden.

5. Es wird überprüft, ob alle konfigurierten KMIP-Server verbunden sind:

   `security key-manager show -status`

   Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "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. Optional können Klartext-Volumes in verschlüsselte Volumes umgewandelt werden.

   `volume encryption conversion start`

   Vor der Konvertierung der Volumes muss ein externer Schlüsselmanager vollständig konfiguriert sein. In einer MetroCluster-Umgebung muss ein externer Schlüsselmanager an beiden Standorten konfiguriert sein.

Konfiguration von gruppierten externen Schlüsselservern in ONTAP

Ab ONTAP 9.11.1 kann die Konnektivität zu gruppierten externen Schlüsselverwaltungsservern auf einer SVM konfiguriert werden. Mit gruppierten Schlüsselservern lassen sich primäre und sekundäre Schlüsselserver auf einer SVM festlegen. Beim Registrieren oder Abrufen von Schlüsseln versucht ONTAP zunächst, auf den primären Schlüsselserver zuzugreifen, bevor nacheinander die sekundären Server angesprochen werden, bis der Vorgang erfolgreich abgeschlossen ist.

Externe Schlüsselserver können für NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE) und NetApp Aggregate Encryption (NAE) Schlüssel verwendet werden. Eine 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 Schlüsselserver, die KMIP verwenden. Eine Liste der unterstützten Schlüsselserver befindet sich im "NetApp Interoperabilitätsmatrix-Tool".

Bevor Sie beginnen

- "Die KMIP-Schlüsselverwaltung muss für die SVM aktiviert sein.".
- Alle Knoten im Cluster müssen ONTAP 9.11.1 oder höher ausführen.
- Die Reihenfolge der im `-secondary-key-servers` Parameter aufgeführten Server entspricht der Zugriffsreihenfolge der externen Key-Management-Server (KMIP).

Einen gruppierten Schlüsselserver erstellen

Das Konfigurationsverfahren hängt davon ab, ob ein Primärschlüsselserver konfiguriert wurde oder nicht.

Primäre und sekundäre Schlüsselserver zu einer SVM hinzufügen

Schritte

1. Bestätigen Sie, dass für den Cluster (admin SVM) keine Schlüsselverwaltung aktiviert wurde:

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

Wenn auf der SVM bereits die maximale Anzahl von vier primären Schlüsselservern aktiviert ist, muss einer der vorhandenen primären Schlüsselserver entfernt werden, bevor ein neuer hinzugefügt werden kann.

2. Primärschlüsselmanager aktivieren:

```
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 im `-key-servers`-Parameter kein Port angegeben wird, wird der Standardport 5696 verwendet.

> Wenn Sie den `security key-manager external enable` Befehl für die administrative SVM in einer MetroCluster Konfiguration ausführen, muss der Befehl auf beiden Clustern ausgeführt werden. Wenn Sie den Befehl für eine einzelne Daten-SVM ausführen, ist es nicht erforderlich, den Befehl auf beiden Clustern auszuführen. NetApp empfiehlt nachdrücklich, auf beiden Clustern dieselben Schlüsselserver zu verwenden.

3. Den primären Schlüsselserver ändern, um sekundäre Schlüsselserver hinzuzufügen. Der `-secondary-key-servers` 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 im `-secondary-key-servers` Parameter keine Portnummer für sekundäre Schlüsselserver an. Es wird dieselbe Portnummer wie für den primären Schlüsselserver verwendet.

> Wenn Sie den `security key-manager external` Befehl für die administrative SVM in einer MetroCluster Konfiguration ausführen, muss der Befehl auf beiden Clustern ausgeführt werden. Wenn Sie den Befehl für eine einzelne Daten-SVM ausführen, ist es nicht erforderlich, den Befehl auf beiden Clustern auszuführen. NetApp empfiehlt nachdrücklich, auf beiden Clustern dieselben Schlüsselserver zu verwenden.

Sekundäre Schlüsselserver zu einem vorhandenen primären Schlüsselserver hinzufügen

Schritte

1. Den primären Schlüsselserver ändern, um sekundäre Schlüsselserver hinzuzufügen. Der `-secondary-key-servers` 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 im `-secondary-key-servers` Parameter keine Portnummer für sekundäre Schlüsselserver an. Es wird dieselbe Portnummer wie für primäre Schlüsselserver verwendet.

> Wenn Sie den `security key-manager external modify-server` Befehl für die administrative SVM in einer MetroCluster Konfiguration ausführen, muss der

Befehl auf beiden Clustern ausgeführt werden. Wenn Sie den Befehl für eine einzelne Daten-SVM ausführen, ist es nicht erforderlich, den Befehl auf beiden Clustern auszuführen. NetApp empfiehlt nachdrücklich, auf beiden Clustern dieselben Schlüsselserver zu verwenden.

Weitere Informationen zu sekundären Schlüsselservern sind unter [mod-secondary] zu finden.

Gruppierte Schlüsselserver ändern

Sie können gruppierte externe Schlüsselserver modifizieren, indem Sie sekundäre Schlüsselserver hinzufügen oder entfernen, die Zugriffsreihenfolge der sekundären Schlüsselserver ändern oder die Bezeichnung (primär oder sekundär) bestimmter Schlüsselserver ändern. Wenn gruppierte externe Schlüsselserver in einer MetroCluster Konfiguration modifiziert werden, empfiehlt NetApp nachdrücklich, in beiden Clustern dieselben Schlüsselserver zu verwenden.

Sekundäre Schlüsselserver ändern

Der `-secondary-key-servers`Parameter des `security key-manager external modify-server`Befehls dient zur Verwaltung sekundärer Schlüsselserver. Der `-secondary-key-servers`Parameter akzeptiert eine durch Kommas getrennte Liste. Die angegebene Reihenfolge der sekundären Schlüsselserver in der Liste bestimmt die Zugriffsreihenfolge für die sekundären Schlüsselserver. Die Zugriffsreihenfolge kann geändert werden, indem der Befehl `security key-manager external modify-server`mit einer anderen Reihenfolge der sekundären Schlüsselserver ausgeführt wird. Für sekundäre Schlüsselserver darf keine Portnummer angegeben werden.

Wenn Sie den `security key-manager external modify-server` Befehl für die administrative SVM in einer MetroCluster Konfiguration ausführen, muss der Befehl auf beiden Clustern ausgeführt werden. Wenn Sie den Befehl für eine einzelne Daten-SVM ausführen, ist es nicht erforderlich, den Befehl auf beiden Clustern auszuführen.

Um einen sekundären Schlüsselserver zu entfernen, die Schlüsselserver, die beibehalten werden sollen, im `-secondary-key-servers` Parameter angeben und den zu entfernenden Server weglassen. Um alle sekundären Schlüsselserver zu entfernen, das Argument – verwenden, was bedeutet, dass keiner angegeben wird.

Primär- und Sekundärschlüsselserver konvertieren

Mit den folgenden Schritten lässt sich die Bezeichnung (primär oder sekundär) bestimmter Schlüsselserver ändern.

Einen primären Schlüsselserver in einen sekundären Schlüsselserver konvertieren

Schritte

1. Entfernung des primären Schlüsselservers aus der SVM:

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

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

2. Das Einen gruppierten Schlüsselserver erstellenVerfahren wird unter Verwendung des ehemaligen primären Schlüsselservers als sekundärer Schlüsselserver durchgeführt.

Einen sekundären Schlüsselserver in einen primären Schlüsselserver umwandeln

Schritte

1. Entfernung des sekundären Schlüsselservers von seinem bestehenden primären Schlüsselserver:

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

- Wenn Sie den `security key-manager external modify-server -secondary-key-servers` Befehl für die administrative SVM in einer MetroCluster Konfiguration ausführen, muss der Befehl auf beiden Clustern ausgeführt werden. Wenn Sie den Befehl für eine einzelne Daten-SVM ausführen, ist es nicht erforderlich, den Befehl auf beiden Clustern auszuführen.
- Wenn ein sekundärer Schlüsselserver in einen primären Schlüsselserver umgewandelt wird, während ein vorhandener Schlüsselserver entfernt wird, kann das Hinzufügen eines neuen Schlüsselservers vor Abschluss der Entfernung und Umwandlung zur Duplizierung von Schlüsseln führen.

1. Das Einen gruppierten Schlüsselserver erstellenVerfahren wird durchgeführt, wobei der ehemalige sekundäre Schlüsselserver als primärer Schlüsselserver des neuen Cluster-Schlüsselservers verwendet wird.

Weitere Informationen finden Sie unter [mod-secondary].

Verwandte Informationen

- Weitere Informationen zu `security key-manager external` finden Sie im "ONTAP-Befehlsreferenz"

Authentifizierungsschlüssel in ONTAP 9.6 und höher erstellen

Mit dem `security key-manager key create`Befehl lassen sich die Authentifizierungsschlüssel für einen Knoten erstellen und auf den konfigurierten KMIP-Servern speichern.

Über diese Aufgabe

Wenn Ihre Sicherheitskonfiguration die Verwendung unterschiedlicher Schlüssel für die Authentifizierung von Daten und die FIPS 140-2 Authentifizierung erfordert, sollte für jeden Zweck ein separater Schlüssel erstellt werden. Ist dies nicht der Fall, kann derselbe Authentifizierungsschlüssel für die FIPS-Konformität verwendet werden, der auch für den Datenzugriff genutzt wird.

ONTAP erstellt Authentifizierungsschlüssel für alle Knoten im Cluster.

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

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

- Sie erhalten eine Warnung, wenn die konfigurierten Schlüsselverwaltungsserver bereits mehr als 128 Authentifizierungsschlüssel speichern.
- Sie können den `security key-manager key delete`Befehl verwenden, um nicht verwendete Schlüssel zu löschen. Der `security key-manager key delete`Befehl schlägt fehl, wenn der angegebene Schlüssel derzeit von ONTAP verwendet wird. (Es sind höhere Berechtigungen als `admin` erforderlich, um diesen Befehl zu verwenden.)



In einer MetroCluster Umgebung muss vor dem Löschen eines Schlüssels sichergestellt werden, dass der Schlüssel im Partnercluster nicht verwendet wird. Mit den folgenden Befehlen im Partnercluster lässt sich 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 Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Die Authentifizierungsschlüssel für Clusterknoten erstellen:

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



Das Setzen von `prompt-for-key=true` bewirkt, dass das System den Clusteradministrator zur Eingabe der Passphrase auffordert, die bei der Authentifizierung verschlüsselter Laufwerke verwendet wird. Andernfalls generiert das System automatisch eine 32-Byte-Passphrase. Der `security key-manager key create` Befehl ersetzt den `security key-manager create-key` Befehl. Weitere Informationen zu `security key-manager key create` finden sich in der "ONTAP-Befehlsreferenz".

Das folgende Beispiel erstellt die Authentifizierungsschlüssel für `cluster1`, wobei automatisch eine 32-Byte-Passphrase generiert wird:

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

2. Es sollte überprüft werden, ob 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 zur Referenzierung des Authentifizierungsschlüssels verwendet wird. Es handelt sich nicht um den eigentlichen

Authentifizierungsschlüssel oder den Datenverschlüsselungsschlüssel.

Das folgende Beispiel überprüft, ob Authentifizierungsschlüssel für `cluster1` erstellt 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>
```

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

Verwandte Informationen

- "storage encryption Disk anzeigen"

Authentifizierungsschlüssel in ONTAP 9.5 und früher erstellen

Mit dem `security key-manager create-key`Befehl lassen sich die Authentifizierungsschlüssel für einen Knoten erstellen und auf den konfigurierten KMIP-Servern speichern.

Über diese Aufgabe

Wenn Ihre Sicherheitskonfiguration die Verwendung unterschiedlicher Schlüssel für die Authentifizierung von Daten und die FIPS 140-2 Authentifizierung erfordert, sollte für jeden Zweck ein separater Schlüssel erstellt werden. Ist dies nicht der Fall, kann derselbe Authentifizierungsschlüssel für die FIPS-Konformität verwendet werden, der auch für den Datenzugriff genutzt wird.

ONTAP erstellt Authentifizierungsschlüssel für alle Knoten im Cluster.

- Dieser Befehl wird nicht unterstützt, wenn die Onboard-Schlüsselverwaltung aktiviert ist.
- Sie erhalten eine Warnung, wenn die konfigurierten Schlüsselverwaltungsserver bereits mehr als 128 Authentifizierungsschlüssel speichern.

  Sie können die Key-Management-Server-Software verwenden, um nicht verwendete Schlüssel zu löschen und dann den Befehl erneut auszuführen.

Bevor Sie beginnen

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

Schritte

1. Die Authentifizierungsschlüssel für Clusterknoten erstellen:

   `security key-manager create-key`

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

   > Die in der Ausgabe angezeigte Schlüssel-ID ist eine Kennung, die zur Referenzierung des Authentifizierungsschlüssels verwendet wird. Es handelt sich nicht um den eigentlichen Authentifizierungsschlüssel oder den Datenverschlüsselungsschlüssel.

   Das folgende Beispiel erstellt die Authentifizierungsschlüssel für `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. Es sollte überprüft werden, ob die Authentifizierungsschlüssel erstellt wurden:

   `security key-manager query`

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

   Das folgende Beispiel überprüft, ob Authentifizierungsschlüssel für `cluster1` erstellt 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>
```

Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder ONTAP SED

Mit dem `storage encryption disk modify` Befehl lässt sich einem FIPS-Laufwerk oder SED ein Datenauthentifizierungsschlüssel zuweisen. Clusterknoten verwenden diesen Schlüssel, um verschlüsselte Daten auf dem Laufwerk zu sperren oder zu entsperren.

Über diese Aufgabe

Ein Self-Encrypting Drive ist nur dann vor unberechtigtem Zugriff geschützt, wenn seine Authentifizierungsschlüssel-ID auf einen Wert ungleich dem Standardwert gesetzt ist. Die Hersteller Secure ID (MSID) mit der Schlüssel-ID 0x0 ist der Standardwert für SAS-Laufwerke. Für NVMe-Laufwerke ist der Standardwert ein Nullschlüssel, dargestellt als leere Schlüssel-ID. Wird die Schlüssel-ID einem Self-Encrypting Drive zugewiesen, ändert das System dessen Authentifizierungsschlüssel-ID auf einen Wert ungleich dem Standardwert.

Dieses Verfahren ist nicht unterbrechend.

Bevor Sie beginnen

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

Schritte

1. Einem FIPS-Laufwerk oder SED einen Authentifizierungsschlüssel für Daten zuweisen:

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

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

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

```
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. Überprüfen, ob die Authentifizierungsschlüssel zugewiesen wurden:

   `storage encryption disk show`

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

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
[...]
```

Verwandte Informationen

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

Onboard-Schlüsselverwaltung konfigurieren

Integrierte Schlüsselverwaltung in ONTAP 9.6 und höher aktivieren

Mit dem Onboard Key Manager können Clusterknoten gegenüber einem FIPS-Laufwerk oder SED authentifiziert werden. Der Onboard Key Manager ist ein integriertes Tool, das Authentifizierungsschlüssel für Knoten aus demselben Speichersystem bereitstellt wie Ihre Daten. Der Onboard Key Manager ist FIPS-140-2 Level 1-konform.

Mit dem Onboard Key Manager können Sie die Schlüssel sichern, die der Cluster für den Zugriff auf verschlüsselte Daten verwendet. Der Onboard Key Manager muss auf jedem Cluster aktiviert sein, der 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 Knoten hinzufügen. In MetroCluster Konfigurationen müssen Sie `security key-manager onboard enable` zuerst auf dem lokalen Cluster und anschließend `security key-manager onboard sync` auf dem Remote-Cluster ausführen, wobei jeweils dieselbe Passphrase verwendet werden muss.

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

Standardmäßig ist die Eingabe der Passphrase für den Schlüsselmanager beim Neustart eines Knotens nicht erforderlich. Außer bei MetroCluster kann die `cc-mode-enabled=yes` Option verwendet werden, 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`, ändert sich das Systemverhalten wie folgt:

- Das System überwacht im Common Criteria-Modus aufeinanderfolgende fehlgeschlagene Cluster-Passphrasenversuche.

  Wenn NetApp Storage Encryption (NSE) aktiviert ist und die korrekte Cluster-Passphrase beim Systemstart nicht eingegeben wird, kann sich das System nicht an seinen Laufwerken authentifizieren und startet automatisch neu. Um dies zu korrigieren, ist die korrekte Cluster-Passphrase an der Boot-Eingabeaufforderung einzugeben. Nach dem Start erlaubt das System innerhalb eines Zeitraums von 24 Stunden bis zu 5 aufeinanderfolgende Versuche, die Cluster-Passphrase für jeden Befehl, der die Cluster-Passphrase als Parameter benötigt, korrekt einzugeben. Wird das Limit erreicht (zum Beispiel wenn die Cluster-Passphrase 5-mal hintereinander falsch eingegeben wurde), muss entweder das Ablaufintervall von 24 Stunden (Zeitüberschreitung) abgewartet oder der Node neu gestartet werden, um das Limit zurückzusetzen.

- Systemabbildaktualisierungen verwenden das NetApp RSA-3072-Codesignaturzertifikat zusammen mit SHA-384-codesignierten Digests zur Überprüfung der Abbildintegrität, anstelle des üblichen NetApp RSA-2048-Codesignaturzertifikats und SHA-256-codesignierten Digests.

  Der Upgrade-Befehl überprüft anhand verschiedener digitaler Signaturen, ob der Image-Inhalt verändert oder beschädigt wurde. Wenn die Validierung erfolgreich ist, geht das Image-Update zum nächsten Schritt über. Wenn die Validierung nicht erfolgreich ist, schlägt das Image-Update fehl. Weitere Informationen zu `cluster image` finden sich in der "ONTAP-Befehlsreferenz".

Der integrierte Schlüsselmanager speichert Schlüssel im flüchtigen Speicher. Der Inhalt des flüchtigen Speichers wird beim Neustart oder Anhalten des Systems gelöscht. Unter normalen Betriebsbedingungen wird der Inhalt des flüchtigen Speichers innerhalb von 30 Sekunden nach dem Anhalten des Systems gelöscht.

Bevor Sie beginnen

- Wenn Sie NSE mit einem externen Schlüsselverwaltungsserver (KMIP) verwenden, muss die externe Schlüsselverwaltungsdatenbank gelöscht worden sein.

  "Umstellung vom externen auf das integrierte Schlüsselmanagement"

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Die MetroCluster Umgebung muss konfiguriert werden, bevor der Onboard Key Manager konfiguriert wird.

Schritte

1. Starten Sie den Befehl zum Einrichten des Schlüsselmanagers:

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

   > Setzen Sie `cc-mode-enabled=yes` so, dass Benutzer nach einem Neustart die Passphrase des Schlüsselmanagers 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 zur Einrichtung des Schlüsselmanagers auf cluster1, ohne dass die Passphrase nach jedem Neustart eingegeben werden muss:

2. Geben Sie eine Passphrase mit 32 bis 256 Zeichen ein oder für “cc-mode” eine Passphrase mit 64 bis 256 Zeichen.

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

3. Bei der Aufforderung zur Passphrase-Bestätigung wird die Passphrase erneut eingegeben.
4. Überprüfen, 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.

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

Nachdem Sie fertig sind

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

Das System sichert wichtige Verwaltungsinformationen automatisch in der replizierten Datenbank (RDB) für den Cluster. Diese Informationen sollten für die Notfallwiederherstellung zusätzlich manuell gesichert werden.

Verwandte Informationen

- "Cluster Image-Befehle"
- "security key-manager external enable"
- "security key-manager key query"
- "security key-manager onboard enable"
- "Umstellung vom externen auf das integrierte Schlüsselmanagement"

Integrierte Schlüsselverwaltung in ONTAP 9.5 und früher aktivieren

Mit dem Onboard Key Manager können Clusterknoten gegenüber einem FIPS-Laufwerk oder SED authentifiziert werden. Der Onboard Key Manager ist ein integriertes Tool, das Authentifizierungsschlüssel für Knoten aus demselben Speichersystem bereitstellt wie Ihre Daten. Der Onboard Key Manager ist FIPS-140-2 Level 1-konform.

Mit dem Onboard Key Manager können Sie die Schlüssel sichern, die der Cluster für den Zugriff auf verschlüsselte Daten verwendet. Der Onboard Key Manager ist auf jedem Cluster zu aktivieren, 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 Knoten hinzufügen.

Bei einer MetroCluster Konfiguration gelten folgende Richtlinien:

- In ONTAP 9.5 muss `security key-manager setup` auf dem lokalen Cluster und `security key-manager setup -sync-metrocluster-config yes` auf dem Remote-Cluster ausgeführt werden, wobei auf beiden Clustern dieselbe Passphrase verwendet wird.
- Vor ONTAP 9.5 muss `security key-manager setup` auf dem lokalen Cluster ausgeführt werden, etwa 20 Sekunden gewartet werden und dann `security key-manager setup` auf dem Remote-Cluster ausgeführt werden, wobei jeweils die gleiche Passphrase verwendet wird.

Standardmäßig ist die Eingabe der Passphrase für den Schlüsselmanager beim Neustart eines Knotens nicht erforderlich. Ab ONTAP 9.4 kann die `-enable-cc-mode yes` Option verwendet werden, um zu verlangen, dass Benutzer die Passphrase nach einem Neustart eingeben.

Für NVE: Wenn `-enable-cc-mode yes` gesetzt ist, werden Volumes, die Sie mit den Befehlen `volume create` und `volume move start` erstellen, automatisch verschlüsselt. Für `volume create` muss `-encrypt true` nicht angegeben werden. Für `volume move start` muss `-encrypt-destination true` nicht angegeben werden.

Nach einem fehlgeschlagenen Passphrase-Versuch ist ein erneuter Neustart des Knotens erforderlich.

Bevor Sie beginnen

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

  "Umstellung vom externen auf das integrierte Schlüsselmanagement"

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Die MetroCluster Umgebung wird konfiguriert, bevor der Onboard Key Manager konfiguriert wird.

Schritte

1. Die Einrichtung des Schlüsselmanagers wird gestartet:

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

   Ab ONTAP 9.4 kann die `-enable-cc-mode yes` Option verwendet werden, um zu

verlangen, dass Benutzer nach einem Neustart die Passphrase des Schlüsselmanagers eingeben. Für NVE: Wenn `-enable-cc-mode yes` gesetzt ist, werden Volumes, die Sie mit den Befehlen `volume create` und `volume move start` erstellen, automatisch verschlüsselt.

Das folgende Beispiel zeigt den Beginn der Einrichtung des Schlüsselmanagers auf Cluster1, 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. Bei der Aufforderung zur Eingabe der Passphrase ist eine Passphrase mit 32 bis 256 Zeichen einzugeben, oder für “cc-mode” eine Passphrase mit 64 bis 256 Zeichen.

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

4. Bei der Aufforderung zur Passphrase-Bestätigung wird die Passphrase erneut eingegeben.
5. Überprüfen, ob die Schlüssel für alle Knoten konfiguriert sind:

   `security key-manager show-key-store`

   Weitere Informationen zu `security key-manager show-key-store` finden sich in der "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 automatisch wichtige Verwaltungsinformationen in der replizierten Datenbank (RDB) für den Cluster.

Nachdem die Passphrase des Onboard Key Managers konfiguriert wurde, sollten die Informationen manuell an einem sicheren Ort außerhalb des Speichersystems gesichert werden. Siehe "Onboard-Schlüsselverwaltungsinformationen manuell sichern".

Verwandte Informationen

- "Onboard-Schlüsselverwaltungsinformationen manuell sichern"
- "security key-manager setup"
- "security key-manager show-key-store"
- "Umstellung vom externen auf das integrierte Schlüsselmanagement"

Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder ONTAP SED

Mit dem `storage encryption disk modify` Befehl lässt sich einem FIPS-Laufwerk oder SED ein Datenauthentifizierungsschlüssel zuweisen. Clusterknoten verwenden diesen Schlüssel, um auf die Daten auf dem Laufwerk zuzugreifen.

Über diese Aufgabe

Ein Self-Encrypting Drive ist nur dann vor unberechtigtem Zugriff geschützt, wenn seine Authentifizierungsschlüssel-ID auf einen Wert ungleich dem Standardwert gesetzt ist. Die Hersteller Secure ID (MSID) mit der Schlüssel-ID 0x0 ist der Standardwert für SAS-Laufwerke. Für NVMe-Laufwerke ist der Standardwert ein Nullschlüssel, dargestellt als leere Schlüssel-ID. Wird die Schlüssel-ID einem Self-Encrypting Drive zugewiesen, ändert das System dessen Authentifizierungsschlüssel-ID auf einen Wert ungleich dem Standardwert.

Bevor Sie beginnen

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

Schritte

1. Einem FIPS-Laufwerk oder SED einen Authentifizierungsschlüssel für Daten zuweisen:

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

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

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

```
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.
```

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

2. Überprüfen, ob die Authentifizierungsschlüssel zugewiesen wurden:

   `storage encryption disk show`

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

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
[...]
```

Verwandte Informationen

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

Einem ONTAP FIPS-Laufwerk einen FIPS 140-2-Authentifizierungsschlüssel zuweisen

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. Clusterknoten verwenden diesen Schlüssel für Laufwerksvorgänge, die nicht dem Datenzugriff dienen, wie zum Beispiel zur Verhinderung von Denial-of-Service-Angriffen auf das Laufwerk.

Über diese Aufgabe

Ihre Sicherheitskonfiguration erfordert möglicherweise die Verwendung unterschiedlicher Schlüssel für die Authentifizierung und die FIPS 140-2-Authentifizierung. Ist dies nicht der Fall, kann derselbe Authentifizierungsschlüssel für die FIPS-Konformität verwendet werden, der auch für den Datenzugriff genutzt

wird.

Dieses Verfahren ist nicht unterbrechend.

Bevor Sie beginnen

Die Laufwerksfirmware muss die FIPS-140-2-Konformität unterstützen. Die "NetApp Interoperabilitätsmatrix-Tool" enthält Informationen zu unterstützten Laufwerksfirmwareversionen.

Schritte

1. Zunächst muss sichergestellt sein, dass ein Authentifizierungsschlüssel zugewiesen wurde. Dies kann mithilfe eines externer Schlüsselmanager oder eines Onboard Key Manager erfolgen. Die Zuweisung des Schlüssels lässt sich mit dem Befehl `storage encryption disk show` überprüfen.
2. Einem FIPS 140-2-Authentifizierungsschlüssel SEDs zuweisen:

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

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

   ```
   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. Es sollte überprüft werden, ob der Authentifizierungsschlüssel zugewiesen wurde:

   `storage encryption disk show -fips`

   Weitere Informationen zu `storage encryption disk show` finden sich 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 Festplatte ändern"
- "storage encryption Disk anzeigen"
- "storage encryption disk show-status"

Clusterweiten FIPS-konformen Modus für KMIP-Verbindungen in ONTAP aktivieren

Sie können den `security config modify` Befehl mit der `-is-fips-enabled` Option verwenden, um den clusterweiten FIPS-konformen Modus für Daten während der Übertragung zu aktivieren. Dadurch verwendet der Cluster OpenSSL im FIPS-Modus, wenn eine Verbindung zu KMIP-Servern besteht.

Über diese Aufgabe

Wenn der clusterweite FIPS-konforme Modus aktiviert ist, verwendet der Cluster automatisch ausschließlich TLS 1.2 und FIPS-validierte Cipher Suites. Der clusterweite FIPS-konforme Modus ist standardmäßig deaktiviert.

Nach der Änderung der clusterweiten Sicherheitskonfiguration ist ein manueller Neustart der Clusterknoten erforderlich.

Bevor Sie beginnen

- Der Speichercontroller 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 herzustellen, wenn der clusterweite FIPS-konforme Modus aktiviert ist.

Schritte

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

   ```
   set -privilege advanced
   ```

2. Überprüfen, ob TLSv1.2 unterstützt wird:

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

   Weitere Informationen zu `security config show` finden sich 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. Clusterweiter FIPS-konformer Modus:

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

   Weitere Informationen zu `security config modify` finden sich in der "ONTAP-Befehlsreferenz".

4. Cluster-Knoten manuell neu starten.
5. Es sollte überprüft werden, ob der clusterweite FIPS-konforme 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
```

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.