

## Externes Verschlüsselungsmanagement konfigurieren

ONTAP 9

NetApp April 24, 2024

This PDF was generated from https://docs.netapp.com/de-de/ontap/encryption-at-rest/configure-external-key-management-concept.html on April 24, 2024. Always check docs.netapp.com for the latest.

### Inhalt

Externes Verschlüsselungsmanagement konfigurieren 1
Externes Verschlüsselungsmanagement – Übersicht konfigurieren
Erfassen Sie Netzwerkinformationen in ONTAP 9.2 und früher
Installieren Sie SSL-Zertifikate auf dem Cluster
Externes Verschlüsselungsmanagement in ONTAP 9.6 und höher (HW-basiert)
Ermöglichen Sie externes Verschlüsselungsmanagement in ONTAP 9.5 und früher
Konfigurieren Sie externe geclusterte Schlüsselserver
Erstellen Sie Authentifizierungsschlüssel in ONTAP 9.6 und höher.
Erstellen Sie Authentifizierungsschlüssel in ONTAP 9.5 und früher
Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder einer SED (External
Key Management)

# Externes Verschlüsselungsmanagement konfigurieren

## Externes Verschlüsselungsmanagement – Übersicht konfigurieren

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.

Bei ONTAP 9.1 und älteren Versionen müssen Node-Management-LIFs Ports zugewiesen werden, die mit der Node-Managementrolle konfiguriert sind, bevor Sie den externen Schlüsselmanager verwenden können.

NetApp Volume Encryption (NVE) kann mit Onboard Key Manager in ONTAP 9.1 und höher 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.

## Erfassen Sie Netzwerkinformationen in ONTAP 9.2 und früher

Wenn Sie ONTAP 9.2 oder eine frühere Version verwenden, sollten Sie das Arbeitsblatt zur Netzwerkkonfiguration ausfüllen, bevor Sie die externe Schlüsselverwaltung aktivieren.



Ab ONTAP 9.3 erkennt das System automatisch alle benötigten Netzwerkinformationen.

Element	Hinweise	Wert
Name der Key-Management- Netzwerkschnittstelle		
IP-Adresse für die wichtige Management-Netzwerkschnittstelle	IP-Adresse der LIF für das Node- Management im IPv4- oder IPv6- Format	
Key-Management- Netzwerkschnittstelle IPv6-Netzwerk- Präfixlänge	Wenn Sie IPv6 verwenden, Länge des IPv6-Netzwerkpräfixes	
Subnetzmaske für das Schlüsselmanagement-Netzwerk- Interface		

Gateway-IP-Adresse für die wichtige Management-Netzwerkschnittstelle		
IPv6-Adresse für die Cluster- Netzwerkschnittstelle	Nur erforderlich, wenn Sie IPv6 für die Netzwerkschnittstelle des Verschlüsselungsmanagements verwenden	
Port-Nummer für jeden KMIP-Server	Optional Die Portnummer muss für alle KMIP-Server identisch sein. Wenn Sie keine Portnummer angeben, wird standardmäßig der Port 5696 verwendet. Dies ist der für KMIP zugewiesene Port (Internet Assigned Numbers Authority, IANA).	
Tag-Schlüsselname	Optional Der Key-Tag-Name wird verwendet, um alle Schlüssel zu einem Knoten zu identifizieren. Der Standardname für das Tag der Schlüssel ist der Node-Name.	

#### Verwandte Informationen

"Technischer Bericht 3954 von NetApp: Vorherige Installation der NetApp Storage Encryption Anforderungen und Verfahren für IBM Tivoli Lifetime Key Manager"

"Technischer Bericht 4074 von NetApp: Vorabinstallation der Anforderungen und Verfahren für SafeNet KeySecure"

### Installieren Sie SSL-Zertifikate auf dem 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

### Externes Verschlüsselungsmanagement in ONTAP 9.6 und höher (HW-basiert)

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 pro Primärschlüsselserver bis zu 3 sekundäre 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.
- Sie müssen die MetroCluster Umgebung konfigurieren, bevor Sie einen externen Schlüsselmanager konfigurieren.
- In einer MetroCluster-Umgebung müssen Sie das KMIP SSL-Zertifikat auf beiden Clustern 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 Mit dem Befehl wird der ersetzt security key-manager setup Befehl. Sie können die ausführen security keymanager external modify Befehl zum Ändern der Konfiguration für das externe Verschlüsselungsmanagement. Eine vollständige Befehlssyntax finden Sie in den man-Pages.
- Wenn Sie in einer MetroCluster-Umgebung externes Verschlüsselungsmanagement für den Administrator-SVM konfigurieren, müssen Sie die wiederholen security keymanager external enable Befehl auf dem Partner-Cluster.

Mit dem folgenden Befehl wird die externe Schlüsselverwaltung für aktiviert cluster1 Mit drei externen Schlüsselservern zu verwenden. 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:

```
clusterl::> 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|notresponding|unknown



Der security key-manager external show-status Mit dem Befehl wird der ersetzt security key-manager show -status Befehl. Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
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.
```

### Ermöglichen Sie externes Verschlüsselungsmanagement 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 das 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 den folgenden Befehl auf beiden Clustern ausführen.

- 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
```

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster1::> security key-manager show -status
Node
                     Registered Key Manager Status
             Port
_____ ____
                     _____
                                         _____
cluster1-01 5696
                     20.1.1.1
                                         available
                     20.1.1.2
cluster1-01
            5696
                                         available
cluster1-02 5696
                     20.1.1.1
                                         available
cluster1-02
                     20.1.1.2
                                         available
            5696
```

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.

### Konfigurieren Sie externe geclusterte Schlüsselserver

Ab ONTAP 9.11.1 können Sie die Konnektivität mit externen Verschlüsselungsmanagement-Servern auf einer SVM konfigurieren. Mit geclusterten Key Servern können Sie primäre und sekundäre Schlüsselserver auf einer SVM zuweisen. Bei der Registrierung von Schlüsseln versucht ONTAP zuerst, auf einen primären Schlüsselserver zuzugreifen, bevor nacheinander versucht wird, auf sekundäre Server zuzugreifen, bis der Vorgang erfolgreich abgeschlossen ist. Dadurch wird die Duplizierung von Schlüsseln verhindert.

Externe Schlüsselserver können für NSE-, NVE-, NAE- und SED-Schlüssel verwendet werden. Eine SVM kann bis zu vier primäre externe KMIP-Server unterstützen. Jeder primäre Server kann bis zu drei sekundäre Schlüsselserver unterstützen.

#### **Bevor Sie beginnen**

- "KMIP-Verschlüsselungsmanagement muss für die SVM aktiviert sein".
- Dieser Prozess unterstützt nur wichtige Server, die KMIP verwenden. Eine Liste der unterstützten Schlüsselserver finden Sie in "NetApp Interoperabilitäts-Matrix-Tool".
- Alle Nodes im Cluster müssen ONTAP 9.11.1 oder höher ausführen.
- In der Reihenfolge der Server sind die Argumente im aufgelistet -secondary-key-servers Der Parameter gibt die Zugriffsreihenfolge der KMIP-Server (External Key Management) wieder.

#### 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

- Vergewissern Sie sich, dass für das Cluster kein Verschlüsselungsmanagement aktiviert wurde: security key-manager external show -vserver svm\_name Wenn für die SVM bereits maximal vier primäre Schlüsselserver aktiviert sind, müssen Sie einen der vorhandenen primären Schlüsselserver entfernen, bevor Sie einen neuen hinzufügen.
- 2. Aktivieren Sie den primären Schlüsselmanager: security key-manager external enable -vserver svm\_name -key-servers server\_ip -client-cert client\_cert\_name -server-ca-certs server ca cert names
- 3. Ändern Sie den primären Schlüsselserver, um sekundäre Schlüsselserver hinzuzufügen. Der -secondary-key-servers Der Parameter akzeptiert eine kommagetrennte Liste mit 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
```

#### Fügen Sie einem vorhandenen primären Schlüsselserver sekundäre Schlüsselserver hinzu

1. Ändern Sie den primären Schlüsselserver, um sekundäre Schlüsselserver hinzuzufügen. Der -secondary-key-servers Der Parameter akzeptiert eine kommagetrennte Liste mit 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* Weitere Informationen zu sekundären Schlüsselservern finden Sie unter [mod-secondary].

#### Cluster-Key-Server ändern

Sie können externe Schlüsselserver-Cluster ändern, indem Sie den Status (primäre oder sekundäre) bestimmter Schlüsselserver ändern, sekundäre Schlüsselserver hinzufügen und entfernen oder die Zugriffsreihenfolge von sekundären Schlüsselservern ändern.

#### Konvertieren Sie primäre und sekundäre Schlüsselserver

Um einen primären Schlüsselserver in einen sekundären Schlüsselserver zu konvertieren, müssen Sie ihn zuerst mit der von der SVM entfernen security key-manager external remove-servers Befehl.

Um einen sekundären Schlüsselserver in einen primären Schlüsselserver zu konvertieren, müssen Sie zuerst den sekundären Schlüsselserver vom vorhandenen primären Schlüsselserver entfernen. Siehe [mod-secondary]. Wenn Sie einen sekundären Schlüsselserver beim Entfernen eines vorhandenen Schlüssels in einen primären Server konvertieren, kann der Versuch, einen neuen Server hinzuzufügen, bevor Sie den Schlüssel entfernen und konvertieren, zu einer doppelten Tastenanfügung führen.

#### Ändern Sie sekundäre Schlüsselserver

Sekundäre Schlüsselserver werden mit dem verwaltet -secondary-key-servers Parameter von security key-manager external modify-server Befehl. Der -secondary-key-servers Parameter akzeptiert eine kommagetrennte Liste. Die angegebene Reihenfolge der sekundären Schlüsselserver in der Liste bestimmt die Zugriffssequenz für die sekundären Schlüsselserver. Die Zugriffsreihenfolge kann durch Ausführen des Befehls geändert werden security key-manager external modify-server Bei der Eingabe der sekundären Schlüssel-Server in einer anderen Reihenfolge.

Um einen sekundären Schlüsselserver zu entfernen, wird der verwendet -secondary-key-servers Argumente sollten die wichtigsten Server enthalten, die Sie beibehalten möchten, während Sie die zu entfernenden nicht zulassen. Um alle sekundären Schlüsselserver zu entfernen, verwenden Sie das Argument -, Keine zu deuten.

Weitere Informationen finden Sie im security key-manager external Auf der "Befehlsreferenz für ONTAP".

### Erstellen Sie Authentifizierungsschlüssel in ONTAP 9.6 und höher

Sie können das verwenden security key-manager key create Befehl zum Erstellen der Authentifizierungsschlüssel für einen Node und Speichern auf den konfigurierten KMIP-Servern.

#### 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:

- Sie erhalten eine Warnung, wenn auf den konfigurierten Schlüsselverwaltungsservern bereits mehr als 128 Authentifizierungsschlüssel gespeichert werden.
- Sie können das verwenden security key-manager key delete Befehl zum Löschen von nicht verwendeten Schlüsseln. Der security key-manager key delete Befehl schlägt fehl, wenn der angegebene Schlüssel derzeit von ONTAP verwendet wird. (Sie müssen über mehr als "admin" verfügen, um diesen Befehl verwenden zu können.)

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:



#### 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
```



Einstellung prompt-for-key=true Bewirkt, dass das System den Cluster-Administrator zur Verwendung der Passphrase bei der Authentifizierung verschlüsselter Laufwerke auffordert. Andernfalls generiert das System automatisch eine 32-Byte-Passphrase. Der security key-manager key create Mit dem Befehl wird der ersetzt security keymanager create-key Befehl. Eine vollständige Befehlssyntax finden Sie in der man-Page.

Im folgenden Beispiel werden die Authentifizierungsschlüssel für erstellt cluster1, Automatisch eine 32-Byte-Passphrase generieren:

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

security key-manager key query -node node



Der security key-manager key query Mit dem Befehl wird der ersetzt security key-manager query key Befehl. Eine vollständige Befehlssyntax finden Sie in der man-Page. 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 wurden cluster1:

```
cluster1::> security key-manager key query
   Vserver: cluster1
 Key Manager: external
    Node: node1
Key Tag
                 Key Type Restored
_____
                 _____ ____
                  NSE-AK yes
node1
 Key ID:
00000000
                 NSE-AK yes
node1
 Key ID:
00000000
  Vserver: cluster1
 Key Manager: external
    Node: node2
Key Tag
               Key Type Restored
_____
                 _____
                  NSE-AK yes
node2
 Key ID:
00000000
node2
                 NSE-AK yes
 Key ID:
00000000
```

## Erstellen Sie Authentifizierungsschlüssel in ONTAP 9.5 und früher

Sie können das verwenden security key-manager create-key Befehl zum Erstellen der Authentifizierungsschlüssel für einen Node und Speichern auf den

#### konfigurierten KMIP-Servern.

#### 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
```

Eine vollständige Befehlssyntax finden Sie in der man-Page für den 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 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: F1CB30AFF1CB30B001010000000000A68B167F92DD54196297159B5968923C
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

Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

```
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:
F1CB30AFF1CB30B001010000000000000068B167F92DD54196297159B5968923C
        Node: cluster1-02
  Key Manager: 20.1.1.1
 Server Status: available
Key Tag Key Type Restored
----- -----
cluster1-02 NSE-AK yes
     Key ID:
F1CB30AFF1CB30B0010100000000000000068B167F92DD54196297159B5968923C
```

### Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder einer SED (External Key Management)

Sie können das verwenden storage encryption disk modify Befehl zum Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder einer SED. 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
```

Eine vollständige Befehlssyntax finden Sie in der man-Page für den Befehl.



Sie können das verwenden security key-manager query -key-type NSE-AK Befehl zum Anzeigen von Schlüssel-IDs.

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
F1CB30AFF1CB30B00101000000000000000868B167F92DD54196297159B5968923C
```

```
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

Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster1::> storage encryption disk show
Disk Mode Data Key ID
----- ----
0.0.0 data
F1CB30AFF1CB30B00101000000000000000068B167F92DD54196297159B5968923C
0.0.1 data
F1CB30AFF1CB30B00101000000000000068B167F92DD54196297159B5968923C
[...]
```

#### Copyright-Informationen

Copyright © 2024 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.