NVE konfigurieren

ONTAP 9

NetApp
February 12, 2026

Inhalt

NVE konfigurieren

Ermitteln Sie, ob Ihre ONTAP Clusterversion NVE unterstützt

Sie sollten vor der Installation der Lizenz festlegen, ob Ihre Cluster-Version NVE unterstützt. Sie können die `version` Cluster-Version mit dem Befehl bestimmen.

Über diese Aufgabe

Die Cluster-Version ist die niedrigste Version von ONTAP, die auf einem beliebigen Node im Cluster ausgeführt wird.

Schritte

1. Bestimmen Sie, ob Ihre Cluster-Version NVE unterstützt:

   ```
   version -v
   ```

   NVE wird nicht unterstützt, wenn in der Befehlsausgabe der Text angezeigt wird `1Ono-DARE` (für „Keine Data at Rest Encryption“) oder wenn Sie eine Plattform verwenden, die nicht in aufgeführt ist"Support-Details".

Installieren der Volume-Verschlüsselungslizenz auf einem ONTAP Cluster

Eine VE-Lizenz berechtigt Sie zur Nutzung der Funktion auf allen Knoten im Cluster. Diese Lizenz ist erforderlich, bevor Sie Daten mit NVE verschlüsseln können. Es ist im Lieferumfang enthalten"ONTAP One".

Vor ONTAP One war die VE-Lizenz im Verschlüsselungspaket enthalten. Das Encryption Bundle wird nicht mehr angeboten, ist aber weiterhin gültig. Obwohl derzeit nicht erforderlich, können Bestandskunden wählen"Upgrade auf ONTAP One".

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Sie müssen den VE-Lizenzschlüssel von Ihrem Vertriebsmitarbeiter erhalten haben oder ONTAP One installiert haben.

Schritte

1. "Überprüfen Sie, ob die VE-Lizenz installiert ist".

   Der Name des VE-Lizenzpakets lautet `VE`.

2. Wenn die Lizenz nicht installiert ist, "Verwenden Sie System Manager oder die ONTAP CLI, um sie zu installieren".

Externes Verschlüsselungsmanagement konfigurieren

Erfahren Sie mehr über die Konfiguration der externen Schlüsselverwaltung mit ONTAP NetApp Volume Encryption

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 für Knoten mithilfe des Key Management Interoperability Protocol (KMIP) bereitstellt. Zusätzlich zum Onboard Key Manager unterstützt ONTAP mehrere externe Schlüsselverwaltungsserver.

Ab ONTAP 9.10.1 können Sie Folgendes verwenden: Azure Key Vault oder Google Cloud Key Manager-Dienst zum Schutz Ihrer NVE-Schlüssel für Daten-SVMs. Ab ONTAP 9.11.1 können Sie mehrere externe Schlüsselmanager in einem Cluster konfigurieren. SehenKonfigurieren Sie gruppierte Schlüsselserver . Ab ONTAP 9.12.0 können Sie Folgendes verwenden: "KMS VON AWS" zum Schutz Ihrer NVE-Schlüssel für Daten-SVMs. Ab ONTAP 9.17.1 können Sie OpenStacks verwenden Barbican KMS zum Schutz Ihrer NVE-Schlüssel für Daten-SVMs.

Verwalten Sie externe Schlüsselmanager mit ONTAP System Manager

Ab ONTAP 9.7 können Sie die Authentifizierung und Verschlüsselung mit dem Onboard Key Manager speichern und managen. Ab ONTAP 9.13.1 können Sie diese Schlüssel auch mit externen Schlüsselmanagern speichern und verwalten.

Der integrierte Schlüsselmanager speichert und managt Schlüssel in einer sicheren, Cluster-internen Datenbank. Sein Umfang ist das Cluster. Ein externer Schlüsselmanager speichert und managt Schlüssel außerhalb des Clusters. Sein Umfang kann das Cluster oder die Storage-VM sein. Es können ein oder mehrere externe Schlüsselmanager verwendet werden. Es gelten die folgenden Bedingungen:

- Wenn der Onboard Key Manager aktiviert ist, kann ein externer Schlüsselmanager nicht auf Cluster-Ebene aktiviert werden, er kann jedoch auf Storage-VM-Ebene aktiviert werden.
- Wenn ein externer Schlüsselmanager auf Cluster-Ebene aktiviert ist, kann der Onboard Key Manager nicht aktiviert werden.

Beim Einsatz von externen Schlüsselmanagern können Sie bis zu vier primäre Schlüsselserver pro Storage-VM und Cluster registrieren. Jeder primäre Schlüsselserver kann mit bis zu drei sekundären Schlüsselservern gruppiert werden.

Konfigurieren Sie einen externen Schlüsselmanager

Zum Hinzufügen eines externen Schlüsselmanagers für eine Storage-VM sollten Sie beim Konfigurieren der Netzwerkschnittstelle für die Storage-VM ein optionales Gateway hinzufügen. Wenn die Speicher-VM ohne den Netzwerk-Route erstellt wurde, müssen Sie die Route explizit für den externen Schlüsselmanager erstellen. Siehe "LIF erstellen (Netzwerkschnittstelle)".

Schritte

Sie können einen externen Schlüsselmanager von verschiedenen Standorten in System Manager aus konfigurieren.

1. Führen Sie einen der folgenden Startschritte durch, um einen externen Schlüsselmanager zu

konfigurieren.

Workflow	Navigation	Startschritt
Konfigurieren Sie Key Manager	**Cluster** > **Einstellungen**	Blättern Sie zum Abschnitt **Sicherheit**. Wählen Sie unter **Verschlüsselung** ⚙. Wählen Sie **External Key Manager**.
Lokale Ebene hinzufügen	**Storage** > **Tiers**	Wählen Sie **+ Lokale Ebene Hinzufügen**. Aktivieren Sie das Kontrollkästchen „Key Manager konfigurieren“. Wählen Sie **External Key Manager**.
Storage vorbereiten	**Dashboard**	Wählen Sie im Abschnitt **Kapazität** die Option **Speicher vorbereiten** aus. Wählen Sie dann „Configure Key Manager“ aus. Wählen Sie **External Key Manager**.
Konfiguration der Verschlüsselung (nur Schlüsselmanager im Umfang von Storage-VMs)	**Storage** > **Storage VMs**	Wählen Sie die Storage-VM aus. Wählen Sie die Registerkarte **Einstellungen**. Wählen Sie im Abschnitt **Verschlüsselung** unter **Sicherheit** die Option ⚙.

2. Um einen primären Schlüsselserver hinzuzufügen, wählen Sie + Add , und füllen Sie die Felder **IP-Adresse oder Hostname** und **Port** aus.
3. Vorhandene installierte Zertifikate sind in den Feldern **KMIP Server CA Certificates** und **KMIP Client Certificate** aufgeführt. Sie können eine der folgenden Aktionen durchführen:
   - Wählen Sie diese Option ⌄ aus, um installierte Zertifikate auszuwählen, die dem Schlüsselmanager zugeordnet werden sollen. (Es können mehrere Service-CA-Zertifikate ausgewählt werden, es kann jedoch nur ein Client-Zertifikat ausgewählt werden.)
   - Wählen Sie **Neues Zertifikat hinzufügen**, um ein Zertifikat hinzuzufügen, das noch nicht installiert wurde, und ordnen Sie es dem externen Schlüsselmanager zu.
   - Wählen Sie neben dem Zertifikatnamen aus × , um installierte Zertifikate zu löschen, die Sie nicht dem externen Schlüsselmanager zuordnen möchten.
4. Um einen sekundären Schlüsselserver hinzuzufügen, wählen Sie **Add** in der Spalte **Secondary Key Server** aus und geben Sie seine Details an.
5. Wählen Sie **Speichern**, um die Konfiguration abzuschließen.

Bearbeiten Sie einen vorhandenen externen Schlüsselmanager

Wenn Sie bereits einen externen Schlüsselmanager konfiguriert haben, können Sie dessen Einstellungen ändern.

Schritte

1. Führen Sie einen der folgenden Startschritte durch, um die Konfiguration eines externen Schlüsselmanagers zu bearbeiten.

Umfang	Navigation	Startschritt

Externer Schlüsselmanager für den Clusterbereich	**Cluster** > **Einstellungen**	Blättern Sie zum Abschnitt **Sicherheit**. Wählen Sie unter **Verschlüsselung** ⋮, und wählen Sie dann **External Key Manager bearbeiten**.
Externer Schlüsselmanager für Storage VM	**Storage** > **Storage VMs**	Wählen Sie die Storage-VM aus. Wählen Sie die Registerkarte **Einstellungen**. Wählen Sie im Abschnitt **Verschlüsselung** unter **Sicherheit** ⋮, und wählen Sie dann **External Key Manager bearbeiten**.

2. Vorhandene Schlüsselserver sind in der Tabelle **Schlüsselserver** aufgeführt. Sie können folgende Vorgänge durchführen:
   - Fügen Sie einen neuen Schlüsselserver hinzu, indem + Add Sie .
   - Löschen Sie einen Schlüsselserver, indem Sie am Ende der Tabellenzelle auswählen ⋮ , die den Namen des Schlüsselservers enthält. Die sekundären Schlüsselserver, die dem primären Schlüsselserver zugeordnet sind, werden ebenfalls aus der Konfiguration entfernt.

Löschen Sie einen externen Schlüsselmanager

Ein externer Schlüsselmanager kann gelöscht werden, wenn die Volumes unverschlüsselt sind.

Schritte

1. Führen Sie einen der folgenden Schritte aus, um einen externen Schlüsselmanager zu löschen.

Umfang	Navigation	Startschritt
Externer Schlüsselmanager für den Clusterbereich	**Cluster** > **Einstellungen**	Blättern Sie zum Abschnitt **Sicherheit**. Wählen Sie unter **Verschlüsselung** die Option ⋮, und wählen Sie dann **External Key Manager löschen**.
Externer Schlüsselmanager für Storage VM	**Storage** > **Storage VMs**	Wählen Sie die Storage-VM aus. Wählen Sie die Registerkarte **Einstellungen**. Wählen Sie im Abschnitt **Verschlüsselung** unter **Sicherheit** ⋮, und wählen Sie dann **External Key Manager löschen**.

Schlüssel zwischen Schlüsselmanagern migrieren

Wenn mehrere Schlüsselmanager auf einem Cluster aktiviert sind, müssen Schlüssel von einem Schlüsselmanager zu einem anderen migriert werden. Dieser Vorgang wird mit System Manager automatisch abgeschlossen.

- Wenn der Onboard Key Manager oder ein externer Schlüsselmanager auf Cluster-Ebene aktiviert ist und einige Volumes verschlüsselt werden, Wenn Sie dann einen externen Schlüsselmanager auf Ebene der Storage-VM konfigurieren, müssen die Schlüssel vom Onboard Key Manager oder externen Schlüsselmanager auf Cluster-Ebene zum externen Schlüsselmanager auf Ebene der Storage-VM migriert werden. Dieser Prozess wird automatisch durch System Manager abgeschlossen.
- Wenn Volumes ohne Verschlüsselung auf einer Storage-VM erstellt wurden, müssen Schlüssel nicht migriert werden.

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 NVE in ONTAP 9.6 und höher

Verwenden Sie KMIP-Server, um die Schlüssel zu sichern, die der Cluster für den Zugriff

auf verschlüsselte Daten verwendet. Ab ONTAP 9.6 haben Sie die Möglichkeit, einen separaten externen Schlüsselmanager zu konfigurieren, um die Schlüssel zu sichern, die ein Daten-SVM für den Zugriff auf verschlüsselte Daten verwendet.

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.

Über diese Aufgabe

Sie können bis zu vier KMIP-Server mit einem Cluster oder SVM verbinden. Verwenden Sie mindestens zwei Server für Redundanz und Notfallwiederherstellung.

Der Umfang des externen Verschlüsselungsmanagement bestimmt, ob wichtige Managementserver alle SVMs im Cluster oder nur ausgewählte SVMs sichern:

- Sie können ein_Cluster Scope_ verwenden, um das externe Verschlüsselungsmanagement für alle SVMs im Cluster zu konfigurieren. Der Clusteradministrator hat Zugriff auf jeden auf den Servern gespeicherten Schlüssel.
- Ab ONTAP 9.6 können Sie mithilfe eines Umfangs *SVM* externes Verschlüsselungsmanagement für eine Daten-SVM im Cluster konfigurieren. Dies eignet sich am besten für mandantenfähige Umgebungen, in denen jeder Mandant eine andere SVM (oder einen Satz SVMs) zur Bereitstellung von Daten verwendet. Nur der SVM-Administrator für einen bestimmten Mandanten hat Zugriff auf die Schlüssel für den jeweiligen Mandanten.
- Installieren Sie für mandantenfähige Umgebungen eine Lizenz für *MT_EK_MGMT*, indem Sie den folgenden Befehl verwenden:

  ```
  system license add -license-code <MT_EK_MGMT license code>
  ```

  Erfahren Sie mehr über `system license add` in der "ONTAP-Befehlsreferenz".

Sie können beide Bereiche im selben Cluster verwenden. Wenn Verschlüsselungsmanagement-Server für eine SVM konfiguriert wurden, verwendet ONTAP nur diese Server zur Sicherung der Schlüssel. Andernfalls sichert ONTAP Schlüssel mit den für den Cluster konfigurierten Verschlüsselungsmanagement-Servern.

Die integrierte Verschlüsselungsmanagement lässt sich für den Cluster-Umfang und das externe Verschlüsselungsmanagement auf der SVM-Ebene konfigurieren. Mit dem `security key-manager key migrate` Befehl können Sie Schlüssel vom integrierten Verschlüsselungsmanagement im Cluster-Umfang zu externen Schlüsselmanagern im SVM-Umfang migrieren.

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

Bevor Sie beginnen

- Die KMIP SSL-Client- und Serverzertifikate müssen installiert sein.
- Der KMIP-Server muss von jedem Knoten-Management-LIF aus erreichbar sein.
- Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.
- In einer MetroCluster -Umgebung:
  - MetroCluster muss vollständig konfiguriert sein, bevor die externe Schlüsselverwaltung aktiviert wird.
  - Sie müssen auf beiden Clustern dasselbe KMIP-SSL-Zertifikat installieren.
  - Auf beiden Clustern muss ein externer Schlüsselmanager konfiguriert werden.

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. Wenn Sie den Befehl an der Cluster-Anmeldeaufforderung ausführen, *`admin_SVM`* standardmäßig auf die Admin-SVM des aktuellen Clusters. Sie können die `security key-manager external modify` Befehl zum Ändern der Konfiguration der externen Schlüsselverwaltung.

   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:

   ```
   clusterl::> security key-manager external enable -vserver cluster1 -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. Konfiguration eines Schlüsselmanagers einer SVM:

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

   > - Wenn Sie den Befehl an der SVM-Anmeldeaufforderung ausführen, `SVM` standardmäßig auf die aktuelle SVM eingestellt. Sie können die `security key-manager external modify` Befehl zum Ändern der Konfiguration der externen Schlüsselverwaltung.
   > - Wenn Sie in einer MetroCluster-Umgebung externes Verschlüsselungsmanagement für eine Daten-SVM konfigurieren, müssen Sie den `security key-manager external enable` Befehl auf dem Partner-Cluster nicht wiederholen.

   Mit dem folgenden Befehl wird die externe Schlüsselverwaltung für `svm1` mit einem einzelnen Schlüsselserver aktiviert, der auf dem Standardport 5696 lauscht:

   ```
   svm1l::> security key-manager external enable -vserver svm1 -key-servers
   keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
   SVM1ServerCaCert
   ```

3. Wiederholen Sie den letzten Schritt für alle weiteren SVMs.

Sie können auch `security key-manager external add-servers` weitere SVMs mit dem Befehl konfigurieren. Der `security key-manager external add-servers` Befehl ersetzt den `security key-manager add` Befehl. Erfahren Sie mehr über `security key-manager external add-servers` in der "ONTAP-Befehlsreferenz".

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

   `security key-manager external show-status -node node_name`

   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
      svm1
               keyserver.svm1.com:5696                         available
      cluster1
               10.0.0.10:5696                                  available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234    available
               ks1.local:15696                                 available
node2
      svm1
               keyserver.svm1.com:5696                         available
      cluster1
               10.0.0.10:5696                                  available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234    available
               ks1.local:15696                                 available

8 entries were displayed.
```

5. Konvertieren Sie optional Klartextvolumes in verschlüsselte Volumes.

   `volume encryption conversion start`

   Ein externer Schlüsselmanager muss vollständig konfiguriert sein, bevor Sie die Volumes konvertieren.

Verwandte Informationen

- Konfigurieren Sie externe geclusterte Schlüsselserver
- "Systemlizenz hinzufügen"
- "Sicherheitsschlüssel-Manager-Schlüsselmigration"

- "Sicherheitsschlüssel-Manager Externe Add-Server"
- "Sicherheitsschlüssel-Manager, externer Show-Status"

Aktivieren Sie die externe Schlüsselverwaltung für NVE 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`

```
cluster1::> 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.

Verwalten Sie NVE-Schlüssel für ONTAP -Daten-SVMs mit einem Cloud-Anbieter

Ab ONTAP 9.10.1 können Sie Ihre ONTAP-Verschlüsselungen in einer Cloud-gehosteten Applikation verwenden "Azure Key Vault (AKV)" und "Der Verschlüsselungsmanagement-Service (Cloud KMS) der Google Cloud-Plattform"schützen. Ab ONTAP 9.12.0 können Sie NVE Schlüssel auch mit schützen"KMS VON AWS".

AWS KMS, AKV und Cloud KMS können "NetApp Volume Encryption (NVE)-Schlüssel"nur für Daten-SVMs eingesetzt werden.

Über diese Aufgabe

Das Verschlüsselungsmanagement mit einem Cloud-Provider kann über die CLI oder die ONTAP REST-API aktiviert werden.

Wenn Sie zum Schutz Ihrer Schlüssel einen Cloud-Provider verwenden, beachten Sie, dass standardmäßig eine Daten-SVM-LIF zur Kommunikation mit dem Cloud-Schlüsselmanagement-Endpunkt verwendet wird. Über ein Node-Managementnetzwerk kommunizieren Sie mit den Authentifizierungsservices des Cloud-Providers (login.microsoftonline.com für Azure, oauth2.googleapis.com für Cloud KMS). Wenn das Cluster-Netzwerk nicht ordnungsgemäß konfiguriert ist, verwendet das Cluster den Schlüsselverwaltungsservice nicht

ordnungsgemäß.

Wenn Sie einen Cloud-Provider-Managementservice nutzen, sollten Sie sich die folgenden Einschränkungen bewusst sein:

- Das Verschlüsselungsmanagement von Cloud-Providern ist für die NetApp Storage-Verschlüsselung (NSE) und die NetApp Aggregate Encryption (NAE) nicht verfügbar. "Externe KMIPs" Kann stattdessen verwendet werden.
- Das Verschlüsselungsmanagement bei MetroCluster-Konfigurationen ist nicht für Cloud-Provider verfügbar.
- Das Verschlüsselungsmanagement von Cloud-Providern kann nur auf einer Daten-SVM konfiguriert werden.

Bevor Sie beginnen

- Sie müssen den KMS auf dem entsprechenden Cloud-Provider konfiguriert haben.
- Die Nodes des ONTAP Clusters müssen NVE unterstützen.
- "Sie müssen die Lizenzen für Volume Encryption (VE) und Multi-Tenant Encryption Key Management (MTEKM) installiert haben". Diese Lizenzen sind in enthalten"ONTAP One".
- Sie müssen ein Cluster- oder SVM-Administrator sein.
- Die Daten-SVM darf keine verschlüsselten Volumes enthalten oder einen Schlüsselmanager beschäftigen. Wenn die Daten-SVM verschlüsselte Volumes enthält, müssen Sie sie vor der Konfiguration des KMS migrieren.

Externes Verschlüsselungsmanagement

Die Aktivierung des externen Schlüsselmanagements hängt von dem jeweiligen Schlüsselmanager ab, den Sie verwenden. Wählen Sie die Registerkarte des entsprechenden Schlüsselmanagers und der entsprechenden Umgebung aus.

AWS

Bevor Sie beginnen

- Sie müssen einen Zuschuss für den AWS-KMS-Schlüssel erstellen, der von der IAM-Rolle zum Managen der Verschlüsselung verwendet wird. Die IAM-Rolle muss eine Richtlinie enthalten, die die folgenden Operationen zulässt:
  - `DescribeKey`
  - `Encrypt`
  - `Decrypt` + Weitere Informationen finden Sie in der AWS-Dokumentation für "Zuschüsse".

Aktivieren Sie AWS KMV auf einer ONTAP SVM

1. Bevor Sie beginnen, erhalten Sie sowohl die Zugriffsschlüssel-ID als auch den geheimen Schlüssel von Ihrem AWS KMS.
2. Legen Sie die Berechtigungsebene auf erweitert fest: `set -priv advanced`
3. AWS KMS aktivieren: `security key-manager external aws enable -vserver` *`svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. Geben Sie den geheimen Schlüssel ein, wenn Sie dazu aufgefordert werden.
5. Überprüfen Sie, ob der AWS-KMS ordnungsgemäß konfiguriert wurde: `security key-manager external aws show -vserver` *`svm_name`*

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

Azure

Aktivieren Sie Azure Key Vault auf einer ONTAP SVM

1. Bevor Sie beginnen, müssen Sie die entsprechenden Authentifizierungsdaten von Ihrem Azure-Konto beziehen, entweder ein Clientgeheimnis oder ein Zertifikat. Sie müssen außerdem sicherstellen, dass alle Nodes im Cluster sich in einem ordnungsgemäßen Zustand befinden. Sie können dies mit dem Befehl überprüfen `cluster show`. Erfahren Sie mehr über `cluster show` in der "ONTAP-Befehlsreferenz".
2. Setzen Sie die privilegierte Ebene auf erweitert `set -priv advanced`
3. Aktivieren Sie AKV auf der SVM `security key-manager external azure enable -client-id` *`client_id`* `-tenant-id` *`tenant_id`* `-name -key-id` *`key_id`* `-authentication-method {certificate|client-secret}` Wenn Sie dazu aufgefordert werden, geben Sie entweder das Client-Zertifikat oder den Client-Schlüssel aus Ihrem Azure-Konto ein.
4. Vergewissern Sie sich, dass AKV korrekt aktiviert `security key-manager external azure show vserver` *`svm_name`* ist: Wenn die Service-Erreichbarkeit nicht in Ordnung ist, stellen Sie die Verbindung zum AKV-Schlüsselverwaltungsservice über die Daten-SVM-LIF her.

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

Google Cloud

Aktivieren Sie Cloud-KMS auf einer ONTAP SVM

1. Bevor Sie beginnen, erhalten Sie den privaten Schlüssel für die Google Cloud KMS-Kontoschlüsseldatei in einem JSON-Format. Dieser Punkt ist in Ihrem GCP-Konto enthalten. Sie

müssen außerdem sicherstellen, dass alle Nodes im Cluster sich in einem ordnungsgemäßen Zustand befinden. Sie können dies mit dem Befehl überprüfen `cluster show`. Erfahren Sie mehr über `cluster show` in der "ONTAP-Befehlsreferenz".

2. Privilegierte Ebene auf erweitert setzen: `set -priv advanced`
3. Cloud-KMS auf der SVM aktivieren `security key-manager external gcp enable -vserver svm_name -project-id project_id-key-ring-name key_ring_name -key -ring-location key_ring_location -key-name key_name` Wenn Sie dazu aufgefordert werden, geben Sie den Inhalt der JSON-Datei mit dem privaten Schlüssel des Servicekontos ein
4. Überprüfen Sie, ob Cloud KMS mit den richtigen Parametern konfiguriert ist: `security key-manager external gcp show vserver svm_name` Der Status von `kms_wrapped_key_status` wird `"UNKNOWN"` wenn keine verschlüsselten Volumes erstellt wurden. Wenn die Diensterreichbarkeit nicht in Ordnung ist, stellen Sie die Verbindung zum GCP-Schlüsselverwaltungsdienst über das Daten-SVM-LIF her.

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

Wenn bereits ein oder mehrere verschlüsselte Volumes für eine Daten-SVM konfiguriert sind und die entsprechenden NVE Schlüssel vom Onboard-Schlüsselmanager des Admin-SVM gemanagt werden, sollten diese Schlüssel zu dem externen Verschlüsselungsmanagement-Service migriert werden. Dazu führen Sie über die CLI den Befehl aus: `security key-manager key migrate -from-Vserver admin_SVM -to -Vserver data_SVM` Neue verschlüsselte Volumes können erst für die Daten-SVM des Mandanten erstellt werden, wenn alle NVE-Schlüssel der Daten-SVM erfolgreich migriert wurden.

Verwandte Informationen

- "Verschlüsseln von Volumes mit NetApp Verschlüsselungslösungen für Cloud Volumes ONTAP"
- "Sicherheitsschlüsselmanager extern"

Verwalten Sie ONTAP -Schlüssel mit Barbican KMS

Ab ONTAP 9.17.1 können Sie OpenStacks "Barbican KMS" zum Schutz von ONTAP Verschlüsselungsschlüsseln. Barbican KMS ist ein Dienst zum sicheren Speichern und Zugreifen auf Schlüssel. Barbican KMS kann zum Schutz von NetApp Volume Encryption (NVE)-Schlüsseln für Daten-SVMs verwendet werden. Barbican basiert auf "OpenStack Keystone" , der Identitätsdienst von OpenStack, zur Authentifizierung.

Über diese Aufgabe

Sie können die Schlüsselverwaltung mit Barbican KMS über die CLI oder die ONTAP REST API konfigurieren. Ab Version 9.17.1 gelten für die Barbican KMS-Unterstützung folgende Einschränkungen:

- Barbican KMS wird für NetApp Storage Encryption (NSE) und NetApp Aggregate Encryption (NAE) nicht unterstützt. Alternativ können Sie "externe KMIPs" oder die "Onboard-Schlüsselmanager (OKM)" für NSE- und NVE-Schlüssel.
- Barbican KMS wird für MetroCluster -Konfigurationen nicht unterstützt.
- Barbican KMS kann nur für eine Daten-SVM konfiguriert werden. Es ist nicht für die Administrator-SVM verfügbar.

Sofern nicht anders angegeben, sind die Administratoren der `admin` Mit dieser Berechtigungsstufe können Sie

die folgenden Verfahren durchführen.

Bevor Sie beginnen

- Barbican KMS und OpenStack Keystone müssen konfiguriert sein. Die SVM, die Sie mit Barbican verwenden, benötigt Netzwerkzugriff auf die Barbican- und OpenStack Keystone Server.
- Wenn Sie eine benutzerdefinierte Zertifizierungsstelle (CA) für die Barbican- und OpenStack Keystone Server verwenden, müssen Sie das CA-Zertifikat mit installieren `security certificate install -type server-ca -vserver <admin_svm>`.

Erstellen und Aktivieren einer Barbican KMS-Konfiguration

Sie können eine neue Barbican KMS-Konfiguration für eine SVM erstellen und aktivieren. Eine SVM kann mehrere inaktive Barbican KMS-Konfigurationen haben, es kann jedoch immer nur eine aktiv sein.

Schritte

1. Erstellen Sie eine neue inaktive Barbican KMS-Konfiguration für eine SVM:

```
security key-manager external barbican create-config -vserver <svm_name>
-config-name <unique_config_name> -key-id <key_id> -keystone-url
<keystone_url> -application-cred-id
<keystone_applications_credentials_id>
```

   - `-key-id` ist die Schlüsselkennung des Barbican-Schlüssels (KEK). Geben Sie eine vollständige URL ein, einschließlich `https://`.

     Einige URLs enthalten das Fragezeichen (?). Das Fragezeichen aktiviert die aktive Hilfe der ONTAP Befehlszeile. Um eine URL mit einem Fragezeichen einzugeben, müssen Sie zunächst die aktive Hilfe mit dem Befehl deaktivieren. `set -active-help false` Die Die aktive Hilfe kann später wieder mit dem Befehl `set -active-help true`. im "ONTAP-Befehlsreferenz".

   - `-keystone-url` ist die URL des OpenStack Keystone Autorisierungshosts. Geben Sie eine vollständige URL ein, einschließlich `https://`.
   - `-application-cred-id` ist die Anmeldeinformations-ID der Anwendung.

     Nach Eingabe dieses Befehls werden Sie zur Eingabe des geheimen Schlüssels für die Anwendungsanmeldeinformationen aufgefordert. Dieser Befehl erstellt eine inaktive Barbican KMS-Konfiguration.

     Das folgende Beispiel erstellt eine neue inaktive Barbican KMS-Konfiguration mit dem Namen `config1` für die SVM `svm1`:

```
cluster1::> security key-manager external barbican create-config
-vserver svm1 -config-name config1 -keystone-url
https://172.21.76.152:5000/v3 -application-cred-id app123 -key-id
https://172.21.76.153:9311/v1/secrets/<id_value>

Enter the Application Credentials Secret for authentication with
Keystone: <key_value>
```

2. Aktivieren Sie die neue Barbican KMS-Konfiguration:

```
security key-manager keystore enable -vserver <svm_name> -config-name
<unique_config_name> -keystore barbican
```

Mit diesem Befehl können Sie zwischen Barbican KMS-Konfigurationen wechseln. Wenn auf dem SVM bereits eine aktive Barbican KMS-Konfiguration vorhanden ist, wird diese deaktiviert und die neue Konfiguration aktiviert.

3. Überprüfen Sie, ob die neue Barbican KMS-Konfiguration aktiv ist:

```
security key-manager external barbican check -vserver <svm_name> -node
<node_name>
```

Dieser Befehl liefert den Status der aktiven Barbican KMS-Konfiguration auf dem SVM oder Knoten. Wenn beispielsweise der SVM `svm1` auf Knoten `node1` über eine aktive Barbican KMS-Konfiguration verfügt, gibt der folgende Befehl den Status dieser Konfiguration zurück:

```
cluster1::> security key-manager external barbican check -node node1

Vserver: svm1
Node: node1

Category: service_reachability
             Status: OK

Category: kms_wrapped_key_status
             Status: OK
```

Aktualisieren Sie die Anmeldeinformationen und Einstellungen einer Barbican KMS-Konfiguration

Sie können die aktuellen Einstellungen einer aktiven oder inaktiven Barbican KMS-Konfiguration anzeigen und aktualisieren.

Schritte

1. Sehen Sie sich die aktuellen Barbican KMS-Konfigurationen für eine SVM an:

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

Die Schlüssel-ID, die OpenStack Keystone -URL und die Anwendungsanmeldeinformations-ID werden für jede Barbican KMS-Konfiguration auf der SVM angezeigt.

2. Aktualisieren Sie die Einstellungen einer Barbican KMS-Konfiguration:

```
security key-manager external barbican update-config -vserver <svm_name>
-config-name <unique_config_name> -timeout <timeout> -verify
<true|false> -verify-host <true|false>
```

Dieser Befehl aktualisiert die Timeout- und Überprüfungseinstellungen der angegebenen Barbican KMS-Konfiguration. `timeout` bestimmt die Zeit in Sekunden, die ONTAP auf eine Antwort von Barbican wartet, bevor die Verbindung fehlschlägt. Der Standardwert `timeout` beträgt zehn Sekunden. `verify` Und `verify-host` Legen Sie fest, ob die Identität bzw. der Hostname des Barbican-Hosts vor der Verbindung überprüft werden soll. Standardmäßig sind diese Parameter auf `true` . Der `vserver` Und `config-name` Parameter sind erforderlich. Die anderen Parameter sind optional.

3. Aktualisieren Sie bei Bedarf die Anmeldeinformationen einer aktiven oder inaktiven Barbican KMS-Konfiguration:

```
security key-manager external barbican update-credentials -vserver
<svm_name> -config-name <unique_config_name> -application-cred-id
<keystone_applications_credentials_id>
```

Nach der Eingabe dieses Befehls werden Sie aufgefordert, den neuen geheimen Schlüssel für die Anwendungsanmeldeinformationen einzugeben.

4. Stellen Sie bei Bedarf einen fehlenden SVM-Schlüsselverschlüsselungsschlüssel (KEK) für eine aktive Barbican KMS-Konfiguration wieder her:

   a. Stellen Sie einen fehlenden SVM-KEK wieder her mit `security key-manager external barbican restore`:

```
security key-manager external barbican restore -vserver <svm_name>
```

Dieser Befehl stellt den SVM KEK für die aktive Barbican KMS-Konfiguration durch Kommunikation mit dem Barbican-Server wieder her.

5. Falls erforderlich, müssen Sie den SVM KEK für eine Barbican KMS-Konfiguration neu kodieren:

   a. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

b. Erneutes Verschlüsseln des SVM-KEK mit `security key-manager external barbican rekey-internal`:

```
security key-manager external barbican rekey-internal -vserver
<svm_name>
```

Dieser Befehl generiert einen neuen SVM-KEK für die angegebene SVM und umschließt die Volume-Verschlüsselungsschlüssel mit dem neuen SVM-KEK. Der neue SVM-KEK wird durch die aktive Barbican-KMS-Konfiguration geschützt.

Migrieren Sie Schlüssel zwischen Barbican KMS und dem Onboard Key Manager

Sie können Schlüssel vom Barbican KMS zum Onboard Key Manager (OKM) und umgekehrt migrieren. Weitere Informationen zum OKM finden Sie unter "Ermöglichen Sie integriertes Verschlüsselungsmanagement in ONTAP 9.6 und höher" .

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Migrieren Sie bei Bedarf Schlüssel vom Barbican KMS zum OKM:

```
security key-manager key migrate -from-vserver <svm_name> -to-vserver
<admin_svm_name>
```

`svm_name` ist der Name der SVM mit der Barbican KMS-Konfiguration.

3. Migrieren Sie bei Bedarf Schlüssel vom OKM zum Barbican KMS:

```
security key-manager key migrate -from-vserver <admin_svm_name> -to
-vserver <svm_name>
```

Deaktivieren und Löschen einer Barbican KMS-Konfiguration

Sie können eine aktive Barbican KMS-Konfiguration ohne verschlüsselte Volumes deaktivieren und eine inaktive Barbican KMS-Konfiguration löschen.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

```
set -privilege advanced
```

2. Deaktivieren Sie eine aktive Barbican KMS-Konfiguration:

```
security key-manager keystore disable -vserver <svm_name>
```

Wenn NVE-verschlüsselte Volumes auf der SVM vorhanden sind, müssen Sie diese entschlüsseln oder Migrieren Sie die Schlüssel bevor Sie die Barbican KMS-Konfiguration deaktivieren. Das Aktivieren einer neuen Barbican KMS-Konfiguration erfordert weder das Entschlüsseln von NVE-Volumes noch das Migrieren von Schlüsseln und deaktiviert die aktuell aktive Barbican KMS-Konfiguration.

3. Löschen Sie eine inaktive Barbican KMS-Konfiguration:

```
security key-manager keystore delete -vserver <svm_name> -config-name
<unique_config_name> -type barbican
```

Aktivieren Sie die integrierte Schlüsselverwaltung für NVE in ONTAP 9.6 und höher

Mit dem integrierten Key Manager werden die Schlüssel gesichert, die das Cluster für den Zugriff auf verschlüsselte Daten verwendet. Sie müssen den 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 sync` Befehl jedes Mal ausführen, wenn Sie dem Cluster einen Node hinzufügen.

Wenn Sie über eine MetroCluster-Konfiguration verfügen, müssen Sie `security key-manager onboard enable` zuerst den Befehl auf dem lokalen Cluster ausführen und dann den `security key-manager onboard sync` Befehl auf dem Remote-Cluster ausführen. Verwenden Sie dabei jeweils dieselbe Passphrase. Wenn Sie den `security key-manager onboard enable` Befehl vom lokalen Cluster aus ausführen und dann auf dem Remote-Cluster synchronisieren, müssen Sie den `enable` Befehl nicht erneut vom Remote-Cluster aus 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 der `cc-mode-enabled=yes` Option können Sie festlegen, dass Benutzer die Passphrase nach einem Neustart eingeben müssen.

Wenn Sie für NVE festlegen, `cc-mode-enabled=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`.

Wenn Sie die ONTAP Datenverschlüsselung im Ruhezustand konfigurieren, müssen Sie NSE mit NVE verwenden und sicherstellen, dass der Onboard Key Manager im Common Criteria-Modus aktiviert ist, um die

Anforderungen für Commercial Solutions for Classified (CSfC) zu erfüllen. Sehen"CSfC Lösungsüberblick" .

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 Sie die Cluster-Passphrase fünfmal nicht eingeben können, warten Sie 24 Stunden oder starten Sie den Knoten neu, 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. Das System fährt mit dem nächsten Schritt im Image-Aktualisierungsprozess fort, wenn die Validierung erfolgreich ist. Andernfalls schlägt die Image-Aktualisierung fehl. Erfahren Sie mehr über `cluster image` im"ONTAP-Befehlsreferenz" .

Der Onboard Key Manager speichert Schlüssel im flüchtigen Speicher. Der Inhalt des flüchtigen Speichers wird gelöscht, wenn das System neu gestartet oder angehalten wird. Das System löscht den flüchtigen Speicher innerhalb von 30 Sekunden, wenn es angehalten wird.

Bevor Sie beginnen

- 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 die Konfiguration des Schlüsselmanagers:

   ```
   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. Wenn Sie für NVE festlegen, `cc-mode-enabled=yes` `volume create` `volume move start` werden Volumes, die Sie mit den Befehlen und erstellen, automatisch verschlüsselt. 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.

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. Vergewissern Sie sich, dass die Authentifizierungsschlüssel erstellt wurden:

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

   > 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".

5. Optional können Sie Nur-Text-Volumes in verschlüsselte Volumes konvertieren.

   `volume encryption conversion start`

   Der Onboard Key Manager muss vor der Konvertierung der Volumes vollständig konfiguriert sein. In einer MetroCluster-Umgebung muss der Onboard Key Manager auf beiden Standorten konfiguriert sein.

Nachdem Sie fertig sind

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

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

- "Cluster-Image-Befehle"
- "Sicherheitsschlüsselmanager extern aktivieren"
- "Sicherheitsschlüssel-Manager-Schlüsselabfrage"
- "Sicherheitsschlüssel-Manager Onboard aktivieren"

Aktivieren Sie die integrierte Schlüsselverwaltung für NVE in ONTAP 9.5 und früher

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 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 oder NVE 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`

   ```
   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
   ```

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

6. Konvertieren Sie optional Klartextvolumes in verschlüsselte Volumes.

   `volume encryption conversion start`

   Konfigurieren Sie den Onboard Key Manager, bevor Sie Volumes konvertieren. Konfigurieren Sie es in MetroCluster -Umgebungen auf beiden Sites.

Nachdem Sie fertig sind

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

Wenn Sie die Passphrase für den Onboard Key Manager konfigurieren, sichern Sie die Informationen für den Fall einer Katastrophe 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"
- "Umstellung auf integriertes Verschlüsselungsmanagement von externem Verschlüsselungsmanagement"
- "Sicherheitsschlüssel-Manager Show-Key-Store"

Aktivieren Sie die integrierte Schlüsselverwaltung in neu hinzugefügten ONTAP Knoten

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.

> Für ONTAP 9.6 und höher müssen Sie Folgendes ausführen: `security key-manager onboard sync` Führen Sie diesen Befehl jedes Mal aus, wenn Sie dem Cluster einen Knoten hinzufügen.
>
> Bei ONTAP 9 5 und früheren Versionen müssen Sie den `security key-manager setup` Befehl jedes Mal ausführen, wenn Sie dem Cluster einen Knoten hinzufügen.
>
> Wenn Sie einem Cluster mit integrierter Schlüsselverwaltung einen Knoten hinzufügen, führen Sie diesen Befehl aus, um fehlende Schlüssel zu aktualisieren.

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

- Ab ONTAP 9.6 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 jedem Cluster ausführen.

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

- 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`.

Wenn die Passphrase-Eingabe fehlschlägt, starten Sie den Knoten neu. Nach dem Neustart können Sie versuchen, die Passphrase erneut einzugeben.

Verwandte Informationen

- "Cluster-Image-Befehle"
- "Sicherheitsschlüsselmanager extern aktivieren"
- "Sicherheitsschlüssel-Manager Onboard aktivieren"