Konfigurieren Sie NVE

ONTAP 9

NetApp
March 30, 2023

Inhaltsverzeichnis

Konfigurieren Sie NVE

Bestimmen Sie, ob Ihre Cluster-Version NVE unterstützt

Sie sollten vor der Installation der Lizenz festlegen, ob Ihre Cluster-Version NVE unterstützt. Sie können das verwenden `version` Befehl zum Bestimmen der Cluster-Version.

Über diese Aufgabe

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

Schritt

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

   `version -v`

   NVE wird nicht unterstützt, wenn in der Befehlsausgabe der Text „`1Ono-DARE`“ (für „`no Data at Rest Encryption`“) angezeigt wird oder wenn Sie eine Plattform verwenden, die nicht in aufgeführt ist "Support-Details".

   Mit dem folgenden Befehl wird festgelegt, ob NVE unterstützt wird `cluster1`.

   ```
   cluster1::> version -v
   NetApp Release 9.1.0: Tue May 10 19:30:23 UTC 2016 <1Ono-DARE>
   ```

   Die Ausgabe von `1Ono-DARE` Gibt an, dass NVE bei Ihrer Cluster-Version nicht unterstützt wird.

Installieren Sie die Lizenz

Eine VE-Lizenz berechtigt Sie zur Nutzung der Funktion auf allen Knoten im Cluster. Bevor Daten mit NVE verschlüsselt werden können, müssen Sie die Lizenz installieren.

Was Sie benötigen

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

Über diese Aufgabe

Sie sollten den VE-Lizenzschlüssel von Ihrem Vertriebsmitarbeiter erhalten haben.

Schritte

1. Installieren Sie die VE-Lizenz für einen Node:

   `system license add -license-code license_key`

   Mit dem folgenden Befehl wird die Lizenz mit dem Schlüssel installiert `AAAAAAAAAAAAAAAAAAAAAAAAAAAA`.

```
cluster1::> system license add -license-code
AAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

2. Vergewissern Sie sich, dass die Lizenz installiert ist, indem Sie alle Lizenzen auf dem Cluster anzeigen:

   `system license show`

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

   Mit dem folgenden Befehl werden alle Lizenzen auf angezeigt `cluster1`:

```
cluster1::> system license show
```

   Der Name des VE-Lizenzpakets lautet „`VE`“.

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) unterstützt Onboard Key Manager in ONTAP 9.1 und höher. Ab ONTAP 9.3 unterstützt NVE externes Verschlüsselungsmanagement (KMIP) und Onboard Key Manager. Ab ONTAP 9.10.1 können Sie dies nutzen Azure Key Vault oder Google Cloud Key Manager Service Zum Schutz Ihrer NVE-Schlüssel Ab ONTAP 9.11.1 können Sie mehrere externe Schlüsselmanager in einem Cluster konfigurieren. Siehe Konfigurieren Sie Cluster-Key-Server.

Installieren Sie SSL-Zertifikate auf dem 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.

Was Sie benötigen

- 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 das KMIP SSL-Zertifikat auf beiden Clustern installieren.

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

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.

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 (NVE)

Ein oder mehrere KMIP-Server dienen zur Sicherung der Schlüssel, die das Cluster für den Zugriff auf verschlüsselte Daten verwendet. Ab ONTAP 9.6 haben Sie die Möglichkeit, einen separaten externen Schlüsselmanager zum Sichern der Schlüssel zu konfigurieren, die von der SVM für den Zugriff auf verschlüsselte Daten verwendet werden.

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- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.
- Wenn Sie externes Verschlüsselungsmanagement für eine MetroCluster Umgebung aktivieren möchten, muss MetroCluster vollständig konfiguriert sein, bevor Sie externes Verschlüsselungsmanagement unterstützen können.

- In einer MetroCluster-Umgebung müssen Sie das KMIP SSL-Zertifikat auf beiden Clustern installieren.

Über diese Aufgabe

Mit einem Cluster oder einer SVM können bis zu vier KMIP-Server verbunden werden. Für Redundanz und Disaster Recovery werden mindestens zwei Server empfohlen.

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>
  ```

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

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. Sie können das verwenden `security key-manager key migrate` Befehl zur Migration von Schlüsseln vom Onboard-Verschlüsselungsmanagement im Cluster-Umfang an externe Schlüsselmanager des Umfangs der SVM

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. Wenn Sie den Befehl an der Eingabeaufforderung für die Anmeldung beim Cluster ausführen, *`admin_SVM`* Standardmäßig wird der Admin-SVM des aktuellen Clusters festgelegt. Sie müssen der Cluster-Administrator sein, um den Clusterumfang zu konfigurieren. Sie können die ausführen `security key-manager external modify` Befehl zum Ändern der Konfiguration für das externe Verschlüsselungsmanagement.
   - Wenn Sie in einer MetroCluster-Umgebung externes Verschlüsselungsmanagement für den Administrator-SVM konfigurieren, müssen Sie die wiederholen `security key-manager 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 -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` Standardeinstellung ist die aktuelle SVM. Zum Konfigurieren des SVM-Umfangs müssen Sie ein Cluster oder SVM-Administrator sein. Sie können die ausführen `security key-manager external modify` Befehl zum Ändern der Konfiguration für das externe Verschlüsselungsmanagement.
- Wenn Sie in einer MetroCluster Umgebung externes Verschlüsselungsmanagement für eine Daten-SVM konfigurieren, müssen Sie die nicht wiederholen `security key-manager external enable` Befehl auf dem Partner-Cluster.

Mit dem folgenden Befehl wird die externe Schlüsselverwaltung für aktiviert `svm1` Wenn ein Server mit einer einzigen Taste auf dem Standardport 5696 angehört:

```
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 die verwenden `security key-manager external add-servers` Befehl zum Konfigurieren weiterer SVMs. Der `security key-manager external add-servers` Mit dem Befehl wird der ersetzt `security key-manager add` Befehl. Eine vollständige Befehlssyntax finden Sie in der man-Page.

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` 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
      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.
```

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.

Was Sie benötigen

- 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.

Über diese Aufgabe

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

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`

   ```
   cluster1::> 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`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   ```
   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
   ```

Verschlüsselungsmanagement mit Azure Key Vault oder Google Cloud KMS

Ab ONTAP 9.10.1 können Sie dies nutzen "Azure Key Vault (AKV)" Und "Der Verschlüsselungsmanagement-Service (Cloud KMS) der Google Cloud-Plattform" Zum Schutz Ihrer ONTAP Verschlüsselungen in einer Applikation, die vom Azure oder Google Cloud Platform implementiert wurde

AKV und Cloud KMS können zum Schutz verwendet werden "NetApp Volume Encryption (NVE)-Schlüssel" Nur für Data SVMs.

Die Schlüsselverwaltung mit AKV oder Cloud KMS kann über die CLI oder die ONTAP REST API aktiviert werden.

Bei Verwendung von AKV oder Cloud KMS ist zu beachten, dass standardmäßig eine LIF der Daten-SVMs zur Kommunikation mit dem Endpunkt des Cloud-Verschlüsselungsmanagement 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 korrekt konfiguriert ist, nutzt das Cluster den Verschlüsselungsmanagementservice nicht ordnungsgemäß.

Voraussetzungen

- Die Nodes des ONTAP-Clusters müssen NVE unterstützen
- Volume Encryption (VE)-Lizenz installiert
- Multi-Tenant Encryption Key Management-Lizenz (MTEKM) installiert
- Sie müssen ein Cluster- oder SVM-Administrator sein

Einschränkungen

- AKV und Cloud KMS sind für NSE und NAE nicht verfügbar. "Externe KMIPs" Kann stattdessen verwendet werden
- AKV und Cloud KMS sind für MetroCluster-Konfigurationen nicht verfügbar.
- AKV und Cloud KMS können nur auf einer Daten-SVM konfiguriert werden

Aktivieren Sie das externe Verschlüsselungsmanagement mit der CLI

Die Aktivierung des externen Schlüsselmanagements hängt von dem jeweiligen Schlüsselmanager ab, den Sie verwenden. Wenn Sie AKV in einem Cloud Volumes ONTAP aktivieren, beachten Sie, dass es eine separate Prozedur gibt. Wählen Sie die Registerkarte des Schlüsselmanagers und der Umgebung aus, die Ihren Anforderungen am besten entspricht:

Azure

Aktivieren Sie Azure Key Vault für ONTAP

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`.
2. Setzen Sie die privilegierte Stufe auf „Erweiterd“
   `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}`Geben Sie bei der entsprechenden Aufforderung entweder das Clientzertifikat oder den Clientschlüssel aus Ihrem Azure-Konto ein.
4. Überprüfen Sie, ob AKV richtig aktiviert ist:
   `security key-manager external azure show vserver *SVM_name*`Wenn die Erreichbarkeit des Dienstes nicht in Ordnung ist, stellen Sie die Verbindung zum AKV-Schlüsselverwaltungsservice über die Daten-SVM-LIF her.

Google Cloud

Aktivieren Sie Cloud KMS mit der CLI für ONTAP

1. Bevor Sie beginnen, müssen Sie den privaten Schlüssel für die Google Cloud KMS-Kontoschlüsseldatei im JSON-Format erhalten. 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`.
2. Setzen Sie die privilegierte Stufe auf „Erweiterd“
   `set -priv advanced`
3. Aktivieren Sie Cloud KMS auf der SVM
   `security key-manager external gcp enable -vserver *data_svm_name* -project-id *project_id*-key-ring -name *key_ring_name* -key-ring-location *key_ring_location* -key-name *key_name*`Geben Sie bei entsprechender Aufforderung den Inhalt der JSON-Datei mit dem privaten Schlüssel für Dienstkonto ein
4. Vergewissern Sie sich, dass Cloud KMS mit den korrekten Parametern konfiguriert ist:
   `security key-manager external gcp show vserver *SVM_name*`Der Status von `kms_wrapped_key_status` Wird sein "`UNKNOWN`" Wenn keine verschlüsselten Volumes erstellt wurden. Wenn die Serviceability nicht in Ordnung ist, stellen Sie die Konnektivität zum GCP-Schlüsselmanagement-Service über die Daten-SVM LIF her.

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. Führen Sie dazu den Befehl mit der CLI aus:
`security key-manager key migrate -from-Vserver *admin_SVM* -to-Vserver *data_SVM*`Neue verschlüsselte Volumes können erst für den Daten-vServer des Mandanten erstellt werden, wenn alle NVE-Schlüssel der Daten-SVM erfolgreich migriert wurden.

Integriertes Verschlüsselungsmanagement in ONTAP 9.6 und höher (NVE)

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.

Was Sie benötigen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Sie müssen die MetroCluster Umgebung konfigurieren, bevor Sie einen externen Schlüsselmanager konfigurieren.

Über diese Aufgabe

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

Wenn Sie über eine MetroCluster-Konfiguration verfügen, müssen Sie ausführen `security key-manager onboard enable` Führen Sie zuerst auf dem lokalen Cluster aus `security key-manager onboard sync` Verwenden Sie im Remote-Cluster jeweils dieselbe Passphrase.

Standardmäßig müssen Sie beim Neustart eines Node nicht die Passphrase für das Schlüsselmanagement eingeben. Sie können das verwenden `cc-mode-enabled=yes` Option zum Eingeben, dass Benutzer nach einem Neustart die Passphrase eingeben.

Wenn Sie die Einstellung für NVE verwenden `cc-mode-enabled=yes`, Volumen, die Sie mit erstellen `volume create` Und `volume move start` Befehle werden automatisch verschlüsselt. Für `volume create`, Sie müssen nicht angeben `-encrypt true`. Für `volume move start`, Sie müssen nicht angeben `-encrypt-destination true`.

Bei der Konfiguration der Verschlüsselung von ONTAP-Daten im Ruhezustand müssen Sie NSE mit NVE gewährleisten, dass der integrierte Schlüsselmanager im Common Criteria-Modus aktiviert ist, um die Anforderungen für kommerzielle Lösungen für die Klassifizierung (CSfC) zu erfüllen. Siehe "CSfC Lösungsüberblick" Weitere Informationen zu CSfC.

Wenn der Onboard Key Manager im Common Criteria-Modus aktiviert ist (`cc-mode-enabled=yes`Das Systemverhalten wird folgendermaßen geändert:

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

  Wenn Sie beim Booten nicht die richtige Cluster-Passphrase eingeben, werden verschlüsselte Volumes nicht angehängt. Um dies zu korrigieren, müssen Sie den Node neu booten und die richtige Cluster-Passphrase eingeben. Sobald das System gebootet wurde, können bis zu 5 aufeinanderfolgende Versuche unternommen werden, um für jeden Befehl, für den die Cluster-Passphrase als Parameter erforderlich ist, in einem Zeitraum von 24 Stunden korrekt einzugeben. Wenn das Limit erreicht wird (beispielsweise konnten Sie den Cluster-Passphrase 5 Mal hintereinander nicht korrekt eingeben), müssen Sie entweder warten, bis der 24-Stunden-Timeout abgelaufen ist, oder Sie müssen den Node neu booten, um das Limit zurückzusetzen.

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

  Der Upgrade-Befehl überprüft, ob der Bildinhalt durch Überprüfen verschiedener digitaler Signaturen nicht verändert oder beschädigt wurde. Der Image-Aktualisierungsprozess wird mit dem nächsten Schritt fortgesetzt, wenn die Validierung erfolgreich ist. Andernfalls schlägt die Image-Aktualisierung fehl. Informationen zu System-Updates finden Sie auf der man-Page „`Cluster Image`“.

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

Schritte

1. Starten Sie die Konfiguration des Schlüsselmanagers:

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

   Einstellen `cc-mode-enabled=yes` Um zu verlangen, dass Benutzer nach einem Neustart die Kennverwaltung-Passphrase eingeben. Wenn Sie die Einstellung für NVE verwenden `cc-mode-enabled=yes`, Volumen, die Sie mit erstellen `volume create` Und `volume move start` Befehle werden automatisch verschlüsselt. Der `- cc-mode-enabled` Die Option wird in MetroCluster-Konfigurationen nicht unterstützt. Der `security key-manager onboard enable` Mit dem Befehl wird der ersetzt `security key-manager setup` Befehl.

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

```
cluster1::> security key-manager onboard enable

Enter the cluster-wide passphrase for onboard key management in Vserver
"cluster1"::    <32..256 ASCII characters long text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. 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.

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

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

```
cluster1::> security key-manager key query -key-type NSE-AK
       Vserver: cluster1
   Key Manager: onboard
          Node: node1

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000020000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
000000000000000020000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: svm1
   Key Manager: onboard
          Node: node1
    Key Server: keyserver.svm1.com:5965
```

```
Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
eb9f8311-e8d8-487e-9663-7642d7788a75  VEK       yes
    Key ID:
000000000000000002000000000004001cb18336f7c8223743d3e75c6a7726e00000000
00000000
9d09cbbf-0da9-4696-87a1-8e083d8261bb  VEK       yes
    Key ID:
000000000000000002000000000004064f2e1533356a470385274a9c3ffb97700000000
00000000

       Vserver: cluster1
   Key Manager: onboard
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000

       Vserver: svm1
   Key Manager: onboard
          Node: node2
    Key Server: keyserver.svm1.com:5965

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
eb9f8311-e8d8-487e-9663-7642d7788a75  VEK       yes
    Key ID:
000000000000000002000000000004001cb18336f7c8223743d3e75c6a7726e00000000
00000000
9d09cbbf-0da9-4696-87a1-8e083d8261bb  VEK       yes
    Key ID:
000000000000000002000000000004064f2e1533356a470385274a9c3ffb97700000000
00000000
```

Nachdem Sie fertig sind

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

Alle Informationen zum Verschlüsselungsmanagement werden automatisch in der replizierten Datenbank (RDB) für den Cluster gesichert. Sie sollten die Informationen auch manuell für den Notfall sichern.

Integriertes Verschlüsselungsmanagement in ONTAP 9.5 und früher (NVE)

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.

Was Sie benötigen

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

  "Umstellung auf integriertes Verschlüsselungsmanagement von externem Verschlüsselungsmanagement"

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

Über diese Aufgabe

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

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

- In ONTAP 9.5 müssen Sie ausführen `security key-manager setup` Auf dem lokalen Cluster und `security key-manager setup -sync-metrocluster-config yes` Verwenden Sie im Remote-Cluster jeweils dieselbe Passphrase.
- Vor ONTAP 9.5 müssen Sie ausführen `security key-manager setup` Warten Sie auf dem lokalen Cluster etwa 20 Sekunden, und führen Sie dann den Betrieb aus `security key-manager setup` Verwenden Sie im Remote-Cluster jeweils dieselbe Passphrase.

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

Wenn Sie die Einstellung für NVE verwenden `-enable-cc-mode yes`, Volumen, die Sie mit erstellen `volume create` Und `volume move start` Befehle werden automatisch verschlüsselt. Für `volume create`, Sie müssen nicht angeben `-encrypt true`. Für `volume move start`, Sie müssen nicht angeben `-encrypt-destination true`.

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

Schritte

1. Starten Sie die Konfiguration des Schlüsselmanagers:

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

Ab ONTAP 9.4 können Sie den verwenden `-enable-cc-mode yes` Option zum Eingeben, dass Benutzer nach einem Neustart die Kennwortphrase für das Schlüsselmanagement eingeben. Wenn Sie die Einstellung für NVE verwenden `-enable-cc-mode yes`, Volumen, die Sie mit erstellen `volume create` Und `volume move start` Befehle werden 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. Eingabe `yes` An der Eingabeaufforderung zur Konfiguration des Onboard-Verschlüsselungsmanagement.
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 key show`

   Die vollständige Befehlssyntax finden Sie in der man-Page.

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

Node: node1
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------------
--------
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK
```

Nachdem Sie fertig sind

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

Alle Informationen zum Verschlüsselungsmanagement werden automatisch in der replizierten Datenbank (RDB) für den Cluster gesichert.

Wenn Sie die Onboard Key Manager-Passphrase konfigurieren, sollten Sie die Informationen auch manuell an einem sicheren Ort außerhalb des Speichersystems sichern, um sie bei einem Notfall zu verwenden. Siehe "Manuelles Backup der integrierten Informationen für das Verschlüsselungsmanagement".

Integriertes Verschlüsselungsmanagement bei neu hinzugefügten Nodes

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

Für ONTAP 9.6 und höher müssen Sie den ausführen `security key-manager sync` Befehl jedes Mal, wenn Sie dem Cluster einen Node hinzufügen.

Wenn Sie einem Cluster einen Node hinzufügen, für das das integrierte Verschlüsselungsmanagement konfiguriert ist, führen Sie diesen Befehl aus, um die fehlenden Schlüssel zu aktualisieren.

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

- Ab ONTAP 9.6 müssen Sie ausgeführt werden `security key-manager onboard enable` Führen Sie zuerst auf dem lokalen Cluster aus `security key-manager onboard sync` Verwenden Sie im Remote-Cluster jeweils dieselbe Passphrase.
- In ONTAP 9.5 müssen Sie ausführen `security key-manager setup` Auf dem lokalen Cluster und `security key-manager setup -sync-metrocluster-config yes` Verwenden Sie im Remote-Cluster jeweils dieselbe Passphrase.
- Vor ONTAP 9.5 müssen Sie ausführen `security key-manager setup` Warten Sie auf dem lokalen Cluster etwa 20 Sekunden, und führen Sie dann den Betrieb aus `security key-manager setup` Verwenden Sie im Remote-Cluster jeweils dieselbe Passphrase.

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

Wenn Sie die Einstellung für NVE verwenden `-enable-cc-mode yes`, Volumen, die Sie mit erstellen `volume create` Und `volume move start` Befehle werden automatisch verschlüsselt. Für `volume create`, Sie müssen nicht angeben `-encrypt true`. Für `volume move start`, Sie müssen nicht angeben `-encrypt-destination true`.

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