NetApp Volume Encryption konfigurieren

ONTAP 9

NetApp
March 30, 2023

Inhaltsverzeichnis

NetApp Volume Encryption konfigurieren

NetApp Volume Encryption Übersicht konfigurieren

NetApp Volume Encryption (NVE) ist eine softwarebasierte Technologie, mit der Daten im Ruhezustand um ein Volume gleichzeitig verschlüsselt werden. Ein Verschlüsselungsschlüssel, auf den nur das Storage-System zugegriffen werden kann, stellt sicher, dass Volume-Daten nicht gelesen werden können, wenn das zugrunde liegende Gerät neu verwendet, zurückgegeben, verlegt oder gestohlen wird.

Allgemeines zu NVE

Beide Daten, einschließlich Snapshot Kopien und Metadaten sind verschlüsselt. Der Zugriff auf die Daten erfolgt über einen eindeutigen XTS-AES-256-Schlüssel, einen pro Volume. Ein externer Verschlüsselungsmanagement-Server oder Onboard Key Manager stellt Schlüssel zu Knoten bereit:

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

Ab ONTAP 9.7 ist die Aggregat- und Volume-Verschlüsselung standardmäßig aktiviert, wenn Sie über eine VE-Lizenz (Volume Encryption) verfügen und einen integrierten oder externen Schlüsselmanager verwenden. Bei der Konfiguration eines externen oder integrierten Schlüsselmanagers ändert sich die Konfiguration der Verschlüsselung von Daten im Ruhezustand für brandneue Aggregate und brandneue Volumes. Bei neuen Aggregaten ist die NetApp Aggregate Encryption (NAE) standardmäßig aktiviert. Für brandneue Volumes, die nicht Teil eines NAE-Aggregats sind, ist NetApp Volume Encryption (NVE) standardmäßig aktiviert. Wenn eine Storage Virtual Machine (SVM) mit einem eigenen Schlüsselmanager über mandantenfähiges Verschlüsselungsmanagement konfiguriert wird, wird das für diese SVM erstellte Volume automatisch mit NVE konfiguriert.

Sie können die Verschlüsselung auf einem neuen oder vorhandenen Volume aktivieren. NVE unterstützt eine breite Palette an Storage-Effizienzfunktionen, einschließlich Deduplizierung und Komprimierung.

> Wenn Sie SnapLock verwenden, können Sie nur die Verschlüsselung auf neuen, leeren SnapLock Volumes aktivieren. Sie können die Verschlüsselung auf einem vorhandenen SnapLock-Volume nicht aktivieren.

NVE kann für jeden Aggregattyp (HDD, SSD, Hybrid, Array LUN), mit jedem RAID-Typ und in jeder unterstützten ONTAP Implementierung, einschließlich ONTAP Select, eingesetzt werden. NVE kann auch mit hardwarebasierter Verschlüsselung verwendet werden, um Daten auf Self-Encrypting Drives `double Encryption` zu verschlüsseln.

> AFF A220, AFF A800, FAS2720, FAS2750 und höher speichern Core Dumps auf ihrem Boot-Gerät. Wenn NVE auf diesen Systemen aktiviert ist, wird der Core Dump ebenfalls verschlüsselt.

Verschlüsselung auf Aggregatebene

Normalerweise wird jedem verschlüsselten Volume ein eindeutiger Schlüssel zugewiesen. Wenn das Volume gelöscht wird, wird der Schlüssel mit ihm gelöscht.

Ab ONTAP 9.6 können Sie *NetApp Aggregate Encryption (NAE)* verwenden, um dem zugehörigen Aggregat Schlüssel zuzuweisen, damit die Volumes verschlüsselt werden. Beim Löschen eines verschlüsselten Volumes bleiben die Schlüssel für das Aggregat erhalten. Die Schlüssel werden gelöscht, wenn das gesamte Aggregat gelöscht wird.

Wenn Sie eine Inline- oder eine Hintergrund-Deduplizierung auf Aggregatebene durchführen möchten, muss die Verschlüsselung auf Aggregatebene verwendet werden. Deduplizierung auf Aggregatebene wird ansonsten von NVE nicht unterstützt.

Ab ONTAP 9.7 ist die Aggregat- und Volume-Verschlüsselung standardmäßig aktiviert, wenn Sie über eine VE-Lizenz (Volume Encryption) verfügen und einen integrierten oder externen Schlüsselmanager verwenden.

NVE und NAE-Volumes können gleichzeitig im selben Aggregat bestehen. Bei der Verschlüsselung von Volumes auf Aggregatebene sind standardmäßig NAE-Volumes enthalten. Sie können den Standardwert überschreiben, wenn Sie das Volume verschlüsseln.

Sie können das verwenden `volume move` Befehl zum Konvertieren eines NVE-Volumes in ein NAE-Volume und umgekehrt. Sie können ein NAE-Volume auf ein NVE Volume replizieren.

Verwenden Sie ihn nicht `secure purge` Befehle auf einem NAE-Volume.

Wann sollten Sie externe Verschlüsselungsmanagementserver verwenden

Die Verwendung des Onboard-Schlüsselmanagers ist kostengünstiger und in der Regel bequemer, doch Sie sollten KMIP-Server einrichten, wenn eine der folgenden Angaben zutrifft:

- Ihre Lösung für das Verschlüsselungsmanagement muss den Federal Information Processing Standards (FIPS) 140-2 oder DEM OASIS KMIP Standard entsprechen.
- Sie benötigen eine Multi-Cluster-Lösung mit zentralem Management von Verschlüsselungen.
- Ihr Unternehmen erfordert die zusätzliche Sicherheit beim Speichern von Authentifizierungsschlüsseln auf einem System oder an einem anderen Speicherort als den Daten.

Umfang des externen Schlüsselmanagements

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 im Cluster genannte SVM 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.
- Ab ONTAP 9.10.1 können Sie dies nutzen Azure Key Vault und Google Cloud KMS NVE-Schlüssel nur für Daten-vserver zu schützen.

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.

Eine Liste validierter externer Schlüsselmanager finden Sie im "NetApp Interoperabilitäts-Matrix-Tool (IMT)". Sie können diese Liste finden, indem Sie in die Suchfunktion des IMT den Begriff „wichtige Manager“ eingeben.

Support-Details

In der folgenden Tabelle sind die Support-Details von NVE aufgeführt:

Ressource oder Funktion	Support-Details
Plattformen	Eine AES-NI-Offload-Funktion ist erforderlich. Überprüfen Sie im Hardware Universe (HWU), ob NVE und NAE für Ihre Plattform unterstützt werden.

Verschlüsselung	Ab ONTAP 9.7 werden neu erstellte Aggregate und Volumes standardmäßig verschlüsselt, wenn Sie eine VE-Lizenz (Volume Encryption) hinzufügen und einen integrierten oder externen Schlüsselmanager konfigurieren. Wenn Sie ein unverschlüsseltes Aggregat erstellen müssen, verwenden Sie den folgenden Befehl:
	
	`storage aggregate create -encrypt-with-aggr-key false`
	
	Wenn Sie ein Klartextvolume erstellen müssen, verwenden Sie den folgenden Befehl:
	
	`volume create -encrypt false`
	
	Die Verschlüsselung ist standardmäßig nicht aktiviert, wenn:
	
	• Die VE-Lizenz ist nicht installiert.
	• Schlüsselmanager ist nicht konfiguriert.
	• Plattform oder Software unterstützt keine Verschlüsselung.
	• Die Hardwareverschlüsselung ist aktiviert.

ONTAP	Alle Implementierungen von ONTAP. Unterstützung für ONTAP Cloud ist in ONTAP 9.5 und höher verfügbar.
Geräte	HDD, SSD, Hybrid, Array-LUN.
RAID	RAID0, RAID4, RAID-DP, RAID-TEC.
Volumes	Daten-Volumes und vorhandene Root-Volumes. Daten können nicht auf einem SVM-Root-Volume oder auf MetroCluster Metadaten-Volumes verschlüsselt werden.

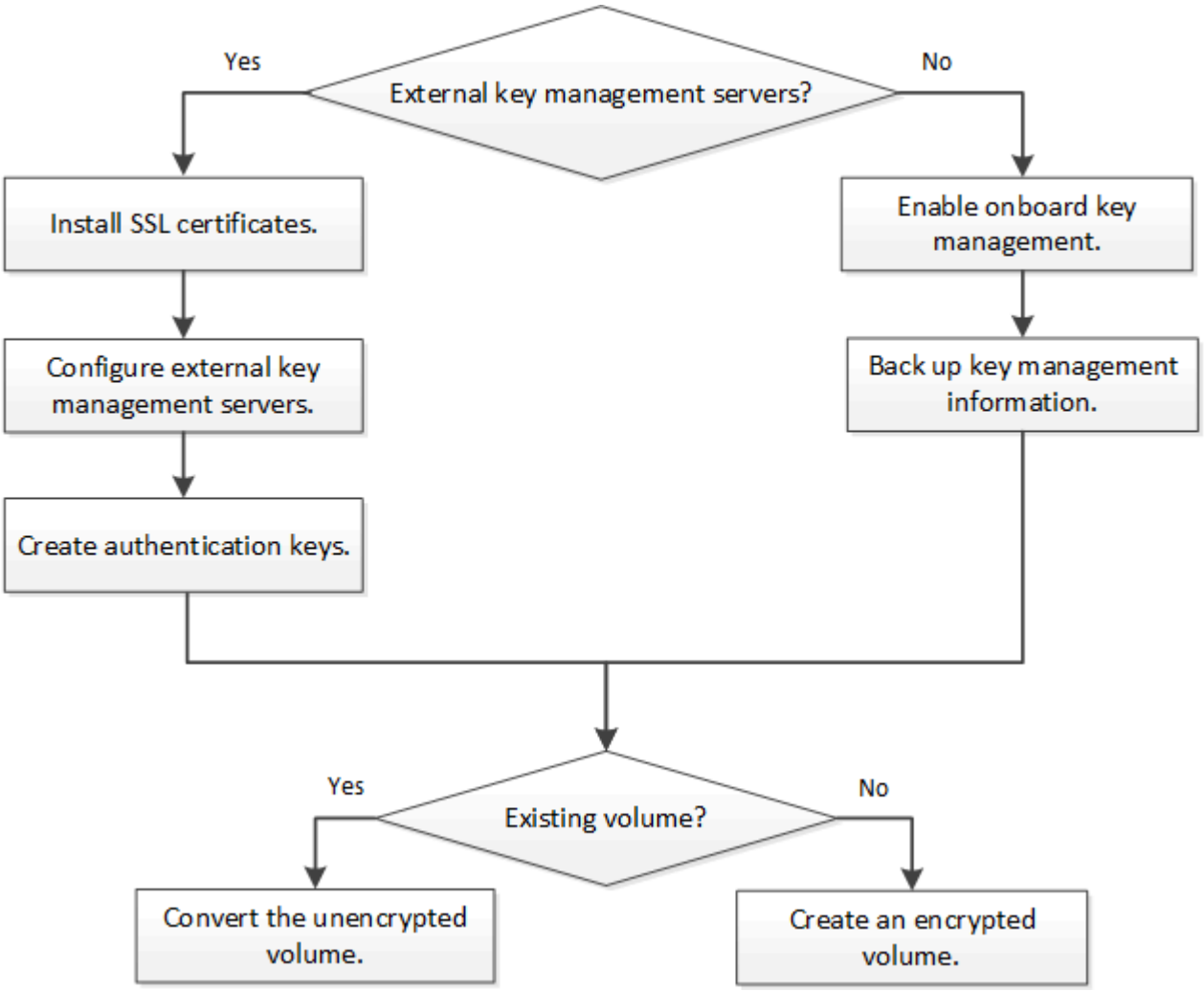
Verschlüsselung auf Aggregatebene	Ab ONTAP 9.6 unterstützt NVE die Verschlüsselung auf Aggregatebene (NAE): • Wenn Sie eine Inline- oder eine Hintergrund-Deduplizierung auf Aggregatebene durchführen möchten, muss die Verschlüsselung auf Aggregatebene verwendet werden. • Sie können ein Verschlüsselungsvolume auf Aggregatebene nicht rekeykey. • Sichere Löschung wird auf Verschlüsselungs-Volumes auf Aggregatebene nicht unterstützt. • Neben Daten-Volumes unterstützt NAE auch die Verschlüsselung von SVM Root-Volumes und dem MetroCluster Metadaten-Volume. NAE unterstützt keine Verschlüsselung des Root-Volumes.
SVM-Umfang	Ab ONTAP 9.6 unterstützt NVE nicht Onboard Key Manager, sondern lediglich den Umfang von SVM für externes Verschlüsselungsmanagement. MetroCluster wird ab ONTAP 9.8 unterstützt.
Storage-Effizienz	Deduplizierung, Komprimierung, Data-Compaction, FlexClone: Klone verwenden denselben Schlüssel wie das übergeordnete Objekt, auch nachdem der Klon vom übergeordneten Objekt geteilt wurde. Sie werden gewarnt, den geteilten Klon erneut zu keylen.
Replizierung	• Für die Volume-Replikation muss das Ziel-Volume zur Verschlüsselung aktiviert sein. Die Verschlüsselung kann für die Quelle konfiguriert und für das Ziel nicht konfiguriert und umgekehrt werden. • Bei der SVM-Replikation wird das Ziel-Volume automatisch verschlüsselt, es sei denn, das Ziel enthält keinen Node, der Volume Encryption unterstützt. In diesem Fall ist die Replikation erfolgreich, das Ziel-Volume ist jedoch nicht verschlüsselt. • Bei MetroCluster-Konfigurationen zieht jedes Cluster externe Verschlüsselungsmanagementschlüssel von den konfigurierten Schlüsselservern ab. OKM-Schlüssel werden vom Konfigurations-Replikationsservice auf den Partnerstandort repliziert.
Compliance	Ab ONTAP 9.2 wird SnapLock sowohl im Compliance- als auch im Enterprise-Modus unterstützt, nur für neue Volumes. Sie können die Verschlüsselung auf einem vorhandenen SnapLock-Volume nicht aktivieren.
FlexGroups	Ab ONTAP 9.2 werden FlexGroups unterstützt. Zielaggregate müssen vom gleichen Typ sein wie Quellaggregate, entweder auf Volume-Ebene oder auf Aggregatebene. Ab ONTAP 9.5 wird auch der in-Place-Rekey von FlexGroup Volumes unterstützt.
Umstieg von 7-Mode	Ab dem 7-Mode Transition Tool 3.3 können Sie mithilfe der CLI des 7-Mode Transition Tool eine Copy-basierte Transition zu NVE-fähigen Ziel-Volumes auf dem geclusterten System durchführen.

Verwandte Informationen

"FAQ – NetApp Volume Encryption und NetApp Aggregate Encryption"

NetApp Volume Encryption Workflow

Sie müssen Verschlüsselungsmanagementservices konfigurieren, bevor Sie die Volume-Verschlüsselung aktivieren können. Sie können die Verschlüsselung auf einem neuen Volume oder auf einem vorhandenen Volume aktivieren.



Bevor Sie Daten mit NVE verschlüsseln können, müssen Sie die VE-Lizenz installieren und Verschlüsselungsmanagementservices konfigurieren. Vor der Installation der Lizenz sollten Sie dies tun "Bestimmen Sie, ob NVE in Ihrer ONTAP-Version unterstützt wird".

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:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
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
--------------------------------------------------------------------
--------
000000000000000002000000000001059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                Used By
--------------------------------------------------------------------
--------
000000000000000002000000000001059851742AF2703FC91369B7DB47C4722 NSE-AK
000000000000000002000000000001008C07CC0AF1EF49E0105300EFC83004BF 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.

Verschlüsseln von Volume-Daten mit NVE

Übersicht über NVE zur Verschlüsselung von Volume-Daten

Ab ONTAP 9.7 ist die Aggregat- und Volume-Verschlüsselung standardmäßig aktiviert, wenn Sie über die VE-Lizenz und die integrierte oder externe Schlüsselverwaltung verfügen. Für ONTAP 9.6 und eine frühere Version können Sie die Verschlüsselung auf einem neuen Volume oder auf einem vorhandenen Volume aktivieren. Bevor Sie die Volume-Verschlüsselung aktivieren können, müssen Sie die VE-Lizenz und die aktivierte Schlüsselverwaltung installiert haben. NVE entspricht FIPS-140-2 Level 1.

Verschlüsselung auf Aggregatebene mit VE-Lizenz aktivieren

Ab ONTAP 9.7 werden neu erstellte Aggregate und Volumes standardmäßig verschlüsselt, wenn Sie über die VE-Lizenz und die integrierte oder externe Schlüsselverwaltung verfügen. Ab ONTAP 9.6 können Sie mithilfe der Verschlüsselung auf Aggregatebene dem enthaltenden Aggregat Schlüssel zuweisen, damit die Volumes verschlüsselt werden können.

Was Sie benötigen

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

Über diese Aufgabe

Wenn Sie eine Inline- oder eine Hintergrund-Deduplizierung auf Aggregatebene durchführen möchten, muss die Verschlüsselung auf Aggregatebene verwendet werden. Deduplizierung auf Aggregatebene wird ansonsten von NVE nicht unterstützt.

Ein Aggregat, das für die Verschlüsselung auf Aggregatebene aktiviert ist, wird als *NAE Aggregat* (für NetApp Aggregatverschlüsselung) bezeichnet. Alle Volumes in einem NAE-Aggregat müssen mit NAE- oder NVE-Verschlüsselung verschlüsselt sein. Bei der Verschlüsselung auf Aggregatebene werden die im Aggregat erstellten Volumes standardmäßig mit NAE-Verschlüsselung verschlüsselt. Sie können die Standardeinstellung für die Verwendung von NVE-Verschlüsselung überschreiben.

Klartextvolumen werden in NAE-Aggregaten nicht unterstützt.

Schritte

1. Aktivieren oder Deaktivieren der Verschlüsselung auf Aggregatebene:

An…	Befehl
Erstellen Sie ein NAE Aggregat mit ONTAP 9.7 oder höher	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`*
Erstellen Sie ein NAE-Aggregat mit ONTAP 9.6	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
Konvertieren Sie ein nicht-NAE Aggregat in ein NAE Aggregat	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
Konvertieren Sie ein NAE Aggregat in ein nicht-NAE Aggregat	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key false`

   Eine vollständige Befehlssyntax finden Sie in den man-Pages.

   Der folgende Befehl ermöglicht die Verschlüsselung auf Aggregatebene `aggr1`:

   - ONTAP 9.7 oder höher:

     ```
     cluster1::> storage aggregate create -aggregate aggr1
     ```

   - ONTAP 9.6 oder früher:

     ```
     cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
     -aggr-key true
     ```

2. Vergewissern Sie sich, dass das Aggregat für die Verschlüsselung aktiviert ist:

   `storage aggregate show -fields encrypt-with-aggr-key`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   Mit dem folgenden Befehl wird das überprüft `aggr1` Für Verschlüsselung aktiviert:

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate            encrypt-aggr-key
-------------------- ----------------
aggr0_vsim4          false
aggr1                true
2 entries were displayed.
```

Nachdem Sie fertig sind

Führen Sie die aus `volume create` Befehl zum Erstellen der verschlüsselten Volumes.

Wenn Sie einen KMIP-Server zum Speichern der Schlüssel für einen Node verwenden, sendet ONTAP bei der Verschlüsselung eines Volumes automatisch „`schiebt`“ einen Verschlüsselungsschlüssel an den Server.

Aktivieren Sie die Verschlüsselung auf einem neuen Volume

Sie können das verwenden `volume create` Befehl zum Aktivieren der Verschlüsselung auf einem neuen Volume.

Über diese Aufgabe

Sie können Volumes mit NetApp Volume Encryption (NVE) und ab ONTAP 9.6 mit NetApp Aggregate Encryption (NAE) verschlüsseln. Weitere Informationen zu NAE und NVE finden Sie im Übersicht über Volume-Verschlüsselung.

Das Verfahren zur Aktivierung der Verschlüsselung auf einem neuen Volume in ONTAP variiert abhängig von der verwendeten ONTAP Version und der spezifischen Konfiguration:

- Beginnend mit ONTAP 9.4, wenn Sie aktivieren `cc-mode` Wenn Sie den Onboard Key M anager einrichten, erstellen Sie mit dem Volumes `volume create` Der Befehl wird automatisch verschlüsselt, unabhängig davon, ob Sie angegeben haben `-encrypt true`.
- In ONTAP 9.6 und älteren Versionen müssen Sie verwenden `-encrypt true` Mit `volume create` Befehle zur Aktivierung der Verschlüsselung (vorausgesetzt, Sie haben die Verschlüsselung nicht aktiviert `cc-mode`).
- Wenn Sie ein NAE-Volume in ONTAP 9.6 erstellen möchten, müssen Sie NAE auf Aggregatebene aktivieren. Siehe Aktivieren Sie die Verschlüsselung auf Aggregatebene mit der VE-Lizenz Für weitere Details zu dieser Aufgabe.
- Ab ONTAP 9.7 werden neu erstellte Volumes standardmäßig verschlüsselt, wenn Sie über die VE-Lizenz und die integrierte oder externe Schlüsselverwaltung verfügen. Standardmäßig sind neue Volumes, die in einem NAE-Aggregat erstellt werden, vom Typ NAE anstatt von NVE aus.
  - Fügen Sie ONTAP 9.7 und höher hinzu `-encrypt true` Bis zum `volume create` Befehl zum Erstellen eines Volumes in einem NAE-Aggregat erhält das Volume NVE-Verschlüsselung statt NAE. Alle Volumes in einem NAE-Aggregat müssen entweder mit NVE oder NAE verschlüsselt sein.

Klartext-Volumes werden in NAE-Aggregaten nicht unterstützt.

Schritte

1. Erstellen Sie ein neues Volume, und geben Sie an, ob die Verschlüsselung auf dem Volume aktiviert ist. Wenn das neue Volume sich in einem NAE-Aggregat befindet, ist das Volume standardmäßig ein NAE-

Volume:

Zu erstellen…	Befehl
Ein NAE-Band	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`*
Ein NVE Volume	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt true` + In ONTAP 9.6 und früher, wo NAE nicht unterstützt wird, `-encrypt true` Gibt an, dass das Volume mit NVE verschlüsselt werden soll. In ONTAP 9.7 und höher wo Volumes in NAE-Aggregaten erstellt werden, `-encrypt true` Überschreibt stattdessen den Standardverschlüsselungstyp von NAE, um ein NVE Volume zu erstellen.
Nur-Text-Lautstärke	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt false`

Vollständige Befehlssyntax finden Sie auf der Befehlssyntax für Link:https://docs.netapp.com/us-en/ontap-cli-9121/volume-create.html[`volume create`^].

2. Vergewissern Sie sich, dass Volumes für die Verschlüsselung aktiviert sind:

   `volume show -is-encrypted true`

   Eine vollständige Befehlssyntax finden Sie im "Befehlsreferenz".

Ergebnis

Wenn Sie einen KMIP-Server zum Speichern der Schlüssel für einen Node verwenden, „sendet“ ONTAP bei der Verschlüsselung eines Volumes automatisch einen Verschlüsselungsschlüssel an den Server.

Aktivieren Sie die Verschlüsselung auf einem vorhandenen Volume mit dem Befehl zur Konvertierung der Volume-Verschlüsselung

Ab ONTAP 9.3 können Sie den verwenden `volume encryption conversion start` Befehl, um die Verschlüsselung eines vorhandenen Volume „in place“ zu aktivieren, ohne das Volume an einen anderen Speicherort verschieben zu müssen.

Über diese Aufgabe

Sobald Sie einen Konvertierungsvorgang starten, muss er abgeschlossen sein. Wenn während des Vorgangs ein Leistungsproblem auftritt, können Sie das ausführen `volume encryption conversion pause` Befehl zum Anhalten des Vorgangs, und `volume encryption conversion resume` Befehl zum Fortsetzen des Vorgangs.

Verwenden Sie ihn nicht `volume encryption conversion start` Um ein SnapLock Volume zu konvertieren.

Schritte

1. Verschlüsselung auf einem vorhandenen Volume aktivieren:

   `volume encryption conversion start -vserver SVM_name -volume volume_name`

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

   Mit dem folgenden Befehl wird die Verschlüsselung auf dem vorhandenen Volume aktiviert `vol1`:

   ```
   cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
   ```

   Das System erstellt einen Verschlüsselungsschlüssel für das Volume. Die Daten auf dem Volume werden verschlüsselt.

2. Überprüfen Sie den Status des Konvertierungsvorgangs:

   `volume encryption conversion show`

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

   Mit dem folgenden Befehl wird der Status des Konvertierungsvorgangs angezeigt:

   ```
   cluster1::> volume encryption conversion show

   Vserver   Volume   Start Time           Status
   -------   ------   ------------------   ---------------------------
   vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
   ```

3. Wenn der Konvertierungsvorgang abgeschlossen ist, vergewissern Sie sich, dass das Volume für die Verschlüsselung aktiviert ist:

   `volume show -is-encrypted true`

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

   Mit dem folgenden Befehl werden die verschlüsselten Volumes auf angezeigt `cluster1`:

   ```
   cluster1::> volume show -is-encrypted true

   Vserver  Volume  Aggregate  State  Type  Size  Available  Used
   -------  ------  ---------  -----  ----  -----  --------- ----
   vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
   ```

Ergebnis

Wenn Sie einen KMIP-Server zum Speichern der Schlüssel für einen Node verwenden, sendet ONTAP bei der Verschlüsselung eines Volumes automatisch „`schiebt`“ einen Verschlüsselungsschlüssel an den Server.

Aktivieren Sie die Verschlüsselung auf einem vorhandenen Volume mit dem Befehl Volume move Start

Sie können das verwenden `volume move start` Befehl zum Aktivieren der Verschlüsselung durch Verschieben eines vorhandenen Volumes Sie müssen verwenden `volume move start` In ONTAP 9.2 und früher. Sie können dasselbe oder ein anderes Aggregat verwenden.

Was Sie benötigen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe durchzuführen, oder ein SVM-Administrator, an den der Cluster-Administrator die Berechtigungen delegiert hat.

"Delegieren von Berechtigungen zum Ausführen des Befehls zum Verschieben von Volumes"

Über diese Aufgabe

Ab ONTAP 9.8 können Sie dies nutzen `volume move start` Aktivieren der Verschlüsselung auf einem SnapLock oder FlexGroup Volume

Beginnend mit ONTAP 9.4, wenn Sie beim Einrichten des Onboard Key Managers „`cc-Mode`“ aktivieren, werden die mit dem erstellten Volumes erstellt `volume move start` Befehl wird automatisch verschlüsselt. Sie müssen nicht angeben `-encrypt-destination true`.

Ab ONTAP 9.6 können Sie mithilfe der Verschlüsselung auf Aggregatebene dem enthaltenden Aggregat Schlüssel zuweisen, damit die Volumes verschoben werden können. Ein mit einem eindeutigen Schlüssel verschlüsseltes Volume wird als *NVE Volume* bezeichnet. Ein mit einem Aggregatschlüssel verschlüsseltes Volume wird als *NAE Volume* (für NetApp Aggregate Encryption) bezeichnet. Klartext-Volumes werden in NAE-Aggregaten nicht unterstützt.

Schritte

1. Verschieben Sie ein vorhandenes Volume und geben Sie an, ob die Verschlüsselung auf dem Volume aktiviert ist:

Konvertieren…	Befehl
Ein Klartext-Volume auf ein NVE Volume	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination true`
Ein NVE oder Klartext Volume auf ein NAE Volume (vorausgesetzt, die Verschlüsselung auf Aggregatebene ist auf dem Zielsystem aktiviert)	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key true`
Ein NAE-Volume auf ein NVE Volume	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key false`

Ein NAE-Volumen zu einem Klartext-Volumen	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false`
Ein NVE Volume auf ein Klartext-Volume	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false`

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

Mit dem folgenden Befehl wird ein Klartext-Volume mit dem Namen konvertiert `vol1` Zu einem NVE Volume:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

Wenn die Verschlüsselung auf Aggregatebene auf dem Zielsystem aktiviert ist, wird mit dem folgenden Befehl ein NVE oder ein Klartext Volume mit dem Namen konvertiert `vol1` Zu einem NAE-Band:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

Mit dem folgenden Befehl wird ein NAE-Volume mit dem Namen konvertiert `vol2` Zu einem NVE Volume:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

Mit dem folgenden Befehl wird ein NAE-Volume mit dem Namen konvertiert `vol2` Zu einem Klartext-Volumen:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

Mit dem folgenden Befehl wird ein NVE-Volume mit dem Namen konvertiert `vol2` Zu einem Klartext-Volumen:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

2. Zeigen Sie den Verschlüsselungstyp von Cluster Volumes an:

`volume show -fields encryption-type none|volume|aggregate`

Der `encryption-type` Field steht in ONTAP 9.6 und höher zur Verfügung.

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

Mit dem folgenden Befehl wird der Verschlüsselungstyp von Volumes in angezeigt `cluster2`:

```
cluster2::> volume show -fields encryption-type

vserver  volume  encryption-type
-------  ------  ---------------
vs1      vol1    none
vs2      vol2    volume
vs3      vol3    aggregate
```

3. Vergewissern Sie sich, dass Volumes für die Verschlüsselung aktiviert sind:

   `volume show -is-encrypted true`

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

   Mit dem folgenden Befehl werden die verschlüsselten Volumes auf angezeigt `cluster2`:

```
cluster2::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

Ergebnis

Wenn Sie einen KMIP-Server zum Speichern der Schlüssel für einen Node verwenden, sendet ONTAP bei der Verschlüsselung eines Volumes automatisch „`schiebt`“ einen Verschlüsselungsschlüssel an den Server.

Node-Root-Volume-Verschlüsselung aktivieren

Ab ONTAP 9.8 können Sie NetApp Volume Encryption zum Schutz des Root-Volumes des Nodes verwenden.

Was Sie benötigen

- Ihr System muss eine HA-Konfiguration verwenden.

  Die Root-Volume-Verschlüsselung wird in Konfigurationen mit einem Node nicht unterstützt.

- Das Root-Volume des Nodes muss bereits erstellt werden.
- Ihr System muss über einen integrierten Schlüsselmanager oder einen externen Verschlüsselungsmanagement-Server mit dem Key Management Interoperability Protocol (KMIP)

verfügen.

Über diese Aufgabe

Dieses Verfahren gilt für das Root-Volume des Nodes. Sie gilt nicht für SVM-Root-Volumes. SVM-Root-Volumes können durch Verschlüsselung auf Aggregatebene gesichert werden.

Sobald die Verschlüsselung des Root-Volumes beginnt, muss sie abgeschlossen sein. Sie können den Vorgang nicht unterbrechen. Nach Abschluss der Verschlüsselung können Sie dem Root-Volume keinen neuen Schlüssel zuweisen und keine sichere Löschung durchführen.

Schritte

1. Verschlüsseln Sie das Root-Volume:

   ```
   volume encryption conversion start -vserver SVM_name -volume root_vol_name
   ```

2. Überprüfen Sie den Status des Konvertierungsvorgangs:

   ```
   volume encryption conversion show
   ```

3. Nach Abschluss des Konvertierungsvorgangs muss überprüft werden, ob das Volume verschlüsselt ist:

   ```
   volume show -fields
   ```

   Das folgende zeigt eine Beispielausgabe für ein verschlüsseltes Volume.

   ```
   ::> volume show -vserver xyz  -volume vol0 -fields is-encrypted
   vserver    volume is-encrypted
   ---------- ------ ------------
   xyz        vol0   true
   ```