Management der Verschlüsselung über CLI

ONTAP 9

NetApp
September 12, 2024

Inhalt

Management der Verschlüsselung über CLI

Übersicht über die NetApp Verschlüsselung

NetApp bietet sowohl Software- als auch hardwarebasierte Verschlüsselungstechnologien, um sicherzustellen, dass Daten im Ruhezustand nicht gelesen werden können, wenn das Storage-Medium neu verwendet, zurückgegeben, verloren gegangen oder gestohlen wird.

- Softwarebasierte Verschlüsselung unter Verwendung von NetApp Volume Encryption (NVE) unterstützt die Datenverschlüsselung für ein Volume gleichzeitig
- Hardwarebasierte Verschlüsselung mit NetApp Storage Encryption (NSE) unterstützt die vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) von Daten beim Schreiben.

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

Mit NVE werden Metadaten und Daten (einschließlich Snapshot Kopien) verschlüsselt. Der Zugriff auf die Daten erfolgt über einen eindeutigen XTS-AES-256-Schlüssel, einen pro Volume. Ein externer Schlüsselmanagementserver oder Onboard Key Manager (OKM) bedient Schlüssel zu Knoten:

- 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. Die VE-Lizenz ist im Lieferumfang enthalten"ONTAP One". 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. Ab ONTAP

9.14.1 ist dies möglich Aktivieren Sie NVE bei vorhandenen SVM-Root-Volumes.

> 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.

Wenn NVE 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 Zum Schutz von NVE-Schlüsseln nur für Daten-SVMs Dies ist für KMS von AWS ab 9.12.0 verfügbar.

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 SVM-Root-Volumes. Daten auf MetroCluster Metadaten-Volumes können nicht verschlüsselt werden. Bei älteren Versionen als ONTAP 9.14.1 können Daten auf dem SVM-Root-Volume nicht mit NVE verschlüsselt werden. Ab ONTAP 9.14.1 unterstützt ONTAP NVE auf SVM Root-Volumes.
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 sollten eine durchführen `volume move` Auf einem geteilten Klon, nach dem der geteilte Klon einen anderen Schlüssel hat.
Replizierung	• Für die Volume-Replikation können die Quell- und Ziel-Volumes über unterschiedliche Verschlüsselungseinstellungen verfügen. 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.

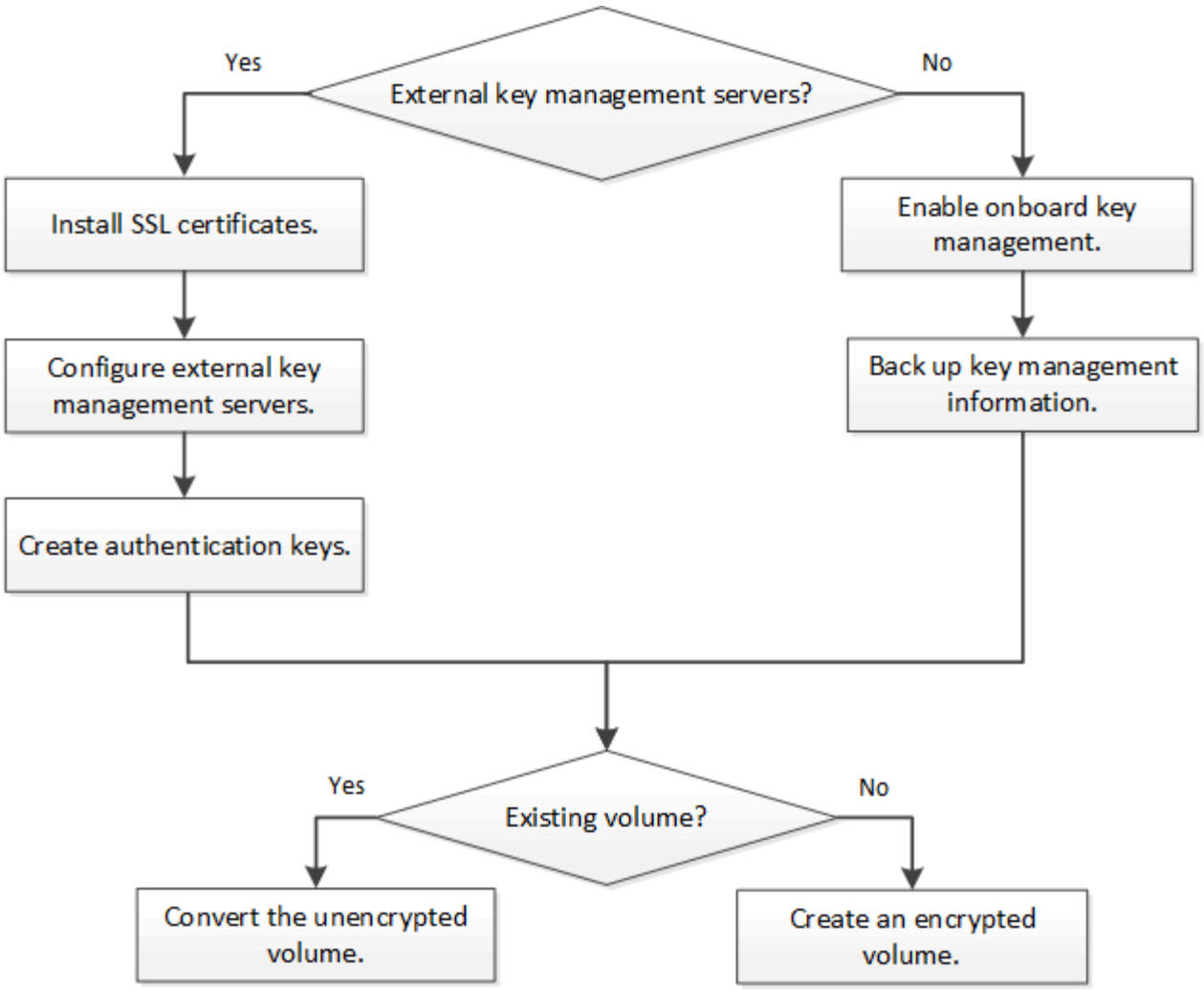
Compliance	Ab ONTAP 9.2 wird SnapLock sowohl im Compliance- als auch im Enterprise-Modus unterstützt, nur für neue Volumes. Sie können die Verschlüsselung auf einem vorhandenen SnapLock-Volume nicht aktivieren.
FlexGroups	Ab ONTAP 9.2 werden FlexGroups unterstützt. Zielaggregate müssen vom gleichen Typ 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.



"Sie müssen die VE-Lizenz installieren" Und konfigurieren Sie Verschlüsselungsmanagement-Services, bevor Sie Daten mit NVE verschlüsseln können. Vor der Installation der Lizenz sollten Sie "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. Diese Lizenz ist erforderlich, bevor Sie Daten mit NVE verschlüsseln können. Es ist im Lieferumfang enthalten"ONTAP One".

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

Bevor Sie beginnen

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

Schritte

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

   Der Name des VE-Lizenzpakets lautet `VE`.

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

Externes Verschlüsselungsmanagement konfigurieren

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.

Management von externen Schlüsselmanagern mit System Manager

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

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

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

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

Konfigurieren Sie einen externen Schlüsselmanager

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

Schritte

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

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

Workflow	Navigation	Startschritt
Konfigurieren Sie Key Manager	**Cluster** > **Einstellungen**	Blättern Sie zum Abschnitt **Sicherheit**. Wählen Sie unter **Verschlüsselung** ⚙. Wählen Sie **External Key Manager**.
Lokale Ebene hinzufügen	**Storage** > **Tiers**	Wählen Sie **+ Lokale Ebene Hinzufügen**. Aktivieren Sie das Kontrollkästchen „Key Manager konfigurieren“. Wählen Sie **External Key Manager**.
Storage vorbereiten	**Dashboard**	Wählen Sie im Abschnitt **Kapazität** die Option **Speicher vorbereiten** aus. Wählen Sie dann „Configure Key Manager“ aus. Wählen Sie **External Key Manager**.

Konfiguration der Verschlüsselung (nur Schlüsselmanager im Umfang von Storage-VMs)	**Storage** > **Storage VMs**	Wählen Sie die Storage-VM aus. Wählen Sie die Registerkarte **Einstellungen**. Wählen Sie im Abschnitt **Verschlüsselung** unter **Sicherheit** die Option ⚙.

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

Bearbeiten Sie einen vorhandenen externen Schlüsselmanager

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

Schritte

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

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

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

Löschen Sie einen externen Schlüsselmanager

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

Schritte

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

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

Schlüssel zwischen Schlüsselmanagern migrieren

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

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

Installieren Sie SSL-Zertifikate auf dem Cluster

Das Cluster und der KMIP-Server verwenden KMIP SSL-Zertifikate, um die Identität des jeweils anderen zu überprüfen und eine SSL-Verbindung herzustellen. Vor dem Konfigurieren der SSL-Verbindung mit dem KMIP-Server müssen die KMIP-Client-SSL-Zertifikate für das Cluster und das öffentliche SSL-Zertifikat für die Root-Zertifizierungsstelle des KMIP-Servers installiert werden.

Über diese Aufgabe

In einem HA-Paar müssen beide Nodes dieselben öffentlichen und privaten KMIP-SSL-Zertifikate verwenden. Wenn Sie mehrere HA-Paare mit demselben KMIP-Server verbinden, müssen alle Nodes der HA-Paare dieselben öffentlichen und privaten KMIP-SSL-Zertifikate verwenden.

Bevor Sie beginnen

- Die Zeit muss auf dem Server synchronisiert werden, der die Zertifikate, den KMIP-Server und das Cluster erstellt.
- Sie müssen das öffentliche SSL KMIP-Client-Zertifikat für den Cluster erhalten haben.

- Sie müssen den privaten Schlüssel für das SSL KMIP Client-Zertifikat für das Cluster erhalten haben.
- Das SSL KMIP-Client-Zertifikat darf nicht durch ein Passwort geschützt sein.
- Sie müssen das öffentliche SSL-Zertifikat für die Root-Zertifizierungsstelle (CA) des KMIP-Servers erhalten haben.
- In einer MetroCluster-Umgebung müssen Sie auf beiden Clustern dieselben KMIP-SSL-Zertifikate installieren.

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

Schritte

1. Installieren Sie die SSL KMIP-Client-Zertifikate für das Cluster:

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

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

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

2. Installieren Sie das öffentliche SSL-Zertifikat für die Root-Zertifizierungsstelle (CA) des KMIP-Servers:

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

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

Externes Verschlüsselungsmanagement in ONTAP 9.6 und höher (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 bis zu 3 sekundäre Schlüsselserver pro primären Schlüsselserver hinzufügen, um einen geclusterten Schlüsselserver zu erstellen. Weitere Informationen finden Sie unter Konfigurieren Sie externe geclusterte Schlüsselserver.

Über diese Aufgabe

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

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.

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.
```

5. Konvertieren Sie optional Klartextvolumes in verschlüsselte Volumes.

   ```
   volume encryption conversion start
   ```

   Ein externer Schlüsselmanager muss vollständig konfiguriert sein, bevor Sie die Volumes konvertieren. In einer MetroCluster-Umgebung muss auf beiden Seiten ein externer Schlüsselmanager konfiguriert werden.

Ermöglichen Sie externes Verschlüsselungsmanagement in ONTAP 9.5 und früher

Ein oder mehrere KMIP-Server dienen zur Sicherung der Schlüssel, die das Cluster für den Zugriff auf verschlüsselte Daten verwendet. Mit einem Node können bis zu vier KMIP-Server verbunden werden. Für Redundanz und Disaster Recovery werden mindestens zwei Server empfohlen.

Über diese Aufgabe

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

Bevor Sie beginnen

- Die KMIP SSL-Client- und Serverzertifikate müssen installiert sein.
- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Sie müssen die MetroCluster Umgebung konfigurieren, bevor Sie einen externen Schlüsselmanager konfigurieren.
- In einer MetroCluster-Umgebung müssen Sie das KMIP SSL-Zertifikat auf beiden Clustern installieren.

Schritte

1. Konfigurieren Sie die Schlüsselmanager-Konnektivität für Cluster-Nodes:

   ```
   security key-manager setup
   ```

   Die Konfiguration des Schlüsselmanagers wird gestartet.

   > In einer MetroCluster-Umgebung müssen Sie den folgenden Befehl auf beiden Clustern ausführen.

2. Geben Sie an jeder Eingabeaufforderung die entsprechende Antwort ein.
3. Hinzufügen eines KMIP-Servers:

   ```
   security key-manager add -address key_management_server_ipaddress
   ```

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

   > In einer MetroCluster-Umgebung müssen Sie den folgenden Befehl auf beiden Clustern ausführen.

4. Fügen Sie aus Redundanzgründen einen zusätzlichen KMIP-Server hinzu:

   ```
   security key-manager add -address key_management_server_ipaddress
   ```

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

   > In einer MetroCluster-Umgebung müssen Sie den folgenden Befehl auf beiden Clustern ausführen.

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

   ```
   security key-manager show -status
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

   Node             Port      Registered Key Manager  Status
   --------------   ----      -----------------------  ---------------
   cluster1-01      5696      20.1.1.1                available
   cluster1-01      5696      20.1.1.2                available
   cluster1-02      5696      20.1.1.1                available
   cluster1-02      5696      20.1.1.2                available
   ```

6. Konvertieren Sie optional Klartextvolumes in verschlüsselte Volumes.

```
volume encryption conversion start
```

Ein externer Schlüsselmanager muss vollständig konfiguriert sein, bevor Sie die Volumes konvertieren. In einer MetroCluster-Umgebung muss auf beiden Seiten ein externer Schlüsselmanager konfiguriert werden.

Schlüsselmanagement bei einem Cloud-Provider

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 Cloud-gehosteten Applikation. Ab ONTAP 9.12.0 können Sie auch NVE-Schlüssel mit schützen "KMS VON AWS".

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

Über diese Aufgabe

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

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

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

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

Bevor Sie beginnen

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

Externes Verschlüsselungsmanagement

Die Aktivierung des externen Schlüsselmanagements hängt von dem jeweiligen Schlüsselmanager ab, den Sie

verwenden. Wählen Sie die Registerkarte des entsprechenden Schlüsselmanagers und der entsprechenden Umgebung aus.

AWS

Bevor Sie beginnen

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

  Weitere Informationen finden Sie in der AWS-Dokumentation für "Zuschüsse".

Aktivieren Sie AWS KMV auf einer ONTAP SVM

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

Azure

Aktivieren Sie Azure Key Vault auf einer ONTAP SVM

1. Bevor Sie beginnen, müssen Sie die entsprechenden Authentifizierungsdaten von Ihrem Azure-Konto beziehen, entweder ein Clientgeheimnis oder ein Zertifikat. Sie müssen außerdem sicherstellen, dass alle Nodes im Cluster sich in einem ordnungsgemäßen Zustand befinden. Sie können dies mit dem Befehl überprüfen `cluster show`.
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 Service nicht in Ordnung ist, stellen Sie die Verbindung zum AKV Key Management Service über die LIF der Daten-SVM her.

Google Cloud

Aktivieren Sie Cloud-KMS auf einer ONTAP SVM

1. Bevor Sie beginnen, erhalten Sie den privaten Schlüssel für die Google Cloud KMS-Kontoschlüsseldatei in einem JSON-Format. Dieser Punkt ist in Ihrem GCP-Konto enthalten.
   Sie müssen außerdem sicherstellen, dass alle Nodes im Cluster sich in einem ordnungsgemäßen

Zustand befinden. Sie können dies mit dem Befehl überprüfen `cluster show`.

2. Privilegierte Ebene auf erweitert setzen:
   `set -priv advanced`
3. Aktivieren Sie Cloud KMS auf der SVM
   `security key-manager external gcp enable -vserver` *`svm_name`* `-project-id` *`project_id`*`-key-ring-name` *`key_ring_name`* `-key-ring-location` *`key_ring_location`* `-key-name` *`key_name`*
   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*` Erst dann können neue verschlüsselte Volumes für die Daten-SVM des Mandanten erstellt werden, wenn alle NVE-Schlüssel der Daten-SVM erfolgreich migriert wurden.

Verwandte Informationen

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

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 den Onboard Key Manager für jedes Cluster aktivieren, das auf ein verschlüsseltes Volume oder eine selbstverschlüsselnde Festplatte zugreift.

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 den ausführen `security key-manager onboard enable` Führen Sie zunächst den Befehl auf dem lokalen Cluster aus, und führen Sie dann den aus `security key-manager onboard sync` Auf dem Remote-Cluster unter Verwendung derselben Passphrase auf beiden. Wenn Sie den ausführen `security key-manager onboard enable` Vom lokalen Cluster aus und dann auf dem Remote-Cluster synchronisieren, müssen Sie den nicht ausführen `enable` Führen Sie einen neuen Befehl aus dem Remote-Cluster aus.

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. Siehe `cluster image` Man-Page für Informationen zu Systemaktualisierungen.

> 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.

Bevor Sie beginnen

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

Schritte

1. Starten Sie die Konfiguration des Schlüsselmanagers:

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

> 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
               Node: node1
            Vserver: cluster1
        Key Manager: onboard
   Key Manager Type: OKM
 Key Manager Policy: -

 Key Tag                                Key Type Encryption   Restored

------------------------------------  -------- ------------ --------

node1                                  NSE-AK   AES-256      true

    Key ID:
00000000000000000200000000000100056178fc6ace6d91472df8a9286daacc00000000
00000000

node1                                  NSE-AK   AES-256      true

    Key ID:
00000000000000000200000000000100df1689a148fdfbf9c2b198ef974d0baa00000000
00000000

2 entries were displayed.
```

5. Konvertieren Sie optional Klartextvolumes in verschlüsselte Volumes.

   `volume encryption conversion start`

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

Nachdem Sie fertig sind

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

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 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.

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.

Bevor Sie beginnen

- Wenn Sie NSE oder NVE 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.

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
```

6. Konvertieren Sie optional Klartextvolumes in verschlüsselte Volumes.

   ```
   volume encryption conversion start
   ```

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

Nachdem Sie fertig sind

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

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 sind neu erstellte Aggregate und Volumes standardmäßig verschlüsselt, wenn Sie über "VE-Lizenz"ein integriertes oder externes Verschlüsselungsmanagement verfügen. Ab ONTAP 9.6 können Sie mithilfe der Verschlüsselung auf Aggregatebene dem enthaltenden Aggregat Schlüssel zuweisen, damit die Volumes verschlüsselt werden können.

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.

Bevor Sie beginnen

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

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 Manager einrichten, erstellen Sie die Volumes mit dem `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 das "VE-Lizenz"integrierte oder externe Verschlüsselungsmanagement 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`

Eine vollständige Befehlssyntax finden Sie auf der Befehlsseite für Link:https://docs.netapp.com/us-en/ontap-cli/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 für ONTAP".

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.

=
:allow-uri-read:

Aktivieren Sie die Verschlüsselung auf einem vorhandenen Volume

Sie können entweder die verwenden `volume move start` Oder im `volume encryption conversion start` Den Befehl, um die Verschlüsselung auf einem vorhandenen Volume zu aktivieren.

Über diese Aufgabe

- 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. Alternativ können Sie den verwenden `volume move start` Befehl.
- Bei ONTAP 9.2 und älteren Versionen können Sie nur die verwenden `volume move start` Befehl zum Aktivieren der Verschlüsselung durch Verschieben eines vorhandenen Volumes

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.

Nachdem Sie eine Konvertierung gestartet haben, muss diese 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`

   Die gesamte Befehlssyntax finden Sie auf der man-Page für den Befehl.

   Mit dem folgenden Befehl wird die Verschlüsselung für ein vorhandenes 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`

   Die gesamte Befehlssyntax finden Sie auf 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, überprüfen Sie, ob das Volume für die Verschlüsselung aktiviert ist:

   `volume show -is-encrypted true`

   Die gesamte Befehlssyntax finden Sie auf 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.

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 (d. h., es verwendet NetApp Volume Encryption). Ein mit einem Aggregatschlüssel verschlüsseltes Volume wird als *NAE Volume* (für NetApp Aggregate Encryption) bezeichnet. Klartext-Volumes werden in NAE-Aggregaten nicht unterstützt.
- Ab ONTAP 9.14.1 können Sie ein SVM Root-Volume mit NVE verschlüsseln. Weitere Informationen finden Sie unter Konfiguration der NetApp-Volume-Verschlüsselung auf einem SVM-Root-Volume.

Bevor Sie beginnen

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"

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`

Die gesamte Befehlssyntax finden Sie auf 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.

   Die gesamte Befehlssyntax finden Sie auf 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`

   Die gesamte Befehlssyntax finden Sie auf 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 zur Speicherung der Verschlüsselungsschlüssel für einen Node verwenden, überträgt ONTAP bei der Verschlüsselung eines Volumes automatisch einen Verschlüsselungsschlüssel an den Server.

Konfiguration der NetApp-Volume-Verschlüsselung auf einem SVM-Root-Volume

Ab ONTAP 9.14.1 können Sie die NetApp Volume Encryption (NVE) auf einem Storage

VM (SVM) Root-Volume aktivieren. Mit NVE wird das Root-Volume mit einem eindeutigen Schlüssel verschlüsselt, was für mehr Sicherheit auf der SVM sorgt.

Über diese Aufgabe

NVE auf einem SVM-Root-Volume kann nur aktiviert werden, nachdem die SVM erstellt wurde.

Bevor Sie beginnen

- Das SVM-Root-Volume darf sich nicht auf einem mit der NetApp-Aggregatverschlüsselung (NAE) verschlüsselten Aggregat befinden.
- Sie müssen die Verschlüsselung mit dem Onboard Key Manager oder einem externen Schlüsselmanager aktiviert haben.
- Sie müssen ONTAP 9.14.1 oder höher ausführen.
- Um eine SVM, die ein mit NVE verschlüsseltes Root-Volume enthält, zu migrieren, müssen Sie das SVM-Root-Volume nach Abschluss der Migration in ein Klartextvolume konvertieren und anschließend das SVM-Root-Volume neu verschlüsseln.
  - Wenn das Zielaggregat der SVM Migration NAE verwendet, übernimmt das Root-Volume standardmäßig NAE.
- Wenn sich die SVM in einer SVM-Disaster-Recovery-Beziehung befindet:
  - Verschlüsselungseinstellungen auf einer gespiegelten SVM werden nicht an das Ziel kopiert. Wenn Sie NVE auf dem Quell- oder Zielsystem aktivieren, müssen Sie NVE auf dem gespiegelten SVM Root-Volume separat aktivieren.
  - Wenn alle Aggregate im Ziel-Cluster NAE verwenden, verwendet das SVM Root-Volume NAE.

Schritte

Sie können NVE auf einem SVM Root-Volume mit der ONTAP CLI oder mit System Manager aktivieren.

CLI

Sie können NVE auf dem Root-Volume der SVM aktivieren oder das Volume zwischen den Aggregaten verschieben.

Verschlüsseln Sie das Root-Volume

1. Konvertieren Sie das Root-Volume in ein verschlüsseltes Volume:

   ```
   volume encryption conversion start -vserver svm_name -volume volume
   ```

2. Bestätigen Sie, dass die Verschlüsselung erfolgreich war. Der `volume show -encryption-type volume` Zeigt eine Liste aller Volumes mit NVE an.

Verschlüsseln Sie das SVM-Root-Volume durch Verschieben

1. Volume-Verschiebung initiieren:

   ```
   volume move start -vserver svm_name -volume volume -destination-aggregate
   aggregate -encrypt-with-aggr-key false -encrypt-destination true
   ```

   Finden Sie weitere Informationen zu `volume move`, Siehe Verschieben Sie ein Volume.

2. Bestätigen Sie das `volume move` Vorgang erfolgreich mit dem ausgeführt `volume move show` Befehl. Der `volume show -encryption-type volume` Zeigt eine Liste aller Volumes mit NVE an.

System Manager

1. Navigieren Sie zu **Storage** > **Volumes**.
2. Wählen Sie neben dem Namen des SVM-Root-Volumes, das Sie verschlüsseln möchten, ⋮ dann **Bearbeiten**.
3. Wählen Sie unter der Überschrift **Speicherung und Optimierung** die Option **Verschlüsselung aktivieren**.
4. Wählen Sie **Speichern**.

Node-Root-Volume-Verschlüsselung aktivieren

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

Über diese Aufgabe

Dieses Verfahren gilt für das Root-Volume des Nodes. Sie gilt nicht für SVM-Root-Volumes. Root-Volumes von SVM können durch Verschlüsselung auf Aggregatebene geschützt werden, Ab ONTAP 9.14.1 ist NVE der Fall.

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.

Bevor Sie beginnen

- Ihr System muss eine HA-Konfiguration verwenden.

- 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.

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
   ```

Konfigurieren Sie die hardwarebasierte NetApp Verschlüsselung

Konfiguration der hardwarebasierten NetApp Verschlüsselung – Übersicht

Die hardwarebasierte Verschlüsselung von NetApp unterstützt die vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) von Daten beim Schreiben. Ohne einen auf der Firmware gespeicherten Verschlüsselungsschlüssel können die Daten nicht gelesen werden. Der Verschlüsselungsschlüssel wiederum ist nur für einen authentifizierten Knoten zugänglich.

Allgemeines zur hardwarebasierten Verschlüsselung von NetApp

Ein Node authentifiziert sich selbst auf einem Self-Encrypting Drive, wobei ein Authentifizierungsschlüssel von einem externen Verschlüsselungsmanagement-Server oder Onboard Key Manager abgerufen wird:

- 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 integrierte Onboard Key Manager ist ein Tool, das Authentifizierungsschlüssel für Nodes aus demselben Storage-System wie Ihre Daten bereitstellt.

Mit NetApp Volume Encryption mit hardwarebasierter Verschlüsselung können Daten auf Self-Encrypting Drives `double Encryption` verschlüsselt werden.

Bei Aktivierung von Self-Encrypting Drives wird der Core Dump ebenfalls verschlüsselt.

> Wenn ein HA-Paar SAS- oder NVMe-Laufwerke (SED, NSE, FIPS) verwendet, müssen Sie die Anweisungen im Thema befolgen Ein FIPS-Laufwerk oder eine SED-Festplatte in den ungeschützten Modus zurückkehren Für alle Laufwerke innerhalb des HA-Paars vor der Initialisierung des Systems (Boot-Optionen 4 oder 9). Andernfalls kann es zu künftigen Datenverlusten kommen, wenn die Laufwerke einer anderen Verwendung zugewiesen werden.

Unterstützte Self-Encrypting Drives

Es werden zwei Arten von Self-Encrypting Drives unterstützt:

- FIPS-zertifizierte Self-Encrypting-SAS- oder NVMe-Laufwerke werden auf allen FAS und AFF Systemen unterstützt. Diese Laufwerke, so genannte *FIPS-Laufwerke*, entsprechen den Anforderungen der Federal Information Processing Standard Publication 140-2, Level 2. Die zertifizierten Funktionen ermöglichen neben der Verschlüsselung auch Schutz, beispielsweise die Verhinderung von Denial-of-Service-Angriffen auf dem Laufwerk. FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden.
- Ab ONTAP 9.6 werden Self-Encrypting-NVMe-Laufwerke, die noch keine FIPS-Tests durchlaufen haben, auf AFF A800, A320 und neueren Systemen unterstützt. Diese Laufwerke, sogenannte *SEDs*, bieten dieselben Verschlüsselungsfunktionen wie FIPS-Laufwerke, können aber ohne Verschlüsselung von Laufwerken auf demselben Node oder HA-Paar kombiniert werden.
- Alle FIPS-validierten Laufwerke verwenden ein kryptografisches Firmware-Modul, das durch die FIPS-Validierung erfolgt. Das FIPS-Laufwerk-kryptografische Modul verwendet keine Schlüssel, die außerhalb des Laufwerks generiert werden (die Authentifizierungs-Passphrase, die an das Laufwerk eingegeben wird, wird vom Laufwerk-Firmware-kryptographic-Modul verwendet, um einen Schlüssel zu erhalten).

> Laufwerke ohne Verschlüsselung sind Laufwerke, die keine SEDs oder FIPS-Laufwerke sind.

> Wenn Sie NSE in einem System mit einem Flash Cache Modul verwenden, sollten Sie auch NVE oder NAE aktivieren. NSE verschlüsselt keine Daten im Flash Cache Modul.

Wann Sie externes Verschlüsselungsmanagement verwenden sollten

Obwohl es kostengünstiger und in der Regel bequemer ist, den Onboard-Schlüsselmanager zu verwenden, sollten Sie ein externes Verschlüsselungsmanagement nutzen, wenn eine der folgenden zutrifft:

- Die Richtlinie Ihres Unternehmens erfordert eine Verschlüsselungsmanagementlösung, die ein kryptografisches Modul nach FIPS 140-2 Level 2 (oder höher) verwendet.
- 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.

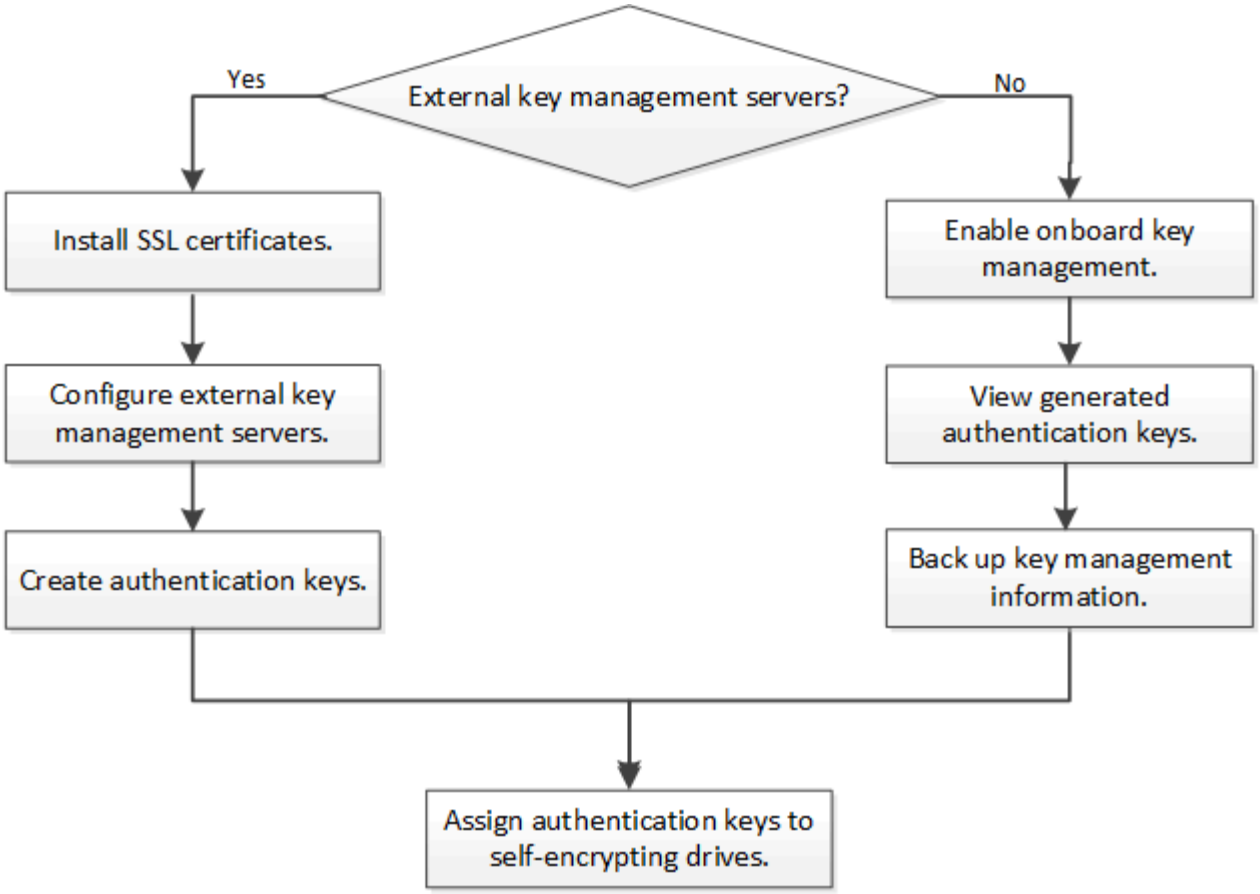
Support-Details

In der folgenden Tabelle sind wichtige Details zur Unterstützung der Hardwareverschlüsselung aufgeführt. In der Interoperabilitäts-Matrix finden Sie die neuesten Informationen zu unterstützten KMIP-Servern, Storage-Systemen und Festplatten-Shelfs.

Ressource oder Funktion	Support-Details
Nicht homogene Festplattengruppen	• FIPS-Laufwerke können nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden. Die Einhaltung der HA-Paare kann bei nicht übereinstimmenden HA-Paaren im selben Cluster vorhanden sein. • SEDs können mit Laufwerken ohne Verschlüsselung auf demselben Node oder HA-Paar kombiniert werden.
Laufwerkstyp	• FIPS-Laufwerke können SAS- oder NVMe-Laufwerke sein. • SEDs müssen NVMe-Laufwerke sein.
10-GB-Netzwerkschnittstellen	Ab ONTAP 9.3 unterstützen die KMIP-Verschlüsselungsmanagementkonfigurationen 10 GB-Netzwerkschnittstellen für die Kommunikation mit externen Verschlüsselungsmanagement-Servern.
Ports für die Kommunikation mit dem Schlüsselverwaltungsserver	Ab ONTAP 9.3 können Sie jeden beliebigen Storage Controller Port zur Kommunikation mit dem Schlüsselmanagement-Server verwenden. Andernfalls sollten Sie Port E0M für die Kommunikation mit Schlüsselmanagement-Servern verwenden. Je nach Storage-Controller-Modell sind während des Bootvorgangs möglicherweise bestimmte Netzwerkschnittstellen zur Kommunikation mit wichtigen Management-Servern nicht verfügbar.
MetroCluster (MCC)	• NVMe-Laufwerke unterstützen MCC. • SAS-Laufwerke unterstützen MCC nicht.

Hardwarebasierter Verschlüsselungs-Workflow

Sie müssen Verschlüsselungsmanagementdienste konfigurieren, bevor sich das Cluster auf dem Self-Encrypting Drive authentifizieren kann. Sie können einen externen Verschlüsselungsmanagementserver oder einen integrierten Schlüsselmanager verwenden.



Verwandte Informationen

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

Externes Verschlüsselungsmanagement konfigurieren

Externes Verschlüsselungsmanagement – Übersicht konfigurieren

Sie können einen oder mehrere externe Verschlüsselungsmanagementserver verwenden, um die Schlüssel zu sichern, die das Cluster zum Zugriff auf verschlüsselte Daten verwendet. Ein externer Verschlüsselungsmanagement-Server ist ein Drittanbietersystem in Ihrer Storage-Umgebung, der mithilfe des Key Management Interoperability Protocol (KMIP) Schlüssel zu Nodes bereitstellt.

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

NetApp Volume Encryption (NVE) kann mit Onboard Key Manager in ONTAP 9.1 und höher implementiert werden. NVE kann in ONTAP 9.3 oder höher mit externem Verschlüsselungsmanagement (KMIP) und Onboard Key Manager implementiert werden. Ab ONTAP 9.11.1 können Sie mehrere externe Schlüsselmanager in einem Cluster konfigurieren. Siehe Konfigurieren Sie Cluster-Key-Server.

Erfassen Sie Netzwerkinformationen in ONTAP 9.2 und früher

Wenn Sie ONTAP 9.2 oder eine frühere Version verwenden, sollten Sie das Arbeitsblatt

zur Netzwerkkonfiguration ausfüllen, bevor Sie die externe Schlüsselverwaltung aktivieren.

Ab ONTAP 9.3 erkennt das System automatisch alle benötigten Netzwerkinformationen.

Element	Hinweise	Wert
Name der Key-Management-Netzwerkschnittstelle		
IP-Adresse für die wichtige Management-Netzwerkschnittstelle	IP-Adresse der LIF für das Node-Management im IPv4- oder IPv6-Format	
Key-Management-Netzwerkschnittstelle IPv6-Netzwerk-Präfixlänge	Wenn Sie IPv6 verwenden, Länge des IPv6-Netzwerkpräfixes	
Subnetzmaske für das Schlüsselmanagement-Netzwerk-Interface		
Gateway-IP-Adresse für die wichtige Management-Netzwerkschnittstelle		
IPv6-Adresse für die Cluster-Netzwerkschnittstelle	Nur erforderlich, wenn Sie IPv6 für die Netzwerkschnittstelle des Verschlüsselungsmanagements verwenden	
Port-Nummer für jeden KMIP-Server	Optional Die Portnummer muss für alle KMIP-Server identisch sein. Wenn Sie keine Portnummer angeben, wird standardmäßig der Port 5696 verwendet. Dies ist der für KMIP zugewiesene Port (Internet Assigned Numbers Authority, IANA).	
Tag-Schlüsselname	Optional Der Key-Tag-Name wird verwendet, um alle Schlüssel zu einem Knoten zu identifizieren. Der Standardname für das Tag der Schlüssel ist der Node-Name.	

Verwandte Informationen

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

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

Installieren Sie SSL-Zertifikate auf dem Cluster

Das Cluster und der KMIP-Server verwenden KMIP SSL-Zertifikate, um die Identität des jeweils anderen zu überprüfen und eine SSL-Verbindung herzustellen. Vor dem Konfigurieren der SSL-Verbindung mit dem KMIP-Server müssen die KMIP-Client-SSL-Zertifikate für das Cluster und das öffentliche SSL-Zertifikat für die Root-Zertifizierungsstelle des KMIP-Servers installiert werden.

Über diese Aufgabe

In einem HA-Paar müssen beide Nodes dieselben öffentlichen und privaten KMIP-SSL-Zertifikate verwenden. Wenn Sie mehrere HA-Paare mit demselben KMIP-Server verbinden, müssen alle Nodes der HA-Paare dieselben öffentlichen und privaten KMIP-SSL-Zertifikate verwenden.

Bevor Sie beginnen

- Die Zeit muss auf dem Server synchronisiert werden, der die Zertifikate, den KMIP-Server und das Cluster erstellt.
- Sie müssen das öffentliche SSL KMIP-Client-Zertifikat für den Cluster erhalten haben.
- Sie müssen den privaten Schlüssel für das SSL KMIP Client-Zertifikat für das Cluster erhalten haben.
- Das SSL KMIP-Client-Zertifikat darf nicht durch ein Passwort geschützt sein.
- Sie müssen das öffentliche SSL-Zertifikat für die Root-Zertifizierungsstelle (CA) des KMIP-Servers erhalten haben.
- In einer MetroCluster-Umgebung müssen Sie auf beiden Clustern dieselben KMIP-SSL-Zertifikate installieren.

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

Schritte

1. Installieren Sie die SSL KMIP-Client-Zertifikate für das Cluster:

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

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

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

2. Installieren Sie das öffentliche SSL-Zertifikat für die Root-Zertifizierungsstelle (CA) des KMIP-Servers:

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

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

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

Ein oder mehrere KMIP-Server dienen zur Sicherung der Schlüssel, die das Cluster für den Zugriff auf verschlüsselte Daten verwendet. Mit einem Node können bis zu vier KMIP-Server verbunden werden. Für Redundanz und Disaster Recovery werden mindestens zwei Server empfohlen.

Ab ONTAP 9.11.1 können Sie pro Primärschlüsselserver bis zu 3 sekundäre Schlüsselserver hinzufügen, um einen geclusterten Schlüsselserver zu erstellen. Weitere Informationen finden Sie unter Konfigurieren Sie externe geclusterte Schlüsselserver.

Bevor Sie beginnen

- Die KMIP SSL-Client- und Serverzertifikate müssen installiert sein.
- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Sie müssen die MetroCluster Umgebung konfigurieren, bevor Sie einen externen Schlüsselmanager konfigurieren.
- In einer MetroCluster-Umgebung müssen Sie das KMIP SSL-Zertifikat auf beiden Clustern installieren.

Schritte

1. Konfigurieren Sie die Schlüsselmanager-Konnektivität für das Cluster:

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

   > - Der `security key-manager external enable` Mit dem Befehl wird der ersetzt `security key-manager setup` Befehl. Sie können die ausführen `security key-manager external modify` Befehl zum Ändern der Konfiguration für das externe Verschlüsselungsmanagement. Eine vollständige Befehlssyntax finden Sie in den man-Pages.
   > - Wenn Sie in einer MetroCluster-Umgebung externes Verschlüsselungsmanagement für den Administrator-SVM konfigurieren, müssen Sie die wiederholen `security 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 -key-servers
   ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
   -client-cert AdminVserverClientCert -server-ca-certs
   AdminVserverServerCaCert
   ```

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

   ```
   security key-manager external show-status -node node_name -vserver SVM -key
   -server host_name|IP_address:port -key-server-status available|not-
   responding|unknown
   ```

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

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

Node  Vserver  Key Server                                       Status
----  -------  ----------------------------------------
-------------
node1
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available
node2
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available

6 entries were displayed.
```

Ermöglichen Sie externes Verschlüsselungsmanagement in ONTAP 9.5 und früher

Ein oder mehrere KMIP-Server dienen zur Sicherung der Schlüssel, die das Cluster für den Zugriff auf verschlüsselte Daten verwendet. Mit einem Node können bis zu vier KMIP-Server verbunden werden. Für Redundanz und Disaster Recovery werden mindestens zwei Server empfohlen.

Über diese Aufgabe

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

Bevor Sie beginnen

- Die KMIP SSL-Client- und Serverzertifikate müssen installiert sein.
- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Sie müssen die MetroCluster Umgebung konfigurieren, bevor Sie einen externen Schlüsselmanager konfigurieren.
- In einer MetroCluster-Umgebung müssen Sie das KMIP SSL-Zertifikat auf beiden Clustern installieren.

Schritte

1. Konfigurieren Sie die Schlüsselmanager-Konnektivität für Cluster-Nodes:

   ```
   security key-manager setup
   ```

   Die Konfiguration des Schlüsselmanagers wird gestartet.

   > In einer MetroCluster-Umgebung müssen Sie den folgenden Befehl auf beiden Clustern ausführen.

2. Geben Sie an jeder Eingabeaufforderung die entsprechende Antwort ein.

3. Hinzufügen eines KMIP-Servers:

   `security key-manager add -address key_management_server_ipaddress`

   ```
   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
   ```

6. Konvertieren Sie optional Klartextvolumes in verschlüsselte Volumes.

   `volume encryption conversion start`

   Ein externer Schlüsselmanager muss vollständig konfiguriert sein, bevor Sie die Volumes konvertieren. In einer MetroCluster-Umgebung muss auf beiden Seiten ein externer Schlüsselmanager konfiguriert werden.

Konfigurieren Sie externe geclusterte Schlüsselserver

Ab ONTAP 9.11.1 können Sie die Konnektivität mit externen Verschlüsselungsmanagement-Servern auf einer SVM konfigurieren. Mit geclusterten Key Servern können Sie primäre und sekundäre Schlüsselserver auf einer SVM

zuweisen. Bei der Registrierung von Schlüsseln versucht ONTAP zuerst, auf einen primären Schlüsselserver zuzugreifen, bevor nacheinander versucht wird, auf sekundäre Server zuzugreifen, bis der Vorgang erfolgreich abgeschlossen ist. Dadurch wird die Duplizierung von Schlüsseln verhindert.

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

Bevor Sie beginnen

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

Erstellen Sie einen Cluster-Schlüsselserver

Das Konfigurationsverfahren hängt davon ab, ob Sie einen primären Schlüsselserver konfiguriert haben oder nicht.

Hinzufügen von primären und sekundären Schlüsselservern zu einer SVM

1. Vergewissern Sie sich, dass für das Cluster kein Verschlüsselungsmanagement aktiviert wurde:
   `security key-manager external show -vserver` *`svm_name`*
   Wenn für die SVM bereits maximal vier primäre Schlüsselserver aktiviert sind, müssen Sie einen der vorhandenen primären Schlüsselserver entfernen, bevor Sie einen neuen hinzufügen.
2. Aktivieren Sie den primären Schlüsselmanager:
   `security key-manager external enable -vserver` *`svm_name`* `-key-servers` *`server_ip`* `-client-cert` *`client_cert_name`* `-server-ca-certs` *`server_ca_cert_names`*
3. Ändern Sie den primären Schlüsselserver, um sekundäre Schlüsselserver hinzuzufügen. Der `-secondary-key-servers` Der Parameter akzeptiert eine kommagetrennte Liste mit bis zu drei Schlüsselservern.
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*

Fügen Sie einem vorhandenen primären Schlüsselserver sekundäre Schlüsselserver hinzu

1. Ändern Sie den primären Schlüsselserver, um sekundäre Schlüsselserver hinzuzufügen. Der `-secondary-key-servers` Der Parameter akzeptiert eine kommagetrennte Liste mit bis zu drei Schlüsselservern.
   `security key-manager external modify-server -vserver` *`svm_name`* `-key-servers` *`primary_key_server`* `-secondary-key-servers` *`list_of_key_servers`*
   Weitere Informationen zu sekundären Schlüsselservern finden Sie unter [mod-secondary].

Cluster-Key-Server ändern

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

Konvertieren Sie primäre und sekundäre Schlüsselserver

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

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

Ändern Sie sekundäre Schlüsselserver

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

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

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

Erstellen Sie Authentifizierungsschlüssel in ONTAP 9.6 und höher

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

Über diese Aufgabe

Wenn Sie in Ihrer Sicherheitseinrichtung unterschiedliche Schlüssel für die Datenauthentifizierung und die FIPS 140-2-Authentifizierung verwenden müssen, sollten Sie jeweils einen separaten Schlüssel erstellen. Ist dies nicht der Fall, können Sie denselben Authentifizierungsschlüssel für die FIPS-Compliance verwenden wie für den Datenzugriff.

ONTAP erstellt Authentifizierungsschlüssel für alle Nodes im Cluster.

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

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

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

> Bevor Sie einen Schlüssel in einer MetroCluster-Umgebung löschen, müssen Sie sicherstellen, dass der Schlüssel nicht im Partner-Cluster verwendet wird. Sie können auf dem Partner-Cluster folgende Befehle verwenden, um zu überprüfen, ob der Schlüssel nicht verwendet wird:
>
> - `storage encryption disk show -data-key-id` *`key-id`*
> - `storage encryption disk show -fips-key-id` *`key-id`*

Bevor Sie beginnen

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

Schritte

1. Authentifizierungsschlüssel für Cluster-Nodes erstellen:

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

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

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

   ```
   cluster1::> security key-manager key create
   Key ID:
   000000000000000002000000000001006268333f870860128fbe17d393e5083b00000000
   00000000
   ```

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

   ```
   security key-manager key query -node node
   ```

   > Der `security key-manager key query` Mit dem Befehl wird der ersetzt `security key-manager query key` Befehl. Eine vollständige Befehlssyntax finden Sie in der man-Page. Die in der Ausgabe angezeigte Schlüssel-ID ist eine Kennung, die auf den Authentifizierungsschlüssel verweist. Es handelt sich nicht um den tatsächlichen Authentifizierungsschlüssel oder den Datenverschlüsselung.

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

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: external
          Node: node1

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

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
00000000
```

Erstellen Sie Authentifizierungsschlüssel in ONTAP 9.5 und früher

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

Über diese Aufgabe

Wenn Sie in Ihrer Sicherheitseinrichtung unterschiedliche Schlüssel für die Datenauthentifizierung und die FIPS 140-2-Authentifizierung verwenden müssen, sollten Sie jeweils einen separaten Schlüssel erstellen. Falls dies nicht der Fall ist, können Sie denselben Authentifizierungsschlüssel für die FIPS-Compliance verwenden, den Sie für den Datenzugriff verwenden.

ONTAP erstellt Authentifizierungsschlüssel für alle Nodes im Cluster.

- Dieser Befehl wird nicht unterstützt, wenn das integrierte Verschlüsselungsmanagement aktiviert ist.
- Sie erhalten eine Warnung, wenn auf den konfigurierten Schlüsselverwaltungsservern bereits mehr als 128 Authentifizierungsschlüssel gespeichert werden.

  Sie können die Verschlüsselungsmanagement-Server-Software verwenden, um alle nicht verwendeten Schlüssel zu löschen, und führen den Befehl erneut aus.

Bevor Sie beginnen

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

Schritte

1. Authentifizierungsschlüssel für Cluster-Nodes erstellen:

   `security key-manager create-key`

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

   > Die in der Ausgabe angezeigte Schlüssel-ID ist eine Kennung, die auf den Authentifizierungsschlüssel verweist. Es handelt sich nicht um den tatsächlichen Authentifizierungsschlüssel oder den Datenverschlüsselung.

   Im folgenden Beispiel werden die Authentifizierungsschlüssel für erstellt `cluster1`:

   ```
   cluster1::> security key-manager create-key
      (security key-manager create-key)
   Verifying requirements...

   Node: cluster1-01
   Creating authentication key...
   Authentication key creation successful.
   Key ID: F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

   Node: cluster1-01
   Key manager restore operation initialized.
   Successfully restored key information.

   Node: cluster1-02
   Key manager restore operation initialized.
   Successfully restored key information.
   ```

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

   `security key-manager query`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

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

  (security key-manager query)

          Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-01    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C


          Node: cluster1-02
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-02    NSE-AK    yes
       Key ID:
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
```

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

Sie können das verwenden `storage encryption disk modify` Befehl zum Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder einer SED. Clusterknoten verwenden diesen Schlüssel zum Sperren oder Entsperren verschlüsselter Daten auf dem Laufwerk.

Über diese Aufgabe

Ein selbstverschlüsselndes Laufwerk ist nur dann vor unberechtigtem Zugriff geschützt, wenn seine Authentifizierungsschlüssel-ID auf einen nicht standardmäßigen Wert eingestellt ist. Der Hersteller Secure ID (MSID), der die Schlüssel-ID 0x0 hat, ist der Standardvorgabewert für SAS-Laufwerke. Bei NVMe-Laufwerken ist der Standardwert ein Null-Schlüssel, der als leere Schlüssel-ID dargestellt wird. Wenn Sie einem selbstverschlüsselnden Laufwerk die Schlüssel-ID zuweisen, ändert das System seine Authentifizierungsschlüssel-ID in einen nicht standardmäßigen Wert.

Dieses Verfahren ist nicht störend.

Bevor Sie beginnen

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

Schritte

1. Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder einer SED:

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

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

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

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

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

   `storage encryption disk show`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   [...]
   ```

Integriertes Verschlüsselungsmanagement

Ermöglichen Sie integriertes Verschlüsselungsmanagement in ONTAP 9.6 und höher

Mit dem Onboard Key Manager können Clusterknoten auf einem FIPS-Laufwerk oder SED authentifiziert werden. Der integrierte Onboard Key Manager ist ein Tool, das Authentifizierungsschlüssel für Nodes aus demselben Storage-System wie Ihre Daten bereitstellt. Der Onboard Key Manager ist nach FIPS-140-2 Level 1 zertifiziert.

Mit dem integrierten Key Manager werden die Schlüssel gesichert, die das Cluster für den Zugriff auf verschlüsselte Daten verwendet. Sie müssen Onboard Key Manager für jedes Cluster aktivieren, das auf ein verschlüsseltes Volume oder eine selbstverschlüsselnde Festplatte zugreift.

Über diese Aufgabe

Sie müssen den ausführen `security key-manager onboard enable` Befehl jedes Mal, wenn Sie dem Cluster einen Node hinzufügen. In MetroCluster Konfigurationen 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. Außer in MetroCluster können Sie den verwenden `cc-mode-enabled=yes` Option zum Eingeben, dass Benutzer nach einem Neustart die Passphrase eingeben.

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 NetApp Storage Encryption (NSE) aktiviert ist und Sie beim Booten nicht die richtige Cluster-Passphrase eingeben, kann sich das System nicht auf seinen Laufwerken authentifizieren und automatisch neu starten. Um dies zu korrigieren, müssen Sie an der Boot-Eingabeaufforderung 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.

Bevor Sie beginnen

- 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 der Onboard Key Manager konfiguriert wird.

Schritte

1. Starten Sie den Key Manager Setup-Befehl:

   `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. 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 -node node`

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

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

```
cluster1::> security key-manager key query
       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: cluster1
   Key Manager: onboard
          Node: node2

Key Tag                                  Key Type  Restored
-----------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001000c11b3863f78c2273343d7ec5a67762e00000000
00000000
node2                                    NSE-AK    yes
    Key ID:
000000000000000002000000000001006f4e2513353a674305872a4c9f3bf79700000000
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.

Ermöglichen Sie integriertes Verschlüsselungsmanagement in ONTAP 9.5 und früher

Mit dem Onboard Key Manager können Clusterknoten auf einem FIPS-Laufwerk oder SED authentifiziert werden. Der integrierte Onboard Key Manager ist ein Tool, das Authentifizierungsschlüssel für Nodes aus demselben Storage-System wie Ihre Daten bereitstellt. Der Onboard Key Manager ist nach FIPS-140-2 Level 1 zertifiziert.

Mit dem integrierten Key Manager werden die Schlüssel gesichert, die das Cluster für den Zugriff auf

verschlüsselte Daten verwendet. Sie müssen Onboard Key Manager für jedes Cluster aktivieren, das auf ein verschlüsseltes Volume oder eine selbstverschlüsselnde Festplatte zugreift.

Über diese Aufgabe

Sie müssen den 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.

Bevor Sie beginnen

- 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 der Onboard Key Manager konfiguriert wird.

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

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".

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

Sie können das verwenden `storage encryption disk modify` Befehl zum Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder einer SED. Cluster-Nodes verwenden diesen Schlüssel für den Zugriff auf die Daten auf dem Laufwerk.

Über diese Aufgabe

Ein selbstverschlüsselndes Laufwerk ist nur dann vor unberechtigtem Zugriff geschützt, wenn seine Authentifizierungsschlüssel-ID auf einen nicht standardmäßigen Wert eingestellt ist. Der Hersteller Secure ID (MSID), der die Schlüssel-ID 0x0 hat, ist der Standardvorgabewert für SAS-Laufwerke. Bei NVMe-Laufwerken ist der Standardwert ein Null-Schlüssel, der als leere Schlüssel-ID dargestellt wird. Wenn Sie einem selbstverschlüsselnden Laufwerk die Schlüssel-ID zuweisen, ändert das System seine Authentifizierungsschlüssel-ID in einen nicht standardmäßigen Wert.

Bevor Sie beginnen

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

Schritte

1. Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder einer SED:

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

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

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

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   0000000000000000020000000000010019215b9738bc7b43d4698c80246db1f4

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

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

   `storage encryption disk show`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------------
0.0.0   data
000000000000000002000000000000010019215b9738bc7b43d4698c80246db1f4
0.0.1   data
000000000000000002000000000000010059851742AF2703FC91369B7DB47C4722
[...]
```

Weisen Sie einem FIPS 140-2-2-Authentifizierungsschlüssel zu

Sie können das verwenden `storage encryption disk modify` Befehl mit dem `-fips-key-id` Option zum Zuweisen eines FIPS-140-2-Authentifizierungsschlüssels zu einem FIPS-Laufwerk. Cluster-Nodes verwenden diesen Schlüssel für andere Laufwerksvorgänge als Datenzugriff, z. B. zur Verhinderung von Denial-of-Service-Angriffen auf das Laufwerk.

Über diese Aufgabe

In Ihrer Sicherheitseinrichtung müssen Sie unter Umständen unterschiedliche Schlüssel zur Datenauthentifizierung und zur FIPS 140-2-2-Authentifizierung verwenden. Falls dies nicht der Fall ist, können Sie denselben Authentifizierungsschlüssel für die FIPS-Compliance verwenden, den Sie für den Datenzugriff verwenden.

Dieses Verfahren ist nicht störend.

Bevor Sie beginnen

Die Laufwerk-Firmware muss FIPS 140-2-2-konform unterstützen. Der "NetApp Interoperabilitäts-Matrix-Tool" Enthält Informationen zu unterstützten Festplatten-Firmware-Versionen.

Schritte

1. Sie müssen zunächst sicherstellen, dass Sie einen Datenauthentifizierungsschlüssel zugewiesen haben. Dies kann mit einem erfolgen Externer Schlüsselmanager Oder an Integriertes Verschlüsselungsmanagement. Vergewissern Sie sich, dass der Schlüssel mit dem Befehl zugewiesen ist `storage encryption disk show`.
2. SEDs einen FIPS 140-2-Authentifizierungsschlüssel zuweisen:

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

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

```
cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

3. Vergewissern Sie sich, dass der Authentifizierungsschlüssel zugewiesen wurde:

   `storage encryption disk show -fips`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster1::> storage encryption disk show -fips
Disk    Mode FIPS-Compliance Key ID
------  ----
-------------------------------------------------------------------
2.10.0  full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
2.10.1  full
6A1E21D8000000000100000000000005A1FB4EE8F62FD6D8AE6754C9019F35A
[...]
```

Cluster-weiter FIPS-konformer Modus für KMIP-Serververbindungen

Sie können das verwenden `security config modify` Befehl mit dem `-is-fips-enabled` Option zur Aktivierung des clusterweiten FIPS-konformen Modus für genutzte Daten Dadurch wird die Verwendung von OpenSSL im FIPS-Modus erzwingt, wenn eine Verbindung zu KMIP-Servern hergestellt wird.

Über diese Aufgabe

Wenn Sie den FIPS-konformen Cluster-Modus aktivieren, verwendet das Cluster automatisch nur TLS1.2 und FIPS-validierte Chiffre Suites. Der clusterweite FIPS-konforme Modus ist standardmäßig deaktiviert.

Sie müssen die Cluster-Nodes manuell neu booten, nachdem Sie die Cluster-weite Sicherheitskonfiguration geändert haben.

Bevor Sie beginnen

- Der Storage Controller muss im FIPS-konformen Modus konfiguriert sein.
- Alle KMIP-Server müssen TLSv1.2 unterstützen. Das System benötigt TLSv1.2, um die Verbindung zum KMIP-Server abzuschließen, wenn der clusterweite FIPS-konforme Modus aktiviert ist.

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   `set -privilege advanced`

2. Vergewissern Sie sich, dass TLSv1.2 unterstützt wird:

   `security config show -supported-protocols`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster1::> security config show
          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       false      TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL
```

3. Cluster-weiten, FIPS-konformen Modus aktivieren:

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

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

4. Manuelles Neubooten der Cluster-Nodes
5. Vergewissern Sie sich, dass der FIPS-konforme Cluster-weite Modus aktiviert ist:

   `security config show`

```
cluster1::> security config show
          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       true       TLSv1.2, TLSv1.1        ALL:!LOW:         yes
                                             !aNULL:!EXP:
                                             !eNULL:!RC4
```

NetApp Verschlüsselung managen

Verschlüsseln Sie Volume-Daten

Sie können das verwenden `volume move start` Befehl zum Verschieben und Entschlüsseln von Volume-Daten.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen. Alternativ können Sie ein SVM-Administrator sein, an den der Cluster-Administrator Berechtigungen delegiert hat. Weitere Informationen finden Sie unter "Delegieren von Berechtigungen zum Ausführen des Befehls Volume Move".

Schritte

1. Verschieben eines vorhandenen verschlüsselten Volumes und Entschlüsseln der Daten auf dem 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 vorhandenes Volume mit dem Namen verschoben `vol1` Auf das Zielaggregat `aggr3` Und entverschlüsselt die Daten auf dem Volume:

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3 -encrypt-destination false
   ```

   Das System löscht den Verschlüsselungsschlüssel für das Volume. Die Daten auf dem Volume werden unverschlüsselt.

2. Vergewissern Sie sich, dass das Volume zur Verschlüsselung deaktiviert ist:

   `volume show -encryption`

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

   Mit dem folgenden Befehl wird angezeigt, ob Volumes auf ausgeführt werden `cluster1` Verschlüsselt:

   ```
   cluster1::> volume show -encryption

   Vserver  Volume   Aggregate   State    Encryption State
   -------  ------   ---------   -----    ----------------
   vs1      vol1     aggr1       online   none
   ```

Verschieben Sie ein verschlüsseltes Volume

Sie können das verwenden `volume move start` Befehl zum Verschieben eines verschlüsselten Volumes. Das verschobene Volume kann auf demselben Aggregat oder einem anderen Aggregat residieren.

Über diese Aufgabe

Die Verschiebung schlägt fehl, wenn der Ziel-Node oder das Ziel-Volume die Volume-Verschlüsselung nicht unterstützt.

Der `-encrypt-destination` Option für `volume move start` Standardmäßig auf „true“ für verschlüsselte Volumes gesetzt. Wenn Sie angeben müssen, dass das Ziel-Volume nicht verschlüsselt werden soll, wird

sichergestellt, dass die Verschlüsselung der Daten auf dem Volume nicht versehentlich aufgehoben wird.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen. Alternativ können Sie ein SVM-Administrator sein, an den der Cluster-Administrator Berechtigungen delegiert hat. Weitere Informationen finden Sie unter "Delegieren Sie die Autorität, um den Befehl Volume move auszuführen".

Schritte

1. Verschieben Sie ein vorhandenes verschlüsseltes Volume, und lassen Sie die Daten auf dem Volume verschlüsselt:

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`*

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

   Mit dem folgenden Befehl wird ein vorhandenes Volume mit dem Namen verschoben `vol1` Auf das Zielaggregat `aggr3` Und lassen die Daten auf dem Volume verschlüsselt:

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3
   ```

2. 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    aggr3     online    RW  200GB    160.0GB  20%
   ```

Delegieren von Berechtigungen zum Ausführen des Befehls Volume Move

Sie können das verwenden `volume move` Befehl zum Verschlüsseln eines vorhandenen Volumes, Verschieben eines verschlüsselten Volumes oder Entschlüsseln eines Volumes Cluster-Administratoren können ausgeführt werden `volume move` Entweder selbst einen Befehl ausführen oder sie können die Berechtigungen delegieren, um den Befehl an SVM-Administratoren auszuführen.

Über diese Aufgabe

Standardmäßig werden SVM-Administratoren das zugewiesen `vsadmin` Rolle, die nicht die Berechtigung zum Verschieben von Volumes beinhaltet. Sie müssen den zuweisen `vsadmin-volume` Rolle für SVM-

Administratoren, damit sie in der Lage sind `volume move` Befehl.

Schritt

1. Delegieren Sie die Berechtigung zum Ausführen des `volume move` Befehl:

   `security login modify -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`vsadmin-volume`*

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

   Mit dem folgenden Befehl erhält der SVM-Administrator die Berechtigung, den auszuführen `volume move` Befehl.

   ```
   cluster1::>security login modify -vserver engData -user-or-group-name
   SVM-admin -application ssh -authmethod domain -role vsadmin-volume
   ```

Ändern Sie den Verschlüsselungsschlüssel für ein Volume mit dem Befehl „Start der Volume-Verschlüsselung“

Es handelt sich hierbei um eine Best Practice für Sicherheit, den Verschlüsselungsschlüssel für ein Volume regelmäßig zu ändern. Ab ONTAP 9.3 können Sie den verwenden `volume encryption rekey start` Befehl zum Ändern des Verschlüsselungsschlüssels.

Über diese Aufgabe

Sobald Sie einen Rekeyvorgang starten, muss er abgeschlossen sein. Es gibt keine Rückkehr zum alten Schlüssel. Wenn während des Vorgangs ein Leistungsproblem auftritt, können Sie das ausführen `volume encryption rekey pause` Befehl zum Anhalten des Vorgangs, und `volume encryption rekey resume` Befehl zum Fortsetzen des Vorgangs.

Bis der Vorgang des Neuschlüssels abgeschlossen ist, verfügt das Volume über zwei Tasten. Neue Schreibzugriffe und die entsprechenden Lesezugriffe nutzen den neuen Schlüssel. Andernfalls wird der alte Schlüssel bei den Lesevorgängen verwendet.

> Verwenden Sie ihn nicht `volume encryption rekey start` Um ein SnapLock Volume erneut zu keyNeuschlüssel.

Schritte

1. Ändern eines Verschlüsselungsschlüssels:

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

   Der Verschlüsselungsschlüssel für wird mit dem folgenden Befehl geändert `vol1` Auf SVM`vs1`:

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

2. Überprüfen Sie den Status der Rekeybedienung:

   `volume encryption rekey show`

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

   Mit dem folgenden Befehl wird der Status der Rekeyoperation angezeigt:

```
cluster1::> volume encryption rekey show

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

3. Vergewissern Sie sich nach Abschluss des Rekeyvorgangs, 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%
```

Ändern Sie den Verschlüsselungsschlüssel für ein Volume mit dem Befehl Volume move Start

Es handelt sich hierbei um eine Best Practice für Sicherheit, den Verschlüsselungsschlüssel für ein Volume regelmäßig zu ändern. Sie können das verwenden `volume move start` Befehl zum Ändern des Verschlüsselungsschlüssels. Sie müssen verwenden `volume move start` In ONTAP 9.2 und früher. Das verschobene Volume kann auf demselben Aggregat oder einem anderen Aggregat residieren.

Über diese Aufgabe

Verwenden Sie ihn nicht `volume move start` Um einen SnapLock oder FlexGroup Volume erneut zu keyNeuschlüssel zu erhalten.

Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen. Alternativ können Sie ein SVM-Administrator sein, an den der Cluster-Administrator Berechtigungen delegiert hat. Weitere Informationen finden Sie unter "Delegieren Sie die Autorität, um den Befehl Volume move auszuführen".

Schritte

1. Verschieben eines vorhandenen Volumes und Ändern des Verschlüsselungsschlüssels:

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-generate-destination-key true`

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

   Mit dem folgenden Befehl wird ein vorhandenes Volume mit dem Namen verschoben **`vol1`** Auf das Zielaggregat **`aggr2`** Und ändert den Verschlüsselungsschlüssel:

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

   Für das Volume wird ein neuer Verschlüsselungsschlüssel erstellt. Die Daten auf dem Volume bleiben verschlüsselt.

2. 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%
   ```

Drehen Sie die Authentifizierungsschlüssel für die NetApp Storage Encryption

Sie können die Authentifizierungsschlüssel mit der NetApp Storage Encryption (NSE) drehen.

Über diese Aufgabe

Die rotierenden Authentifizierungsschlüssel in einer NSE-Umgebung werden unterstützt, wenn Sie External Key Manager (KMIP) verwenden.

> Rotierende Authentifizierungsschlüssel in einer NSE-Umgebung werden von Onboard Key Manager (OKM) nicht unterstützt.

Schritte

1. Verwenden Sie die `security key-manager create-key` Befehl zum Generieren neuer Authentifizierungsschlüssel.

Sie müssen neue Authentifizierungsschlüssel generieren, bevor Sie die Authentifizierungsschlüssel ändern können.

2. Verwenden Sie die `storage encryption disk modify -disk * -data-key-id` Befehl zum Ändern der Authentifizierungsschlüssel.

Löschen Sie ein verschlüsseltes Volume

Sie können das verwenden `volume delete` Befehl zum Löschen eines verschlüsselten Volumes.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen. Alternativ können Sie ein SVM-Administrator sein, an den der Cluster-Administrator Berechtigungen delegiert hat. Weitere Informationen finden Sie unter "Delegieren Sie die Autorität, um den Befehl Volume move auszuführen".
- Das Volume muss sich offline befinden.

Schritt

1. Verschlüsseltes Volume löschen:

   `volume delete -vserver` *`SVM_name`* `-volume` *`volume_name`*

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

   Mit dem folgenden Befehl wird ein verschlüsseltes Volume mit dem Namen gelöscht `vol1`:

   ```
   cluster1::> volume delete -vserver vs1 -volume vol1
   ```

   Eingabe `yes` Wenn Sie zur Bestätigung des Löschvorgangs aufgefordert werden.

   Das System löscht den Verschlüsselungsschlüssel für das Volume nach 24 Stunden.

   Nutzung `volume delete` Mit dem `-force true` Option zum sofortigen Löschen eines Volumes und Löschen des entsprechenden Verschlüsselungsschlüssels. Dieser Befehl erfordert erweiterte Berechtigungen. Weitere Informationen finden Sie auf der man-Page.

Nachdem Sie fertig sind

Sie können das verwenden `volume recovery-queue` Befehl zum Wiederherstellen eines gelöschten Volumes während der Aufbewahrungsfrist nach Ausgabe des `volume delete` Befehl:

`volume recovery-queue` *`SVM_name`* `-volume` *`volume_name`*

"So verwenden Sie die Volume Recovery-Funktion"

Löschen Sie Daten auf einem verschlüsselten Volume sicher

Löschen Sie Daten sicher auf einer Übersicht über ein verschlüsseltes Volume

Ab ONTAP 9.4 können Sie Daten auf NVE-fähigen Volumes durch sicheres Löschen

unterbrechungsfrei abspeichern. Das Scrubbing von Daten auf einem verschlüsselten Volume stellt sicher, dass sie nicht von physischen Medien wiederhergestellt werden können, beispielsweise bei „`s` pillage“, bei denen Spuren von Daten beim Überschreiben von Blöcken hinterlassen wurden oder zum sicheren Löschen der Daten eines Mandanten.

Secure Purge ist nur für zuvor gelöschte Dateien auf Volumes mit NVE geeignet. Sie können ein unverschlüsseltes Volume nicht abreiben. Sie müssen KMIP-Server für die Schlüsselverwendung verwenden, nicht für den integrierten Schlüsselmanager.

Überlegungen zur Verwendung einer sicheren Löschung

- Volumes, die in einem Aggregat erstellt wurden, das für NetApp Aggregate Encryption (NAE) aktiviert ist, unterstützen das sichere Löschen nicht.
- Secure Purge ist nur für zuvor gelöschte Dateien auf Volumes mit NVE geeignet.
- Sie können ein unverschlüsseltes Volume nicht abreiben.
- Sie müssen KMIP-Server für die Schlüsselverwendung verwenden, nicht für den integrierten Schlüsselmanager.

Sichere Spülfunktionen je nach Version von ONTAP unterschiedlich.

ONTAP 9.8 und höher

- Sicheres Löschen wird von MetroCluster und FlexGroup unterstützt.
- Wenn das zu löckige Volume die Quelle einer SnapMirror-Beziehung ist, müssen Sie die SnapMirror-Beziehung nicht unterbrechen, um eine sichere Löschung durchzuführen.
- Die Umverschlüsselungsmethode unterscheidet sich bei Volumes, die SnapMirror Datensicherung verwenden, im Gegensatz zu Volumes, die keine SnapMirror Datensicherung (DP) verwenden, oder solchen, die SnapMirror erweiterte Datensicherung nutzen.
  - Standardmäßig werden Daten bei Volumes im SnapMirror Data Protection (DP)-Modus mit der erneuten Verschlüsselungsmethode für Volume Move neu verschlüsselt.
  - Standardmäßig verwenden Volumes, die keine SnapMirror Datensicherung oder Volumes verwenden, die den XDP-Modus (Extended Data Protection) von SnapMirror verwenden, die in-Place-Reverschlüsselungsmethode.
  - Diese Standardeinstellungen können mit dem geändert werden `secure purge re-encryption-method [volume-move|in-place-rekey]` Befehl.
- Standardmäßig werden alle Snapshot-Kopien in FlexVol Volumes während des sicheren Löschvorgangs automatisch gelöscht. Standardmäßig werden Snapshots in FlexGroup Volumes und Volumes mit SnapMirror Datensicherung nicht automatisch während des sicheren Löschvorgangs gelöscht. Diese Standardeinstellungen können mit dem geändert werden `secure purge delete-all-snapshots [true|false]` Befehl.

ONTAP 9.7 und früher:

- Sicheres Löschen unterstützt Folgendes nicht:
  - FlexClone
  - SnapVault
  - FabricPool
- Wenn das zu löckige Volume die Quelle einer SnapMirror-Beziehung ist, müssen Sie die SnapMirror-Beziehung unterbrechen, bevor Sie das Volume löschen können.

  Falls im Volume bereits Snapshot-Kopien vorhanden sind, müssen Sie die Snapshot-Kopien freigeben, bevor Sie das Volume löschen können. Beispielsweise müssen Sie ein FlexClone Volume unter Umständen von seinem übergeordneten Volume trennen.

- Durch das erfolgreiche Aufrufen der Funktion zum sicheren Löschen wird eine Volume-Verschiebung ausgelöst, die die verbleibenden, nicht gelöschten Daten mit einem neuen Schlüssel erneut verschlüsselt.

  Das verschobene Volume bleibt im aktuellen Aggregat. Der alte Schlüssel wird automatisch zerstört und stellt sicher, dass die gelöschten Daten nicht von den Speichermedien wiederhergestellt werden können.

Löschen Sie Daten auf einem verschlüsselten Volume sicher ohne SnapMirror Beziehung

Ab ONTAP 9.4 können Sie auf NVE-fähigen Volumes sichere Datenlöschung auch für unterbrechungsfreie „`sCrub`“-Daten verwenden.

Über diese Aufgabe

Die sichere Löschung kann in Abhängigkeit von der Datenmenge in den gelöschten Dateien mehrere Minuten bis viele Stunden dauern. Sie können das verwenden `volume encryption secure-purge show` Befehl zum Anzeigen des Status des Vorgangs. Sie können das verwenden `volume encryption secure-purge abort` Befehl zum Beenden des Vorgangs.

> Um eine sichere Löschung auf einem SAN-Host durchzuführen, müssen Sie die gesamte LUN löschen, die die zu löschenden Dateien enthält. Alternativ können Sie Löcher in der LUN für die Blöcke lochen, die zu den Dateien gehören, die gelöscht werden sollen. Wenn Sie die LUN nicht löschen können oder Ihr Host-Betriebssystem keine Stanzlöcher in der LUN unterstützt, können Sie keine sichere Löschung durchführen.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

Schritte

1. Löschen Sie die Dateien oder die LUN, die Sie löschen möchten.
   - Löschen Sie auf einem NAS-Client die Dateien, die Sie sicher löschen möchten.
   - Löschen Sie auf einem SAN-Host die LUN, die Sie löschen oder Löcher in der LUN sicher löschen möchten, damit die Blöcke zu den Dateien gehören, die gelöscht werden sollen.
2. Ändern Sie im Storage-System die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

3. Wenn die Dateien, die Sie sicher löschen möchten, in Snapshots gespeichert sind, löschen Sie die Snapshots:

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

4. Löschen Sie gelöschte Dateien sicher:

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   Mit dem folgenden Befehl werden die gelöschten Dateien auf sicher gelöscht `vol1` Auf SVM`vs1`:

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

5. Überprüfen Sie den Status des Secure-Purge-Vorgangs:

   ```
   volume encryption secure-purge show
   ```

Sicheres Löschen von Daten auf einem verschlüsselten Volume mit asynchroner SnapMirror Beziehung

Ab ONTAP 9.8 können Sie zum unterbrechungsfreien Löschen von „`sCrub`“-Daten auf NVE-fähigen Volumes mit asynchroner SnapMirror Beziehung verwenden.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

Über diese Aufgabe

Die sichere Löschung kann in Abhängigkeit von der Datenmenge in den gelöschten Dateien mehrere Minuten bis viele Stunden dauern. Sie können das verwenden `volume encryption secure-purge show` Befehl zum Anzeigen des Status des Vorgangs. Sie können das verwenden `volume encryption secure-purge abort` Befehl zum Beenden des Vorgangs.

> Um eine sichere Löschung auf einem SAN-Host durchzuführen, müssen Sie die gesamte LUN löschen, die die zu löschenden Dateien enthält. Alternativ können Sie Löcher in der LUN für die Blöcke lochen, die zu den Dateien gehören, die gelöscht werden sollen. Wenn Sie die LUN nicht löschen können oder Ihr Host-Betriebssystem keine Stanzlöcher in der LUN unterstützt, können Sie keine sichere Löschung durchführen.

Schritte

1. Wechseln Sie auf dem Speichersystem auf die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Löschen Sie die Dateien oder die LUN, die Sie löschen möchten.
   - Löschen Sie auf einem NAS-Client die Dateien, die Sie sicher löschen möchten.
   - Löschen Sie auf einem SAN-Host die LUN, die Sie löschen oder Löcher in der LUN sicher löschen möchten, damit die Blöcke zu den Dateien gehören, die gelöscht werden sollen.
3. Bereiten Sie das Zielvolumen in der asynchronen Beziehung vor, die sicher gelöscht werden soll:

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   Wiederholen Sie diesen Schritt für jedes Volume in Ihrer asynchronen SnapMirror Beziehung.

4. Wenn die Dateien, die Sie sicher löschen möchten, in Snapshot-Kopien gespeichert sind, löschen Sie die Snapshot-Kopien:

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

5. Wenn sich die Dateien, die Sie sicher löschen möchten, in den Basiskopien befinden, führen Sie folgende Schritte aus:

   a. Erstellen Sie in der asynchronen Beziehung von SnapMirror eine Snapshot Kopie auf dem Ziel-Volume:

      ```
      volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume
      volume_name
      ```

   b. Aktualisieren Sie SnapMirror, um die Snapshot Basiskopie nach vorn zu verschieben:

      ```
      snapmirror update -source-snapshot snapshot_name -destination-path
      destination_path
      ```

   Wiederholen Sie diesen Schritt für jedes Volume in der asynchronen SnapMirror-Beziehung.

a. Wiederholen Sie die Schritte (A) und (b) entsprechend der Anzahl der Basis-Snapshot-Kopien plus einer.

   Wenn Sie beispielsweise zwei Basis-Snapshot-Kopien haben, sollten Sie die Schritte (A) und (b) dreimal wiederholen.

b. Überprüfen Sie, ob die Snapshot Basiskopie vorhanden ist:

   `snapshot show -vserver SVM_name -volume volume_name`

c. Löschen Sie die Snapshot Basiskopie:

   `snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot`

6. Löschen Sie gelöschte Dateien sicher:

   `volume encryption secure-purge start -vserver svm_name -volume volume_name`

   Wiederholen Sie diesen Schritt für jedes Volume in der asynchronen SnapMirror-Beziehung.

   Mit dem folgenden Befehl werden die gelöschten Dateien auf „`vol1`“ auf SVM „`vs1`“ sicher gelöscht:

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

7. Überprüfen Sie den Status des sicheren Löschvorgangs:

   `volume encryption secure-purge show`

Scrub von Daten auf einem verschlüsselten Volume mit synchroner SnapMirror-Beziehung

Ab ONTAP 9.8 können Sie ein sicheres Löschen verwenden, um Daten auf NVE-fähigen Volumes mit einer synchronen SnapMirror Beziehung unterbrechungsfrei zu „Peeling“.

Über diese Aufgabe

Eine sichere Löschung kann in Abhängigkeit von der Datenmenge in den gelöschten Dateien von mehreren Minuten bis zu vielen Stunden dauern. Sie können das verwenden `volume encryption secure-purge show` Befehl zum Anzeigen des Status des Vorgangs. Sie können das verwenden `volume encryption secure-purge abort` Befehl zum Beenden des Vorgangs.

> Um eine sichere Löschung auf einem SAN-Host durchzuführen, müssen Sie die gesamte LUN löschen, die die zu löschenden Dateien enthält. Alternativ können Sie Löcher in der LUN für die Blöcke lochen, die zu den Dateien gehören, die gelöscht werden sollen. Wenn Sie die LUN nicht löschen können oder Ihr Host-Betriebssystem keine Stanzlöcher in der LUN unterstützt, können Sie keine sichere Löschung durchführen.

Bevor Sie beginnen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

Schritte

1. Ändern Sie im Storage-System die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Löschen Sie die Dateien oder die LUN, die Sie löschen möchten.
   - Löschen Sie auf einem NAS-Client die Dateien, die Sie sicher löschen möchten.
   - Löschen Sie auf einem SAN-Host die LUN, die Sie löschen oder Löcher in der LUN sicher löschen möchten, damit die Blöcke zu den Dateien gehören, die gelöscht werden sollen.
3. Bereiten Sie das Zielvolumen in der asynchronen Beziehung vor, die sicher gelöscht werden soll:

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   Wiederholen Sie diesen Schritt für das andere Volume in Ihrer synchronen SnapMirror-Beziehung.

4. Wenn die Dateien, die Sie sicher löschen möchten, in Snapshot-Kopien gespeichert sind, löschen Sie die Snapshot-Kopien:

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
   ```

5. Falls sich die Datei für die sichere Löschung im Basistelefon oder allgemeinen Snapshot Kopien befindet, aktualisieren Sie das SnapMirror, um die allgemeine Snapshot Kopie vorwärts zu verschieben:

   ```
   snapmirror update -source-snapshot snapshot_name -destination-path
   destination_path
   ```

   Es gibt zwei gemeinsame Snapshot Kopien. Dieser Befehl muss also zweimal ausgeführt werden.

6. Wenn sich die Datei für das sichere Löschen in der applikationskonsistenten Snapshot-Kopie befindet, löschen Sie die Snapshot-Kopie auf beiden Volumes der synchronen SnapMirror-Beziehung:

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot snapshot
   ```

   Führen Sie diesen Schritt auf beiden Volumes durch.

7. Löschen Sie gelöschte Dateien sicher:

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   Wiederholen Sie diesen Schritt für jedes Volume in der synchronen SnapMirror-Beziehung.

   Mit dem folgenden Befehl werden die gelöschten Dateien auf „`vol1`“ auf SMV „`vs1`“ sicher gelöscht.

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

8. Überprüfen Sie den Status des sicheren Löschvorgangs:

   ```
   volume encryption secure-purge show
   ```

Ändern Sie die Onboard-Passphrase für das Verschlüsselungsmanagement

Es handelt sich um eine Best Practice für Sicherheit, die Passphrase für das Onboard-Verschlüsselungsmanagement regelmäßig zu ändern. Sie sollten die neue Onboard-Passphrase für das Verschlüsselungsmanagement zur späteren Verwendung an einen sicheren Ort außerhalb des Storage-Systems kopieren.

Bevor Sie beginnen

- Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Ändern Sie die Onboard-Passphrase für das Verschlüsselungsmanagement:

Für diese ONTAP-Version…	Befehl
ONTAP 9.6 und höher	`security key-manager onboard update-passphrase`
ONTAP 9.5 und früher	`security key-manager update-passphrase`

   Eine vollständige Befehlssyntax finden Sie in den man-Pages.

   Mit dem folgenden Befehl von ONTAP 9.6 können Sie die Passphrase für das Onboard-Verschlüsselungsmanagement ändern `cluster1`:

   ```
   cluster1::> security key-manager onboard update-passphrase
   Warning: This command will reconfigure the cluster passphrase for
   onboard key management for Vserver "cluster1".
   Do you want to continue? {y|n}: y
   Enter current passphrase:
   Enter new passphrase:
   ```

3. Eingabe `y` Bei der Eingabeaufforderung zum Ändern der Onboard-Passphrase für das Verschlüsselungsmanagement.
4. Geben Sie die aktuelle Passphrase an der aktuellen Passphrase-Eingabeaufforderung ein.
5. Geben Sie an der neuen Passphrase-Eingabeaufforderung 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.

6. Geben Sie die Passphrase erneut an der Eingabeaufforderung zur Bestätigung der Passphrase ein.

Nachdem Sie fertig sind

In einer MetroCluster Umgebung müssen Sie die Passphrase im Partner-Cluster aktualisieren:

- In ONTAP 9.5 und früher müssen Sie ausgeführt werden `security key-manager update-passphrase` Mit derselben Passphrase im Partner-Cluster.
- In ONTAP 9.6 und höher werden Sie zur Ausführung aufgefordert `security key-manager onboard sync` Mit derselben Passphrase im Partner-Cluster.

Sie sollten die integrierte Passphrase für das Verschlüsselungsmanagement zur späteren Verwendung an einen sicheren Ort außerhalb des Storage-Systems kopieren.

Sie sollten die Informationen zum Verschlüsselungsmanagement manuell sichern, wenn Sie die Passphrase für das Onboard-Verschlüsselungsmanagement ändern.

"Manuelles Backup der integrierten Verschlüsselungsmanagementinformationen"

Manuelles Backup der integrierten Informationen für das Verschlüsselungsmanagement

Wenn Sie die Onboard-Passphrase für das Verschlüsselungsmanagement an einen sicheren Ort außerhalb des Storage-Systems konfigurieren, sollten Sie die Onboard-Verschlüsselungsmanagement-Informationen an einen sicheren Ort kopieren.

Was Sie benötigen

- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

Über diese Aufgabe

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

Schritte

1. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Anzeigen der Backup-Informationen für das Verschlüsselungsmanagement für das Cluster:

Für diese ONTAP-Version…	Befehl
ONTAP 9.6 und höher	`security key-manager onboard show-backup`
ONTAP 9.5 und früher	`security key-manager backup show`

Eine vollständige Befehlssyntax finden Sie in den man-Pages.

+ mit dem folgenden 9.6 Befehl werden die Backup-Informationen zum Schlüsselmanagement für angezeigt

`cluster1`:

+

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

     --------------------------BEGIN BACKUP--------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAAADuD+byAAAAACEAAAAAAAAA
     QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
     dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAAAACgAAAAAAAAAAA
     3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAAAA
     IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
     QRHwv+1aWvAAAAAAAAAAACQAAAAAAAAAAgAAAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
     BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABOZXRBcHAgS2V5IEJsb2IA
     AQAAAAMAAAAAYAQAAAAAADA5/ccAAAAAIgAAAAAAAAAAoAAAAAAAAAAEOTcR0AAAAA
     AAAAAAAAAAACAAAAAAAJAGr3tJA/LRzUQRHwv+1aWvAAAAAAAAAAACIAAAAAAAAAAA
     KAAAAAAAAACI8z/bAAAAAAAAAAAAAAAAAgAAAAAAAQAbxMcI4qiaMS4Uts5tTUnU
     AAAAAAAAAAAkAAAAAAAAAAIAAAAAAAAAAAqwxTcwAAAACkiwBAI3YeeV3jMFg5Smyj
     LSgoK/qc8FAmMMcrRXY6uriulnL0WPB/AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAE5ldEFwcCBLZXkgQmxvYgABAAAAAwAAABgBAAAAAAAA
     1cNLLwAAAAAiAAAAAAAAAAACgAAAAAAAAAAQ5NxHQAAAAAAAAAAAAAAAAIAAAAAAAkA
     ave0kD8tHNRBEfC/7Vpa8AAAAAAAAAAAIgAAAAAAAAAAoAAAAAAAAAAAJ4/cQsAAAAA
     AAAAAAAAAAACAAAAAAABAF6JCZch+IF+ZeOutovhv8oAAAAAAAAAAAACQAAAAAAAAAAA
     gAAAAAAAAAAN3Zq7AAAAALO7qD20+H8TuGgSauEHoqAyWcLv4uA0m2rrH4nPQM0n
     rDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
     ---------------------------END BACKUP---------------------------
```

1. Backup-Informationen sollten bei einem Notfall an einen sicheren Ort außerhalb des Storage-Systems kopiert werden.

Wiederherstellung der integrierten Verschlüsselungsschlüssel für das Verschlüsselungsmanagement

Das Verfahren zur Wiederherstellung der integrierten Verschlüsselungsschlüssel für das Verschlüsselungsmanagement variiert je nach Ihrer Version von ONTAP.

Bevor Sie beginnen

- Wenn Sie NSE mit einem externen KMIP-Server (Key Management) verwenden, müssen Sie die externe Schlüsselmanager-Datenbank gelöscht haben. Weitere Informationen finden Sie unter "Transition zum Onboard-Verschlüsselungsmanagement von externem Verschlüsselungsmanagement"
- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

> Wenn Sie NSE in einem System mit einem Flash Cache Modul verwenden, sollten Sie auch NVE oder NAE aktivieren. NSE verschlüsselt keine Daten im Flash Cache Modul.

ONTAP 9.6 und höher

> Wenn Sie ONTAP 9.8 oder höher ausführen und Ihr Stammvolume verschlüsselt ist, befolgen Sie das Verfahren für [ontap-9-8].

1. Vergewissern Sie sich, dass der Schlüssel wiederhergestellt werden muss:
   `security key-manager key query -node node`
2. Stellen Sie den Schlüssel wieder her:
   `security key-manager onboard sync`

   Eine vollständige Befehlssyntax finden Sie in den man-Pages.

   Mit dem folgenden ONTAP 9.6-Befehl werden die Schlüssel in der Onboard-Schlüsselhierarchie synchronisiert:

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

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

3. Geben Sie an der Eingabeaufforderung für die Passphrase die integrierte Passphrase für das Verschlüsselungsmanagement für das Cluster ein.

ONTAP 9.8 oder höher mit verschlüsseltem Root-Volume

Wenn Sie ONTAP 9.8 und höher verwenden und Ihr Root-Volume verschlüsselt ist, müssen Sie mit dem Boot-Menü eine integrierte Recovery-Passphrase für das Verschlüsselungsmanagement festlegen. Dieser Vorgang ist auch erforderlich, wenn Sie einen Bootmedienaustausch durchführen.

1. Starten Sie den Knoten im Startmenü, und wählen Sie Option `(10) Set onboard key management recovery secrets`.
2. Eingabe `y` Um diese Option zu verwenden.
3. Geben Sie an der Eingabeaufforderung die integrierte Passphrase für das Verschlüsselungsmanagement für das Cluster ein.
4. Geben Sie an der Eingabeaufforderung die Backup-Schlüsseldaten ein.

   Der Node kehrt zum Startmenü zurück.

5. Wählen Sie im Startmenü Option `(1) Normal Boot`.

ONTAP 9.5 und früher

1. Vergewissern Sie sich, dass der Schlüssel wiederhergestellt werden muss:
   `security key-manager key show`
2. Wenn Sie ONTAP 9.8 und höher verwenden und Ihr Root-Volume verschlüsselt ist, führen Sie folgende Schritte aus:

   Wenn Sie ONTAP 9.6 oder 9.7 verwenden oder ONTAP 9.8 oder höher verwenden und Ihr Root-Volume nicht verschlüsselt ist, überspringen Sie diesen Schritt.

3. Stellen Sie den Schlüssel wieder her:
   `security key-manager setup -node node`

   Eine vollständige Befehlssyntax finden Sie in den man-Pages.

4. Geben Sie an der Eingabeaufforderung für die Passphrase die integrierte Passphrase für das Verschlüsselungsmanagement für das Cluster ein.

Wiederherstellung der externen Verschlüsselungsschlüssel für das Verschlüsselungsmanagement

Sie können die externen Verschlüsselungsschlüssel zum Verschlüsselungsmanagement manuell wiederherstellen und sie auf einen anderen Node verschieben. Dies sollten Sie tun, wenn Sie einen Node neu starten, der während des Erstellungsens der Schlüssel für das Cluster vorübergehend nicht verfügbar war.

Über diese Aufgabe

In ONTAP 9.6 und höher können Sie die verwenden `security key-manager key query -node node_name` Befehl zum Überprüfen, ob Ihr Schlüssel wiederhergestellt werden muss.

In ONTAP 9.5 und früher können Sie die verwenden `security key-manager key show` Befehl zum Überprüfen, ob Ihr Schlüssel wiederhergestellt werden muss.

> Wenn Sie NSE in einem System mit einem Flash Cache Modul verwenden, sollten Sie auch NVE oder NAE aktivieren. NSE verschlüsselt keine Daten im Flash Cache Modul.

Bevor Sie beginnen

Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

Schritte

1. Wenn Sie ONTAP 9.8 oder höher verwenden und Ihr Root-Volume verschlüsselt ist, gehen Sie wie folgt vor:

   Wenn Sie ONTAP 9.7 oder früher oder ONTAP 9.8 oder höher verwenden und Ihr Root-Volume nicht verschlüsselt ist, überspringen Sie diesen Schritt.

   a. Legen Sie die Bootargs fest:
      ```
      setenv kmip.init.ipaddr <ip-address>+
      setenv kmip.init.netmask <netmask>+
      setenv kmip.init.gateway <gateway>+
      setenv kmip.init.interface e0M+
      ```

`boot_ontap`

b. Starten Sie den Knoten im Startmenü, und wählen Sie Option `(11) Configure node for external key management.`

c. Befolgen Sie die Anweisungen zum Eingeben des Managementzertifikats.

   Nachdem alle Informationen zum Managementzertifikat eingegeben wurden, kehrt das System zum Boot-Menü zurück.

d. Wählen Sie im Startmenü Option `(1) Normal Boot.`

2. Wiederherstellen des Schlüssels:

Für diese ONTAP-Version…	Befehl
ONTAP 9.6 und höher	`security key-manager external restore -vserver SVM -node node -key-server host_name
IP_address:port -key-id key_id -key -tag key_tag`	ONTAP 9.5 und früher

> `node` Standardeinstellung für alle Knoten. Eine vollständige Befehlssyntax finden Sie in den man-Pages. Dieser Befehl wird nicht unterstützt, wenn das integrierte Verschlüsselungsmanagement aktiviert ist.

Mit dem folgenden ONTAP 9.6-Befehl werden die Authentifizierungsschlüssel des externen Schlüsselmanagements auf alle Nodes in wiederhergestellt `cluster1`:

```
clusterl::> security key-manager external restore
```

Ersetzen Sie SSL-Zertifikate

Alle SSL-Zertifikate haben ein Ablaufdatum. Sie müssen Ihre Zertifikate aktualisieren, bevor sie ablaufen, um den Verlust des Zugriffs auf Authentifizierungsschlüssel zu verhindern.

Bevor Sie beginnen

- Sie müssen das öffentliche Ersatzzertifikat und den privaten Schlüssel für das Cluster (KMIP-Client-Zertifikat) erhalten haben.
- Sie müssen das öffentliche Ersatzzertifikat für den KMIP-Server (KMIP-Server-Ca-Zertifikat) erhalten haben.
- Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.
- In einer MetroCluster-Umgebung müssen Sie das KMIP SSL-Zertifikat auf beiden Clustern ersetzen.

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

Schritte

1. Installieren Sie das neue KMIP Server-Ca-Zertifikat:

   ```
   security certificate install -type server-ca -vserver <>
   ```

2. Installieren Sie das neue KMIP-Client-Zertifikat:

   ```
   security certificate install -type client -vserver <>
   ```

3. Aktualisieren Sie die Konfiguration des Schlüsselmanagers, um die neu installierten Zertifikate zu verwenden:

   ```
   security key-manager external modify -vserver <> -client-cert <> -server-ca
   -certs <>
   ```

   Wenn Sie ONTAP 9.6 oder höher in einer MetroCluster-Umgebung ausführen und die Schlüsselmanager-Konfiguration auf der Admin-SVM ändern möchten, müssen Sie den Befehl in der Konfiguration auf beiden Clustern ausführen.

> Wenn Sie die Konfiguration des Schlüsselmanagers zur Verwendung der neu installierten Zertifikate aktualisieren, wird ein Fehler ausgegeben, wenn sich die öffentlichen/privaten Schlüssel des neuen Clientzertifikats von den zuvor installierten Schlüsseln unterscheiden. Weitere Informationen finden Sie im Knowledge Base-Artikel "Das neue öffentliche oder private Clientzertifikat unterscheidet sich vom vorhandenen Clientzertifikat" Anweisungen zum Überschreiben dieses Fehlers finden Sie unter.

Ein FIPS-Laufwerk oder SED austauschen

Sie können ein FIPS-Laufwerk oder SED auf dieselbe Weise ersetzen, wie Sie eine normale Festplatte ersetzen. Stellen Sie sicher, dass Sie dem Ersatzlaufwerk neue Datenauthentifizierungsschlüssel zuweisen. Bei einem FIPS-Laufwerk kann auch ein neuer FIPS 140-2-Authentifizierungsschlüssel zugewiesen werden.

> Wenn ein HA-Paar nutzt "Verschlüsselung von SAS- oder NVMe-Laufwerken (SED, NSE, FIPS)", Sie müssen die Anweisungen im Thema folgen "Ein FIPS-Laufwerk oder eine SED-Festplatte in den ungeschützten Modus zurückkehren" Für alle Laufwerke innerhalb des HA-Paars vor der Initialisierung des Systems (Boot-Optionen 4 oder 9). Andernfalls kann es zu künftigen Datenverlusten kommen, wenn die Laufwerke einer anderen Verwendung zugewiesen werden.

Bevor Sie beginnen

- Sie müssen die Schlüssel-ID für den vom Laufwerk verwendeten Authentifizierungsschlüssel kennen.
- Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

Schritte

1. Stellen Sie sicher, dass die Festplatte als fehlgeschlagen markiert wurde:

   ```
   storage disk show -broken
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster1::> storage disk show -broken
Original Owner: cluster1-01
  Checksum Compatibility: block
                                                                    Usable
Physical
    Disk   Outage Reason HA Shelf Bay Chan   Pool  Type    RPM     Size
Size
    ------ ---- ------------ ---- --- ---- ------ -----  -----  -------
-------
    0.0.0  admin  failed  0b    1   0    A  Pool0  FCAL  10000  132.8GB
133.9GB
    0.0.7  admin  removed 0b    2   6    A  Pool1  FCAL  10000  132.8GB
134.2GB
[...]
```

2. Entfernen Sie die ausgefallene Festplatte, und ersetzen Sie sie durch ein neues FIPS-Laufwerk oder eine neue SED. Befolgen Sie die Anweisungen im Hardware-Leitfaden für das Festplatten-Shelf-Modell.
3. Besitzer der neu ersetzten Festplatte zuweisen:

   `storage disk assign -disk disk_name -owner node`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   ```
   cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
   ```

4. Vergewissern Sie sich, dass die neue Festplatte zugewiesen wurde:

   `storage encryption disk show`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
1.10.0  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
1.10.1  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
2.1.1   open 0x0
[...]
```

5. Weisen Sie den Datenauthentifizierungsschlüssel dem FIPS-Laufwerk oder der SED zu.

   "Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder einer SED (externes Verschlüsselungsmanagement)"

6. Weisen Sie bei Bedarf dem FIPS-Laufwerk einen FIPS 140-2-Authentifizierungsschlüssel zu.

   "Zuweisung eines FIPS 140-2-Authentifizierungsschlüssels zu einem FIPS-Laufwerk"

Daten auf einem FIPS-Laufwerk oder SED-Laufwerk können nicht darauf zugegriffen werden

Machen Sie Daten auf einem FIPS-Laufwerk oder SED unzugänglich Übersicht

Wenn Daten auf einem FIPS- oder SED-Laufwerk dauerhaft nicht zugänglich sind, aber den nicht genutzten Speicherplatz des Laufwerks für neue Daten beibehalten werden sollen, kann die Festplatte bereinigen. Wenn Sie Daten dauerhaft unzugänglich machen und Sie das Laufwerk nicht wiederverwenden müssen, können Sie es zerstören.

- Festplattenbereinigung

  Wenn Sie ein selbstverschlüsselndes Laufwerk desinfizieren, ändert das System den Verschlüsselungsschlüssel in einen neuen zufälligen Wert, setzt den Einschloß-Status auf false zurück und setzt die Schlüssel-ID auf einen Standardwert, entweder die Herstellersichere ID 0x0 (SAS-Laufwerke) oder einen Null-Schlüssel (NVMe-Laufwerke). Dadurch werden die Daten auf der Festplatte nicht mehr zugänglich und können nicht abgerufen werden. Sie können desinfizierte Festplatten als nicht auf Null bereinigte Ersatzfestplatten wiederverwenden.

- Festplatte zerstören

  Wenn Sie ein FIPS- oder SED-Laufwerk zerstören, setzt das System den Schlüssel für die Festplattenverschlüsselung auf einen unbekannten zufälligen Wert und sperrt die Festplatte unwiderruflich. Dadurch wird die Festplatte permanent nicht nutzbar und die Daten darauf dauerhaft zugänglich gemacht.

Es können einzelne Self-Encrypting Drives oder alle Self-Encrypting Drives eines Node bereinigen oder zerstört werden.

Ein FIPS-Laufwerk oder SED infizieren

Wenn Daten auf einem FIPS- oder SED-Laufwerk dauerhaft zugänglich gemacht und das Laufwerk für neue Daten verwendet werden soll, können Sie das verwenden `storage encryption disk sanitize` Befehl zum Löschen des Laufwerks.

Über diese Aufgabe

Wenn Sie ein selbstverschlüsselndes Laufwerk desinfizieren, ändert das System den Verschlüsselungsschlüssel in einen neuen zufälligen Wert, setzt den Einschloß-Status auf false zurück und setzt die Schlüssel-ID auf einen Standardwert, entweder die Herstellersichere ID 0x0 (SAS-Laufwerke) oder einen Null-Schlüssel (NVMe-Laufwerke). Dadurch werden die Daten auf der Festplatte nicht mehr zugänglich und können nicht abgerufen werden. Sie können desinfizierte Festplatten als nicht auf Null bereinigte Ersatzfestplatten wiederverwenden.

Bevor Sie beginnen

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

Schritte

1. Migrieren Sie alle Daten, die in einem Aggregat auf einer anderen Festplatte aufbewahrt werden müssen.
2. Löschen Sie das Aggregat auf dem FIPS-Laufwerk oder der SED, das bereinigt werden soll:

   `storage aggregate delete -aggregate` *`aggregate_name`*

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

3. Festplatten-ID für das zu desinfizierte FIPS-Laufwerk oder SED ermitteln:

   `storage encryption disk show -fields data-key-id,fips-key-id,owner`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   --------------------------------------------------------------------
   0.0.0   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   0.0.1   data
   F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
   1.10.2  data
   F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
   [...]
   ```

4. Wenn ein FIPS-Laufwerk im FIPS-Compliance-Modus ausgeführt wird, legen Sie die FIPS-Authentifizierungsschlüssel-ID für den Node wieder auf den Standard MSID 0x0:

   `storage encryption disk modify -disk disk_id -fips-key-id 0x0`

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

   ```
   cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

   Info: Starting modify on 1 disk.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

5. Antrieb desinfizieren:

   `storage encryption disk sanitize -disk disk_id`

   Mit diesem Befehl können Sie nur Hot-Spare- oder defekte Festplatten bereinigen. Um alle Festplatten unabhängig vom Typ zu desinfizieren, verwenden Sie das `-force-all-state` Option. Eine vollständige Befehlssyntax finden Sie in der man-Page.

   > ONTAP fordert Sie auf, eine Bestätigungsaufforderung einzugeben, bevor Sie fortfahren. Geben Sie den Ausdruck genau so ein, wie er auf dem Bildschirm angezeigt wird.

   ```
   cluster1::> storage encryption disk sanitize -disk 1.10.2

   Warning: This operation will cryptographically sanitize 1 spare or
   broken self-encrypting disk on 1 node.
            To continue, enter sanitize disk: sanitize disk

   Info: Starting sanitize on 1 disk.
         View the status of the operation using the
         storage encryption disk show-status command.
   ```

6. Entfernen Sie die desinfizierte Festplatte:
   `storage disk unfail -spare true -disk disk_id`
7. Prüfen Sie, ob die Festplatte einen Eigentümer hat:
   `storage disk show -disk disk_id`

   Wenn der Datenträger keinen Eigentümer hat, weisen Sie einen zu.
   `storage disk assign -owner node -disk disk_id`
8. Geben Sie den Knotenpunkt für den Knoten ein, der die Festplatten besitzt, die Sie desinfizieren möchten:

   `system node run -node node_name`

   Führen Sie die aus `disk sanitize release` Befehl.

9. Verlassen Sie die Nodeshell. Fehler der Festplatte erneut aufheben:
   `storage disk unfail -spare true -disk disk_id`
10. Überprüfen Sie, ob die Festplatte nun frei und in einem Aggregat wiederverwendet werden kann:
   `storage disk show -disk disk_id`

Ein FIPS-Laufwerk oder SED zerstören

Wenn Daten auf einem FIPS- oder SED-Laufwerk dauerhaft zugänglich gemacht werden sollen und Sie das Laufwerk nicht wiederverwenden müssen, können Sie das verwenden `storage encryption disk destroy` Befehl zum Zerstören der Festplatte.

Über diese Aufgabe

Wenn Sie ein FIPS- oder SED-Laufwerk zerstören, setzt das System den Schlüssel für die Festplattenverschlüsselung auf einen unbekannten zufälligen Wert und sperrt das Laufwerk unwiderruflich. Dadurch wird die Festplatte praktisch nicht nutzbar und die Daten auf ihr dauerhaft zugänglich. Sie können die Festplatte jedoch mithilfe der physischen sicheren ID (PSID) auf dem Etikett des Datenträgers auf die werkseitig konfigurierten Einstellungen zurücksetzen. Weitere Informationen finden Sie unter "Ein FIPS-Laufwerk oder eine SED-Appliance wird zurückgegeben, wenn Authentifizierungsschlüssel verloren gehen".

> Ein FIPS- oder SED-Laufwerk darf nur zerstört werden, wenn Sie über den Non-Returnable Disk Plus-Service (NRD Plus) verfügen. Beim Zerstören einer Festplatte wird die Gewährleistung nicht mehr abgedeckt.

Bevor Sie beginnen

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

Schritte

1. Migrieren Sie alle Daten, die in einem Aggregat auf einer anderen, unterschiedlichen Festplatte aufbewahrt werden müssen.
2. Löschen Sie das Aggregat auf dem zu zerstörenden FIPS-Laufwerk oder SED:

   `storage aggregate delete -aggregate aggregate_name`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

3. Identifizieren Sie die Festplatten-ID für das zu zerstörenden FIPS-Laufwerk oder die SED:

   `storage encryption disk show`

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
--------------------------------------------------------------------
0.0.0   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
0.0.1   data
F1CB30AFF1CB30B00101000000000000A68B167F92DD54196297159B5968923C
1.10.2  data
F1CB30AFF1CB30B00101000000000000CF0EFD81EA9F6324EA97B369351C56AC
[...]
```

4. Zerstören Sie die Festplatte:

   ```
   storage encryption disk destroy -disk disk_id
   ```

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

   > Sie werden aufgefordert, einen Bestätigungsphrase einzugeben, bevor Sie fortfahren. Geben Sie den Ausdruck genau so ein, wie er auf dem Bildschirm angezeigt wird.

```
cluster1::> storage encryption disk destroy -disk 1.10.2

Warning: This operation will cryptographically destroy 1 spare or broken
         self-encrypting disks on 1 node.
         You cannot reuse destroyed disks unless you revert
         them to their original state using the PSID value.
         To continue, enter
          destroy disk
         :destroy disk

Info: Starting destroy on 1 disk.
      View the status of the operation by using the
      "storage encryption disk show-status" command.
```

Notfall shred Daten auf einem FIPS-Laufwerk oder SED

Im Falle eines Sicherheitsnotfalls können Sie den Zugriff auf ein FIPS-Laufwerk oder eine SED umgehend verhindern, auch wenn dem Storage-System oder dem KMIP-Server keine Stromversorgung zur Verfügung steht.

Bevor Sie beginnen

- Wenn Sie einen KMIP-Server ohne Stromversorgung verwenden, muss der KMIP-Server mit einem einfach zerstörten Authentifizierungselement (z. B. eine Smartcard oder ein USB-Laufwerk) konfiguriert werden.

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

Schritt

1. Daten im Notfall auf einem FIPS-Laufwerk oder SED sreddern:

Wenn…	Dann…

Das Storage-System verfügt über einen Stromanstieg, und Sie können das Storage-System normal offline schalten	a. Wenn das Storage-System als HA-Paar konfiguriert ist, deaktivieren Sie Takeover. b. Alle Aggregate offline schalten und löschen. c. Stellen Sie die Berechtigungsebene auf Erweiteriert: + ein `set -privilege advanced` d. Wenn sich das Laufwerk im FIPS-Compliance-Modus befindet, setzen Sie die FIPS-Authentifizierungsschlüssel-ID für den Node wieder auf die Standard-MSID: `storage encryption disk modify -disk * -fips-key-id 0x0` e. Stoppen Sie das Speichersystem. f. Booten Sie im Wartungsmodus. g. Desinfizieren oder zerstören Sie die Festplatten: ◦ Wenn Sie die Daten auf den Datenträgern unzugänglich machen und die Festplatten dennoch wiederverwenden können, desinfizieren Sie die Festplatten: `disk encrypt sanitize -all` ◦ Wenn Sie die Daten auf den Laufwerken unzugänglich machen möchten und Sie die Festplatten nicht speichern müssen, zerstören Sie die Festplatten: `disk encrypt destroy disk_id1 disk_id2 …`	Dem Storage-System steht Strom zur Verfügung, und Sie müssen die Daten sofort schüttelt haben

a. **Wenn Sie die Daten auf den Datenträgern unzugänglich machen und die Festplatten noch wiederverwenden können, desinfizieren Sie die Festplatten:**
b. Wenn das Storage-System als HA-Paar konfiguriert ist, deaktivieren Sie Takeover.
c. Legen Sie die Berechtigungsebene auf erweitert fest:
`set -privilege advanced`
d. Wenn sich das Laufwerk im FIPS-Compliance-Modus befindet, legen Sie die FIPS-Authentifizierungsschlüssel-ID für den Node wieder auf die Standard-MSID fest:
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. Festplatte bereinigen:
`storage encryption disk sanitize -disk * -force-all-states true`
	a. **Wenn Sie die Daten auf den Datenträgern unzugänglich machen und Sie nicht brauchen, um die Festplatten zu speichern, zerstören Sie die Festplatten:**
	b. Wenn das Storage-System als HA-Paar konfiguriert ist, deaktivieren Sie Takeover.
	c. Legen Sie die Berechtigungsebene auf erweitert fest:
	`set -privilege advanced`
	d. Zerstören Sie die Festplatten:
	`storage encryption disk destroy -disk * -force-all-states true`
		Das Speichersystem kommt zu einer Panik, sodass das System dauerhaft deaktiviert ist, während alle Daten gelöscht werden. Um das System erneut zu verwenden, müssen Sie es neu konfigurieren.

Der KMIP-Server mit Strom ist, nicht jedoch für das Storage-System verfügbar	a. Melden Sie sich beim KMIP-Server an. b. Vernichten Sie alle Schlüssel, die den FIPS-Laufwerken oder SEDs zugeordnet sind, die die Daten enthalten, auf die Sie Zugriff verhindern möchten. Dadurch wird der Zugriff auf die Festplattenverschlüsselung durch das Speichersystem verhindert.	Der KMIP-Server oder das Storage-System bieten keine Stromversorgung

Eine vollständige Befehlssyntax finden Sie in den man-Pages.

Geben Sie ein FIPS-Laufwerk oder eine SED an den Dienst zurück, wenn Authentifizierungsschlüssel verloren gehen

Das System behandelt ein FIPS-Laufwerk oder eine SED als defekt, wenn die Authentifizierungsschlüssel dafür dauerhaft verloren gehen und nicht vom KMIP-Server abgerufen werden können. Obwohl Sie nicht auf die Daten auf der Festplatte zugreifen oder diese wiederherstellen können, können Sie Schritte Unternehmen, um den nicht genutzten Speicherplatz der SED für Daten erneut verfügbar zu machen.

Bevor Sie beginnen

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

Über diese Aufgabe

Sie sollten diesen Prozess nur verwenden, wenn Sie sicher sind, dass die Authentifizierungsschlüssel für das FIPS-Laufwerk oder die SED dauerhaft verloren gehen und nicht wiederhergestellt werden können.

Wenn die Festplatten partitioniert werden, müssen sie zunächst nicht partitioniert werden, bevor Sie diesen Prozess starten können.

> Der Befehl zum Entpartitionieren einer Festplatte ist nur auf der Diagnose-Ebene verfügbar und sollte nur unter NetApp Support Supervision durchgeführt werden. **Es wird dringend empfohlen, sich vor dem Fortfahren mit dem NetApp Support zu in Verbindung zu setzen.** Diese kann auch im Knowledge Base Artikel beschrieben werden "Wie man ein Ersatzlaufwerk in ONTAP entpartitionieren".

Schritte

1. Rückgabe eines FIPS-Laufwerks oder SED an den Dienst:

Wenn die SEDS…	Verwenden Sie die folgenden Schritte…

Nicht im FIPS-Compliance-Modus oder im FIPS-Compliance-Modus und der FIPS-Schlüssel ist verfügbar	a. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced` b. Setzen Sie den FIPS-Schlüssel auf die Standard-Herstellsichere ID 0x0: `storage encryption disk modify -fips-key-id 0x0 -disk` *`disk_id`* c. Überprüfen Sie, ob der Vorgang erfolgreich war: `storage encryption disk show-status`Wenn der Vorgang fehlgeschlagen ist, verwenden Sie den PSID-Prozess in diesem Thema. d. Bereinigen der defekten Scheibe: `storage encryption disk sanitize -disk` *`disk_id`*`Überprüfen Sie, ob der Vorgang mit dem Befehl erfolgreich war `storage encryption disk show-status` Bevor Sie mit dem nächsten Schritt fortfahren.  e. Entfernen Sie die desinfizierte Festplatte: `storage disk unfail -spare true -disk` *`disk_id`*  f. Prüfen Sie, ob die Festplatte einen Eigentümer hat: `storage disk show -disk` *`disk_id`*  Wenn der Datenträger keinen Eigentümer hat, weisen Sie einen zu. `storage disk assign -owner node -disk` *`disk_id`*  i. Geben Sie den Knotenpunkt für den Knoten ein, der die Festplatten besitzt, die Sie desinfizieren möchten:  `system node run -node` *`node_name`*  Führen Sie die aus `disk sanitize release` Befehl.  g. Verlassen Sie die Nodeshell. Fehler der Festplatte erneut aufheben: `storage disk unfail -spare true -disk` *`disk_id`*  h. Überprüfen Sie, ob die Festplatte nun frei und in einem Aggregat wiederverwendet werden kann: `storage disk show -disk` *`disk_id`*

Im FIPS-Compliance-Modus ist der FIPS-Schlüssel nicht verfügbar, und SEDs haben eine PSID auf dem Etikett	a. Beziehen Sie die PSID des Datenträgers von der Datenträgerbezeichnung. b. Legen Sie die Berechtigungsebene auf erweitert fest: `set -privilege advanced` c. Zurücksetzen der Festplatte auf die werkseitigen Einstellungen: `storage encryption disk revert-to-original-state -disk` *`disk_id`* `-psid` *`disk_physical_secure_id`*`Überprüfen Sie, ob der Vorgang mit dem Befehl erfolgreich war `storage encryption disk show-status` Bevor Sie mit dem nächsten Schritt fortfahren. d. Wenn Sie ONTAP 9.8P5 oder eine frühere Version verwenden, fahren Sie mit dem nächsten Schritt fort. Wenn Sie ONTAP 9.8P6 oder höher verwenden, nehmen Sie die bereinigte Festplatte wieder auf. `storage disk unfail -disk` *`disk_id`* e. Prüfen Sie, ob die Festplatte einen Eigentümer hat: `storage disk show -disk` *`disk_id`*  Wenn der Datenträger keinen Eigentümer hat, weisen Sie einen zu. `storage disk assign -owner node -disk` *`disk_id`*  i. Geben Sie den Knotenpunkt für den Knoten ein, der die Festplatten besitzt, die Sie desinfizieren möchten:  `system node run -node` *`node_name`*  Führen Sie die aus `disk sanitize release` Befehl.  f. Verlassen Sie die Nodeshell.. Fehler der Festplatte erneut aufheben: `storage disk unfail -spare true -disk` *`disk_id`* g. Überprüfen Sie, ob die Festplatte nun frei und in einem Aggregat wiederverwendet werden kann: `storage disk show -disk` *`disk_id`*

Eine vollständige Befehlssyntax finden Sie im "Befehlsreferenz".

Geben Sie ein FIPS-Laufwerk oder eine SED in den ungeschützten Modus zurück

Ein FIPS-Laufwerk oder SED ist nur dann vor unberechtigtem Zugriff geschützt, wenn die Authentifizierungsschlüssel-ID für den Knoten auf einen anderen Wert als den Standardwert gesetzt ist. Sie können ein FIPS-Laufwerk oder eine SED über den in den ungeschützten Modus versetzen `storage encryption disk modify` Befehl zum Festlegen der Schlüssel-ID auf Standard.

Wenn ein HA-Paar SAS- oder NVMe-Laufwerke (SED, NSE, FIPS) verwendet, müssen Sie diesen Prozess für alle Laufwerke innerhalb des HA-Paars befolgen, bevor das System initialisiert wird (Boot-Optionen 4 oder 9). Andernfalls kann es zu künftigen Datenverlusten kommen, wenn die Laufwerke einer anderen Verwendung zugewiesen werden.

Bevor Sie beginnen

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

Schritte

1. Legen Sie die Berechtigungsebene auf erweitert fest:

   ```
   set -privilege advanced
   ```

2. Wenn ein FIPS-Laufwerk im FIPS-Compliance-Modus ausgeführt wird, legen Sie die FIPS-Authentifizierungsschlüssel-ID für den Node wieder auf den Standard MSID 0x0:

   ```
   storage encryption disk modify -disk disk_id -fips-key-id 0x0
   ```

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

   ```
   cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id
   0x0

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

   Bestätigen Sie den Vorgang mit dem Befehl:

   ```
   storage encryption disk show-status
   ```

   Wiederholen Sie den Befehl show-Status, bis die Zahlen in „Disks gestartet“ und „Disks Fertig“ die gleichen sind.

   ```
   cluster1:: storage encryption disk show-status

               FIPS    Latest   Start                Execution   Disks
   Disks Disks
   Node        Support Request  Timestamp            Time (sec)  Begun
   Done  Successful
   -------     ------- -------- ------------------   ---------- ------
   ------  ----------
   cluster1    true    modify   1/18/2022 15:29:38    3           14     5
   5
   1 entry was displayed.
   ```

3. Legen Sie die Daten-Authentifizierungsschlüssel-ID für den Knoten wieder auf die Standard-MSID 0x0:

   ```
   storage encryption disk modify -disk disk_id -data-key-id 0x0
   ```

   Der Wert von `-data-key-id` Sollte auf 0x0 gesetzt werden, ob Sie ein SAS- oder NVMe-Laufwerk in den ungeschützten Modus zurücksenden.

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

```
cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id
0x0

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

Bestätigen Sie den Vorgang mit dem Befehl:

```
storage encryption disk show-status
```

Wiederholen Sie den Befehl show-Status, bis die Zahlen identisch sind. Die Operation ist abgeschlossen, wenn die Zahlen in „Platten begonnen“ und „Platten fertig“ sind die gleichen.

Wartungsmodus

Ab ONTAP 9.7 können Sie eine FIPS-Festplatte aus dem Wartungsmodus neu Schlüssel aktivieren. Sie sollten den Wartungsmodus nur verwenden, wenn Sie die ONTAP-CLI-Anweisungen im vorherigen Abschnitt nicht verwenden können.

Schritte

1. Legen Sie die FIPS-Authentifizierungsschlüssel-ID für den Knoten wieder auf die Standard-MSID 0x0:

   `disk encrypt rekey_fips 0x0 *disklist*`

2. Legen Sie die Daten-Authentifizierungsschlüssel-ID für den Knoten wieder auf die Standard-MSID 0x0:

   `disk encrypt rekey 0x0 *disklist*`

3. Bestätigen Sie, dass der FIPS-Authentifizierungsschlüssel erfolgreich umcodiert wurde:

   `disk encrypt show_fips`

4. Bestätigung der erfolgreichen Verschlüsselung des Datenauthentifizierungsschlüssels mit:

   `disk encrypt show`

   In Ihrer Ausgabe wird wahrscheinlich entweder die Standard-MSID 0x0-Schlüssel-ID oder der 64-stellige Wert des Schlüsselservers angezeigt. Der `Locked?` Feld bezieht sich auf die Datensperrung.

```
Disk       FIPS Key ID                 Locked?
---------- --------------------------- -------
0a.01.0    0x0                          Yes
```

Entfernen Sie eine externe Schlüsselmanager-Verbindung

Sie können einen KMIP-Server von einem Node trennen, wenn Sie den Server nicht

mehr benötigen. Beispielsweise können Sie einen KMIP-Server trennen, wenn Sie die Volume-Verschlüsselung umstellen.

Über diese Aufgabe

Wenn Sie einen KMIP Server von einem Node in einem HA-Paar trennen, trennt das System die Verbindung zwischen dem Server automatisch und allen Cluster-Nodes.

> Wenn Sie nach der Trennung eines KMIP Servers weiterhin externes Verschlüsselungsmanagement nutzen möchten, stellen Sie sicher, dass ein anderer KMIP Server für die Authentifizierung von Schlüsseln zur Verfügung steht.

Bevor Sie beginnen

Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.

Schritt

1. Trennen eines KMIP-Servers vom aktuellen Node:

Für diese ONTAP-Version…	Befehl
ONTAP 9.6 und höher	`security key-manager external remove-servers -vserver SVM -key -servers host_name
IP_address:port,…`	ONTAP 9.5 und früher

In einer MetroCluster Umgebung müssen Sie die folgenden Befehle für beide Cluster für die Administrator-SVM wiederholen.

Eine vollständige Befehlssyntax finden Sie in den man-Pages.

Mit dem folgenden ONTAP 9.6-Befehl werden die Verbindungen zu zwei externen Schlüsselverwaltungsservern für deaktiviert `cluster1`, Der erste benannte `ks1`, Hören auf dem Standardport 5696, der zweite mit der IP-Adresse 10.0.0.20, Hören auf Port 24482:

```
clusterl::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

Ändern Sie die Eigenschaften des Servers für die Verwaltung externer Schlüssel

Ab ONTAP 9.6 können Sie den verwenden `security key-manager external modify-server` Befehl zum Ändern der I/O-Zeitüberschreitung und des Benutzernamens eines externen Schlüsselverwaltungsservers.

Bevor Sie beginnen

- Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.
- In einer MetroCluster Umgebung müssen Sie die folgenden Schritte auf beiden Clustern für den Administrator-SVM wiederholen.

Schritte

1. Ändern Sie im Storage-System die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Ändern der Eigenschaften eines externen Schlüsselmanagers-Servers für das Cluster:

   ```
   security key-manager external modify-server -vserver admin_SVM -key-server
   host_name|IP_address:port,… -timeout 1…60 -username user_name
   ```

   > Der Timeout-Wert wird in Sekunden angegeben. Wenn Sie den Benutzernamen ändern, werden Sie aufgefordert, ein neues Passwort einzugeben. 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 die Eigenschaften eines externen Schlüsselmanager-Servers zu ändern.

   Mit dem folgenden Befehl wird der Zeitüberschreitungswert für das in 45 Sekunden geändert `cluster1` Externer Schlüsselverwaltungsserver, der auf dem Standardport 5696 zuhören wird:

   ```
   clusterl::> security key-manager external modify-server -vserver
   cluster1 -key-server ks1.local -timeout 45
   ```

3. Ändern Sie die Server-Eigenschaften von externen Verschlüsselungsmanagement für eine SVM (nur NVE):

   ```
   security key-manager external modify-server -vserver SVM -key-server
   host_name|IP_address:port,… -timeout 1…60 -username user_name
   ```

   > Der Timeout-Wert wird in Sekunden angegeben. Wenn Sie den Benutzernamen ändern, werden Sie aufgefordert, ein neues Passwort einzugeben. Wenn Sie den Befehl an der SVM-Anmeldeaufforderung ausführen, *SVM* Standardeinstellung ist die aktuelle SVM. Zum Ändern der Eigenschaften des externen Schlüsselmanager-Servers müssen Sie der Cluster oder der SVM-Administrator sein.

   Mit dem folgenden Befehl werden der Benutzername und das Passwort des geändert `svm1` Externer Schlüsselverwaltungsserver, der auf dem Standardport 5696 zuhören wird:

   ```
   svml::> security key-manager external modify-server -vserver svm11 -key
   -server ks1.local -username svm1user
   Enter the password:
   Reenter the password:
   ```

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

Wechsel vom Onboard-Verschlüsselungsmanagement auf externes Verschlüsselungsmanagement

Wenn Sie von Onboard-Verschlüsselungsmanagement auf externes Verschlüsselungsmanagement wechseln möchten, müssen Sie die integrierte Verschlüsselungsmanagementkonfiguration löschen, bevor Sie externes Verschlüsselungsmanagement aktivieren können.

Bevor Sie beginnen

- Bei der hardwarebasierten Verschlüsselung müssen die Datenschlüssel aller FIPS-Laufwerke oder SEDs auf den Standardwert zurückgesetzt werden.

  "Ein FIPS-Laufwerk oder eine SED-Festplatte in den ungeschützten Modus zurückkehren"

- Bei softwarebasierter Verschlüsselung müssen Sie alle Volumes entschlüsseln.

  "Verschlüsselung von Volume-Daten aufheben"

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

Schritt

1. Löschen der integrierten Verschlüsselungsmanagementkonfiguration für ein Cluster:

Für diese ONTAP-Version…	Befehl
ONTAP 9.6 und höher	`security key-manager onboard disable -vserver SVM`
ONTAP 9.5 und früher	`security key-manager delete-key-database`

Vollständige Befehlssyntax finden Sie im "Befehlsreferenz für ONTAP".

Umstellung von externem Verschlüsselungsmanagement auf integriertes Verschlüsselungsmanagement

Wenn Sie von externem Verschlüsselungsmanagement auf integriertes Verschlüsselungsmanagement umsteigen möchten, müssen Sie die Konfiguration für das externe Verschlüsselungsmanagement löschen, bevor Sie integriertes Verschlüsselungsmanagement aktivieren können.

Bevor Sie beginnen

- Bei der hardwarebasierten Verschlüsselung müssen die Datenschlüssel aller FIPS-Laufwerke oder SEDs auf den Standardwert zurückgesetzt werden.

  "Ein FIPS-Laufwerk oder eine SED-Festplatte in den ungeschützten Modus zurückkehren"

- Sie müssen alle externen Schlüsselmanager-Verbindungen gelöscht haben.

  "Löschen einer externen Schlüsselmanager-Verbindung"

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

Verfahren

Die Schritte zur Umstellung Ihres Schlüsselmanagements hängen von der verwendeten Version von ONTAP ab.

ONTAP 9.6 und höher

1. Ändern Sie die erweiterte Berechtigungsebene:

   ```
   set -privilege advanced
   ```

2. Verwenden Sie den Befehl:

   ```
   security key-manager external disable -vserver admin_SVM
   ```

   In einer MetroCluster-Umgebung müssen Sie den Befehl für die Administrator-SVM auf beiden Clustern wiederholen.

ONTAP 9.5 und früher

Verwenden Sie den Befehl:
`security key-manager delete-kmip-config`

Was passiert, wenn während des Startvorgangs keine Schlüsselverwaltungsserver verfügbar sind

ONTAP ergreift Maßnahmen, um unerwünschte Verhaltensweisen zu vermeiden, wenn ein mit NSE konfiguriertes Storage-System während des Bootens keinen der angegebenen Verschlüsselungsmanagementserver erreichen kann.

Wenn das Storage-System für NSE konfiguriert ist, werden die SEDs rekeyed und gesperrt und die SEDs eingeschaltet. Das Storage-System muss die erforderlichen Authentifizierungsschlüssel von den Verschlüsselungsmanagement-Servern abrufen, um sich bei SEDs zu authentifizieren, bevor es auf die Daten zugreifen kann.

Das Storage-System versucht, bis zu drei Stunden lang die angegebenen Schlüsselmanagementserver zu kontaktieren. Sollte das Storage-System zu diesem Zeitpunkt keinen Zugang haben, wird der Bootvorgang abgebrochen und das Storage-System stoppt.

Wenn das Speichersystem einen bestimmten Schlüsselverwaltungsserver erfolgreich kontaktiert, versucht es dann, eine SSL-Verbindung für bis zu 15 Minuten herzustellen. Wenn das Storage-System keine SSL-Verbindung zu einem angegebenen Schlüsselmanagementserver herstellen kann, wird der Bootvorgang angehalten und das Speichersystem wird angehalten.

Während das Speichersystem versucht, sich mit wichtigen Managementservern zu verbinden und eine Verbindung herzustellen, werden in der CLI detaillierte Informationen über fehlgeschlagene Kontaktversuche angezeigt. Sie können die Kontaktversuche jederzeit unterbrechen, indem Sie Strg-C drücken

Als Sicherheitsmaßnahme erlauben SEDs nur eine begrenzte Anzahl von unbefugten Zugriffsversuchen, wonach sie den Zugriff auf die vorhandenen Daten deaktivieren. Wenn das Speichersystem keine bestimmten Schlüsselverwaltungsserver kontaktieren kann, um die richtigen Authentifizierungsschlüssel zu erhalten, kann es nur versuchen, sich mit dem Standardschlüssel zu authentifizieren, der zu einem fehlgeschlagenen Versuch

und einem Panikzustand führt. Wenn das Storage-System so konfiguriert ist, dass es im Falle eines Panikzustands automatisch neu gestartet wird, wird eine Boot-Schleife erzeugt, die zu kontinuierlichen fehlgeschlagenen Authentifizierungsversuchen von SEDs führt.

Das Anhalten des Storage-Systems in diesen Szenarien ist durch das Design zu verhindern, dass das Storage-System in einen Boot-Loop und möglichen unbeabsichtigten Datenverlust durch die dauerhaft gesperrten SEDs gelangt, da es die Sicherheitsgrenze einer bestimmten Anzahl aufeinander folgender fehlgeschlagener Authentifizierungsversuche überschreitet. Der Grenzwert und die Art des Sperrschutzes hängen von den Herstellungsspezifikationen und dem Typ der SED ab:

SED-Typ	Anzahl aufeinanderfolgender fehlgeschlagener Authentifizierungsversuche, die zu einer Sperrung führen	Sicherungstyp sperren, wenn die Sicherheitsgrenze erreicht ist
HDD	1024	Dauerhaft: Daten können nicht wiederhergestellt werden, selbst wenn der richtige Authentifizierungsschlüssel wieder verfügbar ist.
X440_PHM2800MCTO 800 GB NSE SSDs mit Firmware-Versionen NA00 oder NA01	5	Temporär. Die Sperrung wird nur wirksam, bis die Festplatte aus- und wieder eingeschaltet wird.
X577_PHM2800MCTO 800 GB NSE SSDs mit Firmware-Versionen NA00 oder NA01	5	Temporär. Die Sperrung wird nur wirksam, bis die Festplatte aus- und wieder eingeschaltet wird.
X440_PHM2800MCTO 800 GB NSE SSDs mit höherer Firmware-Version	1024	Dauerhaft: Daten können nicht wiederhergestellt werden, selbst wenn der richtige Authentifizierungsschlüssel wieder verfügbar ist.
X577_PHM2800MCTO 800 GB NSE SSDs mit höherer Firmware-Version	1024	Dauerhaft: Daten können nicht wiederhergestellt werden, selbst wenn der richtige Authentifizierungsschlüssel wieder verfügbar ist.
Alle anderen SSD-Modelle	1024	Dauerhaft: Daten können nicht wiederhergestellt werden, selbst wenn der richtige Authentifizierungsschlüssel wieder verfügbar ist.

Bei allen SED-Typen wird durch eine erfolgreiche Authentifizierung die Anzahl der Versuche auf Null zurückgesetzt.

Wenn dieses Szenario auftritt, bei dem das Speichersystem aufgrund eines Fehlers angehalten wird, um irgendwelche angegebenen Schlüsselverwaltungsserver zu erreichen, müssen Sie zuerst die Ursache für den Kommunikationsfehler identifizieren und korrigieren, bevor Sie versuchen, das Speichersystem weiterhin zu booten.

Deaktivieren Sie die Verschlüsselung standardmäßig

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 Bedarf können Sie die Verschlüsselung standardmäßig für den gesamten Cluster deaktivieren.

Bevor Sie beginnen

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

Schritt

1. Führen Sie den folgenden Befehl aus, um die Verschlüsselung für das gesamte Cluster in ONTAP 9.7 oder höher standardmäßig zu deaktivieren:

   ```
   options -option-name encryption.data_at_rest_encryption.disable_by_default
   -option-value on
   ```

Copyright-Informationen

Markeninformationen