Verschlüsselung mit der Befehlszeile verwalten

ONTAP 9

NetApp
November 10, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/encryption-at-rest/index.html on November 10, 2026. Always check docs.netapp.com for the latest.

Inhalt

Verschlüsselung mit der Befehlszeile verwalten . . . 1
- Informationen zur ONTAP Daten im Ruhezustand Verschlüsselung . . . 1
- Informationen zu ONTAP NetApp Volume- und Aggregatverschlüsselung . . . 1
  - Überblick über NVE . . . 1
  - Verschlüsselung auf Aggregatebene . . . 2
  - Wann externe Schlüsselverwaltungsserver verwendet werden . . . 2
  - Umfang des externen Schlüsselmanagements . . . 3
  - Supportdetails . . . 3
- ONTAP NetApp Volume Encryption-Workflow . . . 5
- NVE konfigurieren . . . 6
  - Feststellen, ob Ihre ONTAP Cluster-Version NVE unterstützt . . . 6
  - Die Volumenverschlüsselungslizenz auf einem ONTAP Cluster installieren . . . 7
  - Externe Schlüsselverwaltung konfigurieren . . . 7
  - Integrierte Schlüsselverwaltung für NVE in ONTAP 9.6 und höher aktivieren . . . 24
  - Integrierte Schlüsselverwaltung für NVE in ONTAP 9.5 und früher aktivieren . . . 26
  - Aktivierung der integrierten Schlüsselverwaltung auf neu hinzugefügten ONTAP Knoten . . . 28
- Volumendaten mit NVE oder NAE verschlüsseln . . . 29
  - Informationen zur Verschlüsselung von ONTAP Volume-Daten mit NVE . . . 29
  - Verschlüsselung auf Aggregatebene mit der VE-Lizenz in ONTAP aktivieren . . . 30
  - Verschlüsselung auf einem neuen Volume in ONTAP aktivieren . . . 31
  - NAE oder NVE auf einem vorhandenen ONTAP Volume aktivieren . . . 33
  - Konfiguration von NVE auf einem ONTAP SVM Root-Volume . . . 37
  - Konfiguration von NVE auf einem ONTAP Knoten-Root-Volume . . . 38
- Hardwarebasierte Verschlüsselung von NetApp konfigurieren . . . 39
  - Informationen zu ONTAP hardwarebasierter Verschlüsselung . . . 39
  - Externe Schlüsselverwaltung konfigurieren . . . 42
  - Onboard-Schlüsselverwaltung konfigurieren . . . 55
  - Einem ONTAP FIPS-Laufwerk einen FIPS 140-2-Authentifizierungsschlüssel zuweisen . . . 61
  - Clusterweiten FIPS-konformen Modus für KMIP-Verbindungen in ONTAP aktivieren . . . 62
- Verwaltung der NetApp Verschlüsselung . . . 64
  - Volumendaten in ONTAP entschlüsseln . . . 64
  - Verschieben eines verschlüsselten Volumes in ONTAP . . . 64
  - Änderung des Verschlüsselungsschlüssels für ein ONTAP Volume . . . 65
  - Änderung des Verschlüsselungsschlüssels für ein ONTAP Volume . . . 67
  - Rotation von Authentifizierungsschlüsseln für NetApp Storage Encryption in ONTAP . . . 68
  - Löschen eines verschlüsselten Volumes in ONTAP . . . 68
  - Daten auf einem verschlüsselten Volume sicher löschen . . . 69
  - Die Passphrase für die ONTAP Onboard-Schlüsselverwaltung ändern . . . 74
  - ONTAP Onboard-Schlüsselverwaltungsinformationen manuell sichern . . . 76
  - Onboard Key Management-Verschlüsselungsschlüssel in ONTAP wiederherstellen . . . 77
  - Wiederherstellung der ONTAP externen Schlüsselverwaltungs-Verschlüsselungsschlüssel . . . 79
  - KMIP SSL-Zertifikate auf dem ONTAP Cluster ersetzen . . . 80
  - Austausch eines FIPS-Laufwerks oder SED in ONTAP . . . 81

Daten auf einem FIPS-Laufwerk oder SED unzugänglich machen . . . 83
Wiederherstellung des Betriebs eines FIPS-Laufwerks oder einer ONTAP SED bei verlorenen Schlüsseln . . . 91
Ein FIPS-Laufwerk oder SED in ONTAP in den ungeschützten Modus zurückversetzen . . . 93
Eine externe Schlüsselverwaltungsverbindung in ONTAP entfernen . . . 96
Eigenschaften des externen Schlüsselverwaltungsservers von ONTAP ändern . . . 97
Übergang von der internen zur externen Schlüsselverwaltung in ONTAP . . . 98
Wechsel von externer Schlüsselverwaltung zu ONTAP interner Schlüsselverwaltung . . . 99
Wie ONTAP mit nicht erreichbaren Schlüsselverwaltungsservern während des Systemstarts umgeht . 100
ONTAP Verschlüsselung standardmäßig deaktiviert . . . 101

Verschlüsselung mit der Befehlszeile verwalten

Informationen zur ONTAP Daten im Ruhezustand Verschlüsselung

NetApp bietet sowohl software- als auch hardwarebasierte Verschlüsselungstechnologien, um sicherzustellen, dass Daten im Ruhezustand nicht gelesen werden können, wenn das Speichermedium umfunktioniert, zurückgegeben, verlegt oder gestohlen wird.

- Die softwarebasierte Verschlüsselung mittels NetApp Volume Encryption (NVE) unterstützt die Datenverschlüsselung jeweils eines Volumens
- Die hardwarebasierte Verschlüsselung mittels NetApp Storage Encryption (NSE) unterstützt die vollständige Festplattenverschlüsselung (FDE) der Daten während des Schreibvorgangs.

Informationen zu ONTAP NetApp Volume- und Aggregatverschlüsselung

NetApp Volume Encryption (NVE) ist eine softwarebasierte Technologie zur Verschlüsselung von Daten im Ruhezustand, jeweils eines Volumes. Ein nur dem Speichersystem zugänglicher Verschlüsselungsschlüssel gewährleistet, dass die Volume-Daten nicht gelesen werden können, falls das zugrunde liegende Gerät anderweitig verwendet, zurückgegeben, verlegt oder gestohlen wird.

Überblick über NVE

Bei NVE werden sowohl Metadaten als auch Daten (einschließlich Snapshots) verschlüsselt. Der Zugriff auf die Daten erfolgt über einen eindeutigen XTS-AES-256-Schlüssel, einen pro Volume. Ein externer Schlüsselverwaltungsserver oder Onboard Key Manager (OKM) stellt den Knoten die Schlüssel bereit:

- Der externe Schlüsselverwaltungsserver ist ein Drittanbietersystem in Ihrer Speicherumgebung, das Schlüssel für Knoten mithilfe des Key Management Interoperability Protocol (KMIP) bereitstellt. Es gilt als Best Practice, externe Schlüsselverwaltungsserver auf einem anderen Speichersystem als Ihren Daten zu konfigurieren.
- Der Onboard Key Manager ist ein integriertes Tool, das Schlüssel für Knoten aus demselben Speichersystem bereitstellt, in dem sich auch Ihre Daten befinden.

Ab ONTAP 9.7 ist die Aggregat- und Volumenverschlüsselung standardmäßig aktiviert, sofern Sie über eine Volumenverschlüsselungslizenz (VE) verfügen und einen integrierten oder externen Schlüsselmanager verwenden. Die VE-Lizenz ist mit "ONTAP One" enthalten. Sobald ein externer oder interner Schlüsselmanager konfiguriert ist, ändert sich die Art und Weise, wie die Verschlüsselung von Daten im Ruhezustand für neue Aggregate und neue Volumes konfiguriert wird. Neue Aggregate haben NetApp Aggregate Encryption (NAE) standardmäßig aktiviert. Neue Volumes, die nicht Teil eines NAE-Aggregats sind, haben NetApp Volume Encryption (NVE) standardmäßig aktiviert. Wenn eine Storage Virtual Machine (SVM) mit einem eigenen Schlüsselmanager unter Verwendung von mandantenfähigem Schlüsselmanagement konfiguriert ist, wird das für diese SVM erstellte Volume automatisch mit NVE konfiguriert.

Sie können die Verschlüsselung für ein neues oder bestehendes Volume aktivieren. NVE unterstützt alle

Funktionen zur Speichereffizienz, einschließlich Deduplizierung und Komprimierung. Ab ONTAP 9.14.1 ist es möglich, NVE auf vorhandenen SVM Root-Volumes aktivieren.

> Wenn Sie SnapLock verwenden, kann die Verschlüsselung nur auf neuen, leeren SnapLock Volumes aktiviert werden. Die Verschlüsselung kann auf einem bestehenden SnapLock-Volume nicht aktiviert werden.

NVE kann auf jedem Aggregattyp (HDD, SSD, Hybrid, Array-LUN), mit jedem RAID-Typ und in jeder unterstützten ONTAP Implementierung, einschließlich ONTAP Select, verwendet werden. NVE kann außerdem mit hardwarebasierter Verschlüsselung genutzt werden, um Daten auf selbstverschlüsselnden Laufwerken „doppelt zu verschlüsseln“.

Wenn NVE aktiviert ist, wird auch der Core Dump verschlüsselt.

Verschlüsselung auf Aggregatebene

Normalerweise wird jedem verschlüsselten Datenträger ein eindeutiger Schlüssel zugewiesen. Wenn der Datenträger gelöscht wird, wird auch der Schlüssel gelöscht.

Ab ONTAP 9.6 kann die NetApp Aggregate Encryption (NAE) verwendet werden, um Schlüssel dem Aggregat zuzuweisen, das die zu verschlüsselnden Volumes enthält. Wenn ein verschlüsseltes Volume gelöscht wird, bleiben die Schlüssel für das Aggregat erhalten. Die Schlüssel werden gelöscht, wenn das gesamte Aggregat gelöscht wird.

Eine Verschlüsselung auf Aggregatebene ist erforderlich, wenn eine Inline- oder Hintergrunddeduplizierung auf Aggregatebene vorgesehen ist. Die Deduplizierung auf Aggregatebene wird ansonsten von NVE nicht unterstützt.

Ab ONTAP 9.7 ist die Aggregat- und Volumenverschlüsselung standardmäßig aktiviert, sofern Sie über eine Volumenverschlüsselungslizenz (VE) verfügen und einen integrierten oder externen Schlüsselmanager verwenden.

NVE- und NAE-Volumes können auf demselben Aggregat koexistieren. Volumes, die unter Aggregat-Verschlüsselung verschlüsselt werden, sind standardmäßig NAE-Volumes. Die Standardeinstellung kann bei der Verschlüsselung des Volumes außer Kraft gesetzt werden.

Sie können den `volume move`Befehl verwenden, um ein NVE-Volume in ein NAE-Volume zu konvertieren und umgekehrt. Ein NAE-Volume kann auf ein NVE-Volume repliziert werden.

Sie können `secure purge`-Befehle nicht auf einem NAE-Volume verwenden.

Wann externe Schlüsselverwaltungsserver verwendet werden

Auch wenn die Verwendung des integrierten Schlüsselmanagers kostengünstiger und in der Regel bequemer ist, empfiehlt sich die Einrichtung von KMIP-Servern, wenn eine der folgenden Bedingungen zutrifft:

- Ihre Lösung zur Verwaltung von Verschlüsselungsschlüsseln muss den Federal Information Processing Standards (FIPS) 140-2 oder dem OASIS KMIP Standard entsprechen.
- Sie benötigen eine Multi-Cluster-Lösung mit zentralisierter Verwaltung der Verschlüsselungsschlüssel.
- Ihr Unternehmen benötigt die zusätzliche Sicherheit, Authentifizierungsschlüssel auf einem System oder an einem anderen Ort als die Daten zu speichern.

Umfang des externen Schlüsselmanagements

Der Umfang der externen Schlüsselverwaltung bestimmt, ob Schlüsselverwaltungsserver alle SVMs im Cluster oder nur ausgewählte SVMs sichern:

- Sie können einen Clusterbereich verwenden, um die externe Schlüsselverwaltung für alle SVMs im Cluster zu konfigurieren. Der Clusteradministrator hat Zugriff auf alle auf den Servern gespeicherten Schlüssel.
- Ab ONTAP 9.6 kann mithilfe eines SVM-Bereichs die externe Schlüsselverwaltung für eine benannte SVM im Cluster konfiguriert werden. Das ist optimal für mandantenfähige Umgebungen, in denen jeder Mandant eine andere SVM (oder eine Gruppe von SVMs) zur Datenbereitstellung verwendet. Nur der SVM-Administrator eines bestimmten Mandanten hat Zugriff auf die Schlüssel dieses Mandanten.
  - Ab ONTAP 9.17.1 kann Barbican KMS verwendet werden, um NVE-Schlüssel nur für Daten-SVMs zu schützen.
  - Ab ONTAP 9.10.1 kann Azure Key Vault und Google Cloud KMS verwendet werden, um NVE-Schlüssel nur für Daten-SVMs zu schützen. Dies ist für AWS KMS ab 9.12.0 verfügbar.

Beide Bereiche können im selben Cluster verwendet werden. Wenn Schlüsselverwaltungsserver für eine SVM konfiguriert wurden, verwendet ONTAP ausschließlich diese Server zur Sicherung der Schlüssel. Andernfalls sichert ONTAP die Schlüssel mit den für den Cluster konfigurierten Schlüsselverwaltungsservern.

Eine Liste validierter externer Schlüsselmanager ist verfügbar im "NetApp Interoperabilitätsmatrix Tool (IMT)". Diese Liste lässt sich finden, indem der Begriff „key managers“ in die Suchfunktion des IMT eingegeben wird.

Cloud KMS-Anbieter wie Azure Key Vault und AWS KMS unterstützen KMIP nicht. Daher sind sie nicht im IMT aufgeführt.

Supportdetails

Die folgende Tabelle enthält Details zur NVE-Unterstützung:

Ressource oder Funktion	Supportdetails
Plattformen	AES-NI Offload-Funktionalität erforderlich. Im Hardware Universe (HWU) kann überprüft werden, ob NVE und NAE für Ihre Plattform unterstützt werden.

Verschlüsselung	Ab ONTAP 9.7 werden neu erstellte Aggregate und Volumes standardmäßig verschlüsselt, wenn eine Volume-Verschlüsselungslizenz (VE) hinzugefügt und ein interner oder externer Schlüsselmanager konfiguriert ist. Falls ein unverschlüsseltes Aggregat erstellt werden soll, kann folgender Befehl verwendet werden:
	
	`storage aggregate create -encrypt-with-aggr-key false`
	
	Wenn Sie ein Klartext-Volume erstellen müssen, kann folgender Befehl verwendet werden:
	
	`volume create -encrypt false`
	
	Die Verschlüsselung ist nicht standardmäßig aktiviert, wenn:
	
	• Die VE-Lizenz ist nicht installiert.
	• Der Schlüsselmanager ist nicht konfiguriert.
	• Die Plattform oder Software unterstützt keine Verschlüsselung.
	• Die Hardwareverschlüsselung ist aktiviert.

ONTAP	Alle ONTAP Implementierungen. Unterstützung für Cloud Volumes ONTAP ist ab ONTAP 9.5 verfügbar.
Geräte	HDD, SSD, Hybrid, Array LUN.
RAID	RAID0, RAID4, RAID-DP, RAID-TEC.
Volumes	Datenvolumes und vorhandene SVM-Root-Volumes. Daten auf MetroCluster-Metadaten-Volumes können nicht verschlüsselt werden. In Versionen von ONTAP vor 9.14.1 können Daten auf dem SVM-Root-Volume mit NVE nicht verschlüsselt werden. Ab ONTAP 9.14.1 wird ONTAP NVE auf SVM Root-Volumes unterstützt.
Verschlüsselung auf Aggregatebene	Ab ONTAP 9.6 unterstützt NVE die Verschlüsselung auf Aggregatebene (NAE): • Eine Verschlüsselung auf Aggregatebene ist erforderlich, wenn eine Inline- oder Hintergrunddeduplizierung auf Aggregatebene vorgesehen ist. • Ein Volume mit Verschlüsselung auf Aggregatebene kann nicht neu verschlüsselt werden. • Secure-purge wird auf Verschlüsselungs-Volumes auf Aggregatebene nicht unterstützt. • Zusätzlich zu den Datenvolumes unterstützt NAE die Verschlüsselung von SVM-Root-Volumes und des MetroCluster Metadaten-Volumes. NAE unterstützt die Verschlüsselung des Root-Volumes nicht.
SVM-Bereich	MetroCluster wird ab ONTAP 9.8 unterstützt. Ab ONTAP 9.6 unterstützt NVE den SVM-Bereich nur für die externe Schlüsselverwaltung, nicht für den Onboard Key Manager.
Speichereffizienz	Deduplizierung, Komprimierung, Verdichtung, FlexClone. Klone verwenden denselben Schlüssel wie das Elternobjekt, selbst nachdem sie vom Elternobjekt getrennt wurden. Ein `volume move` sollte auf einem geteilten Klon durchgeführt werden, danach verfügt der geteilte Klon über einen anderen Schlüssel.

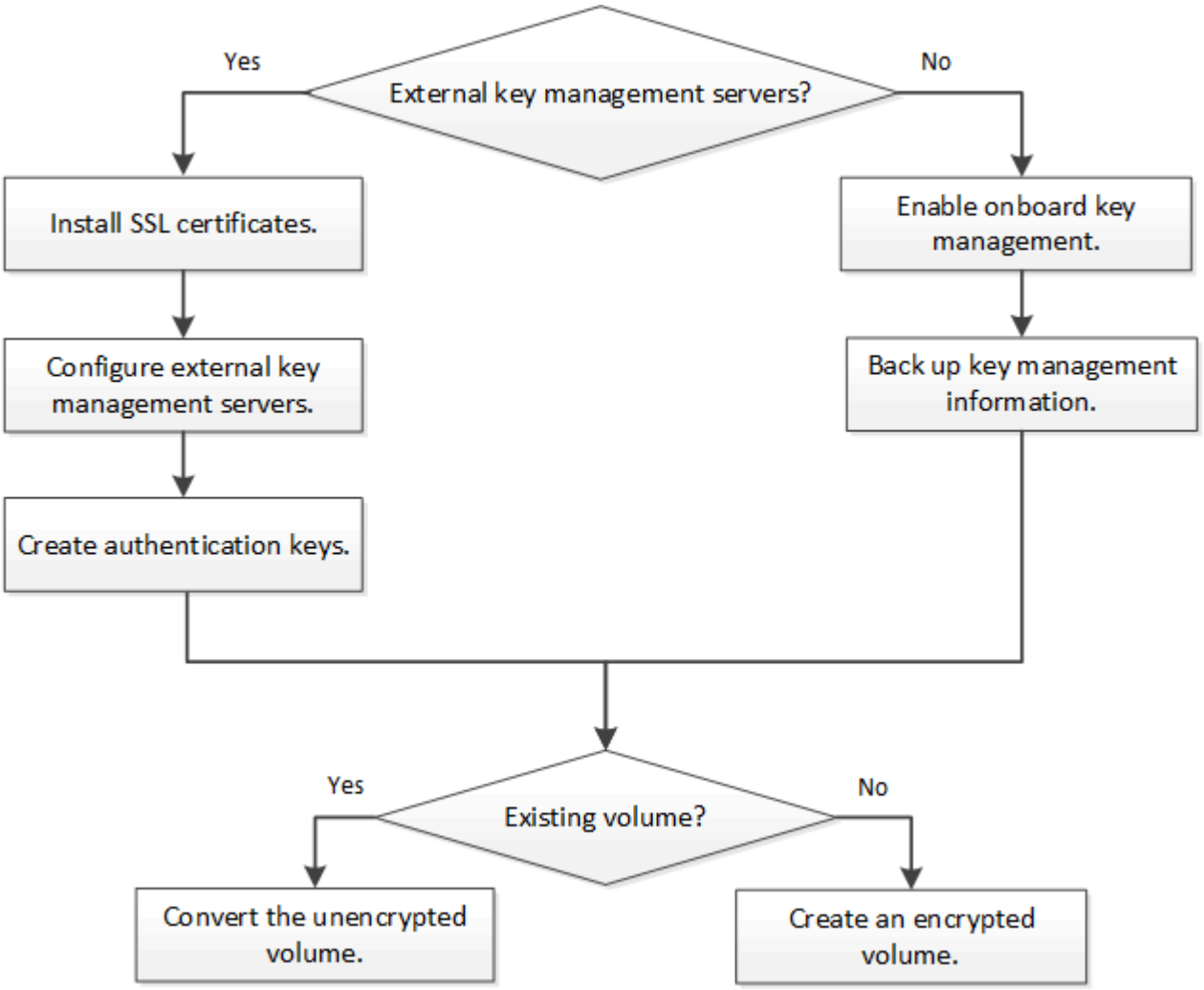
Replication	• Bei der Volume-Replikation können Quell- und Zielvolume unterschiedliche Verschlüsselungseinstellungen aufweisen. Die Verschlüsselung kann für die Quelle konfiguriert und für das Ziel nicht konfiguriert werden, und umgekehrt. Die auf der Quelle konfigurierte Verschlüsselung wird nicht auf das Ziel repliziert. Die Verschlüsselung muss sowohl auf der Quelle als auch auf dem Ziel manuell konfiguriert werden. Siehe NVE konfigurieren und Volumendaten mit NVE verschlüsseln. • Bei der SVM-Replikation wird das Zielvolume automatisch verschlüsselt, es sei denn, das Ziel enthält keinen Knoten, der die Volume-Verschlüsselung unterstützt, in welchem Fall die Replikation erfolgreich ist, das Zielvolume jedoch nicht verschlüsselt wird. • Für MetroCluster Konfigurationen ruft jeder Cluster externe Schlüsselverwaltungsschlüssel von seinen konfigurierten Schlüsselservern ab. OKM-Schlüssel werden vom Konfigurationsreplikationsdienst an den Partnerstandort repliziert.
Einhaltung	SnapLock wird sowohl im Compliance- als auch im Enterprise-Modus unterstützt, jedoch nur für neue Volumes. Die Verschlüsselung kann auf einem bestehenden SnapLock-Volume nicht aktiviert werden.
FlexGroup Volumes	FlexGroup Volumes werden unterstützt. Zielaggregate müssen vom gleichen Typ wie Quellaggregate sein, entweder auf Volume- oder Aggregateebene. Ab ONTAP 9.5 wird die direkte Neuverschlüsselung von FlexGroup Volumes unterstützt.
7-Mode Transition	Ab Version 3.3 des 7-Mode Transition Tool kann die CLI des 7-Mode Transition Tool verwendet werden, um einen kopierbasierten Übergang zu NVE-fähigen Ziel-Volumes auf dem geclusterten System durchzuführen.

Verwandte Informationen

- "Häufig gestellte Fragen – NetApp Volume Encryption und NetApp Aggregate Encryption"
- "Speicheraggregat erstellen"

ONTAP NetApp Volume Encryption-Workflow

Sie müssen die Schlüsselverwaltungsdienste konfigurieren, bevor Sie die Volume-Verschlüsselung aktivieren können. Die Verschlüsselung kann auf einem neuen Volume oder auf einem vorhandenen Volume aktiviert werden.



"Die VE-Lizenz muss installiert werden." und konfigurieren Sie die Schlüsselverwaltungsdienste, bevor Sie Daten mit NVE verschlüsseln können. Vor der Installation der Lizenz sollte "feststellen, ob Ihre ONTAP Version NVE unterstützt" beachtet werden.

NVE konfigurieren

Feststellen, ob Ihre ONTAP Cluster-Version NVE unterstützt

Vor der Installation der Lizenz sollte geprüft werden, ob die Clusterversion NVE unterstützt. Mit dem `version` Befehl lässt sich die Clusterversion ermitteln.

Über diese Aufgabe

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

Schritte

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

   `version -v`

   NVE wird nicht unterstützt, wenn die Befehlsausgabe den Text `1Ono-DARE` (für „no Data At Rest

Encryption“) anzeigt oder wenn Sie eine Plattform verwenden, die nicht in "Supportdetails" aufgeführt ist.

Die Volumenverschlüsselungslizenz auf einem ONTAP Cluster installieren

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

Vor ONTAP One war die VE-Lizenz im Verschlüsselungspaket enthalten. Das Verschlüsselungspaket wird nicht mehr angeboten, ist aber weiterhin gültig. Obwohl es derzeit nicht erforderlich ist, können bestehende Kunden sich dafür entscheiden, "Upgrade auf ONTAP One".

Bevor Sie beginnen

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

Schritte

1. "Es sollte überprüft werden, ob die VE Lizenz installiert ist.".

   Der Name des VE Lizenzpakets ist `VE`.

2. Wenn die Lizenz nicht installiert ist, "System Manager oder die ONTAP Befehlszeilenschnittstelle (CLI) kann zur Installation verwendet werden.".

Externe Schlüsselverwaltung konfigurieren

Informationen zur externen ONTAP Schlüsselverwaltung für NetApp Volume Encryption

Sie können einen oder mehrere externe Schlüsselverwaltungsserver verwenden, um die Schlüssel zu sichern, die der Cluster für den Zugriff auf verschlüsselte Daten verwendet. Ein externer Schlüsselverwaltungsserver ist ein Drittanbietersystem in Ihrer Speicherumgebung, das Schlüssel an Nodes mithilfe des Key Management Interoperability Protocol (KMIP) bereitstellt. Zusätzlich zum integrierten Onboard Key Manager unterstützt ONTAP mehrere externe Schlüsselverwaltungsserver.

Ab ONTAP 9.10.1 kann Azure Key Vault oder Google Cloud Key Manager Service zum Schutz Ihrer NVE-Schlüssel für Daten-SVMs verwendet werden. Ab ONTAP 9.11.1 ist die Konfiguration mehrerer externer Schlüsselmanager in einem Cluster möglich. Siehe Clustered Key-Server konfigurieren. Ab ONTAP 9.12.0 kann "AWS KMS" zum Schutz Ihrer NVE-Schlüssel für Daten-SVMs verwendet werden. Ab ONTAP 9.17.1 kann OpenStacks Barbican KMS zum Schutz Ihrer NVE-Schlüssel für Daten-SVMs verwendet werden.

Ab ONTAP 9.20.1 teilen Knoten in einem Cluster, die einen externen KMIP-Schlüsselmanager verwenden, ihre Verschlüsselungsschlüssel untereinander. Die geteilten Schlüssel werden mit AES-GCM-256 verschlüsselt und authentifiziert. ONTAP teilt Schlüssel in zwei Situationen:

- **Schlüsselerstellung.** Wenn ONTAP einen neuen Schlüssel erstellt, beispielsweise beim Erstellen eines verschlüsselten FlexVol volume, FlexGroup volume oder Aggregats, speichert der Knoten, der den Schlüssel erstellt, diesen auf dem Schlüsselserver und sendet ihn dann an alle anderen Knoten im Cluster.
- **Schlüsselwiederherstellung nach einem Neustart.** Wenn ein Knoten neu startet, beispielsweise im Rahmen eines automatisierten unterbrechungsfreien Upgrade, einer Übernahme und Rückgabe oder eines

ungeplanten Neustarts, stellt er seine Schlüssel von seinem HA-Partner wieder her. ONTAP kontaktiert den Schlüsselserver nur für Schlüssel, die der Partner nicht bereitstellen kann. Verfügt der Partner über alle Schlüssel, kann die Schlüsselwiederherstellung auch dann abgeschlossen werden, wenn der Schlüsselserver nicht verfügbar ist.

Dieses Verhalten wird auf einem neuen ONTAP 9.20.1 Cluster sowie beim Upgrade eines Clusters auf ONTAP 9.20.1 automatisch aktiviert.

Die clusterinterne Schlüsselfreigabe gilt nur für einen externen KMIP Schlüsselmanager. Sie wird nicht mit dem Onboard Key Manager, Azure Key Vault, Google Cloud Key Management Service, AWS KMS oder Barbican verwendet. Sie wird nicht verwendet, wenn MetroCluster konfiguriert ist. Die Wiederherstellung der Schlüssel nach einem Neustart erfordert, dass der HA Partner online ist und die Schlüssel selbst besitzt.

Externe Key Manager mit ONTAP System Manager verwalten

Ab ONTAP 9.7 können Authentifizierungs- und Verschlüsselungsschlüssel mit dem Onboard Key Manager gespeichert und verwaltet werden. Ab ONTAP 9.13.1 ist es außerdem möglich, diese Schlüssel mit externen Key Managern zu speichern und zu verwalten.

Der Onboard Key Manager speichert und verwaltet Schlüssel in einer sicheren Datenbank, die intern im Cluster liegt. Sein Gültigkeitsbereich ist der Cluster. Ein externer Key Manager speichert und verwaltet Schlüssel außerhalb des Clusters. Sein Gültigkeitsbereich kann der Cluster oder die Storage-VM sein.

Über diese Aufgabe

Sie müssen die ONTAP Befehlszeilenschnittstelle (CLI) verwenden, um externe Schlüsselmanager für MetroCluster-Konfigurationen zu konfigurieren. Informationen dazu "Konfiguration der externen Schlüsselverwaltung von ONTAP über die Befehlszeile".

Es können ein oder mehrere externe Schlüsselmanager eingesetzt werden. Die folgenden Bedingungen gelten:

- Wenn der Onboard Key Manager aktiviert ist, kann ein externer Key Manager auf Clusterebene nicht aktiviert werden, wohl aber auf Storage-VM-Ebene.
- Wenn auf Clusterebene ein externer Schlüsselmanager aktiviert ist, kann der Onboard Key Manager nicht aktiviert werden.

Bei Verwendung externer Schlüsselmanager können bis zu vier primäre Schlüsselserver pro Storage-VM und Cluster registriert werden. Jeder primäre Schlüsselserver kann mit bis zu drei sekundären Schlüsselservern in einem Cluster verbunden werden.

Einen externen Schlüsselmanager konfigurieren

Um einen externen Schlüsselmanager für eine Storage-VM hinzuzufügen, sollte beim Konfigurieren der Netzwerkschnittstelle für die Storage-VM ein optionales Gateway hinzugefügt werden. Falls die Storage-VM ohne die Netzwerkrouten erstellt wurde, muss die Route explizit für den externen Schlüsselmanager erstellt werden. Siehe "Eine LIF (Netzwerkschnittstelle) erstellen".

Schritte

Ein externer Schlüsselmanager kann im System Manager von verschiedenen Ausgangspunkten aus konfiguriert werden.

1. Um einen externen Schlüsselmanager zu konfigurieren, ist einer der folgenden ersten Schritte erforderlich.

Workflow	Navigation	Startschritt
Schlüsselmanager konfigurieren	**Cluster** > **Einstellungen**	Zum Abschnitt **Sicherheit** scrollen. Unter **Verschlüsselung** auswählen. **Externe Schlüsselverwaltung** auswählen.
Lokale Ebene hinzufügen	**Speicher** > **Ebenen**	**+ Lokale Ebene hinzufügen** auswählen. Das Kästchen mit der Bezeichnung „Schlüsselmanager konfigurieren“ aktivieren. **Externe Schlüsselverwaltung** auswählen.
Storage vorbereiten	**Dashboard**	Im Abschnitt **Kapazität** die Option **Speicher vorbereiten** auswählen. Anschließend „Schlüsselverwaltung konfigurieren“ auswählen. **Externe Schlüsselverwaltung** auswählen.
Verschlüsselung konfigurieren (Key Manager nur im Storage-VM-Bereich)	**Speicher** > **Storage VMs**	Die Storage-VM auswählen. Die Registerkarte **Einstellungen** auswählen. Im Abschnitt **Verschlüsselung** unter **Sicherheit** auswählen.

2. Um einen Primärschlüsselserver hinzuzufügen, + Add auswählen und die Felder **IP-Adresse oder Hostname** sowie **Port** ausfüllen.
3. Die vorhandenen installierten Zertifikate werden in den Feldern **KMIP Server CA Certificates** und **KMIP Client Certificate** aufgelistet. Folgende Aktionen sind möglich:
   - Wählen Sie aus, um die installierten Zertifikate auszuwählen, die Sie dem Schlüsselmanager zuordnen möchten. (Es können mehrere Dienst-CA-Zertifikate ausgewählt werden, aber nur ein Clientzertifikat.)
   - **Neues Zertifikat hinzufügen** auswählen, um ein noch nicht installiertes Zertifikat hinzuzufügen und es dem externen Schlüsselmanager zuzuordnen.
   - Wählen Sie × neben dem Zertifikatsnamen die Option zum Löschen installierter Zertifikate, die Sie nicht dem externen Schlüsselmanager zuordnen möchten.
4. Um einen sekundären Schlüsselserver hinzuzufügen, in der Spalte **Sekundäre Schlüsselserver Hinzufügen** auswählen und die entsprechenden Details angeben.
5. **Speichern** auswählen, um die Konfiguration abzuschließen.

Einen vorhandenen externen Schlüsselmanager bearbeiten

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

Schritte

1. Um die Konfiguration eines externen Schlüsselmanagers zu bearbeiten, kann einer der folgenden ersten Schritte durchgeführt werden.

Umfang	Navigation	Startschritt
Externer Schlüsselmanager auf Clusterebene	**Cluster** > **Einstellungen**	Zum Abschnitt **Sicherheit** scrollen. Unter **Verschlüsselung** auswählen und dann **Externen Schlüsselmanager bearbeiten** wählen.

Externer Schlüsselmanager für den Storage-VM-Bereich	**Speicher** > **Storage VMs**	Die Storage-VM auswählen. Die Registerkarte **Einstellungen** auswählen. Im Abschnitt **Verschlüsselung** unter **Sicherheit** ⋮ die Option **Externen Schlüsselmanager bearbeiten** auswählen.

2. Vorhandene Schlüsselserver sind in der Tabelle **Key Servers** aufgelistet. Folgende Vorgänge sind möglich:
   - Fügen Sie einen neuen Schlüsselserver hinzu, indem Sie + Add auswählen.
   - Löschen Sie einen Schlüsselserver, indem Sie ⋮ am Ende der Tabellenzelle auswählen, die den Namen des Schlüsselservers enthält. Die mit diesem primären Schlüsselserver verknüpften sekundären Schlüsselserver werden ebenfalls aus der Konfiguration entfernt.

Externen Schlüsselmanager löschen

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

Schritte

1. Um einen externen Schlüsselmanager zu löschen, kann einer der folgenden Schritte durchgeführt werden.

Umfang	Navigation	Startschritt
Externer Schlüsselmanager auf Clusterebene	**Cluster** > **Einstellungen**	Zum Abschnitt **Sicherheit** scrollen. Unter **Verschlüsselung** ⋮ auswählen und dann **Externen Schlüsselmanager löschen** wählen.
Externer Schlüsselmanager für den Storage-VM-Bereich	**Speicher** > **Storage VMs**	Die Storage-VM auswählen. Die Registerkarte **Einstellungen** auswählen. Im Abschnitt **Verschlüsselung** unter **Sicherheit** ⋮ dann **Externen Schlüsselmanager löschen** auswählen.

Schlüssel zwischen Schlüsselmanagern migrieren

Ab ONTAP 9.20.1 migriert ONTAP beim Aktivieren eines externen Schlüsselmanagers auf einer Daten-SVM über System Manager automatisch alle Volume-Verschlüsselungsschlüssel, die vom Schlüsselmanager im Admin-Bereich verwaltet werden, zum neuen Daten-SVM-Schlüsselmanager. In den meisten Fällen ist kein separater Migrationsschritt erforderlich.

Diese automatische Migration ist Teil des Aktivierungsvorgangs. Wenn der Vorgang fehlschlägt, wiederholt ONTAP den Vorgang und setzt die Konfiguration zurück, falls ein nicht behebbarer Fehler auftritt.

Dieser vereinfachte Workflow gilt für Daten-SVMs. Wenn Sie die Admin-SVM (Clusterbereich) von der integrierten Schlüsselverwaltung auf einen externen Schlüsselmanager umstellen, müssen Sie die integrierte Schlüsselverwaltung deaktivieren, bevor Sie die externe Schlüsselverwaltung aktivieren.

SSL-Zertifikate auf dem ONTAP Cluster installieren

Der Cluster und der KMIP-Server verwenden KMIP-SSL-Zertifikate, um gegenseitig die Identität zu verifizieren und eine SSL-Verbindung herzustellen. Vor der Konfiguration der SSL-Verbindung mit dem KMIP-Server müssen die KMIP-Client-SSL-Zertifikate für den Cluster sowie das öffentliche SSL-Zertifikat für die Root-Zertifizierungsstelle (CA) des KMIP-Servers installiert werden.

Über diese Aufgabe

In einem HA-Paar müssen beide Knoten dieselben öffentlichen und privaten KMIP-SSL-Zertifikate verwenden. Wenn mehrere HA-Paare mit demselben KMIP-Server verbunden sind, müssen alle Knoten in den HA-Paaren dieselben öffentlichen und privaten KMIP-SSL-Zertifikate verwenden.

Bevor Sie beginnen

- Die Zeit muss auf dem Server, der die Zertifikate erstellt, dem KMIP Server und dem Cluster synchronisiert sein.
- Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.
- Das öffentliche SSL KMIP-Clientzertifikat für den Cluster muss vorliegen.
- Der private Schlüssel, der dem SSL KMIP Clientzertifikat für den Cluster zugeordnet ist, muss vorliegen.
- Das SSL KMIP-Clientzertifikat darf nicht passwortgeschützt sein.
- Das öffentliche SSL-Zertifikat für die Stammzertifizierungsstelle (CA) des KMIP-Servers muss vorliegen.
- In einer MetroCluster Umgebung müssen auf beiden Clustern die gleichen KMIP SSL-Zertifikate installiert werden.

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

`admin_SVM` ist die Admin-SVM für den Cluster. In den folgenden Beispielen heißt die Admin-SVM `cluster1`, daher erscheint `cluster1` sowohl in der Eingabeaufforderung (`cluster1::>`) als auch als Wert für `-vserver`.

Schritte

1. Die SSL-KMIP-Clientzertifikate für den Cluster installieren:

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

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

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

2. Das öffentliche SSL-Zertifikat für die Root-Zertifizierungsstelle (CA) des KMIP-Servers installieren:

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

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

Verwandte Informationen

- "Sicherheitszertifikat installieren"

Externe Schlüsselverwaltung für NVE in ONTAP 9.6 und höher aktivieren

KMIP-Server dienen der Sicherung der Schlüssel, die der Cluster für den Zugriff auf verschlüsselte Daten verwendet. Ab ONTAP 9.6 besteht die Möglichkeit, einen separaten externen Schlüsselmanager zu konfigurieren, um die Schlüssel zu sichern, die eine Daten-SVM für den Zugriff auf verschlüsselte Daten verwendet.

Ab ONTAP 9.11.1 können bis zu 3 sekundäre Schlüsselserver pro primärem Schlüsselserver hinzugefügt werden, um einen gruppierten Schlüsselserver zu erstellen. Weitere Informationen finden sich unter Clustered

externe Schlüsselserver konfigurieren.

Über diese Aufgabe

Sie können bis zu vier KMIP-Server an einen Cluster oder eine SVM anschließen. Mindestens zwei Server sollten für Redundanz und Notfallwiederherstellung eingesetzt werden.

Der Umfang der externen Schlüsselverwaltung bestimmt, ob Schlüsselverwaltungsserver alle SVMs im Cluster oder nur ausgewählte SVMs sichern:

- Sie können einen Clusterbereich verwenden, um die externe Schlüsselverwaltung für alle SVMs im Cluster zu konfigurieren. Der Clusteradministrator hat Zugriff auf alle auf den Servern gespeicherten Schlüssel.
- Ab ONTAP 9.6 kann ein SVM-Bereich verwendet werden, um die externe Schlüsselverwaltung für eine Daten-SVM im Cluster zu konfigurieren. Das ist optimal für mandantenfähige Umgebungen, in denen jeder Mandant eine andere SVM (oder eine Gruppe von SVMs) zur Datenbereitstellung verwendet. Nur der SVM-Administrator eines bestimmten Mandanten hat Zugriff auf die Schlüssel dieses Mandanten.
- Für mandantenfähige Umgebungen ist eine Lizenz für *MT_EK_MGMT* mit folgendem Befehl zu installieren:

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

  Weitere Informationen zu `system license add` finden sich in der "ONTAP-Befehlsreferenz".

Beide Bereiche können im selben Cluster verwendet werden. Wenn Schlüsselverwaltungsserver für eine SVM konfiguriert wurden, verwendet ONTAP ausschließlich diese Server zur Sicherung der Schlüssel. Andernfalls sichert ONTAP die Schlüssel mit den für den Cluster konfigurierten Schlüsselverwaltungsservern.

Sie können die Onboard-Schlüsselverwaltung auf Clusterebene und die externe Schlüsselverwaltung auf SVM-Ebene konfigurieren. Sie können den `security key-manager key migrate` Befehl verwenden, um Schlüssel von der Onboard-Schlüsselverwaltung auf Clusterebene zu externen Schlüsselverwaltungen auf SVM-Ebene zu migrieren.

Weitere Informationen zu `security key-manager key migrate` finden sich in der "ONTAP-Befehlsreferenz".

> Ab ONTAP 9.20.1 kann ONTAP beim Konfigurieren eines externen Schlüsselmanagers auf einer Daten-SVM alle NVE-Schlüssel, die derzeit vom Schlüsselmanager im Admin-Bereich verwaltet werden, automatisch migrieren. In diesem Workflow ist kein separater `security key-manager key migrate`Befehl erforderlich.
>
> Wenn die Daten-SVM bereits verschlüsselte Volumes enthält, migriert ONTAP die Schlüssel im Rahmen des Aktivierungsvorgangs. Der Keystore wechselt direkt von inaktiv zu aktiv, ohne dass ein separater Migrationsschritt erforderlich ist.
>
> Dieser Workflow wird nur für Daten-SVMs unterstützt. Er wird nicht für die Admin-SVM (Clusterbereich) unterstützt.

Bevor Sie beginnen

- Die KMIP SSL-Client- und Serverzertifikate müssen installiert sein.
- Der KMIP-Server muss von jedem Node-Management-LIF aus erreichbar sein.
- Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.
- In einer MetroCluster Umgebung:
  - MetroCluster muss vollständig konfiguriert sein, bevor die externe Schlüsselverwaltung aktiviert werden

kann.

- Auf beiden Clustern ist dasselbe KMIP SSL-Zertifikat zu installieren.
- Auf beiden Clustern muss ein externer Schlüsselmanager konfiguriert werden.

Schritte

1. Die Key-Manager-Konnektivität für den Cluster konfigurieren:

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

> Der `security key-manager external enable` Befehl ersetzt ab ONTAP 9.6 den `security key-manager setup` Befehl. Wenn Sie den Befehl an der Cluster-Anmeldeaufforderung ausführen, ist *`admin_SVM`* standardmäßig die admin SVM des aktuellen Clusters. Mit dem `security key-manager external modify` Befehl lässt sich die Konfiguration der externen Schlüsselverwaltung ändern.

Der folgende Befehl aktiviert die externe Schlüsselverwaltung für `cluster1` mit drei externen Schlüsselservern. Der erste Schlüsselserver wird über seinen Hostnamen und Port angegeben, der zweite über eine IP-Adresse und den Standardport, und der dritte über eine IPv6-Adresse und den 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. Konfigurieren eines Schlüsselmanagers für eine 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 der Befehl an der SVM-Anmeldeaufforderung ausgeführt wird, `SVM` gilt standardmäßig die aktuelle SVM. Der `security key-manager external modify` Befehl kann verwendet werden, um die Konfiguration der externen Schlüsselverwaltung zu ändern.
> - In einer MetroCluster-Umgebung ist es bei der Konfiguration der externen Schlüsselverwaltung für eine Daten-SVM nicht erforderlich, den `security key-manager external enable` Befehl auf dem Partnercluster zu wiederholen.

Der folgende Befehl aktiviert die externe Schlüsselverwaltung für `svm1` einen einzelnen Schlüsselserver, der auf dem Standardport 5696 lauscht:

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

```
SVM1ServerCaCert
```

3. Den letzten Schritt für alle weiteren SVMs wiederholen.

> Sie können auch den `security key-manager external add-servers` Befehl verwenden, um zusätzliche SVMs zu konfigurieren. Der `security key-manager external add-servers` Befehl ersetzt ab ONTAP 9.6 den `security key-manager add` Befehl. Weitere Informationen zu `security key-manager external add-servers` sind in der "ONTAP-Befehlsreferenz" verfügbar.

4. Es wird überprüft, ob alle konfigurierten KMIP-Server verbunden sind:

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

> Ab ONTAP 9.6 ersetzt der `security key-manager external show-status` Befehl den `security key-manager show -status` Befehl. Weitere Informationen zu `security key-manager external show-status` sind in der "ONTAP-Befehlsreferenz" verfügbar.

```
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. Optional können Klartext-Volumes in verschlüsselte Volumes umgewandelt werden.

```
volume encryption conversion start
```

Vor der Konvertierung der Volumes muss ein externer Schlüsselmanager vollständig konfiguriert sein.

Verwandte Informationen

- Clustered externe Schlüsselserver konfigurieren
- "system license add"
- "security key-manager key migrate"
- "security key-manager external add-servers"
- "security key-manager external show-status"

Externe Schlüsselverwaltung für NVE in ONTAP 9.5 und früher aktivieren

Sie können einen oder mehrere KMIP-Server verwenden, um die Schlüssel zu sichern, die der Cluster für den Zugriff auf verschlüsselte Daten verwendet. Sie können bis zu vier KMIP-Server mit einem Knoten verbinden. Für Redundanz und Notfallwiederherstellung werden mindestens zwei Server empfohlen.

Über diese Aufgabe

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

Bevor Sie beginnen

- Die KMIP SSL-Client- und Serverzertifikate müssen installiert sein.
- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Die MetroCluster Umgebung muss konfiguriert werden, bevor ein externer Schlüsselmanager konfiguriert wird.
- In einer MetroCluster Umgebung muss auf beiden Clustern dasselbe KMIP SSL-Zertifikat installiert werden.

Schritte

1. Konfiguration der Key-Manager-Konnektivität für Clusterknoten:

   `security key-manager setup`

   Die Einrichtung des Schlüsselmanagers beginnt.

   In einer MetroCluster Umgebung muss dieser Befehl auf beiden Clustern ausgeführt werden. Weitere Informationen zu `security key-manager setup` finden sich in der "ONTAP-Befehlsreferenz".

2. Geben Sie bei jeder Eingabeaufforderung die entsprechende Antwort ein.
3. Einen KMIP-Server hinzufügen:

   `security key-manager add -address key_management_server_ipaddress`

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

   In einer MetroCluster Umgebung muss dieser Befehl auf beiden Clustern ausgeführt werden.

4. Einen zusätzlichen KMIP Server für Redundanz hinzufügen:

   `security key-manager add -address key_management_server_ipaddress`

   ```
   cluster1::> security key-manager add -address 20.1.1.2
   ```

   In einer MetroCluster Umgebung muss dieser Befehl auf beiden Clustern ausgeführt werden.

5. Es wird überprüft, ob alle konfigurierten KMIP-Server verbunden sind:

   `security key-manager show -status`

   Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

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

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

6. Optional können Klartext-Volumes in verschlüsselte Volumes umgewandelt werden.

   `volume encryption conversion start`

   Vor der Konvertierung der Volumes muss ein externer Schlüsselmanager vollständig konfiguriert sein. In einer MetroCluster-Umgebung muss ein externer Schlüsselmanager an beiden Standorten konfiguriert sein.

NVE-Schlüssel für ONTAP Daten-SVMs mit einem Cloud-Anbieter verwalten

Ab ONTAP 9.10.1 können "Azure Key Vault (AKV)" und "Key Management Service (Cloud KMS) der Google Cloud Platform" verwendet werden, um Ihre ONTAP-Verschlüsselungsschlüssel in einer cloudbasierten Anwendung zu schützen. Ab ONTAP 9.12.0 können auch NVE-Schlüssel mit "AWS KMS" geschützt werden.

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

Ab ONTAP 9.20.1 migriert ONTAP beim Aktivieren eines Cloud Key Managers auf einer Daten-SVM, die bereits verschlüsselte Volumes über den Key Manager im Admin-Bereich verwaltet, diese NVE-Schlüssel automatisch zum neuen Daten-SVM Key Manager. In diesem Workflow ist kein separater `security key-manager key migrate` Befehl erforderlich.

> Diese automatische Migration gilt für Daten-SVMs. Beim Umstellen der Admin SVM von der integrierten Schlüsselverwaltung oder der externen Schlüsselverwaltung mit Cluster-Scope auf einen Cloud-Schlüsselmanager für Daten-SVMs müssen zunächst die entsprechenden Übergangsaufgaben für den Admin-Bereich abgeschlossen werden.

Über diese Aufgabe

Die Schlüsselverwaltung mit einem Cloud-Anbieter lässt sich mit der CLI oder der ONTAP REST API aktivieren.

Wenn ein Cloud-Anbieter zum Schutz Ihrer Schlüssel verwendet wird, ist zu beachten, dass standardmäßig eine Daten-SVM-LIF für die Kommunikation mit dem Cloud-Schlüsselverwaltungsendpunkt verwendet wird. Ein Knotenverwaltungsnetzwerk wird für die Kommunikation mit den Authentifizierungsdiensten des Cloud-Anbieters verwendet (login.microsoftonline.com für Azure; oauth2.googleapis.com für Cloud KMS). Wenn das Clusternetzwerk nicht korrekt konfiguriert ist, kann der Cluster den Schlüsselverwaltungsdienst nicht ordnungsgemäß nutzen.

Bei der Nutzung eines Schlüsselverwaltungsdienstes eines Cloud-Anbieters sind die folgenden Einschränkungen zu beachten:

- Die Schlüsselverwaltung des Cloud-Anbieters ist für NetApp Storage Encryption (NSE) und NetApp Aggregate Encryption (NAE) nicht verfügbar. "Externe KMIPs" kann stattdessen verwendet werden.
- Die Schlüsselverwaltung durch den Cloud-Anbieter ist für MetroCluster Konfigurationen nicht verfügbar.
- Die Schlüsselverwaltung des Cloud-Anbieters kann nur auf einer Daten-SVM konfiguriert werden.

Bevor Sie beginnen

- Das KMS muss beim entsprechenden Cloud-Anbieter konfiguriert sein.
- Die ONTAP Cluster-Knoten müssen NVE unterstützen.
- "Die Lizenzen für Volume Encryption (VE) und Multi-Tenant Encryption Key Management (MTEKM) müssen installiert sein.". Diese Lizenzen sind im Preis inbegriffen "ONTAP One".
- Sie müssen Cluster- oder SVM-Administrator sein.
- Für ONTAP 9.20.1 und höher kann eine Daten-SVM verschlüsselte Volumes enthalten, sofern deren NVE-Schlüssel vom Schlüsselmanager mit Administratorbereich verwaltet werden. ONTAP migriert diese Schlüssel während des Aktivierungsvorgangs automatisch. Bei früheren Releases sind die Schlüssel vor der Konfiguration des Cloud-Schlüsselmanagers zu migrieren.

Externe Schlüsselverwaltung aktivieren

Die Aktivierung der externen Schlüsselverwaltung hängt vom verwendeten Schlüsselverwaltungsprogramm ab. Die Registerkarte des entsprechenden Schlüsselverwaltungsprogramms und der zugehörigen Umgebung ist auszuwählen.

AWS

Bevor Sie beginnen

- Sie müssen eine Berechtigung für den AWS KMS-Schlüssel erstellen, der von der IAM-Rolle zur Verwaltung der Verschlüsselung verwendet wird. Die IAM-Rolle muss eine Richtlinie enthalten, die die folgenden Operationen zulässt:
  - `DescribeKey`
  - `Encrypt`

- Decrypt

  Weitere Informationen enthält die AWS-Dokumentation zu "Berechtigungen".

AWS KMV auf einer ONTAP SVM aktivieren

1. Bevor Sie beginnen, sowohl die Zugriffsschlüssel-ID als auch den geheimen Schlüssel von Ihrem AWS KMS bereithalten.
2. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `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. Bei Aufforderung ist der geheime Schlüssel einzugeben.
5. Es wird bestätigt, dass AWS KMS korrekt konfiguriert wurde: `security key-manager external aws show -vserver svm_name`

   Weitere Informationen zu `security key-manager external aws` finden sich in der "ONTAP-Befehlsreferenz".

Azure

Azure Key Vault auf einer ONTAP SVM aktivieren

1. Bevor Sie beginnen, müssen Sie die entsprechenden Authentifizierungsdaten von Ihrem Azure-Konto erhalten, entweder ein Clientgeheimnis oder ein Zertifikat. Es muss außerdem sichergestellt sein, dass alle Knoten im Cluster fehlerfrei funktionieren. Dies lässt sich mit dem Befehl `cluster show` überprüfen. Weitere Informationen zu `cluster show` finden sich in der "ONTAP-Befehlsreferenz".
2. Berechtigungsstufe auf „Fortgeschritten“ setzen `set -priv advanced`
3. AKV auf der SVM aktivieren. Ab ONTAP 9.19.1 wird verwendet: `security key-manager external azure create-config -config-name config_name -client-id client_id -tenant-id tenant_id -name URL -key-id key_id -authentication-method {certificate|client-secret} -vserver vserver_name` gefolgt von: `security key-manager keystore enable -vserver vserver_name -keystore-type AKV -config -name config_name` Für ONTAP 9.18.1 und früher wird verwendet: `security key-manager external azure enable -client-id client_id -tenant-id tenant_id -name name -key-id key_id -authentication-method {certificate|client-secret} -vserver vserver_name` Bei entsprechender Aufforderung ist entweder das Clientzertifikat oder das Clientgeheimnis aus dem Azure-Konto einzugeben.
4. Es sollte überprüft werden, ob AKV korrekt aktiviert ist: `security key-manager external azure show vserver svm_name` Ist die Erreichbarkeit des Dienstes nicht in Ordnung, wird die Konnektivität zum AKV Key Management Service über die Daten-SVM-LIF hergestellt.

   Weitere Informationen zu `security key-manager external azure` finden sich in der "ONTAP-Befehlsreferenz".

Google Cloud

Cloud KMS auf einer ONTAP SVM aktivieren

1. Bevor Sie beginnen, den privaten Schlüssel für die Google Cloud KMS Kontoschlüsseldatei im JSON-Format beschaffen. Dieser befindet sich in Ihrem GCP-Konto. Es muss außerdem sichergestellt sein, dass alle Knoten im Cluster fehlerfrei funktionieren. Dies lässt sich mit dem Befehl `cluster show` überprüfen. Weitere Informationen zu `cluster show` finden sich in der "ONTAP-Befehlsreferenz".
2. Berechtigungsstufe auf „Erweitert“ setzen: `set -priv advanced`

3. Cloud KMS auf der SVM aktivieren `security key-manager external gcp enable -vserver svm_name -project-id project_id-key-ring-name key_ring_name -key -ring-location key_ring_location -key-name key_name` Bei Aufforderung den Inhalt der JSON-Datei mit dem Service Account Private Key eingeben
4. Es sollte überprüft werden, ob 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 `"UNKNOWN"` sein, wenn keine verschlüsselten Volumes erstellt wurden. Ist die Erreichbarkeit des Dienstes nicht gegeben, sollte die Konnektivität zum GCP Key Management Service über die Daten-SVM-LIF hergestellt werden.

   Weitere Informationen zu `security key-manager external gcp` finden sich in der "ONTAP-Befehlsreferenz".

Ab ONTAP 9.20.1 migriert ONTAP diese Schlüssel während des Aktivierungsvorgangs automatisch, wenn für eine Daten-SVM bereits ein oder mehrere verschlüsselte Volumes konfiguriert sind und die entsprechenden NVE-Schlüssel vom admin-scope key manager verwaltet werden. Ein separater `security key-manager key migrate`Befehl ist nicht erforderlich.

Bei ONTAP Releases vor 9.20.1 sollten diese Schlüssel zum externen Schlüsselverwaltungsdienst migriert werden. Dies lässt sich mit der CLI mit folgendem Befehl durchführen: `security key-manager key migrate -from-Vserver admin_SVM -to-Vserver data_SVM`

Neue verschlüsselte Volumes können für die Daten-SVM des Mandanten erst erstellt werden, wenn alle NVE-Schlüssel der Daten-SVM erfolgreich migriert wurden.

Verwandte Informationen

- "Verschlüsselung von Volumes mit NetApp Verschlüsselungslösungen für Cloud Volumes ONTAP"
- "security key-manager external"

ONTAP-Schlüssel mit Barbican KMS verwalten

Ab ONTAP 9.17.1 kann OpenStack"Barbican KMS" verwendet werden, um ONTAP-Verschlüsselungsschlüssel zu schützen. Barbican KMS ist ein Dienst zum sicheren Speichern und Zugreifen auf Schlüssel. Barbican KMS kann zum Schutz von NetApp Volume Encryption (NVE)-Schlüsseln für Daten-SVMs verwendet werden. Barbican nutzt "OpenStack Keystone", den Identitätsdienst von OpenStack, zur Authentifizierung.

Über diese Aufgabe

Die Schlüsselverwaltung mit Barbican KMS kann über die Befehlszeilenschnittstelle (CLI) oder die ONTAP REST API konfiguriert werden. Mit der Version 9.17.1 weist die Barbican KMS Unterstützung folgende Einschränkungen auf:

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

Sofern nicht anders angegeben, können Administratoren auf der `admin`Berechtigungsstufe die folgenden Verfahren durchführen.

Bevor Sie beginnen

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

Erstellen und Aktivieren einer Barbican KMS Konfiguration

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

Schritte

1. Eine neue inaktive Barbican KMS Konfiguration für eine SVM erstellen:

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

   - `-key-id` ist der Schlüsselbezeichner des Barbican Key Encryption Key (KEK). Eine vollständige URL, einschließlich `https://`.

     Manche URLs enthalten das Fragezeichen (?). Das Fragezeichen aktiviert die aktive Hilfe der ONTAP-Befehlszeile. Um eine URL mit einem Fragezeichen einzugeben, müssen Sie die aktive Hilfe zunächst mit dem Befehl `set -active-help false` deaktivieren. Sie können die aktive Hilfe später mit dem Befehl `set -active-help true` wieder aktivieren. Weitere Informationen befinden sich in der "ONTAP-Befehlsreferenz".

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

     Nach Eingabe dieses Befehls werden Sie zur Eingabe des geheimen Anwendungsschlüssels aufgefordert. Dieser Befehl erstellt eine inaktive Barbican KMS Konfiguration.

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

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

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

2. Die neue Barbican KMS Konfiguration wird aktiviert:

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

Mit diesem Befehl können Sie zwischen Barbican KMS Konfigurationen wechseln. Falls bereits eine Barbican KMS Konfiguration auf der SVM aktiv ist, wird diese inaktiv gesetzt und die neue Konfiguration aktiviert.

3. Es wird überprüft, ob die neue Barbican KMS Konfiguration aktiv ist:

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

Dieser Befehl liefert den Status der aktiven Barbican KMS-Konfiguration auf der SVM oder dem Node. Wenn die SVM `svm1` auf dem Node `node1` über eine aktive Barbican KMS-Konfiguration verfügt, wird mit dem folgenden Befehl der Status dieser Konfiguration angezeigt:

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

Vserver: svm1
Node: node1

Category: service_reachability
              Status: OK

Category: kms_wrapped_key_status
              Status: OK
```

Die Anmeldeinformationen und Einstellungen einer Barbican KMS Konfiguration aktualisieren

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

Schritte

1. Die aktuellen Barbican KMS Konfigurationen für eine SVM anzeigen:

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

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

2. Die Einstellungen einer Barbican KMS Konfiguration aktualisieren:

```
security key-manager external barbican update-config -vserver <svm_name>
```

```
-config-name <unique_config_name> -timeout <timeout> -verify
<true|false> -verify-host <true|false>
```

Dieser Befehl aktualisiert die Zeitüberschreitung und Verifizierungseinstellungen der angegebenen Barbican KMS-Konfiguration. `timeout` Legt fest, wie viele Sekunden ONTAP auf eine Antwort von Barbican wartet, bevor die Verbindung fehlschlägt. Der Standardwert `timeout` beträgt zehn Sekunden. `verify` und `verify-host` legen fest, ob die Identität bzw. der Hostname des Barbican-Hosts vor der Verbindung überprüft werden sollen. Standardmäßig sind diese Parameter auf `true` gesetzt. Die `vserver` und `config-name` Parameter sind erforderlich. Die übrigen Parameter sind optional.

3. Bei Bedarf können die Zugangsdaten einer aktiven oder inaktiven Barbican KMS Konfiguration aktualisiert werden:

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

Nach Eingabe dieses Befehls erfolgt eine Aufforderung zur Eingabe des neuen geheimen Anwendungsschlüssels für die Anmeldeinformationen.

4. Falls erforderlich, einen fehlenden SVM-Schlüsselverschlüsselungsschlüssel (KEK) für eine aktive Barbican KMS-Konfiguration wiederherstellen:
   a. Einen fehlenden SVM KEK wiederherstellen mit `security key-manager external barbican restore`:

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

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

5. Bei Bedarf sollte der SVM KEK für eine Barbican KMS Konfiguration neu verschlüsselt werden:
   a. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

```
set -privilege advanced
```

   b. Den SVM KEK neu verschlüsseln mit `security key-manager external barbican rekey-internal`:

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

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

Schlüssel zwischen Barbican KMS und dem Onboard Key Manager migrieren

Sie können Schlüssel vom Barbican KMS zum Onboard Key Manager (OKM) migrieren und umgekehrt. Weitere Informationen zum OKM sind unter "Integrierte Schlüsselverwaltung in ONTAP 9.6 und höher aktivieren" verfügbar.

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

```
set -privilege advanced
```

2. Falls erforderlich, können Schlüssel vom Barbican KMS zum OKM migriert werden:

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

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

3. Falls erforderlich, können Schlüssel vom OKM zum Barbican KMS migriert werden:

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

Deaktivieren und Löschen einer Barbican KMS Konfiguration

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

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

```
set -privilege advanced
```

2. Eine aktive Barbican KMS Konfiguration deaktivieren:

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

Falls auf der SVM NVE-verschlüsselte Volumes vorhanden sind, müssen Sie diese entschlüsseln oder die Schlüssel migrieren bevor die Barbican KMS-Konfiguration deaktiviert wird. Die Aktivierung einer neuen Barbican KMS-Konfiguration erfordert weder die Entschlüsselung von NVE-Volumes noch die Migration von Schlüsseln und deaktiviert die aktuell aktive Barbican KMS-Konfiguration.

3. Eine inaktive Barbican KMS Konfiguration löschen:

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

Integrierte Schlüsselverwaltung für NVE in ONTAP 9.6 und höher aktivieren

Mit dem Onboard Key Manager können Sie die Schlüssel sichern, die der Cluster für den Zugriff auf verschlüsselte Daten verwendet. Der Onboard Key Manager muss auf jedem Cluster aktiviert werden, der auf ein verschlüsseltes Volume oder eine selbstverschlüsselnde Festplatte zugreift.

Über diese Aufgabe

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

Wenn Sie eine MetroCluster Konfiguration haben, muss der `security key-manager onboard enable` Befehl zuerst auf dem lokalen Cluster ausgeführt werden, danach der `security key-manager onboard sync` Befehl auf dem Remote-Cluster, wobei auf beiden Clustern dieselbe Passphrase verwendet wird. Wenn der `security key-manager onboard enable` Befehl vom lokalen Cluster ausgeführt und anschließend auf dem Remote-Cluster synchronisiert wird, ist es nicht erforderlich, den `enable` Befehl erneut vom Remote-Cluster auszuführen.

Weitere Informationen zu `security key-manager onboard enable` und `security key-manager onboard sync` finden sich in der "ONTAP-Befehlsreferenz".

Standardmäßig ist die Eingabe der Passphrase für den Schlüsselmanager beim Neustart eines Knotens nicht erforderlich. Sie können die `cc-mode-enabled=yes` Option verwenden, um festzulegen, dass Benutzer die Passphrase nach einem Neustart eingeben müssen.

Für NVE: Wenn `cc-mode-enabled=yes` gesetzt ist, werden Volumes, die Sie mit den Befehlen `volume create` und `volume move start` erstellen, automatisch verschlüsselt. Für `volume create` muss `-encrypt true` nicht angegeben werden. Für `volume move start` muss `-encrypt-destination true` nicht angegeben werden.

Bei der Konfiguration von ONTAP Daten im Ruhezustand Verschlüsselung ist zur Erfüllung der Anforderungen für Commercial Solutions for Classified (CSfC) die Verwendung von NSE mit NVE erforderlich, und es muss sichergestellt werden, dass der Onboard Key Manager im Common Criteria-Modus aktiviert ist. Siehe "CSfC Solution Brief".

Wenn der Onboard Key Manager im Common Criteria-Modus aktiviert ist (`cc-mode-enabled=yes`, ändert sich das Systemverhalten wie folgt:

- Das System überwacht im Common Criteria-Modus aufeinanderfolgende fehlgeschlagene Cluster-Passphrasenversuche.

  Wenn die Cluster-Passphrase 5 Mal nicht korrekt eingegeben wird, ist entweder 24 Stunden zu warten oder der Knoten neu zu starten, um das Limit zurückzusetzen.

- Systemabbildaktualisierungen verwenden das NetApp RSA-3072-Codesignaturzertifikat zusammen mit SHA-384-codesignierten Digests zur Überprüfung der Abbildintegrität, anstelle des üblichen NetApp RSA-2048-Codesignaturzertifikats und SHA-256-

codesignierten Digests.

Der Upgrade-Befehl überprüft anhand verschiedener digitaler Signaturen, ob der Image-Inhalt verändert oder beschädigt wurde. Bei erfolgreicher Validierung fährt das System mit dem nächsten Schritt im Image-Aktualisierungsprozess fort, andernfalls schlägt die Image-Aktualisierung fehl. Weitere Informationen zu `cluster image` finden sich in der "ONTAP-Befehlsreferenz".

Der integrierte Schlüsselmanager speichert Schlüssel im flüchtigen Speicher. Der Inhalt des flüchtigen Speichers wird beim Neustart oder Anhalten des Systems gelöscht. Das System löscht den flüchtigen Speicher innerhalb von 30 Sekunden, wenn es angehalten wird.

Bevor Sie beginnen

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Die MetroCluster Umgebung muss konfiguriert werden, bevor der Onboard Key Manager konfiguriert wird.

Schritte

1. Die Einrichtung des Schlüsselmanagers wird gestartet:

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

   Setzen Sie `cc-mode-enabled=yes` so, dass Benutzer nach einem Neustart die Passphrase des Schlüsselmanagers eingeben müssen. Für NVE: Wenn `cc-mode-enabled=yes` gesetzt ist, werden Volumes, die Sie mit den Befehlen `volume create` und `volume move start` erstellen, automatisch verschlüsselt. Die `- cc-mode-enabled` Option wird in MetroCluster Konfigurationen nicht unterstützt. Der `security key-manager onboard enable` Befehl ersetzt den `security key-manager setup` Befehl.

2. Geben Sie eine Passphrase mit 32 bis 256 Zeichen ein oder für “cc-mode” eine Passphrase mit 64 bis 256 Zeichen.

   Ist die angegebene Passphrase für den “cc-mode” kürzer als 64 Zeichen, tritt eine Verzögerung von fünf Sekunden auf, bevor die Passphrase-Aufforderung im Rahmen der Schlüsselmanager-Einrichtung erneut angezeigt wird.

3. Bei der Aufforderung zur Passphrase-Bestätigung wird die Passphrase erneut eingegeben.
4. Es sollte überprüft werden, ob die Authentifizierungsschlüssel erstellt wurden:

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

   Der `security key-manager key query` Befehl ersetzt den `security key-manager query key` Befehl.

   Weitere Informationen zu `security key-manager key query` finden sich in der "ONTAP-Befehlsreferenz".

5. Optional ist es möglich, Klartext-Volumes in verschlüsselte Volumes zu konvertieren.

   `volume encryption conversion start`

Der Onboard Key Manager muss vollständig konfiguriert sein, bevor die Volumes konvertiert werden. In einer MetroCluster Umgebung muss der Onboard Key Manager an beiden Standorten konfiguriert sein.

Nachdem Sie fertig sind

Die Passphrase sollte an einem sicheren Ort außerhalb des Speichersystems für die zukünftige Verwendung aufbewahrt werden.

Nach der Konfiguration der Passphrase für den Onboard Key Manager die Informationen manuell an einem sicheren Ort außerhalb des Speichersystems sichern. Siehe "Onboard-Schlüsselverwaltungsinformationen manuell sichern".

Verwandte Informationen

- "Cluster Image-Befehle"
- "security key-manager external enable"
- "security key-manager key query"
- "security key-manager onboard enable"

Integrierte Schlüsselverwaltung für NVE in ONTAP 9.5 und früher aktivieren

Mit dem Onboard Key Manager können Sie die Schlüssel sichern, die der Cluster für den Zugriff auf verschlüsselte Daten verwendet. Der Onboard Key Manager muss auf jedem Cluster aktiviert sein, der auf ein verschlüsseltes Volume oder eine selbstverschlüsselnde Festplatte zugreift.

Über diese Aufgabe

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

Bei einer MetroCluster Konfiguration gelten folgende Richtlinien:

- In ONTAP 9.5 muss `security key-manager setup` auf dem lokalen Cluster und `security key-manager setup -sync-metrocluster-config yes` auf dem Remote-Cluster ausgeführt werden, wobei auf beiden Clustern dieselbe Passphrase verwendet wird.
- Vor ONTAP 9.5 muss `security key-manager setup` auf dem lokalen Cluster ausgeführt werden, etwa 20 Sekunden gewartet werden und dann `security key-manager setup` auf dem Remote-Cluster ausgeführt werden, wobei jeweils die gleiche Passphrase verwendet wird.

Standardmäßig ist die Eingabe der Passphrase für den Schlüsselmanager beim Neustart eines Knotens nicht erforderlich. Ab ONTAP 9.4 kann die `-enable-cc-mode yes` Option verwendet werden, um zu verlangen, dass Benutzer die Passphrase nach einem Neustart eingeben.

Für NVE: Wenn `-enable-cc-mode yes` gesetzt ist, werden Volumes, die Sie mit den Befehlen `volume create` und `volume move start` erstellen, automatisch verschlüsselt. Für `volume create` muss `-encrypt true` nicht angegeben werden. Für `volume move start` muss `-encrypt-destination true` nicht angegeben werden.

Nach einem fehlgeschlagenen Passphrase-Versuch ist ein erneuter Neustart des Knotens erforderlich.

Bevor Sie beginnen

- Wenn Sie NSE oder NVE mit einem externen Schlüsselverwaltungsserver (KMIP) verwenden, löschen Sie die externe Schlüsselverwaltungsdatenbank.

  "Umstellung vom externen auf das integrierte Schlüsselmanagement"

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Die MetroCluster Umgebung wird konfiguriert, bevor der Onboard Key Manager konfiguriert wird.

Schritte

1. Die Einrichtung des Schlüsselmanagers wird gestartet:

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

   > Ab ONTAP 9.4 kann die `-enable-cc-mode yes` Option verwendet werden, um zu verlangen, dass Benutzer nach einem Neustart die Passphrase des Schlüsselmanagers eingeben. Für NVE: Wenn `-enable-cc-mode yes` gesetzt ist, werden Volumes, die Sie mit den Befehlen `volume create` und `volume move start` erstellen, automatisch verschlüsselt.

   Das folgende Beispiel zeigt den Beginn der Einrichtung des Schlüsselmanagers auf Cluster1, ohne dass die Passphrase nach jedem Neustart eingegeben werden muss:

   ```
   cluster1::> security key-manager setup
   Welcome to the key manager setup wizard, which will lead you through
   the steps to add boot information.

   ...

   Would you like to use onboard key-management? {yes, no} [yes]:
   Enter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   ```

2. Geben Sie `yes` an der Eingabeaufforderung ein, um die integrierte Schlüsselverwaltung zu konfigurieren.
3. Bei der Aufforderung zur Eingabe der Passphrase ist eine Passphrase mit 32 bis 256 Zeichen einzugeben, oder für “cc-mode” eine Passphrase mit 64 bis 256 Zeichen.

   > Ist die angegebene Passphrase für den “cc-mode” kürzer als 64 Zeichen, tritt eine Verzögerung von fünf Sekunden auf, bevor die Passphrase-Aufforderung im Rahmen der Schlüsselmanager-Einrichtung erneut angezeigt wird.

4. Bei der Aufforderung zur Passphrase-Bestätigung wird die Passphrase erneut eingegeben.
5. Überprüfen, ob die Schlüssel für alle Knoten konfiguriert sind:

   `security key-manager show-key-store`

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

Node: node1
Key Store: onboard
Key ID                                                               Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK

Node: node2
Key Store: onboard
Key ID                                                               Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK
```

Weitere Informationen zu `security key-manager show-key-store` finden sich in der "ONTAP-Befehlsreferenz".

6. Optional können Klartext-Volumes in verschlüsselte Volumes umgewandelt werden.

   `volume encryption conversion start`

   Den Onboard Key Manager vor der Konvertierung der Volumes konfigurieren. In MetroCluster Umgebungen ist die Konfiguration an beiden Standorten erforderlich.

Nachdem Sie fertig sind

Die Passphrase sollte an einem sicheren Ort außerhalb des Speichersystems für die zukünftige Verwendung aufbewahrt werden.

Bei der Konfiguration der Passphrase des Onboard Key Managers sollten die Informationen zur Sicherheit an einem sicheren Ort außerhalb des Speichersystems gesichert werden, um im Katastrophenfall darauf zugreifen zu können. Siehe "Onboard-Schlüsselverwaltungsinformationen manuell sichern".

Verwandte Informationen

- "Onboard-Schlüsselverwaltungsinformationen manuell sichern"
- "Umstellung vom externen auf das integrierte Schlüsselmanagement"
- "security key-manager show-key-store"

Aktivierung der integrierten Schlüsselverwaltung auf neu hinzugefügten ONTAP Knoten

Mit dem Onboard Key Manager können Sie die Schlüssel sichern, die der Cluster für den Zugriff auf verschlüsselte Daten verwendet. Der Onboard Key Manager muss auf jedem Cluster aktiviert sein, der auf ein verschlüsseltes Volume oder eine selbstverschlüsselnde

Festplatte zugreift.

> Für ONTAP 9.6 und höher ist der `security key-manager onboard sync` Befehl jedes Mal auszuführen, wenn dem Cluster ein Knoten hinzugefügt wird.
>
> Bei ONTAP 9.5 und älteren Versionen muss der `security key-manager setup` Befehl jedes Mal ausgeführt werden, wenn ein Knoten zum Cluster hinzugefügt wird.
>
> Wenn Sie einen Knoten zu einem Cluster mit integrierter Schlüsselverwaltung hinzufügen, kann dieser Befehl ausgeführt werden, um fehlende Schlüssel zu aktualisieren.

Bei einer MetroCluster Konfiguration gelten folgende Richtlinien:

- Ab ONTAP 9.6 muss `security key-manager onboard enable`zuerst auf dem lokalen Cluster und dann `security key-manager onboard sync`auf dem Remote-Cluster ausgeführt werden, wobei auf beiden Clustern dieselbe Passphrase verwendet wird.

  Weitere Informationen zu `security key-manager onboard enable` und `security key-manager onboard sync` finden sich in der "ONTAP-Befehlsreferenz".

- In ONTAP 9.5 muss `security key-manager setup` auf dem lokalen Cluster und `security key-manager setup -sync-metrocluster-config yes` auf dem Remote-Cluster ausgeführt werden, wobei auf beiden Clustern dieselbe Passphrase verwendet wird.
- Vor ONTAP 9.5 muss `security key-manager setup` auf dem lokalen Cluster ausgeführt werden, etwa 20 Sekunden gewartet werden und dann `security key-manager setup` auf dem Remote-Cluster ausgeführt werden, wobei jeweils die gleiche Passphrase verwendet wird.

Standardmäßig ist die Eingabe der Passphrase für den Schlüsselmanager beim Neustart eines Knotens nicht erforderlich. Ab ONTAP 9.4 kann die `-enable-cc-mode yes` Option verwendet werden, um zu verlangen, dass Benutzer die Passphrase nach einem Neustart eingeben.

Für NVE: Wenn `-enable-cc-mode yes` gesetzt ist, werden Volumes, die Sie mit den Befehlen `volume create` und `volume move start` erstellen, automatisch verschlüsselt. Für `volume create` muss `-encrypt true` nicht angegeben werden. Für `volume move start` muss `-encrypt-destination true` nicht angegeben werden.

> Wenn der Passphrasenversuch fehlschlägt, sollte der Knoten neu gestartet werden. Nach dem Neustart besteht die Möglichkeit, die Passphrase erneut einzugeben.

Verwandte Informationen

- "Cluster Image-Befehle"
- "security key-manager external enable"
- "security key-manager onboard enable"

Volumendaten mit NVE oder NAE verschlüsseln

Informationen zur Verschlüsselung von ONTAP Volume-Daten mit NVE

Ab ONTAP 9.7 ist die Aggregat- und Volumenverschlüsselung standardmäßig aktiviert, wenn die VE-Lizenz sowie die integrierte oder externe Schlüsselverwaltung vorhanden

sind. Für ONTAP 9.6 und frühere Versionen kann die Verschlüsselung auf einem neuen oder einem bestehenden Volume aktiviert werden. Die VE-Lizenz muss installiert und die Schlüsselverwaltung aktiviert sein, bevor die Volumenverschlüsselung aktiviert werden kann. NVE ist FIPS-140-2 Level 1-konform.

Verschlüsselung auf Aggregatebene mit der VE-Lizenz in ONTAP aktivieren

Ab ONTAP 9.7 werden neu erstellte Aggregate und Volumes standardmäßig verschlüsselt, wenn die "VE-Lizenz" sowie eine integrierte oder externe Schlüsselverwaltung vorhanden sind. Ab ONTAP 9.6 kann die Verschlüsselung auf Aggregatebene verwendet werden, um dem übergeordneten Aggregat Schlüssel für die zu verschlüsselnden Volumes zuzuweisen.

Über diese Aufgabe

Eine Verschlüsselung auf Aggregatebene ist erforderlich, wenn eine Inline- oder Hintergrunddeduplizierung auf Aggregatebene vorgesehen ist. Die Deduplizierung auf Aggregatebene wird ansonsten von NVE nicht unterstützt.

Ein für die Verschlüsselung auf Aggregatebene aktiviertes Aggregat wird als *NAE-Aggregat* (für NetApp Aggregate Encryption) bezeichnet. Alle Volumes in einem NAE-Aggregat müssen mit NAE- oder NVE-Verschlüsselung verschlüsselt sein. Bei der Verschlüsselung auf Aggregatebene werden Volumes, die Sie im Aggregat erstellen, standardmäßig mit NAE-Verschlüsselung verschlüsselt. Sie können die Standardeinstellung überschreiben, um stattdessen NVE-Verschlüsselung zu verwenden.

Plain-Text-Volumes werden in NAE Aggregaten nicht unterstützt.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Verschlüsselung auf Aggregatebene aktivieren oder deaktivieren:

Zu…	Verwenden Sie diesen Befehl…
Ein NAE Aggregat mit ONTAP 9.7 oder höher erstellen	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`*
Ein NAE Aggregat mit ONTAP 9.6 erstellen	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
Ein Nicht-NAE-Aggregat in ein NAE-Aggregat konvertieren	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
Ein NAE-Aggregat in ein Nicht-NAE-Aggregat konvertieren	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key false`

Weitere Informationen zu `storage aggregate modify` finden sich in der "ONTAP-Befehlsreferenz".

Der folgende Befehl aktiviert die Verschlüsselung auf Aggregatebene für `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
```

Weitere Informationen zu `storage aggregate create` finden sich in der "ONTAP-Befehlsreferenz".

2. Überprüfen, ob das Aggregat für die Verschlüsselung aktiviert ist:

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

Der folgende Befehl überprüft, ob `aggr1` für die Verschlüsselung aktiviert ist:

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

Weitere Informationen zu `storage aggregate show` finden sich in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

Den `volume create` Befehl ausführen, um die verschlüsselten Volumes zu erstellen.

Wenn Sie einen KMIP-Server zum Speichern der Verschlüsselungsschlüssel für einen Knoten verwenden, sendet ONTAP beim Verschlüsseln eines Volumes automatisch einen Verschlüsselungsschlüssel an den Server.

Verschlüsselung auf einem neuen Volume in ONTAP aktivieren

Mit dem `volume create` Befehl lässt sich die Verschlüsselung auf einem neuen Volume aktivieren.

Über diese Aufgabe

Volumes lassen sich mit NetApp Volume Encryption (NVE) und ab ONTAP 9.6 mit NetApp Aggregate Encryption (NAE) verschlüsseln. Weitere Informationen zu NAE und NVE enthält die Übersicht zur Volumenverschlüsselung.

Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Die Vorgehensweise zum Aktivieren der Verschlüsselung auf einem neuen Volume in ONTAP variiert je nach

verwendeter ONTAP-Version und Ihrer spezifischen Konfiguration:

- Ab ONTAP 9.4, wenn beim Einrichten des Onboard Key Managers `cc-mode` aktiviert wird, werden Volumes, die mit dem `volume create` Befehl erstellt werden, automatisch verschlüsselt, unabhängig davon, ob `-encrypt true` angegeben wird.
- In ONTAP 9.6 und früheren Versionen muss `-encrypt true` mit `volume create` Befehlen die Verschlüsselung aktiviert werden (sofern `cc-mode` nicht aktiviert wurde).
- Wenn in ONTAP 9.6 ein NAE-Volume erstellt werden soll, muss NAE auf Aggregatebene aktiviert werden. Weitere Details zu dieser Aufgabe sind unter Verschlüsselung auf Aggregatebene mit der VE-Lizenz aktivieren zu finden.
- Ab ONTAP 9.7 werden neu erstellte Volumes standardmäßig verschlüsselt, wenn die "VE-Lizenz" sowie eine integrierte oder externe Schlüsselverwaltung vorhanden sind. Standardmäßig sind neue Volumes, die in einem NAE Aggregat erstellt werden, vom Typ NAE statt NVE.
  - In ONTAP 9.7 und späteren Versionen, wenn `-encrypt true` zum `volume create`-Befehl hinzugefügt wird, um ein Volume in einem NAE-Aggregat zu erstellen, erhält das Volume NVE-Verschlüsselung anstelle von 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. Ein neues Volume erstellen und angeben, ob die Verschlüsselung für das Volume aktiviert ist. Befindet sich das neue Volume in einem NAE Aggregat, ist das Volume standardmäßig ein NAE Volume:

Zum Erstellen…	Verwenden Sie diesen Befehl…
Ein NAE Volume	`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 später, wo Volumes in NAE Aggregaten erstellt werden, `-encrypt true` überschreibt den Standardverschlüsselungstyp von NAE, sodass stattdessen ein NVE Volume erstellt wird.
Ein einfaches Text-Volume	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt false`

   Weitere Informationen zu `volume create` finden sich in der "ONTAP-Befehlsreferenz".

2. Überprüfen, ob Volumes für die Verschlüsselung aktiviert sind:

   ```
   volume show -is-encrypted true
   ```

   Weitere Informationen zu `volume show` finden sich in der "ONTAP-Befehlsreferenz".

Ergebnis

Wenn ein KMIP-Server zum Speichern der Verschlüsselungsschlüssel für einen Knoten verwendet wird, überträgt ONTAP automatisch einen Verschlüsselungsschlüssel an den Server, wenn ein Volume verschlüsselt wird.

NAE oder NVE auf einem vorhandenen ONTAP Volume aktivieren

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

Über diese Aufgabe

Sie können den `volume encryption conversion start`Befehl verwenden, um die Verschlüsselung eines vorhandenen Volumes „an Ort und Stelle“ zu aktivieren, ohne das Volume an einen anderen Speicherort verschieben zu müssen. Alternativ kann der `volume move start` Befehl verwendet werden.

Die Verschlüsselung eines vorhandenen Volumes kann mit dem Befehl volume encryption conversion start aktiviert werden.

Sie können den `volume encryption conversion start`Befehl verwenden, um die Verschlüsselung eines vorhandenen Volumes „an Ort und Stelle“ zu aktivieren, ohne das Volume an einen anderen Speicherort verschieben zu müssen.

Nachdem Sie eine Konvertierungsoperation gestartet haben, muss diese abgeschlossen werden. Wenn während des Vorgangs Leistungsprobleme auftreten, kann der Vorgang mit dem `volume encryption conversion pause` Befehl angehalten und mit dem `volume encryption conversion resume` Befehl fortgesetzt werden.

> Sie können `volume encryption conversion start`nicht verwenden, um ein SnapLock-Volumen zu konvertieren.

Schritte

1. Verschlüsselung für ein vorhandenes Volume aktivieren:

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

   Weitere Informationen zu `volume encryption conversion start` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl aktiviert die Verschlüsselung auf einem bestehenden Volume `vol1`:

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

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

2. Status des Konvertierungsvorgangs überprüfen:

   `volume encryption conversion show`

Weitere Informationen zu `volume encryption conversion show` finden sich in der "ONTAP-Befehlsreferenz".

Der folgende Befehl zeigt den Status des Konvertierungsvorgangs an:

```
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. Nach Abschluss der Konvertierung sollte überprüft werden, ob das Volume für die Verschlüsselung aktiviert ist:

   `volume show -is-encrypted true`

   Weitere Informationen zu `volume show` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl zeigt die verschlüsselten Volumes auf `cluster1` an:

```
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 Verschlüsselungsschlüssel für einen Knoten verwenden, sendet ONTAP beim Verschlüsseln eines Volumes automatisch einen Verschlüsselungsschlüssel an den Server.

Die Verschlüsselung auf einem vorhandenen Volume mit dem Befehl „volume move start“ aktivieren

Sie können den `volume move start` Befehl verwenden, um die Verschlüsselung durch Verschieben eines vorhandenen Volumes zu aktivieren. Sie können dasselbe Aggregat oder ein anderes Aggregat verwenden.

Über diese Aufgabe

- Ab ONTAP 9.8 kann `volume move start` verwendet werden, um die Verschlüsselung auf einem SnapLock- oder FlexGroup-Volume zu aktivieren.
- Ab ONTAP 9.4 werden Volumes, die mit dem `volume move start` Befehl erstellt werden, automatisch verschlüsselt, wenn beim Einrichten des Onboard Key Managers der “cc-mode” aktiviert ist. Eine Angabe von `-encrypt-destination true` ist nicht erforderlich.
- Ab ONTAP 9.6 kann die Verschlüsselung auf Aggregatebene verwendet werden, um dem enthaltenen Aggregat für die zu verschiebenden Volumes Schlüssel zuzuweisen. Ein mit einem eindeutigen Schlüssel verschlüsseltes Volume wird als *NVE Volume* bezeichnet (das bedeutet, es verwendet NetApp Volume Encryption). Ein mit einem Schlüssel auf Aggregatebene verschlüsseltes Volume wird als *NAE Volume* bezeichnet (für NetApp Aggregate Encryption). Klartext-Volumes werden in NAE Aggregaten nicht

unterstützt.

- Ab ONTAP 9.14.1 ist es möglich, ein SVM-Root-Volume mit NVE zu verschlüsseln. Weitere Informationen finden sich unter Konfiguration der NetApp Volume Encryption auf einem SVM Root-Volume.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können, oder SVM-Administrator, dem der Cluster-Administrator die entsprechende Berechtigung delegiert hat.

"Delegierung der Berechtigung zum Ausführen des Volume Move-Befehls"

Schritte

1. Ein vorhandenes Volume verschieben und angeben, ob die Verschlüsselung für das Volume aktiviert ist:

Zum Umwandeln…	Verwenden Sie diesen Befehl…
Ein Klartext-Volume zu einem NVE-Volume	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination true`
Ein NVE- oder Klartext-Volume zu einem NAE-Volume (vorausgesetzt, die Verschlüsselung auf Aggregatebene ist auf dem Ziel aktiviert)	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-with-aggr-key true`
Ein NAE Volume zu einem NVE Volume	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-with-aggr-key false`
Ein NAE Volume zu einem Klartext Volume	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination false -encrypt-with-aggr-key false`
Ein NVE Volume zu einem Klartext Volume	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination false`

Weitere Informationen zu `volume move start` finden sich in der "ONTAP-Befehlsreferenz".

Der folgende Befehl konvertiert ein Klartext-Volume mit dem Namen `vol1` zu einem NVE-Volume:

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

Unter der Annahme, dass die Verschlüsselung auf Aggregatebene auf dem Zielsystem aktiviert ist, konvertiert der folgende Befehl ein NVE- oder Klartext-Volume mit dem Namen `vol1` in ein NAE-Volume:

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

Der folgende Befehl konvertiert ein NAE-Volume mit dem Namen `vol2` zu einem NVE-Volume:

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

Der folgende Befehl konvertiert ein NAE-Volume mit dem Namen `vol2` in ein Klartext-Volume:

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

Der folgende Befehl konvertiert ein NVE-Volume mit dem Namen `vol2` in ein Klartext-Volume:

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

2. Den Verschlüsselungstyp der Cluster-Volumes anzeigen:

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

   Das `encryption-type` Feld ist in ONTAP 9.6 und späteren Versionen verfügbar.

   Weitere Informationen zu `volume show` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl zeigt den Verschlüsselungstyp der Volumes in `cluster2` an:

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

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

3. Überprüfen, ob Volumes für die Verschlüsselung aktiviert sind:

   `volume show -is-encrypted true`

   Weitere Informationen zu `volume show` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl zeigt die verschlüsselten Volumes auf `cluster2` an:

```
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 ein KMIP-Server zum Speichern der Verschlüsselungsschlüssel für einen Knoten verwendet wird, überträgt ONTAP automatisch einen Verschlüsselungsschlüssel an den Server, wenn ein Volume verschlüsselt wird.

Konfiguration von NVE auf einem ONTAP SVM Root-Volume

Ab ONTAP 9.14.1 kann die NetApp Volume Encryption (NVE) auf einem Storage-VM (SVM) Root-Volume aktiviert werden. Mit NVE wird das Root-Volume mit einem eindeutigen Schlüssel verschlüsselt, was eine höhere Sicherheit auf der SVM ermöglicht.

Über diese Aufgabe

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

Bevor Sie beginnen

- Das SVM-Root-Volume darf sich nicht auf einem mit NetApp Aggregate Encryption (NAE) verschlüsselten Aggregat befinden.
- Die Verschlüsselung muss mit dem Onboard Key Manager oder einem externen Key Manager aktiviert sein.
- ONTAP 9.14.1 oder höher muss ausgeführt werden.
- Um eine SVM mit einem mit NVE verschlüsselten Root-Volume zu migrieren, muss das SVM-Root-Volume nach Abschluss der Migration in ein Klartext-Volume konvertiert und anschließend das SVM-Root-Volume erneut verschlüsselt werden.
  - 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:
  - Die Verschlüsselungseinstellungen einer gespiegelten SVM werden nicht auf das Ziel kopiert. Wenn NVE auf dem Quell- oder Zielsystem aktiviert wird, muss NVE separat auf dem Root-Volume der gespiegelten SVM aktiviert werden.
  - Wenn alle Aggregate im Ziel-Cluster NAE verwenden, verwendet das SVM-Root-Volume ebenfalls NAE.

Schritte

NVE kann auf einem SVM-Root-Volume mit der ONTAP CLI oder dem System Manager aktiviert werden.

CLI

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

Das Root-Volume wird direkt verschlüsselt.

1. Das Root-Volume in ein verschlüsseltes Volume umwandeln:

```
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 an, die NVE verwenden.

Das SVM-Root-Volume durch Verschieben verschlüsseln

1. Eine Volumenverschiebung initiieren:

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

   Weitere Informationen zu `volume move` finden sich in der "ONTAP-Befehlsreferenz".

2. Der erfolgreiche Abschluss des `volume move`Vorgangs kann mit dem `volume move show`Befehl bestätigt werden. Der `volume show -encryption-type volume`zeigt eine Liste aller Volumes an, die NVE verwenden.

System Manager

1. Zu **Speicher** > **Volumes** navigieren.
2. Neben dem Namen des SVM-Root-Volumes, das Sie verschlüsseln möchten, ⋮ dann **Bearbeiten** auswählen.
3. Unter der Überschrift **Speicherung und Optimierung** die Option **Verschlüsselung aktivieren** auswählen.
4. **Speichern** auswählen.

Konfiguration von NVE auf einem ONTAP Knoten-Root-Volume

Ab ONTAP 9.8 kann die NetApp Volume Encryption verwendet werden, um das Root-Volume eines Knotens zu schützen.

Über diese Aufgabe

Dieses Verfahren gilt für das Knoten-Root-Volume. Es gilt nicht für SVM-Root-Volumes. SVM-Root-Volumes können durch Verschlüsselung auf Aggregatebene geschützt werden und beginnend mit ONTAP 9.14.1, NVE.

Sobald die Verschlüsselung des Root-Volumes beginnt, muss sie abgeschlossen werden. Der Vorgang kann nicht pausiert werden. Nach Abschluss der Verschlüsselung kann dem Root-Volume kein neuer Schlüssel zugewiesen werden und eine sichere Löschung kann nicht durchgeführt werden.

Bevor Sie beginnen

- Ihr System muss eine HA Konfiguration verwenden.
- Ihr Node Root-Volume muss bereits erstellt sein.
- Ihr System muss über einen integrierten Schlüsselmanager oder einen externen Schlüsselverwaltungsserver verfügen, der das Key Management Interoperability Protocol (KMIP) verwendet.

Schritte

1. Das Root-Volume verschlüsseln:

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

2. Status des Konvertierungsvorgangs überprüfen:

   ```
   volume encryption conversion show
   ```

3. Nach Abschluss der Konvertierung kann überprüft werden, ob das Volume verschlüsselt ist:

   ```
   volume show -fields
   ```

   Nachfolgend wird eine Beispielausgabe für ein verschlüsseltes Volume gezeigt.

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

Hardwarebasierte Verschlüsselung von NetApp konfigurieren

Informationen zu ONTAP hardwarebasierter Verschlüsselung

NetApp hardwarebasierte Verschlüsselung unterstützt die vollständige Festplattenverschlüsselung (FDE) von Daten während des Schreibvorgangs. Die Daten können ohne einen auf der Firmware gespeicherten Verschlüsselungsschlüssel nicht gelesen werden. Der Verschlüsselungsschlüssel ist wiederum nur für einen authentifizierten Knoten zugänglich.

Verständnis der NetApp hardwarebasierten Verschlüsselung

Ein Knoten authentifiziert sich gegenüber einem Self-Encrypting Drive mithilfe eines Authentifizierungsschlüssels, der von einem externen Schlüsselverwaltungsserver oder dem Onboard Key Manager abgerufen wird:

- Der externe Schlüsselverwaltungsserver ist ein Drittanbietersystem in Ihrer Speicherumgebung, das Schlüssel für Knoten mithilfe des Key Management Interoperability Protocol (KMIP) bereitstellt. Es gilt als Best Practice, externe Schlüsselverwaltungsserver auf einem anderen Speichersystem als Ihren Daten zu konfigurieren.
- Der Onboard Key Manager ist ein integriertes Tool, das Authentifizierungsschlüssel für Knoten aus demselben Speichersystem bereitstellt wie Ihre Daten.

Sie können NetApp Volume Encryption mit hardwarebasierter Verschlüsselung verwenden, um Daten auf Self-Encrypting Drives „doppelt zu verschlüsseln“.

Wenn Self-Encrypting Drives aktiviert sind, wird auch der Core Dump verschlüsselt.

> Wenn ein HA-Paar verschlüsselnde SAS- oder NVMe-Laufwerke (SED, NSE, FIPS) verwendet, sind die Anweisungen im Thema Zurückstellen eines FIPS-Laufwerks oder SED in den ungeschützten Modus für alle Laufwerke innerhalb des HA-Paares vor der Initialisierung des Systems (Boot-Optionen 4 oder 9) zu beachten. Andernfalls kann es in Zukunft zu Datenverlust

kommen, wenn die Laufwerke wiederverwendet werden.

Unterstützte Self-Encrypting Drives Typen

Es werden zwei Arten von Self-Encrypting Drives unterstützt:

- Self-Encrypting Drives (FIPS-zertifizierte SAS- oder NVMe-Laufwerke) werden auf allen FAS und AFF Systemen unterstützt. Diese Laufwerke, sogenannte FIPS Drives, erfüllen die Anforderungen der Federal Information Processing Standard Publication 140-2, Level 2. Die zertifizierten Funktionen ermöglichen neben der Verschlüsselung weitere Schutzmechanismen, wie beispielsweise die Abwehr von Denial-of-Service-Angriffen. FIPS-Laufwerke dürfen nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden.
- Ab ONTAP 9.6 werden Self-Encrypting NVMe Drives, die nicht dem FIPS-Test unterzogen wurden, auf AFF A800, A320 und späteren Systemen unterstützt. Diese Laufwerke, sogenannte SEDs, bieten dieselben Verschlüsselungsfunktionen wie FIPS Drives, können aber zusammen mit nicht verschlüsselnden Laufwerken auf demselben Node oder HA-Paar eingesetzt werden.
- Alle FIPS-validierten Laufwerke verwenden ein Firmware-Kryptografiemodul, das die FIPS-Validierung durchlaufen hat. Das FIPS-Kryptografiemodul des Laufwerks verwendet keine Schlüssel, die außerhalb des Laufwerks generiert werden (die Authentifizierungs-Passphrase, die für das Laufwerk eingegeben wird, wird vom Firmware-Kryptografiemodul des Laufwerks verwendet, um einen Schlüssel zur Verschlüsselung zu erhalten).

Nicht verschlüsselnde Laufwerke sind Laufwerke, die weder SEDs noch FIPS-Laufwerke sind.

Wenn Sie NSE auf einem System mit Flash Cache Modul verwenden, sollten Sie auch NVE oder NAE aktivieren. NSE verschlüsselt keine Daten, die sich auf dem Flash Cache Modul befinden.

Wann wird externes Schlüsselmanagement verwendet?

Auch wenn die Verwendung des integrierten Schlüsselmanagers kostengünstiger und in der Regel bequemer ist, empfiehlt sich die Nutzung einer externen Schlüsselverwaltung, wenn einer der folgenden Punkte zutrifft:

- Die Richtlinie Ihrer Organisation erfordert eine Schlüsselverwaltungslösung, die ein kryptografisches Modul gemäß FIPS 140-2 Level 2 (oder höher) verwendet.
- Sie benötigen eine Multi-Cluster-Lösung mit zentralisierter Verwaltung der Verschlüsselungsschlüssel.
- Ihr Unternehmen benötigt die zusätzliche Sicherheit, Authentifizierungsschlüssel auf einem System oder an einem anderen Ort als die Daten zu speichern.

Supportdetails

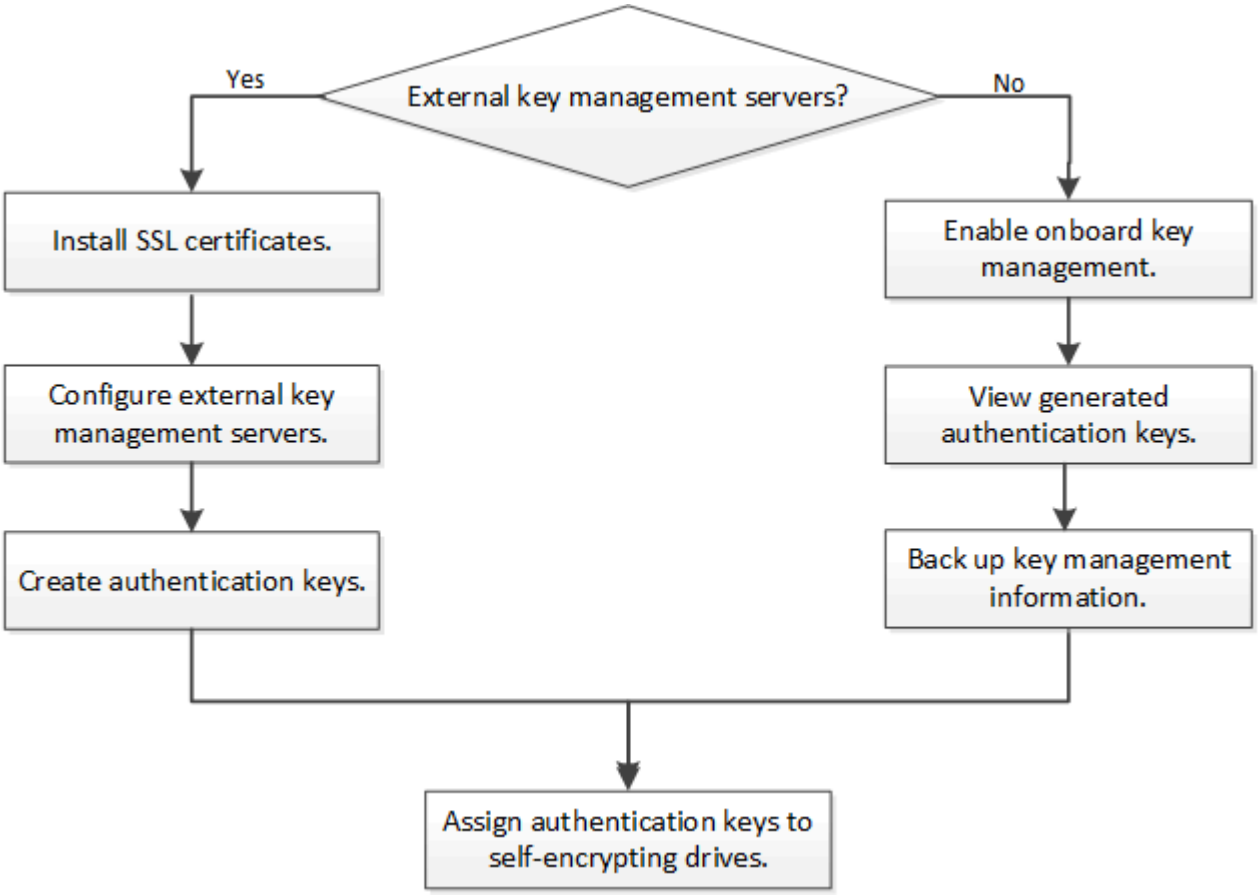
Die folgende Tabelle enthält wichtige Details zur Hardware-Verschlüsselungsunterstützung. Die Interoperabilitätsmatrix enthält aktuelle Informationen zu unterstützten KMIP-Servern, Speichersystemen und Festplattengehäusen.

Ressource oder Funktion	Supportdetails

Nicht-homogene Festplattensätze	• FIPS-Laufwerke dürfen nicht mit anderen Laufwerkstypen auf demselben Node oder HA-Paar kombiniert werden. Konforme HA-Paare können im selben Cluster neben nicht-konformen HA-Paaren existieren. • SEDs können mit nicht verschlüsselnden Laufwerken auf demselben Node oder HA Pair gemischt werden.
Laufwerkstyp	• FIPS-Laufwerke können SAS- oder NVMe-Laufwerke sein. • SEDs müssen NVMe-Laufwerke sein.
10 Gb Netzwerkschnittstellen	Ab ONTAP 9.3 unterstützen KMIP-Schlüsselverwaltungskonfigurationen 10 Gb Netzwerkschnittstellen für die Kommunikation mit externen Schlüsselverwaltungsservern.
Ports für die Kommunikation mit dem Schlüsselverwaltungsserver	Ab ONTAP 9.3 kann jeder beliebige Port des Storage Controllers für die Kommunikation mit dem Key Management Server verwendet werden. Andernfalls sollte Port e0M für die Kommunikation mit Key Management Servern verwendet werden. Je nach Storage Controller Modell sind bestimmte Netzwerkschnittstellen während des Bootvorgangs möglicherweise nicht für die Kommunikation mit Key Management Servern verfügbar.
MetroCluster (MCC)	• NVMe-Laufwerke unterstützen MCC. • SAS-Laufwerke unterstützen MCC nicht.

Hardwarebasierter Verschlüsselungsworkflow

Die Schlüsselverwaltungsdienste müssen konfiguriert werden, bevor sich der Cluster gegenüber den Self-Encrypting Drives authentifizieren kann. Es kann ein externer Schlüsselverwaltungsserver oder ein integrierter Schlüsselmanager verwendet werden.



Verwandte Informationen

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

Externe Schlüsselverwaltung konfigurieren

Informationen zur externen Schlüsselverwaltung in ONTAP

Sie können einen oder mehrere externe Schlüsselverwaltungsserver verwenden, um die Schlüssel zu sichern, die der Cluster für den Zugriff auf verschlüsselte Daten verwendet. Ein externer Schlüsselverwaltungsserver ist ein Drittanbietersystem in Ihrer Speicherumgebung, das Schlüssel an Nodes mithilfe des Key Management Interoperability Protocol (KMIP) bereitstellt.

NetApp Volume Encryption (NVE) kann mit dem Onboard Key Manager implementiert werden. In ONTAP 9.3 und höher kann NVE mit externem Key Management (KMIP) und dem Onboard Key Manager implementiert werden. Ab ONTAP 9.11.1 ist die Konfiguration mehrerer externer Schlüsselmanager in einem Cluster möglich. Siehe Clustered Key-Server konfigurieren.

SSL-Zertifikate auf dem ONTAP Cluster installieren

Der Cluster und der KMIP-Server verwenden KMIP-SSL-Zertifikate, um gegenseitig die Identität zu verifizieren und eine SSL-Verbindung herzustellen. Vor der Konfiguration der SSL-Verbindung mit dem KMIP-Server müssen die KMIP-Client-SSL-Zertifikate für den

Cluster sowie das öffentliche SSL-Zertifikat für die Root-Zertifizierungsstelle (CA) des KMIP-Servers installiert werden.

Über diese Aufgabe

In einem HA-Paar müssen beide Knoten dieselben öffentlichen und privaten KMIP-SSL-Zertifikate verwenden. Wenn mehrere HA-Paare mit demselben KMIP-Server verbunden sind, müssen alle Knoten in den HA-Paaren dieselben öffentlichen und privaten KMIP-SSL-Zertifikate verwenden.

Bevor Sie beginnen

- Die Zeit muss auf dem Server, der die Zertifikate erstellt, dem KMIP Server und dem Cluster synchronisiert sein.
- Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.
- Das öffentliche SSL KMIP-Clientzertifikat für den Cluster muss vorliegen.
- Der private Schlüssel, der dem SSL KMIP Clientzertifikat für den Cluster zugeordnet ist, muss vorliegen.
- Das SSL KMIP-Clientzertifikat darf nicht passwortgeschützt sein.
- Das öffentliche SSL-Zertifikat für die Stammzertifizierungsstelle (CA) des KMIP-Servers muss vorliegen.
- In einer MetroCluster Umgebung müssen auf beiden Clustern die gleichen KMIP SSL-Zertifikate installiert werden.

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

`admin_SVM` ist die Admin-SVM für den Cluster. In den folgenden Beispielen heißt die Admin-SVM `cluster1`, daher erscheint `cluster1` sowohl in der Eingabeaufforderung (`cluster1::>`) als auch als Wert für `-vserver`.

Schritte

1. Die SSL-KMIP-Clientzertifikate für den Cluster installieren:

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

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

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

2. Das öffentliche SSL-Zertifikat für die Root-Zertifizierungsstelle (CA) des KMIP-Servers installieren:

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

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

Verwandte Informationen

- "Sicherheitszertifikat installieren"

Externe Schlüsselverwaltung für die Hardwareverschlüsselung in ONTAP 9.6 und höheren Versionen aktivieren

Sie können einen oder mehrere KMIP-Server verwenden, um die Schlüssel zu sichern,

die der Cluster für den Zugriff auf verschlüsselte Daten verwendet. Sie können bis zu vier KMIP-Server mit einem Knoten verbinden. Für Redundanz und Notfallwiederherstellung werden mindestens zwei Server empfohlen.

Ab ONTAP 9.11.1 können bis zu 3 sekundäre Schlüsselserver pro primärem Schlüsselserver hinzugefügt werden, um einen gruppierten Schlüsselserver zu erstellen. Weitere Informationen finden sich unter Clustered externe Schlüsselserver konfigurieren.

Bevor Sie beginnen

- Die KMIP SSL-Client- und Serverzertifikate müssen installiert sein.
- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- In einer MetroCluster Umgebung:
  - Die MetroCluster Umgebung muss konfiguriert werden, bevor ein externer Schlüsselmanager konfiguriert wird.
  - Auf beiden Clustern ist dasselbe KMIP SSL-Zertifikat zu installieren.

Schritte

1. Die Key-Manager-Konnektivität für den Cluster konfigurieren:

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

   - Der `security key-manager external enable` Befehl ersetzt den `security key-manager setup` Befehl. Der `security key-manager external modify` Befehl kann verwendet werden, um die Konfiguration der externen Schlüsselverwaltung zu ändern. Weitere Informationen zu `security key-manager external enable` finden sich in der "ONTAP-Befehlsreferenz".
   - In einer MetroCluster Umgebung muss bei der Konfiguration der externen Schlüsselverwaltung für die Admin-SVM der `security key-manager external enable` Befehl auf dem Partnercluster wiederholt werden.

   Der folgende Befehl aktiviert die externe Schlüsselverwaltung für `cluster1` mit drei externen Schlüsselservern. Der erste Schlüsselserver wird über seinen Hostnamen und Port angegeben, der zweite über eine IP-Adresse und den Standardport, und der dritte über eine IPv6-Adresse und den 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. Es wird überprüft, ob 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` Befehl ersetzt den `security key-manager show -status` Befehl. Weitere Informationen zu `security key-manager external show-status` finden sich in der "ONTAP-Befehlsreferenz".

```
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.
```

Verwandte Informationen

- Clustered externe Schlüsselserver konfigurieren
- "security-key-manager-external-enable"
- "security-key-manager-external-show-status"

Aktivierung der externen Schlüsselverwaltung für die Hardwareverschlüsselung in ONTAP 9.5 und früheren Versionen

Sie können einen oder mehrere KMIP-Server verwenden, um die Schlüssel zu sichern, die der Cluster für den Zugriff auf verschlüsselte Daten verwendet. Sie können bis zu vier KMIP-Server mit einem Knoten verbinden. Für Redundanz und Notfallwiederherstellung werden mindestens zwei Server empfohlen.

Über diese Aufgabe

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

Bevor Sie beginnen

- Die KMIP SSL-Client- und Serverzertifikate müssen installiert sein.
- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Die MetroCluster Umgebung muss konfiguriert werden, bevor ein externer Schlüsselmanager konfiguriert wird.
- In einer MetroCluster Umgebung muss auf beiden Clustern dasselbe KMIP SSL-Zertifikat installiert werden.

Schritte

1. Konfiguration der Key-Manager-Konnektivität für Clusterknoten:

   `security key-manager setup`

   Die Einrichtung des Schlüsselmanagers beginnt.

   > In einer MetroCluster Umgebung muss dieser Befehl auf beiden Clustern ausgeführt werden. Weitere Informationen zu `security key-manager setup` finden sich in der "ONTAP-Befehlsreferenz".

2. Geben Sie bei jeder Eingabeaufforderung die entsprechende Antwort ein.
3. Einen KMIP-Server hinzufügen:

   `security key-manager add -address key_management_server_ipaddress`

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

   > In einer MetroCluster Umgebung muss dieser Befehl auf beiden Clustern ausgeführt werden.

4. Einen zusätzlichen KMIP Server für Redundanz hinzufügen:

   `security key-manager add -address key_management_server_ipaddress`

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

   > In einer MetroCluster Umgebung muss dieser Befehl auf beiden Clustern ausgeführt werden.

5. Es wird überprüft, ob alle konfigurierten KMIP-Server verbunden sind:

   `security key-manager show -status`

   Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

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

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

6. Optional können Klartext-Volumes in verschlüsselte Volumes umgewandelt werden.

   ```
   volume encryption conversion start
   ```

   Vor der Konvertierung der Volumes muss ein externer Schlüsselmanager vollständig konfiguriert sein. In einer MetroCluster-Umgebung muss ein externer Schlüsselmanager an beiden Standorten konfiguriert sein.

Konfiguration von gruppierten externen Schlüsselservern in ONTAP

Ab ONTAP 9.11.1 kann die Konnektivität zu gruppierten externen Schlüsselverwaltungsservern auf einer SVM konfiguriert werden. Mit gruppierten Schlüsselservern lassen sich primäre und sekundäre Schlüsselserver auf einer SVM festlegen. Beim Registrieren oder Abrufen von Schlüsseln versucht ONTAP zunächst, auf den primären Schlüsselserver zuzugreifen, bevor nacheinander die sekundären Server angesprochen werden, bis der Vorgang erfolgreich abgeschlossen ist.

Externe Schlüsselserver können für NetApp Storage Encryption (NSE), NetApp Volume Encryption (NVE) und NetApp Aggregate Encryption (NAE) Schlüssel verwendet werden. Eine SVM kann bis zu vier primäre externe KMIP-Server unterstützen. Jeder primäre Server kann bis zu drei sekundäre Schlüsselserver unterstützen.

Über diese Aufgabe

- Dieser Prozess unterstützt nur Schlüsselserver, die KMIP verwenden. Eine Liste der unterstützten Schlüsselserver befindet sich im "NetApp Interoperabilitätsmatrix-Tool".

Bevor Sie beginnen

- "Die KMIP-Schlüsselverwaltung muss für die SVM aktiviert sein.".
- Alle Knoten im Cluster müssen ONTAP 9.11.1 oder höher ausführen.
- Die Reihenfolge der im `-secondary-key-servers` Parameter aufgeführten Server entspricht der Zugriffsreihenfolge der externen Key-Management-Server (KMIP).

Einen gruppierten Schlüsselserver erstellen

Das Konfigurationsverfahren hängt davon ab, ob ein Primärschlüsselserver konfiguriert wurde oder nicht.

Primäre und sekundäre Schlüsselserver zu einer SVM hinzufügen

Schritte

1. Bestätigen Sie, dass für den Cluster (admin SVM) keine Schlüsselverwaltung aktiviert wurde:

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

   Wenn auf der SVM bereits die maximale Anzahl von vier primären Schlüsselservern aktiviert ist, muss einer der vorhandenen primären Schlüsselserver entfernt werden, bevor ein neuer hinzugefügt werden kann.

2. Primärschlüsselmanager aktivieren:

   ```
   security key-manager external enable -vserver <svm_name> -key-servers
   <primary_key_server_ip> -client-cert <client_cert_name> -server-ca-certs
   <server_ca_cert_names>
   ```

- Wenn im `-key-servers`-Parameter kein Port angegeben wird, wird der Standardport 5696 verwendet.

> Wenn Sie den `security key-manager external enable` Befehl für die administrative SVM in einer MetroCluster Konfiguration ausführen, muss der Befehl auf beiden Clustern ausgeführt werden. Wenn Sie den Befehl für eine einzelne Daten-SVM ausführen, ist es nicht erforderlich, den Befehl auf beiden Clustern auszuführen. NetApp empfiehlt nachdrücklich, auf beiden Clustern dieselben Schlüsselserver zu verwenden.

3. Den primären Schlüsselserver ändern, um sekundäre Schlüsselserver hinzuzufügen. Der `-secondary-key-servers` Parameter akzeptiert eine durch Kommas getrennte Liste von 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>
```

   - Geben Sie im `-secondary-key-servers` Parameter keine Portnummer für sekundäre Schlüsselserver an. Es wird dieselbe Portnummer wie für den primären Schlüsselserver verwendet.

> Wenn Sie den `security key-manager external` Befehl für die administrative SVM in einer MetroCluster Konfiguration ausführen, muss der Befehl auf beiden Clustern ausgeführt werden. Wenn Sie den Befehl für eine einzelne Daten-SVM ausführen, ist es nicht erforderlich, den Befehl auf beiden Clustern auszuführen. NetApp empfiehlt nachdrücklich, auf beiden Clustern dieselben Schlüsselserver zu verwenden.

Sekundäre Schlüsselserver zu einem vorhandenen primären Schlüsselserver hinzufügen

Schritte

1. Den primären Schlüsselserver ändern, um sekundäre Schlüsselserver hinzuzufügen. Der `-secondary-key-servers` Parameter akzeptiert eine durch Kommas getrennte Liste von 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>
```

   - Geben Sie im `-secondary-key-servers` Parameter keine Portnummer für sekundäre Schlüsselserver an. Es wird dieselbe Portnummer wie für primäre Schlüsselserver verwendet.

> Wenn Sie den `security key-manager external modify-server` Befehl für die administrative SVM in einer MetroCluster Konfiguration ausführen, muss der Befehl auf beiden Clustern ausgeführt werden. Wenn Sie den Befehl für eine einzelne Daten-SVM ausführen, ist es nicht erforderlich, den Befehl auf beiden Clustern auszuführen. NetApp empfiehlt nachdrücklich, auf beiden Clustern dieselben Schlüsselserver zu verwenden.

Weitere Informationen zu sekundären Schlüsselservern sind unter [mod-secondary] zu finden.

Gruppierte Schlüsselserver ändern

Sie können gruppierte externe Schlüsselserver modifizieren, indem Sie sekundäre Schlüsselserver hinzufügen oder entfernen, die Zugriffsreihenfolge der sekundären Schlüsselserver ändern oder die Bezeichnung (primär oder sekundär) bestimmter Schlüsselserver ändern. Wenn gruppierte externe Schlüsselserver in einer MetroCluster Konfiguration modifiziert werden, empfiehlt NetApp nachdrücklich, in beiden Clustern dieselben Schlüsselserver zu verwenden.

Sekundäre Schlüsselserver ändern

Der `-secondary-key-servers`Parameter des `security key-manager external modify-server`Befehls dient zur Verwaltung sekundärer Schlüsselserver. Der `-secondary-key-servers`Parameter akzeptiert eine durch Kommas getrennte Liste. Die angegebene Reihenfolge der sekundären Schlüsselserver in der Liste bestimmt die Zugriffsreihenfolge für die sekundären Schlüsselserver. Die Zugriffsreihenfolge kann geändert werden, indem der Befehl `security key-manager external modify-server`mit einer anderen Reihenfolge der sekundären Schlüsselserver ausgeführt wird. Für sekundäre Schlüsselserver darf keine Portnummer angegeben werden.

> Wenn Sie den `security key-manager external modify-server` Befehl für die administrative SVM in einer MetroCluster Konfiguration ausführen, muss der Befehl auf beiden Clustern ausgeführt werden. Wenn Sie den Befehl für eine einzelne Daten-SVM ausführen, ist es nicht erforderlich, den Befehl auf beiden Clustern auszuführen.

Um einen sekundären Schlüsselserver zu entfernen, die Schlüsselserver, die beibehalten werden sollen, im `-secondary-key-servers` Parameter angeben und den zu entfernenden Server weglassen. Um alle sekundären Schlüsselserver zu entfernen, das Argument – verwenden, was bedeutet, dass keiner angegeben wird.

Primär- und Sekundärschlüsselserver konvertieren

Mit den folgenden Schritten lässt sich die Bezeichnung (primär oder sekundär) bestimmter Schlüsselserver ändern.

Einen primären Schlüsselserver in einen sekundären Schlüsselserver konvertieren

Schritte

1. Entfernung des primären Schlüsselservers aus der SVM:

   ```
   security key-manager external remove-servers
   ```

   > Wenn Sie den `security key-manager external remove-servers` Befehl für die administrative SVM in einer MetroCluster Konfiguration ausführen, muss der Befehl auf beiden Clustern ausgeführt werden. Wenn Sie den Befehl für eine einzelne Daten-SVM ausführen, ist es nicht erforderlich, den Befehl auf beiden Clustern auszuführen.

2. Das Einen gruppierten Schlüsselserver erstellenVerfahren wird unter Verwendung des ehemaligen primären Schlüsselservers als sekundärer Schlüsselserver durchgeführt.

Einen sekundären Schlüsselserver in einen primären Schlüsselserver umwandeln

Schritte

1. Entfernung des sekundären Schlüsselservers von seinem bestehenden primären Schlüsselserver:

   ```
   security key-manager external modify-server -secondary-key-servers
   ```

- Wenn Sie den `security key-manager external modify-server -secondary-key-servers` Befehl für die administrative SVM in einer MetroCluster Konfiguration ausführen, muss der Befehl auf beiden Clustern ausgeführt werden. Wenn Sie den Befehl für eine einzelne Daten-SVM ausführen, ist es nicht erforderlich, den Befehl auf beiden Clustern auszuführen.
- Wenn ein sekundärer Schlüsselserver in einen primären Schlüsselserver umgewandelt wird, während ein vorhandener Schlüsselserver entfernt wird, kann das Hinzufügen eines neuen Schlüsselservers vor Abschluss der Entfernung und Umwandlung zur Duplizierung von Schlüsseln führen.

1. Das Einen gruppierten Schlüsselserver erstellenVerfahren wird durchgeführt, wobei der ehemalige sekundäre Schlüsselserver als primärer Schlüsselserver des neuen Cluster-Schlüsselservers verwendet wird.

Weitere Informationen finden Sie unter [mod-secondary].

Verwandte Informationen

- Weitere Informationen zu `security key-manager external` finden Sie im "ONTAP-Befehlsreferenz"

Authentifizierungsschlüssel in ONTAP 9.6 und höher erstellen

Mit dem `security key-manager key create`Befehl lassen sich die Authentifizierungsschlüssel für einen Knoten erstellen und auf den konfigurierten KMIP-Servern speichern.

Über diese Aufgabe

Wenn Ihre Sicherheitskonfiguration die Verwendung unterschiedlicher Schlüssel für die Authentifizierung von Daten und die FIPS 140-2 Authentifizierung erfordert, sollte für jeden Zweck ein separater Schlüssel erstellt werden. Ist dies nicht der Fall, kann derselbe Authentifizierungsschlüssel für die FIPS-Konformität verwendet werden, der auch für den Datenzugriff genutzt wird.

ONTAP erstellt Authentifizierungsschlüssel für alle Knoten im Cluster.

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

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

- Sie erhalten eine Warnung, wenn die konfigurierten Schlüsselverwaltungsserver bereits mehr als 128 Authentifizierungsschlüssel speichern.
- Sie können den `security key-manager key delete`Befehl verwenden, um nicht verwendete Schlüssel zu löschen. Der `security key-manager key delete`Befehl schlägt fehl, wenn der angegebene Schlüssel derzeit von ONTAP verwendet wird. (Es sind höhere Berechtigungen als `admin` erforderlich, um diesen Befehl zu verwenden.)

> In einer MetroCluster Umgebung muss vor dem Löschen eines Schlüssels sichergestellt werden, dass der Schlüssel im Partnercluster nicht verwendet wird. Mit den folgenden Befehlen im Partnercluster lässt sich 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 Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Die Authentifizierungsschlüssel für Clusterknoten erstellen:

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

> Das Setzen von `prompt-for-key=true` bewirkt, dass das System den Clusteradministrator zur Eingabe der Passphrase auffordert, die bei der Authentifizierung verschlüsselter Laufwerke verwendet wird. Andernfalls generiert das System automatisch eine 32-Byte-Passphrase. Der `security key-manager key create` Befehl ersetzt den `security key-manager create-key` Befehl. Weitere Informationen zu `security key-manager key create` finden sich in der "ONTAP-Befehlsreferenz".

Das folgende Beispiel erstellt die Authentifizierungsschlüssel für `cluster1`, wobei automatisch eine 32-Byte-Passphrase generiert wird:

```
cluster1::> security key-manager key create
Key ID: <id_value>
```

2. Es sollte überprüft werden, ob die Authentifizierungsschlüssel erstellt wurden:

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

> Der `security key-manager key query` Befehl ersetzt den `security key-manager query key` Befehl.
>
> Die in der Ausgabe angezeigte Schlüssel-ID ist eine Kennung, die zur Referenzierung des Authentifizierungsschlüssels verwendet wird. Es handelt sich nicht um den eigentlichen Authentifizierungsschlüssel oder den Datenverschlüsselungsschlüssel.

Das folgende Beispiel überprüft, ob Authentifizierungsschlüssel für `cluster1` erstellt wurden:

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

Key Tag                                 Key Type  Restored
```

```
-----------------------------------  --------  --------
node1                                NSE-AK    yes
    Key ID: <id_value>
node1                                NSE-AK    yes
    Key ID: <id_value>

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                              Key Type  Restored
-----------------------------------  --------  --------
node2                                NSE-AK    yes
    Key ID: <id_value>
node2                                NSE-AK    yes
    Key ID: <id_value>
```

Weitere Informationen zu `security key-manager key query` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "storage encryption Disk anzeigen"

Authentifizierungsschlüssel in ONTAP 9.5 und früher erstellen

Mit dem `security key-manager create-key`Befehl lassen sich die Authentifizierungsschlüssel für einen Knoten erstellen und auf den konfigurierten KMIP-Servern speichern.

Über diese Aufgabe

Wenn Ihre Sicherheitskonfiguration die Verwendung unterschiedlicher Schlüssel für die Authentifizierung von Daten und die FIPS 140-2 Authentifizierung erfordert, sollte für jeden Zweck ein separater Schlüssel erstellt werden. Ist dies nicht der Fall, kann derselbe Authentifizierungsschlüssel für die FIPS-Konformität verwendet werden, der auch für den Datenzugriff genutzt wird.

ONTAP erstellt Authentifizierungsschlüssel für alle Knoten im Cluster.

- Dieser Befehl wird nicht unterstützt, wenn die Onboard-Schlüsselverwaltung aktiviert ist.
- Sie erhalten eine Warnung, wenn die konfigurierten Schlüsselverwaltungsserver bereits mehr als 128 Authentifizierungsschlüssel speichern.

  Sie können die Key-Management-Server-Software verwenden, um nicht verwendete Schlüssel zu löschen und dann den Befehl erneut auszuführen.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Die Authentifizierungsschlüssel für Clusterknoten erstellen:

`security key-manager create-key`

Weitere Informationen zu `security key-manager create-key` finden sich in der "ONTAP-Befehlsreferenz".

> Die in der Ausgabe angezeigte Schlüssel-ID ist eine Kennung, die zur Referenzierung des Authentifizierungsschlüssels verwendet wird. Es handelt sich nicht um den eigentlichen Authentifizierungsschlüssel oder den Datenverschlüsselungsschlüssel.

Das folgende Beispiel erstellt die Authentifizierungsschlüssel für `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: <id_value>

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. Es sollte überprüft werden, ob die Authentifizierungsschlüssel erstellt wurden:

`security key-manager query`

Weitere Informationen zu `security key-manager query` finden sich in der "ONTAP-Befehlsreferenz".

Das folgende Beispiel überprüft, ob Authentifizierungsschlüssel für `cluster1` erstellt wurden:

```
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: <id_value>


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

Key Tag        Key Type  Restored
-------------  --------  --------
cluster1-02    NSE-AK    yes
       Key ID: <id_value>
```

Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder ONTAP SED

Mit dem `storage encryption disk modify` Befehl lässt sich einem FIPS-Laufwerk oder SED ein Datenauthentifizierungsschlüssel zuweisen. Clusterknoten verwenden diesen Schlüssel, um verschlüsselte Daten auf dem Laufwerk zu sperren oder zu entsperren.

Über diese Aufgabe

Ein Self-Encrypting Drive ist nur dann vor unberechtigtem Zugriff geschützt, wenn seine Authentifizierungsschlüssel-ID auf einen Wert ungleich dem Standardwert gesetzt ist. Die Hersteller Secure ID (MSID) mit der Schlüssel-ID 0x0 ist der Standardwert für SAS-Laufwerke. Für NVMe-Laufwerke ist der Standardwert ein Nullschlüssel, dargestellt als leere Schlüssel-ID. Wird die Schlüssel-ID einem Self-Encrypting Drive zugewiesen, ändert das System dessen Authentifizierungsschlüssel-ID auf einen Wert ungleich dem Standardwert.

Dieses Verfahren ist nicht unterbrechend.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Einem FIPS-Laufwerk oder SED einen Authentifizierungsschlüssel für Daten zuweisen:

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

   Weitere Informationen zu `storage encryption disk modify` finden sich in der "ONTAP-Befehlsreferenz".

   > ⓘ Mit dem `security key-manager query -key-type NSE-AK` Befehl lassen sich die Schlüssel-IDs anzeigen.

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

   Info: Starting modify on 14 disks.
   ```

```
      View the status of the operation by using the
      storage encryption disk show-status command.
```

2. Überprüfen, ob die Authentifizierungsschlüssel zugewiesen wurden:

   `storage encryption disk show`

   Weitere Informationen zu `storage encryption disk show` finden sich in der "ONTAP-Befehlsreferenz".

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

Verwandte Informationen

- "storage encryption Disk anzeigen"
- "storage encryption disk show-status"

Onboard-Schlüsselverwaltung konfigurieren

Integrierte Schlüsselverwaltung in ONTAP 9.6 und höher aktivieren

Mit dem Onboard Key Manager können Clusterknoten gegenüber einem FIPS-Laufwerk oder SED authentifiziert werden. Der Onboard Key Manager ist ein integriertes Tool, das Authentifizierungsschlüssel für Knoten aus demselben Speichersystem bereitstellt wie Ihre Daten. Der Onboard Key Manager ist FIPS-140-2 Level 1-konform.

Mit dem Onboard Key Manager können Sie die Schlüssel sichern, die der Cluster für den Zugriff auf verschlüsselte Daten verwendet. Der Onboard Key Manager muss auf jedem Cluster aktiviert sein, der auf ein verschlüsseltes Volume oder eine selbstverschlüsselnde Festplatte zugreift.

Über diese Aufgabe

Sie müssen den `security key-manager onboard enable` Befehl jedes Mal ausführen, wenn Sie dem Cluster einen Knoten hinzufügen. In MetroCluster Konfigurationen müssen Sie `security key-manager onboard enable` zuerst auf dem lokalen Cluster und anschließend `security key-manager onboard sync` auf dem Remote-Cluster ausführen, wobei jeweils dieselbe Passphrase verwendet werden muss.

Weitere Informationen zu `security key-manager onboard enable` und `security key-manager onboard sync` finden sich in der "ONTAP-Befehlsreferenz".

Standardmäßig ist die Eingabe der Passphrase für den Schlüsselmanager beim Neustart eines Knotens nicht erforderlich. Außer bei MetroCluster kann die `cc-mode-enabled=yes` Option verwendet werden, um zu verlangen, dass Benutzer die Passphrase nach einem Neustart eingeben.

Wenn der Onboard Key Manager im Common Criteria-Modus aktiviert ist (`cc-mode-enabled=yes`, ändert sich das Systemverhalten wie folgt:

- Das System überwacht im Common Criteria-Modus aufeinanderfolgende fehlgeschlagene Cluster-Passphrasenversuche.

  Wenn NetApp Storage Encryption (NSE) aktiviert ist und die korrekte Cluster-Passphrase beim Systemstart nicht eingegeben wird, kann sich das System nicht an seinen Laufwerken authentifizieren und startet automatisch neu. Um dies zu korrigieren, ist die korrekte Cluster-Passphrase an der Boot-Eingabeaufforderung einzugeben. Nach dem Start erlaubt das System innerhalb eines Zeitraums von 24 Stunden bis zu 5 aufeinanderfolgende Versuche, die Cluster-Passphrase für jeden Befehl, der die Cluster-Passphrase als Parameter benötigt, korrekt einzugeben. Wird das Limit erreicht (zum Beispiel wenn die Cluster-Passphrase 5-mal hintereinander falsch eingegeben wurde), muss entweder das Ablaufintervall von 24 Stunden (Zeitüberschreitung) abgewartet oder der Node neu gestartet werden, um das Limit zurückzusetzen.

- Systemabbildaktualisierungen verwenden das NetApp RSA-3072-Codesignaturzertifikat zusammen mit SHA-384-codesignierten Digests zur Überprüfung der Abbildintegrität, anstelle des üblichen NetApp RSA-2048-Codesignaturzertifikats und SHA-256-codesignierten Digests.

  Der Upgrade-Befehl überprüft anhand verschiedener digitaler Signaturen, ob der Image-Inhalt verändert oder beschädigt wurde. Wenn die Validierung erfolgreich ist, geht das Image-Update zum nächsten Schritt über. Wenn die Validierung nicht erfolgreich ist, schlägt das Image-Update fehl. Weitere Informationen zu `cluster image` finden sich in der "ONTAP-Befehlsreferenz".

Der integrierte Schlüsselmanager speichert Schlüssel im flüchtigen Speicher. Der Inhalt des flüchtigen Speichers wird beim Neustart oder Anhalten des Systems gelöscht. Unter normalen Betriebsbedingungen wird der Inhalt des flüchtigen Speichers innerhalb von 30 Sekunden nach dem Anhalten des Systems gelöscht.

Bevor Sie beginnen

- Wenn Sie NSE mit einem externen Schlüsselverwaltungsserver (KMIP) verwenden, muss die externe Schlüsselverwaltungsdatenbank gelöscht worden sein.

  "Umstellung vom externen auf das integrierte Schlüsselmanagement"

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Die MetroCluster Umgebung muss konfiguriert werden, bevor der Onboard Key Manager konfiguriert wird.

Schritte

1. Starten Sie den Befehl zum Einrichten des Schlüsselmanagers:

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

   Setzen Sie `cc-mode-enabled=yes` so, dass Benutzer nach einem Neustart die Passphrase des Schlüsselmanagers eingeben müssen. Die `- cc-mode-enabled` Option wird in MetroCluster Konfigurationen nicht unterstützt. Der `security key-manager onboard enable` Befehl ersetzt den `security key-manager setup` Befehl.

Das folgende Beispiel startet den Befehl zur Einrichtung des Schlüsselmanagers auf cluster1, ohne dass die Passphrase nach jedem Neustart eingegeben werden muss:

2. Geben Sie eine Passphrase mit 32 bis 256 Zeichen ein oder für “cc-mode” eine Passphrase mit 64 bis 256 Zeichen.

> Ist die angegebene Passphrase für den “cc-mode” kürzer als 64 Zeichen, tritt eine Verzögerung von fünf Sekunden auf, bevor die Passphrase-Aufforderung im Rahmen der Schlüsselmanager-Einrichtung erneut angezeigt wird.

3. Bei der Aufforderung zur Passphrase-Bestätigung wird die Passphrase erneut eingegeben.
4. Überprüfen, ob das System die Authentifizierungsschlüssel erstellt:

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

> Der `security key-manager key query` Befehl ersetzt den `security key-manager query key` Befehl.

Weitere Informationen zu `security key-manager key query` finden sich in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

Die Passphrase sollte an einem sicheren Ort außerhalb des Speichersystems für die zukünftige Verwendung aufbewahrt werden.

Das System sichert wichtige Verwaltungsinformationen automatisch in der replizierten Datenbank (RDB) für den Cluster. Diese Informationen sollten für die Notfallwiederherstellung zusätzlich manuell gesichert werden.

Verwandte Informationen

- "Cluster Image-Befehle"
- "security key-manager external enable"
- "security key-manager key query"
- "security key-manager onboard enable"
- "Umstellung vom externen auf das integrierte Schlüsselmanagement"

Integrierte Schlüsselverwaltung in ONTAP 9.5 und früher aktivieren

Mit dem Onboard Key Manager können Clusterknoten gegenüber einem FIPS-Laufwerk oder SED authentifiziert werden. Der Onboard Key Manager ist ein integriertes Tool, das Authentifizierungsschlüssel für Knoten aus demselben Speichersystem bereitstellt wie Ihre Daten. Der Onboard Key Manager ist FIPS-140-2 Level 1-konform.

Mit dem Onboard Key Manager können Sie die Schlüssel sichern, die der Cluster für den Zugriff auf verschlüsselte Daten verwendet. Der Onboard Key Manager ist auf jedem Cluster zu aktivieren, der auf verschlüsselte Volumes oder selbstverschlüsselnde Datenträger zugreift.

Über diese Aufgabe

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

Bei einer MetroCluster Konfiguration gelten folgende Richtlinien:

- In ONTAP 9.5 muss `security key-manager setup` auf dem lokalen Cluster und `security key-manager setup -sync-metrocluster-config yes` auf dem Remote-Cluster ausgeführt werden, wobei auf beiden Clustern dieselbe Passphrase verwendet wird.
- Vor ONTAP 9.5 muss `security key-manager setup` auf dem lokalen Cluster ausgeführt werden, etwa 20 Sekunden gewartet werden und dann `security key-manager setup` auf dem Remote-Cluster ausgeführt werden, wobei jeweils die gleiche Passphrase verwendet wird.

Standardmäßig ist die Eingabe der Passphrase für den Schlüsselmanager beim Neustart eines Knotens nicht erforderlich. Ab ONTAP 9.4 kann die `-enable-cc-mode yes` Option verwendet werden, um zu verlangen, dass Benutzer die Passphrase nach einem Neustart eingeben.

Für NVE: Wenn `-enable-cc-mode yes` gesetzt ist, werden Volumes, die Sie mit den Befehlen `volume create` und `volume move start` erstellen, automatisch verschlüsselt. Für `volume create` muss `-encrypt true` nicht angegeben werden. Für `volume move start` muss `-encrypt-destination true` nicht angegeben werden.

Nach einem fehlgeschlagenen Passphrase-Versuch ist ein erneuter Neustart des Knotens erforderlich.

Bevor Sie beginnen

- Wenn Sie NSE mit einem externen Schlüsselverwaltungsserver (KMIP) verwenden, löschen Sie die externe Schlüsselverwaltungsdatenbank.

  "Umstellung vom externen auf das integrierte Schlüsselmanagement"

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Die MetroCluster Umgebung wird konfiguriert, bevor der Onboard Key Manager konfiguriert wird.

Schritte

1. Die Einrichtung des Schlüsselmanagers wird gestartet:

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

   Ab ONTAP 9.4 kann die `-enable-cc-mode yes` Option verwendet werden, um zu verlangen, dass Benutzer nach einem Neustart die Passphrase des Schlüsselmanagers eingeben. Für NVE: Wenn `-enable-cc-mode yes` gesetzt ist, werden Volumes, die Sie mit den Befehlen `volume create` und `volume move start` erstellen, automatisch verschlüsselt.

   Das folgende Beispiel zeigt den Beginn der Einrichtung des Schlüsselmanagers auf Cluster1, ohne dass die Passphrase nach jedem Neustart eingegeben werden muss:

   ```
   cluster1::> security key-manager setup
   Welcome to the key manager setup wizard, which will lead you through
   the steps to add boot information.

   ...
   ```

```
Would you like to use onboard key-management? {yes, no} [yes]:
Enter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
text>
```

2. Geben Sie `yes` an der Eingabeaufforderung ein, um die integrierte Schlüsselverwaltung zu konfigurieren.
3. Bei der Aufforderung zur Eingabe der Passphrase ist eine Passphrase mit 32 bis 256 Zeichen einzugeben, oder für “cc-mode” eine Passphrase mit 64 bis 256 Zeichen.

> ⓘ Ist die angegebene Passphrase für den “cc-mode” kürzer als 64 Zeichen, tritt eine Verzögerung von fünf Sekunden auf, bevor die Passphrase-Aufforderung im Rahmen der Schlüsselmanager-Einrichtung erneut angezeigt wird.

4. Bei der Aufforderung zur Passphrase-Bestätigung wird die Passphrase erneut eingegeben.
5. Überprüfen, ob die Schlüssel für alle Knoten konfiguriert sind:

   `security key-manager show-key-store`

   Weitere Informationen zu `security key-manager show-key-store` finden sich in der "ONTAP-Befehlsreferenz".

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

Node: node1
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK

Node: node2
Key Store: onboard
Key ID                                                           Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK
```

Nachdem Sie fertig sind

ONTAP sichert automatisch wichtige Verwaltungsinformationen in der replizierten Datenbank (RDB) für den Cluster.

Nachdem die Passphrase des Onboard Key Managers konfiguriert wurde, sollten die Informationen manuell an einem sicheren Ort außerhalb des Speichersystems gesichert werden. Siehe "Onboard-

Schlüsselverwaltungsinformationen manuell sichern".

Verwandte Informationen

- "Onboard-Schlüsselverwaltungsinformationen manuell sichern"
- "security key-manager setup"
- "security key-manager show-key-store"
- "Umstellung vom externen auf das integrierte Schlüsselmanagement"

Zuweisen eines Datenauthentifizierungsschlüssels zu einem FIPS-Laufwerk oder ONTAP SED

Mit dem `storage encryption disk modify` Befehl lässt sich einem FIPS-Laufwerk oder SED ein Datenauthentifizierungsschlüssel zuweisen. Clusterknoten verwenden diesen Schlüssel, um auf die Daten auf dem Laufwerk zuzugreifen.

Über diese Aufgabe

Ein Self-Encrypting Drive ist nur dann vor unberechtigtem Zugriff geschützt, wenn seine Authentifizierungsschlüssel-ID auf einen Wert ungleich dem Standardwert gesetzt ist. Die Hersteller Secure ID (MSID) mit der Schlüssel-ID 0x0 ist der Standardwert für SAS-Laufwerke. Für NVMe-Laufwerke ist der Standardwert ein Nullschlüssel, dargestellt als leere Schlüssel-ID. Wird die Schlüssel-ID einem Self-Encrypting Drive zugewiesen, ändert das System dessen Authentifizierungsschlüssel-ID auf einen Wert ungleich dem Standardwert.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Einem FIPS-Laufwerk oder SED einen Authentifizierungsschlüssel für Daten zuweisen:

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

   Weitere Informationen zu `storage encryption disk modify` finden sich in der "ONTAP-Befehlsreferenz".

   > ⓘ Mit dem `security key-manager key query -key-type NSE-AK` Befehl lassen sich die Schlüssel-IDs anzeigen.

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

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

   Weitere Informationen zu `security key-manager key query` finden sich in der "ONTAP-Befehlsreferenz".

2. Überprüfen, ob die Authentifizierungsschlüssel zugewiesen wurden:

```
storage encryption disk show
```

Weitere Informationen zu `storage encryption disk show` finden sich in der "ONTAP-Befehlsreferenz".

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

Verwandte Informationen

- "storage encryption Disk anzeigen"
- "storage encryption disk show-status"

Einem ONTAP FIPS-Laufwerk einen FIPS 140-2-Authentifizierungsschlüssel zuweisen

Sie können den `storage encryption disk modify` Befehl mit der `-fips-key-id` Option verwenden, um einem FIPS-Laufwerk einen FIPS 140-2 Authentifizierungsschlüssel zuzuweisen. Clusterknoten verwenden diesen Schlüssel für Laufwerksvorgänge, die nicht dem Datenzugriff dienen, wie zum Beispiel zur Verhinderung von Denial-of-Service-Angriffen auf das Laufwerk.

Über diese Aufgabe

Ihre Sicherheitskonfiguration erfordert möglicherweise die Verwendung unterschiedlicher Schlüssel für die Authentifizierung und die FIPS 140-2-Authentifizierung. Ist dies nicht der Fall, kann derselbe Authentifizierungsschlüssel für die FIPS-Konformität verwendet werden, der auch für den Datenzugriff genutzt wird.

Dieses Verfahren ist nicht unterbrechend.

Bevor Sie beginnen

Die Laufwerksfirmware muss die FIPS-140-2-Konformität unterstützen. Die "NetApp Interoperabilitätsmatrix-Tool" enthält Informationen zu unterstützten Laufwerksfirmwareversionen.

Schritte

1. Zunächst muss sichergestellt sein, dass ein Authentifizierungsschlüssel zugewiesen wurde. Dies kann mithilfe eines externer Schlüsselmanager oder eines Onboard Key Manager erfolgen. Die Zuweisung des Schlüssels lässt sich mit dem Befehl `storage encryption disk show` überprüfen.
2. Einem FIPS 140-2-Authentifizierungsschlüssel SEDs zuweisen:

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

   Mit dem `security key-manager query` Befehl lassen sich die Schlüssel-IDs anzeigen.

```
cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
<id_value>

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

3. Es sollte überprüft werden, ob der Authentifizierungsschlüssel zugewiesen wurde:

   `storage encryption disk show -fips`

   Weitere Informationen zu `storage encryption disk show` finden sich in der "ONTAP-Befehlsreferenz".

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

Verwandte Informationen

- "Speicherverschlüsselung Festplatte ändern"
- "storage encryption Disk anzeigen"
- "storage encryption disk show-status"

Clusterweiten FIPS-konformen Modus für KMIP-Verbindungen in ONTAP aktivieren

Sie können den `security config modify` Befehl mit der `-is-fips-enabled` Option verwenden, um den clusterweiten FIPS-konformen Modus für Daten während der Übertragung zu aktivieren. Dadurch verwendet der Cluster OpenSSL im FIPS-Modus, wenn eine Verbindung zu KMIP-Servern besteht.

Über diese Aufgabe

Wenn der clusterweite FIPS-konforme Modus aktiviert ist, verwendet der Cluster automatisch ausschließlich TLS 1.2 und FIPS-validierte Cipher Suites. Der clusterweite FIPS-konforme Modus ist standardmäßig deaktiviert.

Nach der Änderung der clusterweiten Sicherheitskonfiguration ist ein manueller Neustart der Clusterknoten erforderlich.

Bevor Sie beginnen

- Der Speichercontroller 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 herzustellen, wenn der clusterweite FIPS-konforme Modus aktiviert ist.

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Überprüfen, ob TLSv1.2 unterstützt wird:

   ```
   security config show -supported-protocols
   ```

   Weitere Informationen zu `security config show` finden sich in der "ONTAP-Befehlsreferenz".

   ```
   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. Clusterweiter FIPS-konformer Modus:

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

   Weitere Informationen zu `security config modify` finden sich in der "ONTAP-Befehlsreferenz".

4. Cluster-Knoten manuell neu starten.
5. Es sollte überprüft werden, ob der clusterweite FIPS-konforme 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
   ```

Verwaltung der NetApp Verschlüsselung

Volumendaten in ONTAP entschlüsseln

Der `volume move start` Befehl kann verwendet werden, um Volumendaten zu verschieben und zu entschlüsseln.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Ein vorhandenes verschlüsseltes Volume verschieben und die Daten auf dem Volume entschlüsseln:

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

   Weitere Informationen zu `volume move start` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl verschiebt ein vorhandenes Volume mit dem Namen `vol1` in das Zielaggregat `aggr3` und entschlüsselt 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 sind unverschlüsselt.

2. Es sollte überprüft werden, ob die Verschlüsselung des Volumes deaktiviert ist:

   `volume show -encryption`

   Weitere Informationen zu `volume show` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl zeigt an, ob Volumes auf `cluster1`verschlüsselt sind:

   ```
   cluster1::> volume show -encryption

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

Verschieben eines verschlüsselten Volumes in ONTAP

Sie können den `volume move start` Befehl verwenden, um ein verschlüsseltes Volume zu verschieben. Das verschobene Volume kann sich auf demselben Aggregat oder auf einem anderen Aggregat befinden.

Über diese Aufgabe

Der Vorgang schlägt fehl, wenn der Zielknoten oder das Zielvolume die Volume-Verschlüsselung nicht unterstützt.

Die `-encrypt-destination`Option für `volume move start` ist bei verschlüsselten Volumes standardmäßig aktiviert. Die Anforderung, explizit anzugeben, dass das Zielvolume nicht verschlüsselt werden soll, stellt sicher, dass die Daten auf dem Volume nicht versehentlich entschlüsselt werden.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Ein vorhandenes verschlüsseltes Volume kann verschoben werden, wobei die Daten auf dem Volume verschlüsselt bleiben:

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

   Weitere Informationen zu `volume move start` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl verschiebt ein vorhandenes Volume mit dem Namen `vol1` in das Zielaggregat `aggr3` und lässt die Daten auf dem Volume verschlüsselt:

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

2. Es sollte überprüft werden, ob das Volume für die Verschlüsselung aktiviert ist:

   `volume show -is-encrypted true`

   Weitere Informationen zu `volume show` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl zeigt die verschlüsselten Volumes auf `cluster1` an:

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

   Vserver  Volume  Aggregate  State  Type  Size  Available  Used
   -------  ------  ---------  -----  ----  -----  ---------  ----
   vs1      vol1    aggr3     online    RW  200GB    160.0GB  20%
   ```

Änderung des Verschlüsselungsschlüssels für ein ONTAP Volume

Es gilt als bewährte Sicherheitsmaßnahme, den Verschlüsselungsschlüssel eines Volumes regelmäßig zu ändern. Ab ONTAP 9.3 kann der Verschlüsselungsschlüssel mit dem `volume encryption rekey start` Befehl geändert werden.

Über diese Aufgabe

Sobald Sie einen Schlüsselerneuerungsvorgang starten, muss dieser abgeschlossen werden. Eine Rückkehr

zum alten Schlüssel ist nicht möglich. Wenn während des Vorgangs Leistungsprobleme auftreten, kann der Vorgang mit dem `volume encryption rekey pause` Befehl angehalten und mit dem `volume encryption rekey resume` Befehl fortgesetzt werden.

Bis zum Abschluss der Neuverschlüsselung verfügt das Volume über zwei Schlüssel. Neue Schreibvorgänge und die zugehörigen Lesevorgänge verwenden den neuen Schlüssel. Andernfalls verwenden Lesevorgänge den alten Schlüssel.

> Es ist nicht möglich, mit `volume encryption rekey start` ein SnapLock Volume neu zu verschlüsseln.

Schritte

1. Ändern eines Verschlüsselungsschlüssels:

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

   Der folgende Befehl ändert den Verschlüsselungsschlüssel für `vol1` auf SVM `vs1`:

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

2. Status des Schlüsselerneuerungsvorgangs überprüfen:

   `volume encryption rekey show`

   Weitere Informationen zu `volume encryption rekey show` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl zeigt den Status des Rekey-Vorgangs an:

   ```
   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. Nach Abschluss der Schlüsselerneuerung kann überprüft werden, ob das Volume für die Verschlüsselung aktiviert ist:

   `volume show -is-encrypted true`

   Weitere Informationen zu `volume show` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl zeigt die verschlüsselten Volumes auf `cluster1` an:

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

   Vserver  Volume  Aggregate  State  Type  Size  Available  Used
   ```

```
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2      online    RW  200GB    160.0GB  20%
```

Änderung des Verschlüsselungsschlüssels für ein ONTAP Volume

Es gilt als bewährte Sicherheitsmaßnahme, den Verschlüsselungsschlüssel eines Volumes regelmäßig zu ändern. Der `volume move start` Befehl kann zum Ändern des Verschlüsselungsschlüssels verwendet werden. Das verschobene Volume kann sich auf demselben Aggregat oder auf einem anderen Aggregat befinden.

Über diese Aufgabe

Sie können `volume move start`nicht verwenden, um ein SnapLock- oder FlexGroup-Volumen neu zu verschlüsseln.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Ein vorhandenes Volume verschieben und den Verschlüsselungsschlüssel ändern:

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

   Weitere Informationen zu `volume move start` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl verschiebt ein vorhandenes Volume mit dem Namen **`vol1`** in 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. Es sollte überprüft werden, ob das Volume für die Verschlüsselung aktiviert ist:

   `volume show -is-encrypted true`

   Weitere Informationen zu `volume show` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl zeigt die verschlüsselten Volumes auf `cluster1` an:

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

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

Rotation von Authentifizierungsschlüsseln für NetApp Storage Encryption in ONTAP

Die Authentifizierungsschlüssel können bei Verwendung von NetApp Storage Encryption (NSE) rotiert werden.

Über diese Aufgabe

Die Rotation von Authentifizierungsschlüsseln in einer NSE-Umgebung wird unterstützt, wenn der External Key Manager (KMIP) verwendet wird.

> Die Rotation von Authentifizierungsschlüsseln in einer NSE-Umgebung wird für Onboard Key Manager (OKM) nicht unterstützt.

Schritte

1. Mit dem `security key-manager create-key` Befehl werden neue Authentifizierungsschlüssel generiert.

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

2. Mit dem `storage encryption disk modify -disk * -data-key-id`Befehl lassen sich die Authentifizierungsschlüssel ändern.

Verwandte Informationen

- "Speicherverschlüsselung Festplatte ändern"

Löschen eines verschlüsselten Volumes in ONTAP

Mit dem `volume delete` Befehl lässt sich ein verschlüsseltes Volume löschen.

Bevor Sie beginnen

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Das Volume muss offline sein.

Schritt

1. Löschen eines verschlüsselten Volumes:

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

   Weitere Informationen zu `volume delete` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl löscht ein verschlüsseltes Volume mit dem Namen `vol1`:

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

   Geben Sie `yes` ein, wenn Sie zur Bestätigung der Löschung aufgefordert werden.

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

Verwenden Sie `volume delete` mit der `-force true` Option, um ein Volume zu löschen und den entsprechenden Verschlüsselungsschlüssel sofort zu zerstören. Dieser Befehl erfordert erweiterte Berechtigungen. Weitere Informationen zu `volume delete` finden sich in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

Mit dem `volume recovery-queue` Befehl kann ein gelöschtes Volume während der Aufbewahrungsfrist nach Ausführung des `volume delete` Befehls wiederhergestellt werden:

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

"Verwendung der Volume Recovery Funktion"

Daten auf einem verschlüsselten Volume sicher löschen

Informationen zum sicheren Löschen von Daten aus einem verschlüsselten ONTAP Volume

Ab ONTAP 9.4 kann die Funktion „Secure Purge“ verwendet werden, um Daten auf NVE-fähigen Volumes unterbrechungsfrei zu löschen. Das Löschen von Daten auf einem verschlüsselten Volume stellt sicher, dass diese nicht vom physischen Medium wiederhergestellt werden können, zum Beispiel in Fällen von „Spillage“, bei denen Datenspuren beim Überschreiben von Blöcken zurückgeblieben sein könnten, oder um die Daten eines ausscheidenden Mandanten sicher zu löschen.

Die sichere Löschung funktioniert nur für zuvor gelöschte Dateien auf NVE-fähigen Volumes. Ein unverschlüsseltes Volume kann nicht bereinigt werden. Es sind KMIP-Server zur Bereitstellung der Schlüssel zu verwenden, nicht der integrierte Schlüsselmanager.

Überlegungen zur Verwendung von Secure Purge

- Volumes, die in einem für NetApp Aggregate Encryption (NAE) aktivierten Aggregat erstellt wurden, unterstützen kein sicheres Löschen.
- Die sichere Löschung funktioniert nur für zuvor gelöschte Dateien auf NVE-fähigen Volumes.
- Ein unverschlüsseltes Volume kann nicht bereinigt werden.
- Es sind KMIP-Server zur Bereitstellung der Schlüssel zu verwenden, nicht der integrierte Schlüsselmanager.

Die Secure Purge Funktion arbeitet je nach Ihrer ONTAP Version unterschiedlich.

ONTAP 9.8 und höher

- Secure Purge wird von MetroCluster und FlexGroup unterstützt.
- Wenn das zu löschende Volume die Quelle einer SnapMirror Beziehung ist, muss die SnapMirror Beziehung nicht getrennt werden, um eine sichere Löschung durchzuführen.
- Die Methode zur erneuten Verschlüsselung unterscheidet sich für Volumes mit SnapMirror Datenschutz im Vergleich zu Volumes ohne SnapMirror Datenschutz (DP) oder solchen mit SnapMirror erweiterter Datenschutzfunktion.
  - Standardmäßig werden Daten auf Volumes, die den SnapMirror Datenschutzmodus (DP) verwenden, mithilfe der Volume Move Re-Verschlüsselungsmethode erneut verschlüsselt.
  - Standardmäßig verwenden Volumes, die keinen SnapMirror Datenschutz verwenden, oder

Volumes, die den SnapMirror erweiterten Datenschutzmodus (XDP) verwenden, die Methode der direkten Neuverschlüsselung.

  - Diese Standardeinstellungen können mit dem `secure purge re-encryption-method [volume-move|in-place-rekey]` Befehl geändert werden.

- Standardmäßig werden alle Snapshots in FlexVol Volumes während der sicheren Bereinigung automatisch gelöscht. Standardmäßig werden Snapshots in FlexGroup Volumes und Volumes, die SnapMirror Datenschutz verwenden, während der sicheren Bereinigung nicht automatisch gelöscht. Diese Standardeinstellungen können mit dem `secure purge delete-all-snapshots [true|false]` Befehl geändert werden.

ONTAP 9.7 und früher:

- Die sichere Bereinigung unterstützt die folgenden Funktionen nicht:
  - FlexClone
  - SnapVault
  - FabricPool
- Wenn das zu löschende Volumen die Quelle einer SnapMirror Beziehung ist, muss die SnapMirror Beziehung getrennt werden, bevor das Volumen gelöscht werden kann.

  Wenn sich im Volume belegte Snapshots befinden, müssen die Snapshots freigegeben werden, bevor das Volume gelöscht werden kann. Beispielsweise kann es erforderlich sein, ein FlexClone Volume von seinem übergeordneten Volume zu trennen.

- Das erfolgreiche Aufrufen der Funktion „secure-purge“ löst eine Volume-Verschiebung aus, bei der die verbleibenden, nicht gelöschten Daten mit einem neuen Schlüssel neu verschlüsselt werden.

  Das verschobene Volume verbleibt auf dem aktuellen Aggregat. Der alte Schlüssel wird automatisch gelöscht, wodurch sichergestellt wird, dass gelöschte Daten nicht vom Speichermedium wiederhergestellt werden können.

Verschlüsselte Daten aus einem ONTAP Volume ohne SnapMirror entfernen

Ab ONTAP 9.4 kann secure-purge verwendet werden, um Daten auf NVE-fähigen Volumes unterbrechungsfrei zu „scrubben“.

Über diese Aufgabe

Die sichere Löschung kann je nach Datenmenge in den gelöschten Dateien einige Minuten bis mehrere Stunden dauern. Der Status des Vorgangs kann mit dem `volume encryption secure-purge show` Befehl angezeigt werden. Der Vorgang kann mit dem `volume encryption secure-purge abort` Befehl beendet werden.

> Um eine sichere Bereinigung auf einem SAN-Host durchzuführen, müssen Sie entweder die gesamte LUN löschen, die die Dateien enthält, die Sie bereinigen möchten, oder Sie müssen in der Lage sein, in der LUN für die Blöcke, die zu den Dateien gehören, die Sie bereinigen möchten, Löcher zu schlagen. Wenn Sie die LUN nicht löschen können oder Ihr Host-Betriebssystem das Schlagen von Löchern in der LUN nicht unterstützt, kann eine sichere Bereinigung nicht durchgeführt werden.

Bevor Sie beginnen

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

Schritte

1. Die Dateien oder die LUN, die sicher gelöscht werden sollen, löschen.
   - Auf einem NAS-Client die Dateien löschen, die Sie sicher entfernen möchten.
   - Auf einem SAN-Host die LUN löschen, die Sie sicher bereinigen möchten, oder Löcher in die LUN für die Blöcke stanzen, die zu den Dateien gehören, die Sie bereinigen möchten.
2. Im Speichersystem zur erweiterten Berechtigungsstufe wechseln:

   ```
   set -privilege advanced
   ```

3. Wenn sich die Dateien, die Sie sicher löschen möchten, in Snapshots befinden, löschen Sie die Snapshots:

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

4. Gelöschte Dateien sicher löschen:

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

   Der folgende Befehl entfernt die gelöschten Dateien sicher von `vol1` auf SVM `vs1`:

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

5. Status des Secure-Purge-Vorgangs überprüfen:

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

Bereinigung verschlüsselter Daten aus einem ONTAP Volume mit asynchronem SnapMirror

Ab ONTAP 9.8 kann ein sicherer Bereinigungsvorgang verwendet werden, um Daten auf NVE-fähigen Volumes mit einer SnapMirror asynchronen Beziehung unterbrechungsfrei zu „scrubben“.

Bevor Sie beginnen

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

Über diese Aufgabe

Die sichere Löschung kann je nach Datenmenge in den gelöschten Dateien einige Minuten bis mehrere Stunden dauern. Der Status des Vorgangs kann mit dem `volume encryption secure-purge show` Befehl angezeigt werden. Der Vorgang kann mit dem `volume encryption secure-purge abort` Befehl beendet werden.



Um eine sichere Bereinigung auf einem SAN-Host durchzuführen, müssen Sie entweder die gesamte LUN löschen, die die Dateien enthält, die Sie bereinigen möchten, oder Sie müssen in der Lage sein, in der LUN für die Blöcke, die zu den Dateien gehören, die Sie bereinigen möchten, Löcher zu schlagen. Wenn Sie die LUN nicht löschen können oder Ihr Host-

> Betriebssystem das Schlagen von Löchern in der LUN nicht unterstützt, kann eine sichere Bereinigung nicht durchgeführt werden.

Schritte

1. Im Speichersystem zur erweiterten Berechtigungsstufe wechseln:

   ```
   set -privilege advanced
   ```

2. Die Dateien oder die LUN, die sicher gelöscht werden sollen, löschen.
   - Auf einem NAS-Client die Dateien löschen, die Sie sicher entfernen möchten.
   - Auf einem SAN-Host die LUN löschen, die Sie sicher bereinigen möchten, oder Löcher in die LUN für die Blöcke stanzen, die zu den Dateien gehören, die Sie bereinigen möchten.
3. Das Zielvolume in der asynchronen Beziehung wird für die sichere Löschung vorbereitet:

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

   Diesen Schritt bei jedem Volume in Ihrer SnapMirror asynchronen Beziehung wiederholen.

4. Wenn sich die Dateien, die Sie sicher löschen möchten, in Snapshots befinden, löschen Sie die Snapshots:

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

5. Wenn sich die Dateien, die Sie sicher löschen möchten, in den Basis-Snapshots befinden, ist Folgendes zu tun:

   a. Einen Snapshot auf dem Quellvolume in der SnapMirror asynchronen Beziehung erstellen:

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

   b. Die SnapMirror Beziehung wird aktualisiert, um den Basissnapshot auf das Ziel zu verschieben:

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

   Diesen Schritt für jedes Volume in der SnapMirror asynchronen Beziehung wiederholen.

   a. Die Schritte (a) und (b) werden so oft wiederholt, wie es Basis-Snapshots plus eins gibt.

      Wenn Sie beispielsweise zwei Basis-Snapshots haben, sollten die Schritte (a) und (b) dreimal wiederholt werden.

   b. Es sollte überprüft werden, ob der Basis-Snapshot vorhanden ist:
      `snapshot show -vserver SVM_name -volume volume_name`

   c. Den Basis-Snapshot löschen:
      `snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot`

6. Gelöschte Dateien sicher löschen:

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

Dieser Schritt ist für jedes Volume in der SnapMirror asynchronen Beziehung zu wiederholen.

Der folgende Befehl entfernt die gelöschten Dateien auf “vol1” auf SVM “vs1” sicher:

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

7. Status des sicheren Löschvorgangs überprüfen:

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

Verwandte Informationen

- "SnapMirror update"

Verschlüsselte Daten aus einem ONTAP Volume mit synchronem SnapMirror bereinigen

Ab ONTAP 9.8 ist es möglich, mit einer sicheren Bereinigung Daten auf NVE-fähigen Volumes mit einer SnapMirror synchronen Beziehung unterbrechungsfrei zu „bereinigen“.

Über diese Aufgabe

Eine sichere Datenlöschung kann je nach Datenmenge in den gelöschten Dateien einige Minuten bis mehrere Stunden dauern. Der Status des Vorgangs kann mit dem `volume encryption secure-purge show` Befehl angezeigt werden. Der Vorgang kann mit dem `volume encryption secure-purge abort` Befehl beendet werden.

> Um eine sichere Bereinigung auf einem SAN-Host durchzuführen, müssen Sie entweder die gesamte LUN löschen, die die Dateien enthält, die Sie bereinigen möchten, oder Sie müssen in der Lage sein, in der LUN für die Blöcke, die zu den Dateien gehören, die Sie bereinigen möchten, Löcher zu schlagen. Wenn Sie die LUN nicht löschen können oder Ihr Host-Betriebssystem das Schlagen von Löchern in der LUN nicht unterstützt, kann eine sichere Bereinigung nicht durchgeführt werden.

Bevor Sie beginnen

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

Schritte

1. Im Speichersystem zur erweiterten Berechtigungsstufe wechseln:

```
set -privilege advanced
```

2. Die Dateien oder die LUN, die sicher gelöscht werden sollen, löschen.
   - Auf einem NAS-Client die Dateien löschen, die Sie sicher entfernen möchten.
   - Auf einem SAN-Host die LUN löschen, die Sie sicher bereinigen möchten, oder Löcher in die LUN für die Blöcke stanzen, die zu den Dateien gehören, die Sie bereinigen möchten.
3. Das Zielvolume in der asynchronen Beziehung wird für die sichere Löschung vorbereitet:

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

Diesen Schritt für das andere Volume in Ihrer SnapMirror synchronen Beziehung wiederholen.

4. Wenn sich die Dateien, die Sie sicher löschen möchten, in Snapshots befinden, löschen Sie die Snapshots:

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

5. Befindet sich die sichere Löschdatei im Basis- oder gemeinsamen Snapshot, wird die SnapMirror Beziehung aktualisiert, um den gemeinsamen Snapshot voranzubewegen:

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

   Es gibt zwei gemeinsame Snapshots, daher muss dieser Befehl zweimal ausgeführt werden.

6. Befindet sich die sichere Löschdatei im applikationskonsistenten Snapshot, wird der Snapshot auf beiden Volumes in der SnapMirror synchronen Beziehung gelöscht:

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

   Führen Sie diesen Schritt auf beiden Volumes durch.

7. Gelöschte Dateien sicher löschen:

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

   Dieser Schritt ist für jedes Volume in der SnapMirror synchronen Beziehung zu wiederholen.

   Der folgende Befehl entfernt die gelöschten Dateien auf “vol1” auf SVM “vs1” sicher und unwiderruflich.

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

8. Status des sicheren Löschvorgangs überprüfen:

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

Verwandte Informationen

- "SnapMirror update"

Die Passphrase für die ONTAP Onboard-Schlüsselverwaltung ändern

NetApp empfiehlt, die Passphrase für die integrierte Schlüsselverwaltung regelmäßig zu ändern. Die neue Passphrase muss an einem sicheren Ort außerhalb des Speichersystems aufbewahrt werden.

Bevor Sie beginnen

- Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.
- Sie müssen die aktuelle Passphrase für die Onboard Schlüsselverwaltung eingeben, bevor Sie eine neue

Passphrase festlegen können.

- In einer MetroCluster Umgebung wird nach der Aktualisierung der Passphrase auf dem lokalen Cluster die Passphrase-Aktualisierung auf dem Partnercluster synchronisiert.

Schritte

1. Wechsel zum erweiterten Berechtigungslevel:

   ```
   set -privilege advanced
   ```

2. Ändern der Passphrase für die integrierte Schlüsselverwaltung. Der verwendete Befehl hängt von der ONTAP-Version ab, die ausgeführt wird.

   Nachdem Sie den Befehl eingegeben haben, antworten Sie auf die Aufforderungen, um die aktuelle Passphrase, die neue Passphrase und zur Bestätigung erneut die neue Passphrase einzugeben.

   ONTAP 9.6 und höher

   ```
   security key-manager onboard update-passphrase
   ```

   ONTAP 9.5 und früher

   ```
   security key-manager update-passphrase
   ```

3. Wenn Sie dazu aufgefordert werden, geben Sie die aktuelle Passphrase ein.
4. Geben Sie eine neue Passphrase mit 32 bis 256 Zeichen ein oder für “cc-mode” eine Passphrase mit 64 bis 256 Zeichen.

   Ist die angegebene Passphrase für den “cc-mode” kürzer als 64 Zeichen, tritt eine Verzögerung von fünf Sekunden auf, bevor die Passphrase-Aufforderung im Rahmen der Schlüsselmanager-Einrichtung erneut angezeigt wird.

5. An der Aufforderung zur Bestätigung der Passphrase ist die neue Passphrase erneut einzugeben.
6. Wenn Sie sich in einer MetroCluster Konfiguration befinden, sollte die aktualisierte Passphrase auf dem Partnercluster synchronisiert werden.
   a. Die Passphrase auf dem Partnercluster wird synchronisiert, indem der richtige Befehl für die jeweilige ONTAP Version ausgewählt wird:

      ONTAP 9.6 und höher

      ```
      security key-manager onboard sync
      ```

      ONTAP 9.5 und früher

      - In ONTAP 9.5 führen Sie Folgendes aus:

        ```
        security key-manager setup -sync-metrocluster-config
        ```

      - In ONTAP 9.4 und früheren Versionen sollte nach der Aktualisierung der Passphrase auf dem lokalen Cluster 20 Sekunden gewartet werden, bevor der folgende Befehl auf dem Partnercluster ausgeführt wird:

        ```
        security key-manager setup
        ```

b. Geben Sie die neue Passphrase ein, wenn Sie dazu aufgefordert werden.

   Für beide Cluster muss dieselbe Passphrase verwendet werden.

Nachdem Sie fertig sind

Die Passphrase für die integrierte Schlüsselverwaltung sollte an einem sicheren Ort außerhalb des Speichersystems für die zukünftige Verwendung aufbewahrt werden.

Schlüsselverwaltungsinformationen sollten manuell gesichert werden, sobald die Passphrase für die integrierte Schlüsselverwaltung geändert wird.

Verwandte Informationen

- "Onboard-Schlüsselverwaltungsinformationen manuell sichern"
- "security key-manager onboard update-passphrase"

ONTAP Onboard-Schlüsselverwaltungsinformationen manuell sichern

Sie sollten die Onboard Key Management-Informationen immer dann an einem sicheren Ort außerhalb des Speichersystems speichern, wenn Sie die Passphrase des Onboard Key Manager konfigurieren.

Bevor Sie beginnen

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.

Über diese Aufgabe

Alle Schlüsselverwaltungsinformationen werden automatisch in der replizierten Datenbank (RDB) des Clusters gesichert. Schlüsselverwaltungsinformationen sollten zusätzlich manuell gesichert werden, um sie im Katastrophenfall verwenden zu können.

Schritte

1. Wechsel zum erweiterten Berechtigungslevel:

   ```
   set -privilege advanced
   ```

2. Die Sicherungsinformationen für die Schlüsselverwaltung des Clusters anzeigen:

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

   Der folgende 9.6-Befehl zeigt die Sicherungsinformationen für die Schlüsselverwaltung für `cluster1` an:

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

     ------------------------BEGIN BACKUP-------------------------
     TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAADuD+byAAAAACEAAAAAAAAA
     QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
```

```
dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
IgAAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
QRHwv+1aWvAAAAAAAAAACQAAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

verwenden. Weitere Details finden sich unter "Übergang von externer Schlüsselverwaltung zur ONTAP internen Schlüsselverwaltung".

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

> Wenn Sie NSE auf einem System mit Flash Cache Modul verwenden, sollten Sie auch NVE oder NAE aktivieren. NSE verschlüsselt keine Daten, die sich auf dem Flash Cache Modul befinden.

ONTAP 9.6 und höher

> Wenn ONTAP 9.8 oder höher verwendet wird und das Root-Volume verschlüsselt ist, ist die Vorgehensweise für ONTAP 9.8 oder höher mit verschlüsseltem Root-Volume zu befolgen.

1. Überprüfen, ob der Schlüssel wiederhergestellt werden muss:
   `security key-manager key query -node node`

   Weitere Informationen zu `security key-manager key query` finden sich in der "ONTAP-Befehlsreferenz".

2. Schlüssel wiederherstellen:
   `security key-manager onboard sync`

   Weitere Informationen zu `security key-manager onboard sync` finden sich in der "ONTAP-Befehlsreferenz".

3. An der Passphrase-Aufforderung die Passphrase für die integrierte Schlüsselverwaltung des Clusters eingeben.

ONTAP 9.8 oder höher mit verschlüsseltem Root-Volume

Wenn Sie ONTAP 9.8 oder höher verwenden und Ihr Root-Volume verschlüsselt ist, muss über das Bootmenü eine Wiederherstellungs-Passphrase für die Onboard-Schlüsselverwaltung festgelegt werden. Dieser Vorgang ist auch erforderlich, wenn ein Bootmedium ersetzt wird.

1. Den Knoten zum Bootmenü starten und Option `(10) Set onboard key management recovery secrets` auswählen.
2. Geben Sie `y` ein, um diese Option zu verwenden.
3. An der Eingabeaufforderung ist die Passphrase für die Onboard-Schlüsselverwaltung des Clusters einzugeben.
4. An der Eingabeaufforderung die Sicherungsschlüsseldaten eingeben.

   Nach Eingabe der Sicherungsschlüsseldaten kehrt der Knoten zum Bootmenü zurück.

5. Im Bootmenü die Option `(1) Normal Boot` auswählen.

ONTAP 9.5 und früher

1. Überprüfen, ob der Schlüssel wiederhergestellt werden muss:
   `security key-manager key show`
2. Schlüssel wiederherstellen:

`security key-manager setup -node node`

Weitere Informationen zu `security key-manager setup` finden sich in der "ONTAP-Befehlsreferenz".

3. An der Passphrase-Aufforderung die Passphrase für die integrierte Schlüsselverwaltung des Clusters eingeben.

Wiederherstellung der ONTAP externen Schlüsselverwaltungs-Verschlüsselungsschlüssel

Sie können Verschlüsselungsschlüssel für die externe Schlüsselverwaltung manuell wiederherstellen und auf einen anderen Knoten übertragen. Dies kann sinnvoll sein, wenn ein Knoten neu gestartet wird, der zum Zeitpunkt der Erstellung der Schlüssel für den Cluster vorübergehend ausgefallen war.

Über diese Aufgabe

In ONTAP 9.6 und höher kann mit dem `security key-manager key query -node node_name` Befehl überprüft werden, ob Ihr Schlüssel wiederhergestellt werden muss.

In ONTAP 9.5 und früher können Sie den `security key-manager key show` Befehl verwenden, um zu überprüfen, ob Ihr Schlüssel wiederhergestellt werden muss.

> Wenn Sie NSE auf einem System mit Flash Cache Modul verwenden, sollten Sie auch NVE oder NAE aktivieren. NSE verschlüsselt keine Daten, die sich auf dem Flash Cache Modul befinden.

Weitere Informationen zu `security key-manager key query` finden sich in der "ONTAP-Befehlsreferenz".

Bevor Sie beginnen

Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Wenn Sie ONTAP 9.8 oder höher verwenden und Ihr Root-Volume verschlüsselt ist, führen Sie Folgendes aus:

   Wenn ONTAP 9.7 oder eine frühere Version verwendet wird oder wenn ONTAP 9.8 oder eine neuere Version verwendet wird und das Root-Volume nicht verschlüsselt ist, kann dieser Schritt übersprungen werden.

   a. Bootargumente festlegen:
   ```
   setenv kmip.init.ipaddr <ip-address>
   setenv kmip.init.netmask <netmask>
   setenv kmip.init.gateway <gateway>
   setenv kmip.init.interface e0M
   boot_ontap
   ```

   b. Den Knoten zum Bootmenü starten und Option `(11) Configure node for external key management` auswählen.

   c. Den Anweisungen zum Eingeben des Managementzertifikats folgen.

Nach Eingabe aller Managementzertifikatsinformationen kehrt das System zum Bootmenü zurück.

d. Im Bootmenü die Option `(1) Normal Boot` auswählen.

2. Stellen Sie den Schlüssel wieder her:

Für diese ONTAP Version…	Verwenden Sie diesen 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`Standardmäßig gilt dies für alle Knoten.

Dieser Befehl wird nicht unterstützt, wenn die Onboard-Schlüsselverwaltung aktiviert ist.

Der folgende ONTAP 9.6 Befehl stellt die Authentifizierungsschlüssel für das externe Schlüsselmanagement auf allen Knoten in `cluster1`wieder her:

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

Verwandte Informationen

- "security key-manager external restore"

KMIP SSL-Zertifikate auf dem ONTAP Cluster ersetzen

Alle SSL-Zertifikate haben ein Ablaufdatum. Die Zertifikate müssen vor ihrem Ablauf aktualisiert werden, um den Verlust des Zugriffs auf Authentifizierungsschlüssel zu verhindern.

Bevor Sie beginnen

- Das Ersatz-Public-Zertifikat und der Ersatz-Private-Key für den Cluster (KMIP-Client-Zertifikat) müssen vorliegen.
- Sie müssen das Ersatzzertifikat für den KMIP-Server (KMIP-Server-CA-Zertifikat) erhalten haben.
- Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.
- Wenn Sie die KMIP-SSL-Zertifikate in einer MetroCluster Umgebung ersetzen, müssen Sie auf beiden Clustern dasselbe Ersatz-KMIP-SSL-Zertifikat installieren.

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

Schritte

1. Das neue KMIP Server-CA-Zertifikat installieren:

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

2. Das neue KMIP Clientzertifikat installieren:

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

3. Die Konfiguration des Schlüsselmanagers wird aktualisiert, sodass die neu installierten Zertifikate verwendet werden:

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

   Wenn Sie ONTAP 9.6 oder höher in einer MetroCluster Umgebung verwenden und die Key-Manager-Konfiguration auf der Admin-SVM ändern möchten, muss der Befehl auf beiden Clustern in der Konfiguration ausgeführt werden.

> ⓘ Die Aktualisierung der Schlüsselverwaltungskonfiguration zur Verwendung der neu installierten Zertifikate führt zu einem Fehler, wenn sich die öffentlichen/privaten Schlüssel des neuen Clientzertifikats von den zuvor installierten Schlüsseln unterscheiden. Siehe die "NetApp Knowledge Base: Die öffentlichen oder privaten Schlüssel des neuen Clientzertifikats unterscheiden sich von den bestehenden Clientzertifikaten." für Anweisungen zum Überschreiben dieses Fehlers.

Verwandte Informationen

- "Sicherheitszertifikat installieren"
- "security key-manager external modify"

Austausch eines FIPS-Laufwerks oder SED in ONTAP

Ein FIPS-Laufwerk oder eine SED kann genauso ausgetauscht werden wie eine herkömmliche Festplatte. Es ist sicherzustellen, dass dem Ersatzlaufwerk neue Datenauthentifizierungsschlüssel zugewiesen werden. Bei einem FIPS-Laufwerk kann außerdem die Zuweisung eines neuen FIPS 140-2 Authentifizierungsschlüssels sinnvoll sein.

> ⓘ Wenn ein HA-Paar "Verschlüsselung von SAS- oder NVMe-Laufwerken (SED, NSE, FIPS)" verwendet wird, müssen Sie die Anweisungen im Thema "Zurückstellen eines FIPS-Laufwerks oder SED in den ungeschützten Modus" für alle Laufwerke innerhalb des HA-Paares befolgen, bevor Sie das System initialisieren (Boot-Optionen 4 oder 9). Andernfalls kann es in Zukunft zu Datenverlust kommen, wenn die Laufwerke wiederverwendet werden.

Bevor Sie beginnen

- Sie müssen die Schlüssel-ID für den Authentifizierungsschlüssel kennen, der vom Laufwerk verwendet wird.
- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

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

   ```
   storage disk show -broken
   ```

   Weitere Informationen zu `storage disk show` finden sich in der "ONTAP-Befehlsreferenz".

```
cluster1::> storage disk show -broken
Original Owner: node1
  Checksum Compatibility: block
                                                    Drawer
Usable Physical
    Disk            Outage Reason  HA Shelf Bay  /Slot Chan   Pool
Type    RPM     Size     Size Model
    --------------- ------------- --- ----- --- ------ ---- ------
------- ------ -------- -------- ----------------
    1.0.12          admin failed   0a     0  12   -/-     A FAILED SSD-
NVM      -   1.75TB   1.75TB X4024S173A1T9NTE

Original Owner: node2
  Checksum Compatibility: block
                                                    Drawer
Usable Physical
    Disk            Outage Reason  HA Shelf Bay  /Slot Chan   Pool
Type    RPM     Size     Size Model
    --------------- ------------- --- ----- --- ------ ---- ------
------- ------ -------- -------- ----------------
    1.0.13          admin failed   0b     0  13   -/-     B FAILED SSD-
NVM      -   1.75TB   1.75TB X4024S173A1T9NTF

2 entries were displayed.
[...]
```

2. Die defekte Festplatte ist durch ein neues FIPS-Laufwerk oder SED zu ersetzen, entsprechend den Anweisungen im Hardware-Handbuch für Ihr Festplattengehäusemodell.
3. Die Besitzrechte der neu ausgetauschten Festplatte zuweisen:

   `storage disk assign -disk disk_name -owner node`

   Weitere Informationen zu `storage disk assign` finden sich in der "ONTAP-Befehlsreferenz".

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

4. Bestätigen, dass die neue Festplatte zugewiesen wurde:

   `storage encryption disk show`

   Weitere Informationen zu `storage encryption disk show` finden sich in der "ONTAP-Befehlsreferenz".

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
```

```
-----   ----
--------------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
1.10.0  data <id_value>
1.10.1  data <id_value>
2.1.1   open 0x0
[...]
```

5. Die Authentifizierungsschlüssel für Daten dem FIPS-Laufwerk oder SED zuweisen.

   "Zuweisung eines Authentifizierungsschlüssels zu einem FIPS-Laufwerk oder SED (externes Schlüsselmanagement)"

6. Falls erforderlich, einen FIPS 140-2-Authentifizierungsschlüssel dem FIPS-Laufwerk zuweisen.

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

Verwandte Informationen

- "Speicherdatenträger zuweisen"
- "Speicherdatenträger anzeigen"
- "storage encryption Disk anzeigen"

Daten auf einem FIPS-Laufwerk oder SED unzugänglich machen

Datenträgerbereinigung und -vernichtung in ONTAP

Wenn Sie Daten auf einem FIPS-Laufwerk oder Self-Encrypting Drive dauerhaft unzugänglich machen möchten, der ungenutzte Speicherplatz jedoch für neue Daten verfügbar bleiben soll, kann das Laufwerk bereinigt werden. Wenn Daten dauerhaft unzugänglich gemacht werden sollen und eine Wiederverwendung des Laufwerks nicht erforderlich ist, kann es zerstört werden.

- Datenträgerbereinigung

  Beim Bereinigen eines Self-Encrypting Drives ändert das System den Verschlüsselungsschlüssel auf einen neuen Zufallswert, setzt den Sperrzustand beim Einschalten auf „false“ und setzt die Schlüssel-ID auf einen Standardwert, entweder die Hersteller Secure ID 0x0 (SAS-Laufwerke) oder einen Null-Schlüssel (NVMe-Laufwerke). Dadurch sind die Daten auf dem Laufwerk unzugänglich und können nicht wiederhergestellt werden. Bereinigte Laufwerke können als nicht mit Nullen überschriebene Ersatzlaufwerke wiederverwendet werden.

- Datenträger zerstören

  Wenn Sie ein FIPS-Laufwerk oder ein Self-Encrypting Drive zerstören, setzt das System den Festplattenverschlüsselungsschlüssel auf einen unbekannten Zufallswert und sperrt die Festplatte unwiderruflich. Dadurch wird die Festplatte dauerhaft unbrauchbar und die darauf befindlichen Daten sind dauerhaft unzugänglich.

Es besteht die Möglichkeit, einzelne Self-Encrypting Drives zu bereinigen oder zu zerstören oder alle Self-

Encrypting Drives eines Knotens zu zerstören.

Ein FIPS-Laufwerk oder SED in ONTAP bereinigen

Wenn Daten auf einem FIPS-Laufwerk oder Self-Encrypting Drive dauerhaft unzugänglich gemacht werden sollen und das Laufwerk für neue Daten verwendet werden soll, kann der `storage encryption disk sanitize` Befehl zum Bereinigen des Laufwerks verwendet werden.

Über diese Aufgabe

Beim Bereinigen eines Self-Encrypting Drives ändert das System den Verschlüsselungsschlüssel auf einen neuen Zufallswert, setzt den Sperrzustand beim Einschalten auf „false“ und setzt die Schlüssel-ID auf einen Standardwert, entweder die Hersteller Secure ID 0x0 (SAS-Laufwerke) oder einen Null-Schlüssel (NVMe-Laufwerke). Dadurch sind die Daten auf dem Laufwerk unzugänglich und können nicht wiederhergestellt werden. Bereinigte Laufwerke können als nicht mit Nullen überschriebene Ersatzlaufwerke wiederverwendet werden.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Alle Daten, die erhalten bleiben müssen, zu einem Aggregat auf einer anderen Festplatte migrieren.
2. Das Aggregat auf dem FIPS-Laufwerk oder dem zu bereinigenden SED löschen:

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

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

   Weitere Informationen zu `storage aggregate delete` finden sich in der "ONTAP-Befehlsreferenz".

3. Die Datenträger-ID für das zu bereinigende FIPS-Laufwerk oder die Self-Encrypting Drives (SED) identifizieren:

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

   Weitere Informationen zu `storage encryption disk show` finden sich in der "ONTAP-Befehlsreferenz".

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

4. Wenn ein FIPS-Laufwerk im FIPS-Konformitätsmodus betrieben wird, wird die FIPS-Authentifizierungsschlüssel-ID für den Knoten wieder auf den Standardwert MSID 0x0 gesetzt:

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

   Mit dem `security key-manager query` Befehl lassen sich die Schlüssel-IDs anzeigen.

   ```
   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. Das Laufwerk bereinigen:

   `storage encryption disk sanitize -disk disk_id`

   Mit diesem Befehl können nur Hot Spare- oder defekte Festplatten bereinigt werden. Um alle Festplatten unabhängig vom Typ zu bereinigen, ist die Option `-force-all-state` zu verwenden. Weitere Informationen zu `storage encryption disk sanitize` finden sich in der "ONTAP-Befehlsreferenz".

   ONTAP fordert Sie auf, vor dem Fortfahren eine Bestätigungsphrase einzugeben. Die Phrase muss exakt so eingegeben werden, wie sie 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. Die bereinigte Festplatte wiederherstellen:
   `storage disk unfail -spare true -disk disk_id`
7. Es ist zu prüfen, ob die Festplatte einen Besitzer hat:
   `storage disk show -disk disk_id` + Falls die Festplatte keinen Besitzer hat, ist einer zuzuweisen.
   `storage disk assign -owner node -disk disk_id`
8. Öffnen Sie die Nodeshell für den Node, dem die Festplatten gehören, die Sie bereinigen möchten:

   `system node run -node node_name`

   Führe den `disk sanitize release` Befehl aus.

9. Beenden Sie die Nodeshell. Die Festplatte wird erneut in den betriebsbereiten Zustand versetzt:

```
storage disk unfail -spare true -disk disk_id
```

10. Es sollte überprüft werden, dass die Festplatte nun als Ersatzfestplatte verfügbar ist und zur Wiederverwendung in einem Aggregat bereitsteht:
    `storage disk show -disk disk_id`

Verwandte Informationen

- "Speicherdatenträger zuweisen"
- "Speicherdatenträger anzeigen"
- "Speicherfestplatte wiederherstellen"
- "Speicherverschlüsselung Festplatte ändern"
- "Speicherverschlüsselung Festplattenbereinigung"
- "storage encryption disk show-status"

Ein FIPS-Laufwerk oder eine SED in ONTAP zerstören

Wenn Daten auf einem FIPS-Laufwerk oder Self-Encrypting Drive dauerhaft unzugänglich gemacht werden sollen und das Laufwerk nicht wiederverwendet werden muss, kann der `storage encryption disk destroy` Befehl verwendet werden, um die Festplatte zu zerstören.

Über diese Aufgabe

Wenn Sie ein FIPS-Laufwerk oder eine Self-Encrypting Drive zerstören, setzt das System den Festplattenverschlüsselungsschlüssel auf einen unbekannten Zufallswert und sperrt das Laufwerk unwiderruflich. Dadurch wird die Festplatte praktisch unbrauchbar und die darauf befindlichen Daten dauerhaft unzugänglich. Es besteht jedoch die Möglichkeit, die Festplatte mithilfe der auf dem Etikett aufgedruckten physischen Secure ID (PSID) auf die werkseitig konfigurierten Einstellungen zurückzusetzen. Weitere Informationen finden sich unter "Wiederinbetriebnahme eines FIPS-Laufwerks oder SED, wenn Authentifizierungsschlüssel verloren gegangen sind".

> Ein FIPS-Laufwerk oder Self-Encrypting Drive sollte nur zerstört werden, wenn der Non-Returnable Disk Plus Service (NRD Plus) vorhanden ist. Durch das Zerstören eines Datenträgers erlischt die Garantie.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Alle Daten, die erhalten bleiben müssen, werden in ein Aggregat auf einer anderen Festplatte migriert.
2. Das Aggregat auf dem FIPS-Laufwerk oder dem zu zerstörenden SED löschen:

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

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

   Weitere Informationen zu `storage aggregate delete` finden sich in der "ONTAP-Befehlsreferenz".

3. Die Datenträger-ID für das FIPS-Laufwerk oder den zu zerstörenden Self-Encrypting Drive (SED) identifizieren:

   `storage encryption disk show`

   Weitere Informationen zu `storage encryption disk show` finden sich in der "ONTAP-Befehlsreferenz".

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

4. Zerstören der Festplatte:

   `storage encryption disk destroy -disk disk_id`

   Weitere Informationen zu `storage encryption disk destroy` finden sich in der "ONTAP-Befehlsreferenz".

   ⓘ Sie werden aufgefordert, vor dem Fortfahren eine Bestätigungsphrase einzugeben. Die Phrase muss exakt so eingegeben werden, wie sie 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.
   ```

Verwandte Informationen

- "Speicherverschlüsselungsfestplatte zerstören"
- "storage encryption Disk anzeigen"
- "storage encryption disk show-status"

Daten auf einem FIPS-Laufwerk oder SED im Notfall in ONTAP vernichten

Im Falle eines Sicherheitsnotfalls kann der Zugriff auf ein FIPS-Laufwerk oder eine SED sofort verhindert werden, selbst wenn das Speichersystem oder der KMIP-Server nicht mit Strom versorgt wird.

Bevor Sie beginnen

- Wenn ein KMIP-Server ohne verfügbare Stromversorgung verwendet wird, muss der KMIP-Server mit einem leicht zu zerstörenden Authentifizierungsobjekt (zum Beispiel einer Smartcard oder einem USB-Laufwerk) konfiguriert werden.
- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritt

1. Notfallvernichtung von Daten auf einem FIPS-Laufwerk oder SED durchführen:

Wenn…	Dann…

Die Stromversorgung des Speichersystems ist gewährleistet und es besteht ausreichend Zeit, das Speichersystem ordnungsgemäß offline zu nehmen.	a. Wenn das Speichersystem als HA-Paar konfiguriert ist, sollte die Übernahme deaktiviert werden. b. Alle Aggregate offline nehmen und löschen. c. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced` d. Wenn sich das Laufwerk im FIPS-Konformitätsmodus befindet, wird die FIPS-Authentifizierungsschlüssel-ID für den Knoten wieder auf die Standard-MSID gesetzt: `storage encryption disk modify -disk * -fips-key-id 0x0` e. Das Speichersystem anhalten. f. Im Wartungsmodus starten. g. Datenträger bereinigen oder zerstören: ◦ Wenn die Daten auf den Festplatten unzugänglich gemacht werden sollen und die Festplatten dennoch wiederverwendet werden können, empfiehlt sich eine Bereinigung der Festplatten: `disk encrypt sanitize -all` ◦ Wenn die Daten auf den Datenträgern unzugänglich gemacht werden sollen und die Datenträger nicht aufbewahrt werden müssen, zerstören Sie die Datenträger: `disk encrypt destroy disk_id1 disk_id2 …` Die `disk encrypt sanitize` und	Die Stromversorgung des Speichersystems ist gewährleistet, und die Daten müssen sofort vernichtet werden.

a. **Wenn Sie die Daten auf den Festplatten unzugänglich machen und die Festplatten dennoch wiederverwenden möchten, bereinigen Sie die Festplatten:**
b. Wenn das Speichersystem als HA-Paar konfiguriert ist, sollte die Übernahme deaktiviert werden.
c. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:
`set -privilege advanced`
d. Wenn sich das Laufwerk im FIPS-Konformitätsmodus befindet, wird die FIPS-Authentifizierungsschlüssel-ID für den Knoten wieder auf die Standard-MSID gesetzt:
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. Festplatte bereinigen:
`storage encryption disk sanitize -disk * -force-all-states true`
	a. **Wenn die Daten auf den Datenträgern unzugänglich gemacht werden sollen und die Datenträger nicht aufbewahrt werden müssen, die Datenträger zerstören:**
	b. Wenn das Speichersystem als HA-Paar konfiguriert ist, sollte die Übernahme deaktiviert werden.
	c. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:
	`set -privilege advanced`
	d. Zerstören Sie die Festplatten:
	`storage encryption disk destroy -disk * -force-all-states true`
		Das Speichersystem stürzt ab und befindet sich dadurch in einem dauerhaft deaktivierten Zustand, wobei alle Daten gelöscht werden. Um das System erneut zu verwenden, ist eine Neukonfiguration erforderlich.

Strom ist für den KMIP-Server verfügbar, jedoch nicht für das Speichersystem.	a. Melden Sie sich beim KMIP Server an. b. Alle Schlüssel, die mit den FIPS-Laufwerken oder Self-Encrypting Drives verknüpft sind und die Daten enthalten, auf die kein Zugriff mehr möglich sein soll, werden zerstört. Dadurch wird der Zugriff des Speichersystems auf die Festplattenverschlüsselungsschlüssel verhindert.	Strom ist für den KMIP-Server oder das Speichersystem nicht verfügbar.

Verwandte Informationen

- "Speicherverschlüsselungsfestplatte zerstören"
- "Speicherverschlüsselung Festplatte ändern"

- "Speicherverschlüsselung Festplattenbereinigung"

Wiederherstellung des Betriebs eines FIPS-Laufwerks oder einer ONTAP SED bei verlorenen Schlüsseln

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 auf die Daten auf der Festplatte nicht zugegriffen oder sie wiederhergestellt werden können, besteht die Möglichkeit, den ungenutzten Speicherplatz der SED wieder für Daten verfügbar zu machen.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Über diese Aufgabe

Dieses Verfahren sollte nur verwendet werden, wenn Sie sicher sind, dass die Authentifizierungsschlüssel für das FIPS-Laufwerk oder SED dauerhaft verloren sind und nicht wiederhergestellt werden können.

Falls die Festplatten partitioniert sind, müssen sie zuerst entpartitioniert werden, bevor Sie mit diesem Vorgang beginnen können.

> Der Befehl zum Aufheben der Partitionierung einer Festplatte ist nur auf der Diagnoseebene verfügbar und sollte nur unter Aufsicht des NetApp Supports durchgeführt werden. **Es wird dringend empfohlen, vor dem weiteren Vorgehen den NetApp Support zu kontaktieren.** Es kann auch auf die "NetApp Knowledge Base: Wie eine Ersatzfestplatte in ONTAP entpartitioniert wird" verwiesen werden.

Schritte

1. Ein FIPS-Laufwerk oder SED wieder in Betrieb nehmen:

Wenn die SEDS…	Diese Schritte können verwendet werden…

Nicht im FIPS-Konformitätsmodus oder im FIPS-Konformitätsmodus und der FIPS-Schlüssel ist verfügbar	a. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt:
	`set -privilege advanced`
	b. Der FIPS-Schlüssel wird auf die standardmäßige sichere Hersteller-ID 0x0 zurückgesetzt:
	`storage encryption disk modify -fips-key-id 0x0 -disk disk_id`
	c. Es sollte überprüft werden, ob der Vorgang erfolgreich war:
	`storage encryption disk show-status` Falls der Vorgang fehlgeschlagen ist, kann der in diesem Thema beschriebene PSID-Prozess verwendet werden.
	d. Die defekte Festplatte bereinigen:
	`storage encryption disk sanitize -disk disk_id` Mit dem Befehl `storage encryption disk show-status` kann überprüft werden, ob der Vorgang erfolgreich war, bevor zum nächsten Schritt übergegangen wird.
	e. Die bereinigte Festplatte wiederherstellen:
	`storage disk unfail -spare true -disk disk_id`
	f. Es ist zu prüfen, ob die Festplatte einen Besitzer hat:
	`storage disk show -disk disk_id` + Falls die Festplatte keinen Besitzer hat, ist einer zuzuweisen.
	`storage disk assign -owner node -disk disk_id`
	i. Öffnen Sie die Nodeshell für den Node, dem die Festplatten gehören, die Sie bereinigen möchten:
	`system node run -node node_name`
	Führe den `disk sanitize release` Befehl aus.
	g. Beenden Sie die Nodeshell. Die Festplatte wird erneut in den betriebsbereiten Zustand versetzt:
	`storage disk unfail -spare true -disk disk_id`
	h. Es sollte überprüft werden, dass die Festplatte nun als Ersatzfestplatte verfügbar ist und zur Wiederverwendung in einem Aggregat bereitsteht:
	`storage disk show -disk disk_id`

Im FIPS-Konformitätsmodus ist der FIPS-Schlüssel nicht verfügbar und die SEDs haben eine PSID auf dem Etikett aufgedruckt	a. Die PSID der Festplatte lässt sich dem Festplattenetikett entnehmen. b. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -privilege advanced` c. Setzen Sie die Festplatte auf die werkseitigen Einstellungen zurück: `storage encryption disk revert-to-original-state -disk` *`disk_id`* `-psid` *`disk_physical_secure_id`* Mit dem Befehl `storage encryption disk show-status` lässt sich überprüfen, ob der Vorgang erfolgreich war, bevor zum nächsten Schritt übergegangen wird. d. Wenn Sie ONTAP 9.8P5 oder früher verwenden, zum nächsten Schritt wechseln. Wenn Sie ONTAP 9.8P6 oder später verwenden, die bereinigte Festplatte wiederherstellen. `storage disk unfail -disk` *`disk_id`* e. Es ist zu prüfen, ob die Festplatte einen Besitzer hat: `storage disk show -disk` *`disk_id`* + Falls die Festplatte keinen Besitzer hat, ist einer zuzuweisen. `storage disk assign -owner node -disk` *`disk_id`* i. Öffnen Sie die Nodeshell für den Node, dem die Festplatten gehören, die Sie bereinigen möchten: `system node run -node` *`node_name`* Führe den `disk sanitize release` Befehl aus. f. Die Nodeshell wird beendet. Die Festplatte wird erneut in den betriebsbereiten Zustand versetzt: `storage disk unfail -spare true -disk` *`disk_id`* g. Es sollte überprüft werden, dass die Festplatte nun als Ersatzfestplatte verfügbar ist und zur Wiederverwendung in einem Aggregat bereitsteht: `storage disk show -disk` *`disk_id`*

Verwandte Informationen

- "Speicherverschlüsselung Festplatte ändern"
- "Speicherverschlüsselungsfestplatte auf ursprünglichen Zustand zurücksetzen"
- "Speicherverschlüsselung Festplattenbereinigung"
- "storage encryption disk show-status"

Ein FIPS-Laufwerk oder SED in ONTAP in den ungeschützten Modus zurückversetzen

Ein FIPS-Laufwerk oder SED ist nur dann vor unberechtigtem Zugriff geschützt, wenn die Authentifizierungsschlüssel-ID des Knotens auf einen anderen Wert als den Standardwert gesetzt ist. Ein FIPS-Laufwerk oder SED kann in den ungeschützten Modus zurückgesetzt werden, indem mit dem `storage encryption disk modify` Befehl die Schlüssel-ID auf den Standardwert gesetzt wird. Ein FIPS-Laufwerk oder SED im ungeschützten Modus verwendet die Standardverschlüsselungsschlüssel, während ein

FIPS-Laufwerk oder SED im geschützten Modus bereitgestellte, geheime Verschlüsselungsschlüssel verwendet. Wenn sich verschlüsselte Daten auf dem Laufwerk befinden und das Laufwerk in den ungeschützten Modus zurückgesetzt wird, bleiben die Daten weiterhin verschlüsselt und werden nicht offengelegt.

> Dieses Verfahren stellt sicher, dass alle verschlüsselten Daten unzugänglich werden, nachdem das FIPS-Laufwerk oder SED in den ungeschützten Modus zurückgesetzt wurde. Sobald die FIPS- und Datenschlüssel-IDs zurückgesetzt sind, können vorhandene Daten nicht mehr entschlüsselt werden und bleiben unzugänglich, sofern die ursprünglichen Schlüssel nicht wiederhergestellt werden.

Wenn ein HA-Paar verschlüsselnde SAS- oder NVMe-Laufwerke (SED, NSE, FIPS) verwendet, muss dieser Prozess für alle Laufwerke innerhalb des HA-Paares vor der Initialisierung des Systems (Boot-Optionen 4 oder 9) durchgeführt werden. Andernfalls kann es in Zukunft zu Datenverlust kommen, wenn die Laufwerke wiederverwendet werden.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

   ```
   set -privilege advanced
   ```

2. Wenn ein FIPS-Laufwerk im FIPS-Konformitätsmodus betrieben wird, wird die FIPS-Authentifizierungsschlüssel-ID für den Knoten wieder auf den Standardwert MSID 0x0 gesetzt:

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

   Mit dem `security key-manager query` Befehl lassen sich die Schlüssel-IDs anzeigen.

   ```
   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.
   ```

   Der erfolgreiche Abschluss des Vorgangs lässt sich mit folgendem Befehl bestätigen:

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

   Den Befehl show-status so oft ausführen, bis die Zahlen in "Disks Begun" und "Disks Done" identisch 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. Die Authentifizierungsschlüssel-ID für den Knoten wird wieder auf den Standardwert MSID 0x0 gesetzt:

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

   Der Wert `-data-key-id` sollte auf 0x0 gesetzt werden, unabhängig davon, ob Sie ein SAS- oder NVMe-Laufwerk in den ungeschützten Modus zurückversetzen.

   Mit dem `security key-manager query` Befehl lassen sich die Schlüssel-IDs anzeigen.

```
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.
```

   Der erfolgreiche Abschluss des Vorgangs lässt sich mit folgendem Befehl bestätigen:

   `storage encryption disk show-status`

   Wiederholen Sie den Befehl „show-status“, bis die Zahlen übereinstimmen. Der Vorgang ist abgeschlossen, wenn die Zahlen in „disks begun“ und „disks done“ übereinstimmen.

Wartungsmodus

Ab ONTAP 9.7 kann ein FIPS-Laufwerk im Wartungsmodus neu verschlüsselt werden. Der Wartungsmodus sollte nur verwendet werden, wenn die ONTAP CLI-Anweisungen im vorherigen Abschnitt nicht genutzt werden können.

Schritte

1. Die FIPS-Authentifizierungsschlüssel-ID für den Knoten wird wieder auf den Standardwert MSID 0x0 gesetzt:

   `disk encrypt rekey_fips 0x0 *disklist*`

2. Die Authentifizierungsschlüssel-ID für den Knoten wird wieder auf den Standardwert MSID 0x0 gesetzt:

   `disk encrypt rekey 0x0 *disklist*`

3. Bestätigen Sie, dass der FIPS Authentifizierungsschlüssel erfolgreich neu generiert wurde:

```
disk encrypt show_fips
```

4. Bestätigung, dass der Authentifizierungsschlüssel erfolgreich neu verschlüsselt wurde mit:

```
disk encrypt show
```

Ihre Ausgabe zeigt wahrscheinlich entweder die Standard-MSID 0x0-Schlüssel-ID oder den vom Schlüsselserver gespeicherten 64-stelligen Wert an. Das `Locked?` Feld bezieht sich auf die Datensperrung.

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

Verwandte Informationen

- "Speicherverschlüsselung Festplatte ändern"
- "storage encryption disk show-status"

Eine externe Schlüsselverwaltungsverbindung in ONTAP entfernen

Sie können einen KMIP-Server von einem Knoten trennen, wenn der Server nicht mehr benötigt wird. Beispielsweise kann ein KMIP-Server getrennt werden, wenn auf Volumenverschlüsselung umgestellt wird.

Über diese Aufgabe

Wenn ein KMIP-Server von einem Knoten in einem HA-Paar getrennt wird, trennt das System den Server automatisch von allen Cluster-Knoten.

> Wenn nach dem Trennen eines KMIP-Servers weiterhin die externe Schlüsselverwaltung verwendet werden soll, muss ein anderer KMIP-Server verfügbar sein, um Authentifizierungsschlüssel bereitzustellen.

Bevor Sie beginnen

Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.

Schritt

1. Einen KMIP-Server vom aktuellen Knoten trennen:

Für diese ONTAP Version…	Verwenden Sie diesen 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 diese Befehle auf beiden Clustern für die Admin-SVM wiederholt werden.

Der folgende ONTAP 9.6 Befehl deaktiviert die Verbindungen zu zwei externen Schlüsselverwaltungsservern für `cluster1`, der erste mit dem Namen `ks1`, der auf dem Standardport

5696 lauscht, der zweite mit der IP-Adresse 10.0.0.20, der auf Port 24482 lauscht:

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

Weitere Informationen zu `security key-manager external remove-servers` und `security key-manager delete` finden sich in der "ONTAP-Befehlsreferenz".

Eigenschaften des externen Schlüsselverwaltungsservers von ONTAP ändern

Ab ONTAP 9.6 kann mit dem `security key-manager external modify-server` Befehl die I/O-Zeitüberschreitung und der Benutzername eines externen Schlüsselverwaltungsservers geändert werden.

Bevor Sie beginnen

- Sie müssen Cluster- oder SVM-Administrator sein, um diese Aufgabe ausführen zu können.
- Für diese Aufgabe sind erweiterte Berechtigungen erforderlich.
- In einer MetroCluster Umgebung müssen diese Schritte auf beiden Clustern für die Admin-SVM wiederholt werden.

Schritte

1. Im Speichersystem zur erweiterten Berechtigungsstufe wechseln:

   ```
   set -privilege advanced
   ```

2. Eigenschaften des externen Schlüsselverwaltungsservers für den Cluster anpassen:

   ```
   security key-manager external modify-server -vserver admin_SVM -key-server
   host_name|IP_address:port,… -timeout 0…60 -username user_name
   ```

   - Der Zeitüberschreitungswert ist die Zeit in Sekunden, die zum Aufbau der Verbindung mit dem KMIP Server benötigt wird. Wenn 0 angegeben wird, gibt es keine Zeitüberschreitung und die Verbindungsanfrage kann unbegrenzt warten. Wenn ein Wert im Bereich von 1 bis 60 angegeben wird, tritt eine Zeitüberschreitung der Verbindungsanfrage ein, wenn innerhalb der angegebenen Sekunden keine Verbindung zum KMIP Key Server hergestellt werden kann.
   - Wenn der Benutzername geändert wird, erscheint eine Aufforderung zur Eingabe eines neuen Passworts.
   - Wenn der Befehl an der Cluster-Anmeldeaufforderung ausgeführt wird, *`admin_SVM`* ist standardmäßig die Admin-SVM des aktuellen Clusters voreingestellt. Um die Eigenschaften des externen Key Manager-Servers zu ändern, ist die Rolle des Cluster-Administrators erforderlich.

Der folgende Befehl ändert den Zeitüberschreitungswert auf 45 Sekunden für den `cluster1` externen Schlüsselverwaltungsserver, der auf dem Standardport 5696 lauscht:

```
clusterl::> security key-manager external modify-server -vserver
```

```
cluster1 -key-server ks1.local -timeout 45
```

3. Eigenschaften des externen Schlüsselverwaltungsservers für eine SVM ändern:

   `security key-manager external modify-server -vserver SVM -key-server host_name|IP_address:port,… -timeout 0…60 -username user_name`

   - Der Zeitüberschreitungswert ist die Zeit in Sekunden, die zum Aufbau der Verbindung mit dem KMIP Server benötigt wird. Wenn 0 angegeben wird, gibt es keine Zeitüberschreitung und die Verbindungsanfrage kann unbegrenzt warten. Wenn ein Wert im Bereich von 1 bis 60 angegeben wird, tritt eine Zeitüberschreitung der Verbindungsanfrage ein, wenn innerhalb der angegebenen Sekunden keine Verbindung zum KMIP Key Server hergestellt werden kann.
   - Wenn der Benutzername geändert wird, erscheint eine Aufforderung zur Eingabe eines neuen Passworts.
   - Wenn der Befehl an der SVM-Anmeldeaufforderung ausgeführt wird, *SVM* gilt standardmäßig die aktuelle SVM. Zum Ändern der Eigenschaften des externen Schlüsselverwaltungsservers sind Cluster- oder SVM-Administratorrechte erforderlich.

   Der folgende Befehl ändert den Benutzernamen und das Passwort des `svm1` externen Schlüsselverwaltungsservers, der auf dem Standardport 5696 lauscht:

```
svm1::> security key-manager external modify-server -vserver svm11 -key
-server ks1.local -username svm1user
Enter the password:
Reenter the password:
```

4. Den letzten Schritt für alle weiteren SVMs wiederholen.

Verwandte Informationen

- "security key-manager external modify-server"

Übergang von der internen zur externen Schlüsselverwaltung in ONTAP

Wenn Sie von der Onboard-Schlüsselverwaltung zur externen Schlüsselverwaltung wechseln möchten, hängen die erforderlichen Schritte vom Geltungsbereich des Schlüsselmanagers ab. Für die Admin SVM (Cluster-Geltungsbereich) müssen Sie die Konfiguration der Onboard-Schlüsselverwaltung deaktivieren, bevor Sie einen externen Schlüsselmanager aktivieren können. Ab ONTAP 9.20.1 können Daten-SVMs einen externen Schlüsselmanager direkt aktivieren, und ONTAP migriert die Volume-Verschlüsselungsschlüssel der SVM automatisch vom Schlüsselmanager mit Admin-Geltungsbereich zum neuen Schlüsselmanager der Daten-SVM.

Ab ONTAP 9.20.1 ist diese Aufgabe nur noch erforderlich, wenn Sie die admin SVM von der internen Schlüsselverwaltung auf die externe Schlüsselverwaltung umstellen. Wenn Sie einen externen Schlüsselmanager für eine data SVM konfigurieren, müssen Sie die interne Schlüsselverwaltung nicht zuerst deaktivieren.

Bevor Sie beginnen

- Für hardwarebasierte Verschlüsselung müssen die Datenschlüssel aller FIPS-Laufwerke oder Self-Encrypting Drives auf den Standardwert zurückgesetzt werden.

  "Zurückstellen eines FIPS-Laufwerks oder SED in den ungeschützten Modus"

- Bei softwarebasierter Verschlüsselung müssen alle Volumes entschlüsselt werden.

  "Entschlüsselung der Volumendaten"

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritt

1. Löschen der Konfiguration der integrierten Schlüsselverwaltung für die admin SVM:

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

   Weitere Informationen zu `security key-manager onboard disable` und `security key-manager delete-key-database` finden sich in der "ONTAP-Befehlsreferenz".

Wechsel von externer Schlüsselverwaltung zu ONTAP interner Schlüsselverwaltung

Um auf die integrierte Schlüsselverwaltung umzuschalten, muss die externe Schlüsselverwaltungskonfiguration gelöscht werden, bevor die integrierte Schlüsselverwaltung aktiviert wird.

Bevor Sie beginnen

- Für hardwarebasierte Verschlüsselung müssen die Datenschlüssel aller FIPS-Laufwerke oder Self-Encrypting Drives auf den Standardwert zurückgesetzt werden.

  "Zurückstellen eines FIPS-Laufwerks oder SED in den ungeschützten Modus"

- Alle externen Schlüsselverwaltungsverbindungen müssen gelöscht worden sein.

  "Löschen einer externen Schlüsselverwaltungsverbindung"

- Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

Die Schritte zur Umstellung Ihrer Schlüsselverwaltung hängen von der Version von ONTAP ab, die Sie verwenden.

ONTAP 9.6 und höher

1. Wechsel zur erweiterten Berechtigungsstufe:

   ```
   set -privilege advanced
   ```

2. Verwenden Sie den Befehl:

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

> In einer MetroCluster Umgebung muss der Befehl für die Admin-SVM auf beiden Clustern wiederholt werden.

Weitere Informationen zu `security key-manager external disable` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP 9.5 und früher

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

Weitere Informationen zu `security key-manager delete-kmip-config` finden sich in der "ONTAP-Befehlsreferenz".

Verwandte Informationen

- "security key-manager external disable"

Wie ONTAP mit nicht erreichbaren Schlüsselverwaltungsservern während des Systemstarts umgeht

ONTAP trifft bestimmte Vorkehrungen, um unerwünschtes Verhalten zu vermeiden, falls ein für NSE konfiguriertes Speichersystem während des Bootvorgangs keinen der angegebenen Schlüsselverwaltungsserver erreichen kann.

Wenn das Speichersystem für NSE konfiguriert ist, die SEDs neu verschlüsselt und gesperrt sind und die SEDs eingeschaltet sind, muss das Speichersystem die erforderlichen Authentifizierungsschlüssel von den Schlüsselverwaltungsservern abrufen, um sich gegenüber den SEDs zu authentifizieren, bevor auf die Daten zugegriffen werden kann.

Das Speichersystem versucht bis zu drei Stunden lang, die angegebenen Schlüsselverwaltungsserver zu kontaktieren. Wenn das Speichersystem nach dieser Zeit keinen von ihnen erreichen kann, stoppt der Startvorgang und das Speichersystem wird angehalten.

Wenn das Speichersystem erfolgreich Kontakt zu einem angegebenen Schlüsselverwaltungsserver aufnimmt, versucht es anschließend bis zu 15 Minuten lang, eine SSL-Verbindung herzustellen. Wenn das Speichersystem keine SSL-Verbindung zu einem angegebenen Schlüsselverwaltungsserver herstellen kann, wird der Startvorgang gestoppt und das Speichersystem angehalten.

Während das Speichersystem versucht, Kontakt zu den Schlüsselverwaltungsservern aufzunehmen und eine Verbindung herzustellen, werden in der Befehlszeile detaillierte Informationen über die fehlgeschlagenen Kontaktversuche angezeigt. Die Kontaktversuche lassen sich jederzeit durch Drücken von Strg+C unterbrechen.

Als Sicherheitsmaßnahme erlauben SEDs nur eine begrenzte Anzahl unautorisierter Zugriffsversuche, danach wird der Zugriff auf die vorhandenen Daten deaktiviert. Wenn das Speichersystem keinen der angegebenen Schlüsselverwaltungsserver kontaktieren kann, um die richtigen Authentifizierungsschlüssel zu erhalten, kann es nur versuchen, sich mit dem Standardschlüssel zu authentifizieren, was zu einem Fehlschlag und einem Systemabsturz führt. Wenn das Speichersystem so konfiguriert ist, dass es im Falle eines Systemabsturzes

automatisch neu startet, gerät es in eine Boot-Schleife, was zu kontinuierlich fehlgeschlagenen Authentifizierungsversuchen auf den SEDs führt.

Das Anhalten des Speichersystems in diesen Szenarien ist beabsichtigt, um zu verhindern, dass das Speichersystem in eine Boot-Schleife gerät und möglicher unbeabsichtigter Datenverlust entsteht, wenn die SEDs dauerhaft gesperrt werden, weil das Sicherheitslimit für eine bestimmte Anzahl aufeinanderfolgender fehlgeschlagener Authentifizierungsversuche überschritten wurde. Das Limit und die Art des Sperrschutzes hängen von den Herstellerspezifikationen und dem jeweiligen SED-Typ ab.

SED-Typ	Anzahl aufeinanderfolgender fehlgeschlagener Authentifizierungsversuche, die zur Sperrung führen	Sperrschutzart bei Erreichen des Sicherheitsgrenzwerts
HDD	1024	Unwiderruflich. Die Daten können nicht wiederhergestellt werden, selbst wenn der korrekte Authentifizierungsschlüssel wieder verfügbar ist.
X440_PHM2800MCTO 800GB NSE SSDs mit Firmware-Revisionen NA00 oder NA01	5	Vorübergehend. Die Sperre ist nur bis zum Neustart der Festplatte aktiv.
X577_PHM2800MCTO 800GB NSE SSDs mit Firmware-Revisionen NA00 oder NA01	5	Vorübergehend. Die Sperre ist nur bis zum Neustart der Festplatte aktiv.
X440_PHM2800MCTO 800GB NSE SSDs mit höheren Firmware-Revisionen	1024	Unwiderruflich. Die Daten können nicht wiederhergestellt werden, selbst wenn der korrekte Authentifizierungsschlüssel wieder verfügbar ist.
X577_PHM2800MCTO 800GB NSE SSDs mit höheren Firmware-Revisionen	1024	Unwiderruflich. Die Daten können nicht wiederhergestellt werden, selbst wenn der korrekte Authentifizierungsschlüssel wieder verfügbar ist.
Alle anderen SSD Modelle	1024	Unwiderruflich. Die Daten können nicht wiederhergestellt werden, selbst wenn der korrekte Authentifizierungsschlüssel wieder verfügbar ist.

Für alle SED-Typen wird der Versuchszähler nach einer erfolgreichen Authentifizierung auf null zurückgesetzt.

Wenn Sie auf dieses Szenario stoßen, in dem das Speichersystem aufgrund des Nichterreichens eines der angegebenen Schlüsselverwaltungsserver angehalten wird, muss zunächst die Ursache für den Kommunikationsfehler ermittelt und behoben werden, bevor versucht wird, das Speichersystem weiter zu starten.

ONTAP Verschlüsselung standardmäßig deaktiviert

Ab ONTAP 9.7 ist die Aggregat- und Volumenverschlüsselung standardmäßig aktiviert, sofern Sie über eine Volumenverschlüsselungslizenz (VE) verfügen und einen integrierten oder externen Schlüsselmanager verwenden. Falls erforderlich, kann die

Verschlüsselung standardmäßig für den gesamten Cluster deaktiviert werden.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können, oder SVM-Administrator, dem der Cluster-Administrator die entsprechende Berechtigung delegiert hat.

Schritt

1. Um die Verschlüsselung für den gesamten Cluster in ONTAP 9.7 oder höher standardmäßig zu deaktivieren, ist folgender Befehl auszuführen:

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

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.