NetApp Volume Encryption konfigurieren

ONTAP 9

NetApp
September 12, 2024

This PDF was generated from https://docs.netapp.com/de-de/ontap/encryption-at-rest/configure-netapp-volume-encryption-concept.html on September 12, 2024. Always check docs.netapp.com for the latest.

Inhalt

NetApp Volume Encryption konfigurieren . . . 1
NetApp Volume Encryption Übersicht konfigurieren . . . 1
NetApp Volume Encryption Workflow . . . 5
Konfigurieren Sie NVE . . . 5
Verschlüsseln von Volume-Daten mit NVE . . . 25

NetApp Volume Encryption konfigurieren

NetApp Volume Encryption Übersicht konfigurieren

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

Allgemeines zu NVE

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

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

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

Sie können die Verschlüsselung auf einem neuen oder vorhandenen Volume aktivieren. NVE unterstützt eine breite Palette an Storage-Effizienzfunktionen, einschließlich Deduplizierung und Komprimierung. Ab ONTAP 9.14.1 ist dies möglich Aktivieren Sie NVE bei vorhandenen SVM-Root-Volumes.

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

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

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

Verschlüsselung auf Aggregatebene

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

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

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

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

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

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

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

Wann sollten Sie externe Verschlüsselungsmanagementserver verwenden

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

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

Umfang des externen Schlüsselmanagements

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

- Sie können ein_Cluster Scope_ verwenden, um das externe Verschlüsselungsmanagement für alle SVMs im Cluster zu konfigurieren. Der Clusteradministrator hat Zugriff auf jeden auf den Servern gespeicherten Schlüssel.
- Ab ONTAP 9.6 können Sie mithilfe eines Umfangs *SVM* externes Verschlüsselungsmanagement für eine im Cluster genannte SVM konfigurieren. Dies eignet sich am besten für mandantenfähige Umgebungen, in denen jeder Mandant eine andere SVM (oder einen Satz SVMs) zur Bereitstellung von Daten verwendet. Nur der SVM-Administrator für einen bestimmten Mandanten hat Zugriff auf die Schlüssel für den jeweiligen Mandanten.
- Ab ONTAP 9.10.1 können Sie dies nutzen Azure Key Vault und Google Cloud KMS Zum Schutz von NVE-Schlüsseln nur für Daten-SVMs Dies ist für KMS von AWS ab 9.12.0 verfügbar.

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

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

Support-Details

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

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

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

ONTAP	Alle Implementierungen von ONTAP. Unterstützung für ONTAP Cloud ist in ONTAP 9.5 und höher verfügbar.
Geräte	HDD, SSD, Hybrid, Array-LUN.
RAID	RAID0, RAID4, RAID-DP, RAID-TEC.
Volumes	Daten-Volumes und vorhandene SVM-Root-Volumes. Daten auf MetroCluster Metadaten-Volumes können nicht verschlüsselt werden. Bei älteren Versionen als ONTAP 9.14.1 können Daten auf dem SVM-Root-Volume nicht mit NVE verschlüsselt werden. Ab ONTAP 9.14.1 unterstützt ONTAP NVE auf SVM Root-Volumes.

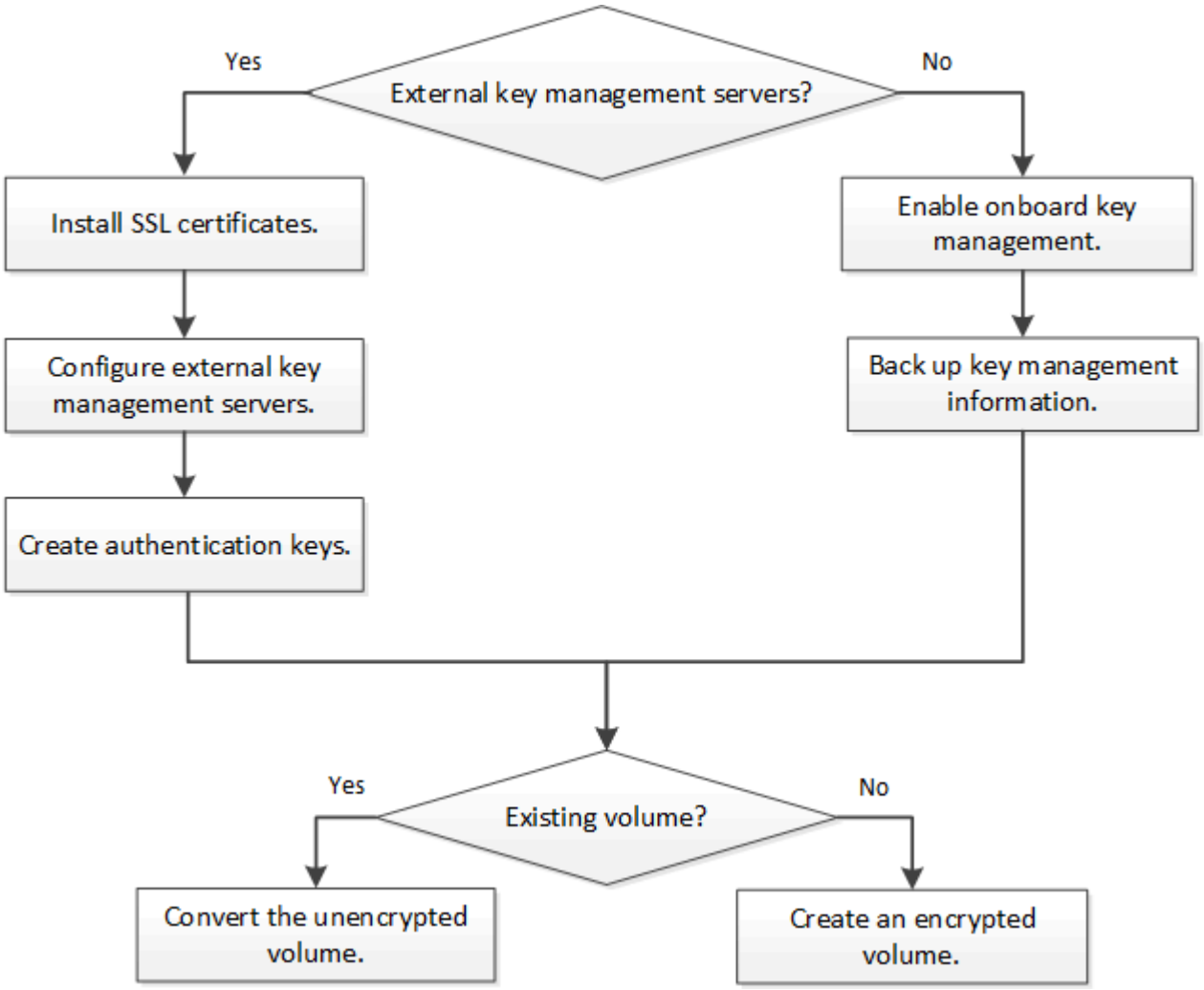
Verschlüsselung auf Aggregatebene	Ab ONTAP 9.6 unterstützt NVE die Verschlüsselung auf Aggregatebene (NAE): • Wenn Sie eine Inline- oder eine Hintergrund-Deduplizierung auf Aggregatebene durchführen möchten, muss die Verschlüsselung auf Aggregatebene verwendet werden. • Sie können ein Verschlüsselungsvolume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

Verwandte Informationen

"FAQ – NetApp Volume Encryption und NetApp Aggregate Encryption"

NetApp Volume Encryption Workflow

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



"Sie müssen die VE-Lizenz installieren" Und konfigurieren Sie Verschlüsselungsmanagement-Services, bevor Sie Daten mit NVE verschlüsseln können. Vor der Installation der Lizenz sollten Sie "Bestimmen Sie, ob NVE in Ihrer ONTAP-Version unterstützt wird".

Konfigurieren Sie NVE

Bestimmen Sie, ob Ihre Cluster-Version NVE unterstützt

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

Über diese Aufgabe

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

Schritt

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

   `version -v`

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

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

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

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

Installieren Sie die Lizenz

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

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

Bevor Sie beginnen

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

Schritte

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

   Der Name des VE-Lizenzpakets lautet `VE`.

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

Externes Verschlüsselungsmanagement konfigurieren

Externes Verschlüsselungsmanagement – Übersicht konfigurieren

Sie können einen oder mehrere externe Verschlüsselungsmanagementserver verwenden, um die Schlüssel zu sichern, die das Cluster zum Zugriff auf verschlüsselte

Daten verwendet. Ein externer Verschlüsselungsmanagement-Server ist ein Drittanbietersystem in Ihrer Storage-Umgebung, der mithilfe des Key Management Interoperability Protocol (KMIP) Schlüssel zu Nodes bereitstellt.

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

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

Management von externen Schlüsselmanagern mit System Manager

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

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

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

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

Konfigurieren Sie einen externen Schlüsselmanager

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

Schritte

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

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

Workflow	Navigation	Startschritt

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

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

Bearbeiten Sie einen vorhandenen externen Schlüsselmanager

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

Schritte

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

Umfang	Navigation	Startschritt
Externer Schlüsselmanager für den Clusterbereich	**Cluster** > **Einstellungen**	Blättern Sie zum Abschnitt **Sicherheit**. Wählen Sie unter **Verschlüsselung** ⋮, und wählen Sie dann **External Key Manager bearbeiten**.

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

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

Löschen Sie einen externen Schlüsselmanager

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

Schritte

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

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

Schlüssel zwischen Schlüsselmanagern migrieren

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

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

Installieren Sie SSL-Zertifikate auf dem Cluster

Das Cluster und der KMIP-Server verwenden KMIP SSL-Zertifikate, um die Identität des

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

Über diese Aufgabe

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

Bevor Sie beginnen

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

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

Schritte

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

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

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

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

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

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

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

Externes Verschlüsselungsmanagement in ONTAP 9.6 und höher (NVE)

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

Ab ONTAP 9.11.1 können Sie bis zu 3 sekundäre Schlüsselserver pro primären Schlüsselserver hinzufügen,

um einen geclusterten Schlüsselserver zu erstellen. Weitere Informationen finden Sie unter Konfigurieren Sie externe geclusterte Schlüsselserver.

Über diese Aufgabe

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

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

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

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

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

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

Die integrierte Verschlüsselungsmanagement lässt sich für den Cluster-Umfang und das externe Verschlüsselungsmanagement auf der SVM-Ebene konfigurieren. Sie können das verwenden `security key-manager key migrate` Befehl zur Migration von Schlüsseln vom Onboard-Verschlüsselungsmanagement im Cluster-Umfang an externe Schlüsselmanager des Umfangs der SVM

Bevor Sie beginnen

- Die KMIP SSL-Client- und Serverzertifikate müssen installiert sein.
- Sie müssen ein Cluster- oder SVM-Administrator sein, um diese Aufgabe durchzuführen.
- Wenn Sie externes Verschlüsselungsmanagement für eine MetroCluster Umgebung aktivieren möchten, muss MetroCluster vollständig konfiguriert sein, bevor Sie externes Verschlüsselungsmanagement unterstützen können.
- In einer MetroCluster-Umgebung müssen Sie das KMIP SSL-Zertifikat auf beiden Clustern installieren.

Schritte

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

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

- Der `security key-manager external enable` Mit dem Befehl wird der ersetzt `security key-manager setup` Befehl. Wenn Sie den Befehl an der Eingabeaufforderung für die Anmeldung beim Cluster ausführen, *`admin_SVM`* Standardmäßig wird der Admin-SVM des aktuellen Clusters festgelegt. Sie müssen der Cluster-Administrator sein, um den Clusterumfang zu konfigurieren. Sie können die ausführen `security key-manager external modify` Befehl zum Ändern der Konfiguration für das externe Verschlüsselungsmanagement.
- Wenn Sie in einer MetroCluster-Umgebung externes Verschlüsselungsmanagement für den Administrator-SVM konfigurieren, müssen Sie die wiederholen `security key-manager external enable` Befehl auf dem Partner-Cluster.

Mit dem folgenden Befehl wird die externe Schlüsselverwaltung für aktiviert `cluster1` Mit drei externen Schlüsselservern zu verwenden. Der erste Schlüsselserver wird mit seinem Hostnamen und Port angegeben, der zweite mit einer IP-Adresse und dem Standardport und der dritte mit einer IPv6-Adresse und einem IPv6-Port:

```
clusterl::> security key-manager external enable -vserver cluster1 -key
-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. Konfiguration eines Schlüsselmanagers einer SVM:

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

- Wenn Sie den Befehl an der SVM-Anmeldeaufforderung ausführen, `SVM` Standardeinstellung ist die aktuelle SVM. Zum Konfigurieren des SVM-Umfangs müssen Sie ein Cluster oder SVM-Administrator sein. Sie können die ausführen `security key-manager external modify` Befehl zum Ändern der Konfiguration für das externe Verschlüsselungsmanagement.
- Wenn Sie in einer MetroCluster Umgebung externes Verschlüsselungsmanagement für eine Daten-SVM konfigurieren, müssen Sie die nicht wiederholen `security key-manager external enable` Befehl auf dem Partner-Cluster.

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

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

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

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

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

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

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

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

   Node  Vserver  Key Server                                       Status
   ----  -------  ----------------------------------------
   -------------
   node1
         svm1
                  keyserver.svm1.com:5696                          available
         cluster1
                  10.0.0.10:5696                                   available
                  fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
                  ks1.local:15696                                  available
   node2
         svm1
                  keyserver.svm1.com:5696                          available
         cluster1
                  10.0.0.10:5696                                   available
                  fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
                  ks1.local:15696                                  available

   8 entries were displayed.
   ```

5. Konvertieren Sie optional Klartextvolumes in verschlüsselte Volumes.

   `volume encryption conversion start`

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

Ermöglichen Sie externes Verschlüsselungsmanagement in ONTAP 9.5 und früher

Ein oder mehrere KMIP-Server dienen zur Sicherung der Schlüssel, die das Cluster für den Zugriff auf verschlüsselte Daten verwendet. Mit einem Node können bis zu vier

KMIP-Server verbunden werden. Für Redundanz und Disaster Recovery werden mindestens zwei Server empfohlen.

Über diese Aufgabe

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

Bevor Sie beginnen

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

Schritte

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

   ```
   security key-manager setup
   ```

   Die Konfiguration des Schlüsselmanagers wird gestartet.

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

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

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

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

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

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

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

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

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

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

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

Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

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

6. Konvertieren Sie optional Klartextvolumes in verschlüsselte Volumes.

   ```
   volume encryption conversion start
   ```

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

Schlüsselmanagement bei einem Cloud-Provider

Ab ONTAP 9.10.1 können Sie dies nutzen "Azure Key Vault (AKV)" Und "Der Verschlüsselungsmanagement-Service (Cloud KMS) der Google Cloud-Plattform" Zum Schutz Ihrer ONTAP-Verschlüsselungen in einer Cloud-gehosteten Applikation. Ab ONTAP 9.12.0 können Sie auch NVE-Schlüssel mit schützen "KMS VON AWS".

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

Über diese Aufgabe

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

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

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

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

Bevor Sie beginnen

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

Externes Verschlüsselungsmanagement

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

AWS

Bevor Sie beginnen

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

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

Aktivieren Sie AWS KMV auf einer ONTAP SVM

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

Azure

Aktivieren Sie Azure Key Vault auf einer ONTAP SVM

1. Bevor Sie beginnen, müssen Sie die entsprechenden Authentifizierungsdaten von Ihrem Azure-Konto beziehen, entweder ein Clientgeheimnis oder ein Zertifikat. Sie müssen außerdem sicherstellen, dass alle Nodes im Cluster sich in einem ordnungsgemäßen Zustand befinden. Sie können dies mit dem Befehl überprüfen `cluster show`.
2. Setzen Sie die privilegierte Stufe auf „Erweiterd“
   `set -priv advanced`
3. Aktivieren Sie AKV auf der SVM
   `security key-manager external azure enable -client-id *client_id* -tenant-id *tenant_id* -name -key-id *key_id* -authentication-method {certificate|client-secret}`Geben Sie bei der entsprechenden Aufforderung entweder das Clientzertifikat oder den Clientschlüssel aus Ihrem Azure-Konto ein.
4. Überprüfen Sie, ob AKV richtig aktiviert ist:
   `security key-manager external azure show vserver` *`svm_name`*
   Wenn die Erreichbarkeit des Service nicht in Ordnung ist, stellen Sie die Verbindung zum AKV Key Management Service über die LIF der Daten-SVM her.

Google Cloud

Aktivieren Sie Cloud-KMS auf einer ONTAP SVM

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

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

2. Privilegierte Ebene auf erweitert setzen:
   `set -priv advanced`
3. Aktivieren Sie Cloud KMS auf der SVM
   `security key-manager external gcp enable -vserver` *`svm_name`* `-project-id` *`project_id`*`-key-ring-name` *`key_ring_name`* `-key-ring-location` *`key_ring_location`* `-key-name` *`key_name`*
   Geben Sie bei entsprechender Aufforderung den Inhalt der JSON-Datei mit dem privaten Schlüssel für Dienstkonto ein
4. Vergewissern Sie sich, dass Cloud KMS mit den korrekten Parametern konfiguriert ist:
   `security key-manager external gcp show vserver` *`svm_name`*
   Der Status von `kms_wrapped_key_status` Wird sein "`UNKNOWN`" Wenn keine verschlüsselten Volumes erstellt wurden.
   Wenn die Serviceability nicht in Ordnung ist, stellen Sie die Konnektivität zum GCP-Schlüsselmanagement-Service über die Daten-SVM LIF her.

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

Verwandte Informationen

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

Integriertes Verschlüsselungsmanagement in ONTAP 9.6 und höher (NVE)

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

Über diese Aufgabe

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

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

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

Wenn Sie die Einstellung für NVE verwenden `cc-mode-enabled=yes`, Volumen, die Sie mit erstellen

`volume create` Und `volume move start` Befehle werden automatisch verschlüsselt. Für `volume create`, Sie müssen nicht angeben `-encrypt true`. Für `volume move start`, Sie müssen nicht angeben `-encrypt-destination true`.

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

> Wenn der Onboard Key Manager im Common Criteria-Modus aktiviert ist (`cc-mode-enabled=yes`Das Systemverhalten wird folgendermaßen geändert:
>
> - Das System überwacht bei der Verwendung im Common Criteria-Modus auf aufeinanderfolgende fehlgeschlagene Cluster-Passphrase.
>
> Wenn Sie beim Booten nicht die richtige Cluster-Passphrase eingeben, werden verschlüsselte Volumes nicht angehängt. Um dies zu korrigieren, müssen Sie den Node neu booten und die richtige Cluster-Passphrase eingeben. Sobald das System gebootet wurde, können bis zu 5 aufeinanderfolgende Versuche unternommen werden, um für jeden Befehl, für den die Cluster-Passphrase als Parameter erforderlich ist, in einem Zeitraum von 24 Stunden korrekt einzugeben. Wenn das Limit erreicht wird (beispielsweise konnten Sie den Cluster-Passphrase 5 Mal hintereinander nicht korrekt eingeben), müssen Sie entweder warten, bis der 24-Stunden-Timeout abgelaufen ist, oder Sie müssen den Node neu booten, um das Limit zurückzusetzen.
>
> - Updates für das System-Image nutzen das Code-Signing-Zertifikat von NetApp RSA-3072 zusammen mit dem von SHA-384 signierten Code, um die Image-Integrität anstelle des üblichen NetApp RSA-2048-Code-Signaturzertifikats und den von SHA-256 signierten Digests zu überprüfen.
>
> Der Upgrade-Befehl überprüft, ob der Bildinhalt durch Überprüfen verschiedener digitaler Signaturen nicht verändert oder beschädigt wurde. Der Image-Aktualisierungsprozess wird mit dem nächsten Schritt fortgesetzt, wenn die Validierung erfolgreich ist. Andernfalls schlägt die Image-Aktualisierung fehl. Siehe `cluster image` Man-Page für Informationen zu Systemaktualisierungen.

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

Bevor Sie beginnen

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

Schritte

1. Starten Sie die Konfiguration des Schlüsselmanagers:

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

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

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

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

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

2. Geben Sie an der Eingabeaufforderung für die Passphrase eine Passphrase zwischen 32 und 256 Zeichen oder für „`cc-Mode`“ eine Passphrase zwischen 64 und 256 Zeichen ein.

> Wenn die angegebene „`cc-Mode`“-Passphrase weniger als 64 Zeichen beträgt, liegt eine Verzögerung von fünf Sekunden vor, bevor die Eingabeaufforderung für das Setup des Schlüsselmanagers die Passphrase erneut anzeigt.

3. Geben Sie die Passphrase erneut an der Eingabeaufforderung zur Bestätigung der Passphrase ein.
4. Vergewissern Sie sich, dass die Authentifizierungsschlüssel erstellt wurden:

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

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

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

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

 Key Tag                                Key Type Encryption   Restored

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

node1                                  NSE-AK   AES-256      true

    Key ID:
0000000000000000020000000000000100056178fc6ace6d91472df8a9286daacc00000000
00000000

node1                                  NSE-AK   AES-256      true

    Key ID:
0000000000000000020000000000000100df1689a148fdfbf9c2b198ef974d0baa00000000
00000000

2 entries were displayed.
```

5. Konvertieren Sie optional Klartextvolumes in verschlüsselte Volumes.

   `volume encryption conversion start`

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

Nachdem Sie fertig sind

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

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

Integriertes Verschlüsselungsmanagement in ONTAP 9.5 und früher (NVE)

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

Über diese Aufgabe

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

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

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

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

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

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

Bevor Sie beginnen

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

  "Umstellung auf integriertes Verschlüsselungsmanagement von externem Verschlüsselungsmanagement"

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

Schritte

1. Starten Sie die Konfiguration des Schlüsselmanagers:

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

   > Ab ONTAP 9.4 können Sie den verwenden `-enable-cc-mode yes` Option zum Eingeben, dass Benutzer nach einem Neustart die Kennwortphrase für das Schlüsselmanagement eingeben. Wenn Sie die Einstellung für NVE verwenden `-enable-cc-mode yes`, Volumen, die Sie mit erstellen `volume create` Und `volume move start` Befehle werden automatisch verschlüsselt.

   Das folgende Beispiel beginnt mit dem Einrichten des Schlüsselmanagers auf Clustered 1, ohne dass die Passphrase nach jedem Neustart eingegeben werden muss:

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

...

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

2. Eingabe `yes` An der Eingabeaufforderung zur Konfiguration des Onboard-Verschlüsselungsmanagement.
3. Geben Sie an der Eingabeaufforderung für die Passphrase eine Passphrase zwischen 32 und 256 Zeichen oder für „`cc-Mode`“ eine Passphrase zwischen 64 und 256 Zeichen ein.

> Wenn die angegebene „`cc-Mode`“-Passphrase weniger als 64 Zeichen beträgt, liegt eine Verzögerung von fünf Sekunden vor, bevor die Eingabeaufforderung für das Setup des Schlüsselmanagers die Passphrase erneut anzeigt.

4. Geben Sie die Passphrase erneut an der Eingabeaufforderung zur Bestätigung der Passphrase ein.
5. Vergewissern Sie sich, dass die Schlüssel für alle Nodes konfiguriert sind:

   `security key-manager key show`

   Die vollständige Befehlssyntax finden Sie in der man-Page.

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

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

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

6. Konvertieren Sie optional Klartextvolumes in verschlüsselte Volumes.

   ```
   volume encryption conversion start
   ```

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

Nachdem Sie fertig sind

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

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

Integriertes Verschlüsselungsmanagement bei neu hinzugefügten Nodes

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

> Für ONTAP 9.5 und früher müssen Sie den ausführen `security key-manager setup` Befehl jedes Mal, wenn Sie dem Cluster einen Node hinzufügen.
>
> Für ONTAP 9.6 und höher müssen Sie den ausführen `security key-manager sync` Befehl jedes Mal, wenn Sie dem Cluster einen Node hinzufügen.
>
> Wenn Sie einem Cluster einen Node hinzufügen, für das das integrierte Verschlüsselungsmanagement konfiguriert ist, führen Sie diesen Befehl aus, um die fehlenden Schlüssel zu aktualisieren.

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

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

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

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

`-encrypt-destination true`.

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

Verschlüsseln von Volume-Daten mit NVE

Übersicht über NVE zur Verschlüsselung von Volume-Daten

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

Verschlüsselung auf Aggregatebene mit VE-Lizenz aktivieren

Ab ONTAP 9.7 sind neu erstellte Aggregate und Volumes standardmäßig verschlüsselt, wenn Sie über "VE-Lizenz"ein integriertes oder externes Verschlüsselungsmanagement verfügen. Ab ONTAP 9.6 können Sie mithilfe der Verschlüsselung auf Aggregatebene dem enthaltenden Aggregat Schlüssel zuweisen, damit die Volumes verschlüsselt werden können.

Über diese Aufgabe

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

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

Klartextvolumen werden in NAE-Aggregaten nicht unterstützt.

Bevor Sie beginnen

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

Schritte

1. Aktivieren oder Deaktivieren der Verschlüsselung auf Aggregatebene:

An…	Befehl
Erstellen Sie ein NAE Aggregat mit ONTAP 9.7 oder höher	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`*

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

Eine vollständige Befehlssyntax finden Sie in den man-Pages.

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

- ONTAP 9.7 oder höher:

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

- ONTAP 9.6 oder früher:

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

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

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

   Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

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

Nachdem Sie fertig sind

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

Wenn Sie einen KMIP-Server zum Speichern der Schlüssel für einen Node verwenden, sendet ONTAP bei der

Verschlüsselung eines Volumes automatisch „`schiebt`“ einen Verschlüsselungsschlüssel an den Server.

Aktivieren Sie die Verschlüsselung auf einem neuen Volume

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

Über diese Aufgabe

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

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

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

> Klartext-Volumes werden in NAE-Aggregaten nicht unterstützt.

Schritte

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

Zu erstellen…	Befehl
Ein NAE-Band	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`*

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

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

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

   `volume show -is-encrypted true`

   Eine vollständige Befehlssyntax finden Sie im "Befehlsreferenz für ONTAP".

Ergebnis

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

=
:allow-uri-read:

Aktivieren Sie die Verschlüsselung auf einem vorhandenen Volume

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

Über diese Aufgabe

- Ab ONTAP 9.3 können Sie den verwenden `volume encryption conversion start` Befehl, um die Verschlüsselung eines vorhandenen Volume „in place“ zu aktivieren, ohne das Volume an einen anderen Speicherort verschieben zu müssen. Alternativ können Sie den verwenden `volume move start` Befehl.
- Bei ONTAP 9.2 und älteren Versionen können Sie nur die verwenden `volume move start` Befehl zum Aktivieren der Verschlüsselung durch Verschieben eines vorhandenen Volumes

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

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

Nachdem Sie eine Konvertierung gestartet haben, muss diese abgeschlossen sein. Wenn während des Vorgangs ein Leistungsproblem auftritt, können Sie das ausführen `volume encryption conversion pause` Befehl zum Anhalten des Vorgangs, und `volume encryption conversion resume` Befehl zum Fortsetzen des Vorgangs.

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

Schritte

1. Verschlüsselung auf einem vorhandenen Volume aktivieren:

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

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

   Mit dem folgenden Befehl wird die Verschlüsselung für ein vorhandenes Volume aktiviert `vol1`:

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

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

2. Überprüfen Sie den Status des Konvertierungsvorgangs:

   `volume encryption conversion show`

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

   Mit dem folgenden Befehl wird der Status des Konvertierungsvorgangs angezeigt:

   ```
   cluster1::> volume encryption conversion show

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

3. Wenn der Konvertierungsvorgang abgeschlossen ist, überprüfen Sie, ob das Volume für die Verschlüsselung aktiviert ist:

   `volume show -is-encrypted true`

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

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

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

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

Ergebnis

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

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

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

Über diese Aufgabe

- Ab ONTAP 9.8 können Sie dies nutzen `volume move start` Aktivieren der Verschlüsselung auf einem SnapLock oder FlexGroup Volume
- Beginnend mit ONTAP 9.4, wenn Sie beim Einrichten des Onboard Key Managers „`cc-Mode`“ aktivieren, werden die mit dem erstellten Volumes erstellt `volume move start` Befehl wird automatisch verschlüsselt. Sie müssen nicht angeben `-encrypt-destination true`.
- Ab ONTAP 9.6 können Sie mithilfe der Verschlüsselung auf Aggregatebene dem enthaltenden Aggregat Schlüssel zuweisen, damit die Volumes verschoben werden können. Ein mit einem eindeutigen Schlüssel verschlüsseltes Volume wird als „*NVE Volume*“ bezeichnet (d. h., es verwendet NetApp Volume Encryption). Ein mit einem Aggregatschlüssel verschlüsseltes Volume wird als *NAE Volume* (für NetApp Aggregate Encryption) bezeichnet. Klartext-Volumes werden in NAE-Aggregaten nicht unterstützt.
- Ab ONTAP 9.14.1 können Sie ein SVM Root-Volume mit NVE verschlüsseln. Weitere Informationen finden Sie unter Konfiguration der NetApp-Volume-Verschlüsselung auf einem SVM-Root-Volume.

Bevor Sie beginnen

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

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

Schritte

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

Konvertieren…	Befehl
Ein Klartext-Volume auf ein NVE Volume	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination true`

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

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

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

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

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

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

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

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

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

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

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

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

2. Zeigen Sie den Verschlüsselungstyp von Cluster Volumes an:

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

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

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

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

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

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

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

   `volume show -is-encrypted true`

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

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

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

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

Ergebnis

Wenn Sie einen KMIP-Server zur Speicherung der Verschlüsselungsschlüssel für einen Node verwenden, überträgt ONTAP bei der Verschlüsselung eines Volumes automatisch einen Verschlüsselungsschlüssel an den Server.

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

Ab ONTAP 9.14.1 können Sie die NetApp Volume Encryption (NVE) auf einem Storage VM (SVM) Root-Volume aktivieren. Mit NVE wird das Root-Volume mit einem eindeutigen Schlüssel verschlüsselt, was für mehr Sicherheit auf der SVM sorgt.

Über diese Aufgabe

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

Bevor Sie beginnen

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

Schritte

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

CLI

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

Verschlüsseln Sie das Root-Volume

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

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

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

Verschlüsseln Sie das SVM-Root-Volume durch Verschieben

1. Volume-Verschiebung initiieren:

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

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

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

System Manager

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

Node-Root-Volume-Verschlüsselung aktivieren

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

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

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

Bevor Sie beginnen

- Ihr System muss eine HA-Konfiguration verwenden.

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

Schritte

1. Verschlüsseln Sie das Root-Volume:

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

2. Überprüfen Sie den Status des Konvertierungsvorgangs:

   `volume encryption conversion show`

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

   `volume show -fields`

   Das folgende zeigt eine Beispielausgabe für ein verschlüsseltes Volume.

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

Copyright-Informationen

Copyright © 2024 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.