



Externes Verschlüsselungsmanagement konfigurieren

ONTAP 9

NetApp
April 24, 2024

Inhalt

- Externes Verschlüsselungsmanagement konfigurieren 1
 - Externes Verschlüsselungsmanagement – Übersicht konfigurieren 1
 - Management von externen Schlüsselmanagern mit System Manager 1
 - Installieren Sie SSL-Zertifikate auf dem Cluster 4
 - Externes Verschlüsselungsmanagement in ONTAP 9.6 und höher (NVE) 5
 - Ermöglichen Sie externes Verschlüsselungsmanagement in ONTAP 9.5 und früher 8
 - Schlüsselmanagement bei einem Cloud-Provider 9

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 Schlüsselservers pro Storage-VM und Cluster registrieren. Jeder primäre Schlüsselservers kann mit bis zu drei sekundären Schlüsselserversn 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 die Option aus  . 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 aus  .



2. Um einen primären Schlüsselserver hinzuzufügen, wählen Sie aus  **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  Zum Auswählen installierter Zertifikate, 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, 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 die Option aus  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 die Option aus  Wählen Sie dann External Key Manager bearbeiten .

2. Vorhandene Schlüsselservers sind in der Tabelle **Schlüsselservers** aufgeführt. Sie können folgende Vorgänge durchführen:
 - Fügen Sie einen neuen Schlüsselservers hinzu, indem Sie auswählen  **Add**.
 - Löschen Sie einen Schlüsselservers, indem Sie auswählen  Am Ende der Tabellenzelle, die den Namen des Schlüsselservers enthält. Die sekundären Schlüsselservers, die dem primären Schlüsselservers 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 SELECT aus  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 die Option aus  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 Schlüssellservern zu verwenden. Der erste Schlüssellserver 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:

```
cluster1::> 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:

```
svm11::> 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
```

```
cluster1::> security key-manager add -address 20.1.1.1
```



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

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

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

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



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

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

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

Eine vollständige Befehlssyntax finden Sie in der man-Page.

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

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

6. Konvertieren Sie optional Klartextvolumes in verschlüsselte Volumes.

```
volume encryption conversion start
```

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

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 KMS 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 „Erweitert“
`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"](#)

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 IRGEND EINER 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.