Externe Schlüsselverwaltung konfigurieren

ONTAP 9

NetApp
November 10, 2026

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

Inhalt

Externe Schlüsselverwaltung konfigurieren . . . 1
- Informationen zur externen ONTAP Schlüsselverwaltung für NetApp Volume Encryption . . . 1
- Externe Key Manager mit ONTAP System Manager verwalten . . . 1
  - Einen externen Schlüsselmanager konfigurieren . . . 2
  - Einen vorhandenen externen Schlüsselmanager bearbeiten . . . 3
  - Externen Schlüsselmanager löschen . . . 3
  - Schlüssel zwischen Schlüsselmanagern migrieren . . . 4
- SSL-Zertifikate auf dem ONTAP Cluster installieren . . . 4
- Externe Schlüsselverwaltung für NVE in ONTAP 9.6 und höher aktivieren . . . 5
- Externe Schlüsselverwaltung für NVE in ONTAP 9.5 und früher aktivieren . . . 8
- NVE-Schlüssel für ONTAP Daten-SVMs mit einem Cloud-Anbieter verwalten . . . 10
  - Externe Schlüsselverwaltung aktivieren . . . 11
- ONTAP-Schlüssel mit Barbican KMS verwalten . . . 13
  - Erstellen und Aktivieren einer Barbican KMS Konfiguration . . . 13
  - Die Anmeldeinformationen und Einstellungen einer Barbican KMS Konfiguration aktualisieren . . . 15
  - Schlüssel zwischen Barbican KMS und dem Onboard Key Manager migrieren . . . 16
  - Deaktivieren und Löschen einer Barbican KMS Konfiguration . . . 17

Externe Schlüsselverwaltung konfigurieren

Informationen zur externen ONTAP Schlüsselverwaltung für NetApp Volume Encryption

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

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

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

- **Schlüsselerstellung.** Wenn ONTAP einen neuen Schlüssel erstellt, beispielsweise beim Erstellen eines verschlüsselten FlexVol volume, FlexGroup volume oder Aggregats, speichert der Knoten, der den Schlüssel erstellt, diesen auf dem Schlüsselserver und sendet ihn dann an alle anderen Knoten im Cluster.
- **Schlüsselwiederherstellung nach einem Neustart.** Wenn ein Knoten neu startet, beispielsweise im Rahmen eines automatisierten unterbrechungsfreien Upgrade, einer Übernahme und Rückgabe oder eines ungeplanten Neustarts, stellt er seine Schlüssel von seinem HA-Partner wieder her. ONTAP kontaktiert den Schlüsselserver nur für Schlüssel, die der Partner nicht bereitstellen kann. Verfügt der Partner über alle Schlüssel, kann die Schlüsselwiederherstellung auch dann abgeschlossen werden, wenn der Schlüsselserver nicht verfügbar ist.

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

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

Externe Key Manager mit ONTAP System Manager verwalten

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

Der Onboard Key Manager speichert und verwaltet Schlüssel in einer sicheren Datenbank, die intern im

Cluster liegt. Sein Gültigkeitsbereich ist der Cluster. Ein externer Key Manager speichert und verwaltet Schlüssel außerhalb des Clusters. Sein Gültigkeitsbereich kann der Cluster oder die Storage-VM sein.

Über diese Aufgabe

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

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

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

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

Einen externen Schlüsselmanager konfigurieren

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

Schritte

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

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

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

2. Um einen Primärschlüsselserver hinzuzufügen, + Add auswählen und die Felder **IP-Adresse oder**

Hostname sowie **Port** ausfüllen.

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

Einen vorhandenen externen Schlüsselmanager bearbeiten

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

Schritte

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

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

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

Externen Schlüsselmanager löschen

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

Schritte

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

Umfang	Navigation	Startschritt

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

Schlüssel zwischen Schlüsselmanagern migrieren

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

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

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

SSL-Zertifikate auf dem ONTAP Cluster installieren

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

Über diese Aufgabe

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

Bevor Sie beginnen

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

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

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

Schritte

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

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

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

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

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

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

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

Verwandte Informationen

- "Sicherheitszertifikat installieren"

Externe Schlüsselverwaltung für NVE in ONTAP 9.6 und höher aktivieren

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

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

Über diese Aufgabe

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

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

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

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

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

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

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

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

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

Bevor Sie beginnen

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

Schritte

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

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

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

Der folgende Befehl aktiviert die externe Schlüsselverwaltung für `cluster1` mit drei externen

Schlüsselservern. Der erste Schlüsselserver wird über seinen Hostnamen und Port angegeben, der zweite über eine IP-Adresse und den Standardport, und der dritte über eine IPv6-Adresse und den Port:

```
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. Konfigurieren eines Schlüsselmanagers für eine SVM:

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

- Wenn der Befehl an der SVM-Anmeldeaufforderung ausgeführt wird, `SVM` gilt standardmäßig die aktuelle SVM. Der `security key-manager external modify` Befehl kann verwendet werden, um die Konfiguration der externen Schlüsselverwaltung zu ändern.
- In einer MetroCluster-Umgebung ist es bei der Konfiguration der externen Schlüsselverwaltung für eine Daten-SVM nicht erforderlich, den `security key-manager external enable` Befehl auf dem Partnercluster zu wiederholen.

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

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

3. Den letzten Schritt für alle weiteren SVMs wiederholen.

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

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

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

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

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

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

8 entries were displayed.
```

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

   `volume encryption conversion start`

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

Verwandte Informationen

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

Externe Schlüsselverwaltung für NVE in ONTAP 9.5 und früher aktivieren

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

Über diese Aufgabe

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

Bevor Sie beginnen

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

Schritte

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

   `security key-manager setup`

   Die Einrichtung des Schlüsselmanagers beginnt.

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

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

   `security key-manager add -address key_management_server_ipaddress`

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

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

4. Einen zusätzlichen KMIP Server für Redundanz hinzufügen:

   `security key-manager add -address key_management_server_ipaddress`

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

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

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

   `security key-manager show -status`

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

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

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

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

   `volume encryption conversion start`

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

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

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

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

> Ab ONTAP 9.20.1 migriert ONTAP beim Aktivieren eines Cloud Key Managers auf einer Daten-SVM, die bereits verschlüsselte Volumes über den Key Manager im Admin-Bereich verwaltet, diese NVE-Schlüssel automatisch zum neuen Daten-SVM Key Manager. In diesem Workflow ist kein separater `security key-manager key migrate` Befehl erforderlich.
>
> Diese automatische Migration gilt für Daten-SVMs. Beim Umstellen der Admin SVM von der integrierten Schlüsselverwaltung oder der externen Schlüsselverwaltung mit Cluster-Scope auf einen Cloud-Schlüsselmanager für Daten-SVMs müssen zunächst die entsprechenden Übergangsaufgaben für den Admin-Bereich abgeschlossen werden.

Über diese Aufgabe

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

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

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

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

Bevor Sie beginnen

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

Externe Schlüsselverwaltung aktivieren

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

AWS

Bevor Sie beginnen

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

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

AWS KMV auf einer ONTAP SVM aktivieren

1. Bevor Sie beginnen, sowohl die Zugriffsschlüssel-ID als auch den geheimen Schlüssel von Ihrem AWS KMS bereithalten.
2. Die Berechtigungsstufe wird auf „Erweitert“ gesetzt: `set -priv advanced`
3. AWS KMS aktivieren: `security key-manager external aws enable -vserver` *`svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. Bei Aufforderung ist der geheime Schlüssel einzugeben.
5. Es wird bestätigt, dass AWS KMS korrekt konfiguriert wurde: `security key-manager external aws show -vserver` *`svm_name`*

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

Azure

Azure Key Vault auf einer ONTAP SVM aktivieren

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

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

Google Cloud

Cloud KMS auf einer ONTAP SVM aktivieren

1. Bevor Sie beginnen, den privaten Schlüssel für die Google Cloud KMS Kontoschlüsseldatei im JSON-Format beschaffen. Dieser befindet sich in Ihrem GCP-Konto. Es muss außerdem sichergestellt sein, dass alle Knoten im Cluster fehlerfrei funktionieren. Dies lässt sich mit dem Befehl `cluster show` überprüfen. Weitere Informationen zu `cluster show` finden sich in der "ONTAP-Befehlsreferenz".
2. Berechtigungsstufe auf „Erweitert“ setzen: `set -priv advanced`
3. Cloud KMS auf der SVM aktivieren `security key-manager external gcp enable -vserver` *`svm_name`* `-project-id` *`project_id`*`-key-ring-name` *`key_ring_name`* `-key -ring-location` *`key_ring_location`* `-key-name` *`key_name`* Bei Aufforderung den Inhalt der JSON-Datei mit dem Service Account Private Key eingeben
4. Es sollte überprüft werden, ob Cloud KMS mit den korrekten Parametern konfiguriert ist: `security key-manager external gcp show vserver` *`svm_name`* Der Status von `kms_wrapped_key_status` wird `"UNKNOWN"` sein, wenn keine verschlüsselten Volumes erstellt wurden. Ist die Erreichbarkeit des Dienstes nicht gegeben, sollte die Konnektivität zum GCP Key Management Service über die Daten-SVM-LIF hergestellt werden.

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

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

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

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

Verwandte Informationen

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

ONTAP-Schlüssel mit Barbican KMS verwalten

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

Über diese Aufgabe

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

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

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

Bevor Sie beginnen

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

Erstellen und Aktivieren einer Barbican KMS Konfiguration

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

Schritte

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

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

```
-config-name <unique_config_name> -key-id <key_id> -keystone-url
<keystone_url> -application-cred-id
<keystone_applications_credentials_id>
```

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

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

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

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

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

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

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

2. Die neue Barbican KMS Konfiguration wird aktiviert:

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

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

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

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

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

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

Vserver: svm1
Node: node1

Category: service_reachability
              Status: OK

Category: kms_wrapped_key_status
              Status: OK
```

Die Anmeldeinformationen und Einstellungen einer Barbican KMS Konfiguration aktualisieren

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

Schritte

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

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

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

2. Die Einstellungen einer Barbican KMS Konfiguration aktualisieren:

   ```
   security key-manager external barbican update-config -vserver <svm_name>
   -config-name <unique_config_name> -timeout <timeout> -verify
   <true|false> -verify-host <true|false>
   ```

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

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

   ```
   security key-manager external barbican update-credentials -vserver
   ```

```
<svm_name> -config-name <unique_config_name> -application-cred-id
<keystone_applications_credentials_id>
```

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

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

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

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

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

      ```
      set -privilege advanced
      ```

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

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

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

Schlüssel zwischen Barbican KMS und dem Onboard Key Manager migrieren

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

Schritte

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

   ```
   set -privilege advanced
   ```

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

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

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

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

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

Deaktivieren und Löschen einer Barbican KMS Konfiguration

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

Schritte

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

```
set -privilege advanced
```

2. Eine aktive Barbican KMS Konfiguration deaktivieren:

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

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

3. Eine inaktive Barbican KMS Konfiguration löschen:

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

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.