設定外部金鑰管理
ONTAP 9

NetApp
February 12, 2026

目錄

設定外部金鑰管理 1
了解如何使用ONTAP NetApp磁碟區加密設定外部金鑰管理 1
使用ONTAP系統管理員管理外部金鑰管理器 1
設定外部金鑰管理程式 1
編輯現有的外部金鑰管理程式 2
刪除外部金鑰管理程式 2
在關鍵經理之間移轉金鑰 3
在ONTAP叢集上安裝 SSL 憑證 3
在ONTAP 9.6 及更高版本中為 NVE 啟用外部金鑰管理 4
在ONTAP 9.5 及更早版本中為 NVE 啟用外部金鑰管理 7
透過雲端供應商管理ONTAP資料 SVM 的 NVE 金鑰 8
啟用外部金鑰管理 9
使用 Barbican KMS 管理ONTAP金鑰 11
建立並啟動 Barbican KMS 配置 12
更新 Barbican KMS 配置的憑證和設置 13
在 Barbican KMS 和 Onboard Key Manager 之間遷移金鑰 14
停用並刪除 Barbican KMS 配置 15

設定外部金鑰管理

了解如何使用ONTAP NetApp磁碟區加密設定外部金鑰管理

您可以使用一個或多個外部金鑰管理伺服器來保護叢集用於存取加密資料的金鑰。外部金鑰管理伺服器是儲存環境中的第三方系統，它使用金鑰管理互通性協定 (KMIP) 向節點提供金鑰。除了板載金鑰管理器之外， ONTAP還支援多個外部金鑰管理伺服器。

從ONTAP 9.10.1 開始，您可以使用 Azure Key Vault 或 Google Cloud Key Manager 服務 保護您的資料 SVM 的 NVE 金鑰。從ONTAP 9.11.1 開始，您可以在叢集中設定多個外部金鑰管理員。看配置叢集金鑰伺服器。從ONTAP 9.12.0 開始，您可以使用 "AWS 的 KMS" 保護您的資料 SVM 的 NVE 金鑰。從ONTAP 9.17.1 開始，您可以使用 OpenStack 的 巴比肯 KMS 保護您的資料 SVM 的 NVE 金鑰。

使用ONTAP系統管理員管理外部金鑰管理器

從 ONTAP 9.7 開始、您可以使用內建金鑰管理程式來儲存及管理驗證與加密金鑰。從 ONTAP 9.13.1 開始、您也可以使用外部金鑰管理員來儲存及管理這些金鑰。

Onboard Key Manager 會將金鑰儲存並管理在叢集內部的安全資料庫中。其範圍是叢集。外部金鑰管理程式會儲存和管理叢集外部的金鑰。其範圍可以是叢集或儲存 VM 。可以使用一或多個外部金鑰管理員。適用下列條件：

- 如果已啟用 Onboard Key Manager 、則無法在叢集層級啟用外部金鑰管理程式、但可以在儲存 VM 層級啟用外部金鑰管理程式。
- 如果在叢集層級啟用外部金鑰管理程式、則無法啟用 Onboard Key Manager 。

使用外部金鑰管理程式時、每個儲存 VM 和叢集最多可註冊四個主要金鑰伺服器。每個主要金鑰伺服器最多可叢集三個次要金鑰伺服器。

設定外部金鑰管理程式

若要新增儲存 VM 的外部金鑰管理程式、您應該在設定儲存 VM 的網路介面時新增選用閘道。如果儲存 VM 是在沒有網路路由的情況下建立的、您必須為外部金鑰管理程式明確建立路由。請參閱 "建立 LIF （網路介面）"。

步驟

您可以從 System Manager 的不同位置設定外部金鑰管理程式。

1. 若要設定外部金鑰管理程式、請執行下列其中一個啟動步驟。

工作流程	導覽	開始步驟
設定金鑰管理程式	• 叢集 * > * 設定 *	捲動至 * 安全性 * 區段。在 * 加密 * 下，選擇 ⚙。選取 * 外部金鑰管理員 * 。
新增本機層	• 儲存 * > * Tiers*	選取 *+ 新增本機層 * 。核取標有「 Configure Key Manager 」的核取方塊。選取 * 外部金鑰管理員 * 。

準備儲存設備	• 儀表板 *	在 * 容量 * 區段中、選取 * 準備儲存 * 。 然後選取「設定金鑰管理程式」。選取 * 外部金鑰管理員 * 。
設定加密（僅限儲存 VM 範圍的金鑰管理程式）	• 儲存 * > * 儲存 VM *	選取儲存VM。選取 * 設定 * 索引標籤。在 * 安全 * 下的 * 加密 * 區段中，選擇 。

2. 要添加主密鑰服務器，請選擇 + Add ，然後填寫 **IP** 地址或主機名 * 和 ***Port** 字段。
3. 現有安裝的憑證會列在 * KMIP 伺服器 CA 憑證 * 和 * KMIP 用戶端憑證 * 欄位中。 您可以執行下列任一動作：
   - 選取 ⌄ 以選取您要對應至金鑰管理程式的已安裝憑證。（可以選取多個服務 CA 憑證、但只能選取一個用戶端憑證。）
   - 選取 * 新增憑證 * 以新增尚未安裝的憑證、並將其對應至外部金鑰管理員。
   - 選取 × 憑證名稱旁的、以刪除您不想對應至外部金鑰管理程式的已安裝憑證。
4. 若要新增次要金鑰伺服器、請在 * 次要金鑰伺服器 * 欄中選取 * 新增 * 、並提供詳細資料。
5. 選取 * 儲存 * 以完成組態。

編輯現有的外部金鑰管理程式

如果您已設定外部金鑰管理員、則可以修改其設定。

步驟

1. 若要編輯外部金鑰管理程式的組態、請執行下列其中一個開始步驟。

範圍	導覽	開始步驟
叢集範圍外部金鑰管理程式	• 叢集 * > * 設定 *	捲動至 * 安全性 * 區段。在 * 加密 * 下，選擇 ⋮ ，然後選擇 * 編輯外部金鑰管理程式 * 。
儲存 VM 範圍外部金鑰管理程式	• 儲存 * > * 儲存 VM *	選取儲存VM。選取 * 設定 * 索引標籤。在 * 安全性 * 下的 * 加密 * 區段中、選取 ⋮ 、然後選取 * 編輯外部金鑰管理員 * 。

2. 現有的主要伺服器會列在 * 金鑰伺服器 * 表中。您可以執行下列作業：
   - 選取以新增金鑰伺服器 + Add 。
   - 選取包含金鑰伺服器名稱的表格儲存格結尾處、以刪除金鑰伺 ⋮ 服器。與該主要金鑰伺服器相關的次要金鑰伺服器也會從組態中移除。

刪除外部金鑰管理程式

如果磁碟區未加密、則可以刪除外部金鑰管理程式。

步驟

1. 若要刪除外部金鑰管理程式、請執行下列其中一個步驟。

範圍	導覽	開始步驟
叢集範圍外部金鑰管理程式	• 叢集 * > * 設定 *	捲動至 * 安全性 * 區段。在 * 加密 * 下、選取 ⋮、然後選取 * 刪除外部金鑰管理員 * 。
儲存 VM 範圍外部金鑰管理程式	• 儲存 * > * 儲存 VM *	選取儲存VM。選取 * 設定 * 索引標籤。在 * 安全性 * 下的 * 加密 * 區段中、選取 ⋮、然後選取 * 刪除外部金鑰管理員 * 。

在關鍵經理之間移轉金鑰

當叢集上啟用多個金鑰管理程式時、金鑰必須從一個金鑰管理程式移轉至另一個金鑰管理程式。系統管理員會自動完成此程序。

- 如果已在叢集層級啟用 Onboard Key Manager 或外部金鑰管理程式、且某些磁碟區已加密、 然後、當您在儲存 VM 層級設定外部金鑰管理程式時、金鑰必須從叢集層級的 Onboard Key Manager 或外部金鑰管理程式移轉至儲存 VM 層級的外部金鑰管理程式。系統管理員會自動完成此程序。
- 如果在儲存 VM 上建立的磁碟區沒有加密、則不需要移轉金鑰。

在ONTAP叢集上安裝 SSL 憑證

叢集與KMIP伺服器使用KMIP SSL憑證來驗證彼此的身分、並建立SSL連線。在使用KMIP伺服器設定SSL連線之前、您必須先安裝叢集的KMIP用戶端SSL憑證、以及KMIP伺服器根憑證授權單位（CA）的SSL公開憑證。

關於這項工作

在HA配對中、兩個節點必須使用相同的公有和私有KMIP SSL憑證。如果您將多個HA配對連線至相同的KMIP伺服器、HA配對中的所有節點都必須使用相同的公有和私有KMIP SSL憑證。

開始之前

- 建立憑證、KMIP伺服器和叢集的伺服器上、必須同步時間。
- 您必須已取得叢集的公用SSL KMIP用戶端憑證。
- 您必須取得與叢集SSL KMIP用戶端憑證相關的私密金鑰。
- SSL KMIP用戶端憑證不得受密碼保護。
- 您必須已取得KMIP伺服器根憑證授權單位（CA）的SSL公開憑證。
- 在 MetroCluster 環境中、您必須在兩個叢集上安裝相同的 KMIP SSL 憑證。

您可以在叢集上安裝憑證之前或之後、在KMIP伺服器上安裝用戶端和伺服器憑證。

步驟

1. 安裝叢集的SSL KMIP用戶端憑證：

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

系統會提示您輸入SSL KMIP公開和私有憑證。

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

2. 安裝KMIP伺服器根憑證授權單位（CA）的SSL公開憑證：

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

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

相關資訊

- "安全性憑證安裝"

在ONTAP 9.6 及更高版本中為 NVE 啟用外部金鑰管理

使用 KMIP 伺服器來保護叢集用於存取加密資料的金鑰。從ONTAP 9.6 開始，您可以選擇配置單獨的外部金鑰管理器來保護資料 SVM 用於存取加密資料的金鑰。

從 ONTAP 9.11.1 開始、每個主要金鑰伺服器最多可新增 3 個次要金鑰伺服器、以建立叢集金鑰伺服器。如需詳細資訊、請參閱 設定叢集式外部金鑰伺服器。

關於這項工作

您最多可以將四個 KMIP 伺服器連接到叢集或 SVM。使用至少兩台伺服器以實現冗餘和災難復原。

外部金鑰管理的範圍決定了金鑰管理伺服器是保護叢集中的所有SVM、還是僅保護選取的SVM：

- 您可以使用_叢集範圍_來設定叢集中所有SVM的外部金鑰管理。叢集管理員可以存取儲存在伺服器上的每個金鑰。
- 從ONTAP 功能表9.6開始、您可以使用_SVM範圍來設定叢集中資料SVM的外部金鑰管理。這最適合多租戶環境、每個租戶使用不同的SVM（或一組SVM）來提供資料。只有特定租戶的SVM管理員可以存取該租戶的金鑰。
- 對於多租戶環境、請使用下列命令安裝_MT_EK-Mgmt_的授權：

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

  如"指令參考資料ONTAP"需詳細 `system license add`資訊，請參閱。

您可以在同一個叢集中使用這兩個範圍。如果SVM已設定金鑰管理伺服器、ONTAP 則僅使用這些伺服器來保護金鑰。否則ONTAP 、利用為叢集設定的金鑰管理伺服器來保護金鑰。

您可以在叢集範圍設定內建金鑰管理、並在SVM範圍設定外部金鑰管理。您可以使用 `security key-manager key migrate` 命令將金鑰從叢集範圍內的機載金鑰管理移轉至 SVM 範圍內的外部金鑰管理程式。

如"指令參考資料ONTAP"需詳細 `security key-manager key migrate`資訊，請參閱。

開始之前

- KMIP SSL用戶端和伺服器憑證必須已安裝。
- KMIP 伺服器必須能夠從每個節點的節點管理 LIF 存取。

- 您必須是叢集或SVM管理員、才能執行此工作。
- 在MetroCluster環境中：
  - 在啟用外部金鑰管理之前，必須完全配置MetroCluster 。
  - 您必須在兩個叢集上安裝相同的 KMIP SSL 憑證。
  - 必須在兩個叢集上配置外部密鑰管理器。

步驟

1. 設定叢集的金鑰管理程式連線：

   ```
   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
   ```

   這 `security key-manager external enable`命令替換 `security key-manager setup`命令。如果在叢集登入提示字元下執行該命令， `*admin_SVM*`預設為目前叢集的管理 SVM。您可以運行 `security key-manager external modify`命令來更改外部密鑰管理配置。

   下列命令可啟用的外部金鑰管理 `cluster1` 使用三個外部金鑰伺服器。第一個金鑰伺服器是使用其主機名稱和連接埠來指定、第二個金鑰伺服器是使用IP位址和預設連接埠來指定、第三個金鑰伺服器則是使用IPv6位址和連接埠來指定：

   ```
   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. 設定SVM的金鑰管理程式：

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

   - 如果在 SVM 登入提示字元下執行該命令， `SVM`預設為當前 SVM。您可以運行 `security key-manager external modify`命令來更改外部密鑰管理配置。
   - 在支援資料SVM的環境中、如果您要設定外部金鑰管理、就不需要重複執行MetroCluster `security key-manager external enable` 合作夥伴叢集上的命令。

   下列命令可啟用的外部金鑰管理 `svm1` 使用單一金鑰伺服器聆聽預設連接埠 5696 ：

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

3. 針對任何其他SVM重複最後一個步驟。

> 您也可以使用 `security key-manager external add-servers`命令來設定其他 SVM 。命令會 `security key-manager external add-servers`取代 `security key-manager add`命令。如"指令參考資料ONTAP"需詳細 `security key-manager external add-servers`資訊，請參閱。

4. 確認所有已設定的KMIP伺服器均已連線：

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

> 命令會 `security key-manager external show-status`取代 `security key-manager show -status`命令。如"指令參考資料ONTAP"需詳細 `security key-manager external show-status`資訊，請參閱。

```
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. 也可以將純文字磁碟區轉換為加密磁碟區。

```
volume encryption conversion start
```

在轉換磁碟區之前，必須完全設定外部金鑰管理員。

相關資訊

- 設定叢集式外部金鑰伺服器
- "系統許可證添加"

- "安全金鑰管理員金鑰遷移"
- "安全金鑰管理員外部新增伺服器"
- "安全金鑰管理員外部顯示狀態"

在ONTAP 9.5 及更早版本中為 NVE 啟用外部金鑰管理

您可以使用一或多個KMIP伺服器來保護叢集用來存取加密資料的金鑰。您最多可將四個KMIP伺服器連線至一個節點。建議至少使用兩部伺服器來進行備援和災難恢復。

關於這項工作

可為叢集中的所有節點設定KMIP伺服器連線。ONTAP

開始之前

- KMIP SSL用戶端和伺服器憑證必須已安裝。
- 您必須是叢集管理員才能執行此工作。
- 在設定外部金鑰管理程式之前、您必須先設定MetroCluster 此解決方案。
- 在 MetroCluster 環境中、您必須在兩個叢集上安裝相同的 KMIP SSL 憑證。

步驟

1. 設定叢集節點的金鑰管理程式連線：

   ```
   security key-manager setup
   ```

   金鑰管理程式設定隨即開始。

   在MetroCluster環境中，您必須在兩個叢集上執行此命令。詳細了解 `security key-manager setup`在"指令參考資料ONTAP"。

2. 在每個提示字元輸入適當的回應。
3. 新增KMIP伺服器：

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

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

   在這個不支援的環境中、您必須在兩個叢集上執行此命令MetroCluster 。

4. 新增額外的KMIP伺服器以提供備援：

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

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

在這個不支援的環境中、您必須在兩個叢集上執行此命令MetroCluster 。

5. 確認所有已設定的KMIP伺服器均已連線：

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

   詳細了解此過程中所述的命令"指令參考資料ONTAP"。

   ```
   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. 也可以將純文字磁碟區轉換為加密磁碟區。

   ```
   volume encryption conversion start
   ```

   在轉換磁碟區之前、必須先完整設定外部金鑰管理程式。在 MetroCluster 環境中、必須在兩個站台上設定外部金鑰管理員。

透過雲端供應商管理ONTAP資料 SVM 的 NVE 金鑰

從 ONTAP 9.10.1 開始，您可以在雲端代管應用程式中使用"Azure Key Vault（AKV）"和"Google Cloud Platform的金鑰管理服務（雲端KMS）"保護 ONTAP 加密金鑰。從 ONTAP 9.12.0 開始，您也可以使用來保護 NVE 金鑰"AWS 的 KMS"。

AWS KMS 、 AKV 和 Cloud KMS 可用於保護 "NetApp Volume Encryption（NVE）金鑰" 僅適用於資料SVM。

關於這項工作

您可以使用 CLI 或 ONTAP REST API 來啟用雲端供應商的金鑰管理。

使用雲端供應商保護金鑰時、請注意、根據預設、資料 SVM LIF 會用於與雲端金鑰管理端點通訊。節點管理網路用於與雲端供應商的驗證服務（login.microsoftonline.com for Azure；oauth2.googleapis.com for Cloud KMS ）進行通訊。如果叢集網路未正確設定，叢集將無法正確使用金鑰管理服務。

使用雲端供應商金鑰管理服務時、您應注意下列限制：

- 雲端供應商金鑰管理不適用於 NetApp 儲存加密（ NSE ）和 NetApp Aggregate Encryption （ NAE ）。"外部KMIP" 可以改用。
- 雲端供應商金鑰管理不適用於 MetroCluster 組態。
- 雲端供應商金鑰管理只能在資料 SVM 上設定。

開始之前

- 您必須在適當的雲端供應商上設定 KMS 。
- ONTAP 叢集的節點必須支援 NVE 。
- "您必須已安裝 Volume Encryption （ VE ）和多租戶加密金鑰管理（ MTEKM ）授權"。這些授權隨附於"ONTAP One"。
- 您必須是叢集或 SVM 管理員。
- 資料 SVM 不得包含任何加密的磁碟區、也不得採用金鑰管理程式。如果資料 SVM 包含加密的磁碟區、您必須先移轉這些磁碟區、才能設定 KMS 。

啟用外部金鑰管理

啟用外部金鑰管理取決於您使用的特定金鑰管理程式。選擇適當的金鑰管理程式和環境標籤。

AWS

開始之前

- 您必須為 AWS KMS 金鑰建立授權、以便由管理加密的 IAM 角色使用。IAM 角色必須包含允許下列作業的原則：
  - `DescribeKey`
  - `Encrypt`
  - `Decrypt`

    如需詳細資訊、請參閱 AWS 文件 "補助"。

在 **ONTAP SVM** 上啟用 **AWS KMV**

1. 開始之前、請先從 AWS KMS 取得存取金鑰 ID 和秘密金鑰。
2. 將權限層級設為進階： `set -priv advanced`
3. 啟用 AWS KMS ： `security key-manager external aws enable -vserver` *`svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. 出現提示時、請輸入秘密金鑰。
5. 確認 AWS KMS 已正確設定： `security key-manager external aws show -vserver` *`svm_name`*

   如"指令參考資料ONTAP"需詳細 `security key-manager external aws`資訊，請參閱。

Azure

在 **ONTAP SVM** 上啟用 **Azure Key Vault**

1. 開始之前、您必須先從Azure帳戶取得適當的驗證認證資料、包括用戶端機密或憑證。您也必須確保叢集中的所有節點都正常運作。您可以使用命令來檢查 `cluster show`。如"指令參考資料ONTAP"需詳細 `cluster show`資訊，請參閱。
2. 將權限層級設為進階 `set -priv advanced`
3. 在 SVM 上啟用 AKV `security key-manager external azure enable -client-id` *`client_id`* `-tenant-id` *`tenant_id`* `-name -key-id` *`key_id`* `-authentication-method {certificate|client-secret}` 出現提示時、請輸入 Azure 帳戶的用戶端憑證或用戶端機密。
4. 確認 AKV 已正確啟用： `security key-manager external azure show vserver` *`svm_name`* 如果服務連線能力不正常、請透過資料 SVM LIF 建立與 AKV 金鑰管理服務的連線。

   如"指令參考資料ONTAP"需詳細 `security key-manager external azure`資訊，請參閱。

Google Cloud

在 **ONTAP SVM** 上啟用雲端 **KMS**

1. 開始之前、請先以 JSON 格式取得 Google Cloud KMS 帳戶金鑰檔案的私密金鑰。您可以在GCP帳戶中找到這項資訊。您也必須確保叢集中的所有節點都正常運作。您可以使用命令來檢查 `cluster show`。如"指令參考資料ONTAP"需詳細 `cluster show`資訊，請參閱。
2. 將權限等級設為進階： `set -priv advanced`

3. 在 SVM 上啟用 Cloud KMS `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` 出現提示時、請使用服務帳戶私密金鑰輸入 JSON 檔案的內容
4. 驗證 Cloud KMS 是否配置了正確的參數： `security key-manager external gcp show vserver svm_name`現狀 `kms_wrapped_key_status`將 `"UNKNOWN"`如果沒有建立加密磁碟區。如果服務可達性不正常，則透過資料 SVM LIF 建立與 GCP 金鑰管理服務的連線。

   如"指令參考資料ONTAP"需詳細 `security key-manager external gcp`資訊，請參閱。

如果已為資料SVM設定一或多個加密磁碟區、且對應的NVE金鑰由管理SVM內建金鑰管理程式管理、則這些金鑰應移轉至外部金鑰管理服務。若要使用 CLI 執行此作業、請執行命令： `security key-manager key migrate -from-Vserver admin_SVM -to-Vserver data_SVM` 在成功移轉資料 SVM 的所有 NVE 金鑰之前、無法為租戶的資料 SVM 建立新的加密磁碟區。

相關資訊

- "使用適用於 Cloud Volumes ONTAP 的 NetApp 加密解決方案來加密磁碟區"
- "安全金鑰管理員外部"

使用 Barbican KMS 管理ONTAP金鑰

從ONTAP 9.17.1 開始，您可以使用 OpenStack 的"巴比肯 KMS"保護ONTAP加密金鑰。BarbicanKMS 是一項安全儲存和存取金鑰的服務。 BarbicanKMS 可用於保護資料 SVM 的NetApp磁碟區加密 (NVE) 金鑰。 Barbican依賴"OpenStack Keystone" ，OpenStack 的身份服務，用於身份驗證。

關於這項工作

您可以使用 CLI 或ONTAP REST API 使用 Barbican KMS 設定金鑰管理。在 9.17.1 版本中，Barbican KMS 支援有以下限制：

- Barbican KMS 不支援NetApp儲存加密 (NSE) 和NetApp聚合加密 (NAE)。或者，您可以使用"外部 KMIP"或"板載密鑰管理器 (OKM)"用於 NSE 和 NVE 金鑰。
- MetroCluster配置不支援 Barbican KMS。
- Barbican KMS 只能為資料 SVM 配置，不適用於管理 SVM。

除非另有說明，管理員 `admin`特權等級可以執行下列操作程序。

開始之前

- 必須配置 Barbican KMS 和 OpenStack Keystone 。您用於 Barbican 的 SVM 必須能夠透過網路存取 Barbican 和 OpenStack Keystone伺服器。
- 如果您正在為 Barbican 和 OpenStack Keystone伺服器使用自訂憑證授權單位 (CA)，則必須使用 `security certificate install -type server-ca -vserver <admin_svm>` 。

建立並啟動 **Barbican KMS** 配置

您可以為 SVM 建立新的 Barbican KMS 配置並將其啟動。一個 SVM 可以有多個非活動的 Barbican KMS 配置，但一次只能有一個處於活動狀態。

步驟

1. 為 SVM 建立新的非活動 Barbican KMS 配置：

```
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`是 `Barbican 密鑰加密密鑰 (KEK) 的密鑰標識符。請輸入完整的 URL，包括 `https:// 。

> 某些 URL 包含問號 (?)。問號用於啟動ONTAP命令列活動幫助。要輸入帶有問號的 URL，您需要先使用以下命令停用活動協助 `set -active-help false` 。稍後可以使用以下命令重新啟用主動協助 `set -active-help true`了解更多信息"指令參考資料ONTAP" 。

   - `-keystone-url`是 `OpenStack Keystone授權主機的 URL。請輸入完整的 URL，包括 `https:// 。
   - `-application-cred-id`是應用程式憑證 ID。

     輸入此命令後，系統將提示您輸入應用程式憑證金鑰。此指令將建立一個非活動的 Barbican KMS 配置。

     以下範例建立一個名為的非活動 Barbican KMS 配置 `config1`對於`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. 啟動新的 Barbican KMS 配置：

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

   您可以使用此命令在 Barbican KMS 配置之間切換。如果 SVM 上已存在活動的 Barbican KMS 配置，則該配置將處於非活動狀態，並啟動新的配置。

3. 驗證新的 Barbican KMS 配置是否處於活動狀態：

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

此指令將提供 SVM 或節點上活動的 Barbican KMS 配置的狀態。例如，如果 SVM `svm1`在節點上 `node1` 具有活動的 Barbican KMS 配置，以下命令將傳回該配置的狀態：

```
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
```

更新 **Barbican KMS** 配置的憑證和設置

您可以檢視和更新活動或非活動的 Barbican KMS 配置的目前設定。

步驟

1. 查看 SVM 的目前 Barbican KMS 配置：

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

顯示 SVM 上每個 Barbican KMS 配置的金鑰 ID、OpenStack Keystone URL 和應用程式憑證 ID。

2. 更新 Barbican KMS 配置的設定：

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

此指令更新指定 Barbican KMS 設定的逾時和驗證設定。 `timeout`確定ONTAP在連線失敗前等待 `Barbican` 回應的時間（以秒為單位）。預設 `timeout`是十秒。 `verify`和 `verify-host`確定在連線之前是否應分別驗證 `Barbican` 主機的身份和主機名稱。預設情況下，這些參數設定為 `true` 。這 `vserver`和 `config-name`參數是必需的。其他參數是可選的。

3. 如果需要，請更新活動或非活動的 Barbican KMS 配置的憑證：

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

輸入此命令後，系統將提示您輸入新的應用程式憑證金鑰。

4. 如果需要，為活動的 Barbican KMS 設定恢復遺失的 SVM 金鑰加密金鑰 (KEK)：
   a. 使用以下方式恢復遺失的 SVM KEK `security key-manager external barbican restore` ：

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

      此命令將透過與 Barbican 伺服器通訊來恢復活動 Barbican KMS 配置的 SVM KEK。

5. 如果需要，請為 Barbican KMS 設定重新金鑰 SVM KEK：
   a. 將權限層級設為進階：

      ```
      set -privilege advanced
      ```

   b. 使用以下方式重新金鑰 SVM KEK `security key-manager external barbican rekey-internal` ：

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

      此指令會為指定的 SVM 產生新的 SVM KEK，並使用新的 SVM KEK 重新封裝磁碟區加密金鑰。新的 SVM KEK 將受到有效的 Barbican KMS 配置的保護。

在 **Barbican KMS** 和 **Onboard Key Manager** 之間遷移金鑰

您可以將密鑰從 Barbican KMS 遷移到板載密鑰管理器 (OKM)，反之亦然。要了解有關 OKM 的更多信息，請參閱"啟用更新版本的更新版本、以利執行內建金鑰管理ONTAP" 。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 如果需要，將密鑰從 Barbican KMS 遷移到 OKM：

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

`svm_name`是具有 Barbican KMS 配置的 SVM 的名稱。

3. 如果需要，將密鑰從 OKM 遷移到 Barbican KMS：

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

停用並刪除 **Barbican KMS** 配置

您可以停用沒有加密磁碟區的活動 Barbican KMS 配置，並且可以刪除非活動的 Barbican KMS 配置。

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 禁用活動的 Barbican KMS 配置：

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

如果 SVM 上存在 NVE 加密磁碟區，則必須解密它們，否則遷移金鑰在停用 Barbican KMS 配置之前。啟動新的 Barbican KMS 配置不需要解密 NVE 磁碟區或遷移金鑰，並且會停用目前活動的 Barbican KMS 配置。

3. 刪除不活動的 Barbican KMS 配置：

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