設定外部金鑰管理
ONTAP 9

NetApp
February 12, 2026

目錄

設定外部金鑰管理

了解如何設定ONTAP外部金鑰管理

您可以使用一或多個外部金鑰管理伺服器來保護叢集用來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、使用金鑰管理互通性傳輸協定（KMIP）為節點提供金鑰。

NetApp Volume Encryption （ NVE ）可透過內建金鑰管理程式來實作。在更新版本的支援中、NVE可透過外部金鑰管理（KMIP）和內建金鑰管理程式來實作。ONTAP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。請參閱 設定叢集式金鑰伺服器。

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 及更高版本中啟用基於硬體的加密的外部金鑰管理

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。

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。

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MetroCluster環境中：
  - 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。
  - 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
   ```

   - 命令會 `security key-manager external enable`取代 `security key-manager setup`命令。您可以執行 `security key-manager external modify`命令來變更外部金鑰管理組態。如"指令參考資料ONTAP"需詳細 `security key-manager external enable`資訊，請參閱。
   - 在支援管理SVM的環境中、如果您要設定外部金鑰管理、則必須重複執行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 `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 -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. 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 -vserver SVM -key
   ```

```
-server host_name|IP_address:port -key-server-status available|not-
responding|unknown
```

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
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available
node2
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available

6 entries were displayed.
```

相關資訊

- 設定叢集式外部金鑰伺服器
- "安全金鑰管理員外部啟用"
- "安全金鑰管理員外部顯示狀態"

在ONTAP 9.5 及更早版本中啟用基於硬體的加密的外部金鑰管理

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。

在 ONTAP 中設定叢集式外部金鑰伺服器

從ONTAP 9.11.1 開始，您可以在 SVM 上設定與叢集外部金鑰管理伺服器的連線。使用叢集金鑰伺服器，您可以在 SVM 上指定主金鑰伺服器和輔助金鑰伺服器。註冊或檢索金鑰時， ONTAP首先嘗試存取主密鑰伺服器，然後依序嘗試存取輔助伺服器，直到操作成功完成。

您可以使用外部金鑰伺服器來取得NetApp儲存加密 (NSE)、 NetApp磁碟區加密 (NVE) 和NetApp聚合加密 (NAE) 金鑰。一個 SVM 最多可以支援四個主外部 KMIP 伺服器。每個主伺服器最多可支援三個輔助密鑰伺服器。

關於這項工作

- 此程序僅支援使用KMIP的主要伺服器。如需支援的金鑰伺服器清單、請查看 "NetApp 互通性對照表工具"。

開始之前

- "必須為 SVM 啟用 KMIP 金鑰管理"。
- 叢集中的所有節點都必須執行ONTAP 版本不符合要求的9.11.1或更新版本。
- 伺服器的排列順序 `-secondary-key-servers`此參數反映了外部金鑰管理（KMIP）伺服器的存取順序。

建立叢集式金鑰伺服器

組態程序取決於您是否已設定主要金鑰伺服器。

將主要和次要金鑰伺服器新增至**SVM**

步驟

1. 確認叢集（admin SVM）未啟用任何金鑰管理功能：

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

   如果 SVM 已啟用最多四個主金鑰伺服器，則必須先刪除一個現有的主金鑰伺服器，然後再新增新的主金鑰伺服器。

2. 啟用主密鑰管理器：

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

   - 如果您沒有在參數中指定端口， `-key-servers`如果使用參數，則預設使用連接埠 5696。

   > 如果你正在運行 `security key-manager external enable`對於MetroCluster配置中的管理 SVM 指令，必須在兩個叢集上執行此命令。如果你要為單一資料 SVM 執行命令，則無需在兩個叢集上執行該命令。 NetApp強烈建議在兩個叢集上使用相同的金鑰伺服器。

3. 修改主密鑰伺服器，新增輔助密鑰伺服器。這 `-secondary-key-servers`此參數接受一個以逗號分隔的列表，最多可包含三個金鑰伺服器：

   ```
   security key-manager external modify-server -vserver <svm_name> -key
   -servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
   ```

   - 請勿在輔助密鑰伺服器中包含連接埠號碼。 `-secondary-key-servers`範圍。它使用與主密鑰伺服器相同的連接埠號碼。

   > 如果你正在運行 `security key-manager external`對於MetroCluster配置中的管理 SVM 指令，必須在兩個叢集上執行此命令。如果你要為單一資料 SVM 執行命令，則無需在兩個叢集上執行該命令。 NetApp強烈建議在兩個叢集上使用相同的金鑰伺服器。

新增次要金鑰伺服器至現有的主要金鑰伺服器

步驟

1. 修改主密鑰伺服器，新增輔助密鑰伺服器。這 `-secondary-key-servers`此參數接受一個以逗號分隔的列表，最多可包含三個金鑰伺服器：

   ```
   security key-manager external modify-server -vserver <svm_name> -key
   -servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
   ```

   - 請勿在輔助密鑰伺服器中包含連接埠號碼。 `-secondary-key-servers`範圍。它使用與主密鑰伺服器相同的連接埠號碼。

如果你正在運行 `security key-manager external modify-server`對於MetroCluster配置中的管理 SVM 指令，必須在兩個叢集上執行此命令。如果你要為單一資料 SVM 執行命令，則無需在兩個叢集上執行該命令。 NetApp強烈建議在兩個叢集上使用相同的金鑰伺服器。

有關輔助密鑰伺服器的更多信息，請參閱 [mod-secondary]。

修改叢集式金鑰伺服器

您可以透過新增和刪除輔助金鑰伺服器、變更輔助金鑰伺服器的存取順序或變更特定金鑰伺服器的指定（主金鑰伺服器或輔助金鑰伺服器）來修改叢集外部金鑰伺服器。如果在MetroCluster配置中修改叢集外部金鑰伺服器，NetApp強烈建議在兩個叢集上使用相同的金鑰伺服器。

修改次要金鑰伺服器

使用 `security key-manager external modify-server` 指令的 `-secondary-key-servers` 參數來管理次要金鑰伺服器。這 `-secondary-key-servers` 參數接受以逗號分隔的清單。清單中輔助密鑰伺服器的指定順序決定了輔助密鑰伺服器的存取順序。您可以透過執行指令 `security key-manager external modify-server`，並以不同順序輸入次要金鑰伺服器，來修改存取順序。輔助密鑰伺服器無需提供連接埠號碼。

如果你正在運行 `security key-manager external modify-server`對於MetroCluster配置中的管理 SVM 指令，必須在兩個叢集上執行此命令。如果你要為單一資料 SVM 執行命令，則無需在兩個叢集上執行該命令。

若要移除輔助密鑰伺服器，請將要保留的密鑰伺服器新增至清單中。 `-secondary-key-servers`參數，並省略要刪除的參數。若要刪除所有輔助密鑰伺服器，請使用下列參數 `-`表示無。

轉換主要和次要金鑰伺服器

您可以使用下列步驟變更特定金鑰伺服器的指定（主金鑰伺服器或輔助金鑰伺服器）。

將主密鑰伺服器轉換為輔助密鑰伺服器

步驟

1. 從SVM中移除主密鑰伺服器：

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

> 如果你正在運行 `security key-manager external remove-servers`對於MetroCluster配置中的管理 SVM 指令，必須在兩個叢集上執行此命令。如果你要為單一資料 SVM 執行命令，則無需在兩個叢集上執行該命令。

2. 執行[建立叢集式金鑰伺服器]使用原主密鑰伺服器作為輔助密鑰伺服器進行此程序。

將輔助金鑰伺服器轉換為主金鑰伺服器

步驟

1. 從現有的主密鑰伺服器移除輔助密鑰伺服器：

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

- 如果你正在運行 `security key-manager external modify-server -secondary-key-servers`對於MetroCluster配置中的管理 SVM 指令，必須在兩個叢集上執行此命令。如果你要為單一資料 SVM 執行命令，則無需在兩個叢集上執行該命令。
- 如果在刪除現有密鑰伺服器的同時將輔助密鑰伺服器轉換為主密鑰伺服器，則在完成刪除和轉換之前嘗試新增新的密鑰伺服器可能會導緻密鑰重複。

1. 執行[建立叢集式金鑰伺服器]使用原輔助金鑰伺服器作為新叢集金鑰伺服器的主金鑰伺服器進行此程序。

請參閱[mod-secondary]了解更多。

相關資訊

- 了解更多 `security key-manager external`在"指令參考資料ONTAP"

建立ONTAP 驗證金鑰、請使用32個以上版本

您可以使用 `security key-manager key create` 命令可建立節點的驗證金鑰、並將其儲存在設定的 KMIP 伺服器上。

關於這項工作

如果您的安全性設定要求您使用不同的金鑰進行資料驗證和FIPS 140-2驗證、您應該為每個金鑰建立個別的金鑰。如果情況並非如此、您可以使用與資料存取相同的 FIPS 法規遵循驗證金鑰。

此功能可為叢集中的所有節點建立驗證金鑰。ONTAP

- 啟用Onboard Key Manager時、不支援此命令。不過、啟用Onboard Key Manager時、會自動建立兩個驗證金鑰。您可以使用下列命令來檢視金鑰：

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

- 如果設定的金鑰管理伺服器已儲存超過128個驗證金鑰、您會收到警告。
- 您可以使用 `security key-manager key delete`命令刪除任何未使用的金鑰。 `security key-manager key delete`如果指定金鑰目前正由 ONTAP 使用，則命令會失敗。（ Privileges 必須大於 `admin`才能使用此命令。）

> 在支援功能環境中、刪除金鑰之前、您必須先確定合作夥伴叢集上沒有使用金鑰MetroCluster。您可以在合作夥伴叢集上使用下列命令、檢查金鑰是否未被使用：
>
> - `storage encryption disk show -data-key-id <key-id>`
> - `storage encryption disk show -fips-key-id <key-id>`

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 建立叢集節點的驗證金鑰：

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

> 此設定 `prompt-for-key=true`會讓系統提示叢集管理員在驗證加密磁碟機時使用複雜密碼。否則、系統會自動產生32位元組的通關密碼。命令會 `security key-manager key create`取代 `security key-manager create-key`命令。如"指令參考資料ONTAP"需詳細 `security key-manager key create`資訊，請參閱。

下列範例會建立的驗證金鑰 `cluster1`，自動產生 32 位元組的複雜密碼：

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

2. 確認已建立驗證金鑰：

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

> 命令會 `security key-manager key query`取代 `security key-manager query key`命令。
>
> 輸出中顯示的金鑰ID是用來參照驗證金鑰的識別碼。它不是實際的驗證金鑰或資料加密金鑰。

下列範例會驗證是否已為建立驗證金鑰 `cluster1`：

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

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID: <id_value>
node1                                    NSE-AK    yes
    Key ID: <id_value>

       Vserver: cluster1
   Key Manager: external
          Node: node2

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

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

相關資訊

- "儲存加密磁碟顯示"

在ONTAP 更新版本的版本中建立驗證金鑰

您可以使用 `security key-manager create-key` 命令可建立節點的驗證金鑰、並將其儲存在設定的 KMIP 伺服器上。

關於這項工作

如果您的安全性設定要求您使用不同的金鑰進行資料驗證和FIPS 140-2驗證、您應該為每個金鑰建立個別的金鑰。如果情況並非如此、您可以使用與資料存取相同的FIPS法規遵循驗證金鑰。

此功能可為叢集中的所有節點建立驗證金鑰。ONTAP

- 啟用內建金鑰管理時、不支援此命令。
- 如果設定的金鑰管理伺服器已儲存超過128個驗證金鑰、您會收到警告。

  您可以使用金鑰管理伺服器軟體刪除任何未使用的金鑰、然後再次執行命令。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 建立叢集節點的驗證金鑰：

   `security key-manager create-key`

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

   > 輸出中顯示的金鑰ID是用來參照驗證金鑰的識別碼。它不是實際的驗證金鑰或資料加密金鑰。

   下列範例會建立的驗證金鑰 `cluster1`：

   ```
   cluster1::> security key-manager create-key
      (security key-manager create-key)
   Verifying requirements...

   Node: cluster1-01
   Creating authentication key...
   Authentication key creation successful.
   Key ID: <id_value>

   Node: cluster1-01
   Key manager restore operation initialized.
   Successfully restored key information.

   Node: cluster1-02
   Key manager restore operation initialized.
   Successfully restored key information.
   ```

2. 確認已建立驗證金鑰：

   `security key-manager query`

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

   下列範例會驗證是否已為建立驗證金鑰 `cluster1`：

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

  (security key-manager query)

          Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-01     NSE-AK    yes
       Key ID: <id_value>


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

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

使用ONTAP外部金鑰管理將資料驗證金鑰指派給 FIPS 磁碟機或 SED

您可以使用 `storage encryption disk modify` 命令將資料驗證金鑰指派給 FIPS 磁碟機或 SED 。叢集節點使用此金鑰來鎖定或解除鎖定磁碟機上的加密資料。

關於這項工作

自我加密磁碟機只有在驗證金鑰ID設定為非預設值時、才會受到保護、不受未獲授權的存取。製造商安全ID（MSID）具有金鑰ID 0x0、是SAS磁碟機的標準預設值。對於NVMe磁碟機、標準預設值為null金鑰、表示為空白金鑰ID。當您將金鑰ID指派給自我加密磁碟機時、系統會將其驗證金鑰ID變更為非預設值。

此程序不會中斷營運。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 指派資料驗證金鑰給FIPS磁碟機或SED：

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

   如"指令參考資料ONTAP"需詳細 `storage encryption disk modify`資訊，請參閱。

您可以使用 `security key-manager query -key-type NSE-AK` 檢視金鑰ID的命令。

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

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

2. 確認已指派驗證金鑰：

   `storage encryption disk show`

   如"指令參考資料ONTAP"需詳細 `storage encryption disk show`資訊，請參閱。

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

相關資訊

- "儲存加密磁碟顯示"
- "儲存加密磁碟顯示狀態"

版權資訊

商標資訊