



設定 NVE ONTAP 9

NetApp
April 24, 2024

目錄

設定 NVE	1
判斷叢集版本是否支援NVE	1
安裝授權	1
設定外部金鑰管理	2
啟用ONTAP 更新版本（NVE）的內建金鑰管理	12
啟用ONTAP 更新版本（NVE）的內建金鑰管理	15
在新增的節點中啟用內建金鑰管理	17

設定 NVE

判斷叢集版本是否支援NVE

安裝授權之前、您應該先判斷叢集版本是否支援NVE。您可以使用 `version` 判斷叢集版本的命令。

關於這項工作

叢集版本是ONTAP 叢集內任何節點上執行的最低版本的功能。

步驟

1. 判斷叢集版本是否支援NVE：

```
version -v
```

如果命令輸出顯示文字「100-DARE」（針對「no Data at REST Encryption」）、或您使用的平台未列於中、則不支援NVE ["支援詳細資料"](#)。

下列命令可決定是否支援 NVE cluster1。

```
cluster1::> version -v
NetApp Release 9.1.0: Tue May 10 19:30:23 UTC 2016 <10no-DARE>
```

的輸出 10no-DARE 表示叢集版本不支援NVE。

安裝授權

VE授權可讓您在叢集中的所有節點上使用此功能。使用 NVE 加密資料之前、必須先取得此授權。隨附於 ["ONTAP One"](#)。

在 ONTAP One 之前、VE 授權已包含在加密套件中。加密套件已不再提供、但仍然有效。雖然目前並不需要、但現有客戶可以選擇 ["升級至 ONTAP One"](#)。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 您必須已從銷售代表處收到 VE 授權金鑰、或已安裝 ONTAP。

步驟

1. ["確認已安裝 VE 授權"](#)。


VE 授權套件名稱為 VE。

2. 如果未安裝授權、["使用系統管理器或 ONTAP CLI 進行安裝"](#)。

設定外部金鑰管理

設定外部金鑰管理總覽

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。



對於更新版本的版本、節點管理生命期必須指派給以節點管理角色設定的連接埠、才能使用外部金鑰管理程式。ONTAP

NetApp Volume Encryption（NVE）支援ONTAP 採用支援更新版本的Onboard Key Manager。NVE從ONTAP 支援外部金鑰管理（KMIP）和內建金鑰管理程式開始、從功能性的9.10.1開始ONTAP、您就可以開始使用 [Azure Key Vault](#)或[Google Cloud Key Manager](#)服務 保護您的NVE金鑰。從ONTAP 功能表9.11.1開始、您可以在叢集中設定多個外部金鑰管理程式。請參閱 [設定叢集式金鑰伺服器](#)。

使用 **System Manager** 管理外部金鑰管理員

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	<ul style="list-style-type: none">• 叢集 * > * 設定 *	捲動至 * 安全性 * 區段。在 * 加密 * 下、選取  。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 * 安全性 * 下的 * 加密 * 區段中、選取  。

- 若要新增主要金鑰伺服器、請選取  **Add**，然後填寫 **IP** 地址或主機名 * 和 ***Port** 字段。
- 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  可選擇要映射至密鑰管理器的已安裝證書。（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  在憑證名稱旁、刪除您不想對應至外部金鑰管理程式的已安裝憑證。
- 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。
- 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

- 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、選取  ，然後選擇 * 編輯外部金鑰管理員 * 。
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  ，然後選擇 * 編輯外部金鑰管理員 * 。

- 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** 。
 - 選取以刪除金鑰伺服器  在包含金鑰伺服器名稱的表格儲存格結尾處。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

- 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、選取選取  ，然後選擇 * 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  ，然後選擇 * 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

- 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
```

在ONTAP 支援外部金鑰管理的過程中、於支援內部金鑰管理功能的版本 (NVE)

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。從功能支援支援的9.6開始ONTAP、您可以選擇設定獨立的外部金鑰管理程式、以保護資料SVM用來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

您最多可將四個KMIP伺服器連線至叢集或SVM。建議至少使用兩部伺服器來進行備援和災難恢復。

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>
```

如需完整的命令語法、請參閱命令的手冊頁。

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。

開始之前

- KMIP SSL用戶端和伺服器憑證必須已安裝。
- 您必須是叢集或SVM管理員、才能執行此工作。
- 如果您想要啟用MetroCluster 外部金鑰管理功能來管理整個環境、MetroCluster 則必須先完整設定好、才能啟用外部金鑰管理。

- 在這個不支援的環境中、您必須在兩個叢集上安裝KMIP SSL憑證MetroCluster。

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
```



- security key-manager external enable 命令會取代 security key-manager setup 命令。如果您在叢集登入提示字元中執行命令、admin_SVM 預設為目前叢集的管理SVM。您必須是叢集管理員、才能設定叢集範圍。您可以執行 security key-manager external modify 命令以變更外部金鑰管理組態。
- 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：

```
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. 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
```



- 如果您在 SVM 登入提示字元下執行命令、SVM 預設為目前的 SVM。您必須是叢集或SVM管理員、才能設定SVM範圍。您可以執行 security key-manager external modify 命令以變更外部金鑰管理組態。
- 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：

```
svm11::> 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` 用於設定其他 SVM 的命令。◦ `security key-manager external add-servers` 命令會取代 `security key-manager add` 命令。如需完整的命令語法、請參閱手冊頁。

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
```



◦ `security key-manager external show-status` 命令會取代 `security key-manager show -status` 命令。如需完整的命令語法、請參閱手冊頁。

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

Node	Vserver	Key Server	Status

node1			
	svml	keyserver.svml.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			
	svml	keyserver.svml.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。

在支援外部金鑰管理**ONTAP**的過程中、請使用支援更新版本的版本

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。
- 在這個不支援的環境中、您必須在兩個叢集上安裝KMIP SSL憑證MetroCluster 。

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。



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

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
```

```
cluster1::> 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
```

```
cluster1::> 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
```

如需完整的命令語法、請參閱手冊頁。

```
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。

使用雲端供應商管理金鑰

從功能性的9.10.1開始ONTAP、您就可以開始使用 "[Azure Key Vault \(AKV\)](#) " 和 "[Google Cloud Platform的金鑰管理服務 \(雲端KMS\)](#) " 保護雲端代管應用程式中的 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。如果叢集網路設定不正確、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`

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`。
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。

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`。
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. 確認 Cloud KMS 已設定正確的參數：

```
security key-manager external gcp show vservers svm_name
```

狀態 `kms_wrapped_key_status` 將會是 "UNKNOWN" 如果尚未建立加密磁碟區、
如果服務連線能力不正常、請透過資料SVM LIF建立與GCP金鑰管理服務的連線。

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"](#)

啟用ONTAP 更新版本（NVE）的內建金鑰管理

您可以使用Onboard Key Manager來保護叢集用來存取加密資料的金鑰。您必須在存取加密磁碟區或自我加密磁碟的每個叢集上啟用 Onboard Key Manager。

關於這項工作

您必須執行 `security key-manager onboard sync` 每次將節點新增至叢集時的命令。

如果您有 MetroCluster 組態、則必須執行 `security key-manager onboard enable` 命令先在本機叢集上執行、然後執行 `security key-manager onboard sync` 在遠端叢集上使用相同密碼的命令。當您執行時 `security key-manager onboard enable` 本機叢集的命令、然後在遠端叢集上進行同步處理、您不需要執行 `enable` 從遠端叢集再次執行命令。

根據預設、當節點重新開機時、您不需要輸入金鑰管理程式密碼。您可以使用 `cc-mode-enabled=yes` 選項要求使用者在重新開機後輸入複雜密碼。

如果您已設定、則適用於 NVE `cc-mode-enabled=yes`、您使用建立的磁碟區 `volume create` 和 `volume move start` 命令會自動加密。適用於 `volume create`，您不需要指定 `-encrypt true`。適用於 `volume move start`，您不需要指定 `-encrypt-destination true`。

設定ONTAP 靜止資料加密時、若要符合商業分類解決方案（CSfC）的要求、您必須搭配NVE使用NSE、並確保在「一般條件」模式中啟用「內建金鑰管理程式」。請參閱 ["CSfC解決方案簡介"](#) 如需CSfC的詳細資訊、

當「內建金鑰管理程式」在「一般條件」模式中啟用時 (cc-mode-enabled=yes) 、系統行為會以下列方式變更：

- 系統會監控在「一般準則」模式下運作時、連續嘗試失敗的叢集密碼。



如果您在開機時未輸入正確的叢集密碼、則不會掛載加密的磁碟區。若要修正此問題、您必須重新啟動節點、然後輸入正確的叢集密碼。一旦開機、系統最多可連續5次嘗試在24小時內、針對任何需要叢集密碼作為參數的命令、正確輸入叢集密碼。如果達到限制（例如、您連續5次未正確輸入叢集密碼）、則必須等待24小時逾時期間、或是重新啟動節點、才能重設限制。

- 系統映像更新會使用NetApp RSA-3072程式碼簽署憑證搭配SHA-384程式碼簽署摘要、來檢查映像完整性、而非一般的NetApp RSA-2048程式碼簽署憑證和SHA-256程式碼簽署摘要。

升級命令會檢查各種數位簽章、以確認映像內容未遭竄改或毀損。如果驗證成功、映像更新程序會繼續下一步；否則映像更新會失敗。請參閱 cluster image 有關係統更新的信息，請參見手冊頁。



Onboard Key Manager可將金鑰儲存在揮發性記憶體中。當系統重新開機或停止時、揮發性記憶體內容會被清除。在正常操作條件下、系統停止時、揮發性記憶體內容將在30秒內清除。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 在設定Onboard Key Manager之前、您必須先設定MetroCluster 這個靜態環境。

步驟

1. 啟動金鑰管理程式設定：

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



設定 cc-mode-enabled=yes 要求使用者在重新開機後輸入金鑰管理密碼。如果您已設定、則適用於 NVE cc-mode-enabled=yes、您使用建立的磁碟區 volume create 和 volume move start 命令會自動加密。 - cc-mode-enabled MetroCluster 組態不支援此選項。 security key-manager onboard enable 命令會取代 security key-manager setup 命令。

下列範例會在叢集1上啟動金鑰管理程式設定命令、而不要求在每次重新開機後輸入通關密碼：

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

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

2. 在通關密碼提示字元中、輸入32到256個字元之間的通關密碼、或輸入「cc-mode」（64到256個字元之間的通關密碼）。



如果指定的"cc-mode"通關密碼少於64個字元、則在金鑰管理程式設定作業再次顯示通關密碼提示之前、會有五秒鐘的延遲。

3. 在通關密碼確認提示下、重新輸入通關密碼。

4. 確認已建立驗證金鑰：

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



◦ security key-manager key query 命令會取代 security key-manager query key 命令。如需完整的命令語法、請參閱手冊頁。

下列範例會驗證是否已為建立驗證金鑰 cluster1：

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

Key Tag	Key Type	Encryption	Restored
node1	NSE-AK	AES-256	true
Key ID: 00000000000000000200000000000100056178fc6ace6d91472df8a9286daacc00000000 00000000			
node1	NSE-AK	AES-256	true
Key ID: 00000000000000000200000000000100df1689a148fdfbf9c2b198ef974d0baa00000000 00000000			

2 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、必須先完整設定 Onboard Key Manager。在 MetroCluster 環境中、兩個站台都必須設定內建金鑰管理員。

完成後

將通關密碼複製到儲存系統外部的安全位置、以供未來使用。

每當您設定Onboard Key Manager複雜密碼時、也應該手動將資訊備份到儲存系統外部的安全位置、以便在發生災難時使用。請參閱 ["手動備份內建金鑰管理資訊"](#)。

啟用ONTAP 更新版本（NVE）的內建金鑰管理

您可以使用Onboard Key Manager來保護叢集用來存取加密資料的金鑰。您必須在每個存取加密磁碟區或自我加密磁碟的叢集上啟用Onboard Key Manager。

關於這項工作

您必須執行 `security key-manager setup` 每次將節點新增至叢集時的命令。

如果您使用MetroCluster 的是「不確定」組態、請參閱下列準則：

- 在 ONTAP 9.5 中、您必須執行 `security key-manager setup` 在本機叢集和上 `security key-manager setup -sync-metrocluster-config yes` 在遠端叢集上、使用相同的複雜密碼。
- 在 ONTAP 9.5 之前、您必須執行 `security key-manager setup` 在本機叢集上、等待大約 20 秒、然後執行 `security key-manager setup` 在遠端叢集上、使用相同的複雜密碼。

根據預設、當節點重新開機時、您不需要輸入金鑰管理程式密碼。從 ONTAP 9.4 開始、您可以使用 `-enable-cc-mode yes` 選項要求使用者在重新開機後輸入複雜密碼。

如果您已設定、則適用於 NVE `-enable-cc-mode yes`、您使用建立的磁碟區 `volume create` 和 `volume move start` 命令會自動加密。適用於 `volume create`，您不需要指定 `-encrypt true`。適用於 `volume move start`，您不需要指定 `-encrypt-destination true`。



密碼嘗試失敗後、您必須重新啟動節點。

開始之前

- 如果您使用 NSE 或 NVE 搭配外部金鑰管理（KMIP）伺服器、則必須刪除外部金鑰管理程式資料庫。

["從外部金鑰管理移轉至內建金鑰管理"](#)

- 您必須是叢集管理員才能執行此工作。
- 在設定Onboard Key Manager之前、您必須先設定MetroCluster 這個靜態環境。

步驟

1. 啟動金鑰管理程式設定：

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



從 ONTAP 9.4 開始、您可以使用 `-enable-cc-mode yes` 此選項可要求使用者在重新開機後輸入金鑰管理密碼。如果您已設定、則適用於 NVE `-enable-cc-mode yes`、您使用建立的磁碟區 `volume create` 和 `volume move start` 命令會自動加密。

下列範例會在叢集1上開始設定金鑰管理程式、而不要求在每次重新開機後輸入通關密碼：

• • •

-

- 通關密碼確認提示下、重新輸入通關密碼。
證是否已為所有節點設定金鑰：

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

需完整的命令語法、請參閱手冊頁。

```

Key ID                                                    Used By
-----
-----
00000000000000000000200000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
0000000000000000000020000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

Node: node2
Key Store: onboard

Key ID                                                    Used By
-----
-----
00000000000000000000200000000000010059851742AF2703FC91369B7DB47C4722 NSE-AK
0000000000000000000020000000000001008C07CC0AF1EF49E0105300EFC83004BF NSE-AK

```

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 Onboard Key Manager。在 MetroCluster 環境中、兩個站台都必須設定內建金鑰管理員。

完成後

將通關密碼複製到儲存系統外部的安全位置、以供未來使用。

每當您設定 Onboard Key Manager 複雜密碼時、也應該手動將資訊備份到儲存系統外部的安全位置、以便在發生災難時使用。請參閱 ["手動備份內建金鑰管理資訊"](#)。

在新增的節點中啟用內建金鑰管理

您可以使用 Onboard Key Manager 來保護叢集用來存取加密資料的金鑰。您必須在每個存取加密磁碟區或自我加密磁碟的叢集上啟用 Onboard Key Manager。



若為 ONTAP 9.5 或更早版本、您必須執行 `security key-manager setup` 每次將節點新增至叢集時的命令。

對於 ONTAP 9.6 及更新版本、您必須執行 `security key-manager sync` 每次將節點新增至叢集時的命令。

如果將節點新增至已設定內建金鑰管理的叢集、您將會執行此命令來重新整理遺失的金鑰。

如果您使用 MetroCluster 的是「不確定」組態、請參閱下列準則：

- 從 ONTAP 9.6 開始、您必須執行 `security key-manager onboard enable` 先在本機叢集上執行 `security key-manager onboard sync` 在遠端叢集上、使用相同的複雜密碼。
- 在 ONTAP 9.5 中、您必須執行 `security key-manager setup` 在本機叢集和上 `security key-manager setup -sync-metrocluster-config yes` 在遠端叢集上、使用相同的複雜密碼。
- 在 ONTAP 9.5 之前、您必須執行 `security key-manager setup` 在本機叢集上、等待大約 20 秒、然後執行 `security key-manager setup` 在遠端叢集上、使用相同的複雜密碼。

根據預設、當節點重新開機時、您不需要輸入金鑰管理程式密碼。從 ONTAP 9.4 開始、您可以使用 `-enable-cc-mode yes` 選項要求使用者在重新開機後輸入複雜密碼。

如果您已設定、則適用於 NVE `-enable-cc-mode yes`、您使用建立的磁碟區 `volume create` 和 `volume move start` 命令會自動加密。適用於 `volume create`，您不需要指定 `-encrypt true`。適用於 `volume move start`，您不需要指定 `-encrypt-destination true`。



密碼嘗試失敗後、您必須重新啟動節點。

版權資訊

Copyright © 2024 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 <http://www.netapp.com/TM> 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。