設定NetApp Volume Encryption

ONTAP 9

NetApp
July 11, 2025

目錄

設定NetApp Volume Encryption

設定NetApp Volume Encryption總覽

NetApp Volume Encryption（NVE）是一項軟體技術、可一次加密閒置一個磁碟區的資料。只有儲存系統才能存取的加密金鑰、可確保在基礎裝置重新調整用途、退回、放錯位置或遭竊時、無法讀取Volume資料。

瞭解NVE

使用 NVE 時，中繼資料和資料（包括快照）都會加密。資料的存取權是由唯一的XTS-AES-256金鑰提供、每個磁碟區一個金鑰。外部金鑰管理伺服器或 Onboard Key Manager （ OKM ）可為節點提供金鑰：

- 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。最佳實務做法是在不同的儲存系統上設定外部金鑰管理伺服器與資料。
- 內建金鑰管理程式是一項內建工具、可從與資料相同的儲存系統、為節點提供金鑰。

從支援支援支援的版本起、如果您擁有Volume加密（VE）授權、並使用內建或外部金鑰管理程式、則根據預設會啟用Aggregate和Volume加密。ONTAPVE 授權隨附於"ONTAP One"。設定外部或內建金鑰管理程式時、靜止資料加密的設定方式會改變、以供全新的集合體和全新的磁碟區使用。全新的Aggregate依預設會啟用NetApp Aggregate Encryption（NAE）。非NAE Aggregate一部分的全新磁碟區預設會啟用NetApp Volume Encryption（NVE）。如果資料儲存虛擬機器（SVM）是使用多租戶金鑰管理、以自己的金鑰管理程式進行設定、則為該SVM建立的磁碟區會自動設定NVE。

您可以在新的或現有的磁碟區上啟用加密。NVE支援完整的儲存效率功能、包括重複資料刪除與壓縮。從 ONTAP 9.14.1 開始、您就可以了 在現有 SVM 根磁碟區上啟用 NVE。

> 如果您使用SnapLock 的是功能區、則只能在新的空白SnapLock 版的功能區上啟用加密功能。您無法在現有SnapLock 的流通量上啟用加密功能。

您可以在任何類型的Aggregate（HDD、SSD、混合式、陣列LUN）上使用NVE、搭配任何RAID類型、也可以在ONTAP 任何支援的支援功能中使用、包括ONTAP Select 用作支援的功能、包括用作支援的功能。您也可以使用NVE搭配硬體加密、在自我加密磁碟機上使用「雙重加密」資料。

啟用 NVE 時、核心傾印也會加密。

Aggregate層級加密

通常、每個加密磁碟區都會指派一個唯一的金鑰。刪除磁碟區時、金鑰會隨之刪除。

從ONTAP SURF9.6開始、您可以使用_NetApp Aggregate Encryption（NAE）_將金鑰指派給內含的Aggregate、以便加密磁碟區。刪除加密磁碟區時、會保留該集合體的金鑰。如果刪除整個Aggregate、則會刪除金鑰。

如果您打算執行即時或背景Aggregate層級的重複資料刪除、則必須使用Aggregate層級的加密。NVE不支援Aggregate層級的重複資料刪除。

從支援支援支援的版本起、如果您擁有Volume加密（VE）授權、並使用內建或外部金鑰管理程式、則根據預設會啟用Aggregate和Volume加密。ONTAP

NVE與NAE磁碟區可共存於同一個Aggregate上。根據預設、在Aggregate層級加密下加密的磁碟區為NAE磁碟區。加密磁碟區時、您可以覆寫預設值。

您可以使用 `volume move` 將 NVE Volume 轉換為 NAE Volume 的命令、反之亦然。您可以將NAE磁碟區複寫至NVE磁碟區。

您無法使用 `secure purge` NAE 磁碟區上的命令。

何時使用外部金鑰管理伺服器

雖然使用內建金鑰管理程式的成本較低、而且通常更方便、但如果下列任一項屬實、您應該設定KMIP伺服器：

- 您的加密金鑰管理解決方案必須符合聯邦資訊處理標準（FIPS）140-2或OASIS KMIP標準。
- 您需要一套多叢集解決方案、集中管理加密金鑰。
- 您的企業需要更高的安全性、將驗證金鑰儲存在系統或與資料不同的位置。

外部金鑰管理範圍

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 S9.6開始、您可以使用_SVM範圍_來設定叢集中命名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。
- 從功能升級到功能升級到ONTAP 功能升級、您可以使用 Azure Key Vault與Google Cloud KMS 僅保護資料 SVM 的 NVE 金鑰。從 9.12.0 開始、 AWS 的 KMS 都可以使用這項功能。

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。

中提供已驗證的外部金鑰管理程式清單 "NetApp互通性對照表工具IMT （不含）"。您可以在 IMT 的搜尋功能中輸入「關鍵經理」一詞來找到此清單。

Azure Key Vault 和 AWS KMS 等雲端 KMS 供應商不支援 KMIP 。因此，這些項目並未列在 IMT 上。

支援詳細資料

下表顯示NVE支援詳細資料：

資源或功能	支援詳細資料
平台	需要AES-NI卸載功能。請參閱Hardware Universe 《銷售支援》（HWU）、確認您的平台是否支援NVE和NAE。

加密	從推出更新版本時開始ONTAP 、新建立的Aggregate和Volume會在您新增Volume加密（VE）授權、並設定內建或外部金鑰管理程式時、依預設進行加密。如果您需要建立未加密的Aggregate、請使用下列命令：
	
	`storage aggregate create -encrypt-with-aggr-key false`
	
	如果您需要建立純文字Volume、請使用下列命令：
	
	`volume create -encrypt false`
	
	在下列情況下、預設不會啟用加密：
	
	• 未安裝ve授權。
	• 未設定金鑰管理程式。
	• 平台或軟體不支援加密。
	• 硬體加密已啟用。

ONTAP	所有ONTAP 的部分實作。支援不支援支援支援功能可在支援支援支援功能的版本上找到。ONTAP ONTAP
裝置	HDD、SSD、混合式陣列LUN。
RAID	RAID0、RAID4、RAID-DP、RAID-TEC
磁碟區	資料磁碟區和現有 SVM 根磁碟區。您無法加密 MetroCluster 中繼資料磁碟區上的資料。在早於 9.14.1 的 ONTAP 版本中、您無法使用 NVE 加密 SVM 根 Volume 上的資料。從 ONTAP 9.14.1 開始、 ONTAP 支援 SVM 根磁碟區上的 NVE。
Aggregate層級加密	從推出支援Aggregate層級加密（NAE）的ONTAP NVE開始： • 如果您打算執行即時或背景Aggregate層級的重複資料刪除、則必須使用Aggregate層級的加密。 • 您無法重新輸入Aggregate層級加密Volume的金鑰。 • Aggregate層級加密磁碟區不支援安全清除。 • 除了資料磁碟區之外、NAE也支援加密SVM根磁碟區和MetroCluster 元資料Volume。Nae不支援加密根磁碟區。
SVM範圍	從支援SVM範圍開始ONTAP 、NVE僅支援外部金鑰管理、不支援Onboard Key Manager。支援從支援的功能為從支援的功能之一直到支援的功能。MetroCluster ONTAP
儲存效率	重複資料刪除、壓縮、壓縮、FlexClone。 即使將實體複本從父複本分割出去、複本仍會使用與父複本相同的金鑰。您應該執行 `volume move` 在分割複本上、分割複本之後會有不同的金鑰。

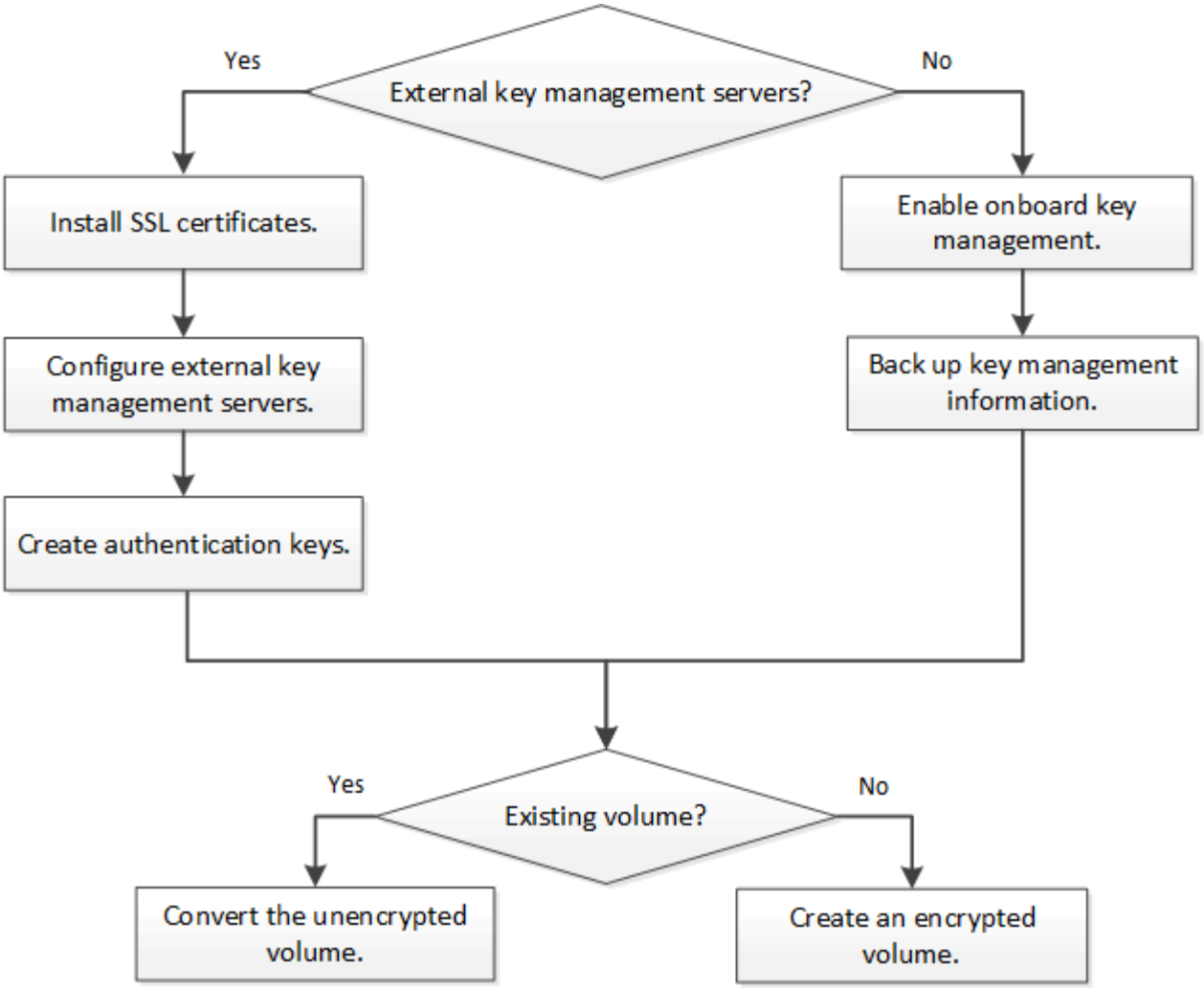
複寫	• 對於 Volume 複寫、來源和目的地磁碟區可以有不同的加密設定。可針對來源設定加密、也可針對目的地設定未設定加密、反之亦然。來源上設定的加密不會複寫到目的地。加密必須在來源和目的地上手動設定。請參閱設定 NVE和使用NVE加密Volume資料。 • 對於SVM複寫、目的地磁碟區會自動加密、除非目的地不包含支援Volume加密的節點、在這種情況下、複寫會成功、但目的地磁碟區不會加密。 • 針對部分組態、每個叢集都會從其設定的金鑰伺服器擷取外部金鑰管理金鑰。MetroCluster組態複寫服務會將OKM金鑰複寫至合作夥伴站台。
法規遵循	合規模式和企業模式均支援SnapLock ，但僅適用於新卷。您無法在現有SnapLock的流通量上啟用加密功能。
資料量FlexGroup	支援FlexGroup磁碟區。目的地Aggregate必須與來源Aggregate的類型相同、無論是Volume層級或Aggregate層級。從功能更新版開始、支援就地重新更新功能、以取代功能。ONTAP FlexGroup
7-Mode轉換	從7-Mode Transition Tool 3.3開始、您可以使用7-Mode Transition Tool CLI、在叢集式系統上執行以複製為基礎的移轉、移轉至啟用NVE的目的地磁碟區。

相關資訊

"常見問題集- NetApp Volume Encryption與NetApp Aggregate Encryption"

NetApp Volume Encryption工作流程

您必須先設定金鑰管理服務、才能啟用磁碟區加密。您可以在新磁碟區或現有磁碟區上啟用加密。



"您必須安裝 VE 授權"並在使用 NVE 加密資料之前、先設定金鑰管理服務。在安裝授權之前"判斷ONTAP 您的版本是否支援NVE"，您應該：

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（針對「無靜態資料加密」），或您使用的平台未列於"支援詳細資料"，則不支援 NVE `1Ono-DARE` 。

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"升級至 ONTAP One"、但現有客戶仍可選擇。

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

瞭解如何使用 **ONTAP** 設定外部金鑰管理

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 ）支援 Onboard Key Manager 。從 ONTAP 9.3 開始， NVE 支援外部金鑰管理（ KMIP ）和內建金鑰管理器。從 ONTAP 9.10.1 開始，您可以使用來Azure Key Vault或Google Cloud Key Manager服務保護 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。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	• 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** 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"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。
- 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 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 ：

```
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。

相關資訊

- "安全金鑰管理程式設定"

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 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。

   > 在這個不支援的環境中、您必須在兩個叢集上執行此命令MetroCluster 。如"指令參考資料ONTAP"需詳細 `security key-manager setup`資訊，請參閱。

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
   ```

   如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

   ```
   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 **ONTAP** 中的雲端供應商來管理金鑰

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. 確認 Cloud KMS 已設定正確的參數：
   `security key-manager external gcp show vserver 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"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"

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。

深入瞭解 `security key-manager onboard enable`及 `security key-manager onboard sync` "指令參考資料ONTAP"。

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。如"指令參考資料ONTAP"需詳細 `cluster image` 資訊，請參閱。

> 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`

   命令會 `security key-manager key query`取代 `security key-manager query key`命令。

   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: <id_value>

node1                                    NSE-AK   AES-256      true

    Key ID: <id_value>

2 entries were displayed.
```

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

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"。

相關資訊

- "安全金鑰管理程式設定"

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：

   ```
   cluster1::> security key-manager setup
   Welcome to the key manager setup wizard, which will lead you through
   the steps to add boot information.

   ...

   Would you like to use onboard key-management? {yes, no} [yes]:
   Enter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   ```

2. 輸入 `yes` 在提示下設定內建金鑰管理。
3. 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。

4. 在通關密碼確認提示下、重新輸入通關密碼。
5. 驗證是否已為所有節點設定金鑰：

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

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

Node: node1
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK

Node: node2
Key Store: onboard
Key ID                                                                   Used By
-------------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK
```

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

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"。

相關資訊

- "安全金鑰管理程式設定"

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。

  深入瞭解 `security key-manager onboard enable`及 `security key-manager onboard sync` "指令參考資料ONTAP"。

- 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。

相關資訊

- "安全金鑰管理程式設定"

使用NVE加密Volume資料

使用NVE總覽加密Volume資料

從使用支援功能9.7開始ONTAP 、如果您擁有VE授權、以及內建或外部金鑰管理、則根據預設會啟用Aggregate和Volume加密。對於支援更新版本的支援、您可以在新磁碟區或現有磁碟區上啟用加密功能。ONTAP您必須先安裝VE授權並啟用金鑰管理、才能啟用Volume加密。NVE符合FIPS-140-2第1級標準。

在 ONTAP 中啟用含 VE 授權的 Aggregate 層級加密

從 ONTAP 9 7 開始"VE 授權"、新建立的集合體和磁碟區會在您擁有和內建或外部金鑰管理時、依預設進行加密。從ONTAP 功能區9.6開始、您可以使用Aggregate層級加密、將金鑰指派給內含的Aggregate、以便加密磁碟區。

關於這項工作

如果您打算執行即時或背景Aggregate層級的重複資料刪除、則必須使用Aggregate層級的加密。NVE不支援Aggregate層級的重複資料刪除。

啟用Aggregate層級加密的Aggregate稱為_NAE Aggregate（適用於NetApp Aggregate Encryption）。NAE Aggregate中的所有磁碟區都必須使用NAE或NVE加密進行加密。使用Aggregate層級加密、您在Aggregate中建立的磁碟區預設會使用NAE加密進行加密。您可以置換預設值、改用NVE加密。

NAE Aggregate不支援純文字磁碟區。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 啟用或停用Aggregate層級加密：

至…	使用此命令…
使用ONTAP NetApp 9.7或更新版本建立NAE Aggregate	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`*
使用ONTAP NetApp 9.6建立NAE Aggregate	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
將非NAE Aggregate轉換為NAE Aggregate	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
將NAE Aggregate轉換為非NAE Aggregate	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key false`

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

下列命令可在上啟用彙總層級加密 `aggr1`：

- 更新版本：ONTAP

```
cluster1::> storage aggregate create -aggregate aggr1
```

- 更新版本：ONTAP

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

2. 確認已啟用Aggregate進行加密：

   `storage aggregate show -fields encrypt-with-aggr-key`

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

   下列命令會驗證是否存在此問題 `aggr1` 已啟用加密：

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate            encrypt-aggr-key
-------------------- ----------------
aggr0_vsim4          false
aggr1                true
2 entries were displayed.
```

完成後

執行 `volume create` 建立加密磁碟區的命令。

如果您使用KMIP伺服器來儲存節點的加密金鑰、ONTAP 則當您加密磁碟區時、會自動將加密金鑰「推送」至伺服器。

在 ONTAP 的新磁碟區上啟用加密

您可以使用 `volume create` 在新磁碟區上啟用加密的命令。

關於這項工作

您可以使用NetApp Volume Encryption（NVE）加密磁碟區、從ONTAP NetApp Aggregate Encryption（NAE）開始加密磁碟區。若要深入瞭解NAE和NVE、請參閱 Volume加密總覽。

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

啟用更新版本的加密程序ONTAP 會因ONTAP 您使用的版本和您的特定組態而有所不同：

- 如果ONTAP 啟用、請從支援的問題9.4開始 `cc-mode` 設定Onboard Key Manager時、您可以使用建立的磁碟區 `volume create` 無論您是否指定、命令都會自動加密 `-encrypt true`。
- 在更新版本的版本中、您必須使用ONTAP `-encrypt true` 與 `volume create` 啟用加密的命令（前提是您未啟用 `cc-mode`）。
- 如果您想要在ONTAP 32位址9.6中建立NAE Volume、則必須在Aggregate層級啟用NAE。請參閱 使用VE授權啟用Aggregate層級加密 以取得此工作的詳細資料。
- 從 ONTAP 9 7 開始"VE 授權"、新建立的磁碟區會在您擁有和內建或外部金鑰管理時、依預設進行加密。根據預設、在NAE Aggregate中建立的新磁碟區將為NAE類型、而非NVE。
  - 如有新增、請參閱ONTAP 更新版本的 `-encrypt true` 至 `volume create` 命令若要在NAE Aggregate中建立磁碟區、該磁碟區將採用NVE加密、而非NAE。NAE Aggregate中的所有磁碟區都必須使用NVE或NAE進行加密。

NAE集合體不支援純文字磁碟區。

步驟

1. 建立新磁碟區、並指定是否在磁碟區上啟用加密。如果新磁碟區位於NAE Aggregate中、則根據預設、該磁碟區將是NAE磁碟區：

若要建立…	使用此命令…
NAE Volume	`volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name`
NVE Volume	`volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt true` + 在不支援NAE的情況下、使用支援的版本為ONTAP `-encrypt true` 指定應使用NVE加密磁碟區。在以NAE集合體建立Volume的版本中ONTAP 、 `-encrypt true` 取代預設的NAE加密類型、改為建立NVE Volume。
純文字Volume	`volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt false`

如"指令參考資料ONTAP"需詳細 `volume create`資訊，請參閱。

2. 確認已啟用磁碟區進行加密：

```
volume show -is-encrypted true
```

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

結果

如果您使用KMIP伺服器來儲存節點的加密金鑰、ONTAP 則當您加密磁碟區時、會自動將加密金鑰「推送」至伺服器。

使用 **ONTAP** 中的 **Volume** 加密轉換啟動命令，在現有磁碟區上啟用加密

從功能介紹9.3開始ONTAP 、您可以使用 `volume encryption conversion start` 命令可「就地」加密現有的磁碟區、而無需將磁碟區移至其他位置。

關於這項工作

一旦開始轉換作業、就必須完成。如果您在作業期間遇到效能問題、可以執行 `volume encryption conversion pause` 暫停作業的命令、以及 `volume encryption conversion resume` 命令以恢復作業。

從 ONTAP 9.14.1 開始、您可以使用 `volume encryption conversion start` 在 SVM 根磁碟區上。如需詳細資訊、請參閱 在 SVM 根磁碟區上設定 NetApp Volume Encryption。

您無法使用 `volume encryption conversion start` 轉換 SnapLock Volume 。

步驟

1. 在現有磁碟區上啟用加密：

   `volume encryption conversion start -vserver svm_name -volume volume_name`

   如"指令參考資料ONTAP"需詳細 `volume encryption conversion start`資訊，請參閱。

   下列命令可在現有磁碟區上啟用加密 `vol1`：

   ```
   cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
   ```

   系統會為磁碟區建立加密金鑰。磁碟區上的資料已加密。

2. 確認轉換作業的狀態：

   `volume encryption conversion show`

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

   下列命令會顯示轉換作業的狀態：

   ```
   cluster1::> volume encryption conversion show

   Vserver   Volume   Start Time           Status
   -------   ------   ------------------   ----------------------------
   vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
   ```

3. 完成轉換作業後、請確認磁碟區已啟用加密：

   `volume show -is-encrypted true`

   如"指令參考資料ONTAP"需詳細 `volume show -is-encrypted true`資訊，請參閱。

   下列命令會顯示上的加密磁碟區 `cluster1`：

   ```
   cluster1::> volume show -is-encrypted true

   Vserver  Volume  Aggregate  State  Type  Size  Available  Used
   -------  ------  ---------  -----  ----  -----  ---------  ----
   vs1      vol1    aggr2      online    RW  200GB    160.0GB  20%
   ```

結果

如果您使用 KMIP 伺服器來儲存節點的加密金鑰、 ONTAP 會在您加密磁碟區時自動將加密金鑰推送至伺服器。

在現有磁碟區上啟用加密

您可以使用 `volume move start` 或 `volume encryption conversion start` 在現有磁碟區上啟用加密的命令。

關於這項工作

您可以使用 `volume encryption conversion start`命令可以「就地」啟用現有磁碟區的加密，而無需將磁碟區移動到其他位置。或者，您可以使用 `volume move start`命令。

使用**Volume Encryption Conversion start**命令、在現有磁碟區上啟用加密

您可以使用 `volume encryption conversion start`命令來啟用現有磁碟區的「就地」加密，而無需將磁碟區移動到其他位置。

在您開始轉換作業之後、必須完成此作業。如果您在作業期間遇到效能問題、可以執行 `volume encryption conversion pause` 暫停作業的命令、以及 `volume encryption conversion resume` 命令以恢復作業。

您無法使用 `volume encryption conversion start` 轉換 SnapLock Volume 。

步驟

1. 在現有磁碟區上啟用加密：

   `volume encryption conversion start -vserver SVM_name -volume volume_name`

   如"指令參考資料ONTAP"需詳細 `volume encryption conversion start`資訊，請參閱。

   下列命令可在現有磁碟區上啟用加密 `vol1`：

   ```
   cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
   ```

   系統會為磁碟區建立加密金鑰。磁碟區上的資料已加密。

2. 確認轉換作業的狀態：

   `volume encryption conversion show`

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

   下列命令會顯示轉換作業的狀態：

   ```
   cluster1::> volume encryption conversion show

   Vserver   Volume   Start Time           Status
   -------   ------   ------------------   ----------------------------
   vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
   ```

3. 轉換作業完成後、請確認磁碟區已啟用加密功能：

   `volume show -is-encrypted true`

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

   下列命令會顯示上的加密磁碟區 `cluster1`：

```
cluster1::> volume show -is-encrypted true

Vserver   Volume   Aggregate   State   Type   Size   Available   Used
-------   ------   ---------   -----   ----   -----   ---------  ----
vs1       vol1     aggr2      online     RW   200GB     160.0GB   20%
```

結果

如果您使用KMIP伺服器來儲存節點的加密金鑰、ONTAP 則當您加密磁碟區時、會自動將加密金鑰「推送」至伺服器。

使用**Volume Move start**命令在現有磁碟區上啟用加密

您可以使用 `volume move start`命令來移動現有的磁碟區來啟用加密。您可以使用相同的Aggregate或不同的Aggregate。

關於這項工作

- 從 ONTAP 9.8 開始、您可以使用 `volume move start` 在 SnapLock 或 FlexGroup 磁碟區上啟用加密。
- 從 ONTAP 9.4 開始、如果您在設定內建金鑰管理程式時啟用「 cc 模式」、就會使用建立磁碟區 `volume move start` 命令會自動加密。您不需要指定 `-encrypt-destination true`。
- 從ONTAP 功能區9.6開始、您可以使用Aggregate層級的加密功能、將金鑰指派給內含的Aggregate、以供移動的磁碟區使用。使用唯一金鑰加密的磁碟區稱為 *NVE Volumes* （意指它使用 NetApp Volume Encryption ）。使用Aggregate層級金鑰加密的Volume稱為_NAE Volume（適用於NetApp Aggregate Encryption ）。NAE集合體不支援純文字磁碟區。
- 從 ONTAP 9.14.1 開始、您可以使用 NVE 加密 SVM 根 Volume 。如需詳細資訊、請參閱 在 SVM 根磁碟區上設定 NetApp Volume Encryption。

開始之前

您必須是叢集管理員才能執行此工作、或是叢集管理員已委派權限的SVM管理員。

"委派權限以執行Volume Move命令"

步驟

1. 移動現有磁碟區、並指定是否在磁碟區上啟用加密：

若要轉換…	使用此命令…

NVE Volume的純文字磁碟區	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination true`
NAE磁碟區的NVE或純文字磁碟區（假設目的地已啟用Aggregate層級加密）	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-with-aggr-key true`
NAE Volume至NVE Volume	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-with-aggr-key false`
NAE磁碟區至純文字磁碟區	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination false -encrypt-with-aggr-key false`
從NVE磁碟區移至純文字磁碟區	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination false`

如"指令參考資料ONTAP"需詳細 `volume move start`資訊，請參閱。

下列命令會轉換名為的純文字磁碟區 `vol1` 至 NVE Volume ：

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

假設目的地上已啟用 Aggregate 層級加密、下列命令會轉換名為的 NVE 或純文字磁碟區 `vol1` 至 NAE Volume ：

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

下列命令會轉換名為的 NAE Volume `vol2` 至 NVE Volume ：

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

下列命令會轉換名為的 NAE Volume `vol2` 至純文字磁碟區：

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

下列命令會轉換名為的 NVE Volume `vol2` 至純文字磁碟區：

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

2. 檢視叢集磁碟區的加密類型：

   `volume show -fields encryption-type none|volume|aggregate`

   ◦ `encryption-type` 欄位可在 ONTAP 9.6 及更新版本中取得。

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

   下列命令會顯示中的磁碟區加密類型 `cluster2`：

```
cluster2::> volume show -fields encryption-type

vserver  volume  encryption-type
-------  ------  ---------------
vs1      vol1    none
vs2      vol2    volume
vs3      vol3    aggregate
```

3. 確認已啟用磁碟區進行加密：

   `volume show -is-encrypted true`

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

   下列命令會顯示上的加密磁碟區 `cluster2`：

```
cluster2::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

結果

如果您使用 KMIP 伺服器來儲存節點的加密金鑰、 ONTAP 會在您加密磁碟區時自動將加密金鑰推送至伺服器。

在 **SVM** 根磁碟區上設定 **NetApp Volume Encryption**

從 ONTAP 9.14.1 開始、您可以在儲存 VM （ SVM ）根磁碟區上啟用 NetApp Volume Encryption （ NVE ）。透過 NVE 、根磁碟區會使用唯一金鑰進行加密、以提高 SVM 的安全性。

關於這項工作

只有在建立 SVM 之後、才能在 SVM 根 Volume 上啟用 NVE 。

開始之前

- SVM 根磁碟區不得位於使用 NetApp Aggregate Encryption （ NAE ）加密的 Aggregate 上。
- 您必須已啟用 Onboard Key Manager 或外部金鑰管理程式的加密。
- 您必須執行 ONTAP 9.14.1 或更新版本。
- 若要移轉包含使用 NVE 加密的根 Volume 的 SVM 、您必須在移轉完成後、將 SVM 根 Volume 轉換為純文字 Volume 、然後重新加密 SVM 根 Volume 。
  - 如果 SVM 移轉的目的地集合體使用 NAE 、則根磁碟區預設會繼承 NAE 。
- 如果 SVM 處於 SVM 災難恢復關係中：
  - 鏡射 SVM 上的加密設定不會複製到目的地。如果您在來源或目的地上啟用 NVE 、則必須在鏡射的 SVM 根 Volume 上個別啟用 NVE 。
  - 如果目的地叢集中的所有集合體都使用 NAE 、則 SVM 根 Volume 將使用 NAE 。

步驟

您可以使用 ONTAP CLI 或系統管理員、在 SVM 根磁碟區上啟用 NVE 。

CLI

您可以在 SVM 根磁碟區就地啟用 NVE 、或是在集合體之間移動磁碟區。

將根磁碟區加密到位

1. 將根磁碟區轉換為加密磁碟區：

   ```
   volume encryption conversion start -vserver svm_name -volume volume
   ```

2. 確認加密成功。。 `volume show -encryption-type volume` 顯示使用 NVE 的所有磁碟區清單。

移動 **SVM** 根 **Volume** 來加密它

1. 啟動磁碟區移動：

   ```
   volume move start -vserver svm_name -volume volume -destination-aggregate
   aggregate -encrypt-with-aggr-key false -encrypt-destination true
   ```

   如"指令參考資料ONTAP"需詳細 `volume move`資訊，請參閱。

2. 確認 `volume move` 操作成功 `volume move show` 命令。。 `volume show -encryption-type volume` 顯示使用 NVE 的所有磁碟區清單。

系統管理員

1. 瀏覽至 儲存空間 > 磁碟區 。
2. 在您要加密的 SVM 根 Volume 名稱旁、選取「 編輯 」。
3. 在「 儲存與最佳化 」標題下、選取「 啟用加密 」。
4. 選擇 儲存 。

啟用節點根磁碟區加密

從功能介紹9.8開始ONTAP 、您可以使用NetApp Volume Encryption來保護節點的根磁碟區。

關於這項工作

此程序適用於節點根磁碟區。不適用於SVM根磁碟區。SVM 根磁碟區可透過集合體層級加密來保護、 從 ONTAP 9.14.1 開始、 NVE。

根磁碟區加密一旦開始、就必須完成。您無法暫停作業。加密完成後、您無法將新金鑰指派給根磁碟區、也無法執行安全清除作業。

開始之前

- 您的系統必須使用HA組態。
- 您的節點根磁碟區必須已建立。
- 您的系統必須具有內建金鑰管理程式、或是使用金鑰管理互通性傳輸協定（KMIP）的外部金鑰管理伺服器。

步驟

1. 加密根磁碟區：

   `volume encryption conversion start -vserver SVM_name -volume root_vol_name`

2. 確認轉換作業的狀態：

   `volume encryption conversion show`

3. 完成轉換作業後、請確認磁碟區已加密：

   `volume show -fields`

   以下顯示加密Volume的輸出範例。

```
::> volume show -vserver xyz  -volume vol0 -fields is-encrypted
vserver    volume is-encrypted
---------- ------ ------------
xyz        vol0   true
```