使用 NVE 或 NAE 加密卷數據

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/zh-tw/ontap/encryption-at-rest/encrypt-volumes-concept.html on February 12, 2026. Always check docs.netapp.com for the latest.

目錄

使用 NVE 或 NAE 加密卷數據 1
了解如何使用 NVE 加密ONTAP磁碟區數據 1
在 ONTAP 中啟用含 VE 授權的 Aggregate 層級加密 1
在 ONTAP 的新磁碟區上啟用加密 2
在現有ONTAP磁碟區上啟用 NAE 或 NVE 4
使用Volume Encryption Conversion start命令、在現有磁碟區上啟用加密 4
使用Volume Move start命令在現有磁碟區上啟用加密 5
在ONTAP SVM 根磁碟區上設定 NVE 8
在ONTAP節點根磁碟區上配置 NVE 9

使用 NVE 或 NAE 加密卷數據

了解如何使用 NVE 加密ONTAP磁碟區數據

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`

詳細了解 `storage aggregate modify`在"指令參考資料ONTAP" 。

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
```

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

2. 確認已啟用Aggregate進行加密：

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

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.
```

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

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。

在現有ONTAP磁碟區上啟用 NAE 或 NVE

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ONTAP SVM 根磁碟區上設定 NVE

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 。

在ONTAP節點根磁碟區上配置 NVE

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
```

版權資訊

Copyright © 2026 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 保留隨時變更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。