



設定NetApp硬體加密

ONTAP 9

NetApp
February 12, 2026

目錄

設定NetApp硬體加密	1
了解ONTAP基於硬體的加密	1
瞭解NetApp硬體型加密	1
支援的自我加密磁碟機類型	1
何時使用外部金鑰管理	1
支援詳細資料	2
硬體型加密工作流程	2
設定外部金鑰管理	3
了解如何設定ONTAP外部金鑰管理	3
在ONTAP叢集上安裝 SSL 憑證	3
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	4
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	6
在 ONTAP 中設定叢集式外部金鑰伺服器	8
建立ONTAP 驗證金鑰、請使用32個以上版本	11
在ONTAP 更新版本的版本中建立驗證金鑰	13
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	15
設定內建金鑰管理	16
啟用更新版本的更新版本、以利執行內建金鑰管理ONTAP	16
啟用更新版本的更新版本ONTAP	18
使用ONTAP板載金鑰管理將資料驗證金鑰指派給 FIPS 磁碟機或 SED	20
將 FIPS 140-2 身份驗證金鑰指派給ONTAP FIPS 驅動器	21
在 ONTAP 中啟用適用於 KMIP 伺服器連線的叢集範圍 FIPS 相容模式	23

設定NetApp硬體加密

了解ONTAP基於硬體的加密

NetApp硬體式加密可在寫入資料時支援完整磁碟加密（FDE）。如果沒有儲存在韌體上的加密金鑰、就無法讀取資料。而加密金鑰則只能由驗證的節點存取。

瞭解NetApp硬體型加密

節點會使用從外部金鑰管理伺服器或Onboard Key Manager擷取的驗證金鑰、將自己驗證到自我加密磁碟機：

- 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、為節點提供驗證金鑰。

您可以使用NetApp Volume Encryption搭配硬體加密、在自我加密磁碟機上「雙重加密」資料。

啟用自我加密磁碟機時、核心傾印也會加密。



如果HA配對使用加密SAS或NVMe磁碟機（SED、NSE、FIPS）、您必須遵循主題中的指示 [將FIPS磁碟機或SED恢復為無保護模式](#) 在初始化系統之前、HA配對內的所有磁碟機（開機選項4或9）。如果未這麼做、可能會在磁碟機重新調整用途時、導致未來的資料遺失。

支援的自我加密磁碟機類型

支援兩種自我加密磁碟機：

- 自我加密FIPS認證SAS或NVMe磁碟機可在FAS 所有的作業系統上支援AFF。這些磁碟機稱為_ FIPS磁碟機_、符合美國聯邦資訊處理標準出版品1402、Level 2的要求。認證的功能除了提供加密保護之外、還能防止磁碟機遭受拒絕服務攻擊。FIPS磁碟機無法與同一個節點或HA配對上的其他類型磁碟機混合使用。
- 從ONTAP 推出支援不通過FIPS測試的自我加密NVMe磁碟機開始、AFF 支援在32、320及更新版本系統上執行。這些磁碟機稱為_ SED__、提供與FIPS磁碟機相同的加密功能、但可以與同一個節點或HA配對上的非加密磁碟機混合使用。
- 所有FIPS驗證的磁碟機都使用已通過FIPS驗證的韌體密碼編譯模組。FIPS磁碟機密碼編譯模組不會使用磁碟機外部產生的任何金鑰（磁碟機的韌體密碼編譯模組會使用輸入磁碟機的驗證密碼來取得金鑰加密金鑰）。



非加密磁碟機是不是SED或FIPS磁碟機的磁碟機。



如果您在具有 Flash Cache 模組的系統上使用 NSE、您也應該啟用 NVE 或 NAE。NSE 不會加密位於 Flash Cache 模組上的資料。

何時使用外部金鑰管理

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、您應該使用外部金鑰管理：

- 貴組織的原則需要使用FIPS 140-2第2級（或更高版本）密碼編譯模組的金鑰管理解決方案。
- 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。

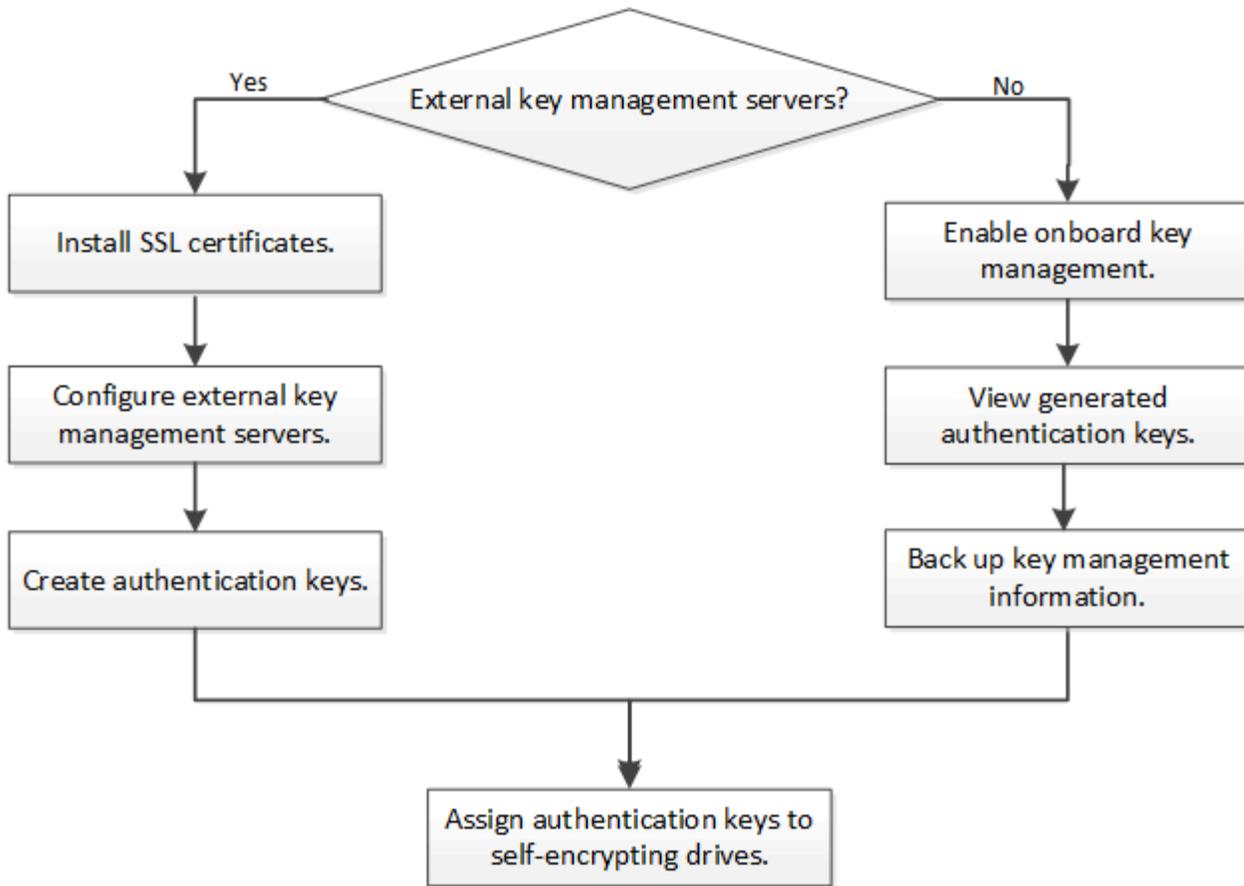
支援詳細資料

下表顯示重要的硬體加密支援詳細資料。如需支援的KMIP伺服器、儲存系統和磁碟櫃的最新資訊、請參閱互通性對照表。

資源或功能	支援詳細資料
非同質磁碟集	<ul style="list-style-type: none"> • FIPS磁碟機無法與同一個節點或HA配對上的其他類型磁碟機混合使用。符合的HA配對可與同一叢集中不符合要求的HA配對共存。 • SED可與同一節點或HA配對上的非加密磁碟機混合使用。
磁碟機類型	<ul style="list-style-type: none"> • FIPS磁碟機可以是SAS或NVMe磁碟機。 • SED必須是NVMe磁碟機。
10 Gb網路介面	KMIP金鑰管理組態從ONTAP 支援10 Gb網路介面開始、可與外部金鑰管理伺服器進行通訊。
用於與金鑰管理伺服器通訊的連接埠	從功能介紹9.3開始ONTAP、您可以使用任何儲存控制器連接埠來與金鑰管理伺服器通訊。否則、您應該使用連接埠 e0M 與金鑰管理伺服器通訊。視儲存控制器機型而定、某些網路介面在開機程序期間可能無法用於與金鑰管理伺服器的通訊。
部分（MCC）MetroCluster	<ul style="list-style-type: none"> • NVMe磁碟機支援MCC。 • SAS磁碟機不支援MCC。

硬體型加密工作流程

您必須先設定金鑰管理服務、叢集才能將自己驗證到自我加密磁碟機。您可以使用外部金鑰管理伺服器或內建金鑰管理程式。



相關資訊

- ["NetApp Hardware Universe"](#)
- ["NetApp Volume Encryption與NetApp Aggregate Encryption"](#)

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金鑰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：

```
cluster1::> 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
```

```
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
```

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致密鑰重複。

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](#)"

設定內建金鑰管理

啟用更新版本的更新版本、以利執行內建金鑰管理ONTAP

您可以使用Onboard Key Manager驗證FIPS磁碟機或SED的叢集節點。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、為節點提供驗證金鑰。Onboard Key Manager符合FIPS-140-2第1級標準。

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 onboard enable` 每次將節點新增至叢集時的命令。在 MetroCluster 組態中、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。

詳細了解 `security key-manager onboard enable` 和 `security key-manager onboard sync` 在"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。除了在 MetroCluster 中、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。

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。

如果已啟用NetApp儲存加密 (NSE)、且您在開機時未輸入正確的叢集密碼、則系統將無法驗證其磁碟機並自動重新開機。若要修正此問題、您必須在開機提示字元中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。

升級命令透過檢查各種數位簽名來驗證影像內容是否已更改或損壞。如果驗證有效、映像更新將進入下一步。如果驗證無效、則影像更新失敗。詳細了解 `cluster image` 在"指令參考資料ONTAP"。

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

- 如果您使用NSE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命令：

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



設 `cc-mode-enabled=yes` 為要求使用者在重新開機後輸入金鑰管理密碼。MetroCluster 組態不支援此 `cc-mode-enabled` 選項。命令會 `security key-manager onboard enable` 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：

2. 輸入一個介於 32 到 256 個字元之間的密碼，或對於“cc-mode”，輸入一個介於 64 到 256 個字元之間的密碼。



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. 驗證系統是否建立了身份驗證金鑰：

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



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

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

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。

系統會自動將關鍵管理資訊備份到叢集的複製資料庫（RDB）。您還應該手動備份此資訊以用於災難復原。

相關資訊

- "[叢集影像命令](#)"
- "[安全金鑰管理員外部啟用](#)"
- "[安全金鑰管理員金鑰查詢](#)"
- "[安全金鑰管理員板載啟用](#)"
- "[從外部金鑰管理移轉至內建金鑰管理](#)"

啟用更新版本的更新版本ONTAP

您可以使用Onboard Key Manager驗證FIPS磁碟機或SED的叢集節點。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、為節點提供驗證金鑰。Onboard Key Manager符合FIPS-140-2第1級標準。

您可以使用板載金鑰管理器來保護叢集用於存取加密資料的金鑰。在存取加密磁碟區或自加密磁碟的每個叢集上啟用板載金鑰管理器。

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

- 如果您將 NSE 與外部金鑰管理 (KMIP) 伺服器一起使用，請刪除外部金鑰管理器資料庫。

["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。
- 在配置板載金鑰管理器之前，請先配置 MetroCluster 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 show-key-store
```

詳細了解 `security key-manager show-key-store` 在 "[指令參考資料ONTAP](#)"。

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

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
```

完成後

ONTAP會自動將金鑰管理資訊備份到叢集的複製資料庫 (RDB)。

設定板載金鑰管理器密碼後，請手動將資訊備份到儲存系統外部的安全位置。看"[手動備份內建金鑰管理資訊](#)"。

相關資訊

- "[手動備份內建金鑰管理資訊](#)"
- "[安全金鑰管理程式設定](#)"
- "[安全金鑰管理員顯示金鑰庫](#)"
- "[從外部金鑰管理移轉至內建金鑰管理](#)"

使用ONTAP板載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存取磁碟機上的資料。

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。

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 key 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.
```

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

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](#)"

將 FIPS 140-2 身份驗證金鑰指派給ONTAP FIPS 驅動器

您可以使用 `storage encryption disk modify` 命令 `-fips-key-id` 將 FIPS 140-2 驗證金鑰指派給 FIPS 磁碟機的選項。叢集節點將此金鑰用於資料存取以外的磁碟機作

業、例如防止磁碟機遭受拒絕服務攻擊。

關於這項工作

您的安全設定可能需要使用不同的金鑰來進行資料驗證和FIPS 140-2驗證。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。

此程序不會中斷營運。

開始之前

磁碟機韌體必須支援FIPS 140-2規範。◦ ["NetApp 互通性對照表工具"](#) 包含支援磁碟機韌體版本的相關資訊。

步驟

1. 您必須先確定已指派資料驗證金鑰。您可以使用來完成這項作業 [外部金鑰管理程式](#) 或是 [內建金鑰管理程式](#)。確認已使用命令指派金鑰 `storage encryption disk show` ◦
2. 指派FIPS 140-2驗證金鑰給SED：

```
storage encryption disk modify -disk disk_id -fips-key-id  
fips_authentication_key_id
```

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

```
cluster1::> storage encryption disk modify -disk 2.10.* -fips-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.
```

3. 確認已指派驗證金鑰：

```
storage encryption disk show -fips
```

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 -fips  
Disk      Mode FIPS-Compliance Key ID  
-----  ----  
-----  
2.10.0    full <id_value>  
2.10.1    full <id_value>  
[...]
```

相關資訊

- ["儲存加密磁碟修改"](#)
- ["儲存加密磁碟顯示"](#)

- "儲存加密磁碟顯示狀態"

在 ONTAP 中啟用適用於 KMIP 伺服器連線的叢集範圍 FIPS 相容模式

您可以使用 `security config modify` 命令 `-is-fips-enabled` 選項可啟用全叢集 FIPS 相容模式、以供傳輸中的資料使用。如此會強制叢集在連接 KMIP 伺服器時、以 FIPS 模式使用 OpenSSL。

關於這項工作

當您啟用全叢集 FIPS 相容模式時、叢集將只自動使用 TLS1.2 和 FIPS 驗證的密碼套件。預設會停用全叢集 FIPS 相容模式。

您必須在修改整個叢集的安全性組態之後、手動重新開機叢集節點。

開始之前

- 儲存控制器必須設定為 FIPS 相容模式。
- 所有 KMIP 伺服器都必須支援 TLSv1.2。啟用叢集範圍 FIPS 相容模式時、系統需要 TLSv1.2 才能完成 KMIP 伺服器的連線。

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 驗證是否支援 TLSv1.2：

```
security config show -supported-protocols
```

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

```
cluster1::> security config show
Cluster
Security
Interface FIPS Mode Supported Protocols Supported Ciphers Config
Ready
-----
-----
SSL false TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:
!aNULL:!EXP:
!eNULL
```

3. 啟用全叢集 FIPS 相容模式：

```
security config modify -is-fips-enabled true -interface SSL
```

如"指令參考資料ONTAP"需詳細 `security config modify` 資訊，請參閱。

4. 手動重新啟動叢集節點。
5. 確認已啟用全叢集FIPS相容模式：

```
security config show
```

```
cluster1::> security config show
      Cluster                                     Cluster
Security
Interface FIPS Mode  Supported Protocols  Supported Ciphers  Config
Ready
-----
-----
SSL          true          TLSv1.2, TLSv1.1    ALL:!LOW:
                !aNULL:!EXP:
                !eNULL:!RC4          yes
```

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。