適用於 VMware vSphere 的 ONTAP 工具安全性強化指南

Enterprise applications

NetApp
May 09, 2024

目錄

適用於 **VMware vSphere** 的 **ONTAP** 工具安全性強化指南

適用於 **VMware vSphere** 的 **ONTAP** 工具安全性強化指南

適用於 VMware vSphere 的 ONTAP 工具安全性強化指南提供一套完整的指示、可協助您設定最安全的設定。

這些指南同時適用於應用程式和應用裝置本身的客體作業系統。

驗證 **VMware vSphere** 安裝套件的 **ONTAP** 工具完整性

有兩種方法可供客戶驗證其 ONTAP 工具安裝套件的完整性。

1. 驗證校驗和
2. 驗證簽名

OTV 安裝套件的下載頁面提供校驗和。使用者必須根據下載頁面所提供的 Checksum 來驗證下載套件的總和。

驗證 **ONTAP** 工具 **OVA** 的簽名

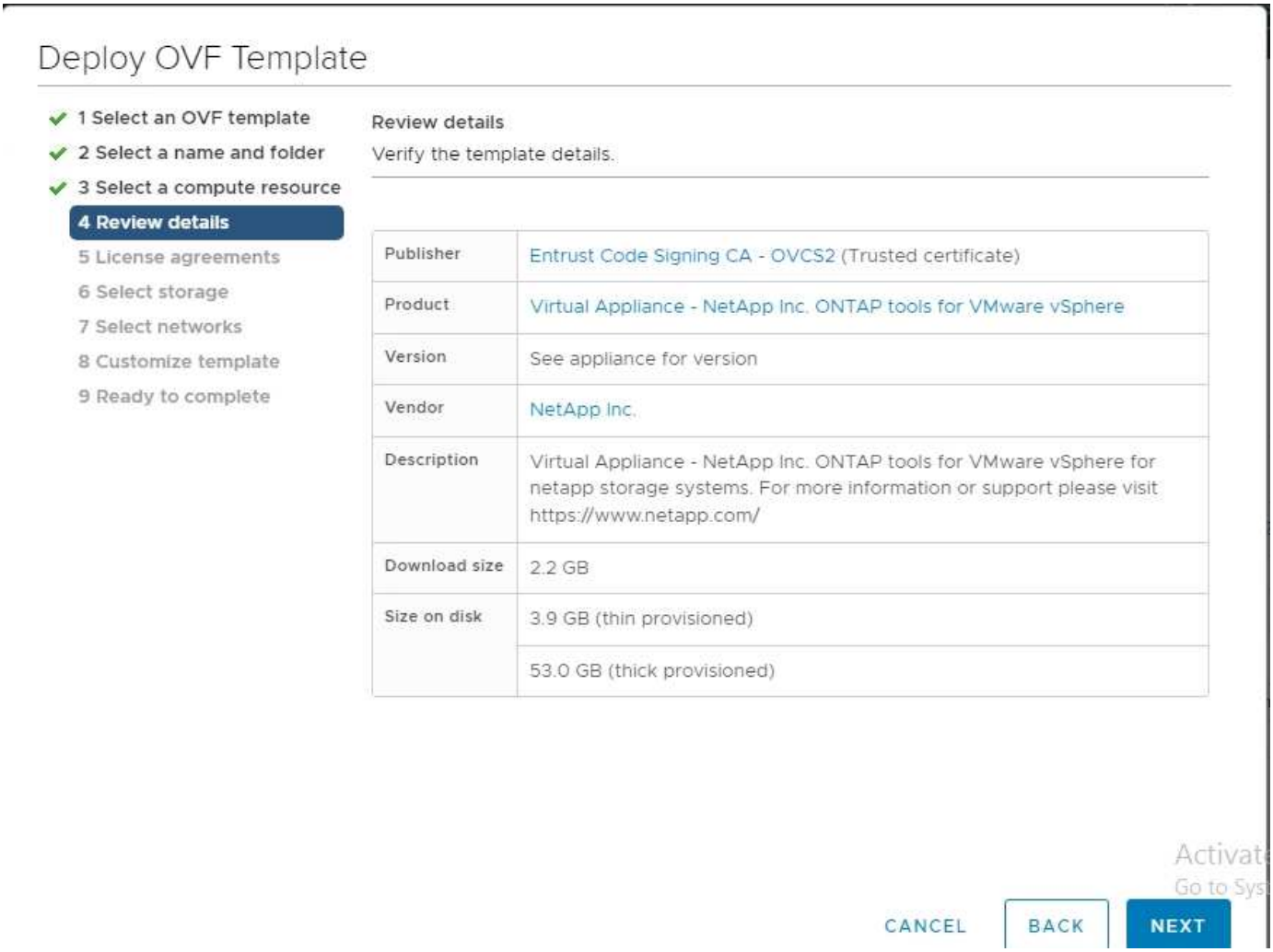
vApp 安裝套件以 tarball 的形式提供。此 tarball 包含虛擬應用裝置的中繼和根憑證、以及 README 檔案和 OVA 套件。README 檔案可引導使用者驗證 vApp OVA 套件的完整性。

客戶也必須在 vCenter 7.0U3E 版及更新版本上傳所提供的根憑證和中介憑證。 對於 7.0.1 與 7.0.U3E 之間的 vCenter 版本、 VMware 不支援驗證憑證的功能。客戶不需要上傳任何 vCenter 6.x 版的憑證

將信任的根憑證上傳至 **vCenter**

1. 使用 VMware vSphere Client 登入 vCenter Server 。
2. 指定管理員 @vspece.pengil 或 vCenter 單一登入管理員群組的其他成員的使用者名稱和密碼。如果您在安裝期間指定不同的網域、請以管理員 @ mydomain.
3. 瀏覽至「憑證管理」使用者介面： a.從主選單中、選取管理。B.按一下 [憑證] 底下的 [憑證管理] 。
4. 如果系統提示您、請輸入 vCenter Server 的認證。
5. 按一下 [信任的根憑證] 底下的 [新增] 。
6. 按一下瀏覽並選取憑證 .pem 檔案（ OTV_OVa_INT_ROOT_CERT_CHERC.pem ）的位置。
7. 按一下「新增」憑證即會新增至儲存區。

請參閱 "將信任的根憑證新增至憑證存放區" 以取得更多資訊。部署 VApp （使用 OVA 檔案）時、可在「 Review details 」（檢閱詳細資料）頁面上驗證 vApp 套件的數位簽章。如果下載的 VApp 套件為正版、「發行者」欄會顯示「信任的憑證」（如下面的螢幕擷取畫面所示）。



驗證工具 **ISO** 和 **ONTAP tar.gz** 的簽名

NetApp 會在產品下載頁面上與客戶共用程式碼簽署憑證、以及適用於 OTV-ISO 和 SRA.tgz 的產品 zip 檔案。

從程式碼簽署憑證中、使用者可以擷取公開金鑰、如下所示：

```
 #> openssl x509 -in <code-sign-cert, pem file> -pubkey -noout > <public-key name>
```

接著應使用公開金鑰來驗證 `ISO` 和 `tgz` 產品 `zip` 的簽名、如下所示：

```
 #> openssl dgst -sha256 -verify <public-key> -signature <signature-file> <binary-name>
```

範例：

```
#> openssl x509 -in OTV_ISO_CERT.pem -pubkey -noout > OTV_ISO.pub
#> openssl dgst -sha256 -verify OTV_ISO.pub -signature netapp-ontap-tools-
for-vmware-vsphere-9.12-upgrade-iso.sig netapp-ontap-tools-for-vmware-
vsphere-9.12-upgrade.iso
Verified OK  => response
```

連接埠與傳輸協定

此處列出的必要連接埠和通訊協定、可讓 VMware vSphere 伺服器的 ONTAP 工具與其他實體（例如託管儲存系統、伺服器和其他元件）之間進行通訊。

OTV 所需的傳入和傳出連接埠

請注意下表列出正確運作 ONTAP 工具所需的輸入和輸出連接埠。請務必確保只開啟表中所述的連接埠、以進行遠端機器的連線、而所有其他連接埠則應封鎖、以進行遠端機器的連線。這將有助於確保系統的安全性。

下表說明開放連接埠的詳細資料。

TCP v4/v6 連接埠 #	方向	* 功能 *
8143.	傳入	用於REST API的HTTPS連線
8043.	傳入	HTTPS連線
9060	傳入	HTTPS 連線 用於透過 HTTPS 連線的 SOAP 此連接埠必須開啟、才能讓用戶端連線至 ONTAP 工具 API 伺服器。
22	傳入	SSH（預設為停用）
9080	傳入	HTTPS連線- VP和SRA -僅從回送進行內部連線
9083.	傳入	HTTPS 連線： VP 與 SRA 用於透過 HTTPS 連線的 SOAP
1162	傳入	VP SNMP設陷封包
8443	傳入	遠端外掛程式
1527.	僅限內部使用	只有在此電腦和本身之間才有 Derby 資料庫連接埠、不接受外部連線—僅限內部連線
8150	僅限內部使用	記錄完整性服務會在連接埠上執行
443..	雙向	用於連線ONTAP 至叢集

控制對 Derby 資料庫的遠端存取

系統管理員可以使用下列命令來存取 derby 資料庫。您可以透過 ONTAP 工具本機 VM 以及遠端伺服器來存取它、步驟如下：

```
java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;
connect 'jdbc:derby://<OTV-
IP>:1527//opt/netapp/vpserver/vvoldb;user=<user>;password=<password>';
```

[.Underline] example:

```
root@UnifiedVSC:~# java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;
ij version 10.15
ij> connect 'jdbc:derby://localhost:1527//opt/netapp/vpserver/vvoldb;user=app;password=[redacted]';
ij> show tables;
TABLE_SCHEM         |TABLE_NAME                   |REMARKS
------------------------------------------------------------------------
SYS                 |SYSALIASES                   |
SYS                 |SYSCHECKS                    |
SYS                 |SYSCOLPERMS                  |
SYS                 |SYSCOLUMNS                   |
SYS                 |SYSCONGLOMERATES             |
SYS                 |SYSCONSTRAINTS               |
SYS                 |SYSDEPENDS                   |
SYS                 |SYSFILES                     |
SYS                 |SYSFOREIGNKEYS               |
SYS                 |SYSKEYS                      |
SYS                 |SYSPERMS                     |
```

適用於 **VMware vSphere** 存取點的 **ONTAP** 工具（使用者）

ONTAP Tools for VMware vSphere 安裝會建立並使用三種類型的使用者：

1. 系統使用者： root 使用者帳戶
2. 應用程式使用者：系統管理員使用者、主要使用者及資料庫使用者帳戶
3. 支援使用者：診斷使用者帳戶

1. 系統使用者

系統（ root ）使用者是由安裝在基礎作業系統（ Debian ）上的 ONTAP 工具所建立。

- 預設的系統使用者「 root 」是由 ONTAP 工具安裝在 Debian 上建立的。其預設值為停用、可透過「 Maint 」主控台在特定的基礎上啟用。

2. 應用程式使用者

應用程式使用者在 ONTAP 工具中會命名為本機使用者。這些是在 ONTAP 工具應用程式中建立的使用者。下表列出應用程式使用者的類型：

使用者	說明
系統管理員使用者	它是在 ONTAP 工具安裝期間建立、使用者在部署 ONTAP 工具時提供認證。使用者可以在「 Maint 」主控台中變更「密碼」。密碼將在 90 天內過期、使用者預期會變更相同的密碼。
維護使用者	它是在 ONTAP 工具安裝期間建立、使用者在部署 ONTAP 工具時提供認證。使用者可以在「 Maint 」主控台中變更「密碼」。這是維護使用者、是為了執行維護主控台作業而建立的。

使用者	說明
資料庫使用者	它是在 ONTAP 工具安裝期間建立、使用者在部署 ONTAP 工具時提供認證。使用者可以在「 Maint 」主控台中變更「密碼」。密碼將在 90 天內過期、使用者預期會變更相同的密碼。

3. 支援使用者（診斷使用者）

在 ONTAP 工具安裝期間、系統會建立支援使用者。此使用者可在伺服器發生任何問題或中斷時、用來存取 ONTAP 工具、並收集記錄。根據預設、此使用者已停用、但可透過「 Maint 」主控台臨時啟用。請務必注意、此使用者將在一段時間後自動停用。

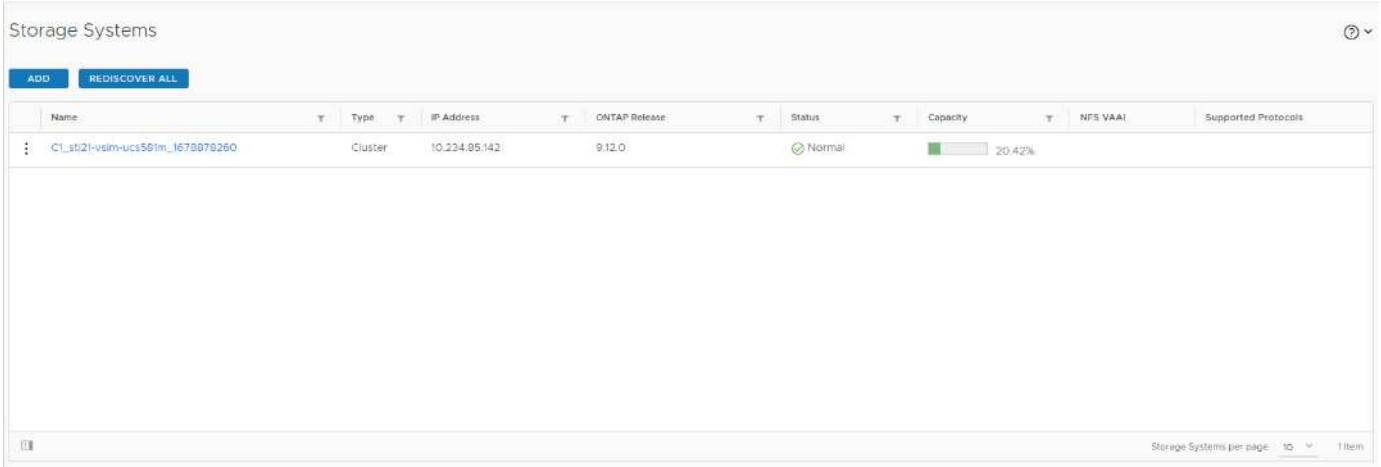
相互 TLS （憑證型驗證）

ONTAP 9.7 版及更新版本支援相互 TLS 通訊。從適用於 VMware 的 ONTAP 工具和 vSphere 9.12 開始、系統會使用相互 TLS 與新增的叢集進行通訊（視 ONTAP 版本而定）。

ONTAP

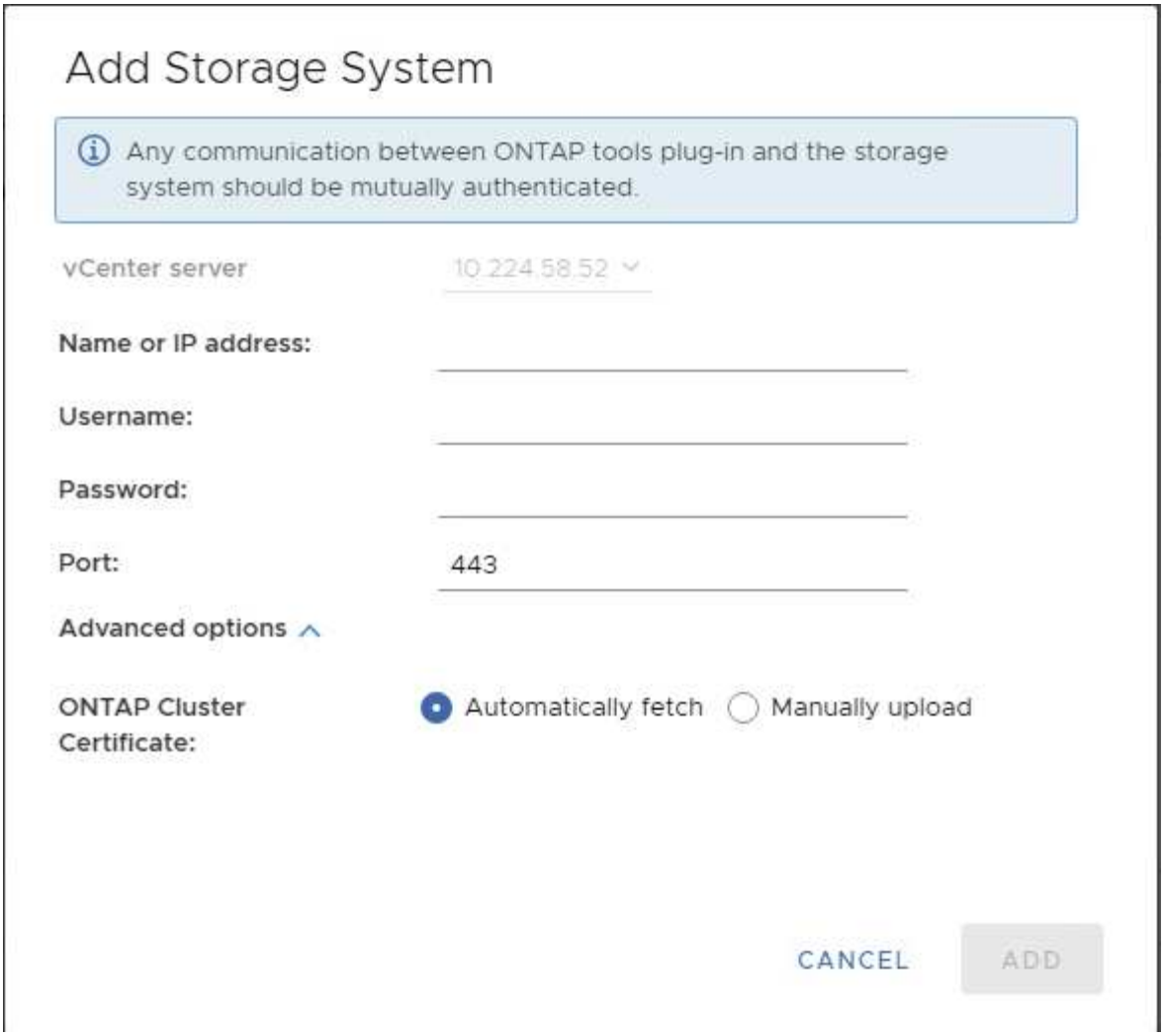
對於所有先前新增的儲存系統：在升級期間、所有新增的儲存系統都會自動受到信任、而且會設定憑證型驗證機制。

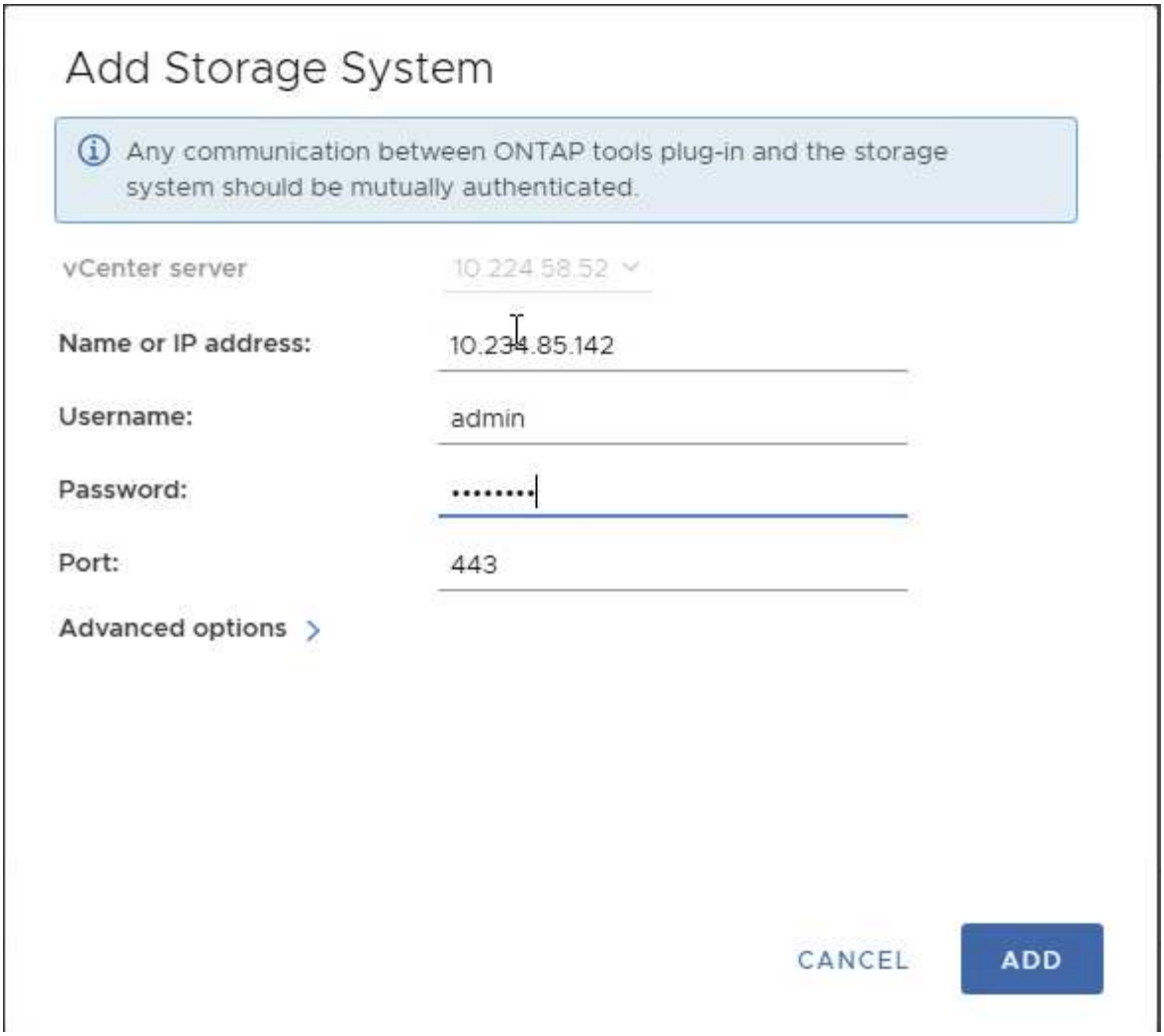
如下面的螢幕擷取畫面所示、叢集設定頁面會顯示為每個叢集設定的相互 TLS （憑證型驗證）狀態。

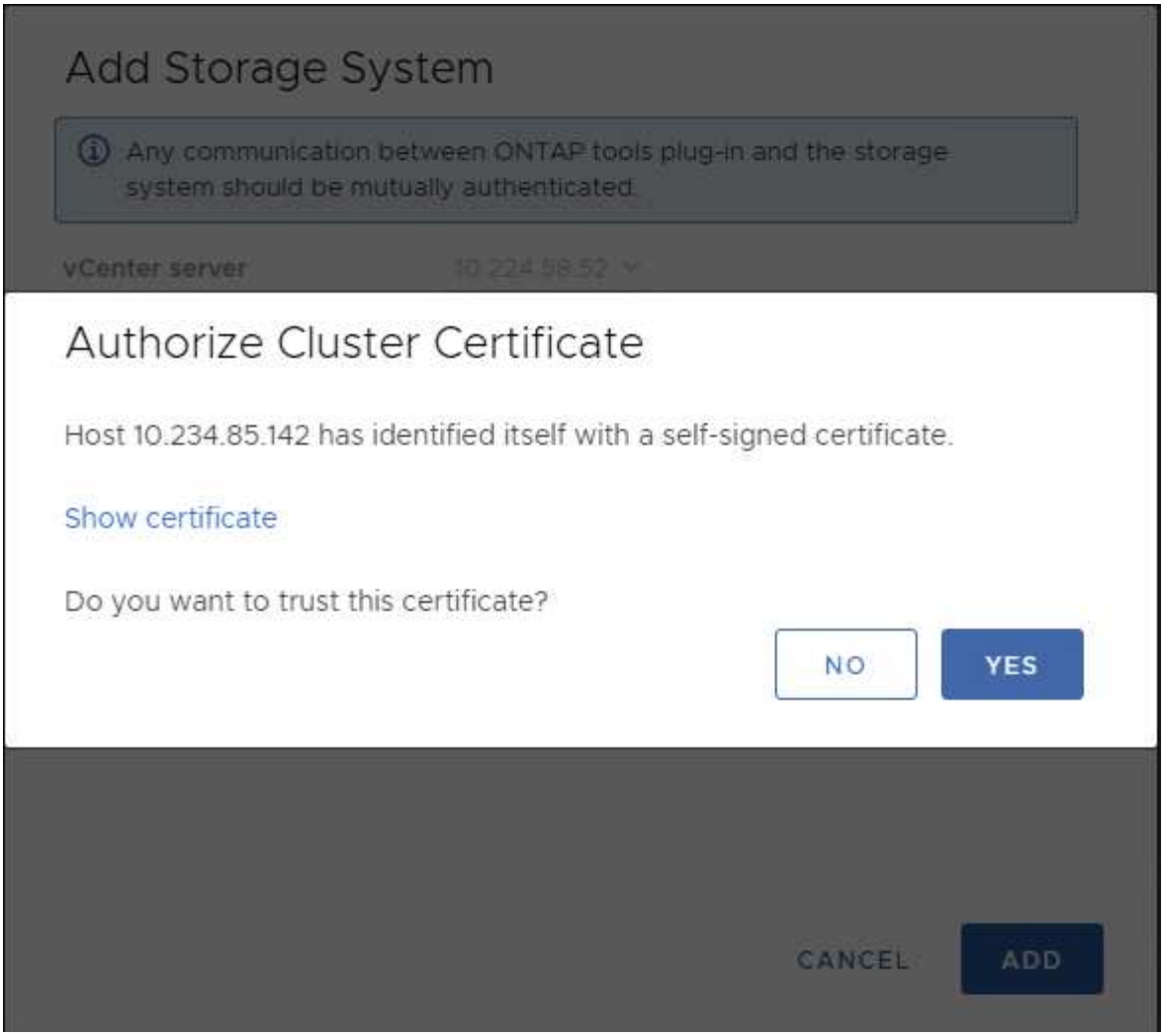


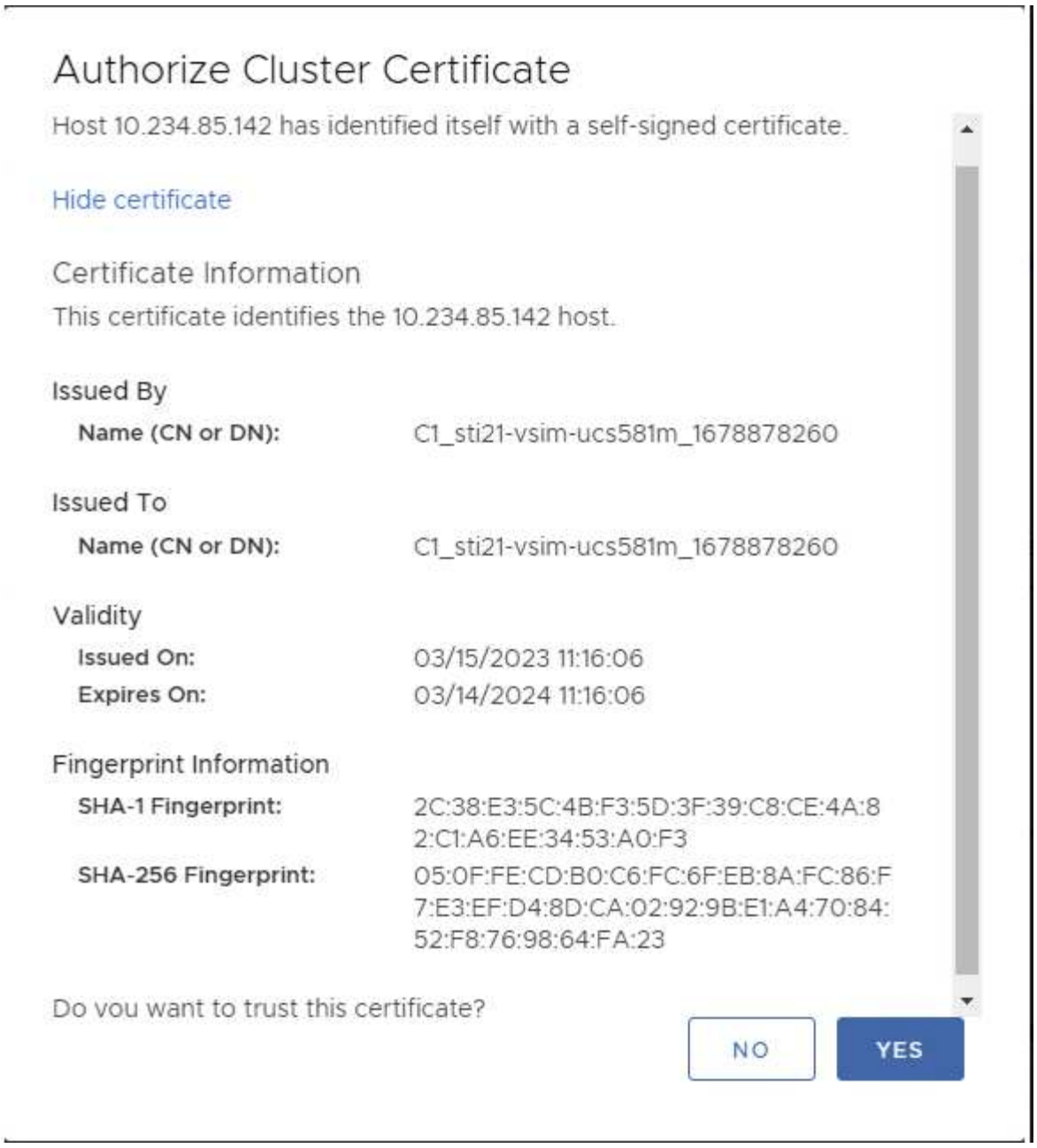
* 叢集新增 *

在叢集新增工作流程期間、如果所新增的叢集支援 MTLS 、則預設會設定 MTLS 。使用者不需要為此進行任何組態。下列螢幕擷取畫面會顯示在叢集新增期間顯示給使用者的畫面。


Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
10.224.58.52
Name or IP address:
Username:
Password:
Port:
443
Advanced options
ONTAP Cluster Certificate:
Automatically fetch
Manually upload
CANCEL
ADD


Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
10.224.58.52
Name or IP address:
10.234.85.142
Username:
admin
Password:
Port:
443
Advanced options
CANCEL
ADD

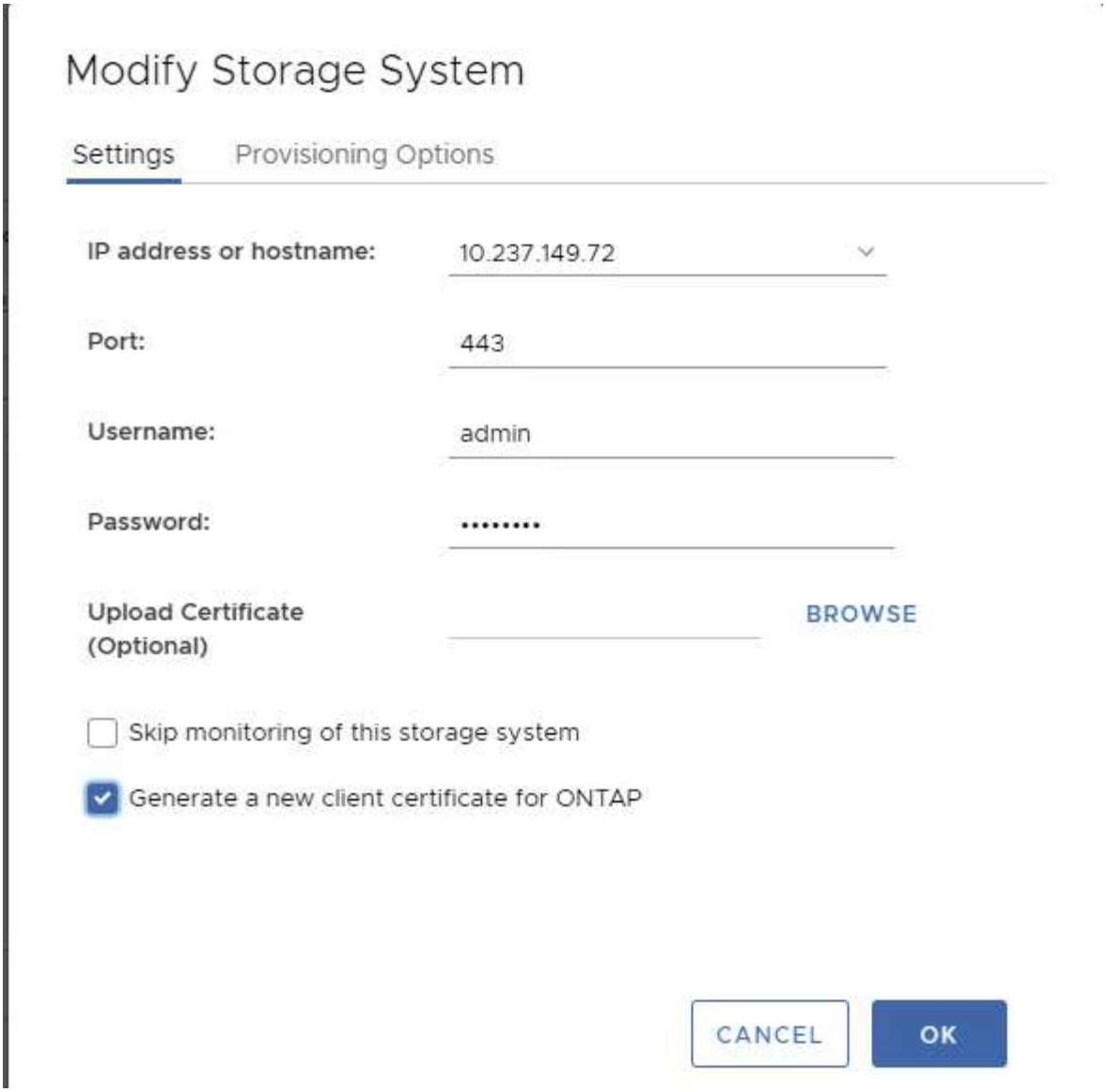

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
Authorize Cluster Certificate
Host 10.234.85.142 has identified itself with a self-signed certificate.
Show certificate
Do you want to trust this certificate?
NO
YES
CANCEL
ADD

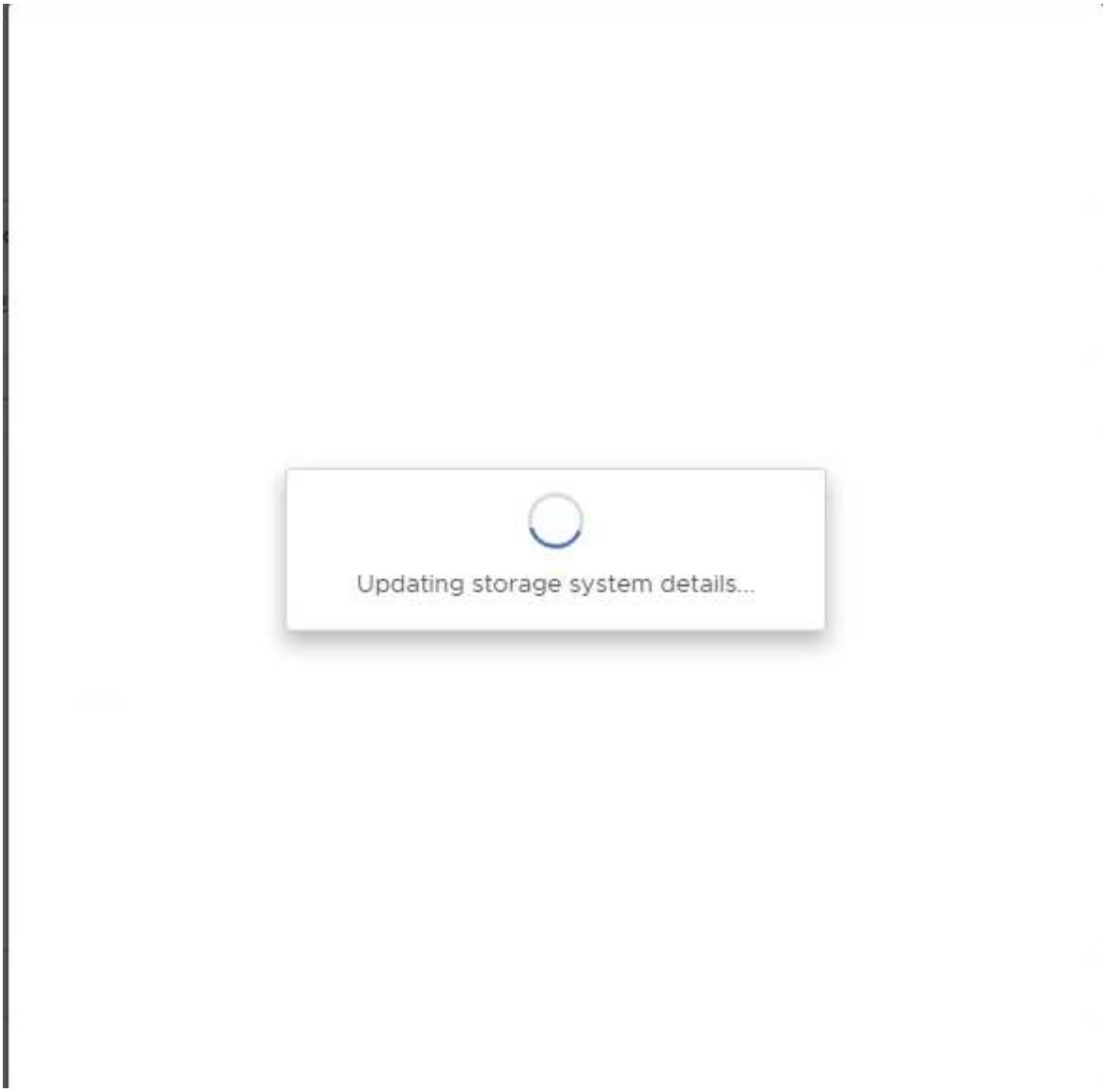


叢集編輯

在叢集編輯作業期間、有兩種情況：

- 如果 ONTAP 憑證過期、則使用者必須取得新憑證並上傳憑證。
- 如果 OTV 憑證過期、則使用者可以勾選核取方塊來重新產生該憑證。
  - 產生 ONTAP 的新用戶端憑證 _


Modify Storage System
Settings
Provisioning Options
IP address or hostname:
10.237.149.72
Port:
443
Username:
admin
Password:
Upload Certificate (Optional)
BROWSE
Skip monitoring of this storage system
Generate a new client certificate for ONTAP
CANCEL
OK



ONTAP 工具 HTTPS 憑證

根據預設、 ONTAP 工具會使用在安裝期間自動建立的自我簽署憑證、以確保 HTTPS 存取安全無虞。ONTAP 工具提供下列功能：

1. 重新產生 HTTPS 憑證

在 ONTAP 工具安裝期間、會安裝 HTTPS CA 憑證、並將憑證儲存在金鑰庫中。使用者可以選擇透過維護主控台重新產生 HTTPS 憑證。

您可以在 *main* 主控台中存取上述選項、方法是瀏覽至「應用程式組態」→「重新產生憑證」。 _

登入橫幅

使用者在登入提示中輸入使用者名稱後、會顯示下列登入橫幅。請注意、 SSH 預設為停用、從 VM 主控台啟用時僅允許一次性登入。

```
WARNING: Unauthorized access to this system is forbidden and will be
prosecuted by law. By accessing this system, you agree that your actions
may be monitored if unauthorized usage is suspected.
```

使用者透過SSH通道完成登入後、會顯示下列文字：

```
Linux UnifiedVSC 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21)
x86_64
```

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

閒置逾時

為了防止未經授權的存取、系統會設定閒置逾時、自動登出在使用授權資源期間處於非使用中狀態的使用者。如此可確保只有授權使用者才能存取資源、並協助維護安全性。

- 根據預設、 vSphere Client 工作階段會在閒置 120 分鐘後關閉、要求使用者再次登入才能繼續使用用戶端。您可以編輯 webclient.properties 檔案來變更逾時值。 您可以設定 vSphere Client 的逾時時間 "設定 vSphere Client 逾時值"
- ONTAP 工具的網路 CLI 工作階段登出時間為 30 分鐘。

每位使用者的並行要求上限（網路安全保護： DOS 攻擊）

依預設、每位使用者的並行要求上限為 48 個。ONTAP 工具中的根使用者可以根據其環境需求變更此值。* 此值不應設為非常高的值、因為它提供了一種機制來防範拒絕服務（ DOS ）攻擊。 *

使用者可以在 ***/opt/NetApp/vscserver/etc/dosfilterParams .json*** 檔案中變更並行工作階段的最大數量及其他支援參數。

我們可以使用下列參數來設定篩選器：

- ***delayMs*** ：在考慮所有請求之前，爲其提供的延遲（以毫秒爲單位）超過了速率限制。給予 -1 即可拒絕要求。
- ***THROLMS_*** ：異步等待信號量的時間。
- ***maxRequestM*** ：允許執行此要求的時間。

- ***ipWhitelist*** ：以逗號分隔的 IP 位址清單、不會受到速率限制。（這可以是 vCenter 、 ESXi 和 SRA IP ）
- ***maxRequestsPerSec*** ：每秒來自連線的最大要求數。
- 在 _dosfilterParams 檔案中的預設值： *

```
{"delayMs":"-1",
"throttleMs":"1800000",
"maxRequestMs":"300000",
"ipWhitelist":"10.224.58.52",
"maxRequestsPerSec":"48"}
```

網路時間傳輸協定（ **NTP** ）組態

有時、網路時間組態不一致、可能會發生安全問題。請務必確保網路中的所有裝置都有正確的時間設定、以避免發生此類問題。

* 虛擬應用裝置 *

您可以從虛擬應用裝置的維護主控台設定 NTP 伺服器。 使用者可以在 _ 系統組態 _ = > _ 新增 NTP 伺服器 _ 選項下新增 NTP 伺服器詳細資料

根據預設、 NTP 的服務為 ntpd 。這是一項舊版服務、在某些情況下、虛擬機器無法順利運作。

* Debian*

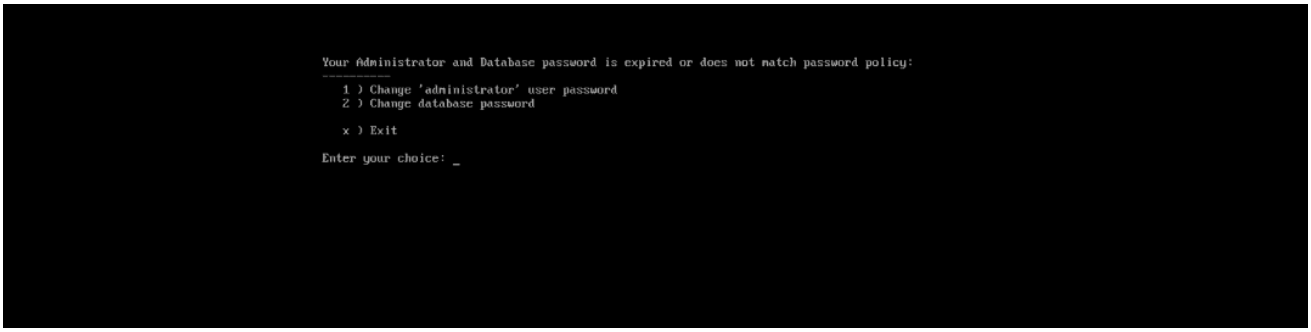
在 Debian 上、使用者可以存取 /etc/ntp.conf 檔案來取得 NTP 伺服器的詳細資料。

密碼原則

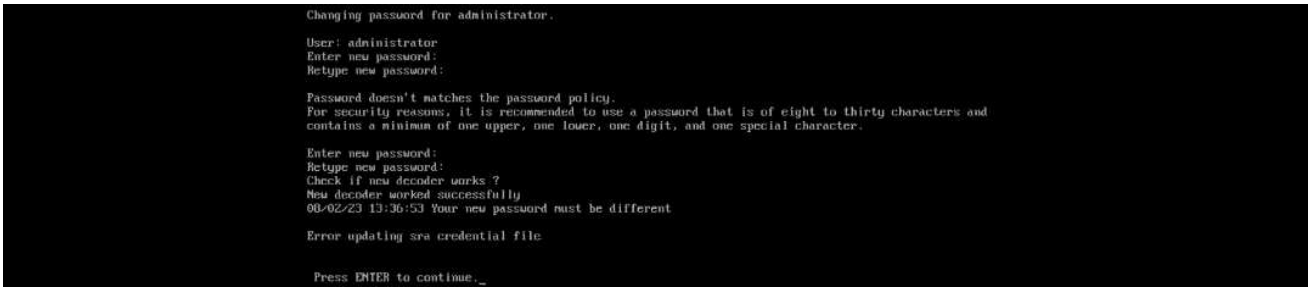
首次部署 ONTAP 工具或升級至 9.12 版或更新版本的使用者、必須同時遵循系統管理員和資料庫使用者的強式密碼原則。在部署過程中、系統會提示新使用者輸入密碼。對於升級至 9.12 版或更新版本的瀏覽欄位使用者、維護主控台將提供遵循強式密碼原則的選項。

- 一旦使用者登入主控台、就會對照複雜的規則集來檢查密碼、如果發現未遵循、則會要求使用者重設相同的密碼。
- 密碼預設有效時間為 90 天、 75 天之後、使用者會開始收到變更密碼的通知。
- 每個週期都需要設定新密碼、系統不會將最後一個密碼當作新密碼。
- 每當使用者登入主控台時、會在載入主功能表之前、先檢查密碼原則、例如下列螢幕擷取畫面：

- 如果發現未遵循密碼原則或 ONTAP 工具 9.11 或更早版本的升級設定、然後使用者會看到下列畫面來重設密碼：



- 如果使用者嘗試設定弱密碼或再次輸入上一個密碼、則使用者將會看到下列錯誤：



版權資訊

商標資訊