Guida alla protezione avanzata per gli strumenti ONTAP per VMware vSphere

Enterprise applications

NetApp
May 09, 2024

Sommario

Guida alla protezione avanzata per gli strumenti ONTAP per VMware vSphere

Guida alla protezione avanzata per gli strumenti ONTAP per VMware vSphere

La guida alla protezione avanzata per gli strumenti ONTAP per VMware vSphere fornisce una serie completa di istruzioni per la configurazione delle impostazioni più sicure.

Queste guide si applicano sia alle applicazioni che al sistema operativo guest dell'appliance stessa.

Verifica dell'integrità dei tool ONTAP per i pacchetti di installazione di VMware vSphere

Sono disponibili due metodi per verificare l'integrità dei pacchetti di installazione degli strumenti ONTAP.

1. Verifica dei checksum
2. Verifica della firma

I checksum sono disponibili nelle pagine di download dei pacchetti di installazione di OTV. Gli utenti devono verificare i checksum dei pacchetti scaricati in base al checksum fornito nella pagina di download.

Verifica della firma degli strumenti ONTAP OVA

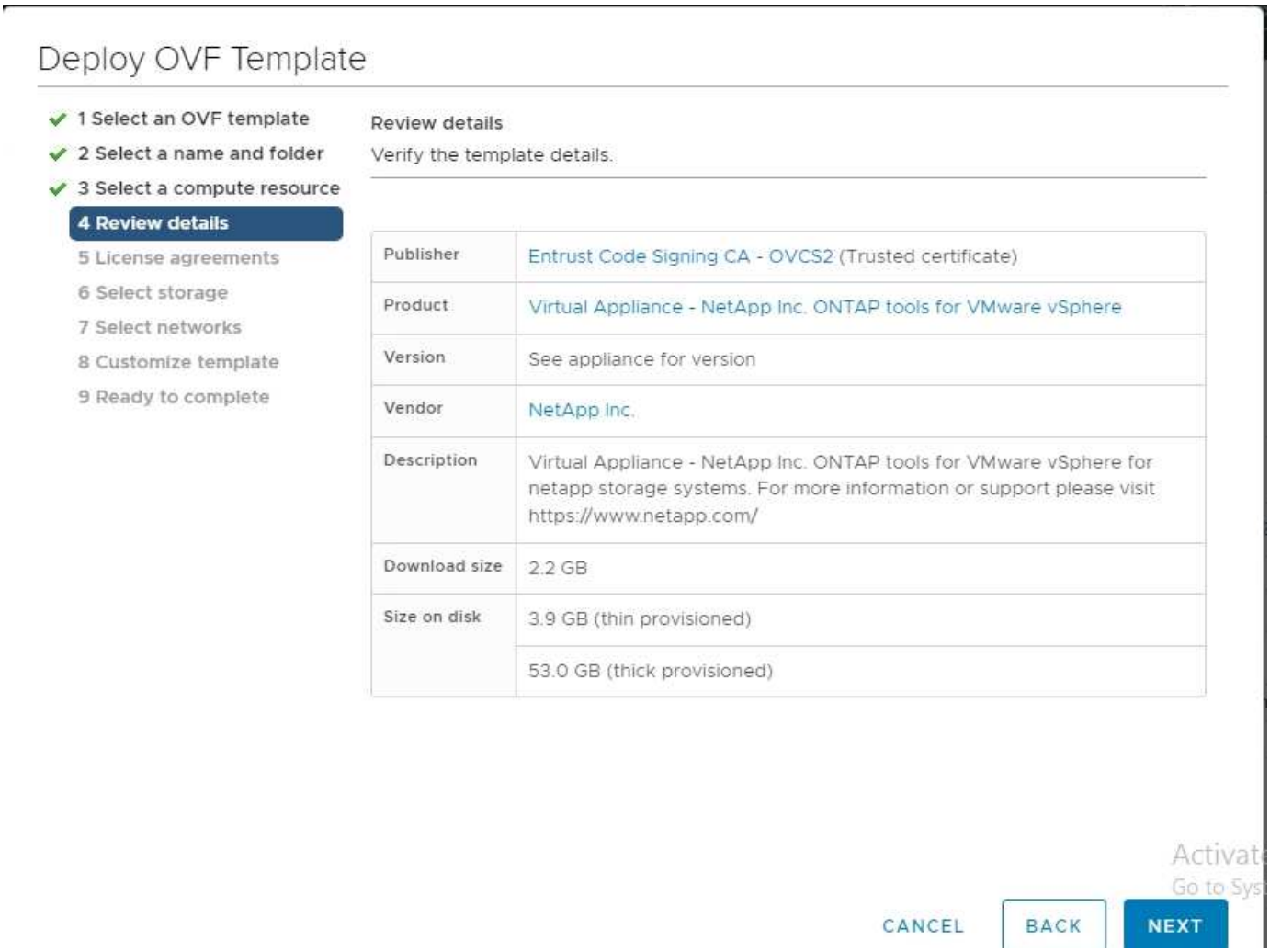
Il pacchetto di installazione vApp viene fornito sotto forma di tarball. Questo tarball contiene certificati intermedi e root per l'appliance virtuale insieme a un file README e un pacchetto OVA. Il file README guida gli utenti su come verificare l'integrità del pacchetto vApp OVA.

I clienti devono inoltre caricare il certificato root e intermedio fornito su vCenter versione 7.0U3E e successive. Per le versioni vCenter comprese tra 7.0.1 e 7,0.U3E, la funzionalità di verifica del certificato non è supportata da VMware. I clienti non devono caricare alcun certificato per le versioni 6.x. di vCenter

Caricamento del certificato root attendibile in vCenter

1. Accedere con il client VMware vSphere a vCenter Server.
2. Specificare il nome utente e la password per adminutator@vsphere.local o un altro membro del gruppo vCenter Single Sign-on Administrators. Se durante l'installazione è stato specificato un dominio diverso, accedere come Administrator@mydomain.
3. Accedere all'interfaccia utente di Gestione certificati: a. Dal menu principale, selezionare Amministrazione. b. Nella sezione certificati, fare clic su Gestione certificati.
4. Se richiesto dal sistema, immettere le credenziali di vCenter Server.
5. In certificati principali attendibili, fare clic su Aggiungi.
6. Fare clic su Sfoglia e selezionare la posizione del file .pem del certificato (OTV_OVA_INTER_ROOT_CERT_CHAIN.pem).
7. Fare clic su Aggiungi. Il certificato viene aggiunto al negozio.

Fare riferimento a. "Aggiungere un certificato radice attendibile all'archivio certificati" per ulteriori informazioni. Durante la distribuzione di una vApp (utilizzando il file OVA), la firma digitale per il pacchetto vApp può essere verificata nella pagina "Dettagli revisione". Se il pacchetto vApp scaricato è originale, nella colonna 'Publisher' viene visualizzato 'Trusted Certificate' (certificato attendibile) (come nella seguente schermata).



Verifica della firma degli attrezzi ONTAP ISO e SRA tar.gz

NetApp condivide il proprio certificato di firma del codice con i clienti nella pagina di download del prodotto, insieme ai file zip del prodotto per OTV-ISO e SRA.tgz.

Dal certificato di firma del codice, gli utenti possono estrarre la chiave pubblica nel modo seguente:

```
 #> openssl x509 -in <code-sign-cert, pem file> -pubkey -noout > <public-
key name>
Quindi, utilizzare la chiave pubblica per verificare la firma per il
prodotto zip iso e tgz come indicato di seguito:
```

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

```
#> 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
```

Porte e protocolli

Di seguito sono elencate le porte e i protocolli necessari per consentire la comunicazione tra gli strumenti ONTAP per il server VMware vSphere e altre entità come i sistemi di storage gestito, i server e altri componenti.

Porte in entrata e in uscita richieste per OTV

Tenere presente la tabella riportata di seguito che elenca le porte in entrata e in uscita necessarie per il corretto funzionamento degli strumenti ONTAP. È importante assicurarsi che solo le porte menzionate nella tabella siano aperte per i collegamenti da macchine remote, mentre tutte le altre porte devono essere bloccate per i collegamenti da macchine remote. In questo modo si garantisce la sicurezza e la sicurezza del sistema.

La seguente tabella descrive i dettagli della porta aperta.

Porta TCP v4/V6 #	Direzione	Funzione
8143	in entrata	Connessioni HTTPS per API REST
8043	in entrata	Connessioni HTTPS
9060	in entrata	Connessioni HTTPS Utilizzato per connessioni SOAP su HTTPS Questa porta deve essere aperta per consentire a un client di connettersi al server API degli strumenti ONTAP.
22	in entrata	SSH (Disattivato per impostazione predefinita)
9080	in entrata	Connessioni HTTPS - VP e SRA - connessioni interne solo da loopback
9083	in entrata	Connessioni HTTPS - VP e SRA Utilizzato per le connessioni SOAP su HTTPS
1162	in entrata	Pacchetti di trap SNMP VP
8443	in entrata	Plugin remoto
1527	solo interno	Porta del database Derby, solo tra questo computer e se stesso, connessioni esterne non accettate — solo connessioni interne

Porta TCP v4/V6 #	Direzione	Funzione
8150	solo interno	Il servizio integrità registro viene eseguito sulla porta
443	bidirezionale	Utilizzato per le connessioni ai cluster ONTAP

Controllo dell'accesso remoto al database Derby

Gli amministratori possono accedere al database derby con i seguenti comandi. È possibile accedervi tramite la VM locale degli strumenti ONTAP e un server remoto con i seguenti passaggi:

```
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>';
```

esempio:

```
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                      |
```

Tool ONTAP per access point VMware vSphere (utenti)

L'installazione di ONTAP Tools per VMware vSphere consente di creare e utilizzare tre tipi di utenti:

1. System User (utente di sistema): L'account utente root
2. Utente dell'applicazione: Gli account utente amministratore, utente principale e utente di database
3. Support user: L'account utente diag

1. Utente di sistema

L'utente System(root) viene creato dall'installazione degli strumenti ONTAP sul sistema operativo sottostante (Debian).

- Un utente di sistema predefinito "root" viene creato su Debian tramite l'installazione degli strumenti ONTAP. L'impostazione predefinita è disattivata e può essere attivata ad hoc tramite la console 'Maint'.

2. Utente dell'applicazione

L'utente dell'applicazione viene denominato come utente locale negli strumenti di ONTAP. Si tratta di utenti creati nell'applicazione ONTAP Tools. Nella tabella seguente sono elencati i tipi di utenti dell'applicazione:

Utente	Descrizione
Administrator User (utente amministratore)	Viene creato durante l'installazione degli strumenti di ONTAP e l'utente fornisce le credenziali durante la distribuzione degli strumenti di ONTAP. Gli utenti hanno la possibilità di modificare la 'password' nella console 'Mainta'. La password scadrà tra 90 giorni e gli utenti saranno tenuti a cambiarla.
Utente manutenzione	Viene creato durante l'installazione degli strumenti di ONTAP e l'utente fornisce le credenziali durante la distribuzione degli strumenti di ONTAP. Gli utenti hanno la possibilità di modificare la 'password' nella console 'Mainta'. Si tratta di un utente addetto alla manutenzione che viene creato per eseguire le operazioni della console di manutenzione.
Utente database	Viene creato durante l'installazione degli strumenti di ONTAP e l'utente fornisce le credenziali durante la distribuzione degli strumenti di ONTAP. Gli utenti hanno la possibilità di modificare la 'password' nella console 'Mainta'. La password scadrà tra 90 giorni e gli utenti saranno tenuti a cambiarla.

3. Utente di assistenza (utente diag)

Durante l'installazione di ONTAP Tools, viene creato un utente di supporto. Questo utente può essere utilizzato per accedere agli strumenti ONTAP in caso di problemi o interruzioni del server e per raccogliere i registri. Per impostazione predefinita, questo utente è disattivato, ma può essere attivato su base adhoc tramite la console 'Maint'. È importante notare che l'utente verrà disattivato automaticamente dopo un determinato periodo di tempo.

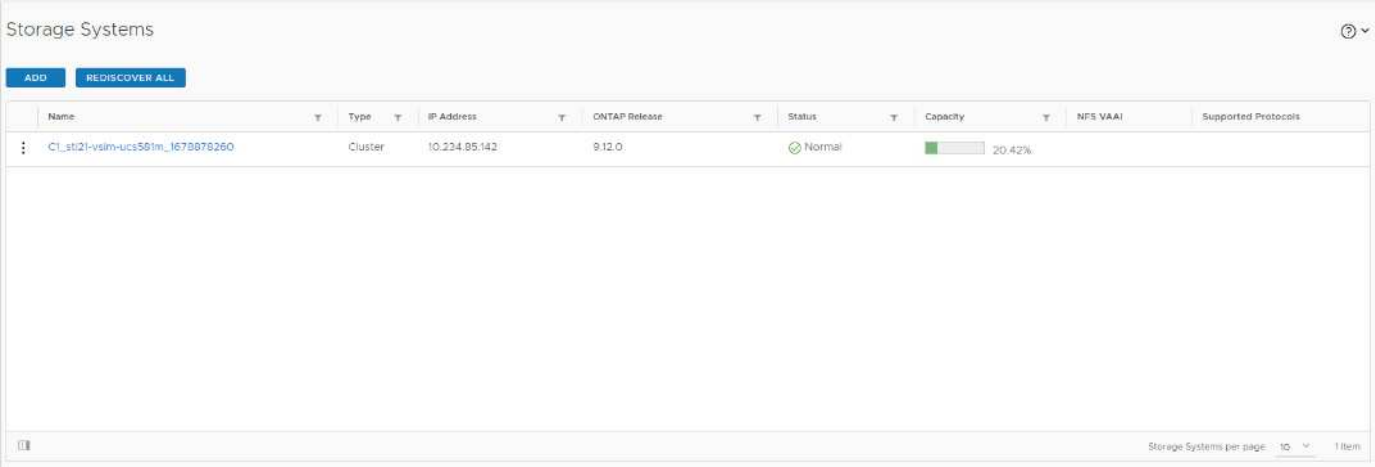
Mutual TLS (autenticazione basata su certificato)

Le versioni ONTAP 9,7 e successive supportano la comunicazione mutua TLS. A partire dai tool ONTAP per VMware e vSphere 9,12, il TLS reciproco viene utilizzato per la comunicazione con i cluster appena aggiunti (in base alla versione di ONTAP).

ONTAP

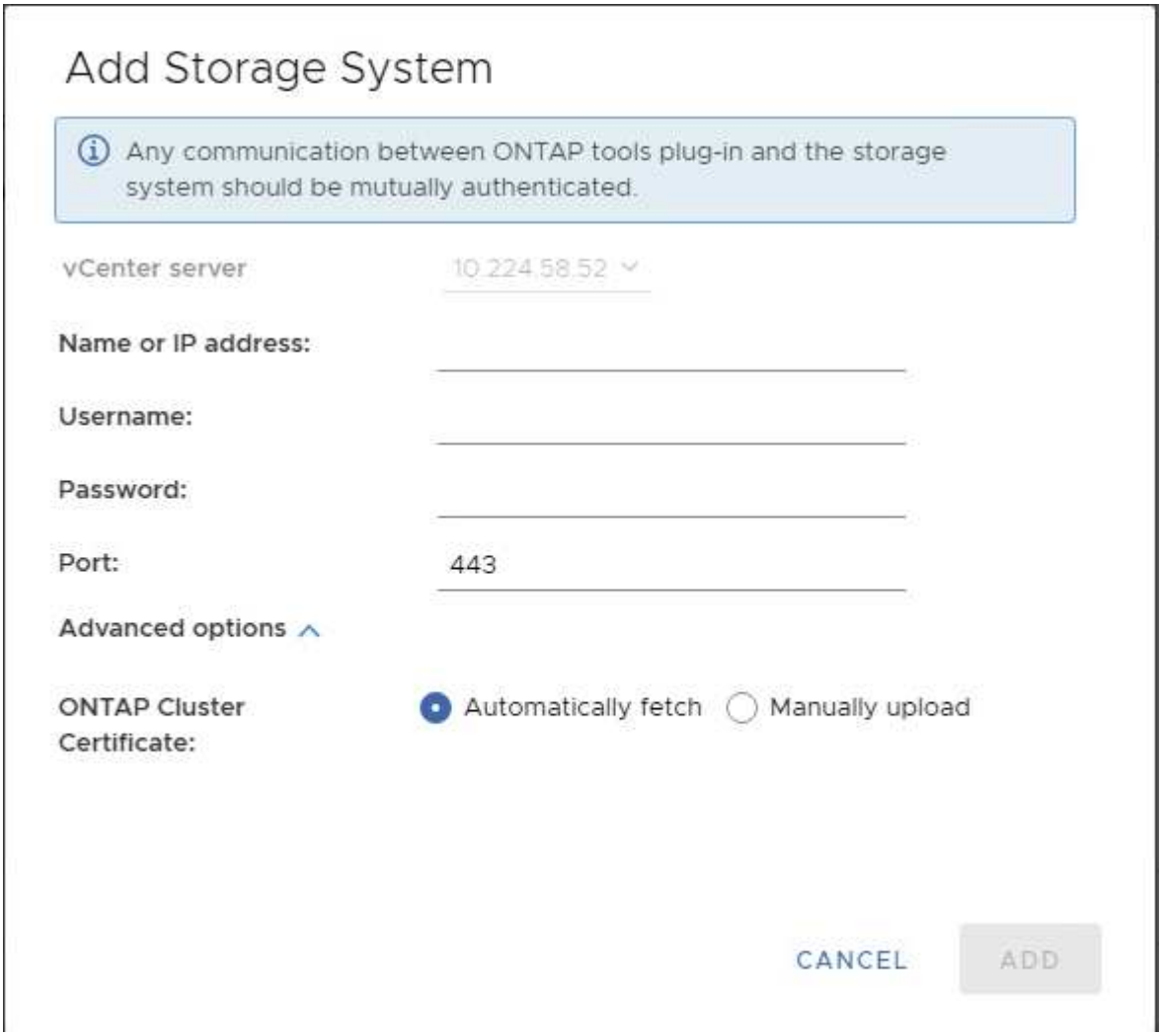
Per tutti i sistemi storage aggiunti in precedenza: Durante un aggiornamento, tutti i sistemi storage aggiunti diventeranno automaticamente attendibili e verranno configurati i meccanismi di autenticazione basati su certificato.

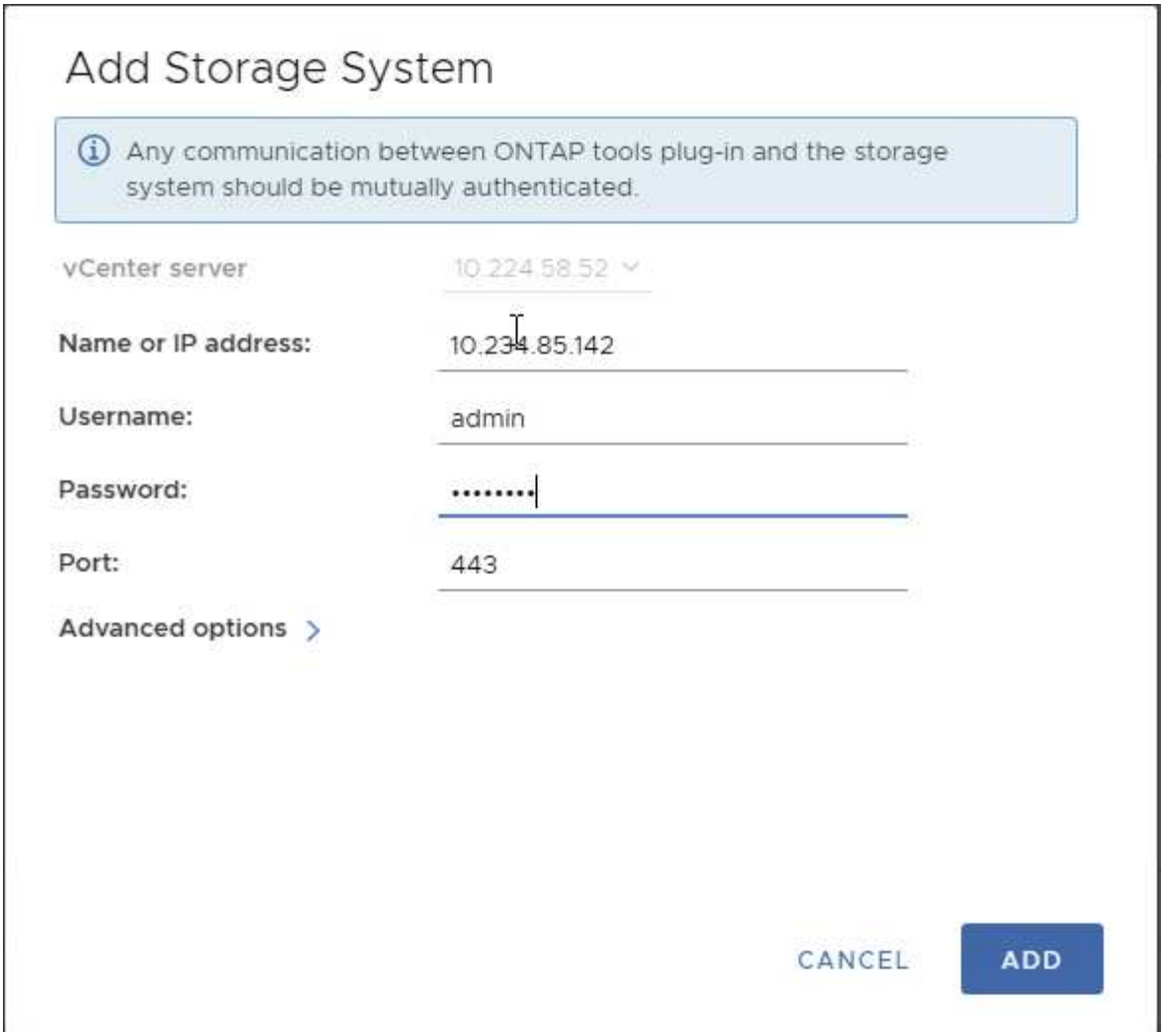
Come nella schermata riportata di seguito, nella pagina di configurazione del cluster viene visualizzato lo stato di Mutual TLS (autenticazione basata su certificato), configurato per ciascun cluster.

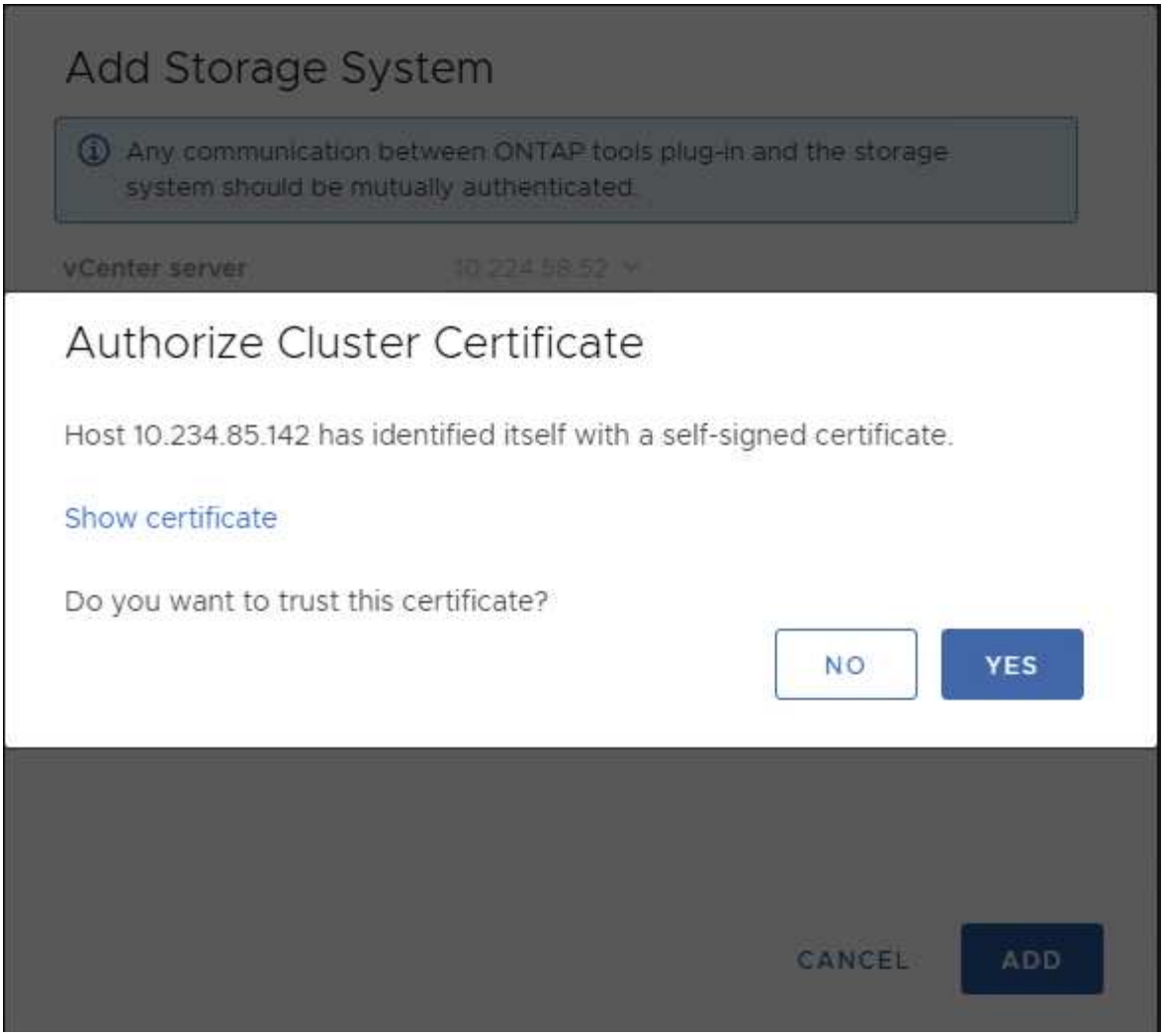


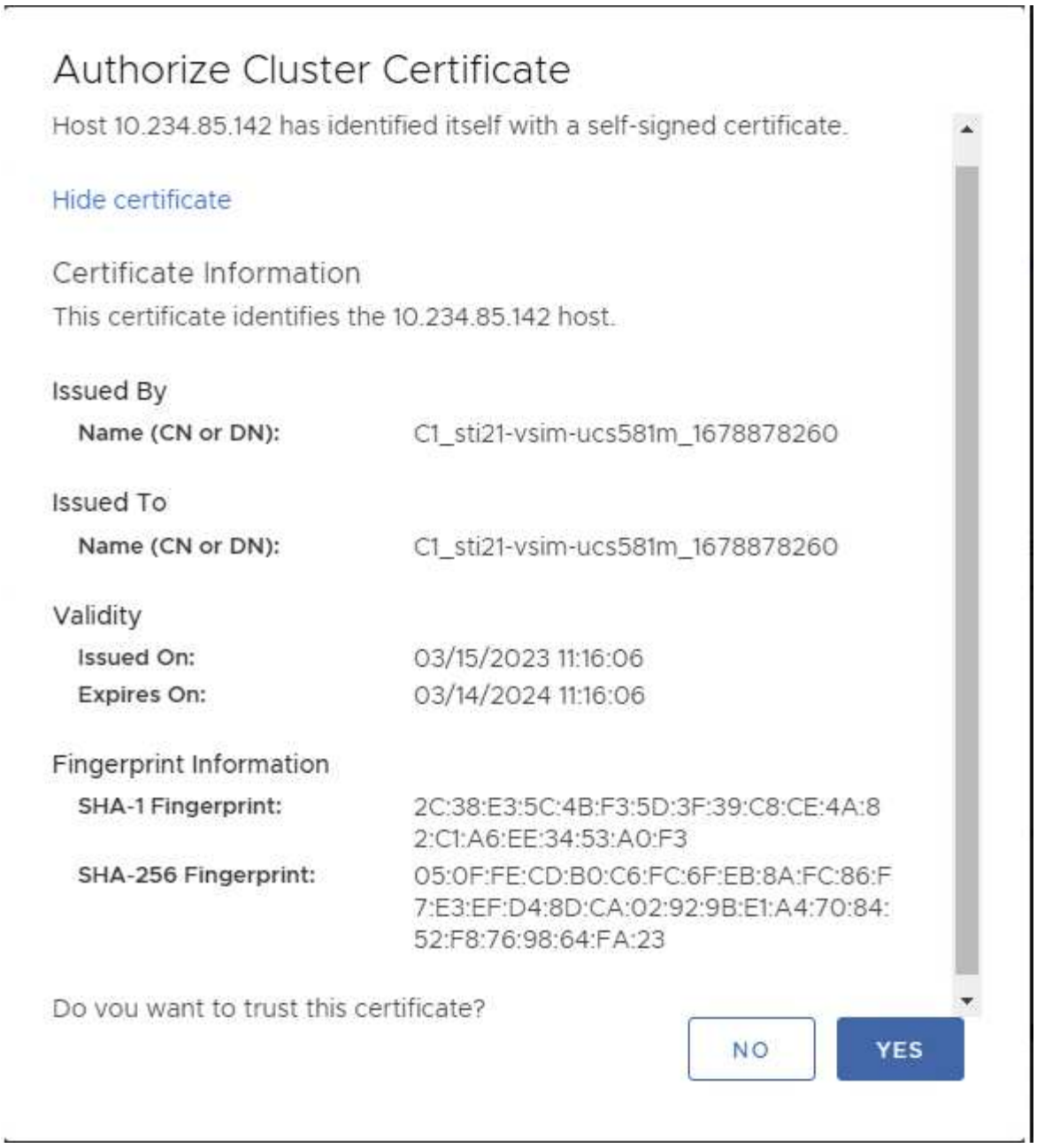
Aggiunta cluster

Durante il flusso di lavoro di aggiunta del cluster, se il cluster che viene aggiunto supporta MTLS, MTLS verrà configurato per impostazione predefinita. L'utente non deve eseguire alcuna configurazione per questo. La schermata riportata di seguito mostra la schermata presentata all'utente durante l'aggiunta del cluster.




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

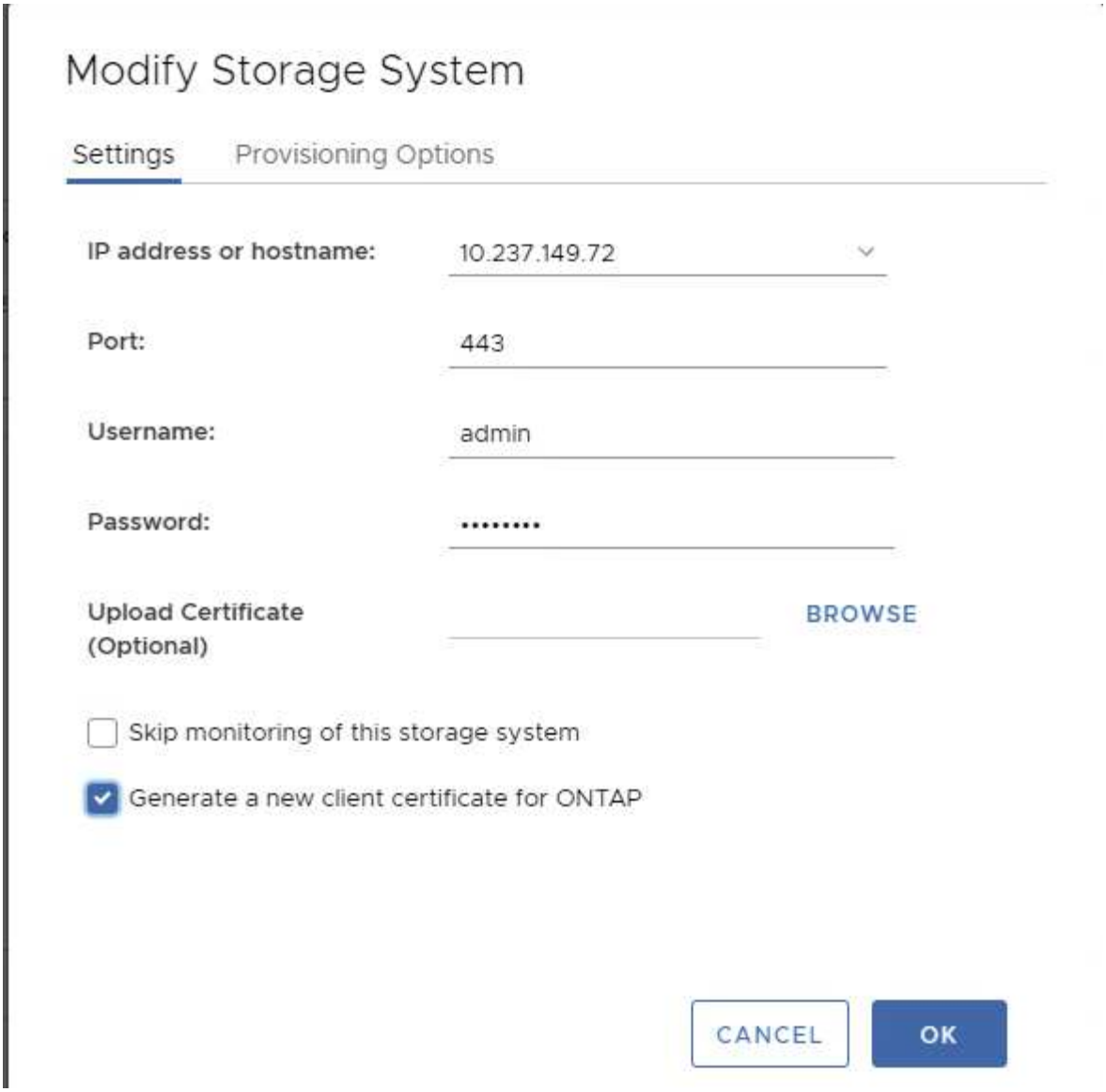

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
Authorize Cluster Certificate
Host 10.234.85.142 has identified itself with a self-signed certificate.
Show certificate
Do you want to trust this certificate?
NO
YES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

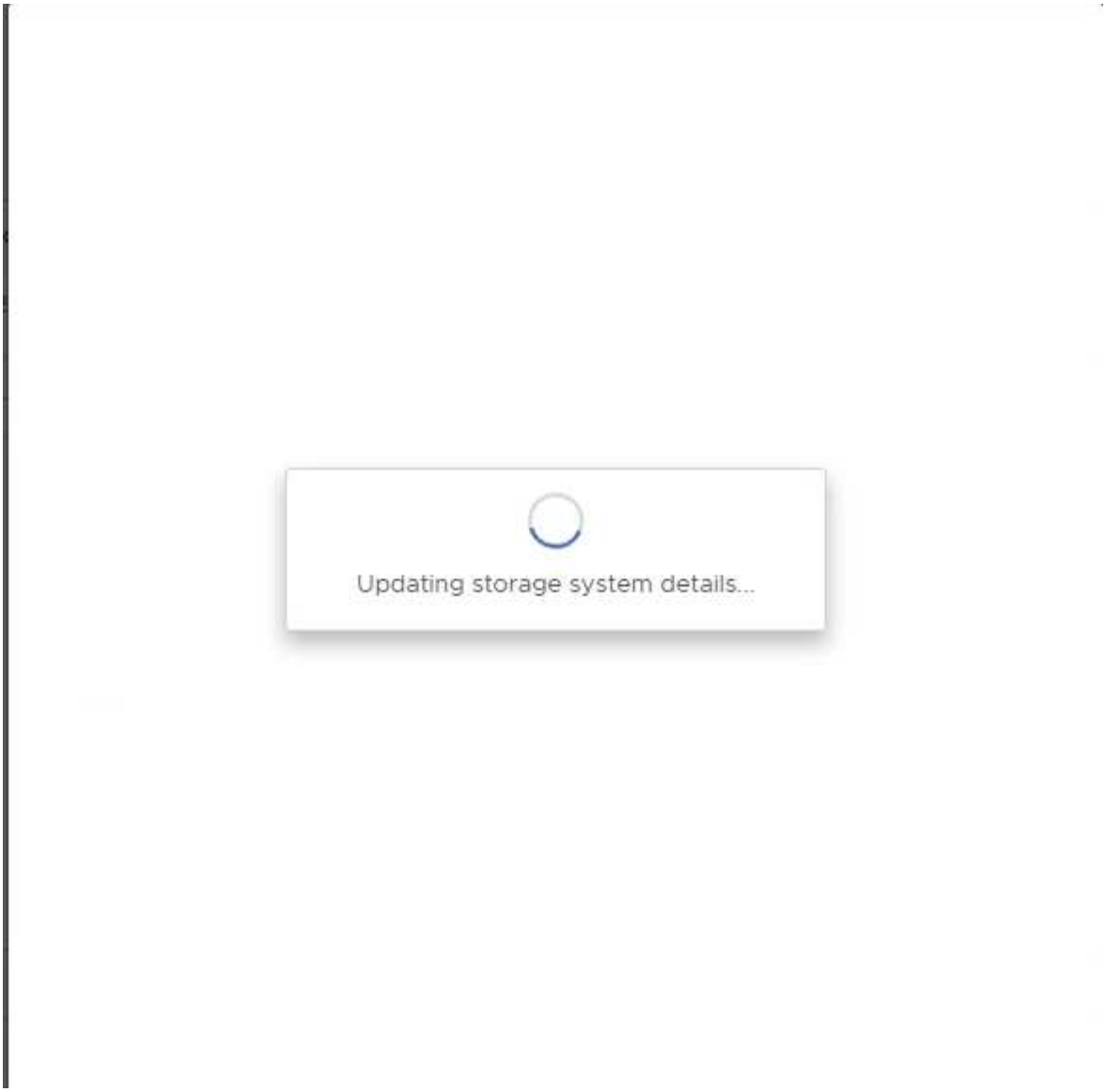


Cluster Edit (Modifica cluster)

Durante l'operazione di modifica del cluster, esistono due scenari:

- Se il certificato ONTAP scade, l'utente dovrà ottenere il nuovo certificato e caricarlo.
- Se il certificato OTV scade, l'utente può rigenerarlo selezionando la casella di controllo.
  - *Genera un nuovo certificato client per ONTAP.*


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



Certificato HTTPS degli strumenti ONTAP

Per impostazione predefinita, gli strumenti ONTAP utilizzano un certificato autofirmato creato automaticamente durante l'installazione per proteggere l'accesso HTTPS all'interfaccia utente Web. Gli strumenti ONTAP offrono le seguenti funzionalità:

1. Rigenerare il certificato HTTPS

Durante l'installazione degli strumenti ONTAP, viene installato un certificato CA HTTPS e il certificato viene memorizzato nell'archivio chiavi. L'utente può rigenerare il certificato HTTPS tramite la console principale.

È possibile accedere alle opzioni sopra riportate nella console *maint* accedendo a *'Configurazione applicazione' → 'rigenerare certificati'.*

Banner di accesso

Il seguente banner di accesso viene visualizzato dopo che l'utente ha immesso un nome utente nel prompt di accesso. Tenere presente che SSH è disattivato per impostazione

predefinita e consente l'accesso una tantum solo se attivato dalla console VM.

```
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.
```

Una volta completato l'accesso tramite il canale SSH, viene visualizzato il seguente testo:

```
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.
```

Timeout di inattività

Per impedire l'accesso non autorizzato, viene impostato un timeout di inattività che disconnette automaticamente gli utenti inattivi per un determinato periodo di tempo durante l'utilizzo di risorse autorizzate. In questo modo, solo gli utenti autorizzati possono accedere alle risorse e mantenere la sicurezza.

- Per impostazione predefinita, le sessioni del client vSphere si chiudono dopo 120 minuti di inattività, richiedendo all'utente di accedere nuovamente per riprendere a utilizzare il client. È possibile modificare il valore di timeout modificando il file webclient.properties. È possibile configurare il timeout del client vSphere "Configurare il valore di timeout del client vSphere"
- Gli strumenti ONTAP hanno un tempo di disconnessione della sessione Web-cli di 30 minuti.

Numero massimo di richieste simultanee per utente (protezione di rete :: Attacco DOS)

Per impostazione predefinita, il numero massimo di richieste simultanee per utente è 48. L'utente root negli strumenti ONTAP può modificare questo valore in base ai requisiti del proprio ambiente. **Questo valore non deve essere impostato su un valore molto alto in quanto fornisce un meccanismo contro gli attacchi DOS (Denial of Service).**

Gli utenti possono modificare il numero massimo di sessioni simultanee e altri parametri supportati nel file ***/opt/netapp/vscserver/etc/dosfilterParams.json***.

Possiamo configurare il filtro con i seguenti parametri :

- ***delayMS***: Il ritardo in millisecondi dato a tutte le richieste oltre il limite di velocità prima che vengano prese in considerazione. Dare -1 per respingere la richiesta.
- ***throttleMS***: Per quanto tempo attendere il semaforo in modalità asincrona.
- ***maxRequestMS***: Per quanto tempo consentire l'esecuzione di questa richiesta.
- ***ipWhitelist***: Un elenco separato da virgole di indirizzi IP che non saranno limitati dalla velocità. (Possono essere indirizzi IP vCenter, ESXi e SRA)
- ***maxRequestsPerSec***: Il numero massimo di richieste da una connessione al secondo.

Valori predefiniti nel file *dosfilterParams*:

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

Network Time Protocol (NTP) Configuration (Configurazione NTP)

A volte, possono verificarsi problemi di protezione dovuti a discrepanze nelle configurazioni dell'ora di rete. È importante assicurarsi che tutti i dispositivi all'interno di una rete dispongano di impostazioni dell'ora precise per evitare tali problemi.

Virtual appliance

È possibile configurare i server NTP dalla console di manutenzione dell'appliance virtuale. Gli utenti possono aggiungere i dettagli del server NTP in *System Configuration* ⇒ *Add new NTP Server* option

Per impostazione predefinita, il servizio per NTP è ntpd. Si tratta di un servizio legacy che in alcuni casi non funziona bene per le macchine virtuali.

Debian

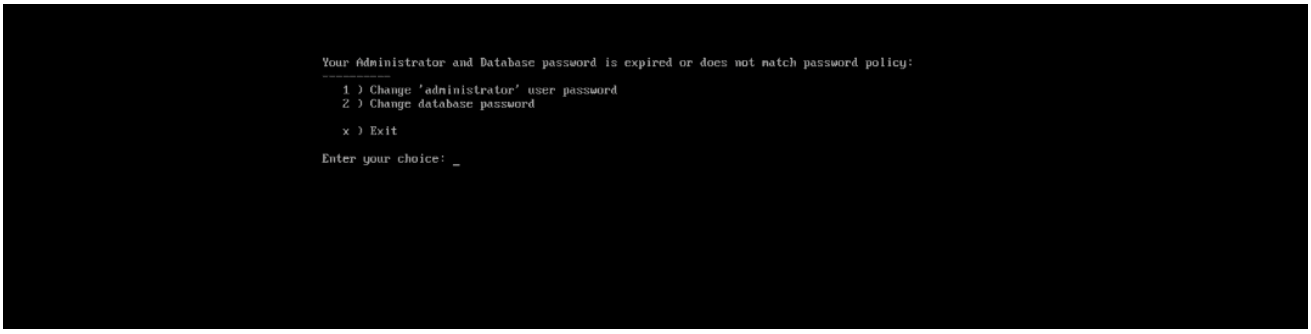
Su Debian, l'utente può accedere al file /etc/ntp.conf per i dettagli del server ntp.

Criteri password

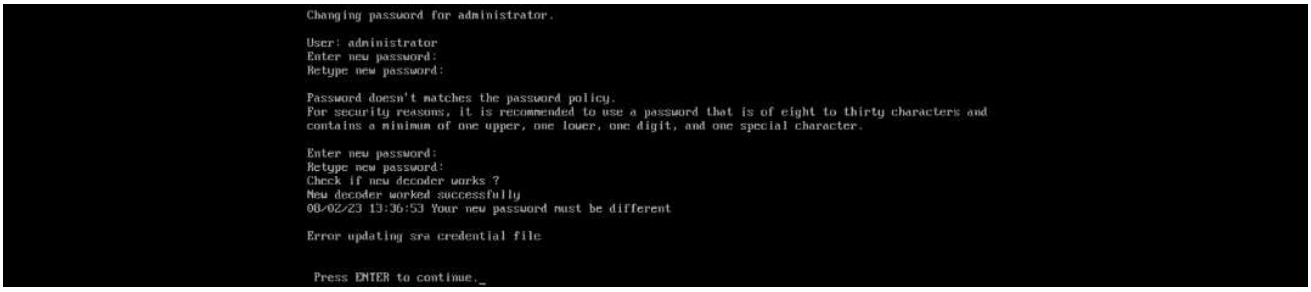
Gli utenti che distribuiscono gli strumenti ONTAP per la prima volta o che eseguono l'aggiornamento alla versione 9,12 o successiva dovranno seguire il criterio password complessa sia per gli utenti dell'amministratore che per quelli del database. Durante il processo di distribuzione, ai nuovi utenti verrà richiesto di immettere le password. Per gli utenti di brownfield che effettuano l'aggiornamento alla versione 9,12 o successiva, l'opzione per seguire il criterio password complessa sarà disponibile nella console di manutenzione.

- Una volta che l'utente accede alla console principale, le password verranno controllate in base al set di regole complesso e, se risulta non essere seguite, all'utente verrà chiesto di reimpostare lo stesso.
- La validità predefinita della password è di 90 giorni e dopo 75 giorni l'utente inizierà a ricevere la notifica di modifica della password.
- È necessario impostare una nuova password ad ogni ciclo; il sistema non utilizzerà l'ultima password come nuova password.
- Ogni volta che un utente accede alla console principale, prima di caricare il menu principale controlla i criteri delle password, come le schermate seguenti:

- Se non viene rilevato seguendo il criterio password o la relativa configurazione di aggiornamento da ONTAP Tools 9,11 o precedenti. L'utente visualizzerà quindi la seguente schermata per reimpostare la password:



- Se l'utente tenta di impostare una password debole o restituisce l'ultima password, viene visualizzato il seguente errore:



Informazioni sul copyright

Informazioni sul marchio commerciale