Leitfaden zur Erhöhung der Sicherheit für ONTAP Tools für VMware vSphere

Enterprise applications

NetApp
May 19, 2024

Inhalt

Leitfaden zur Erhöhung der Sicherheit für ONTAP Tools für VMware vSphere

Leitfaden zur Erhöhung der Sicherheit für ONTAP Tools für VMware vSphere

Der Security Hardening Guide für ONTAP-Tools für VMware vSphere enthält umfassende Anweisungen zur Konfiguration der sichersten Einstellungen.

Diese Anleitungen gelten sowohl für die Anwendungen als auch für das Gastbetriebssystem des Geräts selbst.

Überprüfen der Integrität der ONTAP Tools für VMware vSphere Installationspakete

Es gibt zwei Methoden, mit denen Kunden die Integrität ihrer Installationspakete für ONTAP-Tools überprüfen können.

1. Überprüfen der Prüfsummen
2. Überprüfen der Signatur

Prüfsummen werden auf den Download-Seiten der OTV-Installationspakete zur Verfügung gestellt. Benutzer müssen die Prüfsummen der heruntergeladenen Pakete anhand der auf der Download-Seite angegebenen Prüfsumme überprüfen.

Überprüfen der Signatur der ONTAP-Tools OVA

Das vApp-Installationspaket wird in Form eines Tarballs geliefert. Dieser Tarball enthält Zwischen- und Root-Zertifikate für das virtuelle Gerät sowie eine README-Datei und ein OVA-Paket. Die README-Datei führt Benutzer dazu, wie die Integrität des vApp OVA-Pakets überprüft wird.

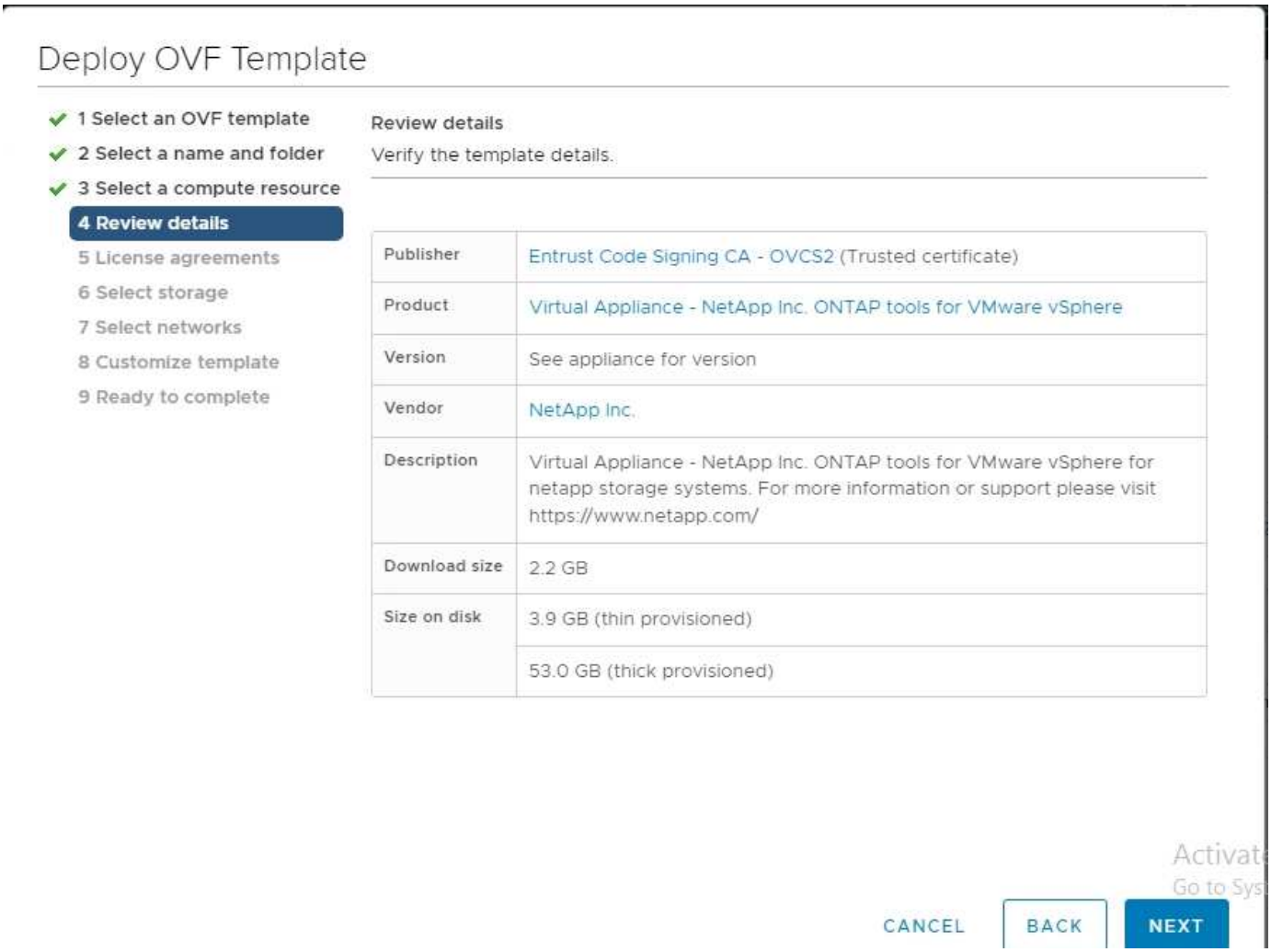
Kunden müssen auch das bereitgestellte Root- und Intermediate-Zertifikat auf vCenter Version 7.0U3E und höher hochladen. Bei vCenter-Versionen zwischen 7.0.1 und 7.0.U3E wird die Funktion zur Überprüfung des Zertifikats von VMware nicht unterstützt. Kunden müssen kein Zertifikat für vCenter Version 6.x hochladen

Hochladen des vertrauenswürdigen Stammzertifikats in vCenter

1. Melden Sie sich mit dem VMware vSphere Client beim vCenter Server an.
2. Geben Sie den Benutzernamen und das Kennwort für administrator@vsphere.local oder ein anderes Mitglied der vCenter Single Sign-On-Administratorgruppe an. Wenn Sie während der Installation eine andere Domäne angegeben haben, melden Sie sich als Administrator@mydomain an.
3. Navigieren Sie zur Benutzeroberfläche Zertifikatverwaltung: a. Wählen Sie im Home-Menü die Option Administration. B. Klicken Sie unter Zertifikate auf Zertifikatverwaltung.
4. Wenn Sie vom System aufgefordert werden, geben Sie die Anmeldedaten Ihres vCenter-Servers ein.
5. Klicken Sie unter Vertrauenswürdige Stammzertifikate auf Hinzufügen.
6. Klicken Sie auf Durchsuchen, und wählen Sie den Speicherort der .pem-Zertifikatdatei (OTV_OVA_INTER_ROOT_CERT_CHAIN.pem) aus.

7. Klicken Sie Auf Hinzufügen. Das Zertifikat wird dem Store hinzugefügt.

Siehe "Fügen Sie dem Zertifikatspeicher ein vertrauenswürdiges Stammzertifikat hinzu" Finden Sie weitere Informationen. Während der Bereitstellung einer vApp (mithilfe der OVA-Datei) kann die digitale Signatur für das vApp-Paket auf der Seite „Details überprüfen“ überprüft werden. Wenn es sich bei dem heruntergeladenen vApp-Paket um ein Originalprodukt handelt, wird in der Spalte „Publisher“ (Herausgeber) die Option „Vertrauenswürdiges Zertifikat“ angezeigt (wie im folgenden Screenshot).



Überprüfen der Signatur der ONTAP-Tools ISO und SRA tar.gz

NetApp teilt sein Code Signing-Zertifikat mit Kunden auf der Produkt-Download-Seite, zusammen mit den Produkt-Zip-Dateien für OTV-ISO und SRA.tgz.

Aus dem Code-Signing-Zertifikat können Benutzer den öffentlichen Schlüssel wie folgt extrahieren:

```
 #> openssl x509 -in <code-sign-cert, pem file> -pubkey -noout > <public-
key name>
Dann sollte der öffentliche Schlüssel verwendet werden, um die Signatur
für iso und tgz Produkt zip wie unten zu überprüfen:
```

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

```
#> 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
```

Ports und Protokolle

In dieser Liste sind die erforderlichen Ports und Protokolle aufgeführt, die die Kommunikation zwischen ONTAP Tools für VMware vSphere Server und anderen Einheiten wie gemanagten Storage-Systeme, Servern und anderen Komponenten ermöglichen.

Für OTV erforderliche ein- und ausgehende Ports

Bitte beachten Sie die folgende Tabelle, in der die ein- und ausgehenden Ports aufgeführt sind, die für das ordnungsgemäße Funktionieren der ONTAP-Tools erforderlich sind. Es ist wichtig sicherzustellen, dass nur die in der Tabelle genannten Ports für Verbindungen von Remotecomputern geöffnet sind, während alle anderen Ports für Verbindungen von Remotecomputern gesperrt werden sollten. Dadurch wird die Sicherheit und Sicherheit Ihres Systems gewährleistet.

In der folgenden Tabelle werden die Details zum offenen Anschluss beschrieben.

TCP v4/v6-Port #	Richtung	Funktion
8143	Eingehend	HTTPS-Verbindungen für REST-API
8043	Eingehend	HTTPS-Verbindungen
9060	Eingehend	HTTPS-Verbindungen Wird für SOAP über HTTPS-Verbindungen verwendet Dieser Port muss geöffnet werden, damit ein Client eine Verbindung zum ONTAP Tools API-Server herstellen kann.
22	Eingehend	SSH (standardmäßig deaktiviert)
9080	Eingehend	HTTPS-Verbindungen - VP und SRA - nur interne Verbindungen von Loopback
9083	Eingehend	HTTPS-Verbindungen - VP und SRA Wird für SOAP-Verbindungen über HTTPS verwendet
1162	Eingehend	VP SNMP-Trap-Pakete
8443	Eingehend	Remote-Plug-In

TCP v4/v6-Port #	Richtung	Funktion
1527	Nur zur internen Nutzung	Derby-Datenbank-Port, nur zwischen diesem Computer und sich selbst, externe Verbindungen nicht akzeptiert - nur interne Verbindungen
8150	Nur zur internen Nutzung	Der Protokollintegritätsservice wird auf dem Port ausgeführt
443	Bidirektional	Wird für Verbindungen zu ONTAP-Clustern verwendet

Steuern des Remote-Zugriffs auf die Derby-Datenbank

Administratoren können mit den folgenden Befehlen auf die derby-Datenbank zugreifen. Der Zugriff ist über die lokale VM der ONTAP-Tools sowie über einen Remote-Server mit den folgenden Schritten möglich:

```
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>';
```

Beispiel:

```
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                     |
```

ONTAP Tools für VMware vSphere Access Points (User)

Mit der Installation der ONTAP Tools für VMware vSphere werden drei Benutzertypen erstellt und verwendet:

1. Systembenutzer: Das root-Benutzerkonto
2. Anwendungsbenutzer: Administratorbenutzer, Benutzerkonten und db-Benutzerkonten
3. Support-Benutzer: Das diag-Benutzerkonto

1. Systembenutzer

System(root) Benutzer wird von ONTAP-Tools-Installation auf dem zugrunde liegenden Betriebssystem (Debian) erstellt.

- Ein Standardsystembenutzer "root" wird auf Debian von der Installation der ONTAP-Tools erstellt. Der Standardwert ist deaktiviert und kann per Ad-hoc-Funktion über die „Wartung“-Konsole aktiviert werden.

2. Anwendungsbenutzer

Der Anwendungsbenutzer wird in ONTAP-Tools als lokaler Benutzer benannt. Diese Benutzer wurden in der Anwendung ONTAP Tools erstellt. In der folgenden Tabelle sind die Typen von Anwendungsbenutzern aufgeführt:

* Benutzer*	Beschreibung
Administratorbenutzer	Es wird während der Installation von ONTAP Tools erstellt, und Benutzer bietet die Anmeldeinformationen während der Bereitstellung der ONTAP Tools. Benutzer haben die Möglichkeit, das 'Passwort' in der 'Wartung'-Konsole zu ändern. Das Passwort läuft in 90 Tagen ab, und Benutzer werden davon ausgehen, dass es sich um dasselbe Passwort handelt.
Wartungsbenutzer	Es wird während der Installation von ONTAP Tools erstellt, und Benutzer bietet die Anmeldeinformationen während der Bereitstellung der ONTAP Tools. Benutzer haben die Möglichkeit, das 'Passwort' in der 'Wartung'-Konsole zu ändern. Dies ist ein Wartungsbenutzer und wird zur Ausführung der Wartungskonsolenoperationen erstellt.
Datenbankbenutzer	Es wird während der Installation von ONTAP Tools erstellt, und Benutzer bietet die Anmeldeinformationen während der Bereitstellung der ONTAP Tools. Benutzer haben die Möglichkeit, das 'Passwort' in der 'Wartung'-Konsole zu ändern. Das Passwort läuft in 90 Tagen ab, und Benutzer werden davon ausgehen, dass es sich um dasselbe Passwort handelt.

3. Support user(diag user)

Während der Installation der ONTAP-Tools wird ein Support-Benutzer erstellt. Dieser Benutzer kann für den Zugriff auf ONTAP-Tools bei Problemen oder Ausfällen im Server und zum Sammeln von Protokollen verwendet werden. Standardmäßig ist dieser Benutzer deaktiviert, kann aber per Ad-hoc-Funktion über die „Wartung“-Konsole aktiviert werden. Beachten Sie, dass dieser Benutzer nach einem bestimmten Zeitraum automatisch deaktiviert wird.

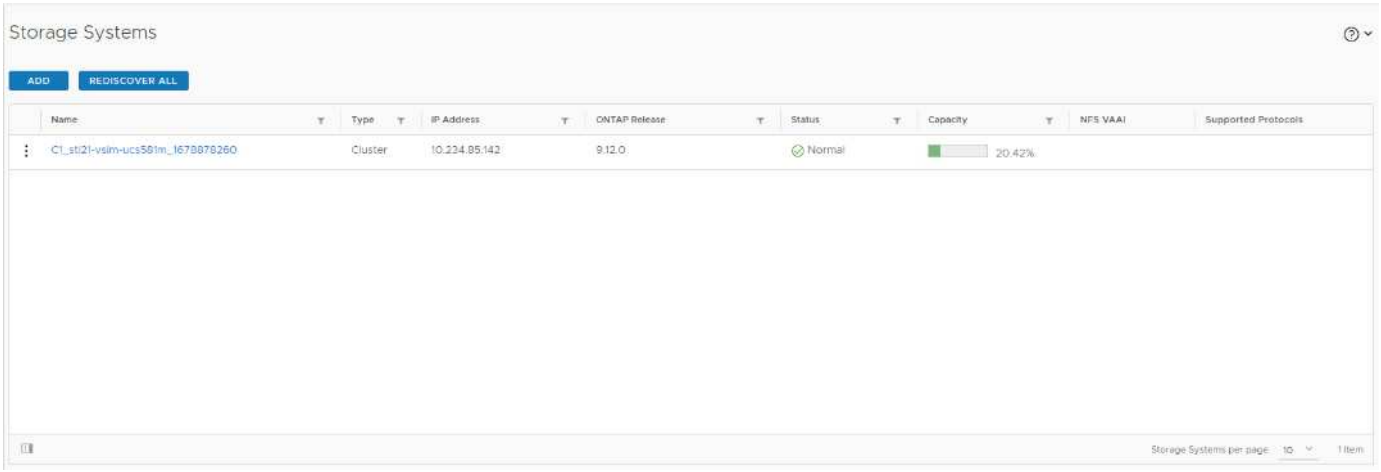
Mutual TLS (Certificate-Based Authentication)

ONTAP Version 9.7 und höher unterstützen die gegenseitige TLS-Kommunikation. Ab ONTAP Tools für VMware und vSphere 9.12 wird wechselseitiges TLS für die Kommunikation mit neu hinzugefügten Clustern verwendet (je nach ONTAP Version).

ONTAP

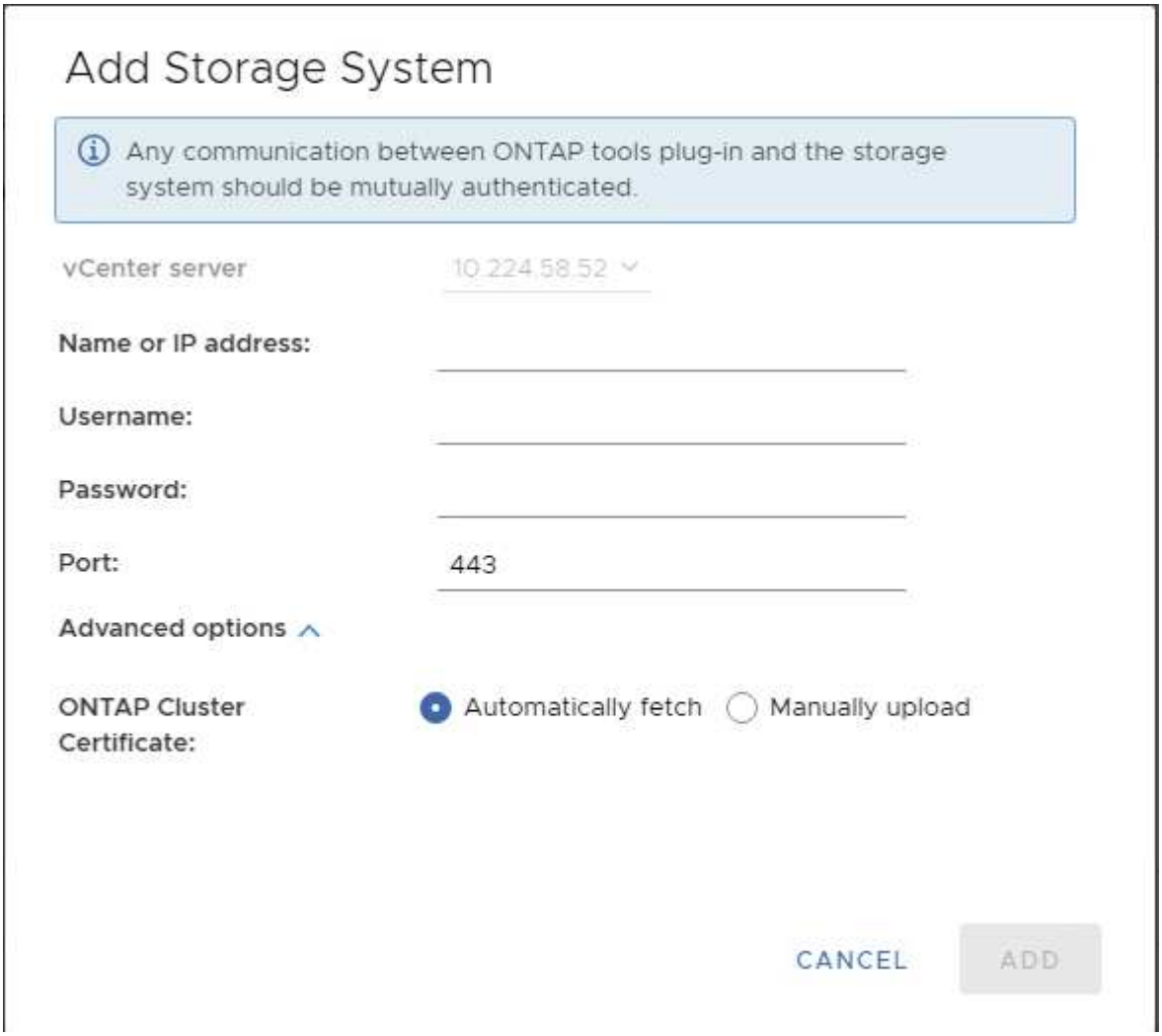
Für alle zuvor hinzugefügten Speichersysteme: Während eines Upgrades werden alle hinzugefügten Speichersysteme automatisch vertrauenswürdig und die zertifikatbasierten Authentifizierungsmechanismen werden konfiguriert.

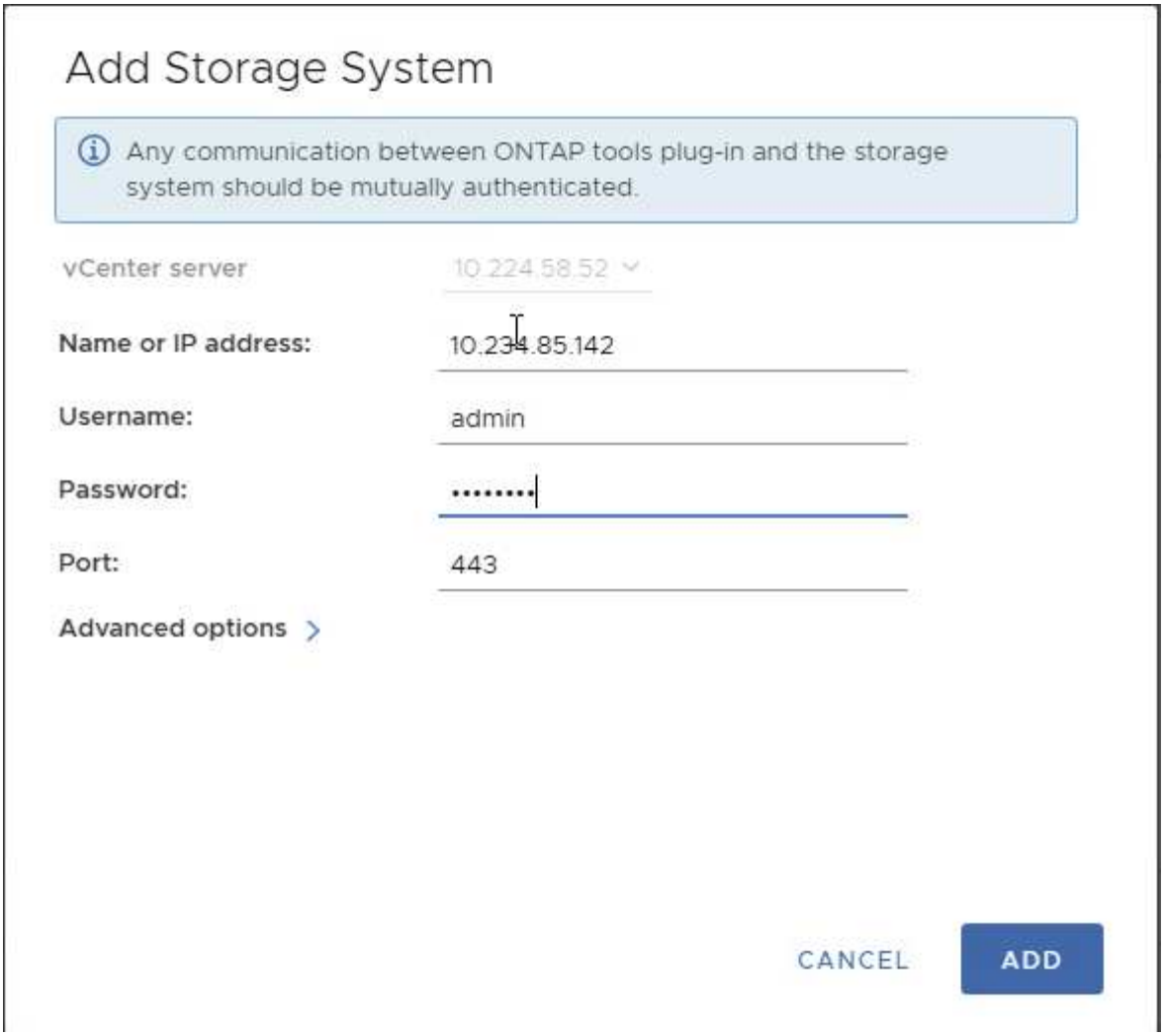
Wie im Screenshot unten gezeigt, zeigt die Cluster-Setup-Seite den Status von Mutual TLS (Certificate-Based Authentication) an, die für jeden Cluster konfiguriert wurden.

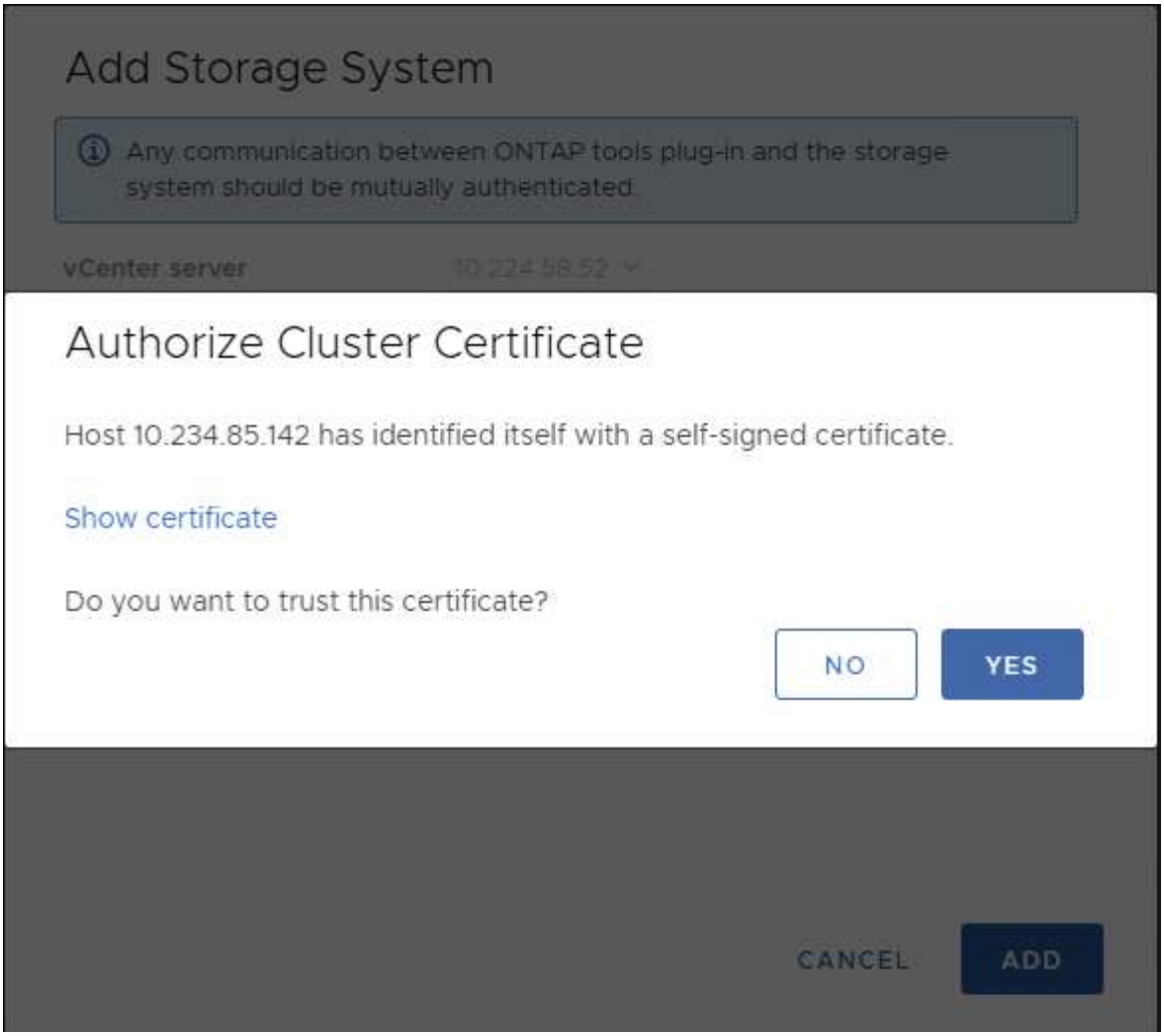


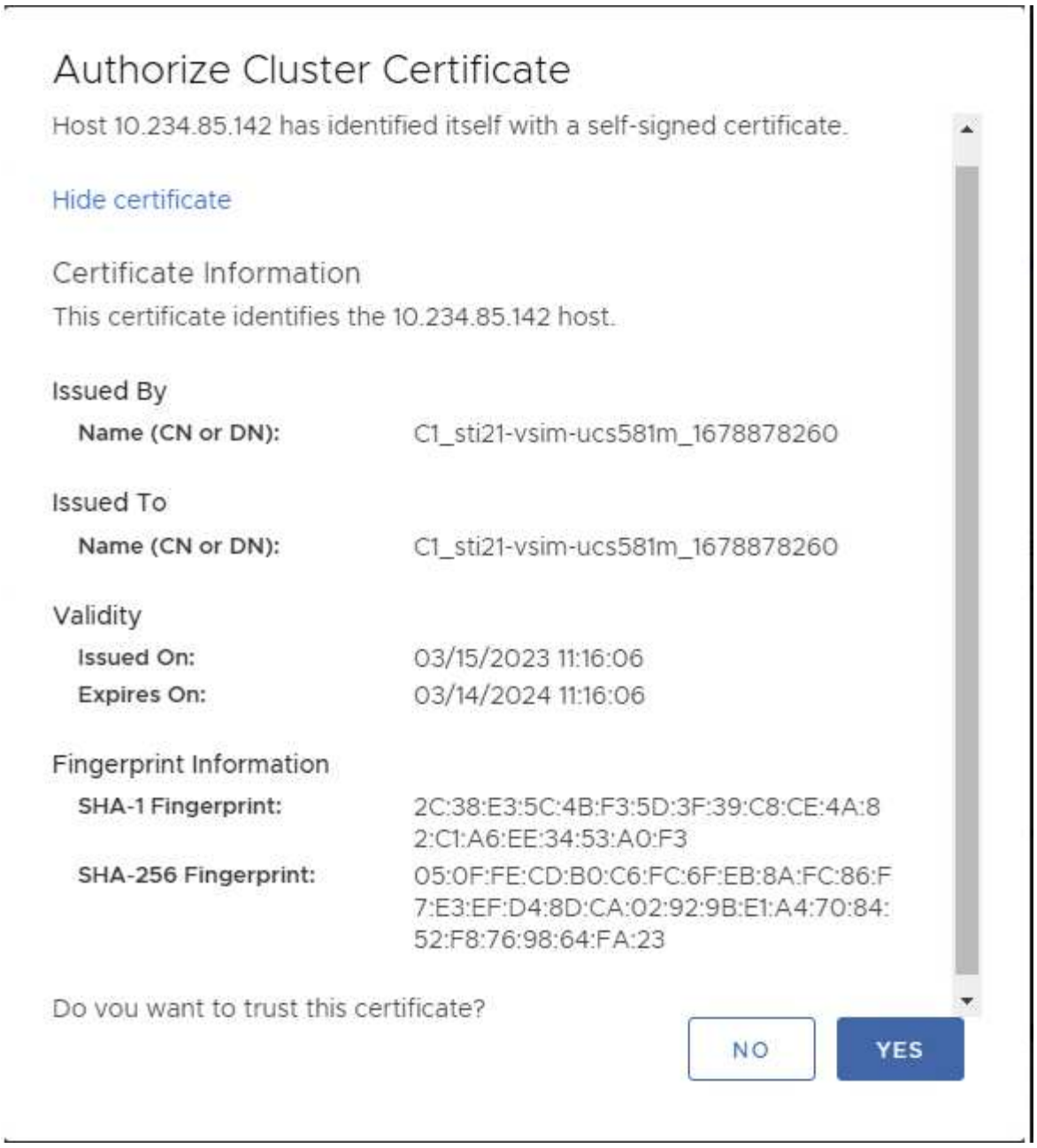
Cluster Hinzufügen

Wenn das hinzugefügte Cluster MTLS unterstützt, wird MTLS während des Cluster-Add-Workflows standardmäßig konfiguriert. Der Benutzer muss hierfür keine Konfiguration vornehmen. Im Screenshot unten wird der Bildschirm angezeigt, der dem Benutzer beim Hinzufügen von Cluster angezeigt wird.




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

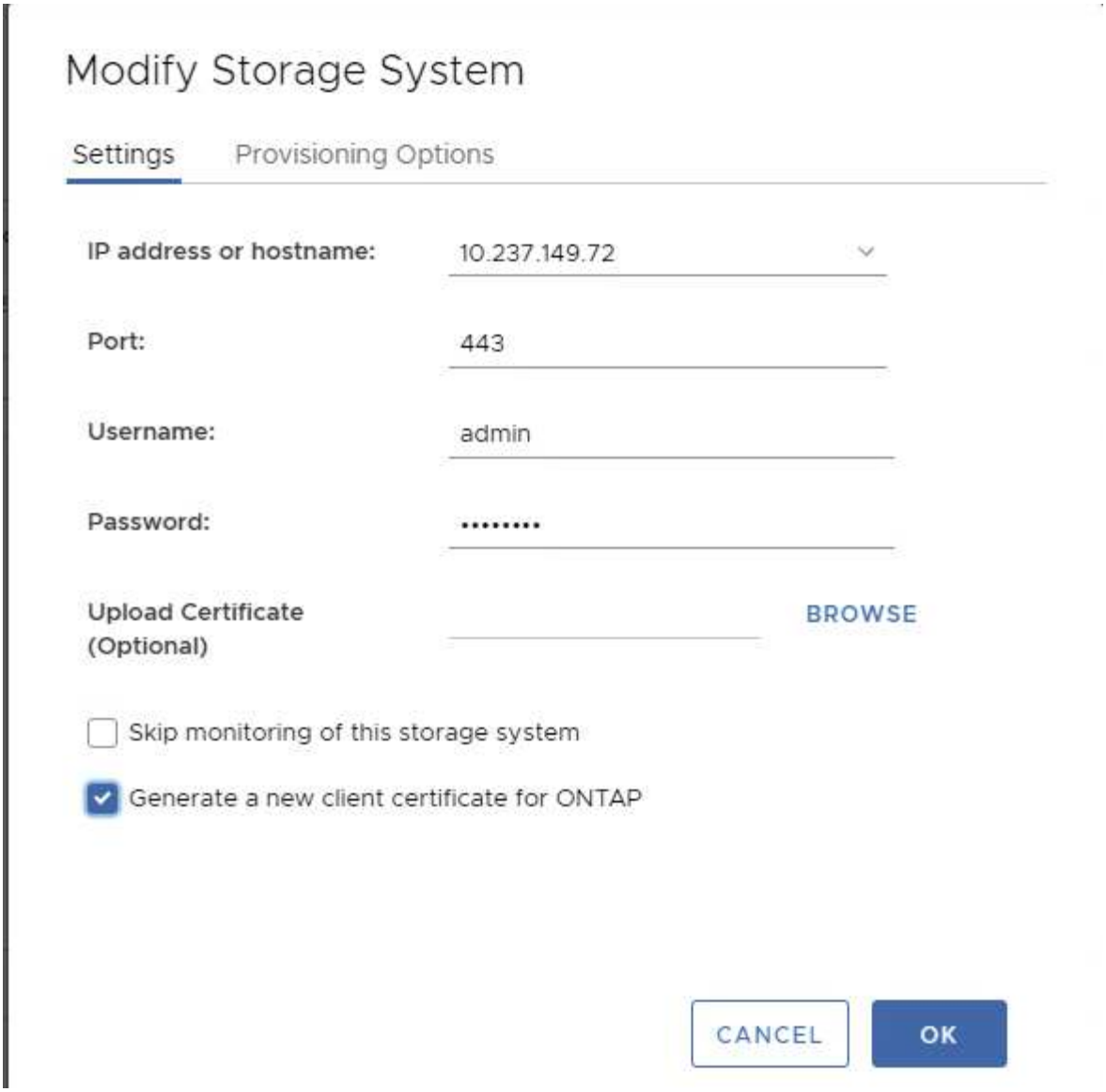

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
Authorize Cluster Certificate
Host 10.234.85.142 has identified itself with a self-signed certificate.
Show certificate
Do you want to trust this certificate?
NO
YES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

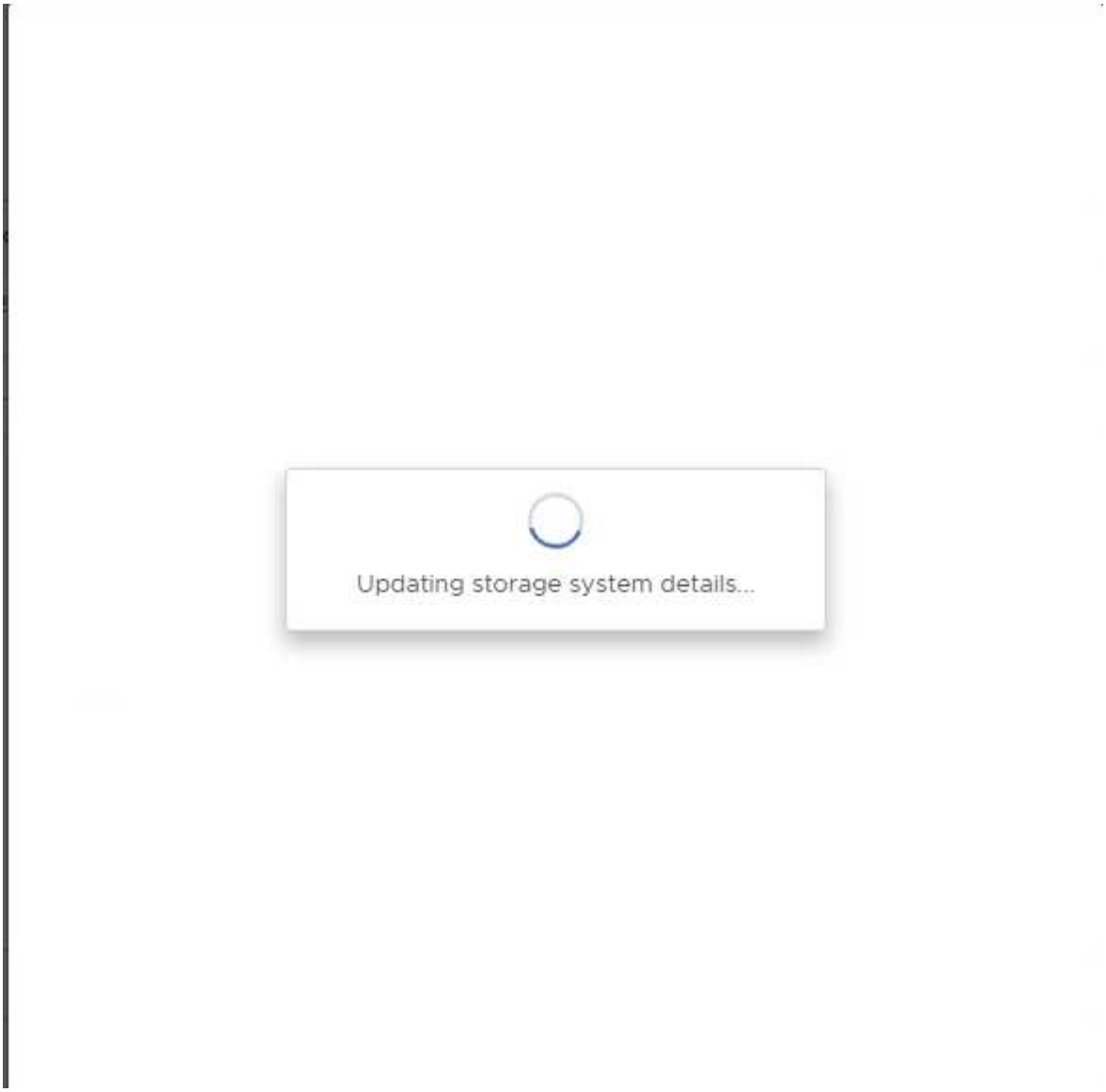


Cluster-Bearbeitung

Während der Cluster-Bearbeitung gibt es zwei Szenarien:

- Wenn das ONTAP-Zertifikat abläuft, muss der Benutzer das neue Zertifikat erhalten und hochladen.
- Wenn das OTV-Zertifikat abläuft, kann der Benutzer es durch Aktivieren des Kontrollkästchens neu generieren.
  - *Generieren Sie ein neues Client-Zertifikat für 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



HTTPS-Zertifikat für ONTAP-Tools

Standardmäßig verwendet ONTAP-Tools ein selbstsigniertes Zertifikat, das bei der Installation automatisch erstellt wird, um den HTTPS-Zugriff auf die Web-Benutzeroberfläche zu sichern. Funktionen der ONTAP Tools:

1. HTTPS-Zertifikat neu generieren

Während der Installation der ONTAP-Tools wird ein HTTPS-CA-Zertifikat installiert und das Zertifikat wird im Keystore gespeichert. Der Benutzer hat die Möglichkeit, das HTTPS-Zertifikat über die maint-Konsole neu zu generieren.

Auf die oben genannten Optionen kann in der *maint*-Konsole zugegriffen werden, indem Sie zu *'Anwendungskonfiguration' → 'Zertifikate erneut generieren' navigieren.*

Anmelde-Banner

Das folgende Anmeldebanner wird angezeigt, nachdem der Benutzer einen

Benutzernamen in die Anmeldeaufforderung eingegeben hat. Beachten Sie bitte, dass SSH standardmäßig deaktiviert ist und nur einmalige Anmeldungen zulässt, wenn sie über die VM-Konsole aktiviert werden.

```
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.
```

Nachdem der Benutzer die Anmeldung über den SSH-Kanal abgeschlossen hat, wird der folgende Text angezeigt:

```
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.
```

Zeitüberschreitung Bei Inaktivität

Um unbefugten Zugriff zu verhindern, wird ein Inaktivitäts-Timeout eingerichtet, das automatisch Benutzer abmeldet, die für einen bestimmten Zeitraum inaktiv sind, während autorisierte Ressourcen verwendet werden. So wird sichergestellt, dass nur autorisierte Benutzer auf die Ressourcen zugreifen können und die Sicherheit gewahrt bleibt.

- Standardmäßig werden die vSphere Client-Sitzungen nach 120 Minuten Leerlaufzeit geschlossen, sodass sich der Benutzer erneut anmelden muss, um die Verwendung des Clients fortzusetzen. Sie können den Timeout-Wert ändern, indem Sie die Datei webclient.properties bearbeiten. Sie können das Timeout des vSphere-Clients konfigurieren "Konfigurieren Sie den Wert für die Zeitüberschreitung des vSphere-Clients"
- Die Abmeldezeit für ONTAP-Tools beträgt 30 Minuten für die Web-cli-Sitzung.

Maximale Anzahl gleichzeitiger Anfragen pro Benutzer (Netzwerksicherheitsschutz :: DOS-Angriff)

Standardmäßig beträgt die maximale Anzahl gleichzeitiger Anfragen pro Benutzer 48. Der Root-Benutzer in ONTAP-Tools kann diesen Wert je nach den Anforderungen seiner Umgebung ändern. **Dieser Wert sollte nicht auf einen sehr hohen Wert gesetzt werden, da er einen Mechanismus gegen Denial-of-Service (DOS) Angriffe bietet.**

Benutzer können die Anzahl der maximalen gleichzeitigen Sessions und andere unterstützte Parameter in der Datei ***/opt/netapp/vscserver/etc/dosfilterParams.json*** ändern.

Wir können den Filter mit folgenden Parametern konfigurieren:

- ***delayMs***: Die Verzögerung in Millisekunden, die allen Anfragen über das Limit der Rate gegeben wird, bevor sie berücksichtigt werden. Geben Sie -1, um die Anfrage einfach abzulehnen.
- ***drossleMS***: Wie lange warten Sie auf Semaphore.
- ***maxRequestms***: Wie lange soll diese Anfrage laufen lassen?
- ***ipWhitelist***: Eine kommagetrennte Liste von IP-Adressen, die nicht ratenbegrenzt ist. (Dies können vCenter-, ESXi- und SRA-IPs sein)
- ***maxRequestsPerSec***: Die maximale Anzahl von Anfragen einer Verbindung pro Sekunde.

Standardwerte in der *dosfilterParams-Datei*:

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

NTP-Konfiguration (Network Time Protocol

Manchmal können Sicherheitsprobleme aufgrund von Diskrepanzen bei der Konfiguration der Netzwerkzeit auftreten. Es ist wichtig, dass alle Geräte innerhalb eines Netzwerks über genaue Zeiteinstellungen verfügen, um solche Probleme zu vermeiden.

Virtuelles Gerät

Sie können den/die NTP-Server über die Wartungskonsole in der virtuellen Appliance konfigurieren. Benutzer können die NTP-Server-Details unter der Option *System Configuration ⇒ Add New NTP Server* hinzufügen

Standardmäßig lautet der Service für NTP ntpd. Es handelt sich hierbei um einen Legacy-Service, der in bestimmten Fällen für virtuelle Maschinen nicht gut funktioniert.

Debian

Auf Debian kann der Benutzer auf die Datei /etc/ntp.conf zugreifen, um ntp-Serverdetails zu erhalten.

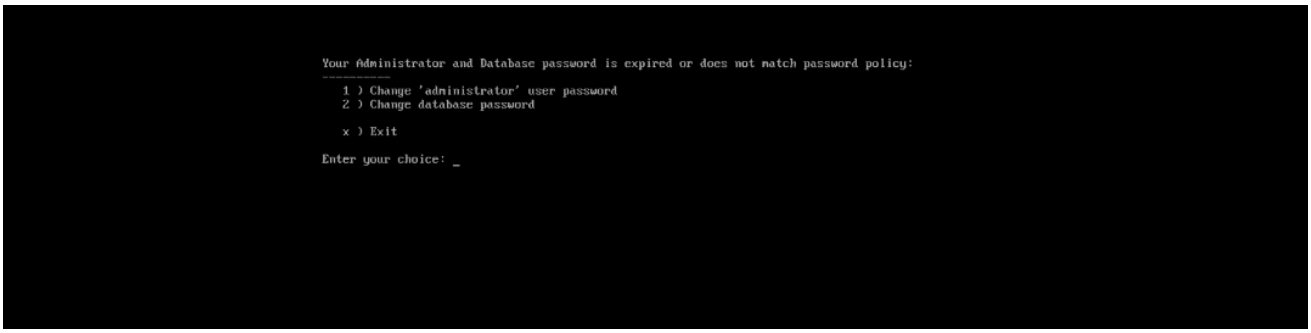
Passwortrichtlinien

Benutzer, die ONTAP-Tools zum ersten Mal bereitstellen oder ein Upgrade auf Version 9.12 oder höher durchführen, müssen die Richtlinie für starkes Kennwort sowohl für den Administrator als auch für Datenbankbenutzer befolgen. Während des Bereitstellungsprozesses werden neue Benutzer aufgefordert, ihre Passwörter einzugeben. Für Brownfield-Benutzer, die auf Version 9.12 oder höher aktualisieren, wird

die Option zur Einhaltung der Richtlinie für starke Kennwörter in der Wartungskonsole verfügbar sein.

- Sobald sich der Benutzer in der maint-Konsole anmeldet, werden die Passwörter anhand der komplexen Regelsammlung überprüft. Wenn er nicht befolgt wird, wird der Benutzer aufgefordert, das gleiche zurückzusetzen.
- Die Standardgültigkeit des Passworts beträgt 90 Tage, und nach 75 Tagen erhält der Benutzer die Benachrichtigung, das Kennwort zu ändern.
- Es ist erforderlich, in jedem Zyklus ein neues Passwort festzulegen, das System nimmt nicht das letzte Passwort als neues Passwort.
- Wenn sich ein Benutzer an der maint-Konsole anmeldet, überprüft er vor dem Laden des Hauptmenüs nach den Passwortrichtlinien wie den folgenden Screenshots:

- Wenn die Kennwortrichtlinie oder das Upgrade-Setup von ONTAP Tools 9.11 oder früher nicht verwendet wurde. Der Benutzer wird dann den folgenden Bildschirm sehen, um das Passwort zurückzusetzen:



- Wenn der Benutzer versucht, ein schwaches Passwort festzulegen oder das letzte Passwort erneut gibt, wird der Benutzer folgende Fehlermeldung sehen: