ONTAP tools for VMware vSphere向けセキュリティ強化ガイド

Enterprise applications

NetApp
May 09, 2024

目次

ONTAP tools for VMware vSphere向けセキュリティ強化ガイド

ONTAP tools for VMware vSphere向けセキュリティ強化ガイド

ONTAP tools for VMware vSphereのセキュリティ強化ガイドには、最も安全な設定を構成するための包括的な手順が記載されています。

これらのガイドは、アプライアンス自体のアプリケーションとゲストOSの両方に適用されます。

ONTAP Tools for VMware vSphereインストールパッケージの整合性の検証

ONTAP toolsインストールパッケージの整合性を検証するには、2つの方法があります。

1. チェックサムの確認
2. シグネチャの検証

チェックサムは、OTVインストールパッケージのダウンロードページで提供されています。ダウンロードしたパッケージのチェックサムを、ダウンロードページに表示されているチェックサムと照合して確認する必要があります。

ONTAP tools OVAの署名の確認

vAppインストールパッケージはtarball形式で提供されます。このtarballには、仮想アプライアンスの中間証明書とルート証明書、READMEファイル、OVAパッケージが含まれています。READMEファイルには、vApp OVAパッケージの整合性を検証する方法が記載されています。

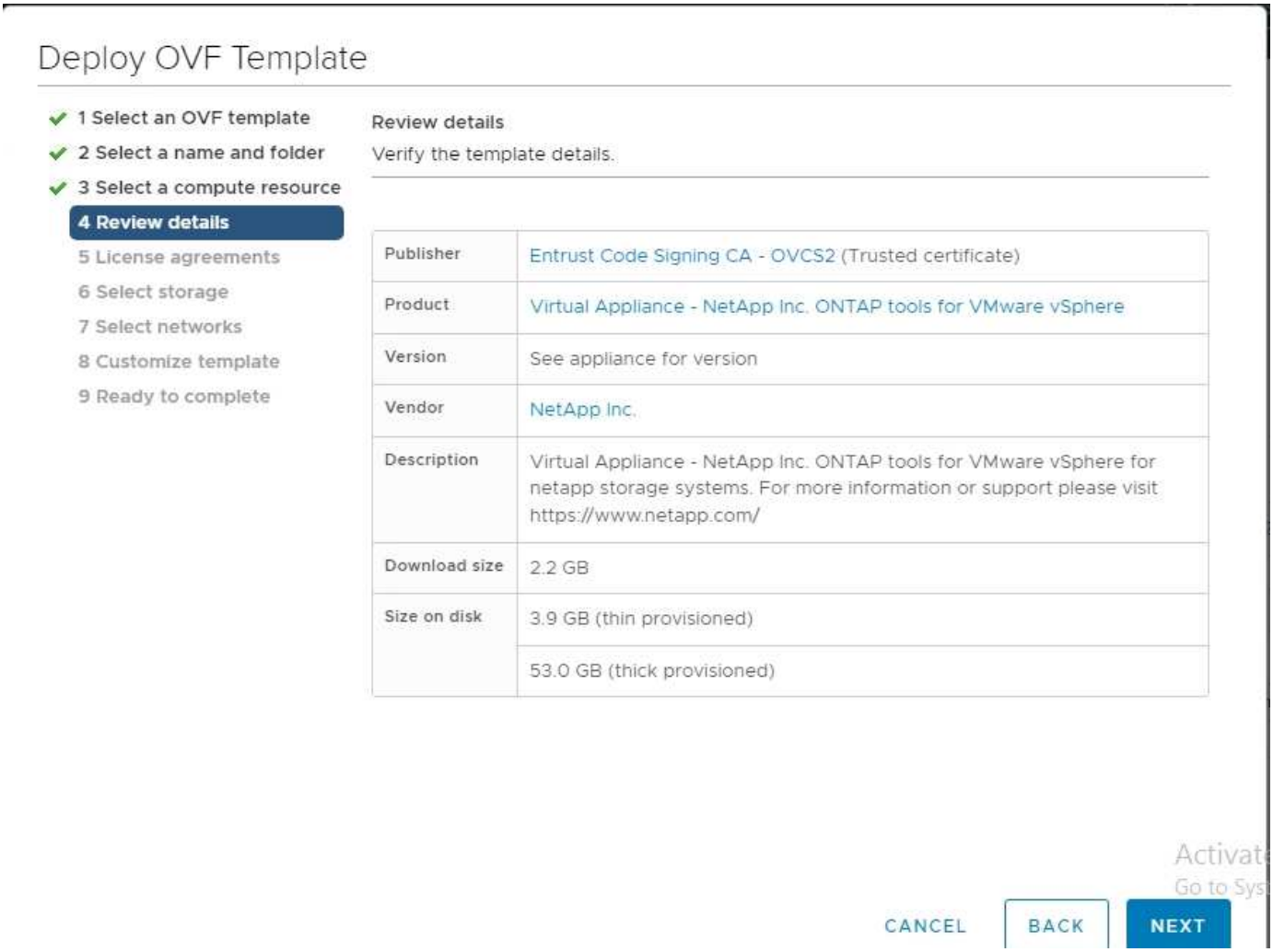
また、提供されたルート証明書と中間証明書をvCenterバージョン7.0U3E以降にアップロードする必要があります。 vCenterのバージョン7.0.1から7.0.U3Eの場合、証明書を検証する機能はVMwareではサポートされていません。vCenterバージョン6.xの証明書はアップロードする必要はありません。

信頼されたルート証明書の**vCenter**へのアップロード

1. VMware vSphere ClientでvCenter Serverにログインします。
2. administrator@vsphere.localまたはvCenter Single Sign-On Administratorsグループの別のメンバーのユーザ名とパスワードを指定します。インストール時に別のドメインを指定した場合は、administrator@mydomainとしてログインします。
3. 証明書管理ユーザーインターフェイスに移動します。a.[ホーム]メニューから[管理]を選択します。B[証明書]で、[証明書管理]をクリックします。
4. プロンプトが表示されたら、vCenter Serverのクレデンシャルを入力します。
5. [信頼されたルート証明書]で、[追加]をクリックします。
6. [browse]をクリックし、証明書の.pemファイル（otv_ova_inter_root_cert_chain.pem）の場所を選択します。

7. 追加をクリックします。証明書がストアに追加されます。

を参照してください "証明書ストアへの信頼されたルート証明書の追加" を参照してください。（OVAファイルを使用して）vAppを導入する際、vAppパッケージのデジタル署名は[Review details]ページで確認できます。ダウンロードしたvAppパッケージが正規のものである場合は、[発行者]列に[信頼された証明書]と表示されます（次のスクリーンショットを参照）。



ONTAP tools ISOおよびSRA tar.gzの署名の確認

NetAppは、製品ダウンロードページでコード署名証明書をお客様と共有し、OTV-ISOおよびsra.tgzの製品zipファイルも提供しています。

コード署名証明書から、ユーザーは次のように公開鍵を抽出できます。

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

公開鍵を使用して、以下のようにISOおよびtgz製品zipの署名を検証する必要があります。

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

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
```

ポートとプロトコル

ここでは、ONTAP tools for VMware vSphereサーバと、管理対象のストレージシステム、サーバ、その他のコンポーネントなどのエンティティ間の通信に必要なポートとプロトコルを示します。

OTVに必要なインバウンドおよびアウトバウンドポート

次の表に、ONTAP toolsが適切に機能するために必要なインバウンドポートとアウトバウンドポートを示します。表に記載されているポートだけがリモートマシンからの接続用に開いていることを確認し、他のすべてのポートはリモートマシンからの接続用にブロックする必要があります。これにより、システムのセキュリティと安全性が確保されます。

次の表に、オープンポートの詳細を示します。

*** TCP v4/V6**ポート番号*****	* 方向 *	機能
8143	インバウンド	REST API 用の HTTPS 接続
8043	インバウンド	HTTPS 接続
9060	インバウンド	HTTPS接続+ SOAP over HTTPS接続に使用+ クライアントがONTAP tools APIサーバに接続できるようにするには、このポートを開く必要があります。
22	インバウンド	SSH （デフォルトでは無効）
9080	インバウンド	HTTPS 接続 - VP および SRA - ループバックからの内部接続のみ
9083年だ	インバウンド	HTTPS接続- VPおよびSRA+ SOAP over HTTPS接続に使用
一一六二	インバウンド	VP SNMP トラップパケット
8443	インバウンド	リモートプラグイン
1527年	内部のみ	Derbyデータベースポート、このコンピュータとそれ自体の間のみ、外部接続は許可されません-内部接続のみ

* TCP v4/V6ポート番号*	* 方向 *	機能
8150	内部のみ	ログ整合性サービスはポートで実行されます
443	双方向	ONTAP クラスタへの接続に使用します

Derbyデータベースへのリモートアクセスの制御

管理者は、次のコマンドを使用してDerbyデータベースにアクセスできます。ONTAP toolsのローカルVMとリモートサーバからアクセスするには、次の手順を実行します。

```
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>';
```

例：

```
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 for VMware vSphereアクセスポイント（ユーザ）

ONTAP Tools for VMware vSphereをインストールすると、次の3種類のユーザが作成され、使用されます。

1. システムユーザ：rootユーザアカウント
2. アプリケーションユーザ：管理者ユーザ、maintユーザ、およびdbユーザアカウント
3. サポートユーザ：diagユーザアカウント

1.システムユーザ

システム(root)ユーザは、基盤となるオペレーティングシステム(Debian)にインストールされたONTAPツールによって作成されます。

- ONTAP toolsのインストールにより、デフォルトのシステムユーザ"root"がDebian上に作成されます。デフォルトでは無効になっており、「メンテナンス」コンソールから個別に有効にすることができます。

2.アプリケーションユーザ

ONTAP toolsでは、アプリケーションユーザの名前はローカルユーザです。これらは、ONTAP toolsアプリケーションで作成されたユーザです。次の表に、アプリケーションユーザのタイプを示します。

* ユーザー *	* 概要 *
管理者ユーザ	ONTAP toolsのインストール時に作成され、ONTAP toolsの導入時にユーザがクレデンシャルを指定します。ユーザは「maint」コンソールで「password」を変更できます。パスワードの有効期限は90日で、ユーザは同じパスワードを変更する必要があります。
メンテナンスユーザ	ONTAP toolsのインストール時に作成され、ONTAP toolsの導入時にユーザがクレデンシャルを指定します。ユーザは「maint」コンソールで「password」を変更できます。これはメンテナンスユーザで、メンテナンスコンソールの処理を実行するために作成されます。
データベースユーザ	ONTAP toolsのインストール時に作成され、ONTAP toolsの導入時にユーザがクレデンシャルを指定します。ユーザは「maint」コンソールで「password」を変更できます。パスワードの有効期限は90日で、ユーザは同じパスワードを変更する必要があります。

3.サポートユーザ（diagユーザ）

ONTAP toolsのインストール中に、サポートユーザが作成されます。このユーザを使用して、サーバで問題や停止が発生した場合にONTAPツールにアクセスしたり、ログを収集したりできます。デフォルトでは、このユーザは無効になっていますが、「メンテナンス」コンソールからアドホックで有効にすることができます。このユーザーは一定期間後に自動的に無効になることに注意することが重要です。

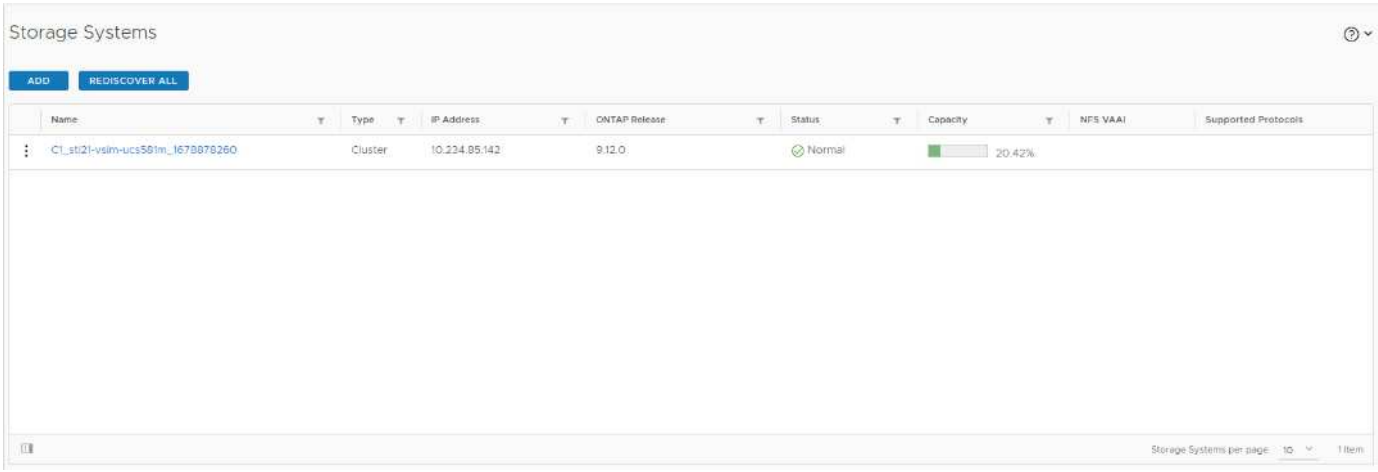
相互TLS（証明書ベースの認証）

ONTAPバージョン9.7以降では、相互TLS通信がサポートされます。ONTAP Tools for VMwareおよびvSphere 9.12以降では、新しく追加したクラスタとの通信に相互TLSが使用されます（ONTAPのバージョンによって異なります）。

ONTAP

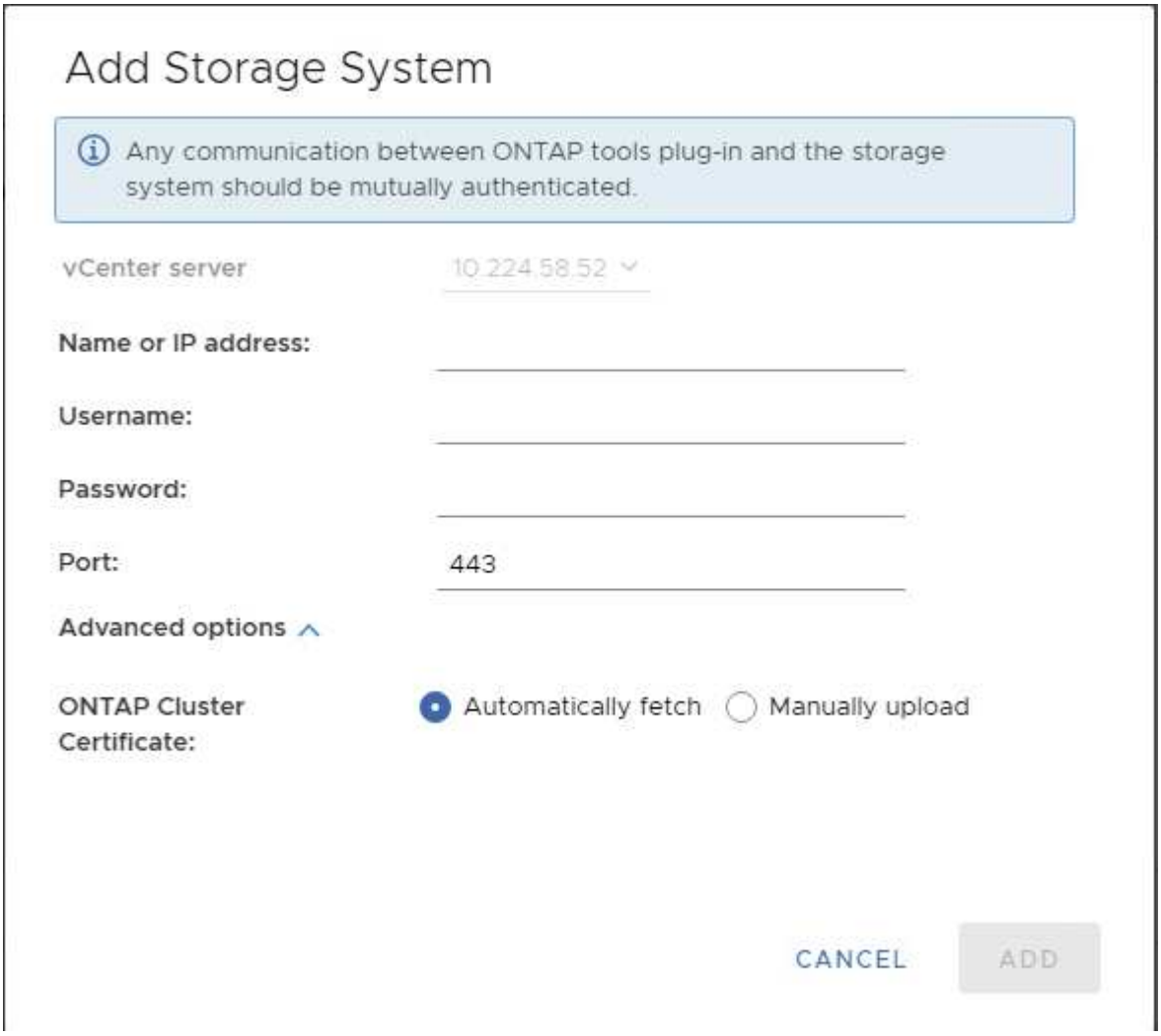
以前に追加されたすべてのストレージシステム：アップグレード中に、追加されたすべてのストレージシステムが自動信頼され、証明書ベースの認証メカニズムが設定されます。

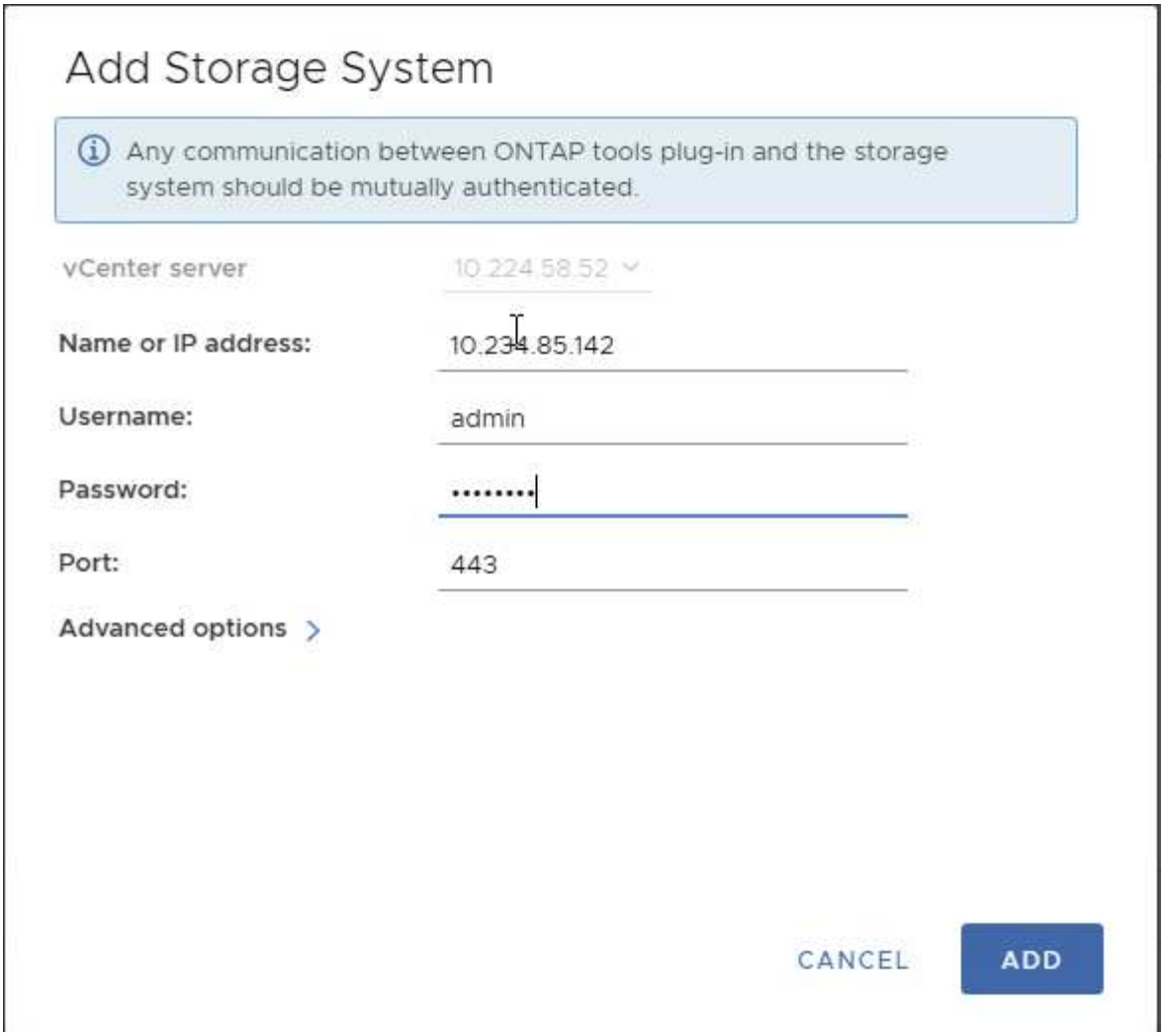
下のスクリーンショットのように、[クラスタセットアップ]ページには、各クラスタに対して設定されたMutual TLS（証明書ベースの認証）のステータスが表示されます。

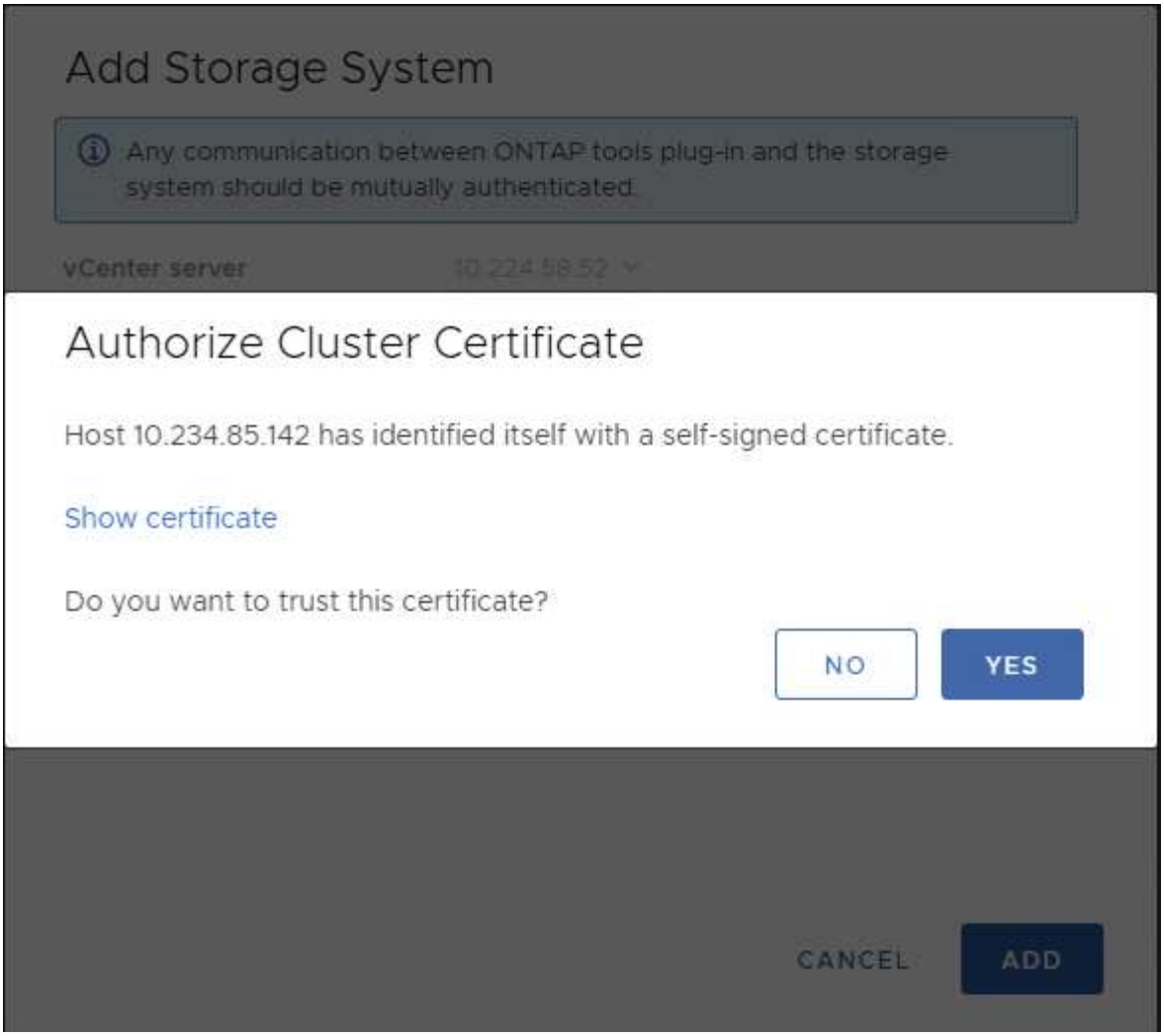


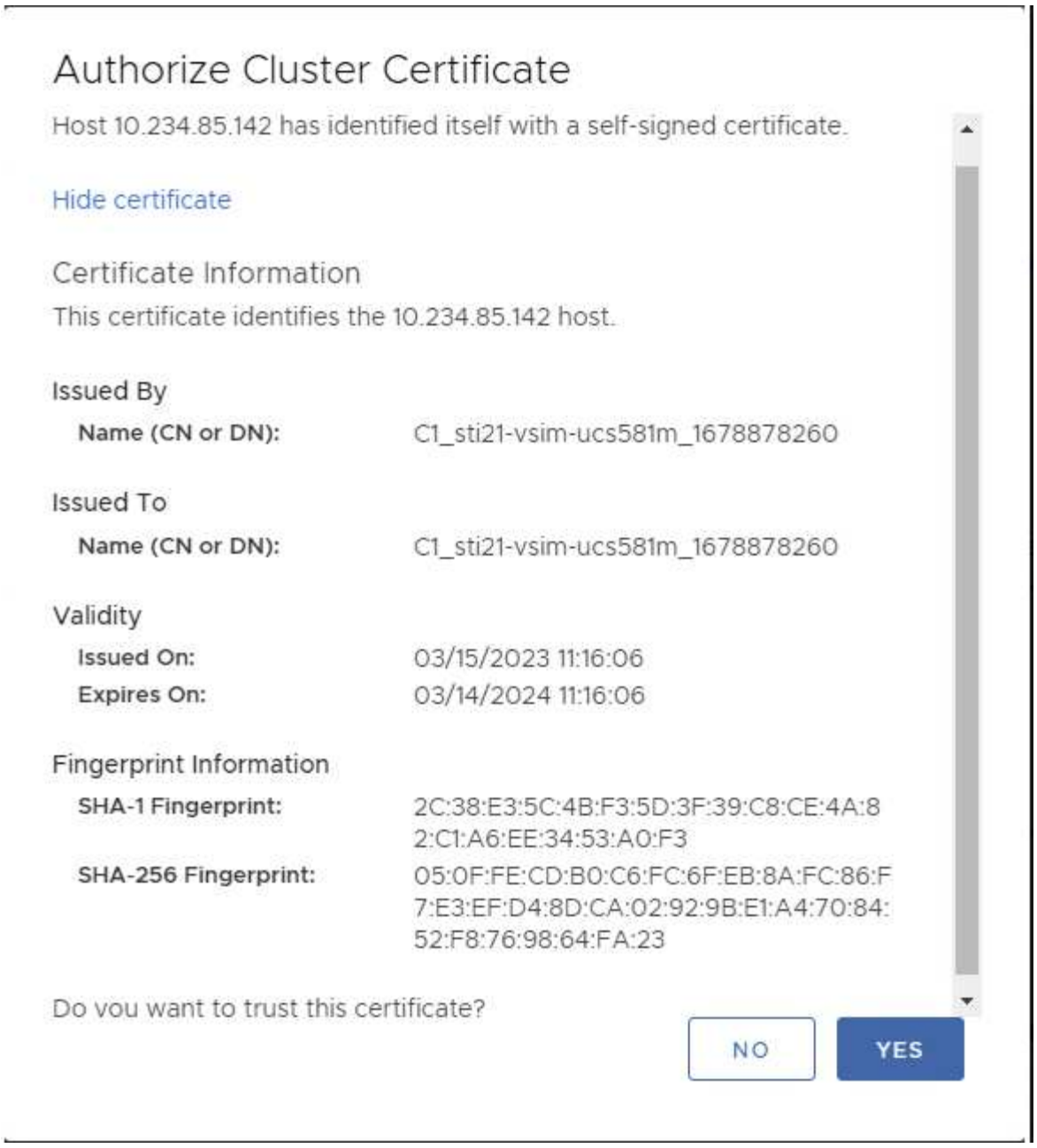
クラスタの追加

クラスタ追加のワークフロー中に、追加するクラスタがMTLSをサポートしている場合、MTLSはデフォルトで設定されます。ユーザはこの設定を行う必要はありません。次のスクリーンショットは、クラスタの追加時にユーザに表示される画面を示しています。




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

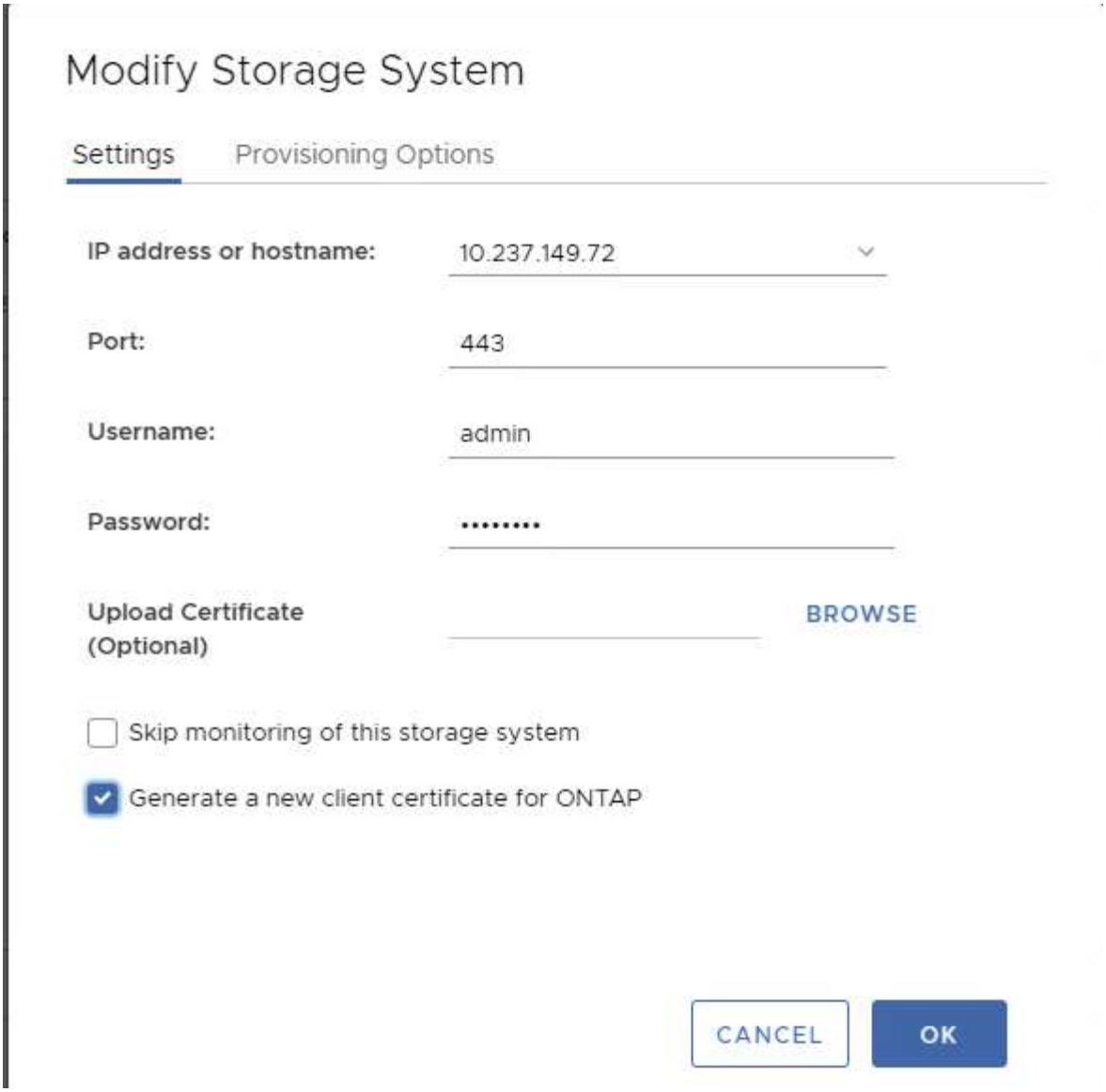

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
Authorize Cluster Certificate
Host 10.234.85.142 has identified itself with a self-signed certificate.
Show certificate
Do you want to trust this certificate?
NO
YES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

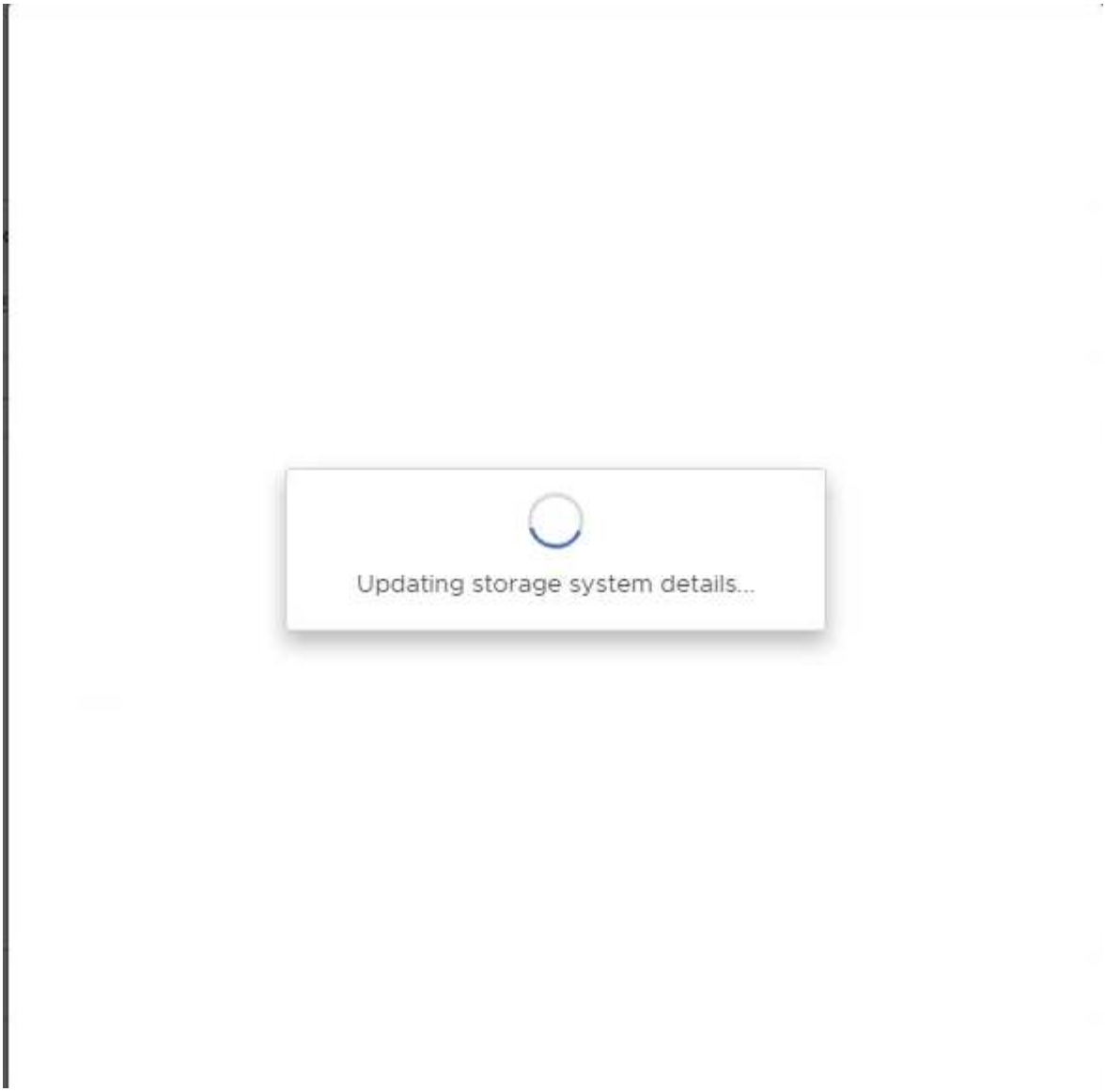


クラスタの編集

クラスタの編集処理には、次の2つのシナリオがあります。

- ONTAP証明書の有効期限が切れた場合、ユーザは新しい証明書を取得してアップロードする必要があります。
- OTV証明書の有効期限が切れた場合は、チェックボックスをオンにして証明書を再生成できます。
  - ONTAPの新しいクライアント証明書を生成します。_


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 toolsのHTTPS証明書

デフォルトでは、ONTAP toolsは、Web UIへのHTTPSアクセスを保護するために、インストール時に自動的に作成される自己署名証明書を使用します。ONTAP toolsには次の機能があります。

1. HTTPS証明書の再生成

ONTAP toolsのインストール時に、HTTPS CA証明書がインストールされ、証明書がキーストアに格納されます。ユーザは、maintコンソールを使用してHTTPS証明書を再生成することができます。

上記のオプションは、'アプリケーション設定'→'証明書の再生成'に移動することで*_maint_console*でアクセスできます。

ログインバナー

ユーザがログインプロンプトにユーザ名を入力すると、次のログインバナーが表示され

ます。SSHはデフォルトで無効になっており、VMコンソールから有効にすると1回限りのログインしか許可されないことに注意してください。

```
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.
```

ユーザが SSH チャネルを介したログインを完了すると、次のテキストが表示されます。

```
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.
```

非アクティブ時のタイムアウト

不正アクセスを防止するために、非アクティブタイムアウトが設定されます。このタイムアウトは、許可されたリソースを使用している間、一定期間非アクティブなユーザを自動的にログアウトします。これにより、許可されたユーザーのみがリソースにアクセスできるようになり、セキュリティの維持に役立ちます。

- デフォルトでは、vSphere Clientセッションはアイドル状態が120分続くと閉じます。そのため、ユーザは再度ログインしてクライアントの使用を再開する必要があります。タイムアウト値を変更するには、webclient.propertiesファイルを編集します。 vSphere Clientのタイムアウトを設定できます。 "vSphere Clientのタイムアウト値の設定"
- ONTAP toolsのWeb-CLIセッションのログアウト時間は30分です。

ユーザあたりの最大同時要求数（ネットワークセキュリティ保護::DOS攻撃）

デフォルトでは、ユーザあたりの最大同時要求数は48です。ONTAP toolsのrootユーザは、環境の要件に応じてこの値を変更できます。この値は、**DoS**攻撃に対するメカニズムを提供するため、非常に大きな値に設定しないでください。

ユーザーは、最大同時セッション数やサポートされているその他のパラメーターを*_/opt/netapp/vscserver/etc/dosfilterParams.json _*ファイルで変更できます。

フィルタを設定するには、次のパラメータを使用します。

- ***delayMs***：レート制限を超えたすべての要求が考慮されるまでの遅延（ミリ秒単位）。要求を拒否するには-1を指定します。
- ***throttlems***:セマフォの非同期待機時間
- ***maxRequestms***：この要求の実行を許可する期間。
- ***ipWhitelist***：レート制限されないIPアドレスのカンマ区切りリスト。（vCenter、ESXi、SRAのIP）
- ***maxRequestsPerSec***：1秒あたりの接続からの最大要求数。

dosfilterParamsファイルのデフォルト値:

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

ネットワークタイムプロトコル（NTP）の設定

ネットワーク時間設定の不一致が原因で、セキュリティの問題が発生する場合があります。このような問題を防ぐには、ネットワーク内のすべてのデバイスに正確な時間設定があることを確認することが重要です。

仮想アプライアンス

NTPサーバは、仮想アプライアンスのメンテナンスコンソールから設定できます。 ユーザは、*System Configuration⇒*_ Add new NTP Server_optionでNTPサーバの詳細を追加できます。

デフォルトでは、NTPのサービスはntpdです。これはレガシーサービスであり、場合によっては仮想マシンでは適切に機能しません。

* Debian *

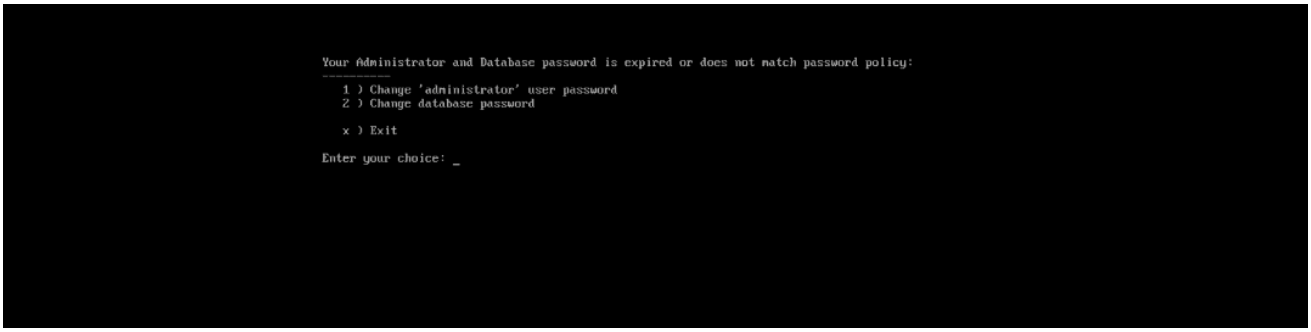
Debianでは、ユーザは/etc/ntp.confファイルにアクセスしてNTPサーバの詳細を確認できます。

パスワードポリシー

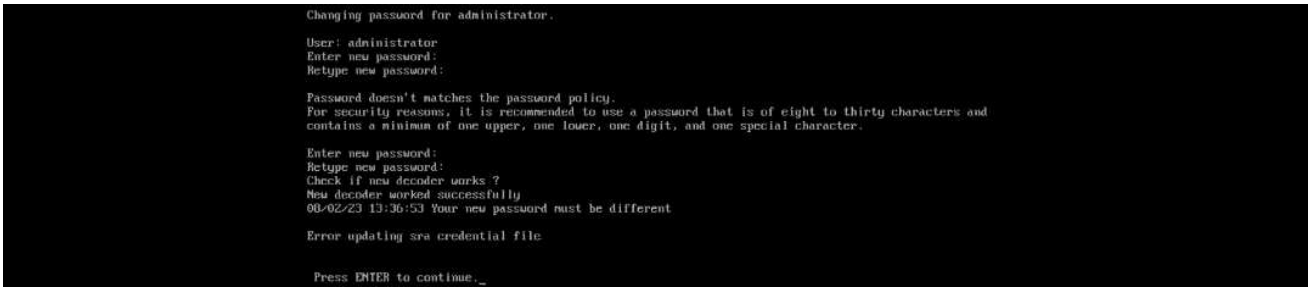
ONTAPツールを初めて導入するユーザ、またはバージョン9.12以降にアップグレードするユーザは、管理者ユーザとデータベースユーザの両方に対して、強力なパスワードポリシーに従う必要があります。導入プロセス中に、新しいユーザにパスワードの入力を求めるプロンプトが表示されます。バージョン9.12以降にアップグレードするBrownfieldユーザの場合は、メンテナンスコンソールで強力なパスワードポリシーに従うオプションを使用できます。

- ユーザがmaintコンソールにログインすると、パスワードが複雑なルールセットに照らしてチェックされ、従わなかった場合、ユーザは同じパスワードをリセットするように求められます。
- パスワードのデフォルトの有効期間は90日です。75日が経過すると、ユーザはパスワードを変更するための通知を受け取り始めます。
- サイクルごとに新しいパスワードを設定する必要があります。システムは最後のパスワードを新しいパスワードとして受け取りません。
- ユーザがmaintコンソールにログインするたびに、メインメニューをロードする前に、次のスクリーンショットのようなパスワードポリシーがチェックされます。

- パスワードポリシーまたはONTAP tools 9.11以前からのアップグレードセットアップに従っていないことが検出された場合。パスワードをリセットするための次の画面が表示されます。



- ユーザが弱いパスワードを設定しようとするか、最後のパスワードをもう一度入力すると、次のエラーが表示されます。



著作権に関する情報

商標に関する情報