Guide de renforcement de la sécurité des outils ONTAP pour VMware vSphere

Enterprise applications

NetApp
May 19, 2024

Sommaire

Guide de renforcement de la sécurité des outils ONTAP pour VMware vSphere

Guide de renforcement de la sécurité des outils ONTAP pour VMware vSphere

Le guide de renforcement de la sécurité des outils ONTAP pour VMware vSphere fournit un ensemble complet d'instructions pour configurer les paramètres les plus sécurisés.

Ces guides s'appliquent à la fois aux applications et au système d'exploitation invité de l'appliance elle-même.

Vérification de l'intégrité des outils ONTAP pour les packages d'installation VMware vSphere

Deux méthodes sont disponibles pour vérifier l'intégrité des packages d'installation des outils ONTAP.

1. Vérification des checksums
2. Vérification de la signature

Les sommes de contrôle sont fournies sur les pages de téléchargement des paquets d'installation d'OTV. Les utilisateurs doivent vérifier les sommes de contrôle des paquets téléchargés par rapport à la somme de contrôle fournie sur la page de téléchargement.

Vérification de la signature des outils ONTAP OVA

Le paquet d'installation de vApp est livré sous la forme d'une boule de commande. Ce tarball contient des certificats intermédiaires et racine pour l'appliance virtuelle, ainsi qu'un fichier README et un package OVA. Le fichier README guide les utilisateurs sur la façon de vérifier l'intégrité du progiciel VApp OVA.

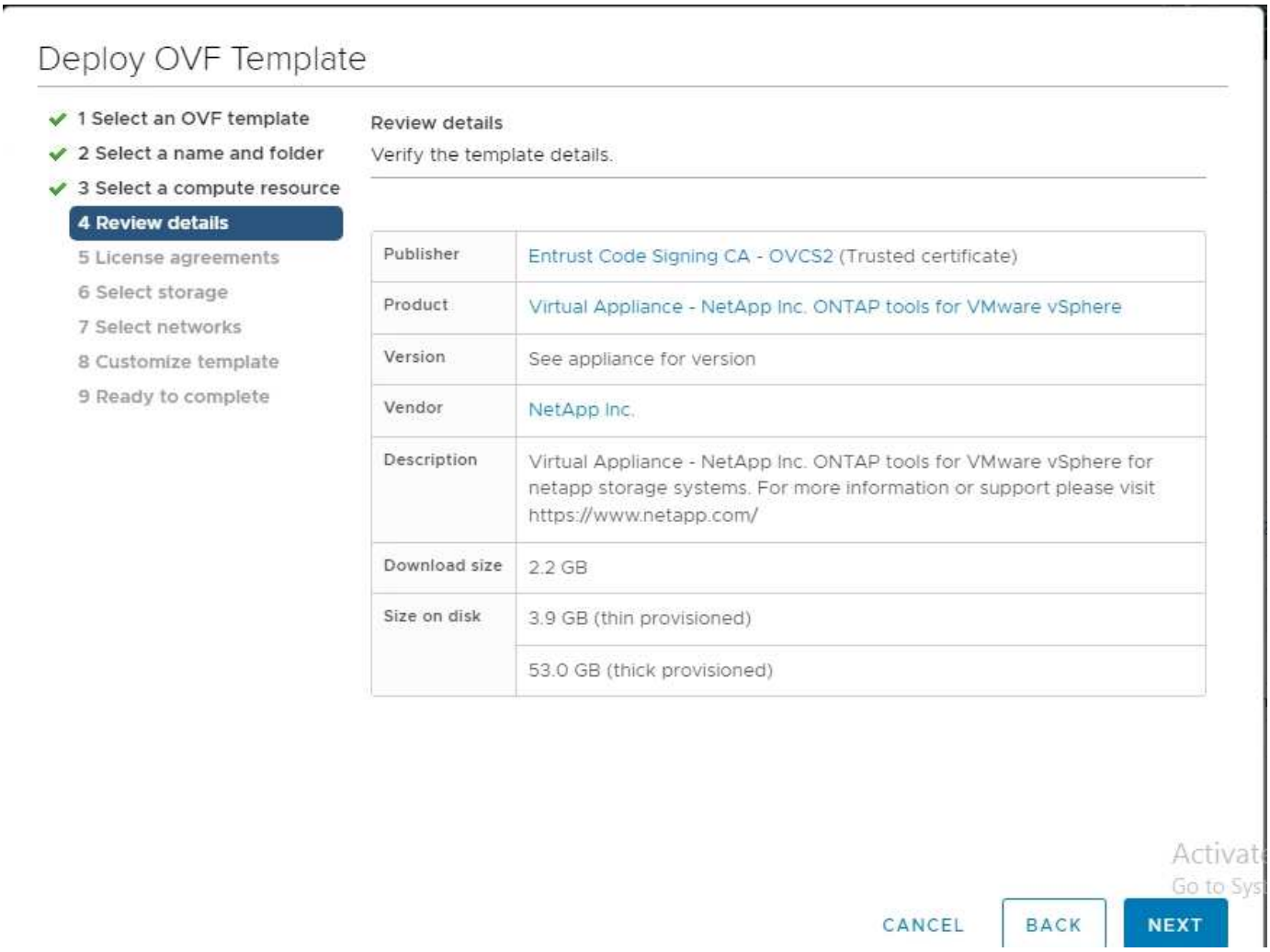
Les clients doivent également télécharger les certificats racine et intermédiaire fournis sur vCenter version 7.0U3E et ultérieure. Pour les versions vCenter comprises entre 7.0.1 et 7.0.U3E, la fonctionnalité de vérification du certificat n'est pas prise en charge par VMware. Les clients n'ont pas besoin de télécharger de certificat pour vCenter versions 6.x.

Téléchargement du certificat racine sécurisé vers vCenter

1. Connectez-vous à vCenter Server à l'aide du client VMware vSphere.
2. Spécifiez le nom d'utilisateur et le mot de passe de laman@vspher.locl ou d'un autre membre du groupe administrateurs d'authentification unique vCenter. Si vous avez spécifié un domaine différent lors de l'installation, connectez-vous en tant qu'administrateur@mondomaine.
3. Accédez à l'interface utilisateur de la gestion des certificats : a. Dans le menu Accueil, sélectionnez Administration. b. Sous certificats, cliquez sur gestion des certificats.
4. Si le système vous y invite, entrez les informations d'identification de votre serveur vCenter.
5. Sous certificats racine approuvés, cliquez sur Ajouter.
6. Cliquez sur Parcourir et sélectionnez l'emplacement du fichier .pem du certificat (OTV_OVA_INTER_ROOT_CERT_CHAIN.pem).

7. Cliquez sur Ajouter. Le certificat est ajouté au magasin.

Reportez-vous à la section "Ajoutez un certificat racine de confiance au magasin de certificats" pour en savoir plus. Lors du déploiement d'une vApp (à l'aide du fichier OVA), la signature numérique du package vApp peut être vérifiée sur la page « Review details » (vérifier les détails). Si le package vApp téléchargé est authentique, la colonne « Éditeur » affiche « certificat de confiance » (comme dans la capture d'écran suivante).



Vérification de la signature des outils ONTAP ISO et SRA tar.gz

NetApp partage son certificat de signature de code avec les clients sur la page de téléchargement du produit, ainsi que les fichiers zip du produit pour OTV-ISO et SRA.tgz.

À partir du certificat de signature de code, les utilisateurs peuvent extraire la clé publique comme suit :

```
 #> openssl x509 -in <code-sign-cert, pem file> -pubkey -noout > <public-
key name>
Ensuite, la clé publique doit être utilisée pour vérifier la signature
pour iso et tgz produit zip comme ci-dessous :
```

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

```
#> 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 et protocoles

La liste ci-dessous répertorie les ports et les protocoles requis permettant la communication entre les outils ONTAP pour le serveur VMware vSphere et d'autres entités telles que les systèmes de stockage géré, les serveurs et d'autres composants.

Ports entrants et sortants requis pour OTV

Veuillez noter le tableau ci-dessous qui répertorie les ports entrants et sortants requis pour le bon fonctionnement des outils ONTAP. Il est important de s'assurer que seuls les ports mentionnés dans le tableau sont ouverts pour les connexions à partir de machines distantes, tandis que tous les autres ports doivent être bloqués pour les connexions à partir de machines distantes. Cela permet d'assurer la sécurité de votre système.

Le tableau suivant décrit les détails du port ouvert.

Port TCP v4/v6 #	Direction	Fonction
8143	entrant	Connexions HTTPS pour l'API REST
8043	entrant	Connexions HTTPS
9060	entrant	Connexions HTTPS Utilisé pour les connexions SOAP sur HTTPS Ce port doit être ouvert pour permettre à un client de se connecter au serveur d'API des outils ONTAP.
22	entrant	SSH (désactivé par défaut)
9080	entrant	Connexions HTTPS - VP et SRA - connexions internes à partir du bouclage uniquement
9083	entrant	Connexions HTTPS - VP et SRA Utilisé pour les connexions SOAP sur HTTPS
1162	entrant	Paquets de déroutement SNMP VP
8443	entrant	Plug-in distant

Port TCP v4/v6 #	Direction	Fonction
1527	diffusion interne uniquement	Port de base de données Derby, uniquement entre cet ordinateur et lui-même, connexions externes non acceptées — connexions internes uniquement
8150	diffusion interne uniquement	Le service d'intégrité des journaux s'exécute sur le port
443	bidirectionnel	Utilisé pour les connexions aux clusters ONTAP

Contrôle de l'accès à distance à la base de données Derby

Les administrateurs peuvent accéder à la base de données derby à l'aide des commandes suivantes. Il est accessible via la machine virtuelle locale des outils ONTAP ainsi qu'un serveur distant en procédant comme suit :

```
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>';
```

exemple:

```
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                      |
```

Outils ONTAP pour les points d'accès VMware vSphere (utilisateurs)

L'installation des outils ONTAP pour VMware vSphere crée et utilise trois types d'utilisateurs :

1. Utilisateur système : compte utilisateur root
2. Utilisateur de l'application : l'utilisateur administrateur, l'utilisateur maint et les comptes utilisateur db
3. Utilisateur de support : compte utilisateur diag

1. Utilisateur du système

L'utilisateur System(root) est créé par l'installation des outils ONTAP sur le système d'exploitation sous-jacent (Debian).

- Un utilisateur système par défaut "root" est créé sur Debian par l'installation des outils ONTAP. Sa valeur par défaut est désactivée et peut être activée ad hoc via la console « maint ».

2. Utilisateur de l'application

L'utilisateur de l'application est nommé en tant qu'utilisateur local dans les outils ONTAP. Il s'agit d'utilisateurs créés dans l'application Outils ONTAP. Le tableau ci-dessous répertorie les types d'utilisateurs d'applications :

Utilisateur	Description
Utilisateur administrateur	Il est créé lors de l'installation des outils ONTAP et l'utilisateur fournit les informations d'identification lors du déploiement des outils ONTAP. Les utilisateurs ont la possibilité de modifier le mot de passe dans la console « maint ». Le mot de passe expirera dans 90 jours et les utilisateurs devraient changer de mot de passe.
Utilisateur de maintenance	Il est créé lors de l'installation des outils ONTAP et l'utilisateur fournit les informations d'identification lors du déploiement des outils ONTAP. Les utilisateurs ont la possibilité de modifier le mot de passe dans la console « maint ». Il s'agit d'un utilisateur de maintenance créé pour exécuter les opérations de la console de maintenance.
Utilisateur de la base de données	Il est créé lors de l'installation des outils ONTAP et l'utilisateur fournit les informations d'identification lors du déploiement des outils ONTAP. Les utilisateurs ont la possibilité de modifier le mot de passe dans la console « maint ». Le mot de passe expirera dans 90 jours et les utilisateurs devraient changer de mot de passe.

3. Support user(diag user)

Lors de l'installation des outils ONTAP, un utilisateur du support est créé. Cet utilisateur peut accéder aux outils ONTAP en cas de problème ou de panne du serveur et collecter les journaux. Par défaut, cet utilisateur est désactivé, mais il peut être activé sur une base ad hoc via la console « maint ». Il est important de noter que cet utilisateur sera automatiquement désactivé après une certaine période.

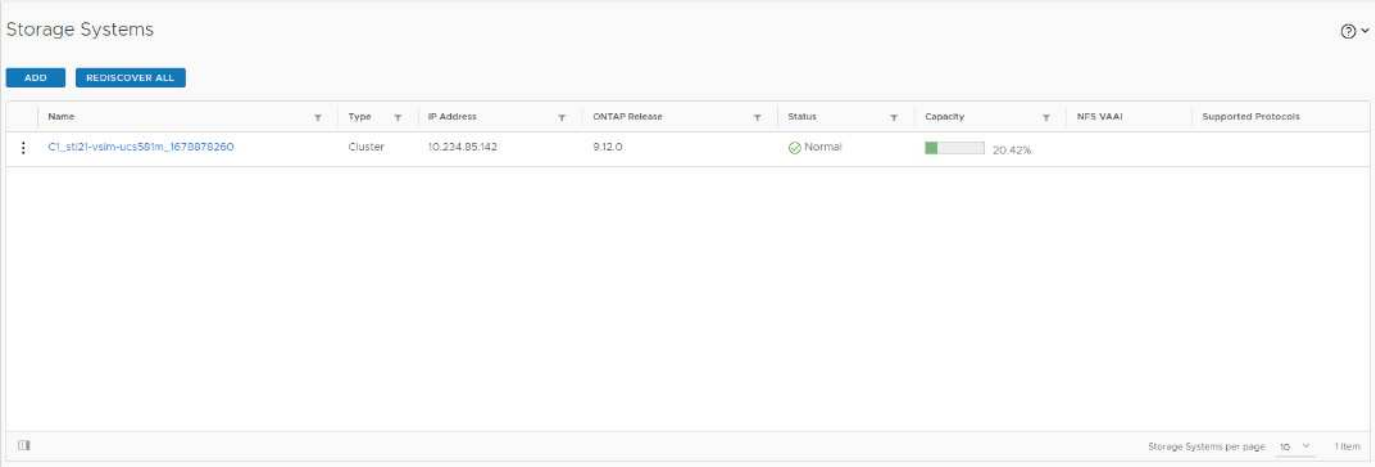
Authentification mutuelle TLS (basée sur un certificat)

Les versions 9.7 et ultérieures de ONTAP prennent en charge les communications TLS mutuelles. Depuis les outils ONTAP pour VMware et vSphere 9.12, le protocole TLS mutuel est utilisé pour la communication avec les nouveaux clusters ajoutés (selon la version de ONTAP).

ONTAP

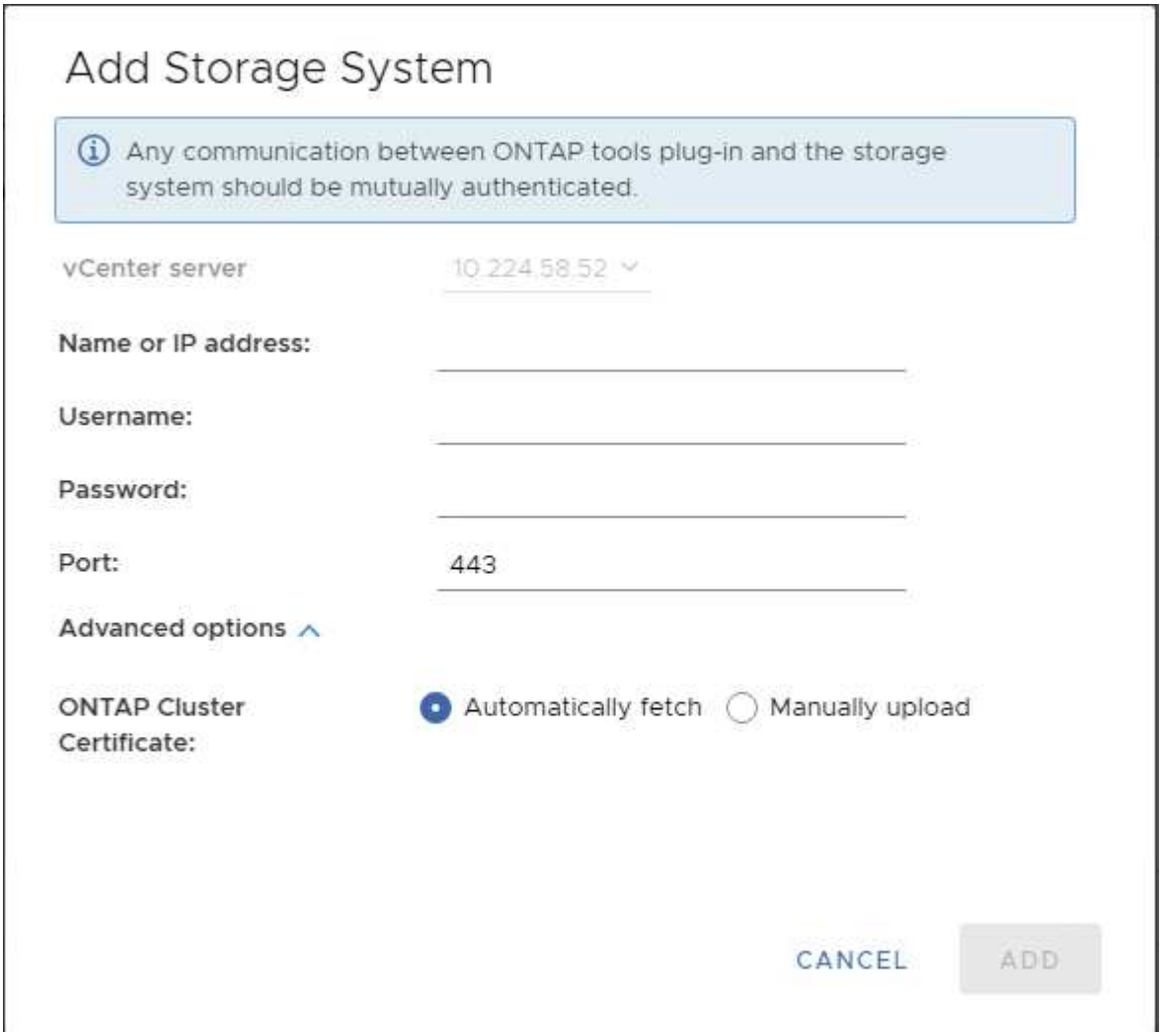
Pour tous les systèmes de stockage précédemment ajoutés : lors d'une mise à niveau, tous les systèmes de stockage ajoutés font l'objet d'une fiabilité automatique et les mécanismes d'authentification basés sur des certificats sont configurés.

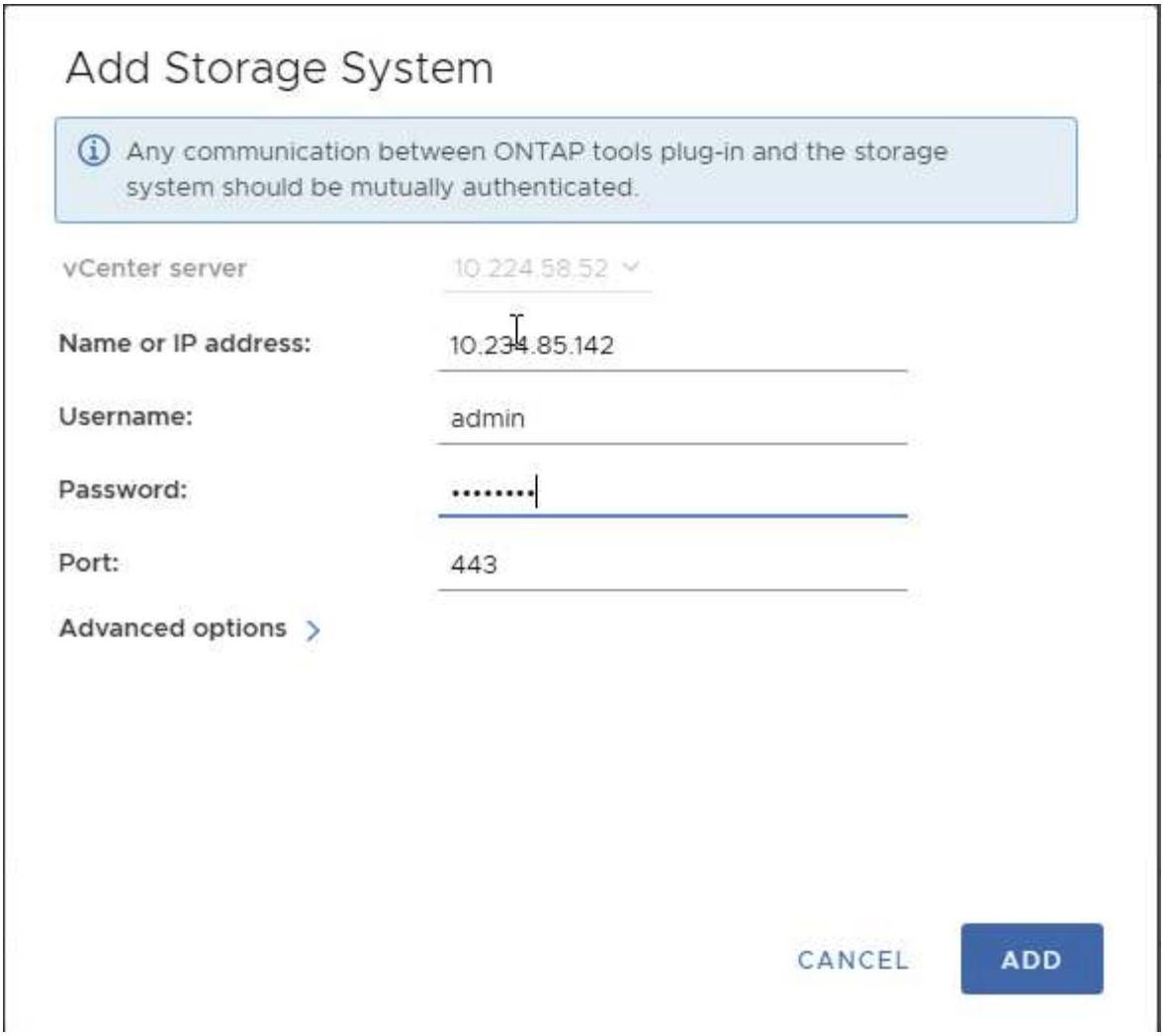
Comme dans la capture d'écran ci-dessous, la page de configuration du cluster affiche l'état d'authentification mutuelle TLS (Certificate Based Authentication), configurée pour chaque cluster.

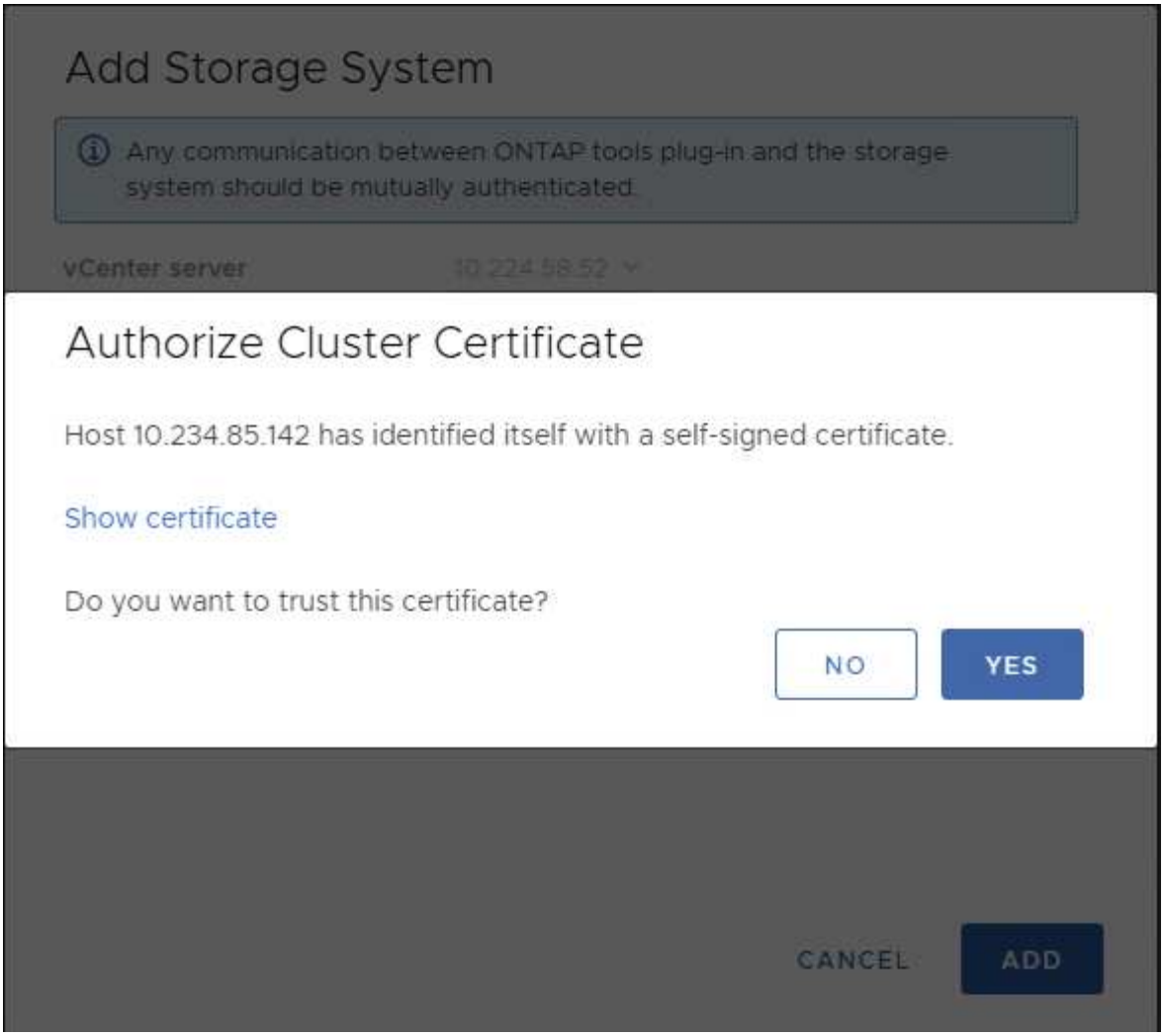


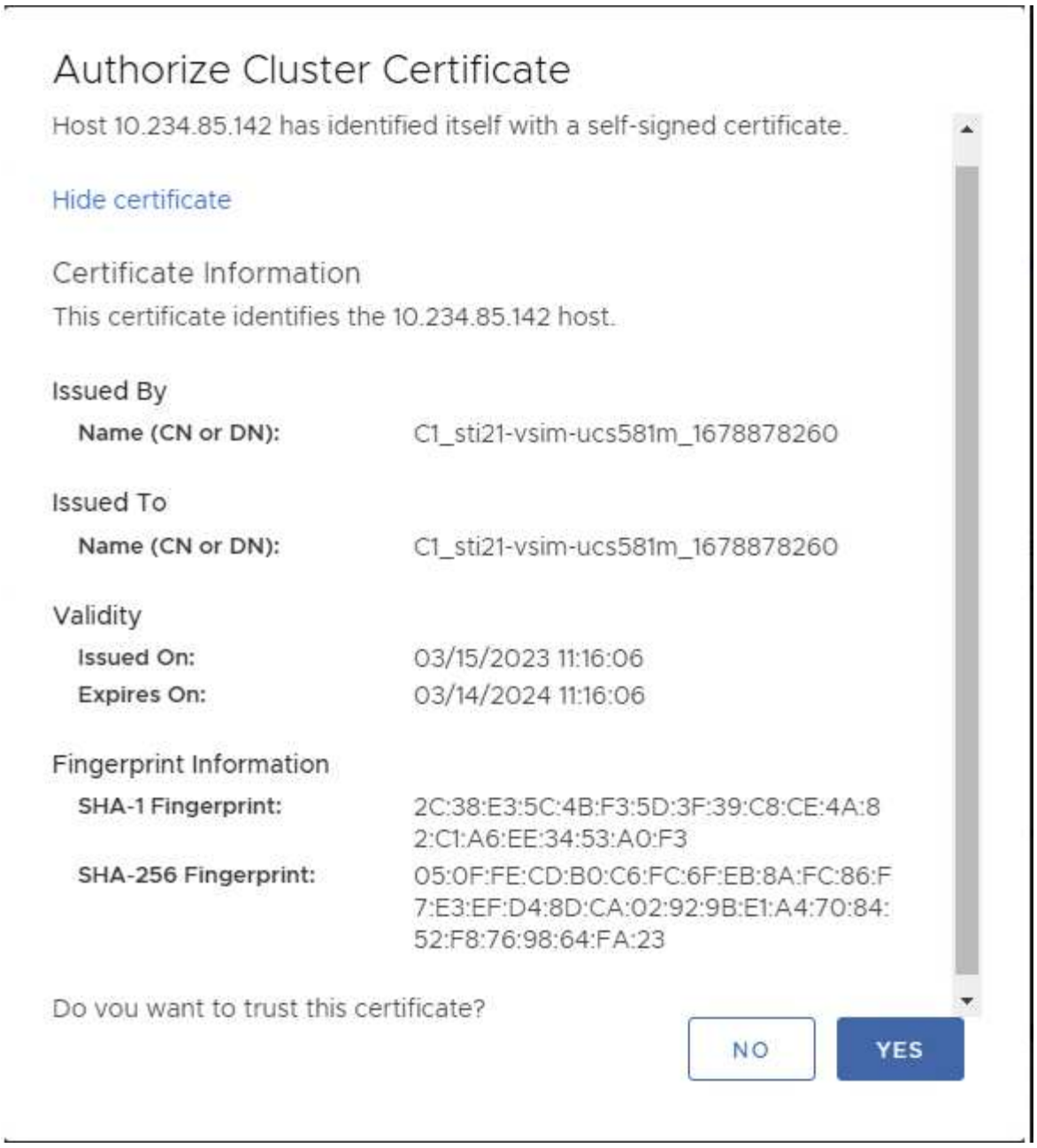
Cluster Add

Lors du workflow d'ajout de cluster, si le cluster ajouté prend en charge MTLS, MTLS sera configuré par défaut. L'utilisateur n'a pas besoin d'effectuer de configuration pour cela. La capture d'écran ci-dessous présente l'écran présenté à l'utilisateur lors de l'ajout d'un 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

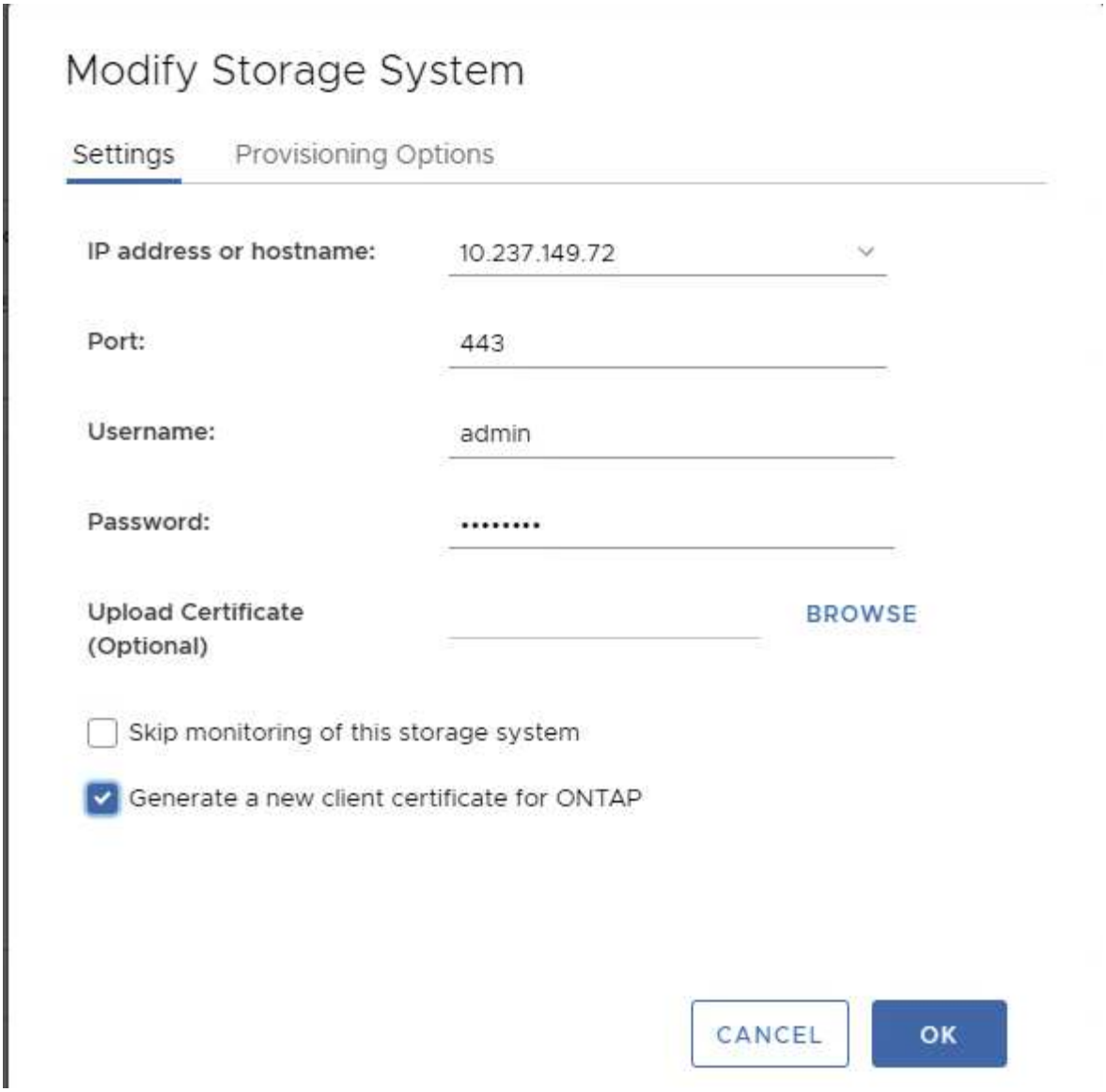

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
Authorize Cluster Certificate
Host 10.234.85.142 has identified itself with a self-signed certificate.
Show certificate
Do you want to trust this certificate?
NO
YES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

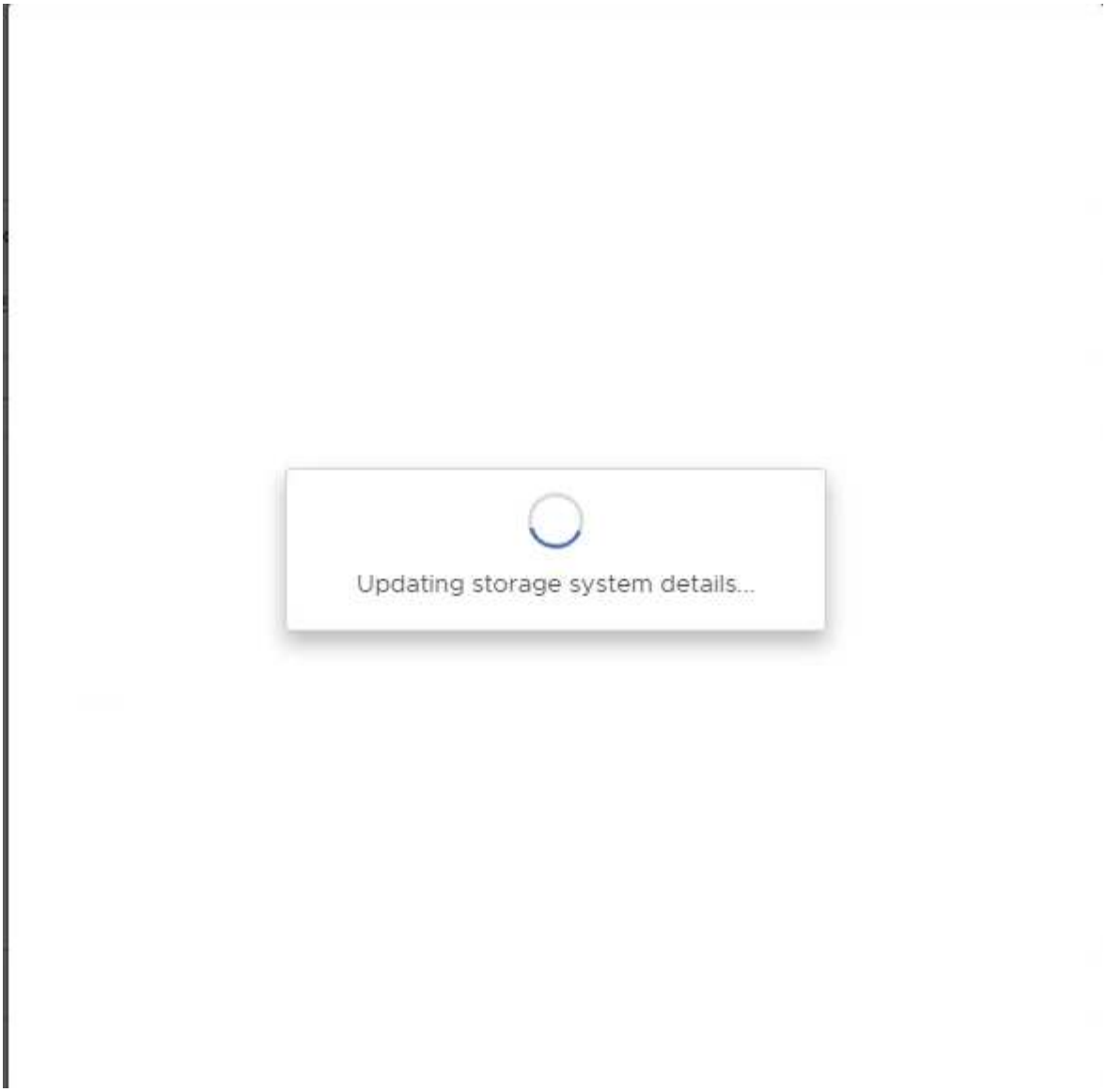


Modification du cluster

Lors de l'opération d'édition de cluster, il existe deux scénarios :

- Si le certificat ONTAP expire, l'utilisateur devra obtenir le nouveau certificat et le télécharger.
- Si le certificat OTV expire, l'utilisateur peut le régénérer en cochant la case.
  - *Générer un nouveau certificat client pour 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



Certificat HTTPS des outils ONTAP

Par défaut, les outils ONTAP utilisent un certificat auto-signé automatiquement créé lors de l'installation pour sécuriser l'accès HTTPS à l'interface utilisateur Web. Les outils ONTAP offrent les fonctionnalités suivantes :

1. Régénérer le certificat HTTPS

Lors de l'installation des outils ONTAP, un certificat d'autorité de certification HTTPS est installé et le certificat est stocké dans le magasin de clés. L'utilisateur a la possibilité de régénérer le certificat HTTPS via la console maint.

Les options ci-dessus sont accessibles dans *maint* console en accédant à *'Configuration de l'application'* → *'régénérer les certificats'.*

Bannière de connexion

La bannière de connexion suivante s'affiche lorsque l'utilisateur saisit un nom d'utilisateur

dans l'invite de connexion. Notez que SSH est désactivé par défaut et n'autorise que les connexions uniques lorsqu'elles sont activées à partir de la console de la machine virtuelle.

```
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.
```

Une fois que l'utilisateur a terminé sa connexion via le canal SSH, le texte suivant s'affiche :

```
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.
```

Délai d'inactivité

Pour empêcher tout accès non autorisé, un délai d'inactivité est défini, ce qui déconnecte automatiquement les utilisateurs inactifs pendant une certaine période pendant l'utilisation des ressources autorisées. Cela permet de garantir que seuls les utilisateurs autorisés peuvent accéder aux ressources et contribue à maintenir la sécurité.

- Par défaut, les sessions du client vSphere se ferment après 120 minutes d'inactivité, ce qui oblige l'utilisateur à se reconnecter pour reprendre à l'aide du client. Vous pouvez modifier la valeur du délai d'attente en modifiant le fichier webclient.properties. Vous pouvez configurer le délai d'expiration du client vSphere "Configurez la valeur du délai d'expiration du client vSphere"
- Les outils ONTAP ont un délai de déconnexion de session de l'interface de ligne de commande Web de 30 minutes.

Nombre maximal de requêtes simultanées par utilisateur (protection de sécurité réseau :: Attaque DOS)

Par défaut, le nombre maximal de requêtes simultanées par utilisateur est de 48. L'utilisateur root des outils ONTAP peut modifier cette valeur en fonction des besoins de son environnement. **Cette valeur ne doit pas être définie sur une valeur très élevée car cela fournit un mécanisme contre les attaques par déni de service (DOS).**

Les utilisateurs peuvent modifier le nombre maximal de sessions simultanées et d'autres paramètres pris en charge dans le fichier ***/opt/netapp/vscserver/etc/dofilterParams.json***.

Nous pouvons configurer le filtre en utilisant les paramètres suivants :

- ***delayMS***: Le délai en millisecondes donné à toutes les demandes au-delà de la limite de taux avant qu'elles ne soient prises en compte. Donnez -1 pour rejeter simplement la demande.
- ***étrangletMs***: Combien de temps pour attendre le sémaphore en mode asynchrone.
- ***maxRequestMS*** : durée d'exécution de cette requête.
- ***ipWhitelist***: Une liste d'adresses IP séparées par des virgules qui ne seront pas à débit limité. (Il peut s'agir d'adresses IP vCenter, ESXi et SRA)
- ***maxRequestsPerSec*** : nombre maximal de requêtes provenant d'une connexion par seconde.

Valeurs par défaut dans le fichier *dofilterParams*:

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

Configuration du protocole NTP (Network Time Protocol)

Des problèmes de sécurité peuvent parfois se produire en raison de différences dans les configurations de l'heure du réseau. Il est important de s'assurer que tous les périphériques d'un réseau disposent de paramètres d'heure précis pour éviter de tels problèmes.

Appareil virtuel

Vous pouvez configurer le ou les serveurs NTP à partir de la console de maintenance de l'appliance virtuelle. Les utilisateurs peuvent ajouter les détails du serveur NTP sous *System Configuration* ⇒ *Add New NTP Server* option

Par défaut, le service NTP est ntpd. Il s'agit d'un service hérité qui ne fonctionne pas bien pour les machines virtuelles dans certains cas.

Debian

Sous Debian, l'utilisateur peut accéder au fichier /etc/ntp.conf pour obtenir des détails sur le serveur ntp.

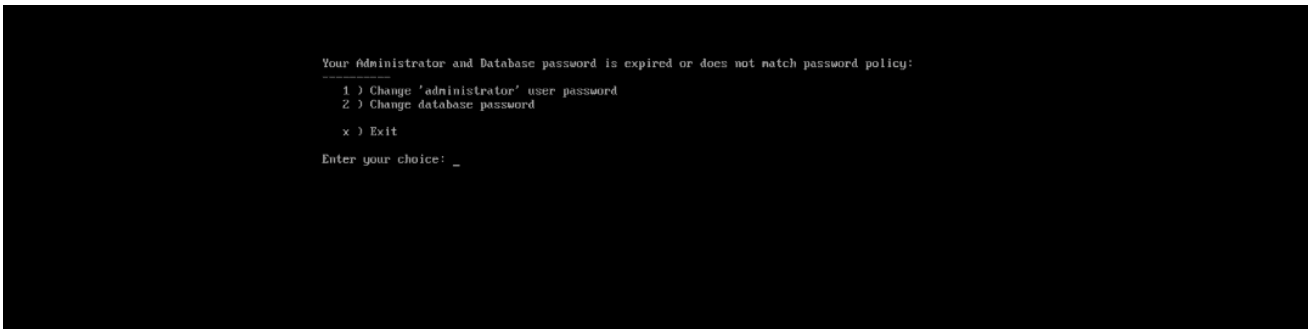
Stratégies de mot de passe

Les utilisateurs qui déploient des outils ONTAP pour la première fois ou qui effectuent une mise à niveau vers la version 9.12 ou ultérieure devront suivre la stratégie de mot de passe robuste pour l'administrateur et les utilisateurs de base de données. Au cours du processus de déploiement, les nouveaux utilisateurs seront invités à entrer leurs mots de

passe. Pour les utilisateurs de brownfield qui effectuent une mise à niveau vers la version 9.12 ou ultérieure, l'option de suivre la stratégie de mot de passe fort sera disponible dans la console de maintenance.

- Une fois que l'utilisateur se connecte à la console maint, les mots de passe sont vérifiés par rapport au jeu de règles complexes et s'il n'est pas suivi, l'utilisateur est invité à les réinitialiser.
- La validité par défaut du mot de passe est de 90 jours et après 75 jours, l'utilisateur commence à recevoir la notification de modification du mot de passe.
- Il est nécessaire de définir un nouveau mot de passe à chaque cycle, le système ne prendra pas le dernier mot de passe comme nouveau mot de passe.
- Chaque fois qu'un utilisateur se connecte à la console maint, il vérifie les stratégies de mot de passe comme les captures d'écran ci-dessous avant de charger le menu principal :

- S'il n'est pas trouvé en suivant la stratégie de mot de passe ou sa configuration de mise à niveau à partir des outils ONTAP 9.11 ou antérieurs. L'utilisateur verra alors l'écran suivant pour réinitialiser le mot de passe :



- Si l'utilisateur tente de définir un mot de passe faible ou donne à nouveau le dernier mot de passe, l'erreur suivante s'affiche :