适用于VMware vSphere的ONTAP工具安全强化指南

Enterprise applications

NetApp
May 19, 2024

目录

适用于VMware vSphere的ONTAP工具安全强化指南

适用于VMware vSphere的ONTAP工具安全强化指南

适用于VMware vSphere的ONTAP工具的安全强化指南提供了一套全面的说明、用于配置最安全的设置。

这些指南适用于设备本身的应用程序和子操作系统。

验证适用于VMware vSphere的ONTAP工具安装包的完整性

客户可以通过两种方法验证其ONTAP工具安装包的完整性。

1. 验证校验和
2. 验证签名

OTV安装包的下载页面上提供了校验和。用户必须根据下载页面上提供的校验和验证已下载软件包的校验和。

验证ONTAP工具OVA的签名

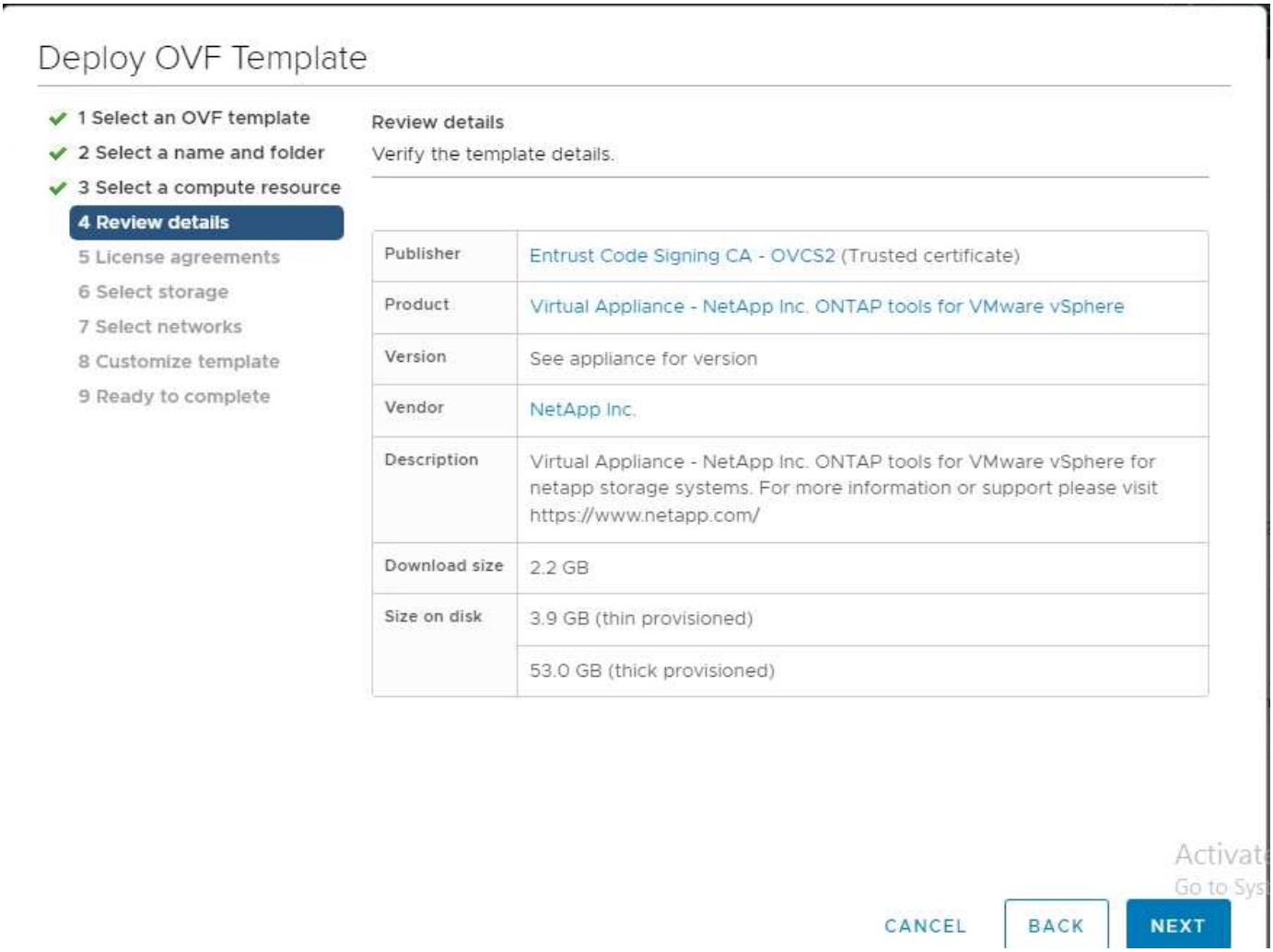
vapp安装包以tarball的形式提供。此tarball包含虚拟设备的中间证书和根证书、以及自述文件和OVA软件包。README文件可指导用户如何验证vapp OVA软件包的完整性。

客户还必须上传vCenter 7.0U3和更高版本上提供的根证书和中间证书。 对于7.0.1和7.0.U三e之间的vCenter版本、VMware不支持验证证书的功能。客户不需要上传vCenter 6.x的任何证书

将可信根证书上传到**vCenter**

1. 使用VMware vSphere Client登录到vCenter Server。
2. 为administrator@vsphere.local或vCenter Single Sign-On Administrators组的其他成员指定用户名和密码。如果您在安装期间指定了其他域、请以管理员身份@mydomain登录。
3. 导航到证书管理用户界面：a.从主菜单中、选择管理。B在"证书"下、单击"证书管理"。
4. 如果系统提示您、请输入vCenter Server的凭据。
5. 在可信根证书下、单击添加。
6. 单击浏览并选择证书.prom文件(OTV_OVA_inter_root_CERT_chain.prom)的位置。
7. 单击添加。此时、证书将添加到存储中。

请参见 "将可信根证书添加到证书存储" 有关详细信息 …在部署vapp时(使用OVA文件)、可以在"查看详细信息"页面上验证vapp包的数字签名。如果下载的vapp软件包为正版、"发布者"列将显示"可信证书"(如以下屏幕截图所示)。



验证ONTAP工具ISO和SRA tar.gz的签名

NetApp会在产品下载页面上与客户共享其代码签名证书、以及OTV-ISO和sra.tgz的产品zip文件。

用户可以从代码签名证书中提取公共密钥、如下所示：

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

然后，应使用公共密钥验证ISO和tgz产品zip的签名，如下所示：

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

示例

```
#> 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
```

端口和协议

此处列出的是支持在适用于VMware vSphere服务器的ONTAP工具与其他实体(如受管存储系统、服务器和其他组件)之间进行通信所需的端口和协议。

OTV需要入站和出站端口

请注意下表、其中列出了ONTAP工具正常运行所需的入站和出站端口。请务必确保仅为远程计算机的连接打开表中提到的端口、而为远程计算机的连接应阻止所有其他端口。这将有助于确保系统的安全性和安全性。

下表介绍了打开的端口详细信息。

TCP v4/v6端口#	* 方向 *	函数
8143.	入站	用于 REST API 的 HTTPS 连接
8043	入站	HTTPS 连接
9060	入站	HTTPS连接+ 用于基于HTTPS的SOAP连接+ 必须打开此端口、客户端才能连接到ONTAP工具API服务器。
22.	入站	SSH （默认为禁用）
9080	入站	HTTPS 连接— VP 和 SRA —仅从环回进行内部连接
9083.	入站	HTTPS连接- VP和SRA 用于基于HTTPS的SOAP连接
1162.	入站	VP SNMP 陷阱数据包
8443	入站	远程插件
1527.	仅限内部	Derby数据库端口、仅在此计算机与自身之间、不接受外部连接—仅限内部连接
8150	仅限内部	日志完整性服务在端口上运行
443.	双向	用于连接到 ONTAP 集群

控制对Derby数据库的远程访问

管理员可以使用以下命令访问derby数据库。可通过ONTAP工具本地VM和远程服务器通过以下步骤访问它：

```
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>';
```

示例：

```
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                       |
```

适用于VMware vSphere访问点(用户)的ONTAP工具

适用于VMware vSphere的ONTAP工具安装会创建和使用三种类型的用户：

1. System User：root用户帐户
2. 应用程序用户：管理员用户、maintuser和数据库用户帐户
3. 支持用户：diag用户帐户

1.系统用户

system(root)用户是通过在底层操作系统(DeBM)上安装ONTAP工具来创建的。

- 默认系统用户"root"是通过安装ONTAP工具在Debian上创建的。其默认值为禁用、可通过"aint"控制台临时启用。

2.应用程序用户

应用程序用户在ONTAP工具中命名为本地用户。这些用户是在ONTAP工具应用程序中创建的。下表列出了应用程序用户的类型：

* 用户 *	* 问题描述 *
管理员用户	它是在ONTAP工具安装期间创建的、用户在部署ONTAP工具时提供凭据。用户可以选择在"aint"控制台中更改密码。密码将在90天后过期、用户应更改此密码。
维护用户	它是在ONTAP工具安装期间创建的、用户在部署ONTAP工具时提供凭据。用户可以选择在"aint"控制台中更改密码。此用户为维护用户、创建此用户名是为了执行维护控制台操作。

* 用户 *	* 问题描述 *
数据库用户	它是在ONTAP工具安装期间创建的、用户在部署ONTAP工具时提供凭据。用户可以选择在"aint"控制台中更改密码。密码将在90天后过期、用户应更改此密码。

3.支持用户(diag用户)

在ONTAP工具安装期间、系统会创建一个支持用户。此用户可用于在服务器发生任何问题描述或中断时访问ONTAP工具并收集日志。默认情况下、此用户处于禁用状态、但可以通过"aint"控制台临时启用。需要注意的是、此用户将在特定时间段后自动禁用。

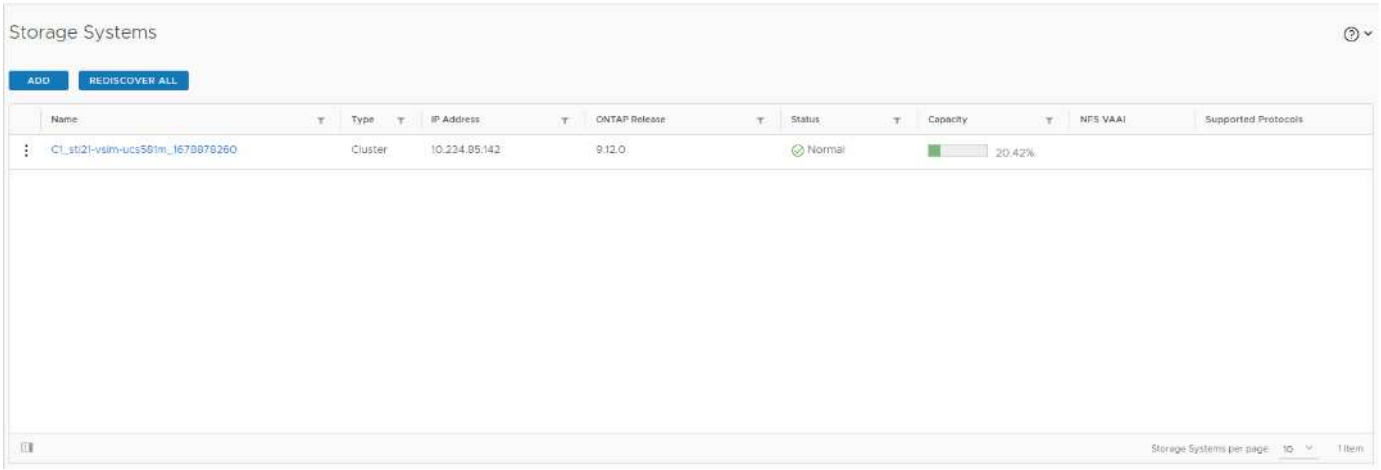
相互TLS (基于证书的身份验证)

ONTAP 9.7及更高版本支持相互TLS通信。从适用于VMware和vSphere 9.12的ONTAP工具开始、可使用相互TLS与新添加的集群进行通信(具体取决于ONTAP版本)。

ONTAP

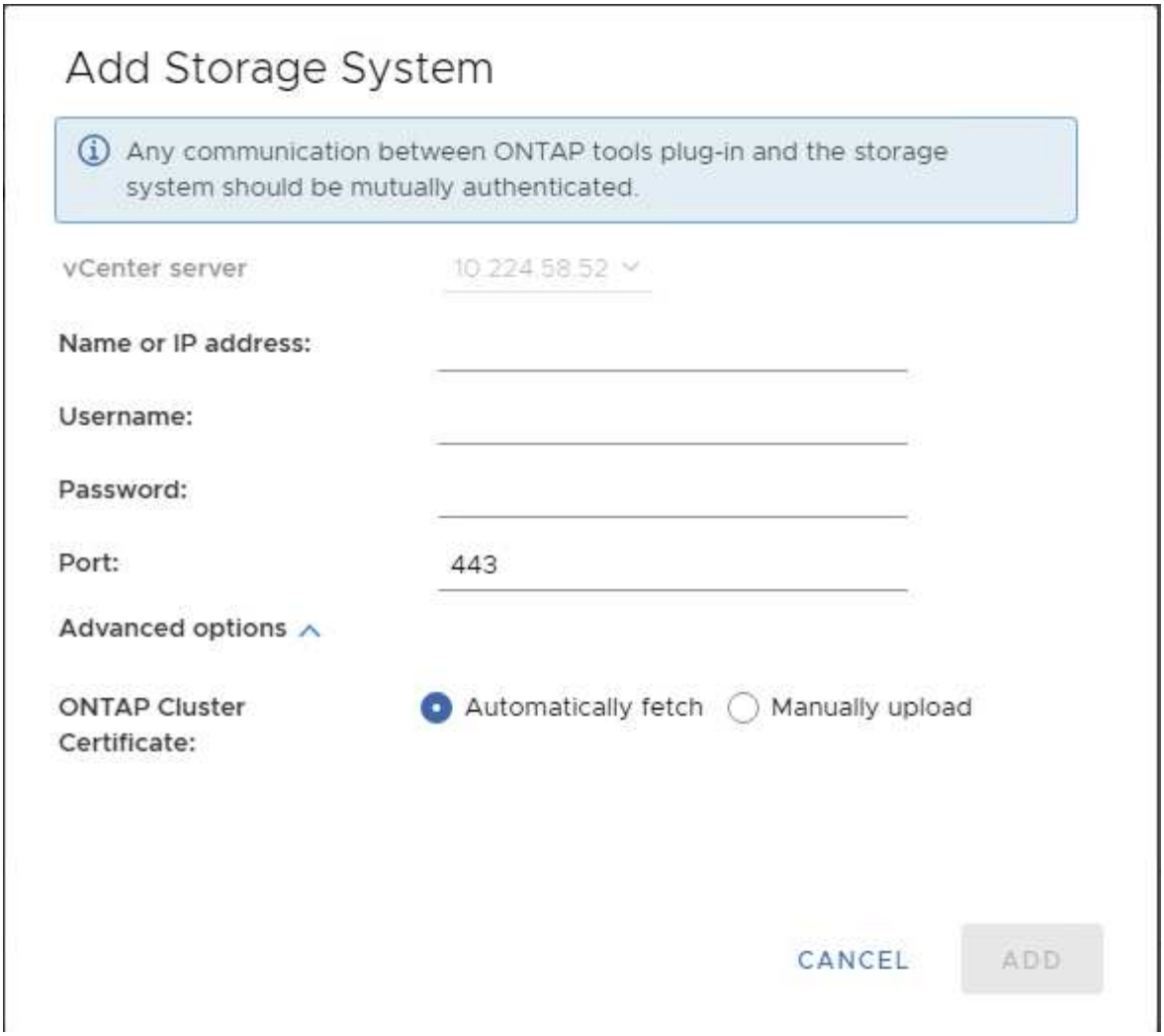
对于先前添加的所有存储系统：在升级期间、所有添加的存储系统都将获得自动信任、并配置基于证书的身份验证机制。

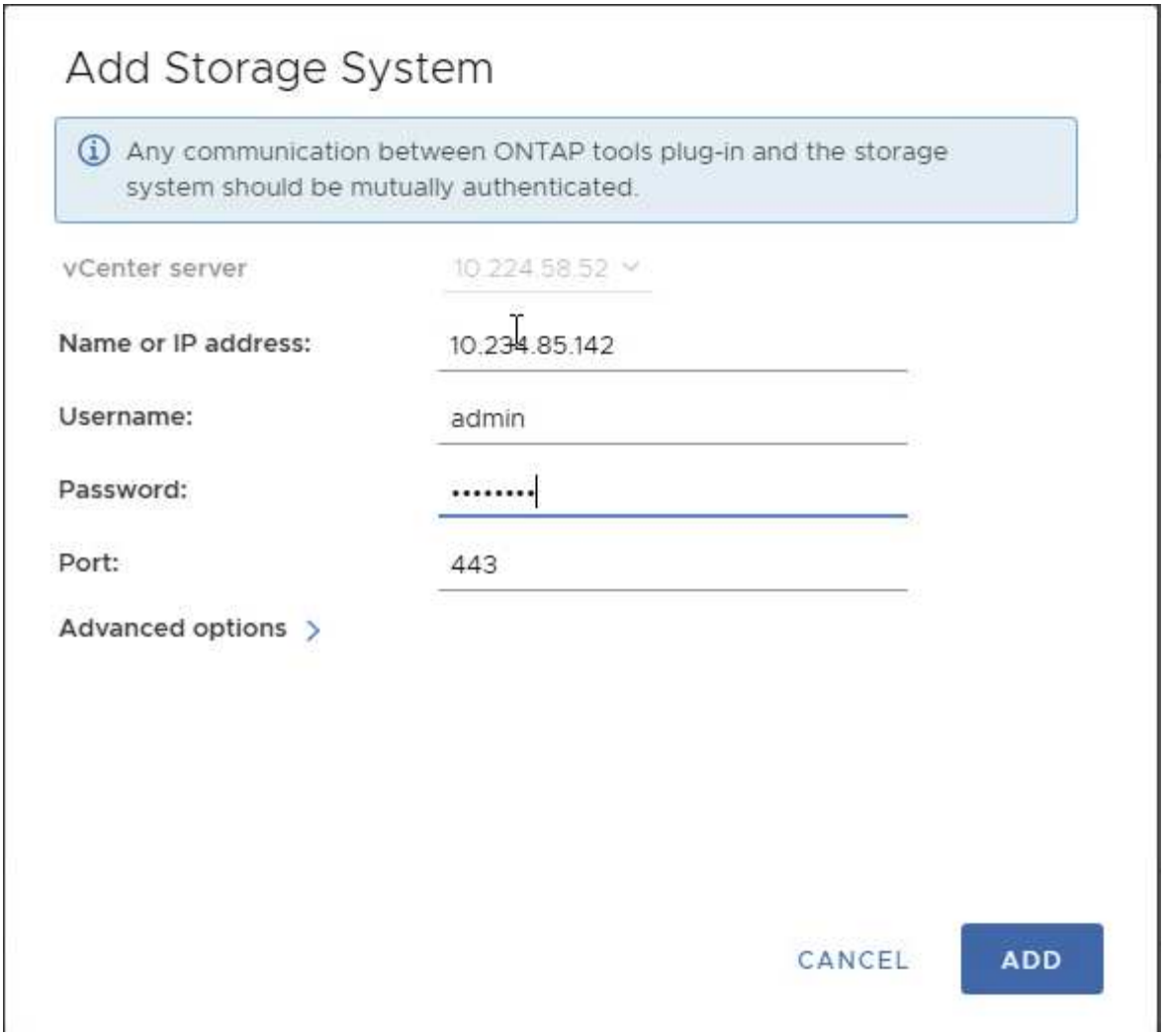
如以下屏幕截图所示、集群设置页面将显示为每个集群配置的相互TLS (基于证书的身份验证)的状态。

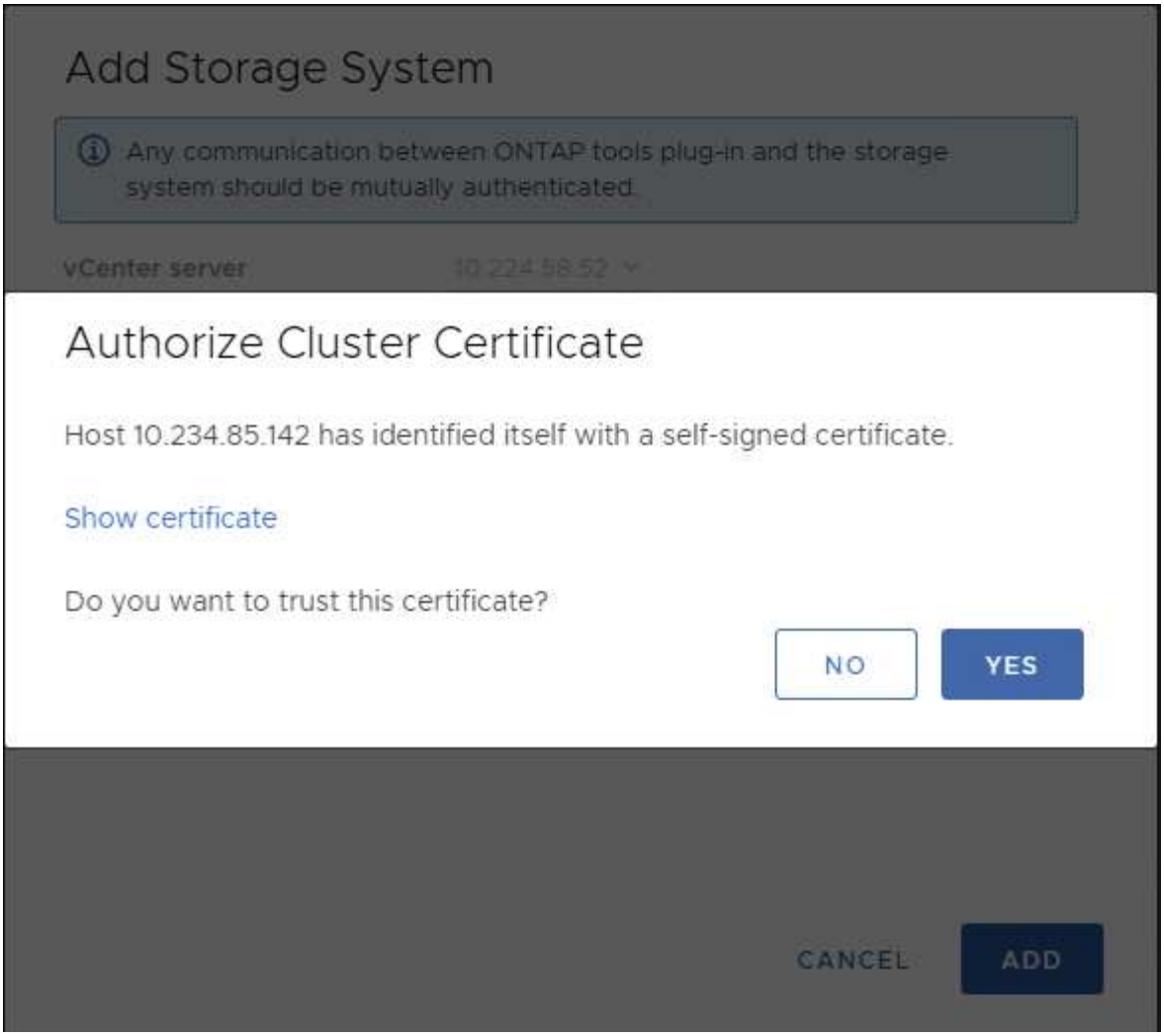


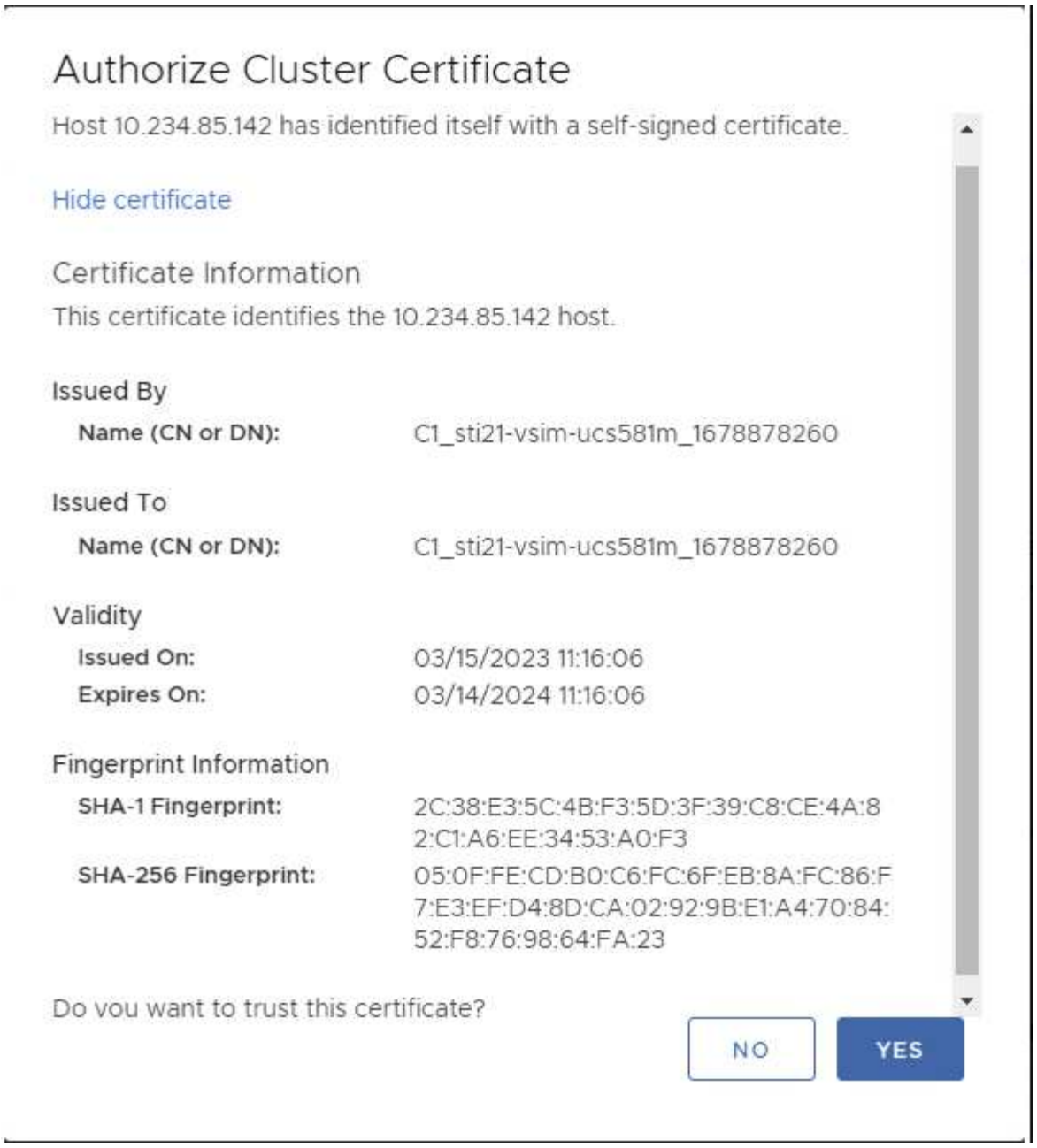
集群添加

在集群添加工作流期间、如果要添加的集群支持MTLS、则默认情况下会配置MTLS。用户无需为此执行任何配置。以下屏幕截图显示了在添加集群期间向用户显示的屏幕。


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

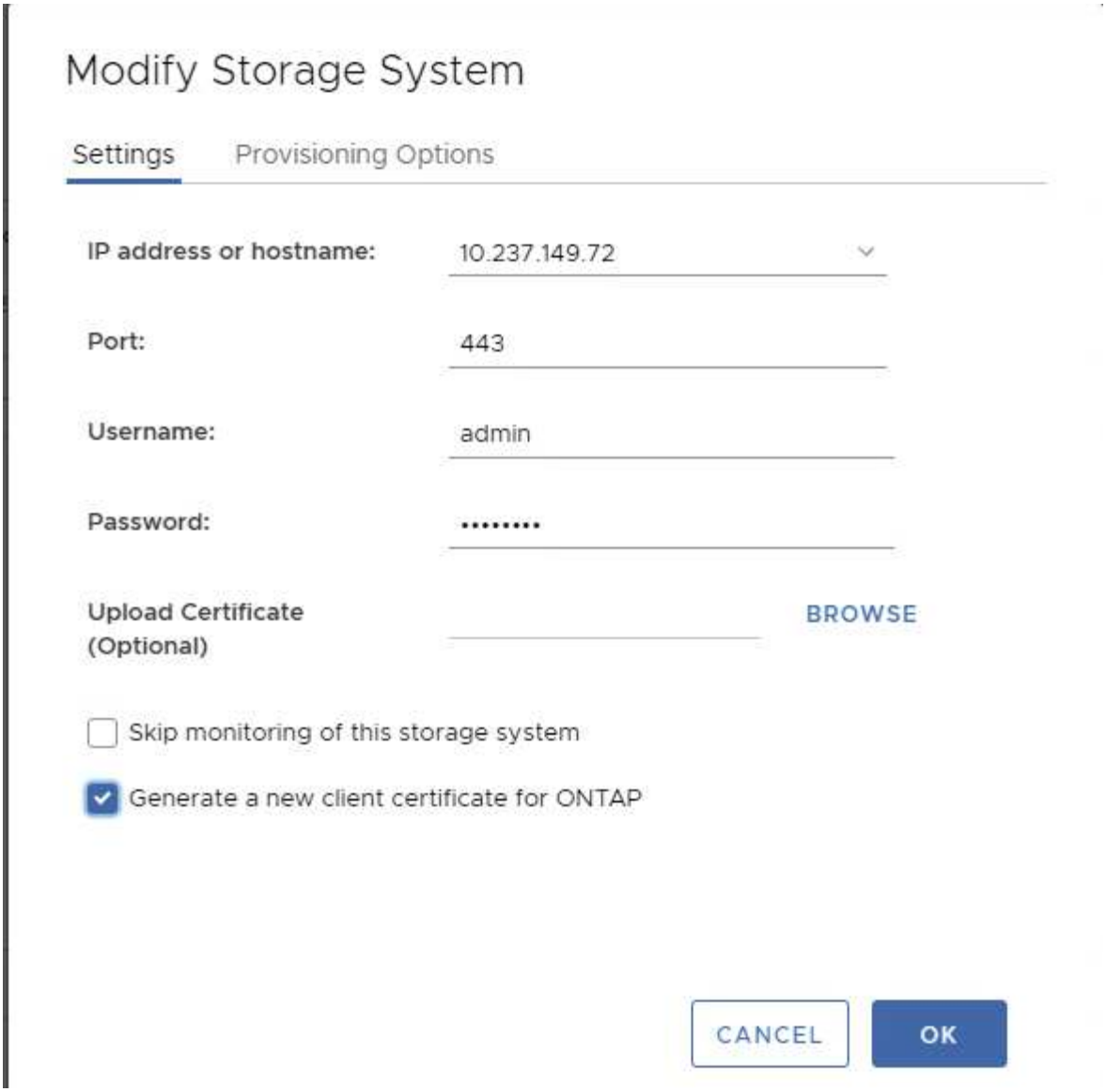

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
Authorize Cluster Certificate
Host 10.234.85.142 has identified itself with a self-signed certificate.
Show certificate
Do you want to trust this certificate?
NO
YES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

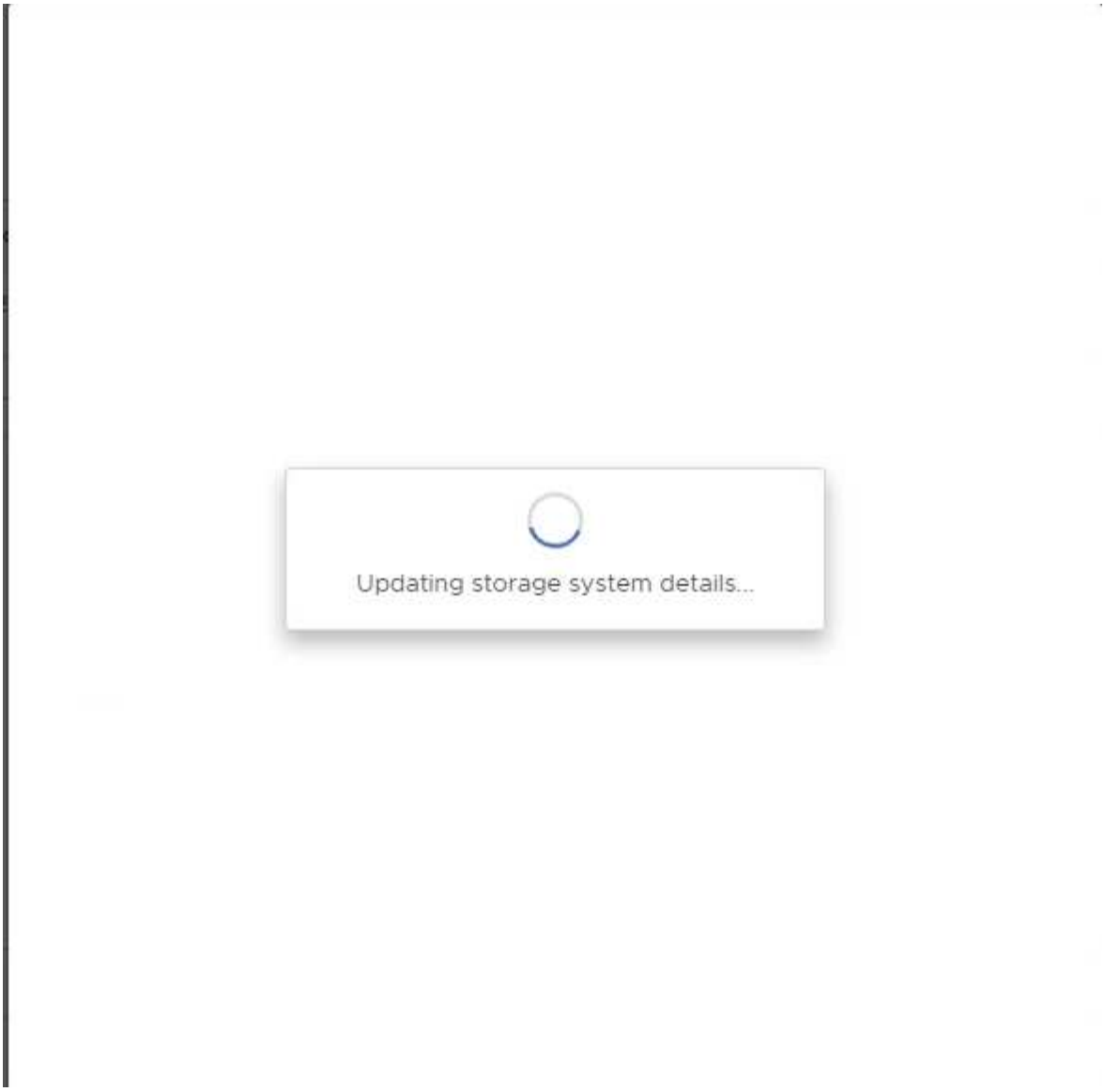


集群编辑

在集群编辑操作期间、有两种情形：

- 如果ONTAP证书过期、则用户必须获取新证书并上传。
- 如果OTV证书过期、则用户可以通过选中复选框来重新生成它。
  - 为ONTAP生成新的客户端证书_


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证书

默认情况下、ONTAP工具会使用安装期间自动创建的自签名证书来保护对Web UI的HTTPS访问。ONTAP工具提供以下功能：

1. 重新生成HTTPS证书

在ONTAP工具安装期间、会安装HTTPS CA证书、并将该证书存储在密钥库中。用户可以选择通过maine控制台重新生成HTTPS证书。

通过导航到"Application Configuration"(应用程序配置)→"Re-generate certificates"(重新生成证书)、可以在_maint_控制台中访问上述选项

登录横幅

用户在登录提示符中输入用户名后、将显示以下登录横幅。请注意、默认情况下、SSH处于禁用状态、从VM控制台启用SSH后、它仅允许一次性登录。

```
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.
```

用户通过 SSH 通道完成登录后，将显示以下文本：

```
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.
```

非活动超时

为了防止未经授权的访问、系统会设置非活动超时、以便在使用授权资源时自动注销在特定时间段内处于非活动状态的用户。这样可以确保只有授权用户才能访问资源、并有助于保持安全性。

- 默认情况下、vSphere Client会话会在空闲120分钟后关闭、需要用户重新登录才能继续使用客户端。您可以通过编辑webclient.properties文件来更改超时值。 您可以配置vSphere Client的超时 "配置vSphere Client超时值"
- ONTAP工具的web-cli会话注销时间为30分钟。

每个用户的最大并发请求数(网络安全保护：DOS攻击)

默认情况下、每个用户的最大并发请求数为48个。ONTAP工具中的root用户可以根据其环境的要求更改此值。此值不应设置为非常高的值，因为它提供了一种防止拒绝服务(DOS)攻击的机制。

用户可以在*_/opt/NetApp/vscserver/etc/dosfilterParams.json*文件中更改最大并发会话数和其他受支持的参数。

我们可以通过以下参数配置筛选器：

- ***delayMs***：在考虑之前，所有请求超出速率限制的延迟(以毫秒为单位)。提供-1仅拒绝请求。
- ***throtleMs***：等待信标的非同步等待时间。

- ***maxRequestMs***：允许此请求运行的时间长度。
- ***ipWhitlist***：不受速率限制的IP地址的逗号分隔列表。(可以是vCenter、ESXi和SRA IP)
- ***maxRequestsPerSec***：每秒从连接发出的最大请求数。

**dosfilterParams file:*中的默认值

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

网络时间协议(NTP)配置

有时、由于网络时间配置的差异、可能会出现安全问题。请务必确保网络中的所有设备都具有准确的时间设置、以防止出现此类问题。

虚拟设备

您可以从虚拟设备的维护控制台配置NTP服务器。 用户可以在_System Configuration_⇒_Add new NTP Server_选项下添加NTP服务器详细信息

默认情况下、NTP的服务为ntpd.这是一项传统服务、在某些情况下不适用于虚拟机。

*Debian

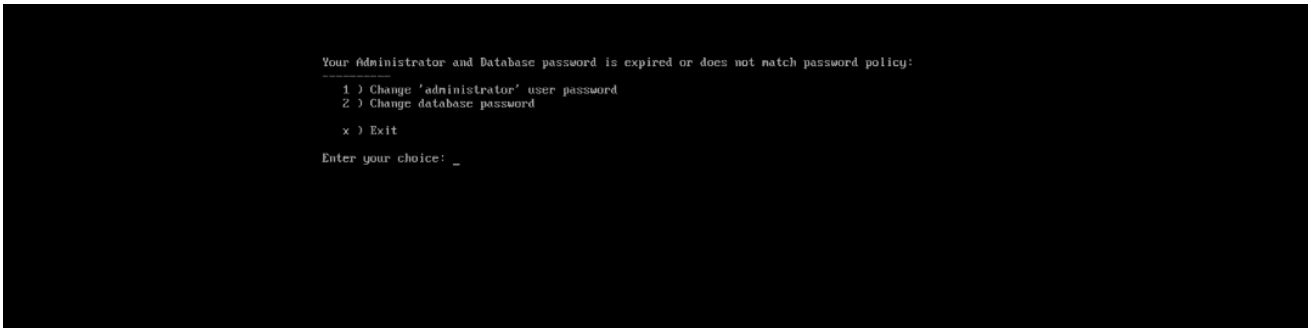
在Debian上、用户可以访问/etc/ntp.conf文件以获取NTP服务器详细信息。

密码策略

首次部署ONTAP工具或升级到9.12或更高版本的用户需要同时遵循管理员和数据库用户的强密码策略。在部署过程中、系统将提示新用户输入其密码。对于升级到9.12或更高版本的brownfield用户、维护控制台中将提供遵循强密码策略的选项。

- 用户登录maIT控制台后、系统将根据复杂规则集检查密码、如果发现未遵循此规则、则会要求用户重置相同密码。
- 密码默认有效期为90天、75天后、用户将开始收到更改密码的通知。
- 需要在每个周期设置新密码、系统不会将最后一个密码作为新密码。
- 每当用户登录maIT控制台时、它都会检查密码策略、如以下屏幕截图、然后再加载主菜单：

- 如果发现不符合密码策略、或者不符合ONTAP工具9.11或更早版本的升级设置。然后、用户将看到以下屏幕以重置密码：



- 如果用户尝试设置弱密码或再次提供最后一个密码、则用户将看到以下错误：