



# 管理管理员帐户

## ONTAP 9

NetApp  
February 12, 2026

# 目录

管理管理员帐户	1
了解如何管理ONTAP管理员帐户	1
将公共密钥与ONTAP管理员帐户关联	1
为ONTAP管理员管理SSH公共密钥和X.509证书	2
将公共密钥和X.509证书与管理员帐户关联	2
从管理员帐户的SSH公共密钥中删除证书关联	3
从管理员帐户中删除公共密钥和证书关联	3
为ONTAP SSH登录配置Cisco Duo 2FA	4
配置Cisco Duo	4
更改Cisco Duo配置	5
删除Cisco Duo配置	5
查看Cisco Duo配置	6
创建Duo组	6
查看Duo组	7
删除Duo组	7
为用户绕过Duo身份验证	8
在ONTAP中生成并安装CA签名的服务器证书	8
生成证书签名请求	9
安装 CA 签名的服务器证书	10
使用System Manager管理ONTAP证书	12
查看证书信息	12
生成证书签名请求	13
安装（添加）可信证书颁发机构	13
删除可信证书颁发机构	13
续订可信证书颁发机构	14
安装（添加）客户端 / 服务器证书	14
生成（添加）自签名客户端 / 服务器证书	14
删除客户端 / 服务器证书	15
续订客户端 / 服务器证书	15
创建新的本地证书颁发机构	15
使用本地证书颁发机构对证书进行签名	15
删除本地证书颁发机构	16
续订本地证书颁发机构	16
在ONTAP中配置Active Directory域控制器访问	16
配置身份验证通道	17
在域上创建 SVM 计算机帐户	18
在ONTAP中配置LDAP或NIS服务器访问	19
配置 LDAP 服务器访问	19
配置NIS服务器访问	20

创建名称服务切换 .....	21
更改ONTAP管理员密码 .....	21
锁定和解锁ONTAP管理员帐户 .....	22
在ONTAP中管理失败的登录尝试 .....	23
如何知道登录尝试失败 .....	23
重复登录尝试失败时应执行的操作 .....	23
对ONTAP管理员帐户密码强制实施SHA-2 .....	24
使用System Manager诊断和更正ONTAP文件访问问题 .....	25

# 管理管理员帐户

## 了解如何管理ONTAP管理员帐户

根据您启用帐户访问的方式，您可能需要将公有密钥与本地帐户关联，安装 CA 签名的服务器数字证书或配置 AD，LDAP 或 NIS 访问。您可以在启用帐户访问之前或之后执行所有这些任务。

## 将公共密钥与ONTAP管理员帐户关联

对于 SSH 公有密钥身份验证，您必须先将公有密钥与管理员帐户关联，然后此帐户才能访问 SVM。您可以使用 `security login publickey create` 命令将密钥与管理员帐户关联。

关于此任务

如果使用密码和 SSH 公有密钥通过 SSH 对帐户进行身份验证，则首先使用公有密钥对帐户进行身份验证。

开始之前

- 您必须已生成 SSH 密钥。
- 要执行此任务，您必须是集群或 SVM 管理员。

步骤

1. 将公有密钥与管理员帐户关联：

```
security login publickey create -vserver SVM_name -username user_name -index index -publickey certificate -comment comment
```

有关的详细信息 `security login publickey create`，请参见"[ONTAP 命令参考](#)"。

2. 查看公共密钥以验证更改：

```
security login publickey show -vserver SVM_name -username user_name -index index
```

有关的详细信息 `security login publickey show`，请参见"[ONTAP 命令参考](#)"。

示例

以下命令会将公共密钥与SVM管理员帐户关联 `svmadmin1` 对于SVM `engData1`。公有密钥的索引编号为 5。

```
cluster1::> security login publickey create -vserver engData1 -username svmadmin1 -index 5 -publickey "<key text>"
```

# 为ONTAP管理员管理SSH公共密钥和X.509证书

为了提高管理员帐户的SSH身份验证安全性、您可以使用 `security login publickey` 一组命令来管理SSH公共密钥及其与X.509证书的关联。

## 将公共密钥和X.509证书与管理员帐户关联

从ONTAP 9.13.1开始、您可以将X.509证书与与管理员帐户关联的公共密钥相关联。这样、您就可以在该帐户通过SSH登录时提高证书到期或撤消检查的安全性。

### 关于此任务

如果使用SSH公共密钥和X.509证书通过SSH对帐户进行身份验证、则ONTAP会在使用SSH公共密钥进行身份验证之前检查X.509证书的有效性。如果此证书已过期或已撤销、则SSH登录将被拒绝、并且公共密钥将自动禁用。

### 开始之前

- 要执行此任务，您必须是集群或 SVM 管理员。
- 您必须已生成 SSH 密钥。
- 如果您只需要检查X.509证书是否过期、则可以使用自签名证书。
- 如果需要检查X.509证书的到期和吊销情况：
  - 您必须已从证书颁发机构(CA)收到证书。
  - 您必须使用命令安装证书链(中间CA证书和根CA证书) `security certificate install`。有关的详细信息 `security certificate install`，请参见"ONTAP 命令参考"。
  - 您需要为SSH启用OCSP。请参见 "使用 OCSP 验证数字证书是否有效" 有关说明，请参见。

### 步骤

1. 将公共密钥和X.509证书与管理员帐户关联：

```
security login publickey create -vserver SVM_name -username user_name -index index -publickey certificate -x509-certificate install
```

有关的详细信息 `security login publickey create`，请参见"ONTAP 命令参考"。

2. 查看公共密钥以验证更改：

```
security login publickey show -vserver SVM_name -username user_name -index index
```

有关的详细信息 `security login publickey show`，请参见"ONTAP 命令参考"。

### 示例

以下命令会将公共密钥和X.509证书与SVM管理员帐户关联 `svmadmin2` 对于SVM `engData2`。公共密钥的索引编号为6。

```
cluster1::> security login publickey create -vserver engData2 -username
svmadmin2 -index 6 -publickey
"<key text>" -x509-certificate install
Please enter Certificate: Press <Enter> when done
<certificate text>
```

## 从管理员帐户的SSH公共密钥中删除证书关联

您可以从帐户的SSH公共密钥中删除当前证书关联、同时保留公共密钥。

开始之前

要执行此任务，您必须是集群或 SVM 管理员。

步骤

1. 从管理员帐户中删除X.509证书关联、并保留现有SSH公共密钥：

```
security login publickey modify -vserver SVM_name -username user_name -index
index -x509-certificate delete
```

有关的详细信息 security login publickey modify, 请参见"[ONTAP 命令参考](#)"。

2. 查看公共密钥以验证更改：

```
security login publickey show -vserver SVM_name -username user_name -index
index
```

示例

以下命令将从SVM管理员帐户中删除X.509证书关联 svmadmin2 对于SVM engData2 索引编号为6。

```
cluster1::> security login publickey modify -vserver engData2 -username
svmadmin2 -index 6 -x509-certificate delete
```

## 从管理员帐户中删除公共密钥和证书关联

您可以从帐户中删除当前公共密钥和证书配置。

开始之前

要执行此任务，您必须是集群或 SVM 管理员。

步骤

1. 从管理员帐户中删除公共密钥和X.509证书关联：

```
security login publickey delete -vserver SVM_name -username user_name -index
index
```

有关的详细信息 `security login publickey delete`, 请参见["ONTAP 命令参考"](#)。

## 2. 查看公共密钥以验证更改:

```
security login publickey show -vserver SVM_name -username user_name -index index
```

### 示例

以下命令将从SVM管理员帐户中删除公共密钥和X.509证书 `svmadmin3` 对于SVM `engData3` 索引编号为7。

```
cluster1::> security login publickey delete -vserver engData3 -username svmadmin3 -index 7
```

### 相关信息

- ["安全登录公钥"](#)

## 为ONTAP SSH登录配置Cisco Duo 2FA

从ONTAP 9.14.1开始、您可以将ONTAP配置为在SSH登录期间使用Cisco Duo进行双重身份验证(2FA)。您可以在集群级别配置Duo、并默认配置IT适用场景所有用户帐户。或者、您也可以Storage VM (以前称为Vserver)级别配置Duo、在这种情况下、它仅适用于该Storage VM的用户。如果您启用并配置Duo、它将作为一种附加的身份验证方法、对所有用户的现有方法进行补充。

如果您为SSH登录启用Duo身份验证、用户下次使用SSH登录时需要注册设备。有关注册信息, 请参阅Cisco Duo ["注册文档"](#)。

您可以使用ONTAP命令行界面对Cisco Duo执行以下任务:

- [配置Cisco Duo](#)
- [更改Cisco Duo配置](#)
- [删除Cisco Duo配置](#)
- [查看Cisco Duo配置](#)
- [删除Duo组](#)
- [查看Duo组](#)
- [为用户绕过Duo身份验证](#)

## 配置Cisco Duo

您可以使用命令为整个集群或特定Storage VM (在ONTAP命令行界面中称为Vserver)创建Cisco Duo配置 `security login duo create`。执行此操作时、系统会为此集群或Storage VM启用Cisco Duo SSH登录。有关的详细信息 `security login duo create`, 请参见["ONTAP 命令参考"](#)。

### 步骤

1. 登录到Cisco Duo管理面板。
2. 转到\*应用程序> UNIX应用程序\*。
3. 记录您的集成密钥、机密密钥和API主机名。
4. 使用SSH登录到您的ONTAP帐户。
5. 为此Storage VM启用Cisco Duo身份验证、将环境中的信息替换为方括号中的值：

```
security login duo create \  
-vserver <STORAGE_VM_NAME> \  
-integration-key <INTEGRATION_KEY> \  
-secret-key <SECRET_KEY> \  
-apihost <API_HOSTNAME>
```

## 更改Cisco Duo配置

您可以更改Cisco Duo对用户进行身份验证的方式(例如、提供的身份验证提示数或使用的HTTP代理)。如果您需要更改Storage VM (在ONTAP命令行界面中称为Vserver)的Cisco Duo配置、可以使用命令。 `security login duo modify` 有关的详细信息，请参见"[ONTAP 命令参考](#)"。

### 步骤

1. 登录到Cisco Duo管理面板。
2. 转到\*应用程序> UNIX应用程序\*。
3. 记录您的集成密钥、机密密钥和API主机名。
4. 使用SSH登录到您的ONTAP帐户。
5. 更改此Storage VM的Cisco Duo配置、将您环境中的更新信息替换为方括号中的值：

```
security login duo modify \  
-vserver <STORAGE_VM_NAME> \  
-integration-key <INTEGRATION_KEY> \  
-secret-key <SECRET_KEY> \  
-apihost <API_HOSTNAME> \  
-pushinfo true|false \  
-http-proxy <HTTP_PROXY_URL> \  
-autopush true|false \  
-max-prompts 1|2|3 \  
-is-enabled true|false \  
-fail-mode safe|secure
```

## 删除Cisco Duo配置

您可以删除Cisco Duo配置、这样SSH用户无需在登录时使用Duo进行身份验证。要删除Storage VM (在ONTAP命令行界面中称为Vserver)的Cisco Duo配置、可以使用命令。 `security login duo delete` 有关的详细

信息 ``security login duo delete`, 请参见["ONTAP 命令参考"](#)。

#### 步骤

1. 使用SSH登录到您的ONTAP帐户。
2. 删除此Storage VM的Cisco Duo配置、将您的Storage VM名称替换为 `<STORAGE_VM_NAME>`:

```
security login duo delete -vserver <STORAGE_VM_NAME>
```

此操作将永久删除此Storage VM的Cisco Duo配置。

## 查看Cisco Duo配置

您可以使用命令查看Storage VM (在ONTAP命令行界面中称为Vserver)的现有Cisco Duo配置。 `security login duo show``有关的详细信息 ``security login duo show`, 请参见["ONTAP 命令参考"](#)。

#### 步骤

1. 使用SSH登录到您的ONTAP帐户。
2. 显示了此Storage VM的Cisco Duo配置。(可选)您可以使用 `vserver` 参数以指定Storage VM、并将Storage VM名称替换为 `<STORAGE_VM_NAME>`:

```
security login duo show -vserver <STORAGE_VM_NAME>
```

您应看到类似于以下内容的输出:

```
Vserver: testcluster
Enabled: true

Status: ok
INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
SKEY SHA Fingerprint:
b79ffa4b1c50b1c747fbacdb34g671d4814
API Host: api-host.duosecurity.com
Autopush: true
Push info: true
Failmode: safe
Http-proxy: 192.168.0.1:3128
Prompts: 1
Comments: -
```

## 创建Duo组

您可以指示Cisco Duo在Duo身份验证过程中仅包括特定Active Directory、LDAP或本地用户组中的用户。如果您

创建Duo组、则只会提示该组中的用户进行Duo身份验证。您可以使用命令创建Duo组 `security login duo group create`。创建组时、您可以选择从Duo身份验证过程中排除该组中的特定用户。有关的详细信息 `security login duo group create`，请参见["ONTAP 命令参考"](#)。

#### 步骤

1. 使用SSH登录到您的ONTAP帐户。
2. 创建Duo组、将环境中的信息替换为方括号中的值。如果省略 `-vserver` 参数、则在集群级别创建组：

```
security login duo group create -vserver <STORAGE_VM_NAME> -group-name  
<GROUP_NAME> -excluded-users <USER1, USER2>
```

Duo组的名称必须与Active Directory、LDAP或本地组匹配。使用可选参数指定的用户 `-excluded-users` 不会包括在Duo身份验证过程中。

## 查看Duo组

您可以使用命令查看现有Cisco Duo组条目 `security login duo group show`。有关的详细信息 `security login duo group show`，请参见["ONTAP 命令参考"](#)。

#### 步骤

1. 使用SSH登录到您的ONTAP帐户。
2. 显示Duo组条目、将环境中的信息替换为方括号中的值。如果省略 `-vserver` 参数中、组将在集群级别显示：

```
security login duo group show -vserver <STORAGE_VM_NAME> -group-name  
<GROUP_NAME> -excluded-users <USER1, USER2>
```

Duo组的名称必须与Active Directory、LDAP或本地组匹配。使用可选参数指定的用户 `-excluded-users` 将不会显示。

## 删除Duo组

您可以使用命令删除Duo组条目 `security login duo group delete`。如果删除组、则该组中的用户将不再包括在Duo身份验证过程中。有关的详细信息 `security login duo group delete`，请参见["ONTAP 命令参考"](#)。

#### 步骤

1. 使用SSH登录到您的ONTAP帐户。
2. 删除Duo组条目、将环境中的信息替换为方括号中的值。如果省略 `-vserver` 参数、则组将在集群级别删除：

```
security login duo group delete -vserver <STORAGE_VM_NAME> -group-name  
<GROUP_NAME>
```

Duo组的名称必须与Active Directory、LDAP或本地组匹配。

## 为用户绕过Duo身份验证

您可以从Duo SSH身份验证过程中排除所有用户或特定用户。

### 排除所有Duo用户

您可以为所有用户禁用Cisco Duo SSH身份验证。

#### 步骤

1. 使用SSH登录到您的ONTAP帐户。
2. 为SSH用户禁用Cisco Duo身份验证、并将Vserver名称替换为 <STORAGE\_VM\_NAME>:

```
security login duo modify -vserver <STORAGE_VM_NAME> -is-enabled false
```

### 排除Duo组用户

您可以从Duo SSH身份验证过程中排除属于Duo组的某些用户。

#### 步骤

1. 使用SSH登录到您的ONTAP帐户。
2. 为组中的特定用户禁用Cisco Duo身份验证。将组名称和要排除的用户列表替换为方括号中的值:

```
security login duo group modify -group-name <GROUP_NAME> -excluded-users  
<USER1, USER2>
```

Duo组的名称必须与Active Directory、LDAP或本地组匹配。使用参数指定的用户`-excluded-users`不会包括在Duo身份验证过程中。

有关的详细信息 `security login duo group modify`，请参见["ONTAP 命令参考"](#)。

### 排除本地Duo用户

您可以使用Cisco Duo管理面板排除特定本地用户使用Duo身份验证。有关说明，请参见 ["Cisco Duo文档"](#)。

## 在ONTAP中生成并安装CA签名的服务器证书

在生产系统上，最佳做法是安装 CA 签名的数字证书，以便将集群或 SVM 作为 SSL 服务器进行身份验证。您可以使用 `security certificate generate-csr`命令生成证书签名请求(CSR)、并使用`security certificate install`命令安装从证书颁发机构收到的证书。有关和的`security certificate install`详细信息`security certificate generate-csr，请参见"ONTAP 命令参考"。`

## 生成证书签名请求

您可以使用 `security certificate generate-csr` 用于生成证书签名请求(CSR)的命令。处理请求后，证书颁发机构（CA）会向您发送签名数字证书。

开始之前

要执行此任务，您必须是集群或 SVM 管理员。

步骤

### 1. 生成 CSR

```
security certificate generate-csr -common-name FQDN_or_common_name -size
512|1024|1536|2048 -country country -state state -locality locality
-organization organization -unit unit -email-addr email_of_contact -hash
-function SHA1|SHA256|MD5
```

以下命令将使用散列函数生成的2048位专用密钥创建CSR，SHA256`以供自定义公用名为的公司所在部门的组`IT`使用`Software，该公司 `server1.companyname.com``位于美国加利福尼亚州的桑尼维尔。SVM联系人管理员的电子邮件地址为``web@example.com`。系统将在输出中显示 CSR 和私钥。

创建CSR的示例

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California
-locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
```

```
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
```

```
Private Key :
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----
```

NOTE: Keep a copy of your certificate request and private key for future reference.

### 2. 复制 CSR 输出中的证书请求，并以电子形式（如电子邮件）将其发送到可信的第三方 CA 进行签名。

处理完您的请求后，CA 会向您发送已签名的数字证书。您应保留一份私钥和 CA 签名数字证书的副本。

## 安装 CA 签名的服务器证书

您可以使用 `security certificate install`` 命令在 SVM 上安装 CA 签名的服务器证书。ONTAP 会提示您输入证书颁发机构（CA）根证书和中间证书，这些证书构成服务器证书的证书链。有关的详细信息 `security certificate install``，请参见["ONTAP 命令参考"](#)。

### 开始之前

要执行此任务，您必须是集群或 SVM 管理员。

### 步骤

1. 安装 CA 签名的服务器证书：

```
security certificate install -vserver SVM_name -type certificate_type
```



ONTAP 会提示您输入 CA 根证书和中间证书，以构成服务器证书的证书链。此链从颁发服务器证书的 CA 的证书开始，最多可以包含 CA 的根证书。如果缺少任何中间证书，则会导致服务器证书安装失败。

以下命令将在 SVM 上安装 CA 签名的服务器证书和中间证书 `engData2`。

## 安装CA签名服务器证书中间证书的示例

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

Do you want to continue entering root and/or intermediate
certificates {y|n}: n

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.
```

### 相关信息

- ["安全证书generate-csr"](#)

# 使用System Manager管理ONTAP证书

从 ONTAP 9.10.1 开始，您可以使用 System Manager 管理可信证书颁发机构，客户端 / 服务器证书以及本地（板载）证书颁发机构。

使用 System Manager ，您可以管理从其他应用程序收到的证书，以便对来自这些应用程序的通信进行身份验证。您还可以管理自己的证书，以便向其他应用程序标识您的系统。

## 查看证书信息

使用 System Manager ，您可以查看集群上存储的可信证书颁发机构，客户端 / 服务器证书以及本地证书颁发机构。

### 步骤

1. 在System Manager中、选择\*集群>设置\*。
2. 滚动到 \* 安全性 \* 区域。  
在 \* 证书 \* 部分中，将显示以下详细信息：
  - 存储的受信任证书颁发机构的数量。
  - 存储的客户端 / 服务器证书的数量。
  - 存储的本地证书颁发机构的数量。
3. 选择任意数字可查看有关证书类别的详细信息，或选择 [→](#) 打开包含所有类别信息的\*证书\*页。此列表将显示整个集群的信息。如果要仅显示特定 Storage VM 的信息，请执行以下步骤：
  - a. 选择\*存储> Storage VM\*。
  - b. 选择 Storage VM 。
  - c. 切换到\*Settings\*选项卡。
  - d. 选择\*证书\*部分中显示的数字。

### 下一步操作

- 在 \* 证书 \* 页面中，您可以 [\[生成证书签名请求\]](#)。
- 证书信息分为三个选项卡，每个类别一个。您可以从每个选项卡执行以下任务：

在此选项卡上 ...	您可以执行以下过程 ...
<ul style="list-style-type: none"><li>• 可信证书颁发机构 *</li></ul>	<ul style="list-style-type: none"><li>• <a href="#">[install-trusted-cert]</a></li><li>• <a href="#">[删除可信证书颁发机构]</a></li><li>• <a href="#">[续订可信证书颁发机构]</a></li></ul>
<ul style="list-style-type: none"><li>• 客户端 / 服务器证书 *</li></ul>	<ul style="list-style-type: none"><li>• <a href="#">[install-cs-cert]</a></li><li>• <a href="#">[gen-cs-cert]</a></li><li>• <a href="#">[delete-cs-cert]</a></li><li>• <a href="#">[renew-cs-cert]</a></li></ul>

<ul style="list-style-type: none"> <li>• 本地证书颁发机构 *</li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">[创建新的本地证书颁发机构]</a></li> <li>• <a href="#">[使用本地证书颁发机构对证书进行签名]</a></li> <li>• <a href="#">[删除本地证书颁发机构]</a></li> <li>• <a href="#">[续订本地证书颁发机构]</a></li> </ul>
--	---

## 生成证书签名请求

您可以从 \* 证书 \* 页面的任何选项卡使用 System Manager 生成证书签名请求（CSR）。此时将生成私钥和相应的 CSR，可以使用证书颁发机构对其进行签名，以生成公有证书。

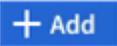
### 步骤

1. 查看 \* 证书 \* 页面。请参见 [\[查看证书信息\]](#)。
2. 选择 \*+Generate CSR\*
3. 填写主题名称的信息：
  - a. 输入 \* 公用名 \*。
  - b. 选择一个 \* 国家 / 地区 \*。
  - c. 输入 \* 组织 \*。
  - d. 输入 \* 组织单位 \*。
4. 如果要覆盖默认值，请选择 \* 更多选项 \* 并提供追加信息。

## 安装（添加）可信证书颁发机构

您可以在 System Manager 中安装其他受信任的证书颁发机构。

### 步骤

1. 查看 \* 可信证书颁发机构 \* 选项卡。请参见 [\[查看证书信息\]](#)。
2. 选择。 
3. 在 \* 添加可信证书颁发机构 \* 面板上，执行以下操作：
  - 输入 \* 名称 \*。
  - 对于 \* 范围 \*，选择一个 Storage VM。
  - 输入 \* 公用名 \*。
  - 选择 \* 类型 \*。
  - 输入或导入 \* 证书详细信息 \*。

## 删除可信证书颁发机构

使用 System Manager，您可以删除受信任的证书颁发机构。



您不能删除预安装了ONTAP的可信证书颁发机构。

## 步骤

1. 查看 \* 可信证书颁发机构 \* 选项卡。请参见 [\[查看证书信息\]](#)。
2. 选择可信证书颁发机构的名称。
3. 选择  名称旁边的，然后选择 \*Delete\*。

## 续订可信证书颁发机构

使用 System Manager ，您可以续订已过期或即将过期的可信证书颁发机构。

## 步骤

1. 查看 \* 可信证书颁发机构 \* 选项卡。请参见 [\[查看证书信息\]](#)。
2. 选择可信证书颁发机构的名称。
3. 选择  证书名称旁边的 \*续订\*。

## 安装（添加）客户端 / 服务器证书

使用 System Manager ，您可以安装其他客户端 / 服务器证书。

## 步骤

1. 查看 \* 客户端 / 服务器证书 \* 选项卡。请参见 [\[查看证书信息\]](#)。
2. 选择。 
3. 在 \* 添加客户端 / 服务器证书 \* 面板上，执行以下操作：
  - 输入 \* 证书名称 \* 。
  - 对于 \* 范围 \* ，选择一个 Storage VM 。
  - 输入 \* 公用名 \* 。
  - 选择 \* 类型 \* 。
  - 输入或导入 \* 证书详细信息 \* 。
  - 您可以从文本文件写入或复制并粘贴证书详细信息，也可以通过单击 \* 导入 \* 从证书文件导入文本。
  - 输入 \* 专用密钥\* 。
  - 您可以从文本文件写入或复制并粘贴私钥，也可以通过单击 \* 导入 \* 从私钥文件导入文本。

## 生成（添加）自签名客户端 / 服务器证书

使用 System Manager ，您可以生成其他自签名客户端 / 服务器证书。

## 步骤

1. 查看 \* 客户端 / 服务器证书 \* 选项卡。请参见 [\[查看证书信息\]](#)。
2. 选择 \*+生成自签名证书\*。
3. 在 \* 生成自签名证书 \* 面板上，执行以下操作：
  - 输入 \* 证书名称 \* 。
  - 对于 \* 范围 \* ，选择一个 Storage VM 。

- 输入 \* 公用名 \*。
- 选择 \* 类型 \*。
- 选择 \* 哈希函数 \*。
- 选择 \* 密钥大小 \*。
- 选择一个 \* 存储虚拟机 \*。

## 删除客户端 / 服务器证书

使用 System Manager ，您可以删除客户端 / 服务器证书。

### 步骤

1. 查看 \* 客户端 / 服务器证书 \* 选项卡。请参见 [\[查看证书信息\]](#)。
2. 选择客户端/服务器证书的名称。
3. 选择  名称旁边的，然后单击 \*Delete\*。

## 续订客户端 / 服务器证书

使用 System Manager ，您可以续订已过期或即将过期的客户端 / 服务器证书。

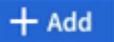
### 步骤

1. 查看 \* 客户端 / 服务器证书 \* 选项卡。请参见 [\[查看证书信息\]](#)。
2. 选择客户端/服务器证书的名称。
3. 选择  名称旁边的，然后单击 \*Renew\*。

## 创建新的本地证书颁发机构

使用 System Manager ，您可以创建新的本地证书颁发机构。

### 步骤

1. 查看 \* 本地证书颁发机构 \* 选项卡。请参见 [\[查看证书信息\]](#)。
2. 选择。 
3. 在 \* 添加本地证书颁发机构 \* 面板上，执行以下操作：
  - 输入 \* 名称 \*。
  - 对于 \* 范围 \* ，选择一个 Storage VM 。
  - 输入 \* 公用名 \*。
4. 如果要覆盖默认值，请选择 \* 更多选项 \* 并提供追加信息。

## 使用本地证书颁发机构对证书进行签名

在 System Manager 中，您可以使用本地证书颁发机构对证书进行签名。

### 步骤

1. 查看 \* 本地证书颁发机构 \* 选项卡。请参见 [\[查看证书信息\]](#)。
2. 选择本地证书颁发机构的名称。
3. 选择名称旁边的，然后选择  签署证书。
4. 填写 \* 签署证书签名请求 \* 表单。
  - 您可以粘贴证书签名内容，也可以单击 \* 导入 \* 导入证书签名请求文件。
  - 指定证书有效的天数。

## 删除本地证书颁发机构

使用 System Manager ，您可以删除本地证书颁发机构。

### 步骤

1. 查看 \* 本地证书颁发机构 \* 选项卡。请参见 [\[查看证书信息\]](#)。
2. 选择本地证书颁发机构的名称。
3. 选择名称旁边的，然后选择  **Delete**。

## 续订本地证书颁发机构

使用 System Manager ，您可以续订已过期或即将过期的本地证书颁发机构。

### 步骤

1. 查看 \* 本地证书颁发机构 \* 选项卡。请参见 [\[查看证书信息\]](#)。
2. 选择本地证书颁发机构的名称。
3. 选择  名称旁边的，然后单击 \*Renew\*。

## 在ONTAP中配置Active Directory域控制器访问

您必须先配置 AD 域控制器对集群或 SVM 的访问，AD 帐户才能访问 SVM 。如果您已为数据SVM配置SMB服务器、则可以将此SVM配置为网关或\_tunnel"、以便对集群进行AD访问。如果尚未配置 SMB 服务器，则可以在 AD 域上为 SVM 创建计算机帐户。

ONTAP 支持以下域控制器身份验证服务：

- Kerberos
- LDAP
- 网络登录
- 本地安全机构（LSA）

ONTAP 支持以下会话密钥算法来实现安全的网络登录连接：

会话密钥算法	可用开头为...
--------	----------

HMAC-SHA256，基于高级加密标准（AES）	ONTAP 9.10.1
如果集群运行的是ONTAP 9.9.1或更早版本、并且域控制器对安全Netlogon服务强制实施AES、则连接将失败。在这种情况下、您需要重新配置域控制器、以接受与ONTAP的强密钥连接。	
DES 和 HMAC-MD5（设置了强密钥时）	所有 ONTAP 9 版本

如果要在建立Netlogon安全通道期间使用AES会话密钥、则需要验证是否已在SVM上启用AES。

- 从ONTAP 9.14.1开始、创建SVM时会默认启用AES、您无需修改SVM的安全设置、即可在Netlogon安全通道建立期间使用AES会话密钥。
- 在ONTAP 9.10.1到9.13.1中、创建SVM时、AES默认处于禁用状态。您需要使用以下命令启用AES：

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```



升级到ONTAP 9.14.1或更高版本时、使用旧版ONTAP创建的现有SVM的AES设置不会自动更改。要在这些SVM上启用AES、您仍需要更新此设置的值。

## 配置身份验证通道

如果已为数据SVM配置SMB服务器、则可以使用 `security login domain-tunnel create` 命令将SVM配置为网关或“\_tunnel”、以便对集群进行AD访问。

在ONTAP 9.161之前的版本中、您必须使用身份验证通道来管理使用AD的集群管理员帐户。

### 开始之前

- 您必须已为数据SVM配置SMB服务器。
- 您必须已启用 AD 域用户帐户才能访问集群的管理 SVM。
- 您必须是集群管理员才能执行此任务。

从 ONTAP 9.10.1 开始，如果您有用于 AD 访问的 SVM 网关（域通道），则在 AD 域中禁用 NTLM 后，您可以使用 Kerberos 进行管理员身份验证。在早期版本中，SVM 网关的管理员身份验证不支持 Kerberos。默认情况下，此功能可用；不需要任何配置。



始终先尝试 Kerberos 身份验证。如果发生故障，则会尝试 NTLM 身份验证。

### 步骤

1. 将启用了SMB的数据SVM配置为身份验证通道、以便AD域控制器能够访问集群：

```
security login domain-tunnel create -vserver <svm_name>
```

有关的详细信息 `security login domain-tunnel create`，请参见“[ONTAP 命令参考](#)”。



要对用户进行身份验证，必须运行 SVM。

以下命令会将启用了SMB的数据SVM配置 `engData` 为身份验证通道。

```
cluster1::>security login domain-tunnel create -vserver engData
```

## 在域上创建 SVM 计算机帐户

如果尚未为数据SVM配置SMB服务器、则可以使用 `vserver active-directory create` 命令为域中的SVM创建计算机帐户。

### 关于此任务

输入后 `vserver active-directory create` 命令时、系统会提示您提供AD用户帐户的凭据、该帐户具有足够的权限、可以将计算机添加到域中的指定组织单位。帐户的密码不能为空。

从ONTAP 9.161开始、您可以使用此过程通过AD管理集群管理员帐户。

### 开始之前

要执行此任务，您必须是集群或 SVM 管理员。

### 步骤

1. 在 AD 域上为 SVM 创建计算机帐户：

```
vserver active-directory create -vserver <SVM_name> -account-name  
<NetBIOS_account_name> -domain <domain> -ou <organizational_unit>
```

从ONTAP 9.161开始、`-vserver` 参数接受管理SVM。有关的详细信息、`vserver active-directory create`，请参见["ONTAP 命令参考"](#)。

以下命令将在SVM的 `engData` 域上 `example.com` 创建名为的计算机帐户 `ADSERVER1`。输入命令后，系统将提示您输入 AD 用户帐户凭据。

```
cluster1::>vserver active-directory create -vserver engData -account  
-name ADSERVER1 -domain example.com
```

```
In order to create an Active Directory machine account, you must supply  
the name and password of a Windows account with sufficient privileges to  
add computers to the "CN=Computers" container within the "example.com"  
domain.
```

```
Enter the user name: Administrator
```

```
Enter the password:
```

# 在ONTAP中配置LDAP或NIS服务器访问

您必须先配置对 SVM 的 LDAP 或 NIS 服务器访问，然后 LDAP 或 NIS 帐户才能访问 SVM。通过交换机功能，您可以使用 LDAP 或 NIS 作为备用名称服务源。

## 配置 LDAP 服务器访问

您必须先配置对 SVM 的 LDAP 服务器访问，然后 LDAP 帐户才能访问 SVM。您可以使用 `vserver services name-service ldap client create` 命令以在SVM上创建LDAP客户端配置。然后、您可以使用 `vserver services name-service ldap create` 命令将LDAP客户端配置与SVM关联。

关于此任务

大多数 LDAP 服务器都可以使用 ONTAP 提供的默认模式：

- MS-AD-BIS（大多数 Windows 2012 及更高版本 AD 服务器的首选架构）
- AD-IDMU (Windows 2008、Windows 2016及更高版本的AD服务器)
- AD-SFU（Windows 2003 及更早版本的 AD 服务器）
- RFC-2307（UNIX LDAP 服务器）

除非另有要求，否则最好使用默认模式。如果是，您可以通过复制默认模式并修改副本来创建自己的模式。有关详细信息，请参见

- ["NFS配置"](#)
- ["NetApp 技术报告 4835：《如何在 ONTAP 中配置 LDAP》"](#)

开始之前

- 您必须已在SVM上安装"[CA 签名的服务器数字证书](#)"。
- 要执行此任务，您必须是集群或 SVM 管理员。

步骤

1. 在SVM上创建LDAP客户端配置：

```
vserver services name-service ldap client create -vserver <SVM_name> -client
-config <client_configuration> -servers <LDAP_server_IPs> -schema <schema>
-use-start-tls <true|false>
```



仅支持使用启动 TLS 访问数据 SVM。不支持访问管理 SVM。

有关的详细信息 `vserver services name-service ldap client create`，请参见"[ONTAP 命令参考](#)"。

以下命令将在SVM上 `engData`` 创建名为的LDAP客户端配置 ``corp`。客户端使用IP地址172.160.0.100和172.16.0.101匿名绑定到LDAP服务器。客户端使用RFC 2307模式进行LDAP查询。客户端与服务器的通信使用 Start TLS 进行加密。

```
cluster1::> vserver services name-service ldap client create
-vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
-schema RFC-2307 -use-start-tls true
```



这 `-ldap-servers` 字段替换 `-servers` 字段。您可以使用 `-ldap-servers` 字段指定 LDAP 服务器的主机名或 IP 地址。

2. 将LDAP客户端配置与SVM相关联: `vserver services name-service ldap create -vserver <SVM_name> -client-config <client_configuration> -client-enabled <true|false>`

有关的详细信息 `vserver services name-service ldap create`, 请参见["ONTAP 命令参考"](#)。

以下命令将关联LDAP客户端配置 `corp` 使用SVM `engData`, 并在SVM上启用LDAP客户端。

```
cluster1::>vserver services name-service ldap create -vserver engData
-client-config corp -client-enabled true
```



这 `vserver services name-service ldap create` 如果ONTAP无法联系名称服务器, 该命令将执行自动配置验证并报告错误消息。

3. 使用 `vserver services name-service ldap check` 命令验证名称服务器的状态。

以下命令将验证 SVM `vs0` 上的 LDAP 服务器。

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0 |
| Client Configuration Name: c1 |
| LDAP Status: up |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13". |
```

您可以使用 `name service check` 命令来验证名称服务器的状态。

## 配置NIS服务器访问

您必须先配置对SVM的NIS服务器访问权限、然后NIS帐户才能访问SVM。您可以使用 `vserver services name-service nis-domain create` 命令以在SVM上创建NIS域配置。

开始之前

- 在 SVM 上配置 NIS 域之前, 所有已配置的服务器都必须可用且可访问。
- 要执行此任务, 您必须是集群或 SVM 管理员。

## 步骤

### 1. 在SVM上创建NIS域配置:

```
vserver services name-service nis-domain create -vserver <SVM_name> -domain <client_configuration> -nis-servers <NIS_server_IPs>
```

有关的详细信息 `vserver services name-service nis-domain create`, 请参见"[ONTAP 命令参考](#)".



这 `-nis-servers` 字段替换 `-servers` 字段。您可以使用 `-nis-servers` 字段指定 NIS 服务器的主机名或 IP 地址。

以下命令将在SVM上创建NIS域配置 `engData`。NIS域 `nisdomain` 使用IP地址与NIS服务器进行通信 `192.0.2.180`。

```
cluster1::>vserver services name-service nis-domain create -vserver engData -domain nisdomain -nis-servers 192.0.2.180
```

## 创建名称服务切换

通过名称服务切换功能, 您可以使用 LDAP 或 NIS 作为备用名称服务源。您可以使用 `vserver services name-service ns-switch modify` 命令以指定名称服务源的查找顺序。

### 开始之前

- 您必须已配置 LDAP 和 NIS 服务器访问。
- 要执行此任务, 您必须是集群管理员或 SVM 管理员。

## 步骤

### 1. 指定名称服务源的查找顺序:

```
vserver services name-service ns-switch modify -vserver <SVM_name> -database <name_service_switch_database> -sources <name_service_source_order>
```

有关的详细信息 `vserver services name-service ns-switch modify`, 请参见"[ONTAP 命令参考](#)".

以下命令为SVM上的数据库 `engData` 指定LDAP和NIS名称服务源的查找顺序 `passwd`。

```
cluster1::>vserver services name-service ns-switch modify -vserver engData -database passwd -source files ldap,nis
```

## 更改ONTAP管理员密码

首次登录到系统后, 您应立即更改初始密码。如果您是SVM管理员, 则可以使用

`security login password` 命令以更改您自己的密码。如果您是集群管理员、则可以使用 `security login password` 命令以更改任何管理员的密码。

关于此任务

新密码必须遵循以下规则：

- 不能包含用户名
- 长度必须至少为八个字符
- 它必须至少包含一个字母和一个数字
- 不能与最后六个密码相同



您可以使用 `'security login role config modify'` 命令修改与给定角色关联的帐户的密码规则。

开始之前

- 您必须是集群或 SVM 管理员才能更改自己的密码。
- 您必须是集群管理员才能更改其他管理员的密码。

步骤

1. 更改管理员密码：`security login password -vserver svm_name -username user_name`

以下命令将更改管理员的密码 `admin1` 对于 `SVMvs1.example.com`。系统将提示您输入当前密码，然后输入并重新输入新密码。

```
vs1.example.com::>security login password -vserver engData -username
admin1
Please enter your current password:
Please enter a new password:
Please enter it again:
```

相关信息

- ["安全登录角色配置修改"](#)
- ["安全登录密码"](#)

## 锁定和解锁ONTAP管理员帐户

您可以使用 `security login lock` 用于锁定管理员帐户的命令、以及 `security login unlock` 命令解锁帐户。

开始之前

您必须是集群管理员才能执行这些任务。

步骤

1. 锁定管理员帐户：

```
security login lock -vserver SVM_name -username user_name
```

以下命令将锁定管理员帐户 admin1 对于SVM vs1.example.com:

```
cluster1::>security login lock -vserver engData -username admin1
```

有关的详细信息 security login lock, 请参见"[ONTAP 命令参考](#)".

## 2. 解锁管理员帐户:

```
security login unlock -vserver SVM_name -username user_name
```

以下命令将解锁管理员帐户 admin1 对于SVM vs1.example.com:

```
cluster1::>security login unlock -vserver engData -username admin1
```

有关的详细信息 security login unlock, 请参见"[ONTAP 命令参考](#)".

### 相关信息

- "[安全登录](#)"

## 在ONTAP中管理失败的登录尝试

登录尝试重复失败有时表示入侵者正在尝试访问存储系统。您可以执行多个步骤来确保不发生入侵。

### 如何知道登录尝试失败

事件管理系统 (EMS) 每小时向您发出一次失败登录尝试的通知。您可以在中找到失败登录尝试的记录 audit.log 文件

### 重复登录尝试失败时应执行的操作

从短期来看, 您可以采取多个步骤来防止入侵:

- 要求密码至少包含大写字符, 小写字符, 特殊字符和 / 或数字
- 在登录尝试失败后施加延迟
- 限制允许的失败登录尝试次数, 并在指定失败尝试次数后锁定用户
- 使处于非活动状态的帐户在指定天数内过期并锁定

您可以使用 security login role config modify`命令执行这些任务。有关的详细信息 `security login role config modify, 请参见"[ONTAP 命令参考](#)".

从长期来看, 您还可以执行以下附加步骤:

- 使用 `security ssh modify`` 命令限制所有新创建的 SVM 的失败登录尝试次数。有关的详细信息 ``security ssh modify`，请参见"[ONTAP 命令参考](#)"。
- 通过要求用户更改密码，将现有 MD5 算法帐户迁移到更安全的 SHA-512 算法。

## 对ONTAP管理员帐户密码强制实施SHA-2

升级后，在 ONTAP 9.0 之前创建的管理员帐户将继续使用 MD5 密码，直到手动更改密码为止。MD5 的安全性低于 SHA-2。因此，升级后，您应提示 MD5 帐户的用户更改密码，以使用默认的 SHA-512 哈希函数。

关于此任务

密码哈希功能可用于执行以下操作：

- 显示与指定哈希函数匹配的用户帐户。
- 使使用指定哈希函数（例如 MD5）的帐户过期，从而强制用户在下次登录时更改密码。
- 锁定密码使用指定哈希函数的帐户。
- 还原到 ONTAP 9 之前的版本时，请重置集群管理员自己的密码，以使其与早期版本支持的哈希函数（MD5）兼容。

ONTAP只能使用NetApp易管理性SDK接受哈希前的SHA-2密码 (`security-login-create` 和 `security-login-modify-password`)。

步骤

### 1. 将 MD5 管理员帐户迁移到 SHA-512 密码哈希函数：

- a. 使所有MD5管理员帐户过期：`security login expire-password -vserver * -username * -hash-function md5`

这样做会强制 MD5 帐户用户在下次登录时更改密码。

- b. 要求 MD5 帐户的用户通过控制台或 SSH 会话登录。

系统会检测到帐户已过期，并提示用户更改密码。默认情况下，SHA-512 用于更改的密码。

### 2. 对于用户在一段时间内未登录更改密码的 MD5 帐户，强制迁移帐户：

- a. 锁定仍使用MD5哈希函数的帐户(高级权限级别)：`security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

在指定的天数之后 `-lock-after`，则用户无法访问其MD5帐户。

- b. 当用户准备好更改密码时解锁帐户：`security login unlock -vserver svm_name -username user_name`

- c. 让用户通过控制台或 SSH 会话登录到其帐户，并在系统提示时更改密码。

相关信息

- "[security login expire-password](#)"

- "安全登录解锁"

## 使用System Manager诊断和更正ONTAP文件访问问题

从 ONTAP 9.8 开始，您可以跟踪和查看文件访问问题。

### 步骤

1. 在 System Manager 中，选择 \* 存储 > 存储 VM\* 。
2. 选择要对其执行跟踪的 Storage VM 。
3. 单击  更多。
4. 单击 \* 跟踪文件访问 \* 。
5. 提供用户名和客户端 IP 地址，然后单击 \* 开始跟踪 \* 。

跟踪结果显示在表中。\* 原因 \* 列提供了无法访问文件的原因。

6. 单击  结果表左侧的列以查看文件访问权限。

## 版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

## 商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。