管理管理员帐户

ONTAP 9

NetApp
April 24, 2024

目录

管理管理员帐户 1
管理管理员帐户概述 1
将公有密钥与管理员帐户关联 1
管理管理员帐户的SSH公共密钥和X.509证书 2
为SSH登录配置Cisco Duo 2FA 4
生成并安装 CA 签名的服务器证书概述 8
使用 System Manager 管理证书 12
配置 Active Directory 域控制器访问概述 17
配置 LDAP 或 NIS 服务器访问概述 19
更改管理员密码 22
锁定和解锁管理员帐户 22
管理失败的登录尝试 23
对管理员帐户密码强制执行 SHA-2 24
诊断并更正文件访问问题 24

管理管理员帐户

管理管理员帐户概述

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。

将公有密钥与管理员帐户关联

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` 用于将密钥与管理员帐户关联的命令。

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`*

   有关完整的命令语法、请参见的工作表参考 "将公有密钥与用户帐户关联"。

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>"
```

管理管理员帐户的SSH公共密钥和X.509证书

要提高管理员帐户的SSH身份验证安全性、您可以使用 `security login publickey` 一组命令、用于管理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。
  - 您必须使用安装证书链(中间CA证书和根CA证书) `security certificate install` 命令
  - 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
   ```

   有关完整的命令语法、请参见的工作表参考 "将公有密钥与用户帐户关联"。

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
   ```

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
   ```

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
```

为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、您也可以在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` 命令：执行此操作时、系统会为此集群或Storage VM启用Cisco Duo SSH登录。

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>
```

有关此命令所需参数和可选参数的详细信息、请参阅 "用于管理员身份验证和 RBAC 配置的工作表"。

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 `security login duo modify` 命令：

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 \
-prompts 1|2|3 \
-max-unenrolled-logins <NUM_LOGINS> \
-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、您可以使用 `security login duo delete` 命令：

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` 命令：

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。您可以使用创建Duo组 `security login duo group create` 命令：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。

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> -exclude-users <USER1, USER2>
```

Duo组的名称必须与Active Directory、LDAP或本地组匹配。使用可选指定的用户 `-exclude-users` 参数不会包含在Duo身份验证过程中。

查看Duo组

您可以使用查看现有Cisco Duo组条目 `security login duo group show` 命令：

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> -exclude-users <USER1, USER2>
```

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

删除Duo组

您可以使用删除Duo组条目 `security login duo group delete` 命令：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。

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 -vserver <STORAGE_VM_NAME> -is-duo-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 group modify -group-name <GROUP_NAME> -exclude-users
<USER1, USER2>
```

Duo组的名称必须与Active Directory、LDAP或本地组匹配。使用指定的用户 `-exclude-users` 参数不会包含在Duo身份验证过程中。

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"。

生成并安装 CA 签名的服务器证书概述

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` 用于生成证书签名请求(CSR)的命令、以及 `security certificate install` 命令以安装从证书颁发机构收到的回退证书。

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
```

以下命令将使用一个2048位专用密钥创建一个CSR、该密钥由"*LW_AT*` 25256`"散列函数生成、供一家公司的"`sit S"部门中的" oftware `s "组使用、该公司的自定义公用名为" erver1.companyname.com`"、位于美国加利福尼亚州的森尼韦尔。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-----
MIIBGjCBxQIBADBgMRQwEgYDVQQDEwtleGFtcGxlLmNvbTELMAkGA1UEBhMCVVMx
CTAHBgNVBAgTADEJMAcGA1UEBxMAMQkwBwYDVQQKEwAxCTAHBgNVBAsTADEPMA0G
CSqGSIb3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApT1nzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3a1woUsb13wfEvQnHVFNci
2ninsJ8CAwEAAaAAMA0GCSqGSIb3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----


Private Key :
-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBAPXFanNoJApT1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3a1woUsb13wfEvQnHVFNci2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/ehAiEA+oDbOooWlVvu
xj4aitxVBu6ByVckYU8LbsfeRNsZwD8CIQCbZ1/ENvmlJ/P7N9Exj2NCtEYxd0Q5
cwBZ5NfZeMBpwQIhAPk0KWQSLadGfsKO077itF+h9FGFNHbtuNTrVq4vPW3nAiAA
peMBQgEv28y2r8D4dkYzxcXmjzJluUSZSZ9c/wS6fA==
-----END RSA PRIVATE KEY-----

Note: Please 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` 命令以在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。

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
   ```

   有关完整的命令语法，请参见 "工作表"。

   > 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"`engData2`"上安装CA签名的服务器证书和中间证书。

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-----
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTADEJMAcGA1UECxMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhcHAuY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTADEJMAcGA1UECxMA
MQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAyXrK2sry
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLycsUdXA7hXhumHNpvF
C61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM7OtbUsgPKw+QCCh9dF1jmuQKeDr+wUMWknlDeGrfhILpzfJGHrLJ
z7UCIQDr8d3gOG71UyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuSl8U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEAr1mnrfYC8KwE9k7A0ylRzBLdUwK9
AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIg
aEMAzt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
-----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-----
MIIE+zCCBGSgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFRoZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECxMoR28gRGFkZHkgQ2xhc3MgMiBDZXJ0
-----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-----
```

```
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0
IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTLFZhbGlDZXJ0IENsYXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDExhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEWluZm9AdmFsaWNlcnQuY29tMB4XDTk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBAcTG1ZhbGlDZXJ0IFZhbGlkYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTLFZhbGlDZXJ0IENs
YXNzIDIgUG9saWN5IFZhbGlkYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDExhodHRw
-----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.
```

使用 System Manager 管理证书

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. 选择任意数字以查看有关某类证书的详细信息、或者选择 → 可打开包含所有类别信息的*Certificates*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 …
• 可信证书颁发机构 *	• [install-trusted-cert] • [删除可信证书颁发机构] • [续订可信证书颁发机构]
• 客户端 / 服务器证书 *	• [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]
• 本地证书颁发机构 *	• [创建新的本地证书颁发机构] • [使用本地证书颁发机构对证书进行签名] • [删除本地证书颁发机构] • [续订本地证书颁发机构]

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 … + Add 。
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 … ⋮ 在名称旁边，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 … ⋮ 在证书名称旁边，然后选择*Renew*。

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 … + Add 。
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 … ⋮ 在名称旁边，单击 * 删除 * 。

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 … ⋮ 在名称旁边，单击 * 续订 * 。

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 … + Add 。
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 … ⋮ 然后在名称旁边*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 … ⋮ 在名称旁边，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 … ⋮ 在名称旁边，单击 * 续订 * 。

配置 Active Directory 域控制器访问概述

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_tannel"、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 ） 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。	ONTAP 9.10.1
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_tannel"、以便对集群进行AD访问。

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`*

   有关完整的命令语法，请参见 "工作表"。

   > 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"`engData`"配置为身份验证通道。

   ```
   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。

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`*

   有关完整的命令语法，请参见 "工作表"。

   以下命令会在域"`example.com`" for SVM"`engData`"上创建一个名为"`ADSERVER1`"的计算机帐户。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:
```

配置 LDAP 或 NIS 服务器访问概述

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

- 您必须已安装 "CA 签名的服务器数字证书" 在 SVM 上。
- 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 。

有关完整的命令语法，请参见 "工作表"。

以下命令会在SVM"`engData`"上创建名为"`corp`"的LDAP客户端配置。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。客户端与服务器之间的通信使用 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
```

> 从ONTAP 9.2开始、此字段为 `-ldap-servers` 替换字段 `-servers`。此新字段可以使用 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`

   有关完整的命令语法，请参见 "工作表"。

   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
```

> 从ONTAP 9.2开始、 `vserver services name-service ldap create` 命令会执行自动配置验证、并在ONTAP无法联系名称服务器时报告错误消息。

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".                                              |
```

从 ONTAP 9.2 开始，可以使用 name service check 命令。

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。

关于此任务

您可以创建多个 NIS 域。只能将一个NIS域设置为 `active` 一次。

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 -active true|false -nis-servers` *`NIS_server_IPs`*

   有关完整的命令语法，请参见 "工作表"。

   > 从ONTAP 9.2开始、此字段为 `-nis-servers` 替换字段 `-servers`。此新字段可以使用NIS服务器的主机名或IP地址。

   以下命令会在SVM"`engData`"上创建NIS域配置。NIS域 `nisdomain` 在创建时处于活动状态、并与IP地址为192.0.2.180的NIS服务器通信。

   ```
   cluster1::>vserver services name-service nis-domain create
   -vserver engData -domain nisdomain -active true -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`*

   有关完整的命令语法，请参见 "工作表"。

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

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

更改管理员密码

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` 命令以修改与给定角色关联的帐户的密码规则。有关详细信息，请参见 "命令参考"。

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SVM`vs1.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:
   ```

锁定和解锁管理员帐户

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
   ```

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
   ```

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` 命令来执行这些任务。

从长期来看，您还可以执行以下附加步骤：

- 使用 `security ssh modify` 命令以限制所有新创建的SVM的失败登录尝试次数。
- 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。

对管理员帐户密码强制执行 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。

诊断并更正文件访问问题

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 ⌄ 在结果表的左列中查看文件访问权限。