身份验证和访问控制

ONTAP 9

NetApp
April 24, 2024

目录

身份验证和访问控制

身份验证和访问控制概述

您可以管理ONTAP集群身份验证以及对ONTAP Web服务的访问控制。

您可以使用System Manager或命令行界面控制并保护客户端和管理员对集群和存储的访问。

如果您使用的是经典 System Manager （仅适用于 ONTAP 9.7 及更早版本），请参见 "System Manager 经典版（ ONTAP 9.0 到 9.7 ）"

客户端身份验证和授权

ONTAP 通过向可信源验证客户端计算机和用户的身份来对其进行身份验证。ONTAP 通过将用户凭据与文件或目录上配置的权限进行比较来授权用户访问文件或目录。

管理员身份验证和 **RBAC**

管理员可以使用本地或远程登录帐户向集群和 Storage VM 进行身份验证。基于角色的访问控制（ Role-Based Access Control ， RBAC ）可确定管理员有权访问的命令。

管理管理员身份验证和**RBAC**

使用 **CLI** 进行管理员身份验证和 **RBAC** 概述

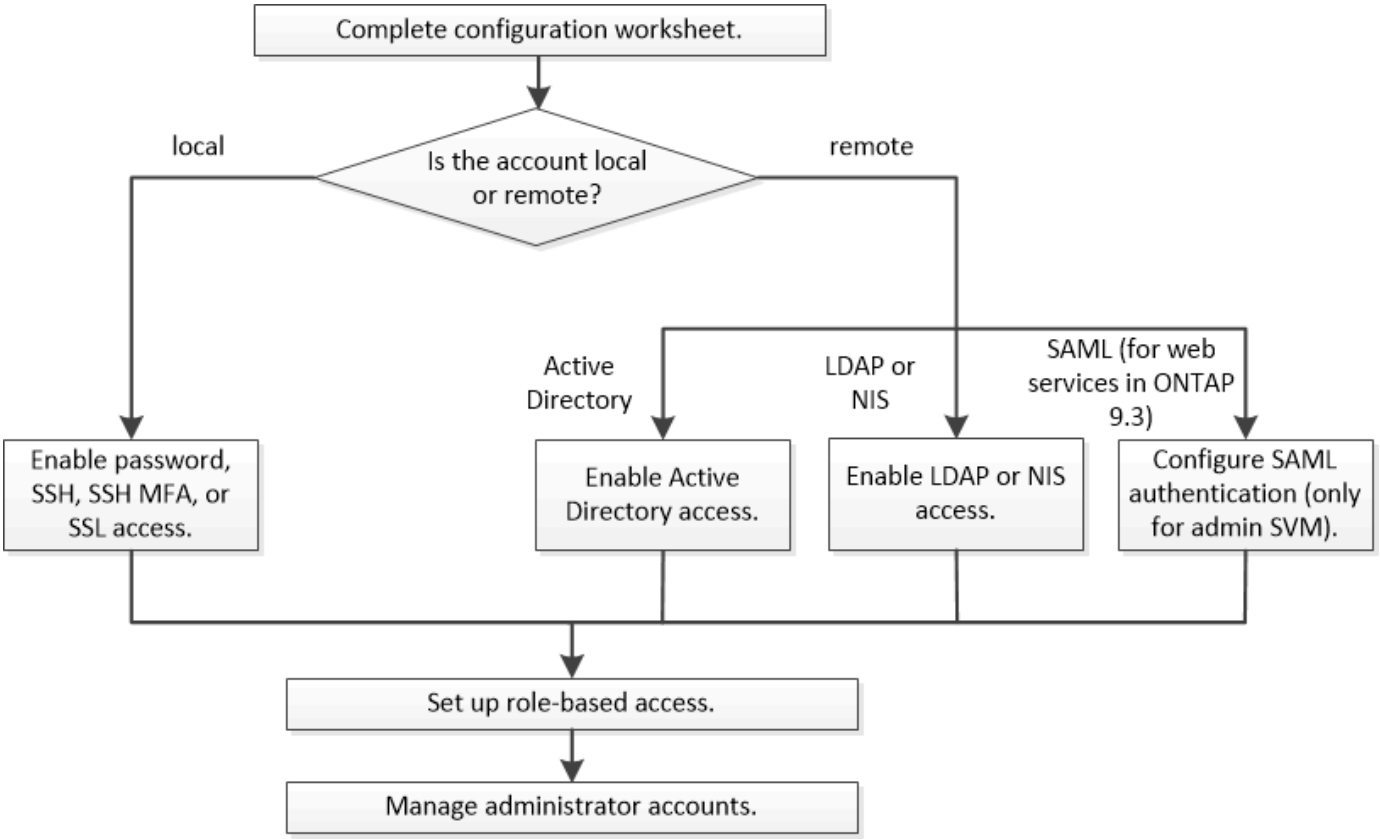
您可以为 ONTAP 集群管理员和 Storage Virtual Machine （ SVM ）管理员启用登录帐户。您还可以使用基于角色的访问控制（ Role-Based Access Control ， RBAC ）定义管理员的功能。

您可以通过以下方式启用登录帐户和 RBAC：

- 您希望使用 ONTAP 命令行界面（ CLI ），而不是 System Manager 或自动化脚本编写工具。
- 您希望使用最佳实践，而不是浏览每个可用选项。
- 您不使用 SNMP 收集有关集群的信息。

管理员身份验证和 **RBAC** 工作流

您可以为本地管理员帐户或远程管理员帐户启用身份验证。本地帐户的帐户信息位于存储系统上，远程帐户的帐户信息位于其他位置。每个帐户可以具有一个预定义角色或一个自定义角色。



您可以启用本地管理员帐户以使用以下类型的身份验证访问管理 Storage Virtual Machine （ SVM ）或数据 SVM：

- Password
- SSH 公有密钥
- SSL证书
- SSH 多因素身份验证（ MFA ）

  从 ONTAP 9.3 开始，支持使用密码和公有密钥进行身份验证。

您可以通过以下类型的身份验证使远程管理员帐户能够访问管理 SVM 或数据 SVM：

- Active Directory
- SAML 身份验证（仅适用于管理 SVM ）

  从 ONTAP 9.3 开始，可以使用安全断言标记语言（ SAML ）身份验证通过以下任一 Web 服务访问管理 SVM： 服务处理器基础架构， ONTAP API 或 System Manager 。

- 从 ONTAP 9.4 开始， SSH MFA 可用于 LDAP 或 NIS 服务器上的远程用户。支持使用 nsswitch 和公有密钥进行身份验证。

用于管理员身份验证和 **RBAC** 配置的工作表

在创建登录帐户和设置基于角色的访问控制（ Role-Based Access Control ， RBAC ）之前，您应收集配置工作表中每个项目的信息。

创建或修改登录帐户

您可以在中提供这些值 `security login create` 命令。您可以在中提供相同的值 `security login modify` 命令。

字段	Description	您的价值
`-vserver`	帐户访问的Storage VM的名称。默认值为集群的管理Storage VM的名称。	
`-user-or-group-name`	帐户的用户名或组名称。通过指定组名称，可以访问组中的每个用户。您可以将一个用户名或组名称与多个应用程序相关联。	
`-application`	用于访问Storage VM的应用程序： • `http` • `ontapi` • `snmp` • `ssh`	
`-authmethod`	用于对帐户进行身份验证的方法： • `cert` 用于SSL证书身份验证 • `domain` 用于Active Directory身份验证 • `nsswitch` 用于LDAP或NIS身份验证 • `password` 用于用户密码身份验证 • `publickey` 用于公共密钥身份验证 • `community` 用于SNMP社区字符串 • `usm` 适用于SNMP用户安全模型 • `saml` 用于安全断言标记语言(SAML)身份验证	

-remote-switch-ipaddress	远程交换机的 IP 地址。远程交换机可以是由集群交换机运行状况监控器（CSHM）监控的集群交换机，也可以是由 MetroCluster 运行状况监控器（MCC-HM）监控的光纤通道（FC）交换机。此选项仅在应用程序为时适用 snmp 身份验证方法为 usm。	
-role	分配给帐户的访问控制角色： • 对于集群(管理Storage VM)、默认值为 admin。 • 对于数据Storage VM、默认值为 vsadmin。	
-comment	（可选）帐户的描述性文本。文本应用双引号（"）括起来。	
-is-ns-switch-group	帐户是LDAP组帐户还是NIS组帐户(yes 或 no）。	
-second-authentication -method	多因素身份验证的第二种身份验证方法： • none 如果不使用多因素身份验证、则为默认值 • publickey 用于公共密钥身份验证 authmethod 是password或nsswitch • password 用于用户密码身份验证 authmethod 是公共密钥 • nsswitch 当auth方法为publickey时用于用户密码身份验证 身份验证顺序始终是公有密钥和密码。	
-is-ldap-fastbind	从ONTAP 9.11.1开始、如果设置为true、则会为nsswitch身份验证启用LDAP快速绑定；默认值为false。要使用LDAP快速绑定、请 -authentication-method 值必须设置为 nsswitch。 "了解用于nsswitch身份验证的LDAP快速绑定。"	

配置**Cisco Duo**安全信息

您可以在中提供这些值 `security login duo create` 命令。

字段	Description	您的价值
`-vserver`	要应用Duo身份验证设置的Storage VM (在ONTAP命令行界面中称为Vserver)。	
`-integration-key`	您的集成密钥、在向Duo注册SSH应用程序时获得。	
`-secret-key`	您的机密密钥、在向Duo注册SSH应用程序时获得。	
`-api-host`	向Duo注册SSH应用程序时获得的API主机名。例如： `api-<HOSTNAME>.duosecurity.com`	
`-fail-mode`	如果出现服务或配置错误、导致无法进行Duo身份验证、则操作将失败 `safe` (允许访问)或 `secure` (拒绝访问)。默认值为 `safe`，这意味着如果Duo身份验证因诸如Duo API服务器不可访问等错误而失败，则会绕过它。	
`-http-proxy`	使用指定的HTTP代理。如果HTTP代理需要身份验证、请在代理URL中包含凭据。例如： `http-proxy=http://username:password@proxy.example.org:8080`	

-autopush	两者之一 true 或 false。默认值为 false。条件 true，Duo会自动向用户的电话发送推入登录请求，如果推入不可用，则恢复到电话呼叫。请注意、这会有效地禁用密码身份验证。条件 false，则系统将提示用户选择一种身份验证方法。 配置时 autopush = true，我们建议设置 max-prompts = 1。	
-max-prompts	如果用户无法通过第二个因素进行身份验证、Duo会提示用户再次进行身份验证。此选项设置Duo拒绝访问前显示的最大提示数。必须为 1， 2`或 `3。默认值为 1。 例如、何时 max-prompts = 1，则用户需要在第一个提示符处成功进行身份验证，而如果 max-prompts = 2，如果用户在初始提示符处输入的信息不正确，则会再次提示他/她进行身份验证。 配置时 autopush = true，我们建议设置 max-prompts = 1。 为了获得最佳体验、仅使用公共密钥身份验证的用户将始终拥有 max-prompts 设置为 1。	
-enabled	启用Duo双重身份验证。设置为 true 默认情况下。启用后、在SSH登录期间会根据配置的参数强制实施Duo双重身份验证。禁用Duo时(设置为 false)、则会忽略Duo身份验证。	

定义自定义角色

您可以在中提供这些值 security login role create 命令。

字段	Description	您的价值
-vserver	(可选)与角色关联的Storage VM的名称(在ONTAP命令行界面中称为Vserver)。	
-role	角色的名称。	

-cmddirname	角色授予访问权限的命令或命令目录。您应将命令子目录名称用双引号（"）括起来。例如： "volume snapshot"。您必须输入 DEFAULT 指定所有命令目录。	
-access	（可选）角色的访问级别。对于命令目录： • none (自定义角色的默认值)拒绝访问命令目录中的命令 • readonly 授予对的访问权限 show 命令目录及其子目录中的命令 • all 授予对命令目录及其子目录中所有命令的访问权限 对于_noninsic commands_(不以 create， modify， delete`或 `show）： • none (自定义角色的默认值)拒绝访问命令 • readonly 不适用 • all 授予对命令的访问权限 要授予或拒绝对内部命令的访问权限，必须指定命令目录。	
-query	（可选）用于筛选访问级别的查询对象，该对象以命令或命令目录中某个命令的有效选项的形式指定。您应将查询对象用双引号（"）括起来。例如、如果命令目录为 volume，查询对象 "-aggr aggr0" 将启用对的访问 aggr0 仅聚合。	

将公有密钥与用户帐户关联

您可以在中提供这些值 security login publickey create 命令。

字段	Description	您的价值
-vserver	(可选)帐户访问的Storage VM的名称。	

`-username`	帐户的用户名。默认值、 `admin`，这是集群管理员的默认名称。	
`-index`	公有密钥的索引编号。如果密钥是为帐户创建的第一个密钥，则默认值为 0 ；否则，默认值将比帐户的最高现有索引编号多一个。	
`-publickey`	OpenSSH 公有密钥。您应将密钥用双引号（ " ）括起来。	
`-role`	分配给帐户的访问控制角色。	
`-comment`	（可选）公有密钥的描述性文本。文本应用双引号（ " ）括起来。	
`-x509-certificate`	(可选)从ONTAP 9.13.1开始、可用于管理与SSH公共密钥的X.509证书关联。 将X.509证书与SSH公共密钥关联后、ONTAP会在SSH登录时检查此证书是否有效。如果已过期或已撤销、则不允许登录、并禁用关联的SSH公共密钥。可能值： • `install`：安装指定的PEM编码X.509证书并将其与SSH公共密钥关联。包括要安装的证书的全文。 • `modify`：使用指定证书更新现有PEM编码的X.509证书，并将其与SSH公共密钥关联。包括新证书的全文。 • `delete`：删除与SSH公共密钥的现有X.509证书关联。	

安装 **CA** 签名的服务器数字证书。

您可以在中提供这些值 `security certificate generate-csr` 命令。

字段	Description	您的价值
`-common-name`	证书的名称，即完全限定域名（ FQDN ）或自定义公用名。	

-size	专用密钥中的位数。值越高，密钥越安全。默认值为 2048。可能值为 512， 1024， 1536，和 2048。	
-country	Storage VM所在的国家/地区、以双字母代码表示。默认值为 US。有关代码列表，请参见手册页。	
-state	Storage VM的州或省。	
-locality	Storage VM的位置。	
-organization	Storage VM的组织。	
-unit	Storage VM组织中的单位。	
-email-addr	Storage VM的联系人管理员的电子邮件地址。	
-hash-function	用于对证书签名的加密哈希函数。默认值为 SHA256。可能值为 SHA1， SHA256，和 MD5。	

您可以在中提供这些值 security certificate install 命令。下表仅显示与帐户配置相关的选项。

字段	Description	您的价值
-vserver	要安装证书的Storage VM的名称。	
-type	证书类型： • server 服务器证书和中间证书 • client-ca SSL客户端根CA的公共密钥证书 • server-ca ONTAP为客户端的SSL服务器的根CA的公共密钥证书 • client 作为SSL客户端的ONTAP的自签名或CA签名数字证书和专用密钥	

配置 **Active Directory** 域控制器访问

您可以在中提供这些值 security login domain-tunnel create 命令。

字段	Description	您的价值
`-vserver`	已配置SMB服务器的Storage VM的名称。	

您可以在中提供这些值 `vserver active-directory create` 命令。

字段	Description	您的价值
`-vserver`	要创建Active Directory计算机帐户的Storage VM的名称。	
`-account-name`	计算机帐户的 NetBIOS 名称。	
`-domain`	完全限定域名（FQDN）。	
`-ou`	域中的组织单位。默认值为 `CN=Computers`。ONTAP 会将此值附加到域名中，以生成 Active Directory 可分辨名称。	

配置 **LDAP** 或 **NIS** 服务器访问

您可以在中提供这些值 `vserver services name-service ldap client create` 命令。

下表仅显示与帐户配置相关的选项：

字段	Description	您的价值
`-vserver`	客户端配置中的Storage VM的名称。	
`-client-config`	客户端配置的名称。	
`-ldap-servers`	客户端所连接的LDAP服务器的IP地址和主机名列表、以英文逗号分隔。	
`-schema`	客户端用于进行 LDAP 查询的模式。	

`-use-start-tls`	客户端是否使用Start TLS对与LDAP服务器的通信进行加密（`true` 或 `false`）。 仅支持使用Start TLS访问数据Storage VM。不支持访问管理Storage VM。	

您可以在中提供这些值 `vserver services name-service ldap create` 命令。

字段	Description	您的价值
`-vserver`	要与客户端配置关联的Storage VM的名称。	
`-client-config`	客户端配置的名称。	
`-client-enabled`	Storage VM是否可以使用LDAP客户端配置 (`true` 或 `false`）。	

您可以在中提供这些值 `vserver services name-service nis-domain create` 命令。

字段	Description	您的价值
`-vserver`	要在其中创建域配置的Storage VM的名称。	
`-domain`	域的名称。	
`-active`	域是否处于活动状态 (`true` 或 `false`）。	
`-servers`	• ONTAP 9.0 ， 9.1*：域配置所使用的 NIS 服务器的 IP 地址列表，以英文逗号分隔。	
`-nis-servers`	域配置所使用的NIS服务器的IP地址和主机名的逗号分隔列表。	

您可以在中提供这些值 `vserver services name-service ns-switch create` 命令。

字段	Description	您的价值

`-vserver`	要配置名称服务查找顺序的Storage VM的名称。	
`-database`	名称服务数据库： • `hosts` 用于文件和DNS名称服务 • `group` 适用于文件、LDAP和NIS名称服务 • `passwd` 适用于文件、LDAP和NIS名称服务 • `netgroup` 适用于文件、LDAP和NIS名称服务 • `namemap` 用于文件和LDAP名称服务	
`-sources`	查找名称服务源的顺序（在逗号分隔列表中）： • `files` • `dns` • `ldap` • `nis`	

配置 **SAML** 访问

从ONTAP 9.3开始、您可以在中提供这些值 `security saml-sp create` 命令以配置SAML身份验证。

字段	Description	您的价值
`-idp-uri`	可从中下载 IdP 元数据的身份提供程序（ Identity Provider ， IdP ）主机的 FTP 地址或 HTTP 地址。	
`-sp-host`	SAML 服务提供程序主机（ ONTAP 系统）的主机名或 IP 地址。默认情况下，使用集群管理 LIF 的 IP 地址。	
`-cert-ca` 和 `-cert-serial`或`-cert-common-name`	服务提供商主机（ ONTAP 系统）的服务器证书详细信息。您可以输入服务提供商的证书颁发机构(CA)和证书的序列号、也可以输入服务器证书通用名称。	

-verify-metadata-server	是否必须验证Idp元数据服务器的身份 true 或 false）。最佳做法是始终将此值设置为 true。	

创建登录帐户

创建登录帐户概述

您可以启用本地或远程集群和 SVM 管理员帐户。本地帐户是指帐户信息，公有密钥或安全证书驻留在存储系统上的帐户。AD 帐户信息存储在域控制器上。LDAP 和 NIS 帐户位于 LDAP 和 NIS 服务器上。

集群和 **SVM** 管理员

集群管理员 _ 访问集群的管理 SVM 。具有预留名称的管理SVM和集群管理员 admin 在设置集群时自动创建。

使用默认值的集群管理员 admin 角色可以管理整个集群及其资源。集群管理员可以根据需要创建具有不同角色的其他集群管理员。

SVM 管理员 _ 访问数据 SVM 。集群管理员根据需要创建数据 SVM 和 SVM 管理员。

为SVM管理员分配了 vsadmin 默认情况下的角色。集群管理员可以根据需要为 SVM 管理员分配不同的角色。

命名约定

以下通用名称不能用于远程集群和SVM管理员帐户：

- "ADM"
- "箱"
- "CLI"
- "守护进程"
- "FTP"
- "游戏"
- "暂停"
- "LP"
- "邮件"
- "手动"
- "纳鲁特"
- " NetApp "
- "新闻"
- "无人"
- "操作员"

- "根"
- "停机"
- "ssshd"
- "同步"
- "系统"
- "uucp"
- "www"

已合并角色

如果为同一用户启用多个远程帐户，则会为该用户分配为这些帐户指定的所有角色的联合。也就是说、如果为分配了LDAP或NIS帐户 `vsadmin` 角色、并为同一用户的AD组帐户分配 `vsadmin-volume` 角色、则AD用户使用更多功能登录 `vsadmin` 功能。这些角色称为 *migered*.

启用本地帐户访问

启用本地帐户访问概述

本地帐户是指帐户信息，公有密钥或安全证书驻留在存储系统上的帐户。您可以使用 `security login create` 命令以使本地帐户能够访问管理员或数据SVM。

启用密码帐户访问

您可以使用 `security login create` 命令以使管理员帐户能够使用密码访问管理员或数据SVM。输入命令后，系统将提示您输入密码。

关于此任务

如果您不确定要分配给登录帐户的访问控制角色、可以使用 `security login modify` 命令以稍后添加此角色。

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 允许本地管理员帐户使用密码访问 SVM：

   ```
   security login create -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   有关完整的命令语法，请参见 "工作表"。

   以下命令将启用集群管理员帐户 `admin1` 和预定义的 `backup` 用于访问管理SVM的角色`engCluster` 使用密码。输入命令后，系统将提示您输入密码。

```
cluster1::>security login create -vserver engCluster -user-or-group-name
admin1 -application ssh -authmethod password -role backup
```

启用 **SSH** 公有密钥帐户

您可以使用 `security login create` 命令以使管理员帐户能够使用SSH公共密钥访问管理员或数据SVM。

关于此任务

- 您必须先将公有密钥与帐户关联，然后帐户才能访问 SVM 。

  将公有密钥与用户帐户关联

  您可以在启用帐户访问之前或之后执行此任务。

- 如果您不确定要分配给登录帐户的访问控制角色、可以使用 `security login modify` 命令以稍后添加此角色。

如果要在集群上启用FIPS模式、则必须使用支持的密钥类型重新配置不支持密钥算法的现有SSH公共密钥帐户。 在启用FIPS之前、应重新配置这些帐户、否则管理员身份验证将失败。

下表显示了ONTAP SSH连接支持的主机密钥类型算法。 这些密钥类型不适用于配置SSH公共身份验证。

ONTAP 版本	FIPS模式支持的密钥类型	非FIPS模式支持的密钥类型
9.11.1及更高版本	ECDSA-SHA2-nistp256	ECDSA-SHA2-nistp256 RSA-SHA2-512 RSA-SHA2-256 SSS-ed25519及更高 SSS-DSS SSS-RSA
9.10.1及更早版本	ECDSA-SHA2-nistp256 SSS-ed25519	ECDSA-SHA2-nistp256 SSS-ed25519及更高 SSS-DSS SSS-RSA

从ONTAP 9.11.1开始、不再支持ssh-ed25519主机密钥算法。

有关详细信息，请参见 "使用 FIPS 配置网络安全性"。

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 允许本地管理员帐户使用 SSH 公有密钥访问 SVM ：

security login create -vserver *SVM_name* -user-or-group-name user_or_group_name -application *application* -authmethod *authentication_method* -role *role* -comment *comment*

有关完整的命令语法，请参见 "工作表"。

以下命令将启用SVM管理员帐户 `svmadmin1` 和预定义的 `vsadmin-volume` 访问SVM的角色`engData1` 使用SSH公共密钥：

```
cluster1::>security login create -vserver engData1 -user-or-group-name
svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
```

完成后

如果您尚未将公有密钥与管理员帐户关联，则必须先将其关联，然后该帐户才能访问 SVM 。

将公有密钥与用户帐户关联

启用多因素身份验证(MFA)帐户

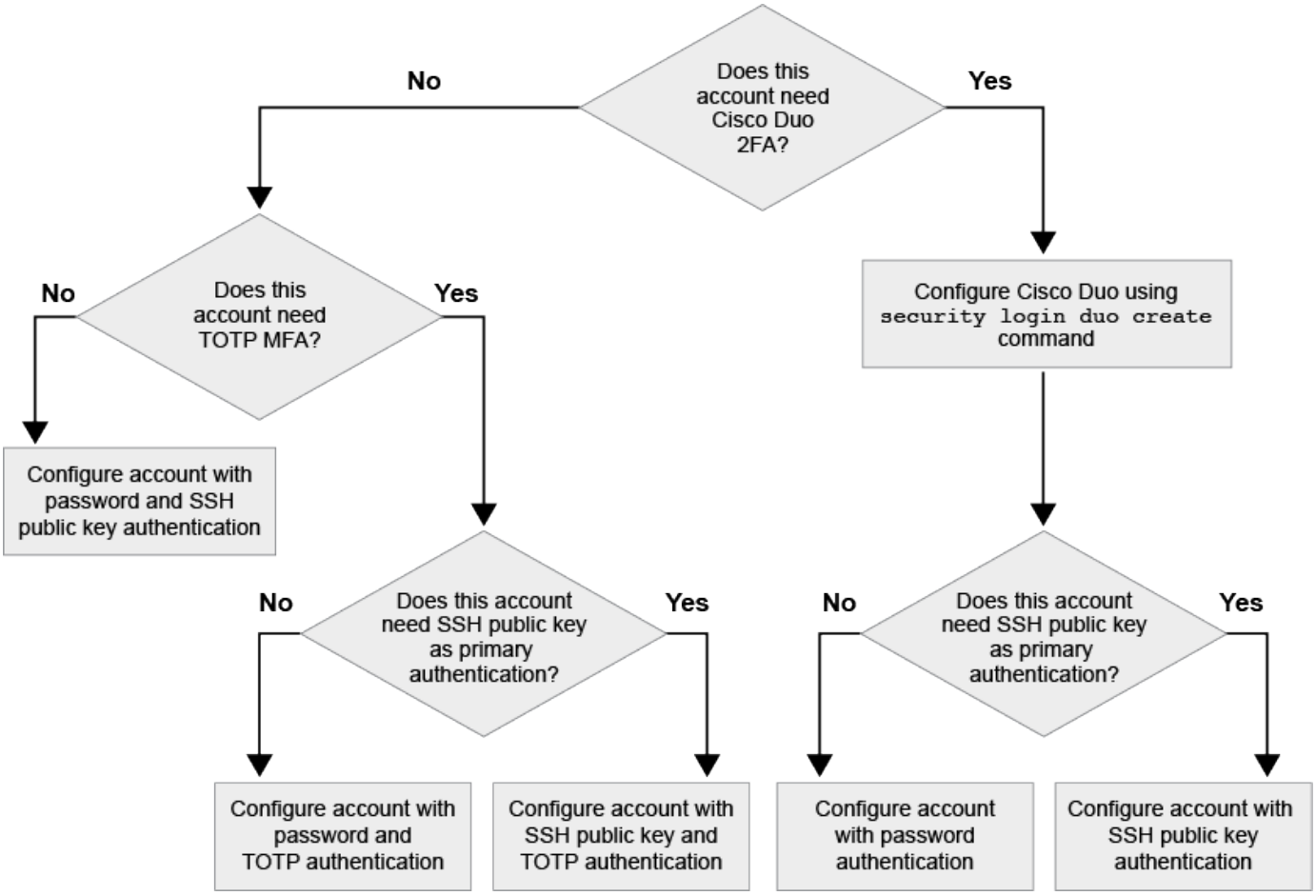
多因素身份验证概述

通过多因素身份验证(MFA)、您可以要求用户提供两种身份验证方法来登录到管理员或数据Storage VM、从而增强安全性。

根据您的ONTAP版本、您可以组合使用SSH公共密钥、用户密码和基于时间的一次性密码(TOTP)进行多因素身份验证。启用并配置Cisco Duo (ONTAP 9.14.1及更高版本)时、它可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。

可用开头为...	第一种身份验证方法	第二种身份验证方法
ONTAP 9.14.1	SSH 公有密钥	TOTP
	用户密码	TOTP
	SSH 公有密钥	Cisco Duo
	User password	Cisco Duo
ONTAP 9.13.1	SSH 公有密钥	TOTP
	User password	TOTP
ONTAP 9.3	SSH 公有密钥	User password

如果配置了MFA、则集群管理员必须先启用本地用户帐户、然后该帐户必须由本地用户配置。



启用多因素身份验证

通过多因素身份验证(MFA)、您可以要求用户提供两种身份验证方法来登录到管理员或数据SVM、从而增强安全性。

关于此任务

- 您必须是集群管理员才能执行此任务。
- 如果您不确定要分配给登录帐户的访问控制角色、可以使用 `security login modify` 命令以稍后添加此角色。

  "修改分配给管理员的角色"

- 如果您使用公共密钥进行身份验证、则必须先将此公共密钥与此帐户关联、然后此帐户才能访问SVM。

  "将公有密钥与用户帐户关联"

  您可以在启用帐户访问之前或之后执行此任务。

- 从ONTAP 9.12.1开始、您可以使用FID02 (快速身份联机)或个人身份验证(PIV)身份验证标准对SSH客户端MFA使用优键硬件身份验证设备。

使用**SSH**公共密钥和用户密码启用**MFA**

从ONTAP 9.3开始、集群管理员可以设置本地用户帐户、以便使用SSH公共密钥和用户密码登录MFA。

1. 使用SSH公共密钥和用户密码在本地用户帐户上启用MFA：

```
security login create -vserver <svm_name> -user-or-group-name
<user_name> -application ssh -authentication-method <password|publickey>
-role admin -second-authentication-method <password|publickey>
```

以下命令需要SVM管理员帐户 `admin2` 和预定义的 `admin` 用于登录到SVM的角色`engData1` 使用SSH公共密钥和用户密码：

```
cluster-1::> security login create -vserver engData1 -user-or-group-name
admin2 -application ssh -authentication-method publickey -role admin
-second-authentication-method password

Please enter a password for user 'admin2':
Please enter it again:
Warning: To use public-key authentication, you must create a public key
for user "admin2".
```

使用**TOTP**启用**MFA**

从ONTAP 9.13.1开始、您可以通过要求本地用户同时使用SSH公共密钥或用户密码以及基于时间的一次性密码(TOTP)登录到管理员或数据SVM来增强安全性。使用TOTP为帐户启用MFA后、本地用户必须登录到 "完成配置"。

TOTP是一种计算机算法、使用当前时间生成一次性密码。 如果使用TOTP、则它始终是继SSH公共密钥或用户密码之后的第二种身份验证形式。

开始之前

您必须是存储管理员才能执行这些任务。

步骤

您可以将MFA设置为、并将用户密码或SSH公共密钥作为第一种身份验证方法、将TOTP作为第二种身份验证方法。

使用用户密码和**TOTP**启用**MFA**

1. 使用用户密码和TOTP为用户帐户启用多因素身份验证。

   新用户帐户

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   用于现有用户帐户

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

2. 验证是否已启用具有TOTP的MFA：

   ```
   security login show
   ```

使用**SSH**公共密钥和**TOTP**启用**MFA**

1. 使用SSH公共密钥和TOTP为用户帐户启用多因素身份验证。

   新用户帐户

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   用于现有用户帐户

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

2. 验证是否已启用具有TOTP的MFA：

```
security login show
```

完成后

- 如果您尚未将公有密钥与管理员帐户关联，则必须先将其关联，然后该帐户才能访问 SVM 。

  "将公有密钥与用户帐户关联"

- 本地用户必须登录才能使用TOTP完成MFA配置。

  "使用TOTP配置MFA的本地用户帐户"

相关信息

了解更多信息 "ONTAP 9中的多因素身份验证(TR-4647)"。

使用**TOTP**配置**MFA**的本地用户帐户

从ONTAP 9.13.1开始、可以使用基于时间的一次性密码(TOTP)为用户帐户配置多因素身份验证(MFA)。

开始之前

- 存储管理员必须执行此操作 "使用TOTP启用MFA" 作为用户帐户的第二种身份验证方法。
- 您的主用户帐户身份验证方法应为用户密码或公共SSH密钥。
- 您必须将TOTP应用程序配置为与智能手机配合使用、并创建TOTP机密密钥。

  各种身份验证程序应用程序(如Google身份验证程序)均支持TOTP。

步骤

1. 使用当前身份验证方法登录到您的用户帐户。

   您当前的身份验证方法应为用户密码或SSH公共密钥。

2. 在您的帐户上创建TOTP配置：

   ```
   security login totp create -vserver "<svm_name>" -username
   "<account_username >"
   ```

3. 验证是否已在您的帐户上启用TOTP配置：

   ```
   security login totp show -vserver "<svm_name>" -username
   "<account_username>"
   ```

重置**TOTP**机密密钥

为了保护您的帐户安全、如果您的TOTP机密密钥泄露或丢失、您应禁用它并创建一个新密钥。

如果您的密钥已损坏、请重置**TOTP**

如果您的TOTP机密密钥已泄露、但您仍可访问该密钥、则可以删除此泄露密钥并创建一个新密钥。

1. 使用您的用户密码或SSH公共密钥以及泄露的TOTP机密密钥登录到您的用户帐户。
2. 删除已泄露的TOTP机密密钥：

```
security login totp delete -vserver <svm_name> -username
<account_username>
```

3. 创建新的TOTP密钥：

```
security login totp create -vserver <svm_name> -username
<account_username>
```

4. 验证是否已在您的帐户上启用TOTP配置：

```
security login totp show -vserver <svm_name> -username
<account_username>
```

如果密钥丢失、请重置**TOTP**

如果您的TOTP机密密钥丢失、请与您的存储管理员联系以获取 "禁用密钥"。禁用密钥后、您可以使用第一种身份验证方法登录并配置新的TOTP。

开始之前

存储管理员必须禁用TOTP机密密钥。
如果您没有存储管理员帐户、请与存储管理员联系以禁用此密钥。

步骤

1. 存储管理员禁用TOTP密钥后、使用主身份验证方法登录到本地帐户。
2. 创建新的TOTP密钥：

```
security login totp create -vserver <svm_name> -username
<account_username >
```

3. 验证是否已在您的帐户上启用TOTP配置：

```
security login totp show -vserver <svm_name> -username
<account_username>
```

禁用本地帐户的TOTP机密密钥

如果本地用户丢失了基于时间的一次性密码(TOTP)密钥、则存储管理员必须先禁用丢失的密钥、然后用户才能创建新的TOTP密钥。

关于此任务

只能使用集群管理员帐户执行此任务。

步骤

1. 禁用TOTP密钥：

```
security login totp delete -vserver "<svm_name>" -username
"<account_username>"
```

启用 SSL 证书帐户

您可以使用 `security login create` 命令以使管理员帐户能够使用SSL证书访问管理员或数据SVM。

关于此任务

- 您必须先安装 CA 签名的服务器数字证书，帐户才能访问 SVM 。

  生成并安装 CA 签名的服务器证书

  您可以在启用帐户访问之前或之后执行此任务。

- 如果您不确定要分配给登录帐户的访问控制角色、可以稍后使用添加此角色 `security login modify` 命令：

  修改分配给管理员的角色

> 对于集群管理员帐户、支持通过证书身份验证 `http`， `ontapi`，和 `rest` 应用程序。对于SVM管理员帐户、只有支持使用证书身份验证 `ontapi` 和 `rest` 应用程序。

步骤

1. 允许本地管理员帐户使用 SSL 证书访问 SVM ：

   ```
   security login create -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   有关完整的命令语法，请参见 "按版本显示 ONTAP 手册页"。

以下命令将启用SVM管理员帐户 `svmadmin2` 使用默认值 `vsadmin` 访问SVM的角色`engData2` 使用SSL数字证书。

```
cluster1::>security login create -vserver engData2 -user-or-group-name
svmadmin2 -application ontapi -authmethod cert
```

完成后

如果您尚未安装 CA 签名的服务器数字证书，则必须先安装此证书，然后帐户才能访问 SVM 。

生成并安装 CA 签名的服务器证书

启用 **Active Directory** 帐户访问

您可以使用 `security login create` 命令以使Active Directory (AD)用户或组帐户能够访问管理员或数据SVM。AD 组中的任何用户都可以使用分配给该组的角色访问 SVM 。

关于此任务

- 您必须先配置对集群或 SVM 的 AD 域控制器访问，然后帐户才能访问 SVM 。

  配置 Active Directory 域控制器访问

  您可以在启用帐户访问之前或之后执行此任务。

- 从ONTAP 9.13.1开始、您可以使用SSH公共密钥作为具有AD用户密码的主身份验证方法或二级身份验证方法。

  如果选择使用SSH公共密钥作为主身份验证、则不会进行AD身份验证。

- 从ONTAP 9.11.1开始、您可以使用 "用于nsswitch身份验证的LDAP快速绑定" AD LDAP服务器是否支持此功能。
- 如果您不确定要分配给登录帐户的访问控制角色、可以使用 `security login modify` 命令以稍后添加此角色。

  修改分配给管理员的角色

> 只有支持AD组帐户访问 `SSH`， `ontapi`，和 `rest` 应用程序。SSH公共密钥身份验证不支持AD组、而SSH公共密钥身份验证通常用于多因素身份验证。

开始之前

- 在 AD 域控制器上，集群时间必须在 5 分钟内同步到。
- 您必须是集群管理员才能执行此任务。

步骤

1. 启用 AD 用户或组管理员帐户以访问 SVM ：

   对于**AD**用户：

ONTAP 版本	主身份验证	二级身份验证	命令
9.13.1及更高版本	公共密钥	无	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role>`

9.13.1及更高版本	domain	公共密钥	新用户
			`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`
			对于现有用户
			`security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`

9.0及更高版本	domain	无	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

对于广告组：

ONTAP 版本	主身份验证	二级身份验证	命令
9.0及更高版本	domain	无	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

有关完整的命令语法，请参见 "用于管理员身份验证和RBAC配置的工作表"

完成后

如果您尚未配置对集群或 SVM 的 AD 域控制器访问，则必须先配置此访问权限，然后帐户才能访问此 SVM 。

配置 Active Directory 域控制器访问

启用 **LDAP** 或 **NIS** 帐户访问

您可以使用 `security login create` 命令以使LDAP或NIS用户帐户能够访问管理员或数据SVM。如果尚未配置对 SVM 的 LDAP 或 NIS 服务器访问，则必须先配置此访问权限，然后帐户才能访问此 SVM 。

关于此任务

- 不支持组帐户。
- 您必须先配置对 SVM 的 LDAP 或 NIS 服务器访问，然后帐户才能访问 SVM 。

  配置 LDAP 或 NIS 服务器访问

  您可以在启用帐户访问之前或之后执行此任务。

- 如果您不确定要分配给登录帐户的访问控制角色、可以使用 `security login modify` 命令以稍后添加此角色。

  修改分配给管理员的角色

- 从 ONTAP 9.4 开始，远程用户可通过 LDAP 或 NIS 服务器支持多因素身份验证（ Multifactor Authentication ， MFA ）。
- 从ONTAP 9.11.1开始、您可以使用 "用于nsswitch身份验证的LDAP快速绑定" 如果LDAP服务器支持此功能。
- 由于LDAP问题描述已知、因此不应使用 `':'` (冒号)字符(例如、 `gecos`， `userPassword`等)。否则，该用户的查找操作将失败。

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 启用 LDAP 或 NIS 用户或组帐户以访问 SVM：

   ```
   security login create -vserver SVM_name -user-or-group-name user_name
   -application application -authmethod nsswitch -role role -comment comment -is
   -ns-switch-group yes|no [-is-ldap-fastbind true]
   ```

   有关完整的命令语法，请参见 "工作表"。

   "创建或修改登录帐户"

   以下命令将启用LDAP或NIS集群管理员帐户 `guest2` 和预定义的 `backup` 用于访问管理SVM的角色`engCluster`。

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name
   guest2 -application ssh -authmethod nsswitch -role backup
   ```

2. 为 LDAP 或 NIS 用户启用 MFA 登录：

   ```
   security login modify -user-or-group-name rem_usr1 -application ssh
   -authentication-method nsswitch -role admin -is-ns-switch-group no -second
   -authentication-method publickey
   ```

   身份验证方法可以指定为 `publickey` 第二种身份验证方法为 `nsswitch`。

   以下示例显示了正在启用的 MFA 身份验证：

   ```
   cluster-1::*> security login modify -user-or-group-name rem_usr2
   -application ssh -authentication-method nsswitch -vserver
   cluster-1 -second-authentication-method publickey"
   ```

完成后

如果尚未配置对 SVM 的 LDAP 或 NIS 服务器访问，则必须先配置此访问权限，然后帐户才能访问此 SVM 。

配置 LDAP 或 NIS 服务器访问

管理访问控制角色

管理访问控制角色概述

分配给管理员的角色决定了管理员有权访问的命令。您可以在为管理员创建帐户时分配角色。您可以根据需要分配其他角色或定义自定义角色。

修改分配给管理员的角色

您可以使用 `security login modify` 命令以更改集群或SVM管理员帐户的角色。您可以分配预定义角色或自定义角色。

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 更改集群或 SVM 管理员的角色：

   ```
   security login modify -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   有关完整的命令语法，请参见 "工作表"。

   "创建或修改登录帐户"

   以下命令将更改AD集群管理员帐户的角色 `DOMAIN1\guest1` 到预定义的 `readonly` 角色。

   ```
   cluster1::>security login modify -vserver engCluster -user-or-group-name
   DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
   ```

   以下命令将更改AD组帐户中SVM管理员帐户的角色 `DOMAIN1\adgroup` 自定义 `vol_role` 角色。

   ```
   cluster1::>security login modify -vserver engData -user-or-group-name
   DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
   ```

定义自定义角色

您可以使用 `security login role create` 用于定义自定义角色的命令。您可以根据需要多次执行此命令，以实现要与角色关联的功能的精确组合。

关于此任务

- 角色（无论是预定义的还是自定义的）可以授予或拒绝对 ONTAP 命令或命令目录的访问权限。

  命令目录 (`volume`(例如)是一组相关命令和命令子目录。除非本操作步骤中所述，否则授予或拒绝对命令目录的访问权限将授予或拒绝对该目录及其子目录中的每个命令的访问权限。

- 特定命令访问或子目录访问将覆盖父目录访问。

  如果使用命令目录定义角色，然后为某个特定命令或父目录的子目录再次定义不同的访问级别，则为该命令或子目录指定的访问级别将覆盖父级的访问级别。

> 您不能为SVM管理员分配一个角色来访问仅对可用的命令或命令目录 `admin` 群集管理员—例如 `security` 命令目录。

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 定义自定义角色：

   ```
   security login role create -vserver SVM_name -role role -cmddirname
   command_or_directory_name -access access_level -query query
   ```

   有关完整的命令语法，请参见 "工作表"。

   以下命令用于授予 `vol_role` 对中命令的角色完全访问权限 `volume` 命令目录以及对中命令的只读访问权限 `volume snapshot` 子目录。

   ```
   cluster1::>security login role create -role vol_role -cmddirname
   "volume" -access all

   cluster1::>security login role create -role vol_role -cmddirname "volume
   snapshot" -access readonly
   ```

   以下命令用于授予 `SVM_storage` 对中的命令的只读角色访问权限 `storage` 命令目录、无法访问中的命令 `storage encryption` 子目录、以及对的完全访问权限 `storage aggregate plex offline` 非内在命令。

   ```
   cluster1::>security login role create -role SVM_storage -cmddirname
   "storage" -access readonly

   cluster1::>security login role create -role SVM_storage -cmddirname
   "storage encryption" -access none

   cluster1::>security login role create -role SVM_storage -cmddirname
   "storage aggregate plex offline" -access all
   ```

集群管理员的预定义角色

集群管理员的预定义角色应满足您的大多数需求。您可以根据需要创建自定义角色。默认情况下、系统会为集群管理员分配预定义的 `admin` 角色。

下表列出了集群管理员的预定义角色：

此角色 ...	具有此访问级别 ...	访问以下命令或命令目录
管理员	全部	所有命令目录 (`DEFAULT`)

admin-no-FSA (从ONTAP 9.12.1开始提供)	读 / 写	• 所有命令目录 (DEFAULT) • security login rest-role • security login role
只读	• security login rest-role create • security login rest-role delete • security login rest-role modify • security login rest-role show • security login role create • security login role create • security login role delete • security login role modify • security login role show • volume activity-tracking • volume analytics	无
volume file show-disk-usage	AutoSupport	全部
• set • system node autosupport	无	所有其他命令目录 (DEFAULT)
backup	全部	vserver services ndmp
-readonly	volume	无
所有其他命令目录 (DEFAULT)	-readonly	全部

• `security login password` 仅用于管理自己的用户帐户本地密码和密钥信息 • `set`	无	`security`
-readonly	所有其他命令目录 (`DEFAULT`)	无

> 。 `autosupport` 已将角色分配给预定义的 `autosupport` 帐户、由AutoSupport OnDemand使用。ONTAP会阻止您修改或删除 `autosupport` 帐户。ONTAP还会阻止您分配 `autosupport` 其他用户帐户的角色。

SVM 管理员的预定义角色

SVM 管理员的预定义角色应满足您的大多数需求。您可以根据需要创建自定义角色。默认情况下、系统会为SVM管理员分配预定义的 `vsadmin` 角色。

下表列出了 SVM 管理员的预定义角色：

Role name	功能
vsadmin	• 管理自己的用户帐户本地密码和密钥信息 • 管理卷，卷移动除外 • 管理配额， qtree ， Snapshot 副本和文件 • 管理 LUN • 执行 SnapLock 操作，但特权删除除外 • 配置协议：NFS、SMB、iSCSI、FC、FCoE、NVMe/FC和NVMe/TCP • 配置服务： DNS ， LDAP 和 NIS • 监控作业 • 监控网络连接和网络接口 • 监控 SVM 的运行状况

vsadmin-volume	• 管理自己的用户帐户本地密码和密钥信息 • 管理卷，包括卷移动 • 管理配额， qtree ， Snapshot 副本和文件 • 管理 LUN • 配置协议：NFS、SMB、iSCSI、FC、FCoE、NVMe/FC和NVMe/TCP • 配置服务： DNS ， LDAP 和 NIS • 监控网络接口 • 监控 SVM 的运行状况
vsadmin-protocol	• 管理自己的用户帐户本地密码和密钥信息 • 配置协议：NFS、SMB、iSCSI、FC、FCoE、NVMe/FC和NVMe/TCP • 配置服务： DNS ， LDAP 和 NIS • 管理 LUN • 监控网络接口 • 监控 SVM 的运行状况
vsadmin-backup	• 管理自己的用户帐户本地密码和密钥信息 • 管理 NDMP 操作 • 使已还原的卷成为读 / 写卷 • 管理 SnapMirror 关系和 Snapshot 副本 • 查看卷和网络信息
vsadmin-SnapLock	• 管理自己的用户帐户本地密码和密钥信息 • 管理卷，卷移动除外 • 管理配额， qtree ， Snapshot 副本和文件 • 执行 SnapLock 操作，包括特权删除 • 配置协议：NFS和SMB • 配置服务： DNS ， LDAP 和 NIS • 监控作业 • 监控网络连接和网络接口

vsadmin-readonly	• 管理自己的用户帐户本地密码和密钥信息 • 监控 SVM 的运行状况 • 监控网络接口 • 查看卷和 LUN • 查看服务和协议

控制管理员访问

分配给管理员的角色决定了管理员可以使用 System Manager 执行的功能。集群管理员和 Storage VM 管理员的预定义角色由 System Manager 提供。 您可以在创建管理员帐户时分配角色，也可以稍后分配其他角色。

根据您启用帐户访问的方式，您可能需要执行以下任一操作：

- 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。
- 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这些任务。

将角色分配给管理员

将角色分配给管理员，如下所示：

步骤

1. 选择*集群>设置*。
2. 选择 … → 在 * 用户和角色 * 旁边。
3. 选择 … + Add 在 * 用户 * 下。
4. 指定用户名，然后在 * 角色 * 的下拉菜单中选择一个角色。
5. 指定用户的登录方法和密码。

更改管理员角色

更改管理员的角色，如下所示：

步骤

1. 单击 * 集群 > 设置 * 。
2. 选择要更改其角色的用户的名称，然后单击 ⋮ 显示在用户名旁边。
3. 单击 * 编辑 * 。
4. 在 * 角色 * 下拉菜单中选择一个角色。

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。

管理多管理员验证

多管理员验证概述

从ONTAP 9.11.1开始、您可以使用多管理员验证(MAV)来确保只有在指定管理员批准后才能执行某些操作、例如删除卷或Snapshot副本。这样可以防止受到影响的管理员、恶意管理员或经验不足的管理员进行不希望的更改或删除数据。

配置多管理员验证包括：

- "创建一个或多个管理员批准组。"
- "启用多管理员验证功能。"
- "添加或修改规则。"

初始配置后、这些元素只能由MAV批准组中的管理员(MAV管理员)进行修改。

启用多管理员验证后、完成每个受保护操作需要三个步骤：

- 当用户启动操作时、将显示 "已生成请求。"
- 在执行之前、请至少执行一个 "MAV管理员必须批准。"
- 用户在批准后完成此操作。

多管理员验证不适用于涉及大量自动化的卷或工作流、因为每个自动化任务都需要获得批准才能完成操作。 如果要同时使用自动化和MAV、建议对特定的MAV操作使用查询。例如、您可以应用 `volume delete` MAV规则仅适用于不涉及自动化的卷、您可以使用特定命名方案来指定这些卷。

> 如果您需要在未经MAV管理员批准的情况下禁用多管理员验证功能、请联系NetApp支持部门并提及以下知识库文章： "如何在MAV管理不可用时禁用多管理员验证"。

多管理员验证的工作原理

多管理员验证包括：

- 由一个或多个具有批准和否决权限的管理员组成的组。
- 规则表_中的一组受保护操作或命令。
- 一个_rules enginer_、用于识别和控制受保护操作的执行。

MAV规则会根据基于角色的访问控制(Role-Based Access Control、RBAC)规则进行评估。因此、执行或批准受保护操作的管理员必须已拥有这些操作的最低RBAC特权。 "了解有关RBAC的更多信息。"

系统定义的规则

启用多管理员验证后、系统定义的规则(也称为_Guard导轨规则)将建立一组MAV操作、以控制绕过MAV进程本身的风险。无法从规则表中删除这些操作。启用MAV后、使用星号(*)指定的操作在执行前需要一个或多个管理员的批准、但*显示*命令除外。

- `security multi-admin-verify modify` 操作*

  控制多管理员验证功能的配置。

- `security multi-admin-verify approval-group` 业务*

  使用多管理员验证凭据控制管理员组中的成员资格。

- `security multi-admin-verify rule` 业务*

  控制需要多管理员验证的一组命令。

- `security multi-admin-verify request` operations

  控制审批流程。

受规则保护的命令

除了系统定义的命令之外、在启用多管理员验证时、以下命令也会默认受到保护、但您可以修改规则以取消对这些命令的保护。

- `security login password`
- `security login unlock`
- `set`

在ONTAP 9.11.1及更高版本中、可以保护以下命令。

`cluster peer delete`	`volume snapshot autodelete modify`
`event config modify`	`volume snapshot delete`
`security login create`	`volume snapshot policy add-schedule`
`security login delete`	`volume snapshot policy create`
`security login modify`	`volume snapshot policy delete`
`system node run`	`volume snapshot policy modify`
`system node systemshell`	`volume snapshot policy modify-schedule`
`volume delete`	`volume snapshot policy remove-schedule`
`volume flexcache delete`	`volume snapshot restore`
	`vserver peer delete`

从ONTAP 9.13.1开始、可以保护以下命令：

- `volume snaplock modify`
- `security anti-ransomware volume attack clear-suspect`
- `security anti-ransomware volume disable`
- `security anti-ransomware volume pause`

从ONTAP 9.14.1开始、可以保护以下命令：

- `volume recovery-queue modify`
- `volume recovery-queue purge`
- `volume recovery-queue purge-all`
- `vserver modify`

多管理员批准的工作原理

每当在受MAV保护的集群上输入受保护操作时、系统都会向指定的MAV管理员组发送操作执行请求。

您可以配置：

- MAV组中的管理员姓名、联系信息和数量。

  MAV管理员应具有具有集群管理员权限的RBAC角色。

- MAV管理员组的数量。
  - 每个受保护操作规则都会分配一个MAV组。

    - 对于多个MAV组、您可以配置哪个MAV组批准给定规则。
- 执行受保护操作所需的MAV批准数量。
- MAV管理员必须对批准请求做出响应的_Approval到期期限。
- 一个_执行到期_期限、在此期限内、发出请求的管理员必须完成此操作。

配置这些参数后、需要获得MAV批准才能对其进行修改。

MAV管理员不能批准自己执行受保护操作的请求。因此：

- 不应在仅包含一个管理员的集群上启用MAV。
- 如果MAV组中只有一人、则该MAV管理员不能输入受保护的操作；常规管理员必须输入这些操作、而MAV管理员只能进行批准。
- 如果您希望MAV管理员能够执行受保护的操作、则MAV管理员的数量必须大于所需批准的数量。
  例如、如果受保护操作需要两个批准、并且您希望MAV管理员执行这些批准、则MAV管理员组中必须有三个人。

MAV管理员可以通过电子邮件警报(使用EMS)接收批准请求、也可以查询请求队列。 收到请求后、他们可以采取以下三种操作之一：

- 批准
- 拒绝(否决)
- 忽略(无操作)

在以下情况下、系统会向与MAV规则关联的所有审批者发送电子邮件通知：

- 已创建请求。
- 请求已获得批准或被否决。
- 已执行批准的请求。

如果请求者属于该操作的同一批准组、则在其请求获得批准后、他们将收到一封电子邮件。

*注意：*请求者无法批准自己的请求、即使他们属于批准组也是如此。但是、他们可以收到电子邮件通知。不属于批准组的请求者(即不是MAV管理员)不会收到电子邮件通知。

受保护操作执行的工作原理

如果已批准对受保护操作执行、则在出现提示时、发出请求的用户将继续执行该操作。如果操作被否决、则发出请求的用户必须先删除此请求、然后才能继续操作。

MAV规则会在获得RBAC权限后进行评估。因此、如果用户没有足够的RBAC权限来执行操作、则无法启动MAV请求过程。

管理管理员批准组

在启用多管理员验证(MAV)之前、您必须创建一个管理员批准组、其中包含一个或多个要授予批准或否决权限的管理员。启用多管理员验证后、对批准组成员资格进行的任何修改都需要获得现有合格管理员之一的批准。

关于此任务

您可以将现有管理员添加到MAV组或创建新管理员。

MAV功能可支持现有的基于角色的访问控制(Role-Based Access Control、RBAC)设置。潜在的MAV管理员必须具有足够的权限来执行受保护的操作、才能将其添加到MAV管理员组。 "了解有关RBAC的更多信息。"

您可以将MAV配置为向MAV管理员发出批准请求待处理的警报。为此，您必须配置电子邮件通知，特别是 `Mail From` 和 `Mail Server` 参数—或者，您可以清除这些参数以禁用通知。如果没有电子邮件警报、MAV管理员必须手动检查批准队列。

System Manager 操作步骤

如果要首次创建MAV批准组、请参见System Manager操作步骤 to "启用多管理员验证。"

要修改现有批准组或创建其他批准组、请执行以下操作：

1. 确定要接收多管理员验证的管理员。
   a. 单击*集群>设置。*
   b. 单击 → 在*用户和角色*旁边
   c. 单击 + Add 在*用户*下
   d. 根据需要修改此名册。

      有关详细信息，请参见 "控制管理员访问。"
2. 创建或修改MAV批准组：
   a. 单击*集群>设置。*
   b. 单击 → 在*安全性*部分中的*多管理员批准*旁边。
      (此时将显示 ⚙ 如果尚未配置MAV、则显示图标。)
      - name：输入组名称。
      - 审批者：从用户列表中选择审批者。
      - 电子邮件地址：输入电子邮件地址。
      - 默认组：选择一个组。

启用MAV后、要编辑现有配置、需要获得MAV批准。

命令行界面操作步骤

1. 验证是否已为设置值 `Mail From` 和 `Mail Server` parameters输入 …

   ```
   event config show
   ```

   显示内容应类似于以下内容：

```
cluster01::> event config show
                           Mail From:  admin@localhost
                         Mail Server:  localhost
                           Proxy URL:  -
                          Proxy User:  -
 Publish/Subscribe Messaging Enabled:  true
```

要配置这些参数、请输入：

`event config modify -mail-from email_address -mail-server server_name`

2. 确定要接收多管理员验证的管理员

如果要...	输入此命令
显示当前管理员	`security login show`
修改当前管理员的凭据	`security login modify <parameters>`
创建新的管理员帐户	`security login create -user-or-group -name admin_name -application ssh -authentication-method password`

3. 创建MAV批准组：

`security multi-admin-verify approval-group create [ -vserver svm_name] -name group_name -approvers approver1[,approver2…] [[-email address1], address1…]`

   - `-vserver` -此版本仅支持管理SVM。
   - `-name` - MAV组名称，最多64个字符。
   - `-approvers` -一个或多个审批人的列表。
   - `-email` -创建、批准、否决或执行请求时通知的一个或多个电子邮件地址。

   *示例：*以下命令将创建一个包含两个成员和关联电子邮件地址的MAV组。

```
cluster-1::> security multi-admin-verify approval-group create -name
mav-grp1 -approvers pavan,julia -email pavan@myfirm.com,julia@myfirm.com
```

4. 验证组创建和成员资格：

`security multi-admin-verify approval-group show`

   - 示例： *

```
cluster-1::> security multi-admin-verify approval-group show
Vserver  Name        Approvers        Email
-------  ---------------- ------------------
------------------------------------------------------------
svm-1    mav-grp1   pavan,julia      email
pavan@myfirm.com,julia@myfirm.com
```

使用以下命令修改初始MAV组配置。

*注：*执行前、所有操作都需要获得MAV管理员的批准。

如果要...	输入此命令
修改组特征或修改现有成员信息	`security multi-admin-verify approval-group modify [parameters]`
添加或删除成员	`security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[,approver2…]][-approvers-to-remove approver1[,approver2…]]`
删除组	`security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name`

启用和禁用多管理员验证

必须明确启用多管理员验证(MAV)。启用多管理员验证后、需要经MAV批准组(MAV管理员)中的管理员批准才能将其删除。

关于此任务

启用MAV后、修改或禁用MAV需要获得MAV管理员的批准。

> 如果您需要在未经MAV管理员批准的情况下禁用多管理员验证功能、请联系NetApp支持部门并提及以下知识库文章： "如何在MAV管理不可用时禁用多管理员验证"。

启用MAV时、可以全局指定以下参数。

批准组

全球批准组列表。要启用MAV功能、至少需要一个组。

> 如果将MAV与自动防病毒保护(ARP)结合使用、请定义一个新的或现有的审批组、负责批准ARP暂停、禁用和清除可疑请求。

所需审批者

执行受保护操作所需的批准者数量。默认值和最小值为1。

> 所需的审批人数量必须小于默认审批组中唯一审批人的总数。

批准到期时间(小时、分钟、秒)

MAV管理员必须对批准请求做出响应的期限。默认值为1小时(1小时)、支持的最小值为1秒(1秒)、支持的最大值为14天(14天)。

执行到期时间(小时、分钟、秒)

发出请求的管理员必须完成：：操作的期限。默认值为1小时(1小时)、支持的最小值为1秒(1秒)、支持的最大值为14天(14天)。

您还可以覆盖特定的任何参数 "操作规则。"

System Manager 操作步骤

1. 确定要接收多管理员验证的管理员。
   a. 单击*集群>设置。*
   b. 单击 → 在*用户和角色*旁边
   c. 单击 + Add 在*用户*下
   d. 根据需要修改此名册。

      有关详细信息，请参见 "控制管理员访问。"
2. 创建至少一个批准组并添加至少一个规则、以启用多管理员验证。
   a. 单击*集群>设置。*
   b. 单击 ⚙ 在*安全性*部分中的*多管理员批准*旁边。
   c. 单击 + Add 至少添加一个批准组。
      - Name—输入组名称。
      - 审批者—从用户列表中选择审批者。
      - 电子邮件地址—输入电子邮件地址。
      - Default group—选择一个组。
   d. 至少添加一个规则。
      - 操作—从列表中选择受支持的命令。
      - 查询—输入任何所需的命令选项和值。
      - 可选参数；留空以应用全局设置、或者为特定规则分配其他值以覆盖全局设置。
        - 所需数量的审批者
        - 批准组
   e. 单击*高级设置*以查看或修改默认值。
      - 所需的批准者数量(默认值：1)

- 执行请求到期(默认：1小时)
- 批准请求到期(默认：1小时)
- 邮件服务器*
- 发件人电子邮件地址*

  *这些更新了"通知管理"下管理的电子邮件设置。如果尚未配置它们、系统将提示您进行设置。

f. 单击*启用*以完成MAV初始配置。

初始配置后、当前MAV状态将显示在*多管理员批准*图块中。

- 状态(已启用或未启用)
- 需要批准的活动操作
- 处于待定状态的未处理请求数

您可以通过单击来显示现有配置 →。要编辑现有配置、需要获得MAV批准。

禁用多管理员验证：

1. 单击*集群>设置。*
2. 单击 ⚙ 在*安全性*部分中的*多管理员批准*旁边。
3. 单击已启用切换按钮。

   要完成此操作、需要获得MAV批准。

命令行界面操作步骤

在命令行界面上启用MAV功能之前、至少需要一个 "MAV管理员组" 必须已创建。

如果要...	输入此命令

启用MAV功能	`security multi-admin-verify modify -approval-groups group1[,group2…] [-required-approvers nn ] -enabled true [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]`
	
	示例：以下命令将启用具有1个批准组、2个所需审批者和默认到期期限的MAV。
	
	`cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true`
	
	至少添加一个以完成初始配置 "操作规则。"

修改MAV配置(需要获得MAV批准)	`security multi-admin-verify approval-group modify [-approval-groups group1[,group2…]] [-required-approvers nn ] [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]`

验证MAV功能	`security multi-admin-verify show`
	
	• 示例： *
	
	`cluster-1::> security multi-admin-verify show`
	`Is Required Execution Approval Approval Enabled Approvers Expiry Expiry Groups`
	`------- --------- --------- -------- ----------`
	`true 2 1h 1h mav-grp1`

禁用MAV功能(需要获得MAV批准)	`security multi-admin-verify modify -enabled false`

管理受保护的操作规则

您可以创建多管理员验证(MAV)规则来指定需要批准的操作。每当启动操作时、受保护的

操作都会被截获、并生成批准请求。

任何具有适当RBAC功能的管理员都可以在启用MAV之前创建规则、但启用MAV后、对规则集进行的任何修改都需要获得MAV批准。

每个操作只能创建一个MAV规则；例如、不能创建多个 `volume-snapshot-delete` 规则。任何所需的规则约束必须包含在一个规则中。

受规则保护的命令

从ONTAP 9.11.1开始、您可以创建规则来保护以下命令。

`cluster peer delete`	`volume snapshot autodelete modify`
`event config modify`	`volume snapshot delete`
`security login create`	`volume snapshot policy add-schedule`
`security login delete`	`volume snapshot policy create`
`security login modify`	`volume snapshot policy delete`
`system node run`	`volume snapshot policy modify`
`system node systemshell`	`volume snapshot policy modify-schedule`
`volume delete`	`volume snapshot policy remove-schedule`
`volume flexcache delete`	`volume snapshot restore`
	`vserver peer delete`

从ONTAP 9.13.1开始、您可以创建规则来保护以下命令：

- `volume snaplock modify`
- `security anti-ransomware volume attack clear-suspect`
- `security anti-ransomware volume disable`
- `security anti-ransomware volume pause`

从ONTAP 9.14.1开始、您可以创建规则来保护以下命令：

- `volume recovery-queue modify`
- `volume recovery-queue purge`
- `volume recovery-queue purge-all`
- `vserver modify`

MAV system-default命令的规则、即 `security multi-admin-verify` "命令"，无法更改。

除了系统定义的命令之外、在启用多管理员验证时、以下命令也会默认受到保护、但您可以修改规则以取消对这些命令的保护。

- `security login password`
- `security login unlock`
- `set`

规则约束

创建规则时、您可以选择指定 `-query` 选项、用于将请求限制为命令功能的一部分。。 `-query` 选项还可用于限制配置元素、例如SVM、卷和Snapshot名称。

例如、在中 `volume snapshot delete` 命令、 `-query` 可以设置为 `-snapshot !hourly*,!daily*,!weekly*`表示以每小时、每天或每周属性为前处理前的卷快照不受MAV保护。

```
smci-vsim20::> security multi-admin-verify rule show
                                            Required  Approval
Vserver Operation                           Approvers Groups
------- ------------------------------------ --------- -------------
vs01    volume snapshot delete               -         -
          Query: -snapshot !hourly*,!daily*,!weekly*
```

> 任何排除的配置元素都不受MAV保护、任何管理员都可以删除或重命名它们。

默认情况下、规则指定对应的 `security multi-admin-verify request create` *"protected_operation"* 输入受保护的操作时、系统会自动生成命令。您可以将此默认值修改为需要 `request create` 命令单独输入。

默认情况下、规则会继承以下全局MAV设置、但您可以指定特定于规则的例外情况：

- 所需数量的批准者
- 批准组
- 批准到期期限
- 执行到期期限

System Manager 操作步骤

如果要首次添加受保护的操作规则、请参见System Manager操作步骤 to "启用多管理员验证。"

要修改现有规则集、请执行以下操作：

1. 选择*集群>设置*。
2. 选择 … ⚙ 在*安全性*部分中的*多管理员批准*旁边。
3. 选择 … + Add 至少添加一个规则；您还可以修改或删除现有规则。
   - 操作—从列表中选择受支持的命令。

- 查询—输入任何所需的命令选项和值。
- 可选参数—留空以应用全局设置、或者为特定规则分配其他值以覆盖全局设置。
  - 所需数量的审批者
  - 批准组

命令行界面操作步骤

> 全部 `security multi-admin-verify rule` 命令执行前需要MAV管理员批准、但除外 `security multi-admin-verify rule show`。

如果要...	输入此命令
创建规则	`security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]`

修改当前管理员的凭据	`security login modify <parameters>`
	
	示例：要删除根卷、需要获得以下规则的批准。
	
	`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"`

修改规则	`security multi-admin-verify rule modify -operation "protected_operation" [parameters]`
删除规则	`security multi-admin-verify rule delete -operation "protected_operation"`
显示规则	`security multi-admin-verify rule show`

有关命令语法的详细信息、请参见 `security multi-admin-verify rule` 手册页。

请求执行受保护操作

当您在启用了多管理员验证(MAV)的集群上启动受保护操作或命令时、ONTAP 会自动截获此操作并要求生成请求、此请求必须由MAV批准组中的一个或多个管理员(MAV管理员)批准。或者、您也可以在不使用对话框的情况下创建MAV请求。

如果获得批准、您必须对查询做出响应、才能在请求到期期限内完成操作。如果被否决、或者超出请求或到期期限、则必须删除此请求并重新提交。

MAV功能会使用现有RBAC设置。也就是说、您的管理员角色必须具有足够的权限来执行受保护的操作、而不考虑MAV设置。 "了解有关RBAC的更多信息"。

如果您是MAV管理员、则执行受保护操作的请求也必须获得MAV管理员的批准。

System Manager 操作步骤

当用户单击某个菜单项以启动操作且该操作受保护时、将生成批准请求、并且用户将收到类似于以下内容的通知：

```
Approval request to delete the volume was sent.
Track the request ID 356 from Events & Jobs > Multi-Admin Requests.
```

启用MAV后、可以使用*多管理员请求*窗口、该窗口将根据用户的登录ID和MAV角色(审批者或非审批者)显示待处理的请求。对于每个待处理请求、将显示以下字段：

- 操作
- 索引(编号)
- 状态(待定、已批准、已拒绝、已执行或已过期)

  如果一个审批者拒绝了某个请求、则无法执行其他操作。

- 查询(请求操作的任何参数或值)
- 正在请求用户
- 请求将于到期
- (数量)待定审批者
- (数量)潜在审批者

请求获得批准后、发出请求的用户可以在到期期限内重试此操作。

如果用户在未获得批准的情况下重试此操作、则会显示类似以下内容的通知：

```
Request to perform delete operation is pending approval.
Retry the operation after request is approved.
```

命令行界面操作步骤

1. 直接输入或使用MAV request命令输入受保护操作。

   示例—要删除卷、请输入以下命令之一：

   - `volume delete`

```
cluster-1::*> volume delete -volume vol1 -vserver vs0

Warning: This operation requires multi-admin verification. To create
a
         verification request use "security multi-admin-verify
request
         create".

         Would you like to create a request for this operation?
          {y|n}: y

Error: command failed: The security multi-admin-verify request (index
3) is
       auto-generated and requires approval.
```

- `security multi-admin-verify request create “volume delete”`

```
Error: command failed: The security multi-admin-verify request (index
3)
       requires approval.
```

2. 检查请求的状态并响应MAV通知。

   a. 如果请求获得批准、请响应命令行界面消息以完成此操作。

      - 示例： *

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: approved
Required Approvers: 1
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Info: Volume "vol1" in Vserver "vs0" will be marked as deleted and
placed in the volume recovery queue. The space used by the volume
will be recovered only after the retention period of 12 hours has
completed. To recover the space immediately, get the volume name
using (privilege:advanced) "volume recovery-queue show vol1_*" and
then "volume recovery-queue purge -vserver vs0 -volume <volume_name>"
command. To recover the volume use the (privilege:advanced) "volume
recovery-queue recover -vserver vs0       -volume <volume_name>"
command.

Warning: Are you sure you want to delete volume "vol1" in Vserver
"vs0" ?
{y|n}: y
```

b. 如果请求被否决或到期期限已过、请删除此请求、然后重新提交或联系MAV管理员。

- 示例： *

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: vetoed
Required Approvers: 1
 Pending Approvers: 1
   Approval Expiry: 2/25/2022 14:38:47
  Execution Expiry: -
         Approvals: -
       User Vetoed: admin2
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:38:47
     Time Approved: -
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Error: command failed: The security multi-admin-verify request (index 3)
hasbeen vetoed. You must delete it and create a new verification
request.
To delete, run "security multi-admin-verify request delete 3".
```

管理受保护的操作请求

当收到有关待处理操作执行请求的通知后、MAV批准组(MAV管理员)中的管理员必须在固定时间段(批准到期)内通过批准或否决消息进行响应。如果未收到足够数量的批准、请求者必须删除此请求并再提交一份。

关于此任务

批准请求使用索引编号进行标识、索引编号包含在电子邮件消息和请求队列的显示中。

可以显示请求队列中的以下信息：

操作
: 创建请求的受保护操作。

查询
: 用户要应用操作的一个或多个对象。

State
: 请求的当前状态；待定、已批准、已拒绝、已过期、 已执行。如果一个审批者拒绝了某个请求、则无法执行

其他操作。

所需审批者

批准请求所需的MAV管理员数量。用户可以为此操作规则设置requireed-approvers参数。如果用户未将所需审批者设置为规则、则会应用全局设置中的所需审批者。

待定审批者

仍然需要批准请求以将此请求标记为已批准的MAV管理员数量。

批准到期

MAV管理员必须对批准请求做出响应的期限。任何授权用户都可以为操作规则设置批准到期时间。如果未为此规则设置Approval expiry、则会应用全局设置中的Approval expiry。

执行到期

发出请求的管理员必须完成操作的期限。任何授权用户都可以为操作规则设置执行到期时间。如果未为此规则设置execing-expiry、则会应用全局设置中的execing-expiry。

已批准用户

批准此请求的MAV管理员。

已否决用户

已否决此请求的MAV管理员。

Storage VM (SVM)

与请求关联的SVM。此版本仅支持管理SVM。

用户已请求

创建请求的用户的用户名。

创建时间

创建请求的时间。

批准时间

请求状态更改为"已批准"的时间。

comment

与请求关联的任何注释。

允许的用户

允许执行请求获得批准的受保护操作的用户列表。条件 `users-permitted` 为空、则具有适当权限的任何用户均可执行此操作。

如果达到1000个请求的限制、或者已过期请求的到期时间超过8小时、则所有已过期或已执行的请求都会被删除。被否决的请求一旦标记为已过期、将被删除。

System Manager 操作步骤

MAV管理员会收到电子邮件消息、其中包含批准请求、请求到期期限以及用于批准或拒绝请求的链接的详细信息。他们可以通过单击电子邮件中的链接来访问批准对话框、或者导航到System Manager中的*事件和作业>请求*。

如果启用了多管理员验证、则可以使用*请求*窗口、该窗口将根据用户的登录ID和MAV角色(审批者或非审批者)显示待处理的请求。

- 操作
- 索引(编号)
- 状态(待定、已批准、已拒绝、已执行或已过期)

  如果一个审批者拒绝了某个请求、则无法执行其他操作。

- 查询(请求操作的任何参数或值)
- 正在请求用户
- 请求将于到期
- (数量)待定审批者
- (数量)潜在审批者

MAV管理员在此窗口中具有其他控件；他们可以批准、拒绝或删除单个操作或选定的操作组。但是、如果MAV管理员是发出请求的用户、他们将无法批准、拒绝或删除自己的请求。

命令行界面操作步骤

1. 通过电子邮件通知待处理请求时、请记下请求的索引编号和批准到期期限。此外、还可以使用下面提到的*显示*或*显示-待定*选项来显示索引编号。
2. 批准或否决此请求。

如果要...	输入此命令
批准请求	`security multi-admin-verify request approve` *`nn`*
否决请求	`security multi-admin-verify request veto` *`nn`*
显示所有请求、待处理请求或单个请求	`security multi-admin-verify request { show
show-pending } [*nn*] { -fields *field1*[,*field2*…]	[-instance] }`  您可以显示队列中的所有请求、也可以仅显示待处理的请求。如果输入索引编号、则仅显示该索引编号的信息。您可以显示有关特定字段的信息(使用 `-fields` 参数)或关于所有字段(使用 `-instance` 参数)。
删除请求	`security multi-admin-verify request delete` *`nn`*

示例

在MAV管理员收到索引编号为3的请求电子邮件后、以下顺序将批准请求、该电子邮件已获得一项批准。

```
          cluster1::> security multi-admin-verify request show-pending
                                          Pending
Index Operation      Query State   Approvers Requestor
----- -------------- ----- ------- --------- ---------
    3 volume delete  -     pending 1         julia


cluster-1::> security multi-admin-verify request approve 3

cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -
             State: approved
Required Approvers: 2
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: mav-admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: julia
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -
```

示例

在MAV管理员收到索引编号为3的请求电子邮件后、以下顺序将否决此请求、此电子邮件已获得一项批准。

```
      cluster1::> security multi-admin-verify request show-pending
                                      Pending
Index Operation      Query State   Approvers Requestor
----- -------------- ----- ------- --------- ---------
    3 volume delete  -     pending 1         pavan


cluster-1::> security multi-admin-verify request veto 3

cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -
             State: vetoed
Required Approvers: 2
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: mav-admin1
       User Vetoed: mav-admin2
           Vserver: cluster-1
    User Requested: pavan
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -
```

使用OAuth2.0进行身份验证和授权

ONTAP OAuth2.0实施概述

从ONTAP 9.14开始、您可以选择使用开放授权(OAuth2.0)框架控制对ONTAP集群的访问。您可以使用任何ONTAP管理界面配置此功能、包括ONTAP命令行界面、System Manager和REST API。但是、只有当客户端使用REST API访问ONTAP时、才能应用OAuth2.0授权和访问控制决策。

> OAuth2.0支持是在ONTAP 9.14.0中首次推出的、因此其可用性取决于您使用的ONTAP版本。请参见 "《 ONTAP 发行说明》" 有关详细信息 …

功能和优势

下面将介绍在ONTAP中使用OAuth2.0的主要功能和优势。

支持**OAuth2.0**标准

OAuth2.0是行业标准授权框架。它用于使用签名访问令牌限制和控制对受保护资源的访问。使用OAuth2.0有几个好处：

- 授权配置有许多选项
- 切勿泄露客户端凭据(包括密码)
- 根据您的配置、令牌可以设置为过期
- 非常适合与REST API结合使用

已通过多个常见授权服务器的测试

ONTAP实施旨在与任何符合OAuth2.0标准的授权服务器兼容。它已通过以下常见服务器或服务的测试、包括：

- auth0
- Active Directory联合身份验证服务(ADFS)
- Keyloak

支持多个并发授权服务器

一个ONTAP集群最多可以定义八个授权服务器。这样、您就可以灵活地满足各种安全环境的需求。

与**REST**角色集成

ONTAP授权决定最终取决于分配给用户或组的REST角色。这些角色或作为独立范围在访问令牌中承载、或基于本地ONTAP定义以及Active Directory或LDAP组。

用于使用受发件人限制的访问令牌的选项

您可以将ONTAP和授权服务器配置为使用相互传输层安全(MTLS)、以增强客户端身份验证。它可以保证OAuth2.0访问令牌仅供最初颁发给的客户端使用。此功能支持并符合多项常见的安全建议、包括由FAPI和miter制定的安全建议。

实施和配置

概括地说、在开始使用时、您应该考虑OAuth2.0实施和配置的几个方面。

ONTAP中的**OAuth2.0**实体

OAuth2.0授权框架定义了多个实体、这些实体可以映射到数据中心或网络中的真实或虚拟元素。下表显示了OAuth2.0实体及其对ONTAP的适应性。

OAuth2.0实体	**Description**
资源	提供通过内部ONTAP命令访问ONTAP资源的REST API端点。
资源所有者	默认情况下、创建或拥有受保护资源的ONTAP集群用户。
资源服务器	ONTAP集群中受保护资源的主机。
客户端	代表资源所有者或在获得资源所有者权限的情况下请求访问REST API端点的应用程序。
授权服务器	通常是一个专用服务器、负责颁发访问令牌并强制实施管理策略。

核心**ONTAP**配置

您需要将ONTAP集群配置为启用并使用OAuth2.0。这包括建立与授权服务器的连接以及定义所需的ONTAP授权

配置。您可以使用任何管理界面执行此配置、其中包括：

- ONTAP 命令行界面
- System Manager
- ONTAP REST API

环境和支持服务

除了ONTAP定义之外、您还需要配置授权服务器。如果您使用的是组到角色映射、则还需要配置Active Directory组或LDAP等效项。

支持的**ONTAP**客户端

从ONTAP 9.14开始、REST API客户端可以使用OAuth2.0访问ONTAP。在发出REST API调用之前、您需要从授权服务器获取访问令牌。然后、客户端使用HTTP授权请求标头将此令牌作为_p承载 令牌_传递到ONTAP集群。根据所需的安全级别、您还可以在客户端创建和安装证书、以使用基于MTLS的受发件人限制的令牌。

选定术语

当您开始探索使用ONTAP部署OAuth2.0时、熟悉其中的一些术语会很有帮助。请参见 "其他资源" 有关OAuth2.0的详细信息的链接。

访问令牌

由授权服务器发出的令牌、由OAuth2.0客户端应用程序使用它来发出访问受保护资源的请求。

JSON Web令牌

用于格式化访问令牌的标准。JSON用于以紧凑格式表示OAuth2.0索赔、索赔分为三个主要部分。

受发件人限制的访问令牌

一项基于相互传输层安全(MTLS)协议的可选功能。通过在令牌中使用额外的确认声明、可确保访问令牌仅供最初发出访问令牌的客户端使用。

JSON Web密钥集

JWKS是ONTAP用来验证客户端提供的JWT令牌 的公共密钥集合。通常、授权服务器会通过专用URI提供这些密钥集。

范围

范围提供了一种限制或控制应用程序对受保护资源(如ONTAP REST API)的访问的方法。它们在访问令牌中以字符串表示。

ONTAP REST角色

REST角色是在ONTAP 9.6中引入的、是ONTAP RBAC框架的核心部分。这些角色与ONTAP仍支持的早期传统角色不同。ONTAP中的OAuth2.0实施仅支持REST角色。

HTTP授权标头

HTTP请求中包含的标头、用于在执行REST API调用时标识客户端和关联权限。根据身份验证和授权的执行方式、可以选择多种模式或实施方式。在向ONTAP提供OAuth2.0访问令牌时、此令牌标识为_承载 令牌_。

HTTP基本身份验证

ONTAP仍支持早期的HTTP身份验证技术。纯文本凭据(用户名和密码)与冒号串联在一起、并以base64进行编码。该字符串将放置在授权请求标头中并发送到服务器。

FAPI

OpenID Foundation的一个工作组、为金融行业提供协议、数据架构和安全建议。API最初称为财务级API。

斜接

一家私营非营利公司、为美国空军和美国政府提供技术和安全指导。

其他资源

下文提供了若干额外资源。您应查看这些站点以获取有关OAuth2.0和相关标准的更多信息。

协议和标准

- "RFC 6749：《OAuth2.0授权框架》"
- "RFC 7519：JSON Web令牌(JWTs)"
- "RFC 7523：《用于OAuth2.0客户端身份验证和授权授予的JSON Web令牌(JWT, Web令牌)配置文件》"
- "RFC 7662：OAuth2.0令牌自省"
- "RFC报废：JWT的拥有证明密钥"
- "RFC 8705：《OAuth2.0相互TLS客户端身份验证和受证书制约的访问令牌》"

组织

- "OpenID Foundation"
- "FAPI工作组"
- "斜接"
- "IANA - JWT"

产品和服务

- "auth0"
- "ADFS概述"
- "Keyloak"

其他工具和实用程序

- "验证0的Jwt"
- "OpenSSL"

NetApp文档和资源

- "ONTAP自动化" 文档。

概念

授权服务器和访问令牌

授权服务器作为OAuth2.0授权框架中的一个中央组件执行多项重要功能。

OAuth2.0授权服务器

授权服务器主要负责创建和签名访问令牌。这些令牌包含身份和授权信息、使客户端应用程序能够有选择地访问受保护的资源。这些服务器通常彼此隔离、可通过多种不同的方式实施、包括作为独立的专用服务器或作为大型身份和访问管理产品的一部分。

> 有时、授权服务器可能会使用不同的术语、尤其是当OAuth2.0功能打包在更大型的身份和访问管理产品或解决方案中时。例如，术语*身份提供程序(IDP)*经常与*authorization server*互换使用。

管理

除了颁发访问令牌之外、授权服务器还通常通过Web用户界面提供相关管理服务。例如、您可以定义和管理：

- 用户和用户身份验证
- 范围
- 通过租户和领域实现管理隔离
- 策略实施
- 与各种外部服务的连接
- 支持其他身份协议(例如SAML)

ONTAP与符合OAuth2.0标准的授权服务器兼容。

定义到**ONTAP**

您需要为ONTAP定义一个或多个授权服务器。ONTAP可以与每台服务器安全地进行通信、以验证令牌并执行其他相关任务来支持客户端应用程序。

下面介绍了ONTAP配置的主要方面。另请参见 "OAuth2.0部署方案" 有关详细信息 …

验证访问令牌的方式和位置

验证访问令牌有两个选项。

- 本地验证

  ONTAP可以根据发出访问令牌的授权服务器提供的信息在本地验证访问令牌。从授权服务器检索到的信息由ONTAP进行缓存、并定期刷新。

- 远程自省

  您还可以使用远程自省在授权服务器上验证令牌。自省是一种协议、允许授权方向授权服务器查询有关访问令牌的信息。它为ONTAP提供了一种从访问令牌中提取某些元数据并对令牌进行验证的方法。出于性能原因、ONTAP会缓存某些数据。

网络位置

ONTAP可能受防火墙保护。在这种情况下、您需要在配置中标识代理。

如何定义授权服务器

您可以使用任何管理界面(包括命令行界面、System Manager或REST API)为ONTAP定义授权服务器。例如、在命令行界面中、您可以使用命令 `security oauth2 client create`。

授权服务器的数量

一个ONTAP集群最多可以定义八个授权服务器。只要颁发者或颁发者/受众声明是唯一的、同一授权服务器就可以多次定义到同一ONTAP集群。例如、使用Keyloak时、使用不同领域时始终会出现这种情况。

使用**OAuth2.0**访问令牌

授权服务器颁发的OAuth2.0访问令牌由ONTAP进行验证、用于针对REST API客户端请求做出基于角色的访问决策。

获取访问令牌

您需要从为使用REST API的ONTAP集群定义的授权服务器获取访问令牌。要获取令牌、您必须直接联系授权服务器。

> ONTAP不会通过问题描述访问令牌、也不会将客户端的请求重定向到授权服务器。

如何请求令牌取决于多个因素、包括：

- 授权服务器及其配置选项
- OAuth2.0授予类型
- 用于问题描述请求的客户端或软件工具

授予类型

_GRANT _是一个定义完善的过程、包括一组网络流、用于请求和接收OAuth2.0访问令牌。根据客户端、环境和安全要求、可以使用多种不同的授予类型。下表列出了最受欢迎的补助金类型。

授予类型	**Description**
客户端凭据	一种仅使用凭据(如ID和共享密钥)的常见授予类型。假定客户端与资源所有者具有密切的信任关系。
Password	如果资源所有者与客户端建立了信任关系、则可以使用资源所有者密码凭据授予类型。在将旧版HTTP客户端迁移到OAuth2.0时、此功能也很有用。
授权代码	这是机密客户端的理想授予类型、并且基于基于重定向的流。它可用于获取访问令牌和刷新令牌。

Jwt内容

OAuth2.0访问令牌格式为JWT.此内容由授权服务器根据您的配置创建。但是、令牌对客户端应用程序是不透明的。客户端没有理由检查令牌或了解其内容。

每个JWT"访问令牌都包含一组声明。这些声明描述了颁发者的特征以及基于授权服务器上管理定义的授权。下表介绍了根据标准登记的一些索赔。所有字符串都区分大小写。

款项申请	关键字	**Description**
颁发者	ISS	标识发出令牌的主体。款项申请处理是针对特定应用程序的。

款项申请	关键字	Description
主题	子	令牌的主题或用户。此名称的范围为全局唯一或本地唯一。
audience	澳元	令牌的目标收件人。以字符串数组的形式实施。
到期日期	有效期	令牌过期后必须拒绝的时间。

请参见 "RFC 7519：JSON Web令牌" 有关详细信息 …

ONTAP客户端授权选项

您可以通过多个选项自定义ONTAP客户端授权。授权决策最终取决于访问令牌中包含或派生的ONTAP REST角色。

> 您只能使用 "ONTAP REST角色" 为OAuth2.0配置授权时。不支持早期的ONTAP传统角色。

简介

ONTAP中的OAuth2.0实施灵活可靠、可为您提供保护ONTAP环境所需的选项。概括地说、用于定义ONTAP客户端授权的主要配置类别有三个。这些配置选项不能同时使用。

ONTAP会根据您的配置应用最合适的选项。请参见 "ONTAP如何确定访问" 有关ONTAP如何处理配置定义以做出访问决策的详细信息。

OAuth2.0自包含范围

这些范围包含一个或多个自定义REST角色、每个角色封装在一个字符串中。它们与ONTAP角色定义无关。您需要在授权服务器上定义这些范围字符串。

本地ONTAP专用的REST角色和用户

根据您的配置、可以使用本地ONTAP标识定义来制定访问决策。选项包括：

- 单个命名的REST角色
- 将用户名与本地ONTAP用户匹配

指定角色的作用域语法为*ONTAP角色<URL-encoded-ONTAP-role-name>。例如、如果角色为"admin"、则范围字符串将为"ONTAP角色-admin"。

Active Directory或LDAP组

如果检查了本地ONTAP定义、但无法做出访问决定、则会使用Active Directory ("域")或LDAP ("nsswitch")组。可以通过以下两种方式之一指定组信息：

- OAuth2.0范围字符串

  支持使用客户端凭据流的机密应用程序、其中没有具有组成员资格的用户。此范围应命名为*ONTAP组-*ONTAP <URL-encoded-ONTAP-group-name>。例如、如果组为"developing"、则范围字符串将为"ONTAP组-developing"。

- 在"组"索赔中

  这适用于ADFS使用资源所有者(密码授予)流颁发的访问令牌。

独立的**OAuth2.0**范围

自包含范围是指访问令牌中包含的字符串。每个角色都是一个完整的自定义角色定义、其中包括ONTAP做出访问决策所需的一切。此范围与ONTAP本身定义的任何REST角色是分开的、并与之不同。

范围字符串的格式

在基本级别、范围表示为连续字符串、由六个冒号分隔值组成。范围字符串中使用的参数如下所述。

ONTAP文字

范围必须以文字值开头 `ontap` 小写。此操作会将范围标识为特定于ONTAP的范围。

集群

此选项用于定义将哪个ONTAP集群范围设置为适用场景。这些值可以包括：

- 集群UUID

  标识单个集群。

- 星号(*)

  指示适用场景all集群的范围。

您可以使用ONTAP命令行界面命令 `cluster identity show` 以显示集群的UUID。如果未指定、则范围为适用场景all集群。

Role

自身作用域中包含的REST角色的名称。ONTAP不会检查此值、也不会将其与定义给ONTAP的任何现有REST角色匹配。此名称用于日志记录。

访问级别

此值指示在范围中使用API端点时应用于客户端应用程序的访问级别。下表介绍了六个可能的值。

访问级别	**Description**
无	拒绝对指定端点的所有访问。
-readonly	仅允许使用GET进行读取访问。
read_create	允许读取访问以及使用POST创建新资源实例。
read_modify	允许读取访问以及使用修补程序更新现有资源的功能。
read_create_modify	允许除删除以外的所有访问。允许的操作包括GET (读取)、POST (创建)和patch (更新)。
全部	允许完全访问。

SVM

集群中SVM的名称(范围为适用场景)。使用***值(星号)表示所有SVM。

> ONTAP 9.14.1不完全支持此功能。您可以忽略SVM参数并使用星号作为占位符。查看 "《ONTAP 发行说明》" 以检查未来是否支持SVM。

REST API URI

指向一个资源或一组相关资源的完整或部分路径。字符串必须以开头 `/api`。如果未指定值、则会将范围限定为适用场景集群中的所有ONTAP端点。

范围示例

以下是一些独立范围的示例。

ONTAP：：joes-Role：read_cree_Modify：：/API/cluster

为分配了此角色的用户提供对的读取、创建和修改访问权限 `/cluster` 端点。

CLI管理工具

为了使独立范围的管理更轻松、更不容易出错、ONTAP提供了命令行界面命令 `security oauth2 scope` 根据输入参数生成范围字符串。

命令 `security oauth2 scope` 根据您的输入、有两个用例：

- CLI参数以限定字符串范围

  您可以使用此版本的命令根据输入参数生成范围字符串。

- 作用域字符串到CLI参数

  您可以使用此版本的命令根据输入范围字符串生成命令参数。

示例

以下示例将生成一个范围字符串、其输出包含在以下命令示例后面。定义适用场景all Clusters。

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

```
ontap:*:joes-role:readonly:*:/api/cluster
```

ONTAP如何确定访问

要正确设计和实施OAuth2.0、您需要了解ONTAP如何使用您的授权配置来决定客户端的访问。

第**1**步：独立的范围

如果访问令牌包含任何自包含范围、则ONTAP会首先检查这些范围。如果没有独立范围、请转至步骤2。

如果存在一个或多个自包含范围，ONTAP将应用每个范围，直到可以明确地作出*ALLOW或*deny*决定为止。如果做出明确的决定、则处理将结束。

如果ONTAP无法做出明确的访问决定、请继续执行步骤2。

第**2**步：检查本地角色标志

ONTAP将检查标志的值 `use-local-roles-if-present`。对于定义为ONTAP的每个授权服务器、此标志的值会单独设置。

- 如果值为 `true` 继续执行步骤3。
- 如果值为 `false` 处理结束、访问被拒绝。

第**3**步：命名**ONTAP REST**角色

如果访问令牌包含一个命名的REST角色、则ONTAP将使用该角色来决定访问权限。这始终会导致*ALLOW或*deny*决定和处理结束。

如果没有已命名的REST角色或未找到此角色、请继续执行步骤4。

第**4**步：本地**ONTAP**用户

从访问令牌中提取用户名、并尝试将其与本地ONTAP用户匹配。

如果匹配了本地ONTAP用户、则ONTAP将使用为该用户定义的角色来决定访问权限。这始终会导致*ALLOW或*deny*决定和处理结束。

如果本地ONTAP用户不匹配或访问令牌中没有用户名、请继续执行步骤5。

第**5**步：组到角色映射

从访问令牌中提取组、并尝试将其与组匹配。这些组使用Active Directory或等效的LDAP服务器进行定义。

如果存在组匹配项、ONTAP将使用为组定义的角色来决定访问权限。这始终会导致*ALLOW或*deny*决定和处理结束。

如果没有组匹配项或访问令牌中没有组、则会拒绝访问并结束处理。

OAuth2.0部署方案

在为ONTAP定义授权服务器时、可以使用多个配置选项。根据这些选项、您可以创建适合您的部署环境的授权服务器。

配置参数摘要

在为ONTAP定义授权服务器时、可以使用多个配置参数。通常、所有管理界面都支持这些参数。

根据ONTAP管理界面的不同、参数名称可能略有不同。例如、在配置远程自省时、可以使用命令行界面命令参数来标识端点 `-introspection-endpoint`。但对于System Manager、等效字段为_Authorizationserver令牌自省URI_。为了支持所有ONTAP管理界面、提供了参数的常规问题描述。根据上下文、确切的参数或字段应显而易见。

参数	Description
Name	ONTAP已知的授权服务器名称。
应用程序	ONTAP内部应用程序定义适用场景。此参数必须为*http*。
颁发者URI	FQDN、其中包含用于标识发出令牌的站点或组织的路径。
提供程序JWKS URI	包含路径和文件名的FQDN、ONTAP可从中获取用于验证访问令牌的JSON Web密钥集。
JWKS刷新间隔	确定ONTAP刷新提供程序JWKS URI中证书信息的频率的时间间隔。该值以ISO－8601格式指定。
自省端点	包含ONTAP用于通过自省执行远程令牌验证的路径的FQDN。
客户端 ID	在授权服务器上定义的客户端名称。如果包含此值、则还需要根据接口提供关联的客户端密钥。
传出代理	这是为了在ONTAP受防火墙保护时提供对授权服务器的访问。此URI必须采用CURL格式。
使用本地角色(如果存在)	一个布尔值标志、用于确定是否使用本地ONTAP定义、包括已命名的REST角色和本地用户。
删除用户声明	ONTAP用于匹配本地用户的备用名称。使用 `sub` 字段以匹配本地用户名。

部署方案

下面介绍了几种常见的部署情形。它们是根据ONTAP在本地执行令牌验证还是授权服务器在远程执行令牌验证进行组织的。每个方案都包含一个所需配置选项的列表。请参见 "在ONTAP中部署OAuth2.0" 有关配置命令的示例。

> 定义授权服务器后、您可以通过ONTAP管理界面显示其配置。例如、使用命令 `security oauth2 client show` 使用ONTAP命令行界面。

本地验证

以下部署方案基于ONTAP在本地执行令牌验证的结果。

无需代理即可使用自包含范围

这是仅使用OAuth2.0自包含范围的最简单部署。不使用任何本地ONTAP标识定义。您需要包含以下参数：

- Name
- 应用程序(http)
- 提供程序JWKS URI
- 颁发者URI

您还需要在授权服务器上添加范围。

将自包含范围与代理结合使用

此部署方案使用OAuth2.0自包含范围。不使用任何本地ONTAP标识定义。但授权服务器受防火墙保护、因此您需要配置代理。您需要包含以下参数：

- Name
- 应用程序(http)
- 提供程序JWKS URI
- 传出代理
- 颁发者URI
- audience

您还需要在授权服务器上添加范围。

使用本地用户角色以及代理的默认用户名映射

此部署方案使用具有默认名称映射的本地用户角色。远程用户声明使用的默认值 `sub` 因此、访问令牌中的此字段用于匹配本地用户名。用户名不得超过40个字符。授权服务器受防火墙保护、因此您还需要配置代理。您需要包含以下参数：

- Name
- 应用程序(http)
- 提供程序JWKS URI
- 使用本地角色(如果存在) (`true`)
- 传出代理
- 颁发者

您需要确保将本地用户定义为ONTAP。

使用本地用户角色和代理的备用用户名映射

此部署方案使用本地用户角色以及用于匹配本地ONTAP用户的备用用户名。授权服务器受防火墙保护、因此您需要配置代理。您需要包含以下参数：

- Name
- 应用程序(http)
- 提供程序JWKS URI
- 使用本地角色(如果存在) (`true`)
- 远程用户声明
- 传出代理
- 颁发者URI
- audience

您需要确保将本地用户定义为ONTAP。

远程自省

以下部署配置基于ONTAP通过自省远程执行令牌验证。

使用不带代理的独立范围

这是一个基于使用OAuth2.0独立范围的简单部署。未使用任何ONTAP标识定义。必须包含以下参数：

- Name
- 应用程序(http)
- 自省端点
- 客户端 ID
- 颁发者URI

您需要在授权服务器上定义范围以及客户端和客户端密钥。

使用相互**TLS**进行客户端身份验证

根据您的安全需求、您可以选择配置相互TLS (MTLS)以实施强大的客户端身份验证。在OAuth2.0部署中与ONTAP结合使用时、MTLS保证访问令牌仅供最初发出访问令牌的客户端使用。

采用**OAuth2.0**的相互**TLS**

传输层安全(Transport Layer Security、TLS)用于在两个应用程序(通常是客户端浏览器和Web服务器)之间建立安全通信通道。相互TLS通过客户端证书提供客户端的强标识来扩展这一功能。在ONTAP集群中与OAuth2.0结合使用时、可以通过创建和使用受发件人限制的访问令牌来扩展基本MTLS功能。

受发件人限制的访问令牌只能由最初颁发该令牌的客户端使用。为了支持此功能、请提交一份新的确认款项申请(`cnf`)将插入令牌中。字段包含属性 `x5t#S256` 用于保存请求访问令牌时使用的客户端证书摘要。在验证令牌时、ONTAP会验证此值。授权服务器发放的非发件人限制的访问令牌不包括额外的确认款项申请。

您需要将ONTAP配置为对每个授权服务器单独使用MTLS。例如、CLI命令 `security oauth2 client` 包括参数 `use-mutual-tls` 根据下表所示的三个值控制MTLS处理。

> 在每个配置中、ONTAP的结果和采取的操作取决于配置参数值以及访问令牌和客户端证书的内容。表中的参数按限制性从低到大的排列。

参数	**Description**
无	授权服务器已完全禁用OAuth2.0相互TLS身份验证。ONTAP不会执行MTLS客户端证书身份验证、即使令牌中存在确认声明或随TLS连接提供了客户端证书也是如此。
请求	如果客户端提供受发件人限制的访问令牌、则会强制实施OAuth2.0相互TLS身份验证。也就是说、只有在确认请求(带有属性 `x5t#S256`)。这是默认设置。
Required	对授权服务器颁发的所有访问令牌强制实施OAuth2.0相互TLS身份验证。因此、所有访问令牌都必须受发件人限制。如果访问令牌中不存在确认请求或存在无效的客户端证书、则身份验证和REST API请求将失败。

高级别实施流程

下面介绍了在ONTAP环境中将MTLS与OAuth2.0结合使用时所涉及的典型步骤。请参见 "RFC 8705：《OAuth2.0相互TLS客户端身份验证和受证书制约的访问令牌》" 有关详细信息：

第**1**步：创建并安装客户端证书

建立客户端身份的基础是证明了解客户端专用密钥。相应的公共密钥将放置在客户端提供的签名X.509证书中。总体而言、创建客户端证书涉及的步骤包括：

1. 生成公共密钥对和专用密钥对
2. 创建证书签名请求
3. 将CSR文件发送到知名的CA
4. CA会验证此请求并颁发签名证书

通常、您可以在本地操作系统中安装客户端证书、也可以直接使用cURL等通用实用程序来使用此证书。

第**2**步：配置**ONTAP**以使用**MTLS**

您需要将ONTAP配置为使用MTLS。此配置是针对每个授权服务器单独完成的。例如、使用命令行界面命令 `security oauth2 client` 与可选参数结合使用 `use-mutual-tls`。请参见 "在ONTAP中部署OAuth2.0" 有关详细信息 ...

第**3**步：客户端请求访问令牌

客户端需要从配置为ONTAP的授权服务器请求访问令牌。客户端应用程序必须将MTLS与步骤1中创建和安装的证书结合使用。

第**4**步：授权服务器生成访问令牌

授权服务器验证客户端请求并生成访问令牌。在此过程中、它会创建客户端证书的消息摘要、此摘要会作为确认请求包含在令牌中(字段 `cnf`）。

第**5**步：客户端应用程序将访问令牌提供给**ONTAP**

客户端应用程序对ONTAP集群进行REST API调用、并将访问令牌作为*承载令牌*包含在授权请求标头中。客户端使用的MTLS必须与请求访问令牌所用的证书相同。

第**6**步：**ONTAP**验证客户端和令牌。

ONTAP接收HTTP请求中的访问令牌以及用作MTLS处理一部分的客户端证书。ONTAP首先验证访问令牌中的签名。ONTAP会根据配置生成客户端证书的消息摘要，并将其与令牌中的确认声明*cnf*进行比较。如果这两个值匹配、则ONTAP已确认发出API请求的客户端与最初向其发出访问令牌的客户端相同。

配置和部署

准备使用**ONTAP**部署**OAuth2.0**

在ONTAP环境中配置OAuth2.0之前、您应做好部署准备。主要任务和决定摘要如下。各部分的排列通常与您应遵循的顺序一致。但是、虽然它适用于大多数部署、但您应根据需要对其进行调整以适应您的环境。您还应考虑制定正式的部署计划。

> 您可以根据您的环境为定义给ONTAP的授权服务器选择配置。其中包括您需要为每种部署类型指定的参数值。请参见 "OAuth2.0部署方案" 有关详细信息 ...

受保护的资源和客户端应用程序

OAuth2.0是一个授权框架、用于控制对受保护资源的访问。因此、任何部署的重要第一步都是确定可用资源是什么以及哪些客户端需要访问这些资源。

识别客户端应用程序

您需要确定哪些客户端在发出REST API调用时将使用OAuth2.0、以及它们需要访问哪些API端点。

查看现有**ONTAP REST**角色和本地用户

您应查看现有ONTAP标识定义、包括REST角色和本地用户。根据您配置OAuth2.0的方式、可以使用这些定义来决定访问。

全局过渡到**OAuth2.0**

虽然您可以逐步实施OAuth2.0授权、但也可以通过为每个授权服务器设置一个全局标志、将所有REST API客户端立即迁移到OAuth2.0。这样、无需创建独立的范围、即可根据现有ONTAP配置做出访问决策。

授权服务器

授权服务器通过颁发访问令牌并强制实施管理策略、在OAuth2.0部署中发挥着重要作用。

选择并安装授权服务器

您需要选择并安装一个或多个授权服务器。熟悉身份提供程序的配置选项和过程非常重要，包括如何定义范围。

确定是否需要安装授权根**CA**证书

ONTAP使用授权服务器的证书来验证客户端提供的签名访问令牌。为此、ONTAP需要根CA证书和任何中间证书。这些可能已随ONTAP预安装。如果不是、则需要安装它们。

评估网络位置和配置

如果授权服务器受防火墙保护、则需要将ONTAP配置为使用代理服务器。

客户端身份验证和授权

您需要考虑客户端身份验证和授权的几个方面。

自包含范围或本地**ONTAP**标识定义

概括地说、您可以定义在授权服务器上定义的自包含范围、也可以依赖现有的本地ONTAP身份定义(包括角色和用户)。

具有本地**ONTAP**处理的选项

如果您使用ONTAP标识定义、则必须确定要应用的定义、包括：

- 已命名REST角色
- 匹配本地用户
- Active Directory或LDAP组

本地验证或远程自省

您需要确定访问令牌是由ONTAP在本地验证、还是通过自省在授权服务器验证。此外、还需要考虑几个相关值、例如刷新间隔。

受发件人限制的访问令牌

对于需要高级别安全性的环境、您可以使用基于MTLS的发送受限访问令牌。这要求每个客户端都有一个证书。

管理界面

您可以通过任意ONTAP接口来管理OAuth2.0、其中包括：

- 命令行界面
- System Manager
- REST API

客户端如何请求访问令牌

客户端应用程序必须直接从授权服务器请求访问令牌。您需要决定如何执行此操作、包括授予类型。

配置 ONTAP

您需要执行多个ONTAP配置任务。

定义**REST**角色和本地用户

根据您的授权配置、可以使用本地ONTAP标识处理。在这种情况下、您需要查看并定义REST角色和用户定义。

核心配置

执行核心ONTAP配置需要三个主要步骤、其中包括：

- (可选)为签署授权服务器证书的CA安装根证书(以及任何中间证书)。
- 定义授权服务器。
- 为集群启用OAuth2.0处理。

在**ONTAP**中部署**OAuth2.0**

部署核心OAuth2.0功能主要包括三个步骤。

开始之前

在配置ONTAP之前、您必须为OAuth2.0部署做准备。例如、您需要评估授权服务器、包括其证书的签名方式以及是否位于防火墙之后。请参见 "准备使用ONTAP部署OAuth2.0" 有关详细信息 …

第**1**步：安装身份验证服务器证书

ONTAP包含大量预安装的根CA证书。因此、在许多情况下、ONTAP将立即识别授权服务器的证书、而无需进行额外配置。但是、根据授权服务器证书的签名方式、您可能需要安装根CA证书和任何中间证书。

如果需要、请按照下面提供的说明安装证书。您应在集群级别安装所有必需的证书。

根据您访问ONTAP的方式选择正确的操作步骤。

示例 **1.** 步骤

System Manager

1. 在System Manager中、选择*集群*>*设置*。
2. 向下滚动到*Security*部分。
3. 单击*Certificates*旁边的*→*。
4. 在“可信证书颁发机构”选项卡下，单击“添加”。
5. 单击*Import*并选择证书文件。
6. 完成环境的配置参数。
7. 单击 * 添加 * 。

命令行界面

1. 开始安装：

   ```
   security certificate install -type server-ca
   ```

2. 查找以下控制台消息：

   ```
   Please enter Certificate: Press <Enter> when done
   ```

3. 使用文本编辑器打开证书文件。
4. 复制整个证书、包括以下行：

   ```
   -----BEGIN CERTIFICATE-----

   -----END CERTIFICATE-----
   ```

5. 在命令提示符后、将证书粘贴到终端中。
6. 按*Enter*键完成安装。
7. 使用以下方法之一确认已安装证书：

   ```
   security certificate show-user-installed

   security certificate show
   ```

第**2**步：配置授权服务器

您需要为ONTAP至少定义一个授权服务器。您应根据配置和部署计划选择参数值。请查看 "OAuth2部署方案" 以确定您的配置所需的确切参数。

> 要修改授权服务器定义，您可以删除现有定义并创建新定义。

下面提供的示例基于第一个简单部署方案、部署方案位于 "本地验证"。自包含范围不需要代理即可使用。

根据您访问ONTAP的方式选择正确的操作步骤。命令行界面操作步骤使用符号变量、您需要在发出命令之前替

换这些变量。

示例 **2.** 步骤

System Manager

1. 在System Manager中、选择*集群*>*设置*。
2. 向下滚动到*Security*部分。
3. 单击*OAuth2.0 authorizes*旁边的*+*。
4. 选择*更多选项*。
5. 为您的部署提供所需的值、例如：
   - Name
   - 应用程序(http)
   - 提供程序JWKS URI
   - 颁发者URI
6. 单击 * 添加 * 。

命令行界面

1. 重新创建定义：

```
security oauth2 client create -config-name <NAME> -provider-jwks-uri
<URI_JWKS> -application http -issuer <URI_ISSUER>
```

例如：

```
security oauth2 client create \
-config-name auth0 \
-provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-
realm/protocol/openid-connect/certs \
-application http \
-issuer https://superzap.dev.netapp.com:8443/realms/my-realm
```

第3步：启用OAuth2.0

最后一步是启用OAuth2.0。这是ONTAP集群的全局设置。

> 在确认ONTAP、授权服务器和任何支持服务均已正确配置之前、请勿启用OAuth2.0处理。

根据您访问ONTAP的方式选择正确的操作步骤。

示例 **3.** 步骤

System Manager

1. 在System Manager中、选择*集群*>*设置*。
2. 向下滚动到*安全性部分*。
3. 单击*OAuth2.0 authorizes*旁边的*→*。
4. 启用*OAuth2.0授权*。

命令行界面

1. 启用OAuth2.0：

   ```
   security oauth2 modify -enabled true
   ```

2. 确认已启用OAuth2.0：

   ```
   security oauth2 show
   Is OAuth 2.0 Enabled: true
   ```

使用**OAuth2.0**对**REST API**调用执行问题描述

ONTAP中的OAuth2.0实施支持REST API客户端应用程序。您可以使用cURL对简单的REST API调用进行问题描述、以便开始使用OAuth2.0。以下示例将检索ONTAP集群版本。

开始之前

您必须为ONTAP集群配置并启用OAuth2.0功能。其中包括定义授权服务器。

第**1**步：获取访问令牌

您需要获取用于REST API调用的访问令牌。令牌请求在ONTAP之外执行、确切的操作步骤取决于授权服务器及其配置。您可以通过Web浏览器、使用CURL命令或使用编程语言来请求令牌。

为了便于说明、下面提供了一个示例、说明如何使用CURL从Key斗 篷请求访问令牌。

Keyloak示例

```
curl --request POST \
--location
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-
connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=dp-client-1' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'client_secret=5iTUf9QKLGxAoYa1iR33vlD5A2xq09V7'
```

您应复制并保存返回的令牌。

第2步：对REST API调用执行问题描述操作

获得有效的访问令牌后、您可以使用带有访问令牌的cURL命令对问题描述A REST API调用进行访问。

参数和变量

下表介绍了cURL示例中的两个变量。

变量	Description
$FQDN_IP	ONTAP管理LIF的完全限定域名或IP地址。
$access_令牌	授权服务器发出的OAuth2.0访问令牌。

您应先在Bash Shell环境中设置这些变量、然后再执行此CURL示例。例如、在Linux命令行界面中键入以下命令以设置和显示FQDN变量：

```
FQDN_IP=172.14.31.224
echo $FQDN_IP
172.14.31.224
```

在本地bash shell中定义了这两个变量后、您可以复制此URL命令并将其粘贴到命令行界面中。按*Enter*键替换变量并问题描述命令。

curl 示例

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster?fields=version" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $ACCESS_TOKEN"
```

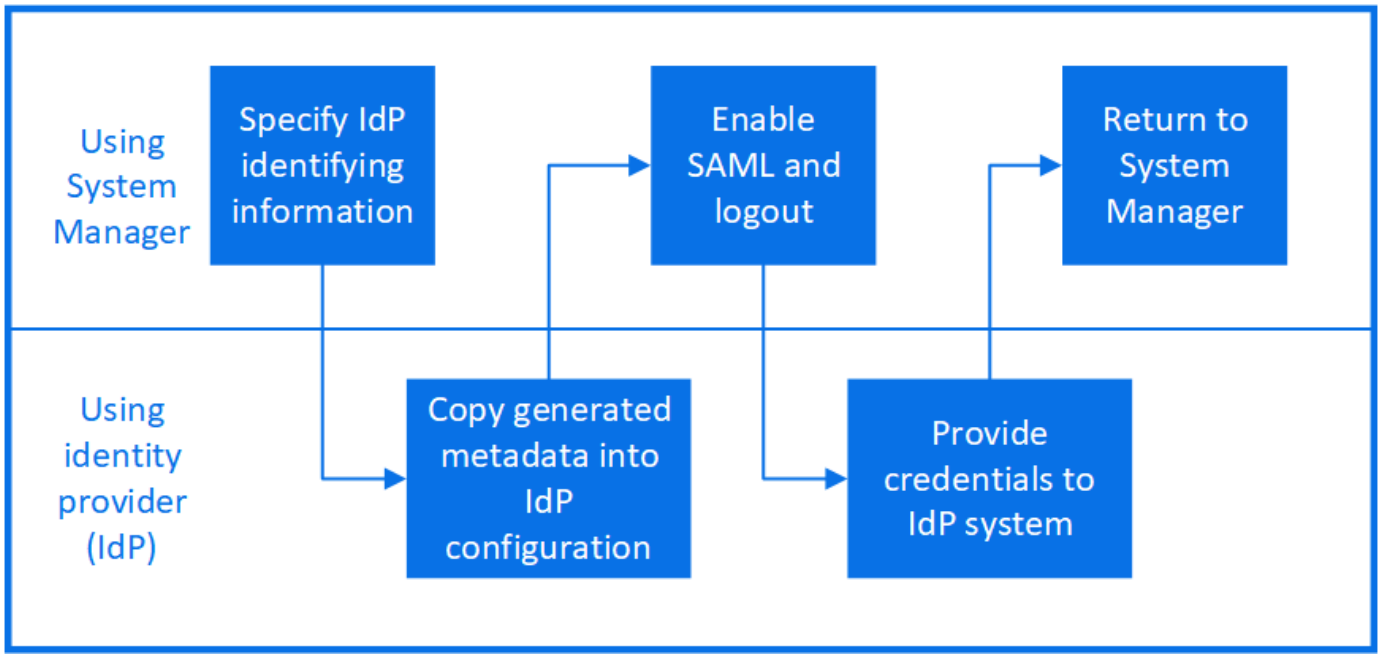
配置 SAML 身份验证

从 ONTAP 9.3 开始，您可以为 Web 服务配置安全断言标记语言（SAML）身份验证。配置并启用 SAML 身份验证后，用户将通过外部身份提供程序（Identity Provider， IdP）进行身份验证，而不是 Active Directory 和 LDAP 等目录服务提供程序进行身份验证。

启用 SAML 身份验证

要使用System Manager或命令行界面启用SAML身份验证、请执行以下步骤。如果集群运行的是ONTAP 9.7或更早版本、则需要遵循的System Manager步骤有所不同。请参阅系统上提供的System Manager联机帮助。

> 启用SAML身份验证后、只有远程用户才能访问System Manager图形用户界面。启用 SAML 身份验证后，本地用户无法访问 System Manager 图形用户界面。



开始之前

- 必须配置计划用于远程身份验证的 IdP 。

  > 请参见您配置的 IdP 提供的文档。

- 您必须具有 IdP 的 URI 。

关于此任务

- SAML身份验证仅适用于 `http` 和 `ontapi` 应用程序。

  。 `http` 和 `ontapi` 应用程序由以下Web服务使用：服务处理器基础架构、ONTAP API或System Manager。

- SAML 身份验证仅适用于访问管理 SVM 。

以下IDP已通过System Manager的验证：

- Active Directory联合身份验证服务
- Cisco Duo (已通过以下ONTAP版本的验证：)
  - 9.7P21及更高版本9.7 (请参阅 "System Manager经典文档")
  - 9.8P17及更高版本9.8
  - 9.9.1P13及更高版本9.9
  - 9.10.1P9及更高版本9.10
  - 9.11.1P4及更高的9.11版本
  - 9.12.1及更高版本
- Shibboleth

根据您的环境执行以下步骤：

示例 **4.** 步骤

System Manager

1. 单击 * 集群 > 设置 * 。
2. 单击 * SAML 身份验证 * 旁边的 ⚙。
3. 确保选中 * 启用 SAML 身份验证 * 复选框。
4. 输入 IdP URI 的 URL （包括 "https://"）。
5. 根据需要修改主机系统地址。
6. 确保使用的证书正确：
   - 如果您的系统只映射了一个类型为 "server" 的证书，则该证书将被视为默认证书，不会显示。
   - 如果您的系统使用多个证书映射为类型 "server" ，则会显示其中一个证书。 要选择其他证书，请单击 * 更改 * 。
7. 单击 * 保存 * 。此时将显示一个确认窗口，其中包含已自动复制到剪贴板的元数据信息。
8. 转到指定的 IdP 系统，然后从剪贴板复制元数据以更新系统元数据。
9. 返回到确认窗口（在 System Manager 中）并选中复选框 * 我已使用主机 URI 或元数据配置 IdP * 。
10. 单击 * 注销 * 以启用基于 SAML 的身份验证。 IdP 系统将显示身份验证屏幕。
11. 在 IdP 系统中，输入基于 SAML 的凭据。验证凭据后，您将转到 System Manager 主页。

命令行界面

1. 创建 SAML 配置，以便 ONTAP 可以访问 IdP 元数据：

   `security saml-sp create -idp-uri` *`idp_uri`* `-sp-host` *`ontap_host_name`*

   `idp_uri` 是可从中下载IdP元数据的IdP主机的FTP或HTTP地址。

   `ontap_host_name` 是SAML服务提供程序主机的主机名或IP地址、此处为ONTAP系统。默认情况下，使用集群管理 LIF 的 IP 地址。

   您可以选择提供 ONTAP 服务器证书信息。默认情况下，使用 ONTAP Web 服务器证书信息。

```
cluster_12::> security saml-sp create -idp-uri
https://example.url.net/idp/shibboleth

Warning: This restarts the web server. Any HTTP/S connections that
are active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 179] Job succeeded: Access the SAML SP metadata using the URL:
https://10.0.0.1/saml-sp/Metadata

Configure the IdP and Data ONTAP users for the same directory server
domain to ensure that users are the same for different
authentication methods. See the "security login show" command for
the Data ONTAP user configuration.
```

此时将显示用于访问 ONTAP 主机元数据的 URL 。

2. 在 IdP 主机中，使用 ONTAP 主机元数据配置 IdP 。

   有关配置 IdP 的详细信息，请参见 IdP 文档。

3. 启用 SAML 配置：

   security saml-sp modify -is-enabled true

   访问的任何现有用户 `http` 或 `ontapi` 系统会自动为应用程序配置SAML身份验证。

4. 如果要为创建用户 `http` 或 `ontapi` 应用程序在配置SAML后、指定SAML作为新用户的身份验证方法。

   a. 使用SAML身份验证为新用户创建登录方法：

      security login create -user-or-group-name *user_name* -application [http | ontapi] -authentication-method saml -vserver *svm_name*

      ```
      cluster_12::> security login create -user-or-group-name admin1
      -application http -authentication-method saml -vserver
      cluster_12
      ```

   b. 验证是否已创建此用户条目：

      security login show

```
cluster_12::> security login show

Vserver: cluster_12

Second
User/Group                  Authentication                 Acct
Authentication
Name            Application Method        Role Name        Locked
Method
-------------- ----------- ------------- ---------------- ------
--------------
admin           console     password      admin            no
none
admin           http        password      admin            no
none
admin           http        saml          admin            -
none
admin           ontapi      password      admin            no
none
admin           ontapi      saml          admin            -
none
admin           service-processor
                            password      admin            no
none
admin           ssh         password      admin            no
none
admin1          http        password      backup           no
none
**admin1        http        saml          backup           -
none**
```

禁用 SAML 身份验证

如果要停止使用外部身份提供程序（ IdP ）对 Web 用户进行身份验证，则可以禁用 SAML 身份验证。禁用 SAML 身份验证后，将使用已配置的目录服务提供程序（例如 Active Directory 和 LDAP ）进行身份验证。

根据您的环境执行以下步骤：

示例 **5.** 步骤

System Manager

1. 单击 * 集群 > 设置 * 。
2. 在 * SAML 身份验证 * 下，单击 * 已启用 * 切换按钮。
3. 可 选：您也可以单击 ⚙ 选中 * SAML 身份验证 * 旁边的 * 启用 SAML 身份验证 * 复选框。

命令行界面

1. 禁用 SAML 身份验证

   ```
   security saml-sp modify -is-enabled false
   ```

2. 如果您不想再使用 SAML 身份验证或要修改 IdP ，请删除 SAML 配置：

   ```
   security saml-sp delete
   ```

对 SAML 配置问题进行故障排除

如果配置安全断言标记语言（ SAML ）身份验证失败，您可以手动修复 SAML 配置失败的每个节点并从故障中恢复。在修复过程中， Web 服务器将重新启动，并且任何活动的 HTTP 连接或 HTTPS 连接将中断。

关于此任务

配置 SAML 身份验证时， ONTAP 会按节点应用 SAML 配置。启用 SAML 身份验证后，如果存在配置问题，ONTAP 会自动尝试修复每个节点。如果任何节点上的 SAML 配置出现问题，您可以禁用 SAML 身份验证，然后重新启用 SAML 身份验证。有时，即使重新启用 SAML 身份验证， SAML 配置也无法应用于一个或多个节点。您可以确定 SAML 配置失败的节点，然后手动修复该节点。

步骤

1. 登录到高级权限级别：

   ```
   set -privilege advanced
   ```

2. 确定 SAML 配置失败的节点：

   ```
   security saml-sp status show -instance
   ```

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                 Update Status: config-success
                Database Epoch: 9
   Database Transaction Count: 997
                    Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                          Node: node2
                 Update Status: config-failed
                Database Epoch: 9
   Database Transaction Count: 997
                    Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

3. 修复故障节点上的 SAML 配置：

   security saml-sp repair -node *node_name*

```
cluster_12::*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are
active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.
[Job 181] Job success.
```

   Web 服务器将重新启动，并且任何活动的 HTTP 连接或 HTTPS 连接将中断。

4. 验证是否已在所有节点上成功配置 SAML：

   security saml-sp status show -instance

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                Update Status: config-success
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                          Node: node2
                Update Status: **config-success**
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

相关信息

"ONTAP 9命令"

管理 Web 服务

管理 Web 服务概述

您可以为集群或 Storage Virtual Machine （SVM）启用或禁用 Web 服务，显示 Web 服务的设置以及控制某个角色的用户是否可以访问 Web 服务。

您可以通过以下方式管理集群或 SVM 的 Web 服务：

- 启用或禁用特定 Web 服务
- 指定对 Web 服务的访问是否仅限于加密 HTTP （SSL）
- 显示 Web 服务的可用性
- 允许或禁止某个角色的用户访问 Web 服务
- 显示允许访问 Web 服务的角色

要使用户能够访问 Web 服务，必须满足以下所有条件：

- 用户必须经过身份验证。

  例如， Web 服务可能会提示输入用户名和密码。用户的响应必须与有效帐户匹配。

- 必须为用户设置正确的访问方法。

只有对给定 Web 服务使用正确访问方法的用户，身份验证才会成功。ONTAP API Web服务 `ontapi`)、则用户必须具有 `ontapi` 访问方法。对于所有其他Web服务、用户必须具有 `http` 访问方法。

> 您可以使用 `security login` 用于管理用户访问方法和身份验证方法的命令。

- 必须将 Web 服务配置为允许用户的访问控制角色。

> 您可以使用 `vserver services web access` 用于控制角色对Web服务的访问的命令。

如果启用了防火墙，则必须将用于 Web 服务的 LIF 的防火墙策略设置为允许 HTTP 或 HTTPS 。

如果使用 HTTPS 访问 Web 服务，则还必须为提供 Web 服务的集群或 SVM 启用 SSL ，并且必须为集群或 SVM 提供数字证书。

管理对 **Web** 服务的访问

Web 服务是用户可以使用 HTTP 或 HTTPS 访问的应用程序。集群管理员可以设置 Web 协议引擎，配置 SSL ，启用 Web 服务以及使某个角色的用户能够访问 Web 服务。

从 ONTAP 9.6 开始，支持以下 Web 服务：

- 服务处理器基础架构 (`spi`)

  此服务使节点的日志，核心转储和 MIB 文件可通过集群管理 LIF 或节点管理 LIF 进行 HTTP 或 HTTPS 访问。默认设置为 `enabled`。

  在请求访问节点的日志文件或核心转储文件时、 `spi` Web服务会自动创建从一个节点到文件所在的另一节点根卷的挂载点。您无需手动创建挂载点。`。

- ONTAP API (`ontapi`)

  通过此服务，您可以运行 ONTAP API ，以便使用远程程序执行管理功能。默认设置为 `enabled`。

  某些外部管理工具可能需要此服务。例如，如果您使用 System Manager ，则应保持此服务处于启用状态。

- Data ONTAP发现 (`disco`)

  通过此服务，机下管理应用程序可以发现网络中的集群。默认设置为 `enabled`。

- 支持诊断 (`supdiag`)

  此服务可控制对系统上特权环境的访问，以协助分析和解决问题。默认设置为 `disabled`。只有在技术支持的指导下，才应启用此服务。

- System Manager (`sysmgr`)

  此服务用于控制 ONTAP 附带的 System Manager 的可用性。默认设置为 `enabled`。此服务仅在集群上受支持。

- 固件基板管理控制器(BMC)更新 (`FW_BMC`)

  通过此服务，您可以下载 BMC 固件文件。默认设置为 `enabled`。

- ONTAP 文档 (`docs`)

  通过此服务可以访问 ONTAP 文档。默认设置为 `enabled`。

- ONTAP REST API (`docs_api`)

  通过此服务，您可以访问 ONTAP RESTful API 文档。默认设置为 `enabled`。

- 文件上传和下载 (`fud`)

  此服务提供文件上传和下载。默认设置为 `enabled`。

- ONTAP消息传送 (`ontapmsg`)

  此服务支持发布和订阅界面，允许您订阅事件。默认设置为 `enabled`。

- ONTAP门户 (`portal`)

  此服务将网关实施到虚拟服务器中。默认设置为 `enabled`。

- ONTAP restful界面 (`rest`)

  此服务支持 RESTful 接口，用于远程管理集群基础架构的所有要素。默认设置为 `enabled`。

- 安全断言标记语言(SAML)服务提供程序支持 (`saml`)

  此服务可提供支持 SAML 服务提供程序的资源。默认设置为 `enabled`。

- SAML服务提供程序 (`saml-sp`)

  此服务可为服务提供商提供 SP 元数据和断言使用者服务等服务。默认设置为 `enabled`。

从 ONTAP 9.7 开始，支持以下附加服务：

- 配置备份文件 (`backups`)

  使用此服务可以下载配置备份文件。默认设置为 `enabled`。

- ONTAP安全性 (`security`)

  此服务支持 CSRF 令牌管理以增强身份验证。默认设置为 `enabled`。

管理 **Web** 协议引擎

您可以在集群上配置 Web 协议引擎，以控制是否允许 Web 访问以及可以使用哪些 SSL 版本。您还可以显示 Web 协议引擎的配置设置。

您可以通过以下方式在集群级别管理 Web 协议引擎：

- 您可以使用指定远程客户端是否可以使用HTTP或HTTPS访问Web服务内容 `system services web modify` 命令 `-external` 参数。
- 您可以使用指定是否应使用SSLv3进行安全Web访问 `security config modify` 命令 `-supported -protocol` 参数。
  默认情况下， SSLv3 处于禁用状态。传输层安全 1.0 （ TLSv1.0 ）已启用，可以根据需要将其禁用。
- 您可以为集群范围控制平面 Web 服务接口启用联邦信息处理标准（ Federal Information Processing Standard ， FIPS ） 140-2 合规模式。

  > 默认情况下， FIPS 140-2 合规模式处于禁用状态。

  - * 禁用 FIPS 140-2 合规模式 *
    您可以通过设置来启用FIPS 140-2合规模式 `is-fips-enabled` 参数设置为 `true` 。 `security config modify` 命令、然后使用 `security config show` 命令以确认联机状态。
  - * 启用 FIPS 140-2 合规模式 *
    - 从ONTAP 9.11.1开始、TLSv1、TLSv1.1和SSLv3将被禁用、只有TSLv1.2和TSLv1.3保持启用状态。它会影响ONTAP 9内部和外部的其他系统和通信。如果启用FIPS 140-2合规模式、然后再禁用、TLSv1、TLSv1.1和SSLv3将保持禁用状态。TLSv.1或TLSv1.3将保持启用状态、具体取决于先前的配置。
    - 对于9.11.1之前的ONTAP 版本、TLSv1和SSLv3均已禁用、只有TLSv1.1和TLSv1.2保持启用状态。启用 FIPS 140-2 合规模式后， ONTAP 会阻止您同时启用 TLSv1 和 SSLv3 。如果启用 FIPS 140-2 合规模式，然后将其禁用， TLSv1 和 SSLv3 将保持禁用状态，但 TLSv1.2 或 TLSv1.1 和 TLSv1.2 均已启用，具体取决于先前的配置。
- 您可以使用显示集群范围安全性的配置 `system security config show` 命令：

如果启用了防火墙，则必须将用于 Web 服务的逻辑接口（ LIF ）的防火墙策略设置为允许 HTTP 或 HTTPS 访问。

如果使用 HTTPS 访问 Web 服务，则还必须为提供 Web 服务的集群或 Storage Virtual Machine （ SVM ）启用 SSL ，并且必须为集群或 SVM 提供数字证书。

在 MetroCluster 配置中，您对集群上的 Web 协议引擎所做的设置更改不会复制到配对集群上。

用于管理 **Web** 协议引擎的命令

您可以使用 `system services web` 用于管理Web协议引擎的命令。您可以使用 `system services firewall policy create` 和 `network interface modify` 允许Web访问请求通过防火墙的命令。

如果您要 ...	使用此命令 ...
在集群级别配置 Web 协议引擎： • 为集群启用或禁用 Web 协议引擎 • 为集群启用或禁用 SSLv3 • 为安全 Web 服务（ HTTPS ）启用或禁用 FIPS 140-2 合规性	`system services web modify`
显示集群级别的 Web 协议引擎配置，确定 Web 协议是否在整个集群中正常运行，并显示 FIPS 140-2 合规性是否已启用并联机	`system services web show`
显示节点级别的 Web 协议引擎配置以及集群中节点的 Web 服务处理活动	`system services web node show`
创建防火墙策略或将 HTTP 或 HTTPS 协议服务添加到现有防火墙策略中，以允许 Web 访问请求通过防火墙	`system services firewall policy create` 设置 `-service` 参数设置为 `http` 或 `https` 允许Web访问请求通过防火墙。
将防火墙策略与 LIF 关联	`network interface modify` 您可以使用 `-firewall-policy` 用于修改LIF的防火墙策略的参数。

配置对 **Web** 服务的访问

通过配置对 Web 服务的访问，授权用户可以使用 HTTP 或 HTTPS 访问集群或 Storage Virtual Machine （ SVM ）上的服务内容。

步骤

1. 如果启用了防火墙，请确保已在防火墙策略中为用于 Web 服务的 LIF 设置 HTTP 或 HTTPS 访问：

   ⓘ 您可以使用检查是否已启用防火墙 `system services firewall show` 命令：

   a. 要验证是否已在防火墙策略中设置HTTP或HTTPS、请使用 `system services firewall policy show` 命令：

      您可以设置 `-service` 的参数 `system services firewall policy create` 命令 `http` 或 `https` 以启用支持Web访问的策略。

   b. 要验证支持HTTP或HTTPS的防火墙策略是否与提供Web服务的LIF关联、请使用 `network interface show` 命令 `-firewall-policy` 参数。

      您可以使用 `network interface modify` 命令 `-firewall-policy` 用于使LIF的防火墙策略生效的参数。

2. 要配置集群级别的Web协议引擎并使Web服务内容可访问、请使用 `system services web modify` 命令：
3. 如果您计划使用安全Web服务(HTTPS)、请使用为集群或SVM启用SSL并提供数字证书信息 `security ssl modify` 命令：
4. 要为集群或SVM启用Web服务、请使用 `vserver services web modify` 命令：

   必须对要为集群或 SVM 启用的每个服务重复此步骤。

5. 要授权某个角色访问集群或SVM上的Web服务、请使用 `vserver services web access create` 命令：

   您授予访问权限的角色必须已存在。您可以使用显示现有角色 `security login role show` 命令或使用创建新角色 `security login role create` 命令：

6. 对于已授权访问Web服务的角色、请检查的输出、确保为其用户配置了正确的访问方法 `security login show` 命令：

   以访问ONTAP API Web服务 `ontapi`)、则必须为用户配置 `ontapi` 访问方法。要访问所有其他Web服务、必须为用户配置 `http` 访问方法。

   > 您可以使用 `security login create` 用于为用户添加访问方法的命令。

用于管理 **Web** 服务的命令

您可以使用 `vserver services web` 用于管理集群或Storage Virtual Machine (SVM)的Web服务可用性的命令。您可以使用 `vserver services web access` 用于控制角色对Web服务的访问的命令。

如果您要 ...	使用此命令 ...
为集群或 SVM 配置 Web 服务： • 启用或禁用 Web 服务 • 指定是否只能使用 HTTPS 访问 Web 服务	`vserver services web modify`
显示集群或 SVM 的 Web 服务的配置和可用性	`vserver services web show`
授权角色访问集群或 SVM 上的 Web 服务	`vserver services web access create`
显示有权访问集群或 SVM 上的 Web 服务的角色	`vserver services web access show`
阻止角色访问集群或 SVM 上的 Web 服务	`vserver services web access delete`

相关信息

"ONTAP 9命令"

用于管理节点上挂载点的命令

。 `spi` 在请求访问节点的日志文件或核心文件时、Web服务会自动创建从一个节点到另一节点根卷的挂载点。尽管您不需要手动管理挂载点、但也可以使用进行管理 `system node root-mount` 命令

如果您要 ...	使用此命令 ...
手动创建从一个节点到另一节点根卷的挂载点	`system node root-mount create` 从一个节点到另一个节点只能存在一个挂载点。
显示集群中节点上的现有挂载点，包括创建挂载点的时间及其当前状态	`system node root-mount show`
删除从一个节点到另一节点根卷的挂载点，并强制关闭与挂载点的连接	`system node root-mount delete`

相关信息

"ONTAP 9命令"

管理SSL

SSL 协议可通过使用数字证书在 Web 服务器和浏览器之间建立加密连接来提高 Web 访问的安全性。

您可以通过以下方式管理集群或 Storage Virtual Machine （ SVM ）的 SSL：

- 启用 SSL
- 生成并安装数字证书并将其与集群或 SVM 关联
- 显示 SSL 配置以查看是否已启用 SSL ，以及 SSL 证书名称（如果可用）
- 为集群或 SVM 设置防火墙策略，以便可以处理 Web 访问请求
- 定义可使用的 SSL 版本
- 限制对 Web 服务的 HTTPS 请求的访问

用于管理SSL的命令

您可以使用 `security ssl` 用于管理集群或Storage Virtual Machine (SVM)的SSL协议的命令。

如果您要 ...	使用此命令 ...
为集群或 SVM 启用 SSL ，并将数字证书与其关联	`security ssl modify`
显示集群或 SVM 的 SSL 配置和证书名称	`security ssl show`

对 Web 服务访问问题进行故障排除

配置错误发生发生原因 Web 服务访问问题。您可以通过确保 LIF ，防火墙策略， Web 协议引擎， Web 服务，数字证书， 和用户访问授权均已正确配置。

下表可帮助您确定并解决 Web 服务配置错误：

此访问问题 ...	由于此配置错误而发生 ...	要解决此错误 ...
您的Web浏览器将返回 `unable to connect` 或 `failure to establish a connection` 尝试访问Web服务时出错。	您的 LIF 可能配置不正确。	确保您可以对提供 Web 服务的 LIF 执行 ping 操作。 您可以使用 `network ping` 命令对LIF执行ping操作。有关网络配置的信息，请参见 *Network Management Guide* 。
防火墙配置可能不正确。	确保防火墙策略已设置为支持 HTTP 或 HTTPS ，并且已将此策略分配给提供 Web 服务的 LIF 。 您可以使用 `system services firewall policy` 用于管理防火墙策略的命令。您可以使用 `network interface modify` 命令 `-firewall -policy` 用于将策略与LIF关联的参数。	您的 Web 协议引擎可能已禁用。
确保已启用 Web 协议引擎，以便可以访问 Web 服务。 您可以使用 `system services web` 用于管理集群的Web协议引擎的命令。	您的Web浏览器将返回 `not found` 尝试访问Web服务时出错。	此 Web 服务可能已禁用。

此访问问题 ...	由于此配置错误而发生 ...	要解决此错误 ...
确保已分别启用要允许访问的每个 Web 服务。 您可以使用 `vserver services web modify` 命令以启用Web服务以进行访问。	Web 浏览器无法使用用户的帐户名称和密码登录到 Web 服务。	无法对用户进行身份验证，访问方法不正确或用户无权访问 Web 服务。
确保用户帐户存在，并使用正确的访问方法和身份验证方法进行配置。此外，确保用户的角色已获得访问 Web 服务的授权。 您可以使用 `security login` 用于管理用户帐户及其访问方法和身份验证方法的命令。访问ONTAP API Web服务需要 `ontapi` 访问方法。访问所有其他Web服务需要 `http` 访问方法。您可以使用 `vserver services web access` 用于管理角色对Web服务的访问权限的命令。	您使用 HTTPS 连接到 Web 服务，而 Web 浏览器指示您的连接已中断。	您可能未在提供 Web 服务的集群或 Storage Virtual Machine （ SVM ）上启用 SSL 。
确保集群或 SVM 已启用 SSL ，并且数字证书有效。 您可以使用 `security ssl` 用于管理HTTP服务器和的SSL配置的命令 `security certificate show` 用于显示数字证书信息的命令。	您使用 HTTPS 连接到 Web 服务，并且 Web 浏览器指示此连接不可信。	您可能正在使用自签名数字证书。

使用证书验证远程服务器的身份

使用证书概述验证远程服务器的身份

ONTAP 支持使用安全证书功能来验证远程服务器的身份。

ONTAP 软件支持使用以下数字证书功能和协议进行安全连接：

- 联机证书状态协议（ Online Certificate Status Protocol， OCSP ）使用 SSL 和传输层安全（ Transport Layer Security， TLS ）连接验证 ONTAP 服务发出的数字证书请求的状态。默认情况下，此功能处于禁用状态。
- ONTAP 软件附带了一组默认的可信根证书。
- 密钥管理互操作性协议（ Key Management Interoperability Protocol， KMIP ）证书支持对集群和 KMIP 服务器进行相互身份验证。

使用 **OCSP** 验证数字证书是否有效

从 ONTAP 9.2 开始，启用联机证书状态协议（ Online Certificate Status Protocol， OCSP ）后，使用传输层安全（ Transport Layer Security， TLS ）通信的 ONTAP 应用程序可以接收数字证书状态。您可以随时为特定应用程序启用或禁用 OCSP 证书状态检查。默认情况下， OCSP 证书状态检查处于禁用状态。

您需要的内容

要执行此任务、您需要具有高级权限级别访问权限。

关于此任务

OCSP 支持以下应用程序：

- AutoSupport
- 事件管理系统（ EMS ）
- 基于 TLS 的 LDAP
- 密钥管理互操作性协议（ KMIP ）
- 审核日志记录
- FabricPool
- SSH (从ONTAP 9.13.1开始)

步骤

1. 将权限级别设置为高级： `set -privilege advanced`。
2. 要为特定 ONTAP 应用程序启用或禁用 OCSP 证书状态检查，请使用相应的命令。

某些应用程序的 **OCSP** 证书状态检查	使用命令 **...**
enabled	`security config ocsp enable -app` app name

某些应用程序的 **OCSP** 证书状态检查	使用命令 **...**
已禁用	`security config ocsp disable -app app name`

以下命令可为 AutoSupport 和 EMS 启用 OCSP 支持。

```
cluster::*> security config ocsp enable -app asup,ems
```

启用 OCSP 后，应用程序将收到以下响应之一：

- 良好—证书有效，通信继续进行。
- 已撤销—证书被其颁发证书颁发机构永久视为不可信，通信无法继续。
- 未知 - 服务器没有任何有关证书的状态信息，通信无法继续。
- 证书中缺少 OCSP 服务器信息—此服务器就像禁用了 OCSP 一样，并继续进行 TLS 通信，但不会进行状态检查。
- OCSP 服务器无响应—应用程序无法继续。

3. 要对使用 TLS 通信的所有应用程序启用或禁用 OCSP 证书状态检查，请使用相应的命令。

希望所有应用程序的 **OCSP** 证书状态检查为 **...**	使用命令 **...**

enabled	`security config ocsp enable`
	
	`-app all`

已禁用	`security config ocsp disable`
	
	`-app all`

启用后，所有应用程序都会收到签名响应，表示指定的证书正常，已撤销或未知。如果证书已被撤销，则应用程序将无法继续。如果应用程序无法从 OCSP 服务器收到响应，或者服务器无法访问，则应用程序将无法继续。

4. 使用 `security config ocsp show` 命令以显示支持OCSP的所有应用程序及其支持状态。

```
cluster::*> security config ocsp show
         Application                          OCSP Enabled?
         --------------------                 ---------------------
         autosupport                          false
         audit_log                            false
         fabricpool                           false
         ems                                  false
         kmip                                 false
         ldap_ad                              true
         ldap_nis_namemap                     true
         ssh                                  true

         8 entries were displayed.
```

查看基于 TLS 的应用程序的默认证书

从 ONTAP 9.2 开始， ONTAP 为使用传输层安全（Transport Layer Security， TLS）的 ONTAP 应用程序提供了一组默认的可信根证书。

您需要的内容

只有在创建管理 SVM 期间或在升级到 ONTAP 9.2 期间，才会安装默认证书。

关于此任务

当前用作客户端并需要证书验证的应用程序包括 AutoSupport， EMS， LDAP，审核日志记录， FabricPool， 和 KMIP。

证书过期后，系统会调用一条 EMS 消息，请求用户删除证书。只能在高级权限级别删除默认证书。

> 删除默认证书可能会导致某些 ONTAP 应用程序无法按预期运行（例如， AutoSupport 和审核日志记录）。

步骤

1. 您可以使用 security certificate show 命令查看管理员 SVM 上安装的默认证书：

   security certificate show -vserver -type server-ca

```
fas2552-2n-abc-3::*> security certificate show -vserver fas2552-2n-abc-3
-type server-ca
Vserver    Serial Number   Common Name                             Type
---------- --------------- ---------------------------------------
------------
fas2552-2n-abc-3
           01              AAACertificateServices
server-ca
    Certificate Authority: AAA Certificate Services
          Expiration Date: Sun Dec 31 18:59:59 2028
```

对集群和KMIP服务器进行相互身份验证

对集群和 KMIP 服务器进行相互身份验证概述

通过对集群和外部密钥管理器（例如密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）服务器）进行相互身份验证，可以使密钥管理器使用基于 SSL 的 KMIP 与集群进行通信。如果某个应用程序或某些功能（例如存储加密功能）需要使用安全密钥来提供安全数据访问，则可以执行此操作。

为集群生成证书签名请求

您可以使用安全证书 `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。

您需要的内容

要执行此任务，您必须是集群管理员或 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

   有关完整的命令语法，请参见手册页。

   以下命令将使用 SHA256 哈希函数生成的 2 ， 048 位专用密钥创建一个 CSR ，以供自定义公用名为 server1.companyname.com 的公司 IT 部门的软件组使用，该公司位于美国加利福尼亚州的森尼韦尔。SVM 联系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。

```
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 :
24 | Administrator Authentication and RBAC
-----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，然后以电子形式（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。

为集群安装 **CA** 签名的服务器证书

要使 SSL 服务器能够将集群或 Storage Virtual Machine （ SVM ）作为 SSL 客户端进行身份验证，您需要在集群或 SVM 上安装客户端类型的数字证书。然后，将 client-ca 证书提供给 SSL 服务器管理员，以便在服务器上安装。

您需要的内容

您必须已使用在集群或SVM上安装SSL服务器的根证书 `server-ca` 证书类型。

步骤

1. 要使用自签名数字证书进行客户端身份验证、请使用 `security certificate create` 命令 `type client` 参数。
2. 要使用 CA 签名的数字证书进行客户端身份验证，请完成以下步骤：

a. 使用安全证书生成数字证书签名请求(CSR) `generate-csr` 命令：

   ONTAP 将显示 CSR 输出，其中包括证书请求和私钥，并提醒您将输出复制到文件中以供将来参考。

b. 以电子形式（如电子邮件）将 CSR 输出中的证书请求发送到可信 CA 进行签名。

   您应保留一份私钥和 CA 签名证书的副本，以供日后参考。

处理完您的请求后， CA 会向您发送已签名的数字证书。

a. 使用安装CA签名证书 `security certificate install` 命令 `-type client` 参数。
b. 出现提示时，输入证书和私钥，然后按 * 输入 * 。
c. 出现提示时，输入任何其他根证书或中间证书，然后按 * 输入 * 。

   如果某个证书链从可信根 CA 开始，并以向您颁发的 SSL 证书结束，但缺少中间证书，则您需要在集群或 SVM 上安装中间证书。中间证书是由受信任根专门为问题描述最终实体服务器证书颁发的从属证书。结果是证书链，该证书链从可信根 CA 开始，经过中间证书，并以向您颁发的 SSL 证书结束。

3. 提供 `client-ca` 将集群或SVM的证书发给SSL服务器的管理员、以便在服务器上安装。

   带有的security certificATE show命令 `-instance` 和 `-type client-ca` 参数显示 `client-ca` 证书信息。

为 **KMIP** 服务器安装 **CA** 签名的客户端证书

密钥管理互操作性协议（ Key Management Interoperability Protocol ， KMIP ）的证书子类型（ -subtype kmip-cert 参数）以及 client 和 server-ca 类型指定使用此证书对集群和外部密钥管理器（例如 KMIP 服务器）进行相互身份验证。

关于此任务

安装 KMIP 证书以将 KMIP 服务器作为 SSL 服务器向集群进行身份验证。

步骤

1. 使用 `security certificate install` 命令 `-type server-ca` 和 `-subtype kmip-cert` 用于为KMIP服务器安装KMIP证书的参数。
2. 出现提示时，输入证书，然后按 Enter 键。

   ONTAP 会提醒您保留一份证书副本，以供日后参考。

```
cluster1::> security certificate install -type server-ca -subtype kmip-
cert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwXzELMAkG
2JhucwNhkcV8sEVAbkSdjbCxlnRhLQ2pRdKkkirWmnWXbj9T/UWZYB2oK0z5XqcJ
2HUw19JlYD1n1khVdWk/kfVIC0dpImmClr7JyDiGSnoscxlIaU5rfGW/D/xwzoiQ
...
-----END CERTIFICATE-----


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

cluster1::>
```