



管理管理员身份验证和RBAC

ONTAP 9

NetApp
April 24, 2024

目录

- 管理管理员身份验证和RBAC 1
 - 使用 CLI 进行管理员身份验证和 RBAC 概述 1
 - 管理员身份验证和 RBAC 工作流 1
 - 用于管理员身份验证和 RBAC 配置的工作表 2
 - 创建登录帐户 13
 - 管理访问控制角色 26
 - 管理管理员帐户 33
 - 管理多管理员验证 57

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

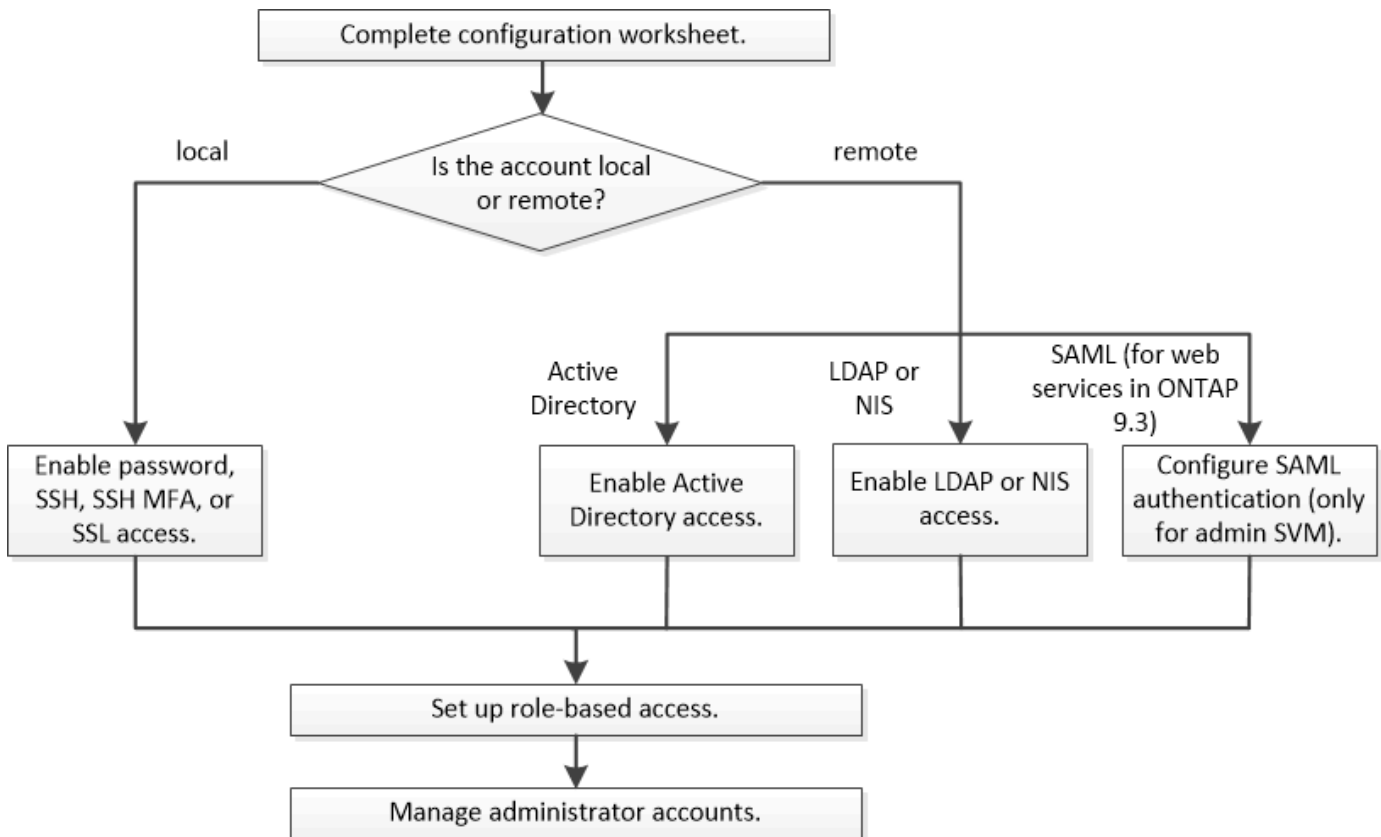
您可以为 ONTAP 集群管理员和 Storage Virtual Machine （ SVM ）管理员启用登录帐户。您还可以使用基于角色的访问控制 （ Role-Based Access Control ， RBAC ）定义管理员的功能。

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
<code>-vserver</code>	帐户访问的Storage VM的名称。默认值为集群的管理Storage VM的名称。	
<code>-user-or-group-name</code>	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。	
<code>-application</code>	用于访问Storage VM的应用程序： <ul style="list-style-type: none"> • http • ontapi • snmp • ssh 	

-authmethod	<p>用于对帐户进行身份验证的方法：</p> <ul style="list-style-type: none"> • 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	<p>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。</p>	
-role	<p>分配给帐户的访问控制角色：</p> <ul style="list-style-type: none"> • 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	<p>（可选）帐户的描述性文本。文本应用双引号（"）括起来。</p>	
-is-ns-switch-group	<p>帐户是LDAP组帐户还是NIS组帐户 (yes 或 no) 。</p>	

-second-authentication-method	<p>多因素身份验证的第二种身份验证方法：</p> <ul style="list-style-type: none"> • 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 <p>身份验证顺序始终是公有密钥和密码。</p>	
-is-ldap-fastbind	<p>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</p> <p>-authentication-method 值必须设置为 nsswitch。 "了解用于nsswitch身份验证的LDAP快速绑定。"</p>	

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	<p>向Duo注册SSH应用程序时获得的API主机名。例如：</p> <pre>api- <HOSTNAME>.duosecurity.com</pre>	
-fail-mode	<p>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 <code>safe</code> (允许访问)或 <code>secure</code> (拒绝访问)。默认值为 <code>safe</code>，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。</p>	
-http-proxy	<p>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：</p> <pre>http- proxy=http://username :password@proxy.example.org:8080</pre>	
-autopush	<p>两者之一 <code>true</code> 或 <code>false</code>。默认值为 <code>false</code>。条件 <code>true</code>，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 <code>false</code>，则系统将提示用户选择一种身份验证方法。</p> <p>配置时 <code>autopush = true</code>，我们建议设置 <code>max-prompts = 1</code>。</p>	

-max-prompts	<p>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。</p> <p>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。</p> <p>配置时 autopush = true, 我们建议设置 max-prompts = 1。</p> <p>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。</p>	
-enabled	<p>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。</p>	

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	<p>(可选) 角色的访问级别。对于命令目录：</p> <ul style="list-style-type: none"> • 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 <p>对于_noninsic commands_(不以 create, modify, delete`或`show)：</p> <ul style="list-style-type: none"> • 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 <p>要授予或拒绝对内部命令的访问权限，必须指定命令目录。</p>	
-query	<p>(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。</p>	

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	<p>(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。</p> <p>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：</p> <ul style="list-style-type: none"> • <code>install</code>：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。 • <code>modify</code>：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。 • <code>delete</code>：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： <ul style="list-style-type: none"> • <code>server</code> 服务器证书和中间证书 • <code>client-ca</code> SSL客户端根CA的公共密钥证书 • <code>server-ca</code> ONTAP为客户端的SSL服务器的根CA的公共密钥证书 • <code>client</code> 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	<p>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) 。</p> <div>  <p>仅支持使用Start TLS访问数据Storage VM。不支持访问管理Storage VM。</p> </div>	
----------------	--	--

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	<ul style="list-style-type: none"> 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	<p>名称服务数据库：</p> <ul style="list-style-type: none"> • <code>hosts</code> 用于文件和DNS名称服务 • <code>group</code> 适用于文件、LDAP和NIS名称服务 • <code>passwd</code> 适用于文件、LDAP和NIS名称服务 • <code>netgroup</code> 适用于文件、LDAP和NIS名称服务 • <code>namemap</code> 用于文件和LDAP名称服务 	
-sources	<p>查找名称服务源的顺序（在逗号分隔列表中）：</p> <ul style="list-style-type: none"> • <code>files</code> • <code>dns</code> • <code>ldap</code> • <code>nis</code> 	

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 `svmin1` 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
svmin1 -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

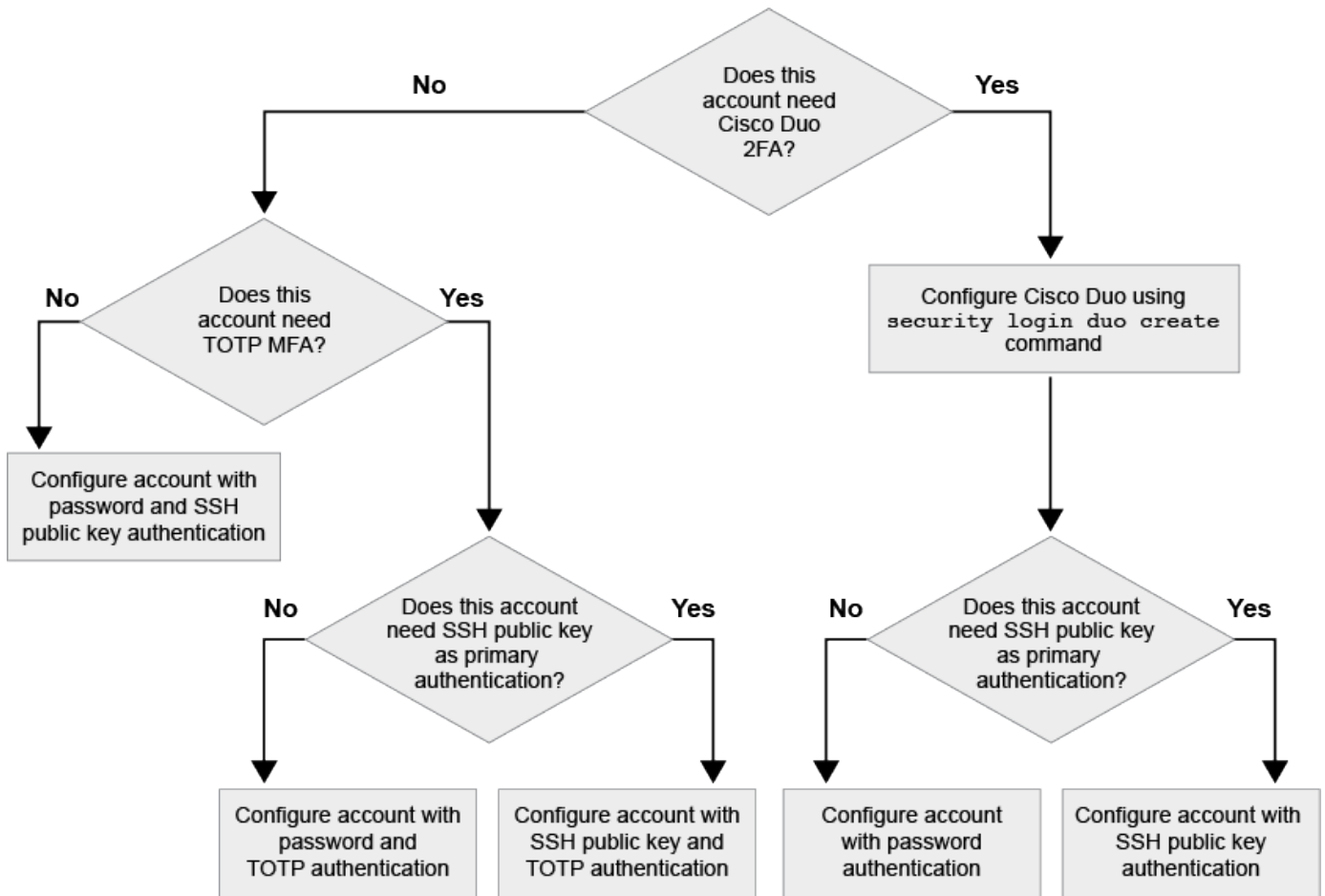
多因素身份验证概述

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FIDO2 (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	<pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role></pre>
9.13.1及更高版本	domain	公共密钥	<p>新用户</p> <pre>security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role></pre> <p>对于现有用户</p> <pre>security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role></pre>
9.0及更高版本	domain	无	<pre>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]</pre>

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	<pre>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]</pre>

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	<ul style="list-style-type: none"> • 所有命令目录 (DEFAULT) • security login rest-role • security login role
只读	<ul style="list-style-type: none"> • 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
<ul style="list-style-type: none"> • 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

<ul style="list-style-type: none"> • security login password <p>仅用于管理自己的用户帐户本地密码和密钥信息</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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销检查的安全性。

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 `svadmin2` 对于SVM `engData2`。公共密钥的索引编号为6。

```
cluster1::> security login publickey create -vserver engData2 -username  
svadmin2 -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 `svadmin2` 对于SVM `engData2` 索引编号为6。

```
cluster1::> security login publickey modify -vserver engData2 -username  
svadmin2 -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 `svadmin3` 对于SVM `engData3` 索引编号为7。

```
cluster1::> security login publickey delete -vserver engData3 -username  
svadmin3 -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、您也可以将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。

```
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
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApTlnzS
xOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJbmXuj6U3alwoUsb13wfEvQnHVFNCi
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBChUAA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
```

Private Key :

-----BEGIN RSA PRIVATE KEY-----

```
MIIBOwIBAAJBAPXFanNoJApTlnzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3alwoUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+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。

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIB8TCCAZugAwIBAwIBADANBgkqhkiG9w0BAQQFADBfMRMwEQYDVQQDEwpuZXRh
cHAuY29tMQswCQYDVQQGEwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNV
BAoTADBJMAcGA1UECzMAMQ8wDQYJKoZIhvcNAQkBFgAwHhcNMTAwNDI2MTk0OTI4
WhcNMTAwNTI2MTk0OTI4WjBfMRMwEQYDVQQDEwpuZXRhY29tMQswCQYDVQQG
EwJVUzEJMAcGA1UECBMAMQkwBwYDVQQHEwAxCTAHBgNVBAoTADBJMAcGA1UECzMA
MQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIaKEAyXrK2sry
-----END CERTIFICATE-----
```

```
Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLyCsUdXA7hXhumHNpvF
C61X2G32Sx8VEa1th94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM70tbUsgPKw+QCCh9dF1jmuQKeDr+wUMWkn1DeGrfhILpzfJGHRlJ
z7UCIQDr8d3gOG71UyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuS18U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEArlmnrFYC8KwE9k7A0ylRzBLdUwK9
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+zCCBGsgAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwwgsxJDAiBgNVBAcTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTTFZhbGlDZXJ0IENsYXNzIDIGUG9saWN5IFZhbGlkYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDEwhodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFroZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECzMOR28gRGFkZkhkQ2xhc3MgMiBDZXJ0
-----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-----
```

```
MIIC5zCCAlACAQEwDQYJKoZIhvcNAQEFBQAwbgsxJDAiBgNVBACtG1ZhbGlDZXJ0
IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAz
BgNVBAsTTFZhbGlDZXJ0IENsYXNzIDIGUG9saWN5IFZhbGlkYXRpb24gQXV0aG9y
aXR5MSEwHwYDVQQDEExodHRwOi8vd3d3LnZhbGljZXJ0LmNvbS8xIDAeBgkqhkiG
9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDtk5MDYyNjAwMTk1NFoXDTE5MDYy
NjAwMTk1NFowgbsxJDAiBgNVBACtG1ZhbGlDZXJ0IFZhbGlkYXRpb24gTmV0d29y
azEXMBUGA1UEChMOVmFsaUNlcnQsIEluYy4xNTAzBgNVBAsTTFZhbGlDZXJ0IENs
YXNzIDIGUG9saWN5IFZhbGlkYXRpb24gQXV0aG9yaXR5MSEwHwYDVQQDEExodHRw
-----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 ...
<ul style="list-style-type: none">• 可信证书颁发机构 *	<ul style="list-style-type: none">• [install-trusted-cert]• [删除可信证书颁发机构]• [续订可信证书颁发机构]
<ul style="list-style-type: none">• 客户端 / 服务器证书 *	<ul style="list-style-type: none">• [install-cs-cert]• [gen-cs-cert]• [delete-cs-cert]• [renew-cs-cert]
<ul style="list-style-type: none">• 本地证书颁发机构 *	<ul style="list-style-type: none">• [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 ... 。
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。

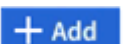
步骤

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 ... 。
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_tunnel"、以便对集群进行AD访问。如果尚未配置 SMB 服务器，则可以在 AD 域上为 SVM 创建计算机帐户。

ONTAP 支持以下域控制器身份验证服务：

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


ONTAP 支持以下会话密钥算法来实现安全的网络登录连接：

会话密钥算法	可用开头为...
HMAC-SHA256 ， 基于高级加密标准（AES） 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_tunnel"、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。客户端与服务端之间的通信使用 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SVMvs1.example.com。系统将提示您输入当前密码，然后输入并重新输入新密码。

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

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 engine_、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	<code>security login show</code>
修改当前管理员的凭据	<code>security login modify <parameters></code>
创建新的管理员帐户	<code>security login create -user-or-group -name <i>admin_name</i> -application ssh -authentication-method password</code>

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	<code>security multi-admin-verify approval-group modify [parameters]</code>
添加或删除成员	<code>security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[,approver2...]] [-approvers-to-remove approver1[,approver2...]]</code>
删除组	<code>security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name</code>

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	<pre>security multi-admin-verify modify -approval-groups group1[,group2...] [- required-approvers nn] -enabled true [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]</pre> <p>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。</p> <pre>cluster-1::> security multi-admin- verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true</pre> <p>至少添加一个以完成初始配置 "操作规则。"</p>
修改MAV配置(需要获得MAV批准)	<pre>security multi-admin-verify approval- group modify [-approval-groups group1 [,group2...]] [-required-approvers nn] [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]</pre>
验证MAV功能	<pre>security multi-admin-verify show</pre> <p>• 示例： *</p> <pre>cluster-1::> security multi-admin- verify show Is Required Execution Approval Approval Enabled Approvers Expiry Expiry Groups ----- true 2 1h 1h mav-grp1</pre>
禁用MAV功能(需要获得MAV批准)	<pre>security multi-admin-verify modify -enabled false</pre>

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功能的管理人员都可以在启用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。

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

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-vsimg20::> 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	<code>security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]</code>
修改当前管理员的凭据	<code>security login modify <parameters></code> 示例：要删除根卷、需要获得以下规则的批准。 <code>security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"</code>
修改规则	<code>security multi-admin-verify rule modify -operation "protected_operation" [parameters]</code>
删除规则	<code>security multi-admin-verify rule delete -operation "protected_operation"</code>
显示规则	<code>security multi-admin-verify rule show</code>

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 voll -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 voll
        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 voll -vserver vs0
```

Info: Volume "voll" 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 voll_*" 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 "voll" 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 voll1
        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 voll1 -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required-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	<code>security multi-admin-verify request approve nn</code>
否决请求	<code>security multi-admin-verify request veto nn</code>
显示所有请求、待处理请求或单个请求	<code>`security multi-admin-verify request { show</code>
<code>show-pending } [nn]</code> <code>{ -fields field1[,field2...]</code>	<code>[-instance]}`</code> 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 <code>-fields</code> 参数)或关于所有字段(使用 <code>-instance</code> 参数)。

如果要...	输入此命令
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
```

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: -
```

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

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

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

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

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

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

商标信息

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