



# 管理多管理员验证

## ONTAP 9

NetApp  
April 24, 2024

# 目录

- 管理多管理员验证..... 1
  - 多管理员验证概述 ..... 1
  - 管理管理员批准组 ..... 4
  - 启用和禁用多管理员验证 ..... 7
  - 管理受保护的操作规则 ..... 10
  - 请求执行受保护操作..... 13
  - 管理受保护的操作请求..... 17

# 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。

<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、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 &lt;parameters&gt;</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	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...]]



如果要...	输入此命令
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::&gt; 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>

如果要...	输入此命令
验证MAV功能	<pre>security multi-admin-verify show</pre> <p>• 示例: *</p> <pre>cluster-1::&gt; 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	<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 &lt;parameters&gt;</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] { -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	Pending 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。