



# 管理访问控制角色

## ONTAP 9

NetApp  
April 24, 2024

# 目录

- 管理访问控制角色..... 1
  - 管理访问控制角色概述..... 1
  - 修改分配给管理员的角色..... 1
  - 定义自定义角色..... 1
  - 集群管理员的预定义角色..... 3
  - SVM 管理员的预定义角色..... 4
  - 控制管理员访问..... 6

# 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"><li>• 所有命令目录 (DEFAULT)</li><li>• security login rest-role</li><li>• security login role</li></ul>
只读	<ul style="list-style-type: none"><li>• security login rest-role create</li><li>• security login rest-role delete</li><li>• security login rest-role modify</li><li>• security login rest-role show</li><li>• security login role create</li><li>• security login role create</li><li>• security login role delete</li><li>• security login role modify</li><li>• security login role show</li><li>• volume activity-tracking</li><li>• volume analytics</li></ul>	无
volume file show-disk-usage	AutoSupport	全部

<ul style="list-style-type: none"> <li>• set</li> <li>• system node autosupport</li> </ul>	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"> <li>• security login password</li> </ul> <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"> <li>• set</li> </ul>	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"> <li>• 管理自己的用户帐户本地密码和密钥信息</li> <li>• 管理卷，卷移动除外</li> <li>• 管理配额， qtree ， Snapshot 副本和文件</li> <li>• 管理 LUN</li> <li>• 执行 SnapLock 操作，但特权删除除外</li> <li>• 配置协议： NFS、 SMB、 iSCSI、 FC、 FCoE、 NVMe/FC和NVMe/TCP</li> <li>• 配置服务： DNS ， LDAP 和 NIS</li> <li>• 监控作业</li> <li>• 监控网络连接和网络接口</li> <li>• 监控 SVM 的运行状况</li> </ul>
vsadmin-volume	<ul style="list-style-type: none"> <li>• 管理自己的用户帐户本地密码和密钥信息</li> <li>• 管理卷，包括卷移动</li> <li>• 管理配额， qtree ， Snapshot 副本和文件</li> <li>• 管理 LUN</li> <li>• 配置协议： NFS、 SMB、 iSCSI、 FC、 FCoE、 NVMe/FC和NVMe/TCP</li> <li>• 配置服务： DNS ， LDAP 和 NIS</li> <li>• 监控网络接口</li> <li>• 监控 SVM 的运行状况</li> </ul>
vsadmin-protocol	<ul style="list-style-type: none"> <li>• 管理自己的用户帐户本地密码和密钥信息</li> <li>• 配置协议： NFS、 SMB、 iSCSI、 FC、 FCoE、 NVMe/FC和NVMe/TCP</li> <li>• 配置服务： DNS ， LDAP 和 NIS</li> <li>• 管理 LUN</li> <li>• 监控网络接口</li> <li>• 监控 SVM 的运行状况</li> </ul>
vsadmin-backup	<ul style="list-style-type: none"> <li>• 管理自己的用户帐户本地密码和密钥信息</li> <li>• 管理 NDMP 操作</li> <li>• 使已还原的卷成为读 / 写卷</li> <li>• 管理 SnapMirror 关系和 Snapshot 副本</li> <li>• 查看卷和网络信息</li> </ul>

vsadmin-SnapLock	<ul style="list-style-type: none"> <li>• 管理自己的用户帐户本地密码和密钥信息</li> <li>• 管理卷，卷移动除外</li> <li>• 管理配额， qtree ， Snapshot 副本和文件</li> <li>• 执行 SnapLock 操作，包括特权删除</li> <li>• 配置协议： NFS和SMB</li> <li>• 配置服务： DNS ， LDAP 和 NIS</li> <li>• 监控作业</li> <li>• 监控网络连接和网络接口</li> </ul>
vsadmin-readonly	<ul style="list-style-type: none"> <li>• 管理自己的用户帐户本地密码和密钥信息</li> <li>• 监控 SVM 的运行状况</li> <li>• 监控网络接口</li> <li>• 查看卷和 LUN</li> <li>• 查看服务和协议</li> </ul>

## 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。

根据您的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。

## 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。