管理访问控制角色
ONTAP 9

NetApp
February 12, 2026

目录

管理访问控制角色

了解如何管理ONTAP访问控制角色

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ONTAP管理员的角色

您可以使用 `security login modify`命令更改集群或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
   ```

   "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
   ```

   有关的详细信息 `security login modify`，请参见"ONTAP 命令参考"。

为ONTAP管理员定义自定义角色

您可以使用 `security login role create`命令定义自定义角色。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
   ```

   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
   ```

   有关的详细信息 `security login role create`，请参见"ONTAP 命令参考"。

相关信息

- "创建安全登录角色"
- "存储聚合丛脱机"
- "存储加密"

ONTAP集群管理员的预定义角色

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

下表列出了集群管理员的预定义角色：

此角色 ...	具有此访问级别 ...	访问以下命令或命令目录
管理员	全部	所有命令目录 (`DEFAULT`)
admin-no-fsa (从ONTAP 9.12.1开始提供)	读 / 写	• 所有命令目录 (`DEFAULT`) • `security login rest-role` • `security login role`

只读	• `security login rest-role create` • `security login rest-role delete` • `security login rest-role modify` • `security login rest-role show` • `security login role create` • `security login role create` • `security login role delete` • `security login role modify` • `security login role show` • `volume activity-tracking` • `volume analytics`	无
`volume file show-disk-usage`	AutoSupport	全部
• `set` • `system node autosupport`	无	所有其他命令目录 (`DEFAULT`)
backup	全部	`vserver services ndmp`
-readonly	`volume`	无
所有其他命令目录 (`DEFAULT`)	-readonly	全部
• `security login password` 仅用于管理自己的用户帐户本地密码和密钥信息 • `set`	• 从ONTAP 9.8开始、只读 • 在ONTAP 9.8之前的版本中、无	`security`

-readonly	所有其他命令目录 (DEFAULT)	SnapLock
全部	• set • volume create • volume modify • volume move • volume show	无
• volume move governor • volume move recommend	无	所有其他命令目录 (DEFAULT)
无	无	所有命令目录 (DEFAULT)

。 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。

相关信息

- "安全登录"
- "设置"
- "volume"
- "Vserver服务NDMP"

ONTAP SVM管理员的预定义角色

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

下表列出了 SVM 管理员的预定义角色：

Role name	功能

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

vsadmin-SnapLock	• 管理自己的用户帐户本地密码和密钥信息 • 管理卷，卷移动除外 • 管理配额、qtrees、快照和文件 • 执行 SnapLock 操作，包括特权删除 • 配置协议：NFS和SMB • 配置服务： DNS ， LDAP 和 NIS • 监控作业 • 监控网络连接和网络接口
vsadmin-readonly	• 管理自己的用户帐户本地密码和密钥信息 • 监控 SVM 的运行状况 • 监控网络接口 • 查看卷和 LUN • 查看服务和协议

使用System Manager管理ONTAP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 → *用户和角色*旁边的。
3. 在*USERS*下选择 + Add 。
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、然后单击该用户名旁边显示的 ⋮ 。
3. 单击 * 编辑 * 。
4. 在 * 角色 * 下拉菜单中选择一个角色。

在ONTAP中访问 JIT 权限提升

从ONTAP 9.17.1 开始，集群管理员可以"配置即时（JIT）权限提升"允许ONTAP用户临时提升其权限以执行某些任务。为用户配置 JIT 后，用户可以将其权限临时提升到具有执行任务所需权限的角色。会话到期后，用户将恢复其原始访问级别。

集群管理员可以配置用户访问 JIT 提升的时长。例如，集群管理员可以将用户访问 JIT 提升的权限配置为每次会话 30 分钟（会话有效期），为期 30 天（JIT 有效期）。在 30 天的期限内，用户可以根据需要多次提升权限，但每次会话的时长限制为 30 分钟。

关于此任务

- JIT 权限提升仅适用于使用 SSH 访问ONTAP的用户。提升的权限仅在当前 SSH 会话中可用，但您可以根据需要在任意数量的并发 SSH 会话中提升权限。
- JIT 权限提升仅支持使用密码、nsswitch 或域身份验证登录的用户。JIT 权限提升不支持多重身份验证 (MFA)。
- 如果配置的会话或 JIT 有效期到期，或者集群管理员撤销用户的 JIT 访问权限，则用户的 JIT 会话将被终止。

开始之前

- 要访问 JIT 权限提升，集群管理员必须为您的帐户配置 JIT 访问权限。集群管理员将确定您可以提升权限的角色，以及您可以访问提升权限的时长。

步骤

1. 暂时将您的权限提升至配置的角色：

```
security jit-privilege elevate
```

输入此命令后，系统会提示您输入登录密码。如果您的帐户配置了 JIT 访问权限，您将在配置的会话时长内获得提升的访问权限。会话时长到期后，您将恢复到原始访问级别。您可以在配置的 JIT 有效期内根据需要多次提升权限。

2. 查看 JIT 会话中的剩余时间：

```
security jit-privilege show-remaining-time
```

如果您当前处于 JIT 会话中，此命令将显示剩余时间。

3. 如果需要，请提前结束 JIT 会话：

```
security jit-privilege reset
```

如果您当前处于 JIT 会话中，此命令将结束 JIT 会话并恢复您的原始访问级别。

在ONTAP中配置 JIT 权限提升

从ONTAP 9.17.1 开始，集群管理员可以配置即时 (JIT) 权限提升，以允许ONTAP用户临时提升其权限以执行某些任务。为用户配置 JIT 后，他们可以临时"提升他们的特权"赋予具有执行任务所需权限的角色。会话持续时间到期后，用户将恢复其原始访问级别。

集群管理员可以配置用户访问 JIT 提升的时长。例如，您可以配置用户访问 JIT 提升的时长，在 30 天的时间段内（即“JIT 有效期”），每次会话的时长限制为 30 分钟（即“会话有效期”）。在这 30 天的时间段内，用户可以根据需要多次提升权限，但每次会话的时长限制为 30 分钟。

JIT 权限提升支持最小权限原则，允许用户执行需要提升权限的任务，而无需永久授予这些权限。这有助于降低未经授权的访问或意外更改系统的风险。以下示例描述了 JIT 权限提升的一些常见用例：

- 允许临时访问 `security login create`和 `security login delete`命令来启用用户的入职和离职。
- 允许临时访问 `system node image update`和 `system node upgrade-revert`在更新窗口期间。更新完成后，命令访问权限将被撤销。
- 允许临时访问 `cluster add-node`， `cluster remove-node`， 和 `cluster modify`以启用集群扩展或重新配置。集群更改完成后，命令访问权限将被撤销。
- 允许临时访问 `volume snapshot restore`启用还原操作和备份目标管理。还原或配置完成后，命令访问权限将被撤销。
- 允许临时访问 `security audit log show`在合规性检查期间启用审计日志审查和导出。

如需查看更详细的常见 JIT 用例列表，请参阅常见的 JIT 用例 。

集群管理员可以为ONTAP用户设置 JIT 访问权限，并在整个集群范围内或为特定 SVM 配置默认 JIT 有效期。

关于此任务

- JIT 权限提升仅适用于使用 SSH 访问ONTAP的用户。提升的权限仅在用户当前的 SSH 会话中可用，但用户可以根据需要在任意数量的并发 SSH 会话中提升权限。
- JIT 权限提升仅支持使用密码、nsswitch 或域身份验证登录的用户。JIT 权限提升不支持多重身份验证 (MFA)。

开始之前

- 您必须是ONTAP集群管理员 `admin`权限级别来执行以下任务。

修改全局 JIT 设置

您可以修改ONTAP集群全局或特定 SVM 的默认 JIT 设置。这些设置决定了已配置 JIT 访问的用户的默认会话有效期和最大 JIT 有效期。

关于此任务

- 默认 `default-session-validity-period`值为一小时。此设置决定用户在 JIT 会话中可以访问提升权限的时间，之后需要重新提升权限。
- 默认 `max-jit-validity-period`值为 90 天。此设置决定了用户在配置的开始日期之后可以访问 JIT 提升权限的最长期限。您可以为单个用户配置 JIT 有效期，但不能超过最长 JIT 有效期。

步骤

1. 检查当前 JIT 设置：

```
security jit-privilege show -vserver <svm_name>
```

`-vserver`是可选的。如果您未指定 SVM，该命令将显示全局 JIT 设置。

2. 全局或针对 SVM 修改 JIT 设置：

```
security jit-privilege modify -vserver <svm_name> -default-session
-validity-period <period> -max-jit-validity-period <period>
```

如果您未指定 SVM，该命令将修改全局 JIT 设置。以下示例将 SVM 的默认 JIT 会话时长设置为 45 分钟，最大 JIT 时长设置为 30 天 `svm1`： +
`security jit-privilege modify -vserver svm1 -default-session-validity-period 45m -max-jit-validity-period 30d`

在此示例中，用户将能够一次访问 45 分钟的 JIT 提升，并且可以在配置的开始日期之后最多 30 天内启动 JIT 会话。

为用户配置 JIT 权限提升访问权限

您可以为ONTAP用户分配 JIT 权限提升访问权限。

步骤

1. 检查用户当前的 JIT 访问权限：

```
security jit-privilege user show -username <username>
```

`-username`是可选的。如果您未指定用户名，该命令将显示所有用户的 JIT 访问权限。

2. 为用户分配新的 JIT 访问权限：

```
security jit-privilege create -username <username> -vserver <svm_name>
-role <rbac_role> -session-validity-period <period> -jit-validity-period
<period> -start-time <date>
```

- 如果 `-vserver`未指定，则在集群级别分配 JIT 访问权限。
- `-role`是用户将被提升到的 RBAC 角色。如果未指定， `-role`默认为 `admin`。
- `-session-validity-period`是用户在需要启动新的 JIT 会话之前可以访问提升角色的时长。如果未指定，则全局或 SVM `default-session-validity-period`被使用。
- `-jit-validity-period`是用户在配置的开始日期之后可以发起 JIT 会话的最长持续时间。如果未指定，则 `session-validity-period`被使用。此参数不能超过全局或 SVM `max-jit-validity-period`。
- `-start-time`是用户可以启动 JIT 会话的日期和时间。如果未指定，则使用当前日期和时间。

  下面的例子将允许 `ontap_user`访问 `admin`角色运行 1 小时后才需要开始新的 JIT 会话。`ontap_user`将能够从 2025 年 7 月 1 日下午 1 点开始启动为期 60 天的 JIT 会话：+
  `security jit-privilege user create -username ontap_user -role admin -session-validity-period 1h -jit-validity-period 60d -start-time "7/1/25 13:00:00"`

3. 如果需要，撤销用户的 JIT 访问权限：

```
security jit-privilege user delete -username <username> -vserver
<svm_name>
```

此命令将撤销用户的 JIT 访问权限，即使其访问权限尚未过期。如果 `-vserver`如果未指定，则 JIT 访问权限将在集群级别撤销。如果用户处于活动的 JIT 会话中，则该会话将被终止。

常见的 JIT 用例

下表包含 JIT 权限提升的常见用例。对于每个用例，都需要配置一个 RBAC 角色来提供对相关命令的访问权限。每个命令都链接到ONTAP命令参考，其中包含有关该命令及其参数的更多信息。

用例	命令	详细信息
用户和角色管理	• `security login create` • `security login delete`	在入职或离职期间临时提升添加/删除用户或更改角色的权限。
证书管理	• `security certificate create` • `security certificate install`	授予证书安装或更新的短期访问权限。

用例	命令	详细信息
SSH/CLI 访问控制	• `security login create -application ssh`	临时授予 SSH 访问权限以进行故障排除或供应商支持。
许可证管理	• `system license add` • `system license delete`	授予在功能激活或停用期间添加或删除许可证的权限。
系统升级和修补	• `system node image update` • `system node upgrade-revert`	提升升级窗口，然后撤销。
网络安全设置	• `security login role create` • `security login role modify`	允许对网络相关的安全角色进行临时更改。
集群管理	• `cluster add-node` • `cluster remove-node` • `cluster modify`	提升集群扩展或重新配置。
SVM 管理	• `vserver create` • `vserver delete` • `vserver modify`	临时授予 SVM 管理员权限以进行配置或停用。
卷管理	• `volume create` • `volume delete` • `volume modify`	提升卷配置、调整大小或删除的权限。
Snapshot 管理	• `volume snapshot create` • `volume snapshot delete` • `volume snapshot restore`	提升快照删除或在恢复期间恢复的权限。
网络配置：	• `network interface create` • `network port vlan create`	授予在维护时段内进行网络更改的权利。

用例	命令	详细信息
磁盘/聚合管理	• `storage disk assign` • `storage aggregate create` • `storage aggregate add-disks`	提升添加或删除磁盘或管理聚合的能力。
数据保护	• `snapmirror create` • `snapmirror modify` • `snapmirror restore`	暂时提升以配置或恢复SnapMirror关系。
性能调优	• `qos policy-group create` • `qos policy-group modify`	提升性能故障排除或调整。
审计日志访问	• `security audit log show`	在合规性检查期间暂时提升审计日志审查或导出权限。
事件和警报管理	• `event notification create` • `event notification modify`	提升配置或测试事件通知或 SNMP 陷阱的权限。
合规性驱动的数据访问	• `volume show` • `security audit log show`	授予审计员临时只读访问权限以审查敏感数据或日志。
特权访问审查	• `security login show` • `security login role show`	暂时提升权限以审查和报告特权访问权限。在限定时间内授予只读权限。

相关信息

- "集群"
- "事件通知"
- "network"
- "QoS策略组"
- "安全性"
- "SnapMirror"
- "存储"
- "系统"
- "volume"

- "vserver"