管理访问控制角色

ONTAP 9

NetApp
April 24, 2024

目录

管理访问控制角色

管理访问控制角色概述

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

修改分配给管理员的角色

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

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 更改集群或 SVM 管理员的角色：

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

   有关完整的命令语法，请参见 "工作表"。

   "创建或修改登录帐户"

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

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

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

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

定义自定义角色

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

关于此任务

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

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

- 特定命令访问或子目录访问将覆盖父目录访问。

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

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

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 定义自定义角色：

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

   有关完整的命令语法，请参见 "工作表"。

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

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

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

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

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

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

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

集群管理员的预定义角色

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

下表列出了集群管理员的预定义角色：

此角色 …	具有此访问级别 …	访问以下命令或命令目录
管理员	全部	所有命令目录 (`DEFAULT`)
admin-no-FSA (从ONTAP 9.12.1开始提供)	读 / 写	• 所有命令目录 (`DEFAULT`) • `security login rest-role` • `security login role`
只读	• `security login rest-role create` • `security login rest-role delete` • `security login rest-role modify` • `security login rest-role show` • `security login role create` • `security login role create` • `security login role delete` • `security login role modify` • `security login role show` • `volume activity-tracking` • `volume analytics`	无
`volume file show-disk-usage`	AutoSupport	全部

• set • system node autosupport	无	所有其他命令目录 (DEFAULT)
backup	全部	vserver services ndmp
-readonly	volume	无
所有其他命令目录 (DEFAULT)	-readonly	全部
• security login password 仅用于管理自己的用户帐户本地密码和密钥信息 • set	无	security
-readonly	所有其他命令目录 (DEFAULT)	无

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

SVM 管理员的预定义角色

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

下表列出了 SVM 管理员的预定义角色：

Role name	功能

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

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

控制管理员访问

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

根据您启用帐户访问的方式，您可能需要执行以下任一操作：

- 将公有密钥与本地帐户关联。
- 安装 CA 签名的服务器数字证书。
- 配置 AD ， LDAP 或 NIS 访问。

您可以在启用帐户访问之前或之后执行这些任务。

将角色分配给管理员

将角色分配给管理员，如下所示：

步骤

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

更改管理员角色

更改管理员的角色，如下所示：

步骤

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