配置基于角色的访问控制（RBAC）

SnapCenter Software 4.8

NetApp
September 26, 2025

This PDF was generated from https://docs.netapp.com/zh-cn/snapcenter-48/install/task_add_a_user_or_group_and_assign_role_and_assets.html on September 26, 2025. Always check docs.netapp.com for the latest.

目录

配置基于角色的访问控制（ RBAC ） . . . 1
添加用户或组并分配角色和资产 . . . 1
创建角色 . . . 3
使用 security login 命令添加 ONTAP RBAC 角色 . . . 4
创建具有最低权限的 SVM 角色 . . . 6
用于创建 SVM 角色和分配权限的 ONTAP 命令行界面命令 . . . 6
创建具有最低权限的 ONTAP 集群角色 . . . 10
用于创建集群角色和分配权限的 ONTAP 命令行界面命令 . . . 10
配置 IIS 应用程序池以启用 Active Directory 读取权限 . . . 16

配置基于角色的访问控制（RBAC）

添加用户或组并分配角色和资产

要为 SnapCenter 用户配置基于角色的访问控制，您可以添加用户或组并分配角色。此角色决定了 SnapCenter 用户可以访问的选项。

- 您需要的内容 *
- 您必须已以 "SnapCenterAdmin" 角色登录。
- 您必须已在操作系统或数据库的 Active Directory 中创建用户或组帐户。您不能使用 SnapCenter 创建这些帐户。

> 从 SnapCenter 4.5 开始，您只能在用户名和组名称中包含以下特殊字符：空格（），连字符（-），下划线（_）和冒号（：）。 如果要使用在早期版本的 SnapCenter 中创建的角色以及这些特殊字符，您可以通过在安装 SnapCenter WebApp 的 web.config 文件中将 "DisableSQLInjectionValidation " 参数的值更改为 true 来禁用角色名称验证。修改此值后，您无需重新启动此服务。

- SnapCenter 包括多个预定义角色。

  您可以将这些角色分配给用户，也可以创建新角色。

- 添加到 SnapCenter RBAC 的 AD 用户和 AD 组必须对 Active Directory 中的用户容器和计算机容器具有读取权限。
- 为包含相应权限的用户或组分配角色后，您必须为用户分配对 SnapCenter 资产（例如主机和存储连接）的访问权限。

  这样，用户就可以执行对分配给他们的资产具有权限的操作。

- 您应在某个时刻为用户或组分配一个角色，以利用 RBAC 权限和效率。
- 您可以分配主机，资源组，策略，存储连接，插件， 创建用户或组时提供给用户的凭据。
- 应分配给用户以执行某些操作的最小资产如下：

操作	资产分配
保护资源	主机，策略
备份	主机，资源组，策略
还原	主机，资源组
克隆	主机，资源组，策略
克隆生命周期	host

操作	资产分配
创建资源组	host

- 将新节点添加到 Windows 集群或 DAG （ Exchange Server 数据库可用性组）资产中后，如果将此新节点分配给用户，则必须将此资产重新分配给用户或组，以便将此新节点包含到用户或组中。

  您应将 RBAC 用户或组重新分配给集群或 DAG ，以便将新节点包含给 RBAC 用户或组。例如，您有一个双节点集群，并且已为此集群分配 RBAC 用户或组。向集群添加另一个节点时，应将 RBAC 用户或组重新分配给集群，以便为 RBAC 用户或组添加新节点。

- 如果您计划复制 Snapshot 副本，则必须将源卷和目标卷的存储连接分配给执行此操作的用户。

  您应先添加资产，然后再为用户分配访问权限。

如果您使用适用于 VMware vSphere 的 SnapCenter 插件功能来保护 VM ， VMDK 或数据存储库，则应使用 VMware vSphere GUI 将 vCenter 用户添加到适用于 VMware vSphere 的 SnapCenter 插件角色中。有关 VMware vSphere 角色的信息，请参见 "适用于 VMware vSphere 的 SnapCenter 插件附带的预定义角色"。

- 步骤 *

1. 在左侧导航窗格中，单击 * 设置 * 。
2. 在设置页面中，单击 * 用户和访问 * >
3. 在从 Active Directory 或工作组添加用户 / 组页面中：

对于此字段 ...	执行此操作 ...
访问类型	选择域或工作组 对于域身份验证类型，您应指定要将用户添加到角色的用户或组的域名。 默认情况下，它会预先填充已登录的域名。 您必须在 * 设置 * > * 全局设置 * > * 域设置 * 页面中注册不可信域。
Type	选择用户或组 SnapCenter 仅支持安全组，而不支持分发组。

对于此字段 ...	执行此操作 ...
用户名	a. 键入部分用户名，然后单击 * 添加 * 。 用户名区分大小写。 b. 从搜索列表中选择用户名。 在添加来自其他域或不可信域的用户时，应完整键入用户名，因为没有跨域用户的搜索列表。 重复此步骤，向选定角色添加其他用户或组。
角色	选择要将用户添加到的角色。

4. 单击 * 分配 * ，然后在分配资产页面中：
   a. 从 * 资产 * 下拉列表中选择资产类型。
   b. 在资产表中，选择资产。

      只有在用户已将资产添加到 SnapCenter 后，才会列出这些资产。

   c. 对所有所需资产重复此操作步骤。
   d. 单击 * 保存 * 。
5. 单击 * 提交 * 。

   添加用户或组并分配角色后，刷新资源列表。

创建角色

除了使用现有 SnapCenter 角色之外，您还可以创建自己的角色并自定义权限。

您应已以 "SnapCenterAdmin" 角色登录。

- 步骤 *

1. 在左侧导航窗格中，单击 * 设置 * 。
2. 在设置页面中，单击 * 角色 * 。
3. 单击 。
4. 在添加角色页面中，指定新角色的名称和问题描述。

从 SnapCenter 4.5 开始，您只能在用户名和组名称中包含以下特殊字符：空格（），连字符（ - ），下划线（ _ ）和冒号（：）。 如果要使用在早期版本的 SnapCenter 中创建的角色以及这些特殊字符，您可以通过在安装 SnapCenter WebApp 的 web.config 文件中将 "DisableSQLInjectionValidation " 参数的值更改为 true 来禁用角色名称验证。修改此值后，您无需重新启动此服务。

5. 选择 * 此角色的所有成员均可查看其他成员的对象 * ，以使该角色的其他成员能够在刷新资源列表后查看卷和主机等资源。

   如果不希望此角色的成员查看分配给其他成员的对象，则应取消选择此选项。

   启用此选项后，如果用户与创建对象或资源的用户具有相同的角色，则不需要为用户分配对对象或资源的访问权限。

1. 在权限页面中，选择要分配给角色的权限，或者单击 * 全选 * 授予该角色的所有权限。
2. 单击 * 提交 * 。

使用 security login 命令添加 ONTAP RBAC 角色

如果存储系统运行的是集群模式 ONTAP ，则可以使用 security login 命令添加 ONTAP RBAC 角色。

- 您需要的内容 *
- 在为运行集群模式 ONTAP 的存储系统创建 ONTAP RBAC 角色之前，您必须确定以下内容：
  - 要执行的一项或多项任务
  - 执行这些任务所需的权限
- 配置 RBAC 角色需要执行以下操作：
  - 为命令和 / 或命令目录授予权限。

    每个命令 / 命令目录有两个访问级别： all-access 和 read-only 。

  您必须始终先分配所有访问权限。

  - 为用户分配角色。
  - 根据 SnapCenter 插件是连接到整个集群的集群管理员 IP 还是直接连接到集群中的 SVM ，更改您的配置。
- 关于此任务 *

要简化在存储系统上配置这些角色的过程，您可以使用适用于 Data ONTAP 的 RBAC User Creator 工具，该工具已发布在 NetApp 社区论坛上。

此工具会自动正确设置 ONTAP 权限。例如，适用于 Data ONTAP 的 RBAC User Creator 工具会自动按正确顺序添加权限，以便首先显示所有访问权限。如果先添加只读权限，然后再添加纯访问权限，则 ONTAP 会将纯访问权限标记为重复项并忽略它们。

如果稍后升级 SnapCenter 或 ONTAP ，则应重新运行适用于 Data ONTAP 的 RBAC 用户创建程序工具以更新先前创建的用户角色。为早期版本的 SnapCenter 或 ONTAP 创建的用户角色无法在升级后的版本中正常工作。重新运行此工具时，它会自动处理升级。您无需重新创建角色。

有关设置 ONTAP RBAC 角色的详细信息，请参见 "《 ONTAP 9 管理员身份验证和 RBAC 高级指南》"。

为了确保一致性， SnapCenter 文档将角色称为使用特权。OnCommand 系统管理器图形用户界面使用术语_attribute_、而不是_privilege。设置ONTAP RBAC角色时、这两个术语的含义相同。

- 步骤 *

1. 在存储系统上，输入以下命令以创建新角色：

   ```
   security login role create <role_name\> -cmddirname "command" -access all
   -vserver <svm_name\>
   ```

   - svm_name 是 SVM 的名称。如果将此字段留空，则默认为集群管理员。
   - role_name 是为角色指定的名称。
   - command 是 ONTAP 功能。

     您必须对每个权限重复此命令。请记住，必须先列出所有访问命令，然后再列出只读命令。

   有关权限列表的信息，请参见 "用于创建角色和分配权限的 ONTAP 命令行界面命令"。

2. 输入以下命令创建用户名：

   ```
   security login create -username <user_name\> -application ontapi -authmethod
   <password\> -role <name_of_role_in_step_1\> -vserver <svm_name\> -comment
   "user_description"
   ```

   - user_name 是要创建的用户的名称。
   - <password> 是您的密码。如果不指定密码，系统将提示您输入一个密码。
   - svm_name 是 SVM 的名称。

3. 输入以下命令，将角色分配给用户：

   ```
   security login modify username <user_name\> -vserver <svm_name\> -role
   <role_name\> -application ontapi -application console -authmethod
   <password\>
   ```

   - <user_name> 是您在步骤 2 中创建的用户的名称。此命令可用于修改用户以将其与角色关联。
   - <SVM_name> 是 SVM 的名称。
   - <role_name> 是您在步骤 1 中创建的角色的名称。
   - <password> 是您的密码。如果不指定密码，系统将提示您输入一个密码。

4. 输入以下命令，验证是否已正确创建用户：

```
security login show -vserver <svm_name\> -user-or-group-name <user_name\>
```

user_name 是您在步骤 3 中创建的用户的名称。

创建具有最低权限的 SVM 角色

在 ONTAP 中为新 SVM 用户创建角色时，必须运行多个 ONTAP 命令行界面命令。如果您在 ONTAP 中将 SVM 配置为与 SnapCenter 结合使用，而您不想使用 vsadmin 角色，则需要此角色。

- 步骤 *

1. 在存储系统上，创建一个角色并为该角色分配所有权限。

```
security login role create -vserver <svm_name\>- role <SVM_Role_Name\>
-cmddirname <permission\>
```

您应对每个权限重复此命令。

1. 创建一个用户并将该角色分配给该用户。

```
security login create -user <user_name\> -vserver <svm_name\> -application
ontapi -authmethod password -role <SVM_Role_Name\>
```

2. 解除用户锁定。

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

用于创建 SVM 角色和分配权限的 ONTAP 命令行界面命令

您应运行多个 ONTAP 命令行界面命令来创建 SVM 角色并分配权限。

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all`

- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all`
- `security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname`

"snapmirror policy remove-rule" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

"vserver export-policy show" -access all

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all

创建具有最低权限的 ONTAP 集群角色

您应创建一个具有最低权限的 ONTAP 集群角色，以便不必使用 ONTAP 管理员角色在 SnapCenter 中执行操作。您可以运行多个 ONTAP 命令行界面命令来创建 ONTAP 集群角色并分配最低权限。

- 步骤 *

1. 在存储系统上，创建一个角色并为该角色分配所有权限。

```
security login role create -vserver <cluster_name\>- role <role_name\>
-cmddirname <permission\>
```

> 您应对每个权限重复此命令。

1. 创建一个用户并将该角色分配给该用户。

```
security login create -user <user_name\> -vserver <cluster_name\>
-application ontapi -authmethod password -role <role_name\>
```

2. 解除用户锁定。

```
security login unlock -user <user_name\> -vserver <cluster_name\>
```

用于创建集群角色和分配权限的 ONTAP 命令行界面命令

您应运行多个 ONTAP 命令行界面命令来创建集群角色和分配权限。

- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly
- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"lun mapping show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all
- security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

"volume create" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```
"vserver modify" -access all
```

- `security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all`

配置 IIS 应用程序池以启用 Active Directory 读取权限

如果需要为 SnapCenter 启用 Active Directory 读取权限，您可以在 Windows 服务器上配置 Internet 信息服务（ Internet Information Services ， IIS ）以创建自定义应用程序池帐户。

- 步骤 *
  1. 在安装了 SnapCenter 的 Windows 服务器上打开 IIS 管理器。
  2. 在左侧导航窗格中，单击 * 应用程序池 * 。
  3. 在应用程序池列表中选择 SnapCenter ，然后单击操作窗格中的 * 高级设置 * 。
  4. 选择身份，然后单击 * 。 * 以编辑 SnapCenter 应用程序池标识。
  5. 在自定义帐户字段中，输入具有 Active Directory 读取权限的域用户或域管理员帐户名称。
  6. 单击确定。

     自定义帐户将替换 SnapCenter 应用程序池的内置 ApplicationPoolIdentity 帐户。

版权信息

版权所有 © 2025 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。