



# **SnapDrive for UNIX 中基于角色的访问控制**

## **Snapdrive for Unix**

NetApp  
June 20, 2025

This PDF was generated from [https://docs.netapp.com/zh-cn/snapdrive-unix/aix/concept\\_what\\_rbac\\_in\\_snapdrive\\_for\\_unix\\_is.html](https://docs.netapp.com/zh-cn/snapdrive-unix/aix/concept_what_rbac_in_snapdrive_for_unix_is.html) on June 20, 2025. Always check docs.netapp.com for the latest.

# 目录

SnapDrive for UNIX 中基于角色的访问控制	1
什么是 SnapDrive for UNIX 中基于角色的访问控制（RBAC）	1
SnapDrive for UNIX 和 Operations Manager 控制台交互	1
在 SnapDrive for UNIX 中配置基于角色的访问控制	2
在 Operations Manager 控制台中配置 SD-admin	3
将 SD 主机名添加到存储系统	4
在 SnapDrive for UNIX 上配置用户凭据	5
用于使用 Operations Manager 控制台执行访问检查的用户名格式	6
基于角色的访问控制的配置变量	6
SnapDrive 命令和功能	7
预配置的角色，便于配置用户角色	10
Operations Manager 控制台上的存储系统自动更新	11
多个 Operations Manager 控制台服务器	11
Operations Manager 控制台不可用	12
RBAC 和存储操作示例	12
对单个存储对象执行单个文件规范操作	13
对多个存储对象执行单个文件规范操作	13
对多个文件规范和存储对象执行的操作	13
对多个存储对象执行的操作	14
使用多个 Operations Manager 控制台服务器管理存储系统的操作	15

# SnapDrive for UNIX 中基于角色的访问控制

基于角色的访问控制（Role-Based Access Control，RBAC）用于用户登录和角色权限。管理员可以通过 RBAC 定义角色来管理用户组。如果需要将数据库的访问权限限制为特定管理员，则必须为其设置管理员帐户。此外，如果要限制这些信息，这些管理员可以查看这些信息以及可以执行的操作，则必须将角色应用于您创建的管理员帐户。

在 SnapDrive for UNIX 中，可借助 Operations Manager 控制台使用 RBAC。通过 Operations Manager 控制台，可以精细地访问存储对象，例如 LUN，qtree，卷，聚合和 vFiler 单元。

- 相关信息 \*

[基于卷的 SnapRestore 的强制检查](#)

[在目标存储系统上还原 Snapshot 副本](#)

[Snap disconnect 操作步骤](#)

## 什么是 SnapDrive for UNIX 中基于角色的访问控制（RBAC）

RBAC 允许 SnapDrive 管理员在执行各种 SnapDrive 操作时限制对存储系统的访问。存储操作的这种有限或完全访问权限取决于分配给用户的角色。

SnapDrive 4.0 for UNIX 及更高版本要求对所有 SnapDrive for UNIX 操作执行 RBAC 访问检查。此行为允许存储管理员根据分配的角色限制 SnapDrive 用户可以执行的操作。RBAC 是使用 Operations Manager 基础架构实施的。在 SnapDrive 4.0 for UNIX 之前的版本中，访问控制受限，只有 root 用户可以执行 SnapDrive for UNIX 操作。SnapDrive 4.0 for UNIX 及更高版本可使用 Operations Manager 控制台的 RBAC 基础架构为非 root 本地用户和网络信息系统（Network Information System，NIS）用户提供支持。SnapDrive for UNIX 不需要存储系统的根密码；它使用 SD-<hostname> 用户与存储系统进行通信。

默认情况下，不使用 Operations Manager 控制台 RBAC 功能。您必须通过在 `snapdrive.conf` 文件中设置变量 `rbac` 方法 `=dfm` 来启用 RBAC 功能，然后重新启动 SnapDrive for UNIX 守护进程。

要使用此功能，必须满足以下要求：

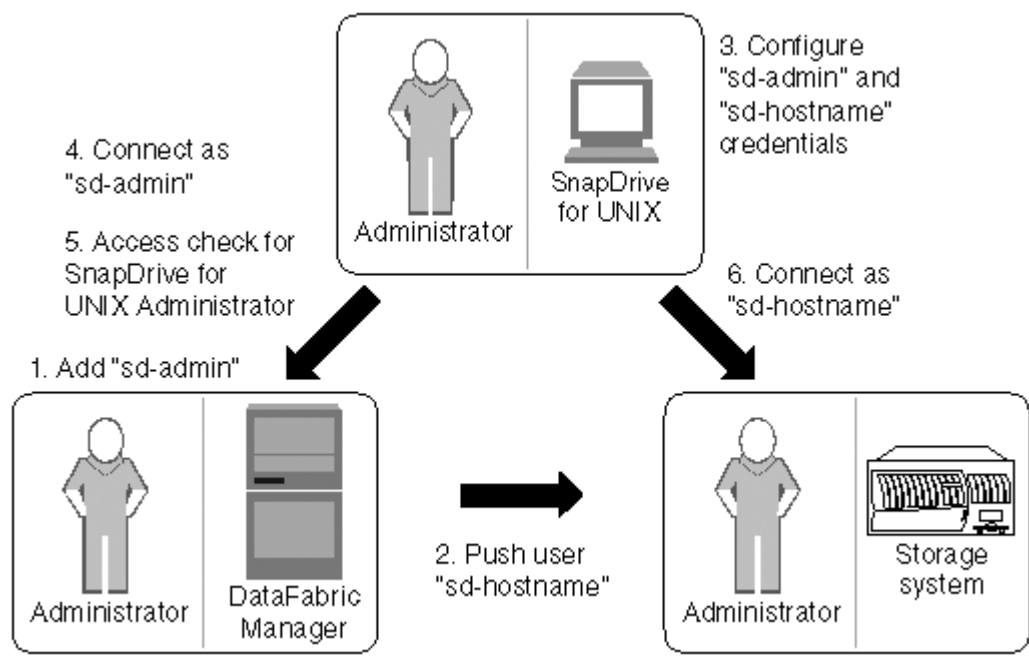
- Operations Manager 控制台 3.7 或更高版本。
- Operations Manager 控制台服务器必须位于包含 SnapDrive 主机和存储系统的 IP 网络中并进行配置。
- 必须在 SnapDrive 安装期间配置 Operations Manager 控制台通信设置。
- SnapDrive for UNIX 守护进程应正在运行。

## SnapDrive for UNIX 和 Operations Manager 控制台交互

使用基于角色的访问控制（Role-Based Access Control，RBAC）取决于 Operations Manager 控制台基础架构。Operations Manager 控制台管理员必须创建用于 UNIX 的 SnapDrive 的用户名。所有存储操作请求都会首先发送到 Operations Manager 控制台以进行访问检查。在 Operations Manager 控制台验证特定 SnapDrive 用户的存储操作后，此

操作将完成。

下图显示了用于存储操作的整个 RBAC 。



1. Operations Manager 控制台管理员在 Operations Manager 控制台上添加了 SD-admin 用户。
2. Operations Manager 控制台管理员可在存储系统上创建 SD 主机名用户。
3. Operations Manager 控制台管理员将 SD-admin 和 SD-hostname 凭据发送给 SnapDrive for UNIX 管理员。
4. SnapDrive 管理员使用收到的用户凭据配置 SnapDrive 。
5. Operations Manager 控制台会使用 SnapDrive 管理员添加的用户凭据检查 SnapDrive for UNIX 的使用情况。
6. 对 SnapDrive 用户进行身份验证后，该用户可以连接到存储系统。

当 SnapDrive 用户希望执行某些存储操作时，用户会在命令行上发出相应的命令。此请求将发送到 Operations Manager 控制台以进行访问检查。Operations Manager 控制台会检查请求的用户是否具有执行 SnapDrive 操作的适当权限。访问检查的结果将返回到 SnapDrive 。根据结果，允许或不允许用户在存储系统上执行存储操作。

如果在访问检查后验证了用户，则用户将以 SD 主机名的形式连接到存储系统。



建议使用 sd-hostname 和 sd-admin 用户名。您可以使用其他用户名配置 SnapDrive for UNIX 。

## 在 SnapDrive for UNIX 中配置基于角色的访问控制

要为适用于 UNIX 的 SnapDrive 配置基于角色的访问控制（ Role-Based Access Control ， RBAC ），您必须完成各种任务。您可以使用 Operations Manager 控制台或命令行界面来执行这些任务。

## 在 Operations Manager 控制台中配置 SD-admin

Operations Manager 控制台管理员可以创建 SD-admin 用户。

Operations Manager 控制台管理员创建一个名为 sd-admin 的用户，该用户能够对全局组（全局 `Dfm.core.AccessCheck`）执行核心访问检查。在 Operations Manager 控制台管理员配置了 SD-admin 用户后，您必须手动将凭据信息发送给 SnapDrive for UNIX 管理员。有关使用 Operations Manager 控制台配置用户和角色的详细信息，请参见 [\\_Operations Manager 控制台管理指南和联机帮助](#)。



您可以使用任何名称来代替 SD-admin；但是，最好使用 SD-admin。

要在 Operations Manager 控制台中创建角色，请选择 \* 设置 \* > \* 角色 \*。在 SD-admin 配置页面中，Operations Manager 控制台管理员必须将全局组上的 `Dfm.Database.Write` 功能分配给 sd-admin-role，以便 SnapDrive for UNIX 可以在 Operations Manager 控制台中刷新存储实体。

### 使用命令行界面配置 SD-admin

存储系统管理员可以使用命令行界面配置 SD-admin 用户。

#### 步骤

1. 添加一个名为 sd-admin 的用户。

```
# useradd sd-admin
```

```
# passwd sd-admin
Changing password for sd-admin.
New password:
Re-enter new password:
Password changed
```

2. 添加一个名为 sd-admin 的管理员。

```
# dfm user add sd-admin
Added administrator sd-admin.
```

3. 创建一个名为 sd-admin-role 的角色。

```
# dfm role create sd-admin-role
Created role sd-admin-role.
```

4. 向步骤 3 中创建的角色添加功能。

```
# dfm role add sd-admin-role DFM.Core.AccessCheck Global
Added 1 capability to role sd-admin-role.
```

5. Operations Manager 管理员还可以将全局组上的 `Dfm.Database.Write` 功能授予 `<sd-admin>`，以使 SnapDrive for UNIX 能够在 Operations Manager 中刷新存储系统实体。

```
# dfm role add sd-admin-role DFM.Database.Write Global
Added 1 capability to role sd-admin-role.
```

6. 将 SD-admin-role 角色添加到 SD-admin 用户。

```
# dfm user role set sd-admin sd-admin-role
Set 1 role for administrator sd-admin.
```

## 将 SD 主机名添加到存储系统

Operations Manager 控制台管理员可以使用 Operations Manager 控制台在存储系统上创建 SD 主机名用户。完成这些步骤后，Operations Manager 控制台管理员必须手动将凭据发送给 SnapDrive for UNIX 管理员。您可以使用任何名称来替代 `sd-hostname`；但最好使用 `sd-hostname`。

### 步骤

1. 获取存储系统的根密码并存储该密码。

要添加存储系统的密码，请选择 `* 管理 * > * 存储系统 *`。

2. 为每个 UNIX 系统创建一个 SD 主机名用户。
3. 将功能 `API-` 和 `login-` 分配给某个角色，例如 `SD-role`。
4. 将此角色（`sd-role`）包括在新用户组中，例如 `sd-usergroup`。
5. 将此用户组（`sd-usergroup`）与存储系统上的 `sd-hostname` 用户关联。

### 使用 CLI 将 SD- 主机名添加到存储系统

存储系统管理员可以使用 `useradmin` 命令创建和配置 `sd-hostname` 用户。

### 步骤

1. 添加存储

```
# dfm host add storage_array1
Added host storage_array1.lab.eng.btc.xyz.in
```

## 2. 设置主机的密码。

```
# dfm host password save -u root -p xxxxxxxx storage_array1
Changed login for host storage_array1.lab.eng.btc.xyz.in to root.
Changed Password for host storage_array1.lab.eng.xyz.netapp
.in
```

## 3. 在主机上创建角色。

```
# dfm host role create -h storage_array1 -c "api-*,login-*" sd-unixhost-
role
Created role sd-unixhost-role on storage_array1
```

## 4. 创建用户组。

```
# dfm host usergroup create -h storage_array1 -r sd-unixhost-role sd-
unixhost-ug
Created usergroup sd-unixhost-ug(44) on storage_array1
```

## 5. 创建本地用户。

```
# dfm host user create -h storage_array1 -p xxxxxxxx -g sd-unixhost-ug
sd-unixhost
Created local user sd-unixhost on storage_array1
```

## 在 SnapDrive for UNIX 上配置用户凭据

SnapDrive for UNIX 管理员从 Operations Manager 控制台管理员处接收用户凭据。要正确执行存储操作，需要在适用于 UNIX 的 SnapDrive 上配置这些用户凭据。

### 步骤

#### 1. 在存储系统上配置 SD-admin。

```
[root]#snapdrive config set -dfm sd-admin ops_mngr_server
Password for sd-admin:
Retype password:
```

#### 2. 在存储系统上配置 SD 主机名。

```
[root]#snapdrive config set sd-unix_host storage_array1
Password for sd-unix_host:
Retype password:
```

3. 使用 `SnapDrive config list`` 命令验证步骤 1 和步骤 2。

```
user name          appliance name      appliance type
-----
sd-admin           ops_mngr_server    DFM
sd-unix_host       storage_array1     StorageSystem
```

4. 通过在 `snapdrive.conf` 文件中设置配置变量 `rbac 路由方法 = "dfm"`，将 SnapDrive for UNIX 配置为使用 Operations Manager 控制台基于角色的访问控制（RBAC）。



用户凭据会进行加密并保存在现有的 `.sdupw`` 文件中。早期文件的默认位置为 `/opt/netapp/snapDrive/.sdupw``。

## 用于使用 **Operations Manager** 控制台执行访问检查的用户名格式

SnapDrive for UNIX 使用用户名格式通过 Operations Manager 控制台执行访问检查。这些格式取决于您是网络信息系统（Network Information System，NIS）还是本地用户。

SnapDrive for UNIX 使用以下格式检查用户是否有权执行某些任务：

- 如果您是运行 SnapDrive` 命令的 NIS 用户，则 SnapDrive for UNIX 将使用格式 `<nisdomain><username>``（例如，`netapp.com\marc`）
- 如果您是 `lnx197-141` 等 UNIX 主机的本地用户，则 SnapDrive for UNIX 将使用格式 `< 主机名 >\< 用户名 >`` 格式（例如，`lnx197-141\john`）
- 如果您是 UNIX 主机的管理员（`root`），则 SnapDrive for UNIX 会始终将此管理员视为本地用户，并使用格式 `lnx197-141\root`。

## 基于角色的访问控制的配置变量

您必须在 `snapdrive.conf` 文件中设置与基于角色的访问控制相关的各种配置变量。

变量	Description
<code>`contact-http-dfm_port = 8088_`</code>	指定用于与 Operations Manager 控制台服务器通信的 HTTP 端口。默认值为 8088.。
<code>`contact-ssl-dfm_port = 8488_`</code>	指定用于与 Operations Manager 控制台服务器通信的 SSL 端口。默认值为 8488.。



变量	Description
`rbac 方法 =dfm_`	<p>指定访问控制方法。可能值为 原生 和 dFM。</p> <p>如果值为 原生 ，则访问检查将使用存储在 `/vol/vol0/sdprbac/sdhost-name.prbac` 中的访问控制文件。</p> <p>如果将此值设置为 dFM ，则前提条件是 Operations Manager 控制台。在这种情况下， SnapDrive for UNIX 会将访问检查发送到 Operations Manager 控制台。</p>
`rbac - cache=on_`	<p>SnapDrive for UNIX 会保留一个访问检查查询以及相应结果的缓存。只有当所有已配置的 Operations Manager 控制台服务器均已关闭时， SnapDrive for UNIX 才会使用此缓存。</p> <p>您可以将此值设置为 on 来启用缓存，也可以将其设置为 off 来禁用。默认值为 off ，因此您可以将 SnapDrive for UNIX 配置为使用 Operations Manager 控制台，并将 RBAC 方法 配置变量设置为 dFM。</p>
`RBAC 缓存超时 _`	<p>指定 RBAC 缓存超时期限，并且仅在启用 `RBAC 缓存 _` 时才适用。默认值为 24 小时。</p> <p>只有当所有已配置的 Operations Manager 控制台服务器均已关闭时， SnapDrive for UNIX 才会使用此缓存。</p>
`使用 https 到 dfm=on_`	<p>通过此变量，您可以将适用于 UNIX 的 SnapDrive 设置为在与 Operations Manager 控制台通信时使用 SSL 加密（HTTPS）。默认值为 on。</p>

## SnapDrive 命令和功能

在基于角色的访问控制（Role-Based Access Control，RBAC）中，要成功执行每个操作，都需要特定的功能。用户必须具有一组正确的功能来执行存储操作。

下表列出了所需的命令和相应功能：

命令	功能
s存储显示	在卷上执行 sd.story.read
s存储列表	在卷上执行 sd.story.read

命令	功能
s 存储创建	<ul style="list-style-type: none"> <li>对于卷内的 LUN： s D.Storage.Write on Volume</li> <li>对于 qtree 内的 LUN： s D.Storage.Write on qtree</li> </ul>
s 存储调整大小	s D 存储写入 在 LUN 上
s 存储删除	s D 存储。删除 LUN 上的
snap show	卷上 s .D.snapshot.read
snap list	卷上 s .D.snapshot.read
snap delete	s D 存储。删除卷上的
snap rename	s D 存储写入 卷
snap connect	<ul style="list-style-type: none"> <li>对于卷中的 LUN 克隆：卷上的 s .D.snapshot.Clone</li> <li>对于 qtree 中的 LUN 克隆： s .D.snapshot.Clone on qtree</li> <li>对于传统卷克隆： s .snapshot.Clone on storage system</li> <li>对于 FlexClone 卷： s 父卷上的 .snapshot.Clone</li> <li>对于不受限制的 FlexClone 卷： s 父卷上的 dsnapshot.UnrestrictedClone</li> </ul>
snap connect-split	<ul style="list-style-type: none"> <li>对于 LUN 克隆（LUN 在卷中克隆和拆分）：卷上为 s .d snapshot.Clone，卷上为 s .d Storage.Write</li> <li>对于 LUN 克隆（在 qtree 中克隆和拆分 LUN）：在 qtree 上为 s .d snapshot.Clone，在 qtree 上为 s .d Storage.Write</li> <li>对于拆分的传统卷克隆：存储系统上为 s .D.snapshot.Clone，存储系统上为 s .D.Storage.Write</li> <li>对于拆分的 Flex 卷克隆： s 父卷上的 .D.snapshot.Clone。</li> </ul>

命令	功能
<code>clone split start</code>	<ul style="list-style-type: none"> <li>对于 LUN 驻留在卷或 qtree 中的 LUN 克隆： <code>s ontsnapshot.Clone</code> containing volume or qtree</li> <li>对于卷克隆： <code>s</code> 父卷上的 <code>.snapshot.Clone</code></li> </ul>
<code>snap disconnect</code>	<ul style="list-style-type: none"> <li>对于 LUN 驻留在卷或 qtree 中的 LUN 克隆： <code>s ontsnapshot.Clone</code> containing volume or qtree</li> <li>对于卷克隆： <code>s</code> 父卷上的 <code>.snapshot.Clone</code></li> <li>要删除不受限制的卷克隆，请执行以下操作：卷上的 <code>s</code> <code>.D.snapshot.DestroyUnrestrictedClone</code></li> </ul>
<code>snap disconnect - split</code>	<ul style="list-style-type: none"> <li>对于 LUN 驻留在卷或 qtree 中的 LUN 克隆： <code>s</code> 包含卷或 qtree 上的 <code>ontsnapshot.Clone</code></li> <li>对于卷克隆： <code>s</code> 父卷上的 <code>.D.Storage.Delete</code></li> <li>要删除不受限制的卷克隆，请执行以下操作：卷上的 <code>s</code> <code>.D.snapshot.DestroyUnrestrictedClone</code></li> </ul>
<code>snap restore</code>	<ul style="list-style-type: none"> <li>对于卷中的 LUN：卷上为 <code>s</code> <code>.D.snapshot.Restore</code>，LUN 上为 <code>s</code> <code>.D.Storage.Write</code></li> <li>对于 qtree 中的 LUN： <code>s .d snapshot.Restore</code> 在 qtree 上， <code>s .d Storage.Write</code> 在 LUN 上</li> <li>对于不在卷中的 LUN：卷上为 <code>s .d snapshot.Restore</code>，卷上为 <code>s .d Storage.Write</code></li> <li>对于不在 qtree 中的 LUN： qtree 上为 <code>s .d snapshot.Restore</code>， qtree 上为 <code>s .d Storage.Write</code></li> <li>对于卷：在存储系统上为 <code>s</code> <code>.snapshot.Restore</code>（对于传统卷）或在聚合上为 <code>s .snapshot.Restore</code>（对于灵活卷）</li> <li>对于卷中的单文件快照还原：卷上的 <code>s</code> <code>.D.snapshot.Restore</code></li> <li>对于 qtree 中的单文件快照还原： <code>s</code> <code>D.snapshot.Restore qtree</code></li> <li>要覆盖基线 Snapshot 副本，请执行以下操作：卷上的 <code>s .Dt.DisruptionBaseline</code></li> </ul>

命令	功能
host connect , host disconnect	s LUN 上的 配置写入
配置访问	s 存储系统上的 .D.Config.Read
配置准备	s 配置写入 至少在一个存储系统上
配置检查	s 配置读取 至少在一个存储系统上
config show	s 配置读取 至少在一个存储系统上
配置集	s 存储系统上的 配置写入
config set -dfm , config set -mgmtpath ,	s 配置写入 至少在一个存储系统上
config delete	s 存储系统上的 配置删除
config delete dfm_appliance , config delete -mgmtpath	s 配置删除 至少在一个存储系统上
配置列表	s 配置读取 至少在一个存储系统上
配置迁移集	s 配置写入 至少在一个存储系统上
config migrate delete	s 配置删除 至少在一个存储系统上
配置迁移列表	s 配置读取 至少在一个存储系统上



SnapDrive for UNIX 不会检查管理员（root）的任何功能。

## 预配置的角色，便于配置用户角色

预配置的角色可简化向用户分配角色的任务。

下表列出了预定义的角色：

Role name	Description
GlobalSDStorage	使用 SnapDrive for UNIX 管理存储
GlobalSDConfig	使用 SnapDrive for UNIX 管理配置

Role name	Description
GlobalSDSnapshot	使用 SnapDrive for UNIX 管理 Snapshot 副本
GlobalSDFullControl	充分利用适用于 UNIX 的 SnapDrive

在上表中，Global 是指由 Operations Manager 控制台管理的所有存储系统。

## Operations Manager 控制台上的存储系统自动更新

Operations Manager 控制台可发现您的网络支持的存储系统。它会定期监控从发现的存储系统收集的数据。数据将按设置的间隔刷新。Operations Manager 控制台管理员可以配置刷新间隔。

LUN 监控间隔，qtree 监控间隔和 vFiler 监控间隔是决定 LUN，qtree 和 vFiler 更新频率的重要字段。例如，如果在存储系统上创建了新的 LUN，则新的 LUN 不会立即在 Operations Manager 控制台上更新。因此，向 Operations Manager 控制台发出的对该 LUN 的访问检查将失败。为了避免这种情况，您可以根据需要修改 LUN 监控间隔。

1. 在 Operations Manager 控制台中选择 \* 设置 \* > \* 选项 \* 以更改监控间隔。
2. Operations Manager 控制台管理员还可以通过在命令行界面中执行 `dfm host discovery filename` 来强制刷新 Operations Manager 控制台。
3. Operations Manager 控制台管理员还可以将全局组上的 `Dfm.Database.Write` 功能授予 SD-admin，以使 SnapDrive for UNIX 能够刷新 Operations Manager 控制台上的存储系统实体。

```
# dfm role add sd-admin-role DFM.Database.Write Global
Added 1 capability to role sd-admin-role.
```

## 多个 Operations Manager 控制台服务器

SnapDrive for UNIX 支持多个 Operations Manager 控制台服务器。如果一组存储系统由多个 Operations Manager 控制台服务器管理，则需要此功能。SnapDrive for UNIX 按照在 SnapDrive for UNIX 中配置 Operations Manager 控制台服务器的相同顺序联系 Operations Manager 控制台服务器。您可以运行 `SnapDrive config list`` 命令来获取配置顺序。

以下示例显示了多个 Operations Manager 控制台服务器的输出：

```
# snapdrive config list
username      appliance name      appliance type
-----
root          storage_array1      StorageSystem
root          storage_array2      StorageSystem
sd-admin      ops_mngr_server1    DFM
sd-admin      ops_mngr_server2    DFM
```

在上面的示例中， storage\_array1 由 ops\_mngr\_server1 管理， storage\_array2 由 ops\_mngr\_server2 管理。在此示例中， SnapDrive for UNIX 会首先联系 ops\_mngr\_server1 。如果 ops\_mngr\_server1 无法确定访问权限，则 SnapDrive for UNIX 将联系 ops\_mngr\_server2 。

只有在以下情况下， SnapDrive for UNIX 才会联系第二个 Operations Manager 控制台：

- 第一个 Operations Manager 控制台无法确定访问权限时。之所以出现这种情况，可能是因为第一个 Operations Manager 控制台不管理存储系统。
- 第一个 Operations Manager 控制台关闭时。

## Operations Manager 控制台不可用

SnapDrive for UNIX 需要 Operations Manager 控制台来执行访问检查。有时， Operations Manager 控制台服务器可能由于各种原因而不可用。

如果设置了 RBAC 方法 `RBAC 方法 = dfm\_` 且 Operations Manager 控制台不可用，则 SnapDrive for UNIX 将显示以下错误消息：

```
[root]# snapdrive storage delete -lun storage_array1:/vol/vol2/qtree1/lun1
0002-333 Admin error: Unable to connect to the DFM ops_mngr_server
```

SnapDrive for UNIX 还可以为 Operations Manager 控制台返回的用户访问检查结果保留一个缓存。此缓存有效期为 24 小时，不可配置。如果 Operations Manager 控制台不可用，则 SnapDrive for UNIX 将使用缓存来确定访问权限。只有在所有已配置的 Operations Manager 控制台服务器均无响应时，才会使用此缓存。

要使 SnapDrive for UNIX 使用缓存进行访问检查，您必须打开 `RBAC cache\_` 配置变量，以保持访问结果的缓存。默认情况下， `RBAC 缓存 \_` 配置变量处于关闭状态。

要在 Operations Manager 控制台不可用的情况下使用 SnapDrive for UNIX ，服务器管理员必须在 snapdrive.conf 文件中将基于角色的访问控制（ Role-Based Access Control ， RBAC ）方法重置为 `RBAC 方法 = 原生` 。更改 snapdrive.conf 文件后，必须重新启动 SnapDrive for UNIX 守护进程。如果设置了 `RBAC 方法 = UNIX\_` ，则只有 root 用户可以使用 SnapDrive for 原生。

## RBAC 和存储操作示例

基于角色的访问控制允许根据分配给您的功能执行存储操作。如果您没有执行存储操作的适当功能，则会收到一条错误消息。

## 对单个存储对象执行单个文件规范操作

如果您不是在指定卷上创建文件规范的授权用户，则 SnapDrive for UNIX 将显示一条错误消息。

*filesSpec* : *filesSpec* 可以是文件系统，主机卷，磁盘组或 LUN。

```
[john]$ snapdrive storage create -fs /mnt/testfs -filervol
storage_array1:/vol/vol1 -dgsiz 100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user unix_host\john on Operations Manager
server ops_mgr_server
```

在此示例中，John 是非 root 用户，无权在指定卷上创建文件规范。John 必须要求 Operations Manager 控制台管理员对卷 storage\_array1 : /vol/vol1 授予 s .D.Storage.Write 访问权限。

## 对多个存储对象执行单个文件规范操作

如果管理员对多个存储对象没有执行存储操作所需的权限，则 SnapDrive for UNIX 将显示一条错误消息。

*filesSpec* : *filesSpec* 可以是文件系统，主机卷，磁盘组或 LUN 的任何人

```
[root]# snapdrive storage create -fs /mnt/testfs -lun
storage_array1:/vol/vol1/lun2 -lun storage_array1:/vol/vol2/lun2 -lunsize
100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user unix_host\root on Operations Manager
server ops_mgr_server
SD.Storage.Write access denied on volume storage_array1:/vol/vol2 for user
unix_host\root on Operations Manager server ops_mgr_server
```

在此示例中，文件规范跨越两个存储系统卷 vol1 和 vol2。unix\_host 的管理员（root）不对这两个卷都具有 s D Storage.Write 访问权限。因此，SnapDrive for UNIX 会为每个卷显示一条错误消息。要继续执行 storage create，管理员（root）必须要求 Operations Manager 控制台管理员对这两个卷授予 s D Storage.Write 访问权限。

## 对多个文件规范和存储对象执行的操作

以下示例显示了当您不是执行特定操作的授权用户时可能会收到的错误消息。

```
[marc]$ snapdrive storage create -lun storage_array1:/vol/vol1/lun5 lun6
-lun storage_array1:/vol/vol2/lun2 -lunsize 100m
0002-332 Admin error:SD.Storage.Write access denied on volume
storage_array1:/vol/vol1 for user nis_domain\marc on Operations Manager
server ops_mngr_server
SD.Storage.Write access denied on volume storage_array1:/vol/vol2 for user
nis_domain\marc on Operations Manager server ops_mngr_server
```

在此示例中，三个 LUN 位于两个存储系统卷 vol1 和 vol2 上。用户 mc 属于 nis\_domain，无权在 vol1 和 vol2 上创建文件规范。SnapDrive for UNIX 在上一示例中显示了两条错误消息。错误消息显示用户必须对 vol1 和 vol2 具有 s .D Storage.Write 访问权限。

## 对多个存储对象执行的操作

以下示例显示了当您不是执行特定操作的授权用户时可能会收到的错误消息。



```
[john]$ snapdrive storage show -all
```

Connected LUNs and devices:

device	filename	adapter	path	size	proto	state	clone	lun	path
backing Snapshot									
-----									
/dev/sdao		-	-	200m	iscsi	online	No		
storage_array1:/vol/vol2/passlun1					-				
/dev/sda1		-	-	200m	fc	online	No		
storage_array1:/vol/vol2/passlun2					-				

Host devices and file systems:

```
dg: testfs1_SdDg          dgtype lvm
hostvol: /dev/mapper/testfs1_SdDg-testfs1_SdHv  state: AVAIL
fs: /dev/mapper/testfs1_SdDg-testfs1_SdHv      mount point: /mnt/testfs1
(persistent) fstype jfs2
```

device	filename	adapter	path	size	proto	state	clone	lun	path
backing Snapshot									
-----									
/dev/sdn		-	P	108m	iscsi	online	No		
storage_array1:/vol/vol2/testfs1_SdLun					-				
/dev/sdn1		-	P	108m	fc	online	No		
storage_array1:/vol/vol2/testfs1_SdLun1					-				

```
0002-719 Warning: SD.Storage.Read access denied on volume
storage_array1:/vol/vol1 for user unix_host\john on Operations Manager
server ops_mgr_server
```

John 有权在 vol2 上列出存储实体，但不能在 vol1 上列出。SnapDrive for UNIX 将显示 vol1 的实体并显示 vol2 的警告消息。



对于 storage list，storage show，snap list 和 snap show 命令，适用于 UNIX 的 SnapDrive 将显示警告而不是错误。

## 使用多个 Operations Manager 控制台服务器管理存储系统的操作

以下输出显示了在存储系统由多个 Operations Manager 控制台管理时您可能会收到的错误消息。

```
[root]# snapdrive storage create -lun storage_array1:/vol/vol1/lun5 lun6  
-lun storage_array2:/vol/vol1/lun2 -lunsize 100m  
0002-332 Admin error:SD.Storage.Write access denied on volume  
storage_array1:/vol/vol1 for user unix_host\root on Operations Manager  
server ops_mngr_server1  
SD.Storage.Write access denied on volume storage_array2:/vol/vol1 for user  
unix_host\root on Operations Manager server ops_mngr_server2
```

storage\_array1 由 ops\_mngr\_server1 管理， storage\_array2 由 ops\_mngr\_server2 管理。unix\_host 的管理员无权在 storage\_array1 和 storage\_array2 上创建文件名。在上述示例中， SnapDrive for UNIX 将显示用于确定访问权限的 Operations Manager 控制台。

## 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。