在 SnapDrive for UNIX 中配置基于角色的访问控制

Snapdrive for Unix

NetApp
June 20, 2025

目录

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
` contact-http-dfm_port = 8088_`	指定用于与 Operations Manager 控制台服务器通信的 HTTP 端口。默认值为 8088. 。
` contact-ssl-dfm_port = 8488_`	指定用于与 Operations Manager 控制台服务器通信的 SSL 端口。默认值为 8488. 。
` rbac 方法 =dfm_`	指定访问控制方法。可能值为 原生 和 `dFM` 。 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。 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。
` rbac - cache=on_`	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。 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` 。
` RBAC 缓存超时 _`	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。 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。
` 使用 https 到 dfm=on_`	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` 。