



SnapDrive for UNIX 中的访问控制

Snapdrive for Unix

NetApp
June 20, 2025

This PDF was generated from https://docs.netapp.com/zh-cn/snapdrive-unix/aix/concept_what_access_control_settings_are.html on June 20, 2025. Always check docs.netapp.com for the latest.

目录

SnapDrive for UNIX 中的访问控制	1
什么是访问控制设置	1
可用的访问控制级别	1
设置访问控制权限	2
查看访问控制权限	3

SnapDrive for UNIX 中的访问控制

通过 SnapDrive for UNIX，您可以控制每个主机对主机所连接的每个存储系统的访问级别。

SnapDrive for UNIX 中的访问级别指示当主机面向给定存储系统时允许执行的操作。除了 show 和 list 操作之外，访问控制权限可能会影响所有 Snapshot 和存储操作。

什么是访问控制设置

为了确定用户访问权限，SnapDrive for UNIX 会检查存储系统根卷中的两个权限文件之一。您必须检查这些文件中设置的规则，以评估访问控制。

- `sdHOST-name.prbac` file is in the directory ``/vol/vol0/sdprbac`` (SnapDrive permissions rols-based access control) .

文件名称为 `sdHOST-name.prbac`，其中 ``host-name_`` 是权限适用的主机的名称。您可以为连接到存储系统的每个主机创建一个权限文件。您可以使用 `SnapDrive config access`` 命令显示有关特定存储系统上主机可用权限的信息。

如果 `sdHOST-name.prbac` 不存在，请使用 `sdgeneric.prbac` 文件检查访问权限。

- `sdgeneric.prbac` file is also in the directory ``/vol/vol0/sdprbac``

文件名 `sdgeneric.prbac` 用作无法访问存储系统上的 `sdHOST-name.prbac` 文件的多个主机的默认访问设置。

如果在 ``/vol/vol0/sdprbac`` 路径中同时存在 `sdHOST-name.prbac` 和 `sdgeneric.prbac` 文件，则使用 `sdHOST-name.prbac` 检查访问权限，因为这会覆盖为 `sdgeneric.prbac` 文件提供的值。

如果您没有 `sdHOST-name.prbac` 和 `sdgeneric.prbac` 文件，请检查在 `snapdrive.conf` 文件中定义的配置变量 ``all-access-if-rbac-unspecified_``。

手动设置从给定主机到给定 vFiler 单元的访问控制。给定主机的访问由位于受影响 vFiler 单元根卷中的文件控制。该文件包含 ``/vol/<vFiler 根卷 >/sdprbac/sdhost-name.prbac``，其中 ``host-name_`` 是受影响主机的名称，由 `gethostname (3)` 返回。您应确保此文件可从可访问它的主机读取，但不可写入。



要确定主机的名称，请运行 `hostname` 命令。

如果文件为空，不可读或格式无效，则 SnapDrive for UNIX 不会授予主机对任何操作的访问权限。

如果缺少此文件，SnapDrive for UNIX 将检查 `snapdrive.conf` 文件中的配置变量 ``全部访问 -if-rbac 未指定_``。如果将变量设置为 `on`（默认值），则允许主机完全访问该存储系统上的所有这些操作。如果将变量设置为 `off`，则 SnapDrive for UNIX 将拒绝主机对该存储系统执行由访问控制管理的任何操作。

可用的访问控制级别

SnapDrive for UNIX 可为用户提供各种访问控制级别。这些访问级别与 Snapshot 副本和

存储系统操作相关。

您可以设置以下访问级别：

- 无—主机无法访问存储系统。
- snap create —主机可以创建 Snapshot 副本。
- snap use —主机可以删除和重命名 Snapshot 副本。
- snap all —主机可以创建，还原，删除和重命名 Snapshot 副本。
- storage create delete —主机可以创建存储，调整存储大小和删除存储。
- 存储使用—主机可以连接和断开存储连接，还可以在存储上执行克隆拆分估计和克隆拆分开始。
- 存储全部—主机可以创建，删除，连接和断开存储连接，还可以在存储上执行克隆拆分估计和克隆拆分启动。
- 所有访问—主机可以访问上述所有 SnapDrive for UNIX 操作。

每个级别都是不同的。如果您仅为某些操作指定权限，则 SnapDrive for UNIX 只能执行这些操作。例如，如果指定了存储使用，则主机可以使用适用于 UNIX 的 SnapDrive 连接和断开存储连接，但它无法执行受访问控制权限管理的任何其他操作。

设置访问控制权限

您可以通过在存储系统的根卷中创建特殊目录和文件来在 SnapDrive for UNIX 中设置访问控制权限。

确保以 root 用户身份登录。

步骤

1. 在目标存储系统的根卷中创建目录 `sdprbac`。

要使根卷可访问，一种方法是使用 NFS 挂载此卷。

2. 在 `sdprbac` 目录中创建权限文件。确保以下陈述正确无误：

- 此文件必须名为 `sdHost-name.prbac`，其中 `host-name` 是要为其指定访问权限的主机的名称。
- 此文件必须为只读文件，以确保 SnapDrive for UNIX 可以读取它，但无法修改它。

要为名为 `dev-sund1` 的主机授予访问权限，您应在存储系统上创建以下文件：
`/vol/vol1/sdprbac/sddev-sund1.prbac``

3. 在文件中设置该主机的权限。

您必须对文件使用以下格式：

- 您只能指定一个权限级别。要为主机授予对所有操作的完全访问权限，请输入字符串 `all access`。
- 权限字符串必须是文件中的第一项。如果权限字符串不在第一行中，则文件格式无效。
- 权限字符串不区分大小写。
- 权限字符串前面不能有空格。

- 不允许添加任何注释。

这些有效权限字符串允许以下访问级别：

- 无一主机无法访问存储系统。
- `snap create` —主机可以创建 Snapshot 副本。
- `snap use` —主机可以删除和重命名 Snapshot 副本。
- `snap all` —主机可以创建，还原，删除和重命名 Snapshot 副本。
- `storage create delete` —主机可以创建存储，调整存储大小和删除存储。
- 存储使用—主机可以连接和断开存储连接，还可以在存储上执行克隆拆分估计和克隆拆分开始。
- 存储全部—主机可以创建，删除，连接和断开存储连接，还可以在存储上执行克隆拆分估计和克隆拆分启动。
- 所有访问—主机可以访问上述所有 SnapDrive for UNIX 操作。其中每个权限字符串都是离散的。如果指定快照使用，则主机可以删除或重命名 Snapshot 副本，但不能创建 Snapshot 副本，还原或执行任何存储配置操作。

无论您设置的权限如何，主机都可以执行 `show` 和 `list` 操作。

4. 输入以下命令以验证访问权限：

```
` * SnapDrive 配置访问 show filer_name `
```

查看访问控制权限

您可以运行 `SnapDrive config access show`` 命令来查看访问控制权限。

步骤

1. 运行 `SnapDrive config access show`` 命令。

此命令的格式如下：`SnapDrive config access { show | list } filename``

无论输入的是 `show` 还是 `list version` 命令，都可以使用相同的参数。

此命令行会检查存储系统的面包机，以确定主机具有哪些权限。根据输出，此存储系统上主机的权限为 `snap all`。

```
# snapdrive config access show toaster
This host has the following access permission to filer, toaster:
SNAP ALL
Commands allowed:
snap create
snap restore
snap delete
snap rename
#
```

在此示例中，权限文件不在存储系统上，因此 SnapDrive for UNIX 会检查 `snapdrive.conf` 文件中的变量 `_all-access-if-rbac unspecified _` 以确定主机具有哪些权限。此变量设置为 `on`，相当于创建一个权限文件，并将访问级别设置为 `all access`。

```
# snapdrive config access list toaster
This host has the following access permission to filer, toaster:
ALL ACCESS
Commands allowed:
snap create
snap restore
snap delete
snap rename
storage create
storage resize
snap connect
storage connect
storage delete
snap disconnect
storage disconnect
clone split estimate
clone split start
#
```

此示例显示了存储系统面板上没有权限文件时您会收到的消息类型，并且 `snapdrive.conf` 文件中的变量 `_all-access-if-rbac unspecified _` 设置为 `off`。

```
# snapdrive config access list toaster
Unable to read the access permission file on filer, toaster. Verify that
the
file is present.
Granting no permissions to filer, toaster.
```

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。