SnapDrive for UNIX 中的安全功能

Snapdrive for Unix

NetApp
June 20, 2025

目录

SnapDrive for UNIX 中的安全功能

在使用 SnapDrive for UNIX 之前，您必须了解其安全功能并了解如何访问它们。

什么是安全功能

SnapDrive for UNIX 提供了一些功能，可让您更安全地使用它。通过这些功能，您可以更好地控制哪些用户可以在存储系统上执行操作以及从哪个主机执行操作。

通过安全功能，您可以执行以下任务：

- 设置访问控制权限
- 指定存储系统的登录信息
- 指定适用于 UNIX 的 SnapDrive 使用 HTTPS

通过访问控制功能，您可以指定运行 SnapDrive for UNIX 的主机可以在存储系统上执行的操作。您可以为每个主机单独设置这些权限。此外，要允许 SnapDrive for UNIX 访问存储系统，您必须提供该存储系统的登录名和密码。

通过 HTTPS 功能，您可以通过管理 ONTAP 界面为与存储系统的所有交互指定 SSL 加密，包括发送密码。这种行为是 SnapDrive 4.1 for UNIX 以及 AIX 主机更高版本中的默认行为；但是，您可以通过将 `use-https-to-filer` 配置变量的值更改为 `off` 来禁用 SSL 加密。

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 `sDHHOST-name.prbac` 不存在，请使用 `sdgenic.prbac` 文件检查访问权限。

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

文件名 `sdgenic.prbac` 用作无法访问存储系统上的 `sDHHOST-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 `sdgenic.prbac` 文件，则使用 `sDHOST-name.prbac` 检查访问权限，因为这会覆盖为 `sdgenic.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—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 ｝ filername`

   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面面面包机，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.
```

存储系统的登录信息

通过用户名或密码， SnapDrive for UNIX 可以访问每个存储系统。它还提供了安全性，因为除了以 root 身份登录之外，运行 SnapDrive for UNIX 的用户还必须在系统提示时提供正确的用户名或密码。如果登录受到影响，您可以将其删除并设置新的用户登录。

您在设置每个存储系统时为其创建了用户登录名。要使 SnapDrive for UNIX 能够与存储系统配合使用，您必须为其提供此登录信息。根据您在设置存储系统时指定的内容，每个存储系统可以使用相同的登录名或唯一的登录名。

SnapDrive for UNIX 会将这些登录和密码以加密形式存储在每个主机上。您可以通过设置 ` *SnapDrive.conf* 配置变量 ` *use-https-to_filer=on*` 来指定 SnapDrive for UNIX 在与存储系统通信时对此信息进行加密。

指定登录信息

您必须指定存储系统的用户登录信息。根据您在设置存储系统时指定的内容，每个存储系

统可以使用相同的用户名或密码，也可以使用唯一的用户名或密码。如果所有存储系统都使用相同的用户名或密码信息，则必须执行以下步骤一次。如果存储系统使用唯一的用户名或密码，则必须对每个存储系统重复以下步骤。

确保以 root 用户身份登录。

步骤

1. 输入以下命令：

   ` * SnapDrive 配置集 *user_name filername* [*filername*…]*`

   ` user_name_` 是首次设置存储系统时为该存储系统指定的用户名。

   ` *filername*` 是存储系统的名称。

   ` *[filername…]*` 定义，如果所有存储系统名称都具有相同的用户登录名或密码，则可以在一个命令行中输入多个存储系统名称。必须至少输入一个存储系统的名称。

2. 在提示符处，输入密码（如果有）。

   如果未设置密码，请在系统提示输入密码时按 Enter 键（空值）。

   此示例为名为 toasters 的存储系统设置一个名为 `root` 的用户：

   ```
   # snapdrive config set `root` toaster
   Password for root:
   Retype Password:
   ```

   此示例为三个存储系统设置了一个名为 `root` 的用户：

   ```
   # snapdrive config set root toaster oven broiler
   Password for root:
   Retype Password:
   ```

3. 如果您的另一个存储系统使用不同的用户名或密码，请重复这些步骤。

验证与 **SnapDrive for UNIX** 关联的存储系统用户名

您可以通过执行 SnapDrive config list` 命令来验证哪个用户名 SnapDrive for UNIX 与存储系统关联。

您必须已以 root 用户身份登录。

步骤

1. 输入以下命令：

` * SnapDrive 配置列表 *`

此命令显示在 SnapDrive for UNIX 中指定了用户的所有系统的用户名或存储系统对。它不会显示存储系统的密码。

此示例显示了与名为 Rapidel 的存储系统和中型存储系统关联的用户：

```
# snapdrive config list
user name           storage system name
-----------------------------
rumplestiltskins    rapunzel
longuser            mediumstoragesystem
```

删除存储系统的用户登录名

您可以通过执行 SnapDrive config delete` 命令来删除一个或多个存储系统的用户登录名。

确保以 root 用户身份登录。

步骤

1. 输入以下命令：

   ` * SnapDrive config delete *appliage_name [appliation_name]**`

   ` 设备名称 _` 是要删除其用户登录信息的存储系统的名称。

   SnapDrive for UNIX 会删除您指定的存储系统的用户名或密码登录信息。

   要使适用于 UNIX 的 SnapDrive 能够访问存储系统，必须指定新的用户登录名。

设置 HTTP

您可以将适用于 UNIX 的 SnapDrive 配置为对主机平台使用 HTTP 。

确保以 root 用户身份登录。

步骤

1. 备份 `snapdrive.conf` 文件。
2. 在文本编辑器中打开 `snapdrive.conf` 文件。
3. 将 ` use-https-to_filer_` 变量的值更改为 `off` 。

   修改 `snapdrive.conf` 文件时，最好执行以下步骤：

   a. 注释掉要修改的行。
   b. 复制已注释掉的行。

c. 删除井号（#），取消对复制的文本的注释。

d. 修改此值。

4. 更改后保存文件。

   SnapDrive for UNIX 会在每次启动此文件时自动对其进行检查。要使更改生效，必须重新启动 SnapDrive for UNIX 守护进程。