# 使用命令行界面管理 SVM 上的 NTFS 文件安全性， NTFS 审核策略和存储级别访问防护

ONTAP 9

NetApp
April 24, 2024

# 目录

# 使用命令行界面管理 SVM 上的 NTFS 文件安全性，NTFS 审核策略和存储级别访问防护

## 使用 CLI 概述管理 SVM 上的 NTFS 文件安全性， NTFS 审核策略和存储级别访问防护

您可以使用命令行界面管理 Storage Virtual Machine （ SVM ）上的 NTFS 文件安全性，NTFS 审核策略和存储级别访问防护。

您可以从 SMB 客户端或使用命令行界面管理 NTFS 文件安全性和审核策略。但是，使用命令行界面配置文件安全性和审核策略后，无需使用远程客户端来管理文件安全性。使用 CLI 可以显著缩短使用一个命令对多个文件和文件夹应用安全性所需的时间。

您可以配置存储级别访问防护，这是 ONTAP 应用于 SVM 卷的另一层安全保护。存储级别访问防护适用场景从所有 NAS 协议访问应用了存储级别访问防护的存储对象。

只能通过 ONTAP 命令行界面配置和管理存储级别访问防护。您不能从 SMB 客户端管理存储级别访问防护设置。此外，如果您从 NFS 或 SMB 客户端查看文件或目录的安全设置，则不会看到存储级别访问防护安全性。即使是系统（ Windows 或 UNIX ）管理员也无法从客户端撤消存储级别访问防护安全性。因此，存储级别访问防护为数据访问提供了额外的安全层，该层由存储管理员独立设置和管理。

> 即使存储级别访问防护仅支持 NTFS 访问权限，但如果 UNIX 用户映射到拥有该卷的 SVM 上的 Windows 用户，则 ONTAP 可以对通过 NFS 访问应用了存储级别访问防护的卷上的数据执行安全检查。

### NTFS 安全模式卷

NTFS 安全模式卷和 qtree 中包含的所有文件和文件夹都具有 NTFS 有效安全性。您可以使用 `vserver security file-directory` 命令系列、用于在NTFS安全模式卷上实施以下类型的安全性：

- 卷中包含的文件和文件夹的文件权限和审核策略
- 卷上的存储级别访问防护安全性

### 混合安全模式卷

混合安全模式卷和 qtree 可以包含一些具有 UNIX 有效安全性并使用 UNIX 文件权限（模式位或 NFSv4.x ACL 和 NFSv4.x 审核策略）的文件和文件夹，以及一些具有 NTFS 有效安全性并使用 NTFS 文件权限和审核策略的文件和文件夹。您可以使用 `vserver security file-directory` 用于将以下类型的安全性应用于混合安全模式数据的命令系列：

- 混合卷或 qtree 中采用 NTFS 有效安全模式的文件和文件夹的文件权限和审核策略
- 对采用 NTFS 和 UNIX 有效安全模式的卷的存储级别访问防护

### UNIX安全模式卷

UNIX 安全模式卷和 qtree 包含具有 UNIX 有效安全性（模式位或 NFSv4.x ACL ）的文件和文件夹。如果要使用、必须牢记以下几点 `vserver security file-directory` 用于在UNIX安全模式卷上实施安全性的命令

系列：

- 。 `vserver security file-directory` 命令系列不能用于管理UNIX安全模式卷和qtrees上的UNIX文件安全性和审核策略。
- 您可以使用 `vserver security file-directory` 命令系列、用于在UNIX安全模式卷上配置存储级别访问防护、前提是带有目标卷的SVM包含CIFS服务器。

相关信息

显示有关文件安全性和审核策略的信息

使用命令行界面在 NTFS 文件和文件夹上配置和应用文件安全性

使用命令行界面配置审核策略并将其应用于 NTFS 文件和文件夹

使用存储级别访问防护确保文件访问安全

# 使用命令行界面设置文件和文件夹安全性的用例

由于您可以在本地应用和管理文件和文件夹安全性，而无需远程客户端的参与，因此可以显著缩短为大量文件或文件夹设置批量安全性所需的时间。

在以下使用情形中，使用命令行界面设置文件和文件夹安全性会很有用：

- 在大型企业环境中存储文件，例如主目录中的文件存储
- 数据迁移
- 更改 Windows 域
- 跨 NTFS 文件系统实现文件安全和审核策略标准化

# 使用命令行界面设置文件和文件夹安全性的限制

在使用命令行界面设置文件和文件夹安全性时，您需要了解某些限制。

- 。 `vserver security file-directory` 命令系列不支持设置NFSv4 ACL。

  您只能将 NTFS 安全描述符应用于 NTFS 文件和文件夹。

# 如何使用安全描述符应用文件和文件夹安全性

安全描述符包含访问控制列表，用于确定用户可以对文件和文件夹执行的操作以及在用户访问文件和文件夹时审核的内容。

- * 权限 *

  权限由对象的所有者允许或拒绝，并确定对象（用户，组或计算机对象）可以对指定文件或文件夹执行的操作。

- * 安全描述符 *

  安全描述符是指包含安全信息的数据结构，用于定义与文件或文件夹关联的权限。

- * 访问控制列表（ACL） *

  访问控制列表是安全描述符中包含的列表，其中包含有关用户，组或计算机对象可以对应用了安全描述符的文件或文件夹执行的操作的信息。安全描述符可以包含以下两种类型的 ACL：

  - 随机访问控制列表（DACL）
  - 系统访问控制列表（SACL）

- * 随机访问控制列表（DACL） *

  DACL 包含允许或拒绝对文件或文件夹执行操作的用户，组和计算机对象的 SID 列表。DACL 包含零个或多个访问控制条目（ACE）。

- * 系统访问控制列表（SACL） *

  SACL 包含记录成功或失败审核事件的用户，组和计算机对象的 SID 列表。SACL 包含零个或多个访问控制条目（ACE）。

- * 访问控制条目（ACE） *

  ACE 是 DACL 或 SACL 中的各个条目：

  - DACL 访问控制条目指定允许或拒绝特定用户，组或计算机对象的访问权限。
  - SACL 访问控制条目指定审核特定用户，组或计算机对象执行的指定操作时要记录的成功或失败事件。

- * 权限继承 *

  权限继承介绍如何将安全描述符中定义的权限从父对象传播到对象。子对象仅继承可继承的权限。在对父对象设置权限时、您可以通过"`Apply to "(应用到)来确定文件夹、子文件夹和文件是否可以继承它们 `this-folder`， `sub-folders`和`files`”。

相关信息

"SMB 和 NFS 审核和安全跟踪"

使用命令行界面配置审核策略并将其应用于 NTFS 文件和文件夹

# 在 SVM 灾难恢复目标上应用使用本地用户或组的文件目录策略的准则

## 如果文件目录策略配置在安全描述符或 DACL 或 SACL 条目中使用本地用户或组，则在 ID 丢弃配置中对 Storage Virtual Machine （SVM）灾难恢复目标应用文件目录策略之前，必须牢记一些特定准则。

您可以为 SVM 配置灾难恢复配置，以便源集群上的源 SVM 将数据和配置从源 SVM 复制到目标集群上的目标 SVM 。

您可以设置以下两种类型的 SVM 灾难恢复之一：

- 身份保留

  在此配置中， SVM 和 CIFS 服务器的标识将保留下来。

- 已丢弃身份

  在此配置中，不会保留 SVM 和 CIFS 服务器的身份。在这种情况下，目标 SVM 上的 SVM 和 CIFS 服务器名称与源 SVM 上的 SVM 和 CIFS 服务器名称不同。

## 身份丢弃配置准则

在身份丢弃配置中，对于包含本地用户，组和权限配置的 SVM 源，必须更改本地域的名称（本地 CIFS 服务器名称），使其与 SVM 目标上的 CIFS 服务器名称匹配。例如，如果源 SVM 名称为 “vs1` " ， CIFS 服务器名称为 "`CIFS1` " ，而目标 SVM 名称为 "`vs1_dst` " ， CIFS 服务器名称为 "`CIFS1_dst` " ，则本地用户的本地域名 "`CIFS1\user1` " 会自动更改为` " 目标 SIFS1\DST1”：

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

即使本地用户和组名称会在本地用户和组数据库中自动更改、但本地用户或组名称不会在文件目录策略配置(使用在命令行界面上配置的策略)中自动更改 `vserver security file-directory` 命令系列)。

例如、对于"`VS1`"、如果您在中配置了DACL条目 `-account` 参数设置为"`CIFS1\user1`"、则此设置不会在目标SVM上自动更改、以反映目标的CIFS服务器名称。

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

您必须使用 `vserver security file-directory modify` 用于手动将CIFS服务器名称更改为目标CIFS服务器名称的命令。

## 包含帐户参数的文件目录策略配置组件

有三个文件目录策略配置组件可以使用可包含本地用户或组的参数设置：

- 安全描述符

  您可以选择指定安全描述符的所有者以及安全描述符所有者的主组。如果安全描述符对所有者和主组条目使用本地用户或组，则必须修改安全描述符，以便在帐户名称中使用目标 SVM 。您可以使用 `vserver security file-directory ntfs modify` 命令以对帐户名称进行任何必要的更改。

- DACL 条目

  每个 DACL 条目都必须与一个帐户相关联。您必须修改任何使用本地用户或组帐户的 DACL ，才能使用目标 SVM 名称。由于您无法修改现有 DACL 条目的帐户名称，因此必须从安全描述符中删除任何具有本地用户或组的 DACL 条目，使用更正后的目标帐户名称创建新的 DACL 条目，并将这些新的 DACL 条目与相应的安全描述符关联。

- SACL条目

  每个SACL条目都必须与一个帐户关联。您必须修改任何使用本地用户或组帐户的 SACL ，以使用目标 SVM 名称。由于您无法修改现有 SACL 条目的帐户名称，因此必须从安全描述符中删除任何具有本地用户或组的 SACL 条目，使用更正后的目标帐户名称创建新的 SACL 条目，并将这些新的 SACL 条目与相应的安全描述符相关联。

在应用此策略之前，您必须对文件目录策略配置中使用的本地用户或组进行任何必要的更改；否则，应用作业将失败。

# 使用命令行界面在 NTFS 文件和文件夹上配置和应用文件安全性

## 创建 NTFS 安全描述符

创建 NTFS 安全描述符（文件安全策略）是配置 NTFS 访问控制列表（ ACL ）并将其应用于 Storage Virtual Machine （ SVM ）中的文件和文件夹的第一步。您可以将安全描述符与策略任务中的文件或文件夹路径相关联。

关于此任务

您可以为 NTFS 安全模式卷中的文件和文件夹或混合安全模式卷上的文件和文件夹创建 NTFS 安全描述符。

默认情况下，在创建安全描述符时，会向该安全描述符添加四个随机访问控制列表（ DACL ）访问控制条目（ ACE ）。四个默认 ACE 如下所示：

| 对象 | 访问类型 | 访问权限 | 应用权限的位置 |
|---|---|---|---|
| BUILTIN\Administrators | 允许 | 完全控制 | 此文件夹，子文件夹，文件 |
| BUILTIN\Users | 允许 | 完全控制 | 此文件夹，子文件夹，文件 |
| Creator 所有者 | 允许 | 完全控制 | 此文件夹，子文件夹，文件 |
| NT AUTHORITIC\SYSTEM | 允许 | 完全控制 | 此文件夹，子文件夹，文件 |

您可以使用以下可选参数自定义安全描述符配置：

- 安全描述符的所有者
- 所有者的主组
- 原始控制标志

存储级别访问防护将忽略任何可选参数的值。有关详细信息，请参见手册页。

## 将NTFS DACL访问控制条目添加到NTFS安全描述符中

向 NTFS 安全描述符添加 DACL （随机访问控制列表）访问控制条目（ ACE ）是配置 NTFS ACL 并将其应用于文件或文件夹的第二步。每个条目都标识允许或拒绝访问的对象，并定义对象可以或不能对 ACE 中定义的文件或文件夹执行的操作。

关于此任务

您可以将一个或多个ACL添加到安全描述符的DACL中。

如果安全描述符包含具有现有 ACE 的 DACL ，则该命令会将新 ACE 添加到 DACL 中。如果安全描述符不包含 DACL ，则该命令将创建 DACL 并向其中添加新 ACE 。

您可以选择通过指定要为中指定的帐户允许或拒绝的权限来自定义DACL条目 `-account` 参数。指定权限的方法有三种，这三种方法是互斥的：

- 权限
- 高级权限
- 原始权限（高级权限）

> 如果未指定DACL条目的权限、则默认为将权限设置为 `Full Control`。

您可以选择通过指定如何应用继承来自定义 DACL 条目。

存储级别访问防护将忽略任何可选参数的值。有关详细信息，请参见手册页。

步骤

1. 将DACL条目添加到安全描述符： `vserver security file-directory ntfs dacl add -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
   -account domain\joe -rights full-control -apply-to this-folder -vserver vs1
   ```

2. 验证DACL条目是否正确： `vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

   ```
   vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

   ```
                        Vserver: vs1
   Security Descriptor Name: sd1
                  Allow or Deny: deny
               Account Name or SID: DOMAIN\joe
                  Access Rights: full-control
         Advanced Access Rights: -
                       Apply To: this-folder
                  Access Rights: full-control
   ```

## 创建安全策略

为 SVM 创建文件安全策略是配置 ACL 并将其应用于文件或文件夹的第三步。策略充当各种任务的容器，其中每个任务都是一个条目，可应用于文件或文件夹。您可以稍后将任务添加到安全策略中。

关于此任务

添加到安全策略的任务包含 NTFS 安全描述符与文件或文件夹路径之间的关联。因此，您应将安全策略与每个 SVM （包含 NTFS 安全模式卷或混合安全模式卷）相关联。

步骤

1. 创建安全策略： `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. 验证安全策略： `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

## 将任务添加到安全策略中

创建策略任务并将其添加到安全策略是配置 ACL 并将其应用于 SVM 中的文件或文件夹的第四步。创建策略任务时，您需要将此任务与安全策略相关联。您可以将一个或多个任务条目添加到安全策略中。

关于此任务

安全策略是任务的容器。任务是指可通过安全策略对具有 NTFS 或混合安全模式的文件或文件夹（如果配置存储级别访问防护，则也可以对卷对象）执行的单个操作。

任务类型有两种：

- 文件和目录任务

  用于指定将安全描述符应用于指定文件和文件夹的任务。通过文件和目录任务应用的 ACL 可以通过 SMB 客户端或 ONTAP 命令行界面进行管理。

- 存储级别访问防护任务

  用于指定将存储级别访问防护安全描述符应用于指定卷的任务。通过存储级别访问防护任务应用的 ACL 只能通过 ONTAP 命令行界面进行管理。

任务包含文件（或文件夹）或一组文件（或文件夹）的安全配置定义。策略中的每个任务都由路径唯一标识。一个策略中的每个路径只能有一个任务。策略不能包含重复的任务条目。

将任务添加到策略的准则：

- 每个策略最多可以包含 10 ， 000 个任务条目。
- 一个策略可以包含一个或多个任务。

  即使策略可以包含多个任务，您也无法将策略配置为同时包含文件目录和存储级别访问防护任务。策略必须

包含所有存储级别访问防护任务或所有文件目录任务。

- 存储级别访问防护用于限制权限。

  它不会提供额外的访问权限。

向安全策略添加任务时，必须指定以下四个必需参数：

- SVM name
- Policy name
- 路径
- 要与路径关联的安全描述符

您可以使用以下可选参数自定义安全描述符配置：

- 安全类型
- 传播模式
- 索引位置
- 访问控制类型

存储级别访问防护将忽略任何可选参数的值。有关详细信息，请参见手册页。

步骤

1. 将具有关联安全描述符的任务添加到安全策略： `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` 是的默认值 `-access-control` 参数。在配置文件和目录访问任务时指定访问控制类型是可选的。

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
   -index-num 1 -access-control file-directory
   ```

2. 验证策略任务配置： `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

```
Vserver: vs1
Policy: policy1

Index    File/Folder    Access           Security   NTFS       NTFS
Security
         Path           Control          Type       Mode
Descriptor Name
-----    --------       -----------      --------   ------
----------------
1        /home/dir1     file-directory   ntfs       propagate  sd2
```

## 应用安全策略

将文件安全策略应用于 SVM 是创建 NTFS ACL 并将其应用于文件或文件夹的最后一步。

关于此任务

您可以将安全策略中定义的安全设置应用于驻留在 FlexVol 卷（ NTFS 或混合安全模式）中的 NTFS 文件和文件夹。

> 应用审核策略和关联的 SACL 后，任何现有 DACL 都会被覆盖。应用安全策略及其关联的DACL后、任何现有DACL都会被覆盖。在创建和应用新安全策略之前，您应查看现有安全策略。

步骤

1. 应用安全策略： `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory apply -vserver vs1 -policy-name policy1`

   此时将计划策略应用作业，并返回作业 ID 。

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

## 监控安全策略作业

在将安全策略应用于 Storage Virtual Machine （ SVM ）时，您可以通过监控安全策略作业来监控任务进度。如果您希望确定安全策略的应用成功，这将非常有用。如果您的作业运行时间较长，并且要对大量文件和文件夹应用批量安全性，则此功能也会很有用。

关于此任务

要显示有关安全策略作业的详细信息、应使用 `-instance` 参数。

步骤

1. 监控安全策略作业：`vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

```
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
53322  Fsecurity Apply      vs1        node1          Success
       Description: File Directory Security Apply Job
```

## 验证应用的文件安全性

### 您可以验证文件安全设置，以确认应用安全策略的 Storage Virtual Machine （SVM）上的文件或文件夹具有所需设置。

#### 关于此任务

您必须提供包含要验证安全设置的文件和文件夹的数据和路径的 SVM 名称。您可以使用可选 `-expand-mask` 用于显示有关安全设置的详细信息的参数。

#### 步骤

1. 显示文件和文件夹安全设置：`vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

   `vserver security file-directory show -vserver vs1 -path /data/engineering -expand-mask true`

```
          Vserver: vs1
               File Path: /data/engineering
      File Inode Number: 5544
          Security Style: ntfs
         Effective Style: ntfs
          DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 0
          Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
```

```
                    ACLs: NTFS Security Descriptor
                          Control:0x8004

                              1... .... .... .... = Self Relative
                              .0.. .... .... .... = RM Control Valid
                              ..0. .... .... .... = SACL Protected
                              ...0 .... .... .... = DACL Protected
                              .... 0... .... .... = SACL Inherited
                              .... .0.. .... .... = DACL Inherited
                              .... ..0. .... .... = SACL Inherit Required
                              .... ...0 .... .... = DACL Inherit Required
                              .... .... ..0. .... = SACL Defaulted
                              .... .... ...0 .... = SACL Present
                              .... .... .... 0... = DACL Defaulted
                              .... .... .... .1.. = DACL Present
                              .... .... .... ..0. = Group Defaulted
                              .... .... .... ...0 = Owner Defaulted

                          Owner:BUILTIN\Administrators
                          Group:BUILTIN\Administrators
                          DACL - ACEs
                            ALLOW-Everyone-0x1f01ff
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...0 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
```

```
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
Write Owner
                              .... .... .... .0.. .... .... .... .... =
Write DAC
                              .... .... .... ..0. .... .... .... .... =
Read Control
                              .... .... .... ...0 .... .... .... .... =
Delete
                              .... .... .... .... .... ...0 .... .... =
Write Attributes
                              .... .... .... .... .... .... 0... .... =
Read Attributes
                              .... .... .... .... .... .... .0.. .... =
Delete Child
                              .... .... .... .... .... .... ..0. .... =
Execute
                              .... .... .... .... .... .... ...0 .... =
Write EA
```

```
                                .... .... .... .... .... .... .... 0... =
Read EA
                                .... .... .... .... .... .... .... .0.. =
Append
                                .... .... .... .... .... .... .... ..0. =
Write
                                .... .... .... .... .... .... .... ...0 =
Read
```

# 使用 CLI 概述配置审核策略并将其应用于 NTFS 文件和文件夹

使用 ONTAP 命令行界面时，要将审核策略应用于 NTFS 文件和文件夹，必须执行几个步骤。首先，创建 NTFS 安全描述符并将 SACL 添加到安全描述符中。接下来，创建安全策略并添加策略任务。然后，将此安全策略应用于 Storage Virtual Machine （ SVM ）。

关于此任务

应用安全策略后，您可以监控安全策略作业，然后验证应用的审核策略的设置。

> 应用审核策略和关联的 SACL 后，任何现有 DACL 都会被覆盖。在创建和应用新安全策略之前，您应查看现有安全策略。

相关信息

使用存储级别访问防护保护文件访问安全

使用命令行界面设置文件和文件夹安全性的限制

如何使用安全描述符应用文件和文件夹安全性

"SMB 和 NFS 审核和安全跟踪"

使用命令行界面在 NTFS 文件和文件夹上配置和应用文件安全性

## 创建 NTFS 安全描述符

创建 NTFS 安全描述符审核策略是配置 NTFS 访问控制列表（ ACL ）并将其应用于 SVM 中的文件和文件夹的第一步。您将在策略任务中将安全描述符与文件或文件夹路径相关联。

关于此任务

您可以为 NTFS 安全模式卷中的文件和文件夹或混合安全模式卷上的文件和文件夹创建 NTFS 安全描述符。

默认情况下，在创建安全描述符时，会向该安全描述符添加四个随机访问控制列表（ DACL ）访问控制条目（ ACE ）。四个默认 ACE 如下所示：

| 对象 | 访问类型 | 访问权限 | 应用权限的位置 |
| --- | --- | --- | --- |
| BUILTIN\Administrators | 允许 | 完全控制 | 此文件夹，子文件夹，文件 |
| BUILTIN\Users | 允许 | 完全控制 | 此文件夹，子文件夹，文件 |
| Creator 所有者 | 允许 | 完全控制 | 此文件夹，子文件夹，文件 |
| NT AUTHORITIC\SYSTEM | 允许 | 完全控制 | 此文件夹，子文件夹，文件 |

您可以使用以下可选参数自定义安全描述符配置：

- 安全描述符的所有者
- 所有者的主组
- 原始控制标志

存储级别访问防护将忽略任何可选参数的值。有关详细信息，请参见手册页。

步骤

1. 如果要使用高级参数、请将权限级别设置为高级： `set -privilege advanced`
2. 创建安全描述符： `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   `vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe`

3. 验证安全描述符配置是否正确： `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

   ```
   vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
   ```

   ```
                                   Vserver: vs1
                         Security Descriptor Name: sd1
                   Owner of the Security Descriptor: DOMAIN\joe
   ```

4. 如果您处于高级权限级别、请返回到管理权限级别： `set -privilege admin`

## 将 **NTFS SACL** 访问控制条目添加到 **NTFS** 安全描述符

向 NTFS 安全描述符添加 SACL （系统访问控制列表）访问控制条目（ ACE ）是为 SVM

中的文件或文件夹创建 NTFS 审核策略的第二步。每个条目都标识要审核的用户或组。SACL 条目用于定义是要审核成功的还是失败的访问尝试。

关于此任务

您可以将一个或多个 ACE 添加到安全描述符的 SACL 中。

如果安全描述符包含具有现有 ACE 的 SACL ，则该命令会将新 ACE 添加到 SACL 。如果安全描述符不包含 SACL ，则该命令将创建 SACL 并将新 ACE 添加到其中。

您可以通过为中指定的帐户指定要审核成功或失败事件的权限来配置SACL条目 `-account` 参数。指定权限的方法有三种，这三种方法是互斥的：

- 权限
- 高级权限
- 原始权限（高级权限）

> 如果未指定SACL条目的权限、则默认设置为 `Full Control`。

您可以选择通过指定如何使用应用继承来自定义SACL条目 `apply to` 参数。如果未指定此参数，则默认情况下会将此 SACL 条目应用于此文件夹，子文件夹和文件。

步骤

1. 将SACL条目添加到安全描述符： `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

   ```
   vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
   failure -account domain\joe -rights full-control -apply-to this-folder
   -vserver vs1
   ```

2. 验证SACL条目是否正确： `vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

   ```
   vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
   -access-type deny -account domain\joe
   ```

   ```
                                   Vserver: vs1
                     Security Descriptor Name: sd1
   Access type for Specified Access Rights: failure
                         Account Name or SID: DOMAIN\joe
                               Access Rights: full-control
                      Advanced Access Rights: -
                                    Apply To: this-folder
                               Access Rights: full-control
   ```

## 创建安全策略

为 Storage Virtual Machine （ SVM ）创建审核策略是配置 ACL 并将其应用于文件或文件夹的第三步。策略充当各种任务的容器，其中每个任务都是一个条目，可应用于文件或文件夹。您可以稍后将任务添加到安全策略中。

### 关于此任务

添加到安全策略的任务包含 NTFS 安全描述符与文件或文件夹路径之间的关联。因此，您应将安全策略与每个 Storage Virtual Machine （ SVM ）（包含 NTFS 安全模式卷或混合安全模式卷）相关联。

### 步骤

1. 创建安全策略： `vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory policy create -policy-name policy1 -vserver vs1`

2. 验证安全策略： `vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

## 将任务添加到安全策略中

创建策略任务并将其添加到安全策略是配置 ACL 并将其应用于 SVM 中的文件或文件夹的第四步。创建策略任务时，您需要将此任务与安全策略相关联。您可以将一个或多个任务条目添加到安全策略中。

### 关于此任务

安全策略是任务的容器。任务是指可通过安全策略对具有 NTFS 或混合安全模式的文件或文件夹（如果配置存储级别访问防护，则也可以对卷对象）执行的单个操作。

任务类型有两种：

- 文件和目录任务

  用于指定将安全描述符应用于指定文件和文件夹的任务。通过文件和目录任务应用的 ACL 可以通过 SMB 客户端或 ONTAP 命令行界面进行管理。

- 存储级别访问防护任务

  用于指定将存储级别访问防护安全描述符应用于指定卷的任务。通过存储级别访问防护任务应用的 ACL 只能通过 ONTAP 命令行界面进行管理。

任务包含文件（或文件夹）或一组文件（或文件夹）的安全配置定义。策略中的每个任务都由路径唯一标识。一

个策略中的每个路径只能有一个任务。策略不能包含重复的任务条目。

将任务添加到策略的准则：

- 每个策略最多可以包含 10 ， 000 个任务条目。
- 一个策略可以包含一个或多个任务。

  即使策略可以包含多个任务，您也无法将策略配置为同时包含文件目录和存储级别访问防护任务。策略必须包含所有存储级别访问防护任务或所有文件目录任务。

- 存储级别访问防护用于限制权限。

  它不会提供额外的访问权限。

您可以使用以下可选参数自定义安全描述符配置：

- 安全类型
- 传播模式
- 索引位置
- 访问控制类型

存储级别访问防护将忽略任何可选参数的值。有关详细信息，请参见手册页。

步骤

1. 将具有关联安全描述符的任务添加到安全策略： `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` 是的默认值 `-access-control` 参数。在配置文件和目录访问任务时指定访问控制类型是可选的。

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
   -index-num 1 -access-control file-directory
   ```

2. 验证策略任务配置： `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

```
Vserver: vs1
Policy: policy1

Index    File/Folder    Access           Security   NTFS       NTFS
Security
         Path           Control          Type       Mode
Descriptor Name
-----    --------       -----------      --------   ------
----------------
1        /home/dir1     file-directory   ntfs       propagate  sd2
```

## 应用安全策略

将审核策略应用于SVM是创建NTFS ACL并将其应用于文件或文件夹的最后一步。

关于此任务

您可以将安全策略中定义的安全设置应用于驻留在 FlexVol 卷（ NTFS 或混合安全模式）中的 NTFS 文件和文件夹。

> 应用审核策略和关联的 SACL 后，任何现有 DACL 都会被覆盖。应用安全策略及其关联的DACL后、任何现有DACL都会被覆盖。在创建和应用新安全策略之前，您应查看现有安全策略。

步骤

1. 应用安全策略： `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory apply -vserver vs1 -policy-name policy1`

   此时将计划策略应用作业，并返回作业 ID 。

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
   53322" command to view the status of the operation
   ```

## 监控安全策略作业

在将安全策略应用于 Storage Virtual Machine （ SVM ）时，您可以通过监控安全策略作业来监控任务进度。如果您希望确定安全策略的应用成功，这将非常有用。如果您的作业运行时间较长，并且要对大量文件和文件夹应用批量安全性，则此功能也会很有用。

关于此任务

要显示有关安全策略作业的详细信息、应使用 `-instance` 参数。

步骤

1. 监控安全策略作业： `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

```
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
53322  Fsecurity Apply      vs1        node1          Success
       Description: File Directory Security Apply Job
```

## 验证应用的审核策略

### 您可以验证审核策略，以确认应用此安全策略的 Storage Virtual Machine （ SVM ）上的文件或文件夹具有所需的审核安全设置。

#### 关于此任务

您可以使用 `vserver security file-directory show` 命令以显示审核策略信息。您必须提供包含要显示其文件或文件夹审核策略信息的数据所在 SVM 的名称以及该数据的路径。

#### 步骤

1. 显示审核策略设置： `vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*

#### 示例

以下命令显示应用于 SVM vs1 中路径 "` /corp` " 的审核策略信息。此路径同时应用了成功和成功 / 失败 SACL 条目：

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

                Vserver: vs1
              File Path: /corp
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

# 管理安全策略作业时的注意事项

## 如果存在安全策略作业，则在某些情况下，您无法修改该安全策略或分配给该策略的任务。您应了解可以或不能在哪些条件下修改安全策略，以便成功尝试修改此策略。对策略的修改包括添加，删除或修改分配给策略的任务以及删除或修改策略。

如果某个安全策略存在作业且该作业处于以下状态，则无法修改该策略或分配给该策略的任务：

- 作业正在运行或正在进行中。
- 作业已暂停。
- 作业将恢复并处于运行状态。
- 作业正在等待故障转移到其他节点。

在以下情况下，如果某个安全策略存在作业，则可以成功修改该安全策略或分配给该策略的任务：

- 策略作业已停止。
- 策略作业已成功完成。

# 用于管理 NTFS 安全描述符的命令

您可以使用特定的 ONTAP 命令来管理安全描述符。您可以创建，修改，删除和显示有关安全描述符的信息。

| 如果您要 ... | 使用此命令 ... |
| --- | --- |
| 创建 NTFS 安全描述符 | `vserver security file-directory ntfs create` |
| 修改现有 NTFS 安全描述符 | `vserver security file-directory ntfs modify` |
| 显示有关现有 NTFS 安全描述符的信息 | `vserver security file-directory ntfs show` |
| 删除 NTFS 安全描述符 | `vserver security file-directory ntfs delete` |

请参见的手册页 `vserver security file-directory ntfs` 有关详细信息、请参见命令。

# 用于管理 NTFS DACL 访问控制条目的命令

您可以使用特定的 ONTAP 命令来管理 DACL 访问控制条目（ACE）。您可以随时将 ACE 添加到 NTFS DACL 中。您还可以通过修改，删除和显示有关 DACL 中 ACE 的信息来管理现有 NTFS DACL 。

| 如果您要 ... | 使用此命令 ... |
| --- | --- |
| 创建 ACE 并将其添加到 NTFS DACL 中 | `vserver security file-directory ntfs dacl add` |
| 修改 NTFS DACL 中的现有 ACE | `vserver security file-directory ntfs dacl modify` |
| 显示有关 NTFS DACL 中现有 ACE 的信息 | `vserver security file-directory ntfs dacl show` |
| 从 NTFS DACL 中删除现有 ACE | `vserver security file-directory ntfs dacl remove` |

请参见的手册页 `vserver security file-directory ntfs dacl` 有关详细信息、请参见命令。

## 用于管理NTFS SACL访问控制条目的命令

您可以使用特定的ONTAP命令来管理SACL访问控制条目(Access Control entries、ACE)。您可以随时将 ACE 添加到 NTFS SACL 。您还可以通过修改，删除和显示有关 SACL 中 ACE 的信息来管理现有 NTFS SACL 。

| 如果您要 ... | 使用此命令 ... |
| --- | --- |
| 创建 ACE 并将其添加到 NTFS SACL | `vserver security file-directory ntfs sacl add` |
| 修改 NTFS SACL 中的现有 ACE | `vserver security file-directory ntfs sacl modify` |
| 显示有关 NTFS SACL 中现有 ACE 的信息 | `vserver security file-directory ntfs sacl show` |
| 从 NTFS SACL 中删除现有 ACE | `vserver security file-directory ntfs sacl remove` |

请参见的手册页 `vserver security file-directory ntfs sacl` 有关详细信息、请参见命令。

## 用于管理安全策略的命令

您可以使用特定的 ONTAP 命令来管理安全策略。您可以显示有关策略的信息，也可以删除策略。您不能修改安全策略。

| 如果您要 ... | 使用此命令 ... |
| --- | --- |
| 创建安全策略 | `vserver security file-directory policy create` |
| 显示有关安全策略的信息 | `vserver security file-directory policy show` |
| 删除安全策略 | `vserver security file-directory policy delete` |

请参见的手册页 `vserver security file-directory policy` 有关详细信息、请参见命令。

## 用于管理安全策略任务的命令

您可以使用 ONTAP 命令添加，修改，删除和显示有关安全策略任务的信息。

| 如果您要 ... | 使用此命令 ... |
| --- | --- |
| 添加安全策略任务 | `vserver security file-directory policy task add` |
| 修改安全策略任务 | `vserver security file-directory policy task modify` |
| 显示有关安全策略任务的信息 | `vserver security file-directory policy task show` |
| 删除安全策略任务 | `vserver security file-directory policy task remove` |

请参见的手册页 `vserver security file-directory policy task` 有关详细信息、请参见命令。

# 用于管理安全策略作业的命令

您可以使用 ONTAP 命令暂停，恢复，停止和显示有关安全策略作业的信息。

| 如果您要 ... | 使用此命令 ... |
| --- | --- |
| 暂停安全策略作业 | `vserver security file-directory job pause -vserver vserver_name -id integer` |
| 恢复安全策略作业 | `vserver security file-directory job resume -vserver vserver_name -id integer` |
| 显示有关安全策略作业的信息 | `vserver security file-directory job show -vserver vserver_name` 您可以使用此命令确定作业的作业ID。 |
| 停止安全策略作业 | `vserver security file-directory job stop -vserver vserver_name -id integer` |

请参见的手册页 `vserver security file-directory job` 有关详细信息、请参见命令。