



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 ONTAP 9

NetApp
April 24, 2024

目录

- 使用 CLI 概述配置审核策略并将其应用于 NTFS 文件和文件夹..... 1
 - 创建 NTFS 安全描述符..... 1
 - 将 NTFS SACL 访问控制条目添加到 NTFS 安全描述符..... 2
 - 创建安全策略..... 3
 - 将任务添加到安全策略中..... 4
 - 应用安全策略..... 5
 - 监控安全策略作业..... 6
 - 验证应用的审核策略..... 6

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

对象	访问类型	访问权限	应用权限的位置
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_name optional_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_SID optional_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
```

版权信息

版权所有 © 2024 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。