



显示有关应用于文件和目录的审核策略的信息 ONTAP 9

NetApp
April 24, 2024

目录

- 显示有关应用于文件和目录的审核策略的信息 1
 - 使用 Windows 安全性选项卡显示有关审核策略的信息 1
 - 使用命令行界面显示有关 FlexVol 卷上 NTFS 审核策略的信息 2
 - 显示有关文件安全性和审核策略信息的方式 4

显示有关应用于文件和目录的审核策略的信息

使用 Windows 安全性选项卡显示有关审核策略的信息

您可以使用 Windows 属性窗口中的安全性选项卡显示已应用于文件和目录的审核策略的信息。这与驻留在 Windows 服务器上的数据使用的方法相同，这样客户就可以使用他们习惯使用的相同图形用户界面。

关于此任务

通过显示应用于文件和目录的审核策略信息，您可以验证是否已在指定文件和文件夹上设置了适当的系统访问控制列表（SACL）。

要显示已应用于 NTFS 文件和文件夹的 SACL 的信息，请在 Windows 主机上完成以下步骤。

步骤

1. 从 Windows 资源管理器的 * 工具 * 菜单中，选择 * 映射网络驱动器 *。
2. 完成 * 映射网络驱动器 * 对话框：
 - a. 选择一个 * 驱动器 * 字母。
 - b. 在 * 文件夹 * 框中，键入 Storage Virtual Machine (SVM) 的 IP 地址或 SMB 服务器名称，该共享包含要审核的数据和共享名称。

如果 SMB 服务器名称为 `SMB_Server`、而共享名为 `share1`、则应输入 `\\SMB_SERVER\share1`。



您可以指定 SMB 服务器数据接口的 IP 地址、而不是 SMB 服务器名称。

- c. 单击 * 完成 *。

您选择的驱动器已挂载并准备就绪，此时将显示 Windows 资源管理器窗口，其中显示共享中包含的文件和文件夹。

3. 选择要显示其审核信息的文件或目录。
4. 右键单击文件或目录，然后选择 * 属性 *。
5. 选择 * 安全性 * 选项卡。
6. 单击 * 高级 *。
7. 选择 * 审核 * 选项卡。
8. 单击 * 继续 *。

此时将打开审核框。"* 审核条目 *" 框显示应用了 SACL 的用户和组的摘要。

9. 在 * 审核条目 * 框中，选择要显示其 SACL 条目的用户或组。
10. 单击 * 编辑 *。

此时将打开 "<objecy> 的审核条目 " 框。

- 11. 在 * 访问 * 框中，查看应用于选定对象的当前 SACL。
- 12. 单击 * 取消 * 以关闭 * 审核条目 < 对象 >* 框。
- 13. 单击 * 取消 * 关闭 * 审核 * 框。

使用命令行界面显示有关 FlexVol 卷上 NTFS 审核策略的信息

您可以显示有关 FlexVol 卷上的 NTFS 审核策略的信息，包括什么是安全模式和有效安全模式，应用了哪些权限以及有关系统访问控制列表的信息。您可以使用这些信息验证安全配置或对审核问题进行故障排除。

关于此任务

通过显示应用于文件和目录的审核策略信息，您可以验证是否已在指定文件和文件夹上设置了适当的系统访问控制列表（SACL）。

您必须提供 Storage Virtual Machine（SVM）的名称以及要显示其审核信息的文件或文件夹的路径。您可以摘要形式或详细列表形式显示输出。

- 对于审核策略，NTFS 安全模式卷和 qtree 仅使用 NTFS 系统访问控制列表（SACL）。
- 具有 NTFS 有效安全性的混合安全模式卷中的文件和文件夹可以应用 NTFS 审核策略。

混合安全模式卷和 qtree 可以包含一些使用 UNIX 文件权限的文件和目录，模式位或 NFSv4 ACL，以及一些使用 NTFS 文件权限的文件和目录。

- 混合安全模式卷的顶层可以具有 UNIX 或 NTFS 有效安全性，并且可能包含也可能不包含 NTFS SACL。
- 由于即使卷根或 qtree 的有效安全模式为 UNIX，也可以在混合安全模式卷或 qtree 上配置存储级别访问防护安全性，配置了存储级别访问防护的卷或 qtree 路径的输出可能会同时显示常规文件和文件夹 NFSv4 SACL 以及存储级别访问防护 NTFS SACL。
- 如果在命令中输入的路径指向采用 NTFS 有效安全模式的数据，则如果为给定文件或目录路径配置了动态访问控制，则输出还会显示有关动态访问控制 ACE 的信息。
- 显示有关具有 NTFS 有效安全性的文件和文件夹的安全信息时，与 UNIX 相关的输出字段包含仅显示的 UNIX 文件权限信息。

在确定文件访问权限时，NTFS 安全模式文件和文件夹仅使用 NTFS 文件权限以及 Windows 用户和组。

- 只有采用 NTFS 或 NFSv4 安全模式的文件和文件夹才会显示 ACL 输出。

对于使用 UNIX 安全性且仅应用模式位权限（无 NFSv4 ACL）的文件和文件夹，此字段为空。

- ACL 输出中的所有者和组输出字段仅适用于 NTFS 安全描述符。

步骤

1. 显示具有所需详细级别的文件和目录审核策略设置：

要显示信息的项	输入以下命令 ...
摘要形式	<code>vserver security file-directory show -vserver vserver_name -path path</code>

作为详细列表	<code>vserver security file-directory show -vserver vserver_name -path path -expand-mask true</code>
--------	------------------------------------------------------------------------------------------------------

示例

以下示例显示了路径的审核策略信息 `/corp` 在SVM VS1中。此路径具有 NTFS 有效安全性。NTFS 安全描述符包含成功和成功 / 失败 SACL 条目。

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
      Vserver: vs1
      File Path: /corp
      File Inode Number: 357
      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
```

以下示例显示了路径的审核策略信息 `/datavol1` 在SVM VS1中。此路径包含常规文件和文件夹 SACL 以及存储级别访问防护 SACL。

```

cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

      Vserver: vs1
      File Path: /datavol1
      File Inode Number: 77
      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:0xaa14
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            SACL - ACEs
                  AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
            DACL - ACEs
                  ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                  ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

      Storage-Level Access Guard security
      SACL (Applies to Directories):
            AUDIT-EXAMPLE\Domain Users-0x120089-FA
            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Directories):
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-EXAMPLE\engineering-0x1f01ff
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
      SACL (Applies to Files):
            AUDIT-EXAMPLE\Domain Users-0x120089-FA
            AUDIT-EXAMPLE\engineering-0x1f01ff-SA
      DACL (Applies to Files):
            ALLOW-EXAMPLE\Domain Users-0x120089
            ALLOW-EXAMPLE\engineering-0x1f01ff
            ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff

```

显示有关文件安全性和审核策略信息的方式

您可以使用通配符（*）显示有关给定路径或根卷下所有文件和目录的文件安全和审核策

略的信息。

通配符（*）可用作给定目录路径的最后一个子组件，在该路径下，您希望显示所有文件和目录的信息。

如果要显示名为 "*" 的特定文件或目录的信息，则需要在双引号（" "）中提供完整路径。

示例

以下带有通配符的命令显示路径下所有文件和目录的信息 /1/ SVM VS1:

```
cluster::> vserver security file-directory show -vserver vs1 -path /1/*
```

```

    Vserver: vs1
    File Path: /1/1
    Security Style: mixed
    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:0x8514
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)

    Vserver: vs1
    File Path: /1/1/abc
    Security Style: mixed
    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:0x8404
            Owner: BUILTIN\Administrators
            Group: BUILTIN\Administrators
            DACL - ACEs
            ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

以下命令显示路径下名为""的文件的信息 /vol1/a SVM VS1。路径用双引号括起来（""）。

```
cluster::> vserver security file-directory show -vserver vs1 -path  
"/vol1/a/*"
```

```
        Vserver: vs1  
        File Path: "/vol1/a/*"  
        Security Style: mixed  
        Effective Style: unix  
        DOS Attributes: 10  
        DOS Attributes in Text: ----D---  
        Expanded Dos Attributes: -  
            Unix User Id: 1002  
            Unix Group Id: 65533  
            Unix Mode Bits: 755  
        Unix Mode Bits in Text: rwxr-xr-x  
        ACLs: NFSV4 Security Descriptor  
            Control:0x8014  
            SACL - ACEs  
                AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA  
            DACL - ACEs  
                ALLOW-EVERYONE@-0x1f00a9-FI|DI  
                ALLOW-OWNER@-0x1f01ff-FI|DI  
                ALLOW-GROUP@-0x1200a9-IG
```


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。