使用存储级别访问防护确保文件访问安全

ONTAP 9

NetApp
September 12, 2024

目录

使用存储级别访问防护确保文件访问安全

使用存储级别访问防护确保文件访问安全

除了使用原生文件级别以及导出和共享安全性来保护访问之外，您还可以配置存储级别访问防护，这是 ONTAP 在卷级别应用的第三层安全保护。从所有 NAS 协议到应用它的存储对象的存储级别访问防护适用场景访问。

仅支持 NTFS 访问权限。要使 ONTAP 对 UNIX 用户执行安全检查，以访问应用了存储级别访问防护的卷上的数据， UNIX 用户必须映射到拥有该卷的 SVM 上的 Windows 用户。

存储级别访问防护行为

- 存储级别访问防护适用场景存储对象中的所有文件或所有目录。

  由于卷中的所有文件或目录都受存储级别访问防护设置的限制，因此不需要通过传播进行继承。

- 您可以将存储级别访问防护配置为仅应用于文件，仅应用于目录或同时应用于卷中的文件和目录。
  - 文件和目录安全性

    适用场景存储对象中的每个目录和文件。这是默认设置。

  - 文件安全性

    适用场景存储对象中的每个文件。应用此安全性不会影响对目录的访问或审核。

  - 目录安全性

    适用场景存储对象中的每个目录。应用此安全性不会影响对文件的访问或审核。

- 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。

- 如果您从 NFS 或 SMB 客户端查看文件或目录的安全设置，则看不到存储级别访问防护安全性。

  它会在存储对象级别应用，并存储在用于确定有效权限的元数据中。

- 即使是系统（ Windows 或 UNIX ）管理员也无法从客户端撤消存储级别的安全性。

  它只能由存储管理员进行修改。

- 您可以将存储级别访问防护应用于采用 NTFS 或混合安全模式的卷。
- 只要包含该卷的 SVM 配置了 CIFS 服务器，您就可以对采用 UNIX 安全模式的卷应用存储级别访问防护。
- 如果卷挂载在卷接合路径下，并且该路径上存在存储级别访问防护，则该防护不会传播到挂载在该路径下的卷。
- 存储级别访问防护安全描述符可通过 SnapMirror 数据复制和 SVM 复制进行复制。

- 病毒扫描程序具有特殊例外。

  即使存储级别访问防护拒绝访问对象，也允许对这些服务器进行异常访问以筛选文件和目录。

- 如果由于存储级别访问防护而拒绝访问，则不会发送 FPolicy 通知。

访问检查的顺序

文件或目录的访问取决于导出或共享权限，卷上设置的存储级别访问防护权限以及应用于文件和 / 或目录的原生文件权限的组合效果。系统会评估所有级别的安全性，以确定文件或目录具有哪些有效权限。安全访问检查按以下顺序执行：

1. SMB 共享或 NFS 导出级别权限
2. 存储级别访问防护
3. NTFS 文件 / 文件夹访问控制列表（ ACL ）， NFSv4 ACL 或 UNIX 模式位

使用存储级别访问防护的用例

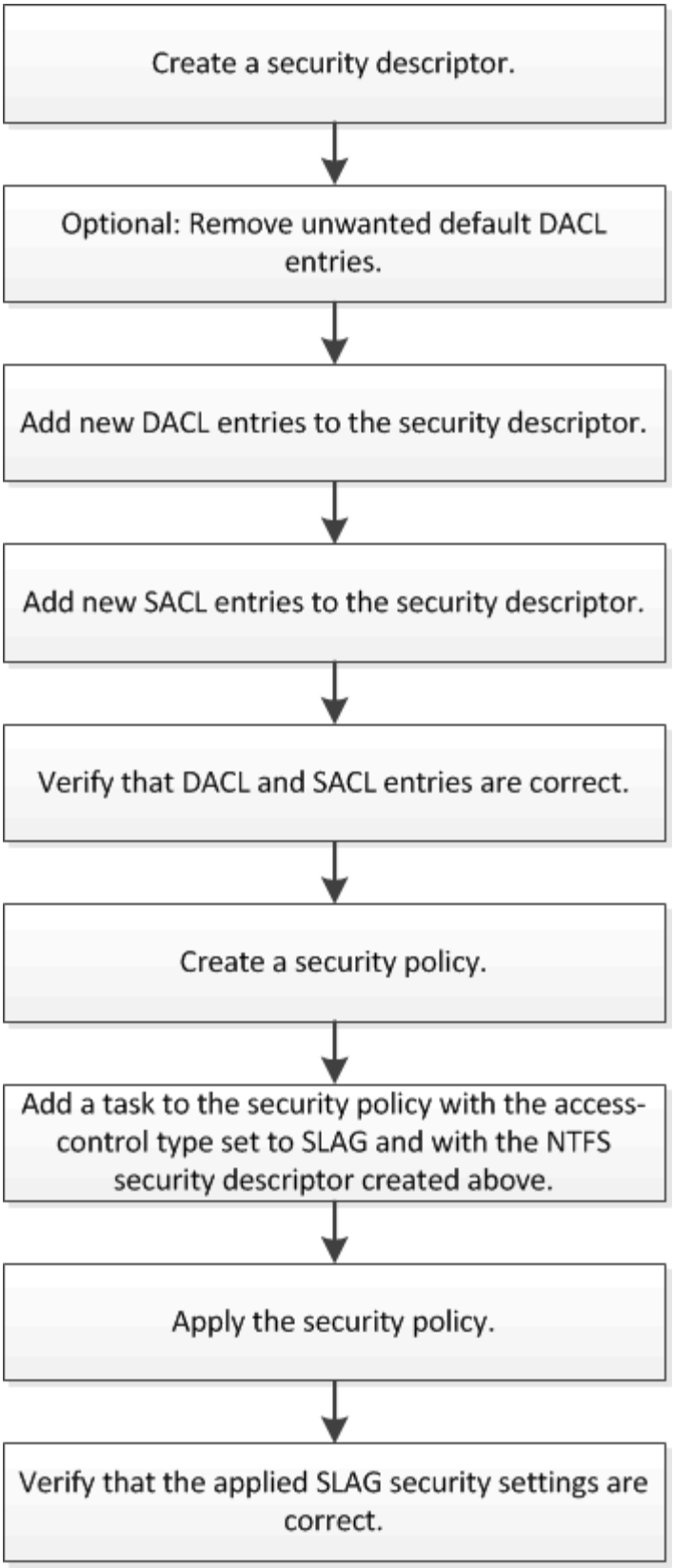
存储级别访问防护可在存储级别提供额外的安全性，这在客户端不可见；因此，任何用户或管理员都无法从其桌面撤消此功能。在某些使用情形下，在存储级别控制访问的功能会很有用。

此功能的典型使用情形包括以下情形：

- 通过审核和控制所有用户在存储级别的` 访问来保护知识产权
- 为金融服务公司提供存储，包括银行和交易团队
- 为各个部门提供单独的文件存储的政府服务
- 保护所有学生档案的大学

用于配置存储级别访问防护的工作流

配置存储级别访问防护（ SLAG ）的工作流使用与配置 NTFS 文件权限和审核策略相同的 ONTAP 命令行界面命令。您无需在指定目标上配置文件和目录访问，而是在指定的 Storage Virtual Machine （ SVM ）卷上配置 SLAG 。



相关信息

配置存储级别访问防护

配置存储级别访问防护

要在卷或 qtree 上配置存储级别访问防护，需要执行多个步骤。存储级别访问防护可提供在存储级别设置的访问安全性级别。它可以确保从所有 NAS 协议对应用了该协议的存储对象进行的所有访问均通过适用场景进行安全保护。

步骤

1. 使用创建安全描述符 `vserver security file-directory ntfs create` 命令：

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

   ```
   Vserver: vs1

      NTFS Security    Owner Name
      Descriptor Name
      ------------     --------------
      sd1              -
   ```

   系统将使用以下四个默认 DACL 访问控制条目（ACE）创建安全描述符：

   ```
   Vserver: vs1
     NTFS Security Descriptor Name: sd1

       Account Name     Access   Access          Apply To
                        Type     Rights
       --------------   -------  -------         -----------
       BUILTIN\Administrators
                        allow    full-control   this-folder, sub-folders,
   files
       BUILTIN\Users    allow    full-control   this-folder, sub-folders,
   files
       CREATOR OWNER    allow    full-control   this-folder, sub-folders,
   files
       NT AUTHORITY\SYSTEM
                        allow    full-control   this-folder, sub-folders,
   files
   ```

   如果您不想在配置存储级别访问防护时使用默认条目，则可以在创建自己的 ACE 并将其添加到安全描述符之前将其删除。

2. 从安全描述符中删除不希望配置存储级别访问防护安全性的任何默认 DACL ACE：

   a. 使用删除任何不需要的DACL ACL ACL `vserver security file-directory ntfs dacl remove` 命令：

在此示例中，将从安全描述符中删除三个默认 DACL ACE： BUILTIN\Administrators， BUILTIN\Users 和 Creator OWNER 。

```
vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
-access-type allow -account builtin\users vserver security file-directory
ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
builtin\administrators vserver security file-directory ntfs dacl remove
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
```

b. 使用验证是否已从安全描述符中删除不想用于存储级别访问防护安全性的DACL ACL ACL ACL `vserver security file-directory ntfs dacl show` 命令：

在此示例中，命令的输出将验证是否已从安全描述符中删除三个默认 DACL ACE ，而仅保留 NT AUTHORITY\SYSTEM 默认 DACL ACE 条目：

```
vserver security file-directory ntfs dacl show -vserver vs1
```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

3. 使用向安全描述符添加一个或多个DACL条目 `vserver security file-directory ntfs dacl add` 命令：

在此示例中，将两个 DACL ACE 添加到安全描述符中：

```
vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
-access-type allow -account example\engineering -rights full-control -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs dacl add
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
-rights read -apply-to this-folder,sub-folders,files
```

4. 使用向安全描述符添加一个或多个SACL条目 `vserver security file-directory ntfs sacl add` 命令：

在此示例中、将两个SACL Aces添加到安全描述符中：

```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. 使用验证是否已正确配置DACL和SACL ACL `vserver security file-directory ntfs dacl show`

和 `vserver security file-directory ntfs sacl show` 命令。

在此示例中，以下命令显示有关安全描述符 " `sD1` " 的 DACL 条目的信息：

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

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    EXAMPLE\Domain Users
                     allow    read           this-folder, sub-folders,
files
    EXAMPLE\engineering
                     allow    full-control   this-folder, sub-folders,
files
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

在此示例中、以下命令显示有关安全描述符"`sd1`"的SACL条目的信息：

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

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    EXAMPLE\Domain Users
                     failure  read           this-folder, sub-folders,
files
    EXAMPLE\engineering
                     success  full-control   this-folder, sub-folders,
files
```

6. 使用创建安全策略 `vserver security file-directory policy create` 命令：

   以下示例将创建一个名为 "`policy1` " 的策略：

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

7. 使用验证是否已正确配置此策略 `vserver security file-directory policy show` 命令：

   `vserver security file-directory policy show`

   ```
   Vserver          Policy Name
   ------------     --------------
   vs1              policy1
   ```

8. 使用将具有关联安全描述符的任务添加到安全策略中 `vserver security file-directory policy task add` 命令 `-access-control` 参数设置为 `slag`。

   即使策略可以包含多个存储级别访问防护任务，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。

   在此示例中，将任务添加到名为 "`policy1` " 的策略中，该策略分配给安全描述符 " `sD1` " 。它将分配给 `/datavol1` 访问控制类型设置为`slag`的路径。

   `vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode propagate -ntfs-sd sd1`

9. 使用验证是否已正确配置此任务 `vserver security file-directory policy task show` 命令：

   `vserver security file-directory policy task show -vserver vs1 -policy-name policy1`

   ```
    Vserver: vs1
     Policy: policy1

      Index  File/Folder  Access           Security  NTFS       NTFS
   Security
             Path         Control          Type      Mode       Descriptor
   Name
      -----  -----------  ---------------  --------  ----------
   ---------------
      1      /datavol1    slag             ntfs      propagate  sd1
   ```

10. 使用应用存储级别访问防护安全策略 `vserver security file-directory apply` 命令：

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

    已计划应用安全策略的作业。

11. 使用验证应用的存储级别访问防护安全设置是否正确 `vserver security file-directory show` 命令：

    在此示例中、命令的输出显示已对NTFS卷应用存储级别访问防护安全性 `/datavol1`。即使默认 DACL 允

许对所有人进行完全控制，存储级别访问防护安全性也会限制（和审核）对存储级别访问防护设置中定义的组的访问。

```
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:0x8004
                          Owner:BUILTIN\Administrators
                          Group:BUILTIN\Administrators
                          DACL - ACEs
                            ALLOW-Everyone-0x1f01ff
                            ALLOW-Everyone-0x10000000-OI|CI|IO


                          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
```

相关信息

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

用于配置存储级别访问防护的工作流

显示有关存储级别访问防护的信息

正在删除存储级别访问防护

有效的 SLAG 列表

您可以在卷或 qtree 上配置 SLAG ，也可以同时在这两者上配置 SLAG 。SLAG 列表定义了在表中列出的各种情形下适用的 SLAG 配置所在的卷或 qtree 。

	AFS 中的卷 **SLAG**	**Snapshot** 副本中的卷 **SLAG**	**AFS** 中的 **qtree SLAG**	**Snapshot** 副本中的 **qtree SLAG**
访问文件系统（AFS）中的卷访问	是的。	否	不适用	不适用
Snapshot 副本中的卷访问	是的。	否	不适用	不适用
AFS 中的 qtree 访问（当 qtree 中存在 SLAG 时）	否	否	是的。	否
AFS 中的 qtree 访问（当 qtree 中不存在 SLAG 时）	是的。	否	否	否
Snapshot 副本中的 qtree 访问（当 qtree AFS 中存在 SLAG 时）	否	否	是的。	否
Snapshot 副本中的 qtree 访问（当 qtree AFS 中不存在 SLAG 时）	是的。	否	否	否

显示有关存储级别访问防护的信息

存储级别访问防护是应用于卷或 qtree 的第三层安全保护。无法使用 Windows 属性窗口查看存储级别访问防护设置。您必须使用 ONTAP 命令行界面查看有关存储级别访问防护安全性的信息，您可以使用这些信息验证配置或对文件访问问题进行故障排除。

关于此任务

您必须提供 Storage Virtual Machine （SVM）的名称以及要显示其存储级别访问防护安全信息的卷或 qtree 的路径。您可以摘要形式或详细列表形式显示输出。

步骤

1. 使用所需的详细信息级别显示存储级别访问防护安全设置：

要显示信息的项	输入以下命令 ...
摘要形式	`vserver security file-directory show -vserver vserver_name -path path`
扩展了详细信息	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

示例

以下示例显示路径为的NTFS安全模式卷的存储级别访问防护安全信息 `/datavol1` 在SVM VS1中：

```
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:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         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
```

以下示例显示路径中混合安全模式卷的存储级别访问防护信息 `/datavol5` 在SVM VS1中。此卷的顶层具有UNIX 有效安全性。此卷具有存储级别访问防护安全性。

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: 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
```

删除存储级别访问防护

如果您不再需要在存储级别设置访问安全性，则可以删除卷或 qtree 上的存储级别访问防护。删除存储级别访问防护不会修改或删除常规 NTFS 文件和目录安全性。

步骤

1. 使用验证卷或qtree是否已配置存储级别访问防护 `vserver security file-directory show` 命令：

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                 Vserver: vs1
               File Path: /datavol2
      File Inode Number: 99
         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:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

                         Storage-Level Access Guard security
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

2. 使用删除存储级别访问防护 `vserver security file-directory remove-slag` 命令：

   ```
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. 使用验证是否已从卷或qtree中删除存储级别访问防护 `vserver security file-directory show` 命令：

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         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:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```