使用 SMB 管理文件访问

ONTAP 9

NetApp
September 12, 2024

目录

使用 SMB 管理文件访问

使用本地用户和组进行身份验证和授权

ONTAP 如何使用本地用户和组

本地用户和组概念

在确定是否在环境中配置和使用本地用户和组之前，您应了解什么是本地用户和组以及有关它们的一些基本信息。

- * 本地用户 *

  具有唯一安全标识符（ SID ）的用户帐户，仅在创建该帐户的 Storage Virtual Machine （ SVM ）上可见。本地用户帐户具有一组属性，包括用户名和 SID 。本地用户帐户使用 NTLM 身份验证在 CIFS 服务器上进行本地身份验证。

  用户帐户有多种用途：

  - 用于向用户授予 *User Rights Management* 权限。
  - 用于控制对 SVM 所拥有的文件和文件夹资源的共享级和文件级访问。

- * 本地组 *

  具有唯一 SID 的组只能在其创建所在的 SVM 上显示。组包含一组成员。成员可以是本地用户，域用户，域组和域计算机帐户。可以创建，修改或删除组。

  组有多种用途：

  - 用于向其成员授予 *User Rights Management* 权限。
  - 用于控制对 SVM 所拥有的文件和文件夹资源的共享级和文件级访问。

- * 本地域 *

  具有本地作用域的域，该域受 SVM 的限制。本地域的名称是 CIFS 服务器名称。本地用户和组包含在本地域中。

- * 安全标识符（ SID ） *

  SID 是一个可变长度的数值，用于标识 Windows 模式的安全主体。例如，典型的 SID 采用以下形式： S-1-5-21-3139654847-1303905135-2517279418-123456 。

- * NTLM 身份验证 *

  一种 Microsoft Windows 安全方法，用于对 CIFS 服务器上的用户进行身份验证。

- * 集群复制数据库（ RDB ） *

  一个复制的数据库，其中集群中的每个节点上都有一个实例。本地用户和组对象存储在 RDB 中。

创建本地用户和本地组的原因

在 Storage Virtual Machine （ SVM ）上创建本地用户和本地组的原因有多种。例如，如果域控制器（ DC ）不可用，您可能希望使用本地组分配权限或 SMB 服务器位于工作组中，则可以使用本地用户帐户访问 SMB 服务器。

您可以出于以下原因创建一个或多个本地用户帐户：

- SMB 服务器位于工作组中，域用户不可用。

  在工作组配置中需要本地用户。

- 您希望在域控制器不可用时能够进行身份验证并登录到 SMB 服务器。

  当域控制器关闭或网络问题导致 SMB 服务器无法联系域控制器时，本地用户可以使用 NTLM 身份验证向 SMB 服务器进行身份验证。

- 您希望将 *User Rights Management* 权限分配给本地用户。

  User Rights Management 是 SMB 服务器管理员控制用户和组对 SVM 拥有的权限的能力。您可以通过为用户的帐户分配权限或使用户成为具有这些权限的本地组的成员来为用户分配权限。

您可以出于以下原因创建一个或多个本地组：

- SMB 服务器位于工作组中，并且域组不可用。

  工作组配置不需要本地组，但它们对于管理本地工作组用户的访问权限非常有用。

- 您希望通过使用本地组进行共享和文件访问控制来控制对文件和文件夹资源的访问。
- 您希望使用自定义的 *User Rights Management* 权限创建本地组。

  某些内置用户组具有预定义的权限。要分配一组自定义权限，您可以创建一个本地组并为该组分配必要的权限。然后，您可以将本地用户，域用户和域组添加到本地组。

相关信息

本地用户身份验证的工作原理

支持的权限列表

本地用户身份验证的工作原理

本地用户必须先创建经过身份验证的会话，然后才能访问 CIFS 服务器上的数据。

由于 SMB 基于会话，因此首次设置会话时，只需确定一次用户身份即可。CIFS 服务器在对本地用户进行身份验证时使用基于 NTLM 的身份验证。支持 NTLMv1 和 NTLMv2 。

ONTAP 在三种使用情形下使用本地身份验证。每个用例取决于用户名的域部分（采用 domain\user 格式）是否与 CIFS 服务器的本地域名（ CIFS 服务器名称）匹配：

- 域部分匹配

请求访问数据时提供本地用户凭据的用户将在 CIFS 服务器上进行本地身份验证。

- 域部分不匹配

  ONTAP 尝试对 CIFS 服务器所属域中的域控制器使用 NTLM 身份验证。如果身份验证成功，则登录完成。如果失败，接下来会发生什么情况取决于身份验证失败的原因。

  例如，如果用户位于 Active Directory 中，但密码无效或已过期，则 ONTAP 不会尝试使用 CIFS 服务器上的相应本地用户帐户。相反，身份验证将失败。在其他情况下， ONTAP 会使用 CIFS 服务器上的相应本地帐户（如果存在）进行身份验证，即使 NetBIOS 域名不匹配也是如此。例如，如果存在匹配的域帐户，但该帐户已禁用，则 ONTAP 会使用 CIFS 服务器上的相应本地帐户进行身份验证。

- 未指定域部分

  ONTAP 首先尝试以本地用户身份进行身份验证。如果以本地用户身份进行身份验证失败，则 ONTAP 会使用 CIFS 服务器所属域中的域控制器对用户进行身份验证。

成功完成本地或域用户身份验证后， ONTAP 将根据本地组成员资格和权限构建完整的用户访问令牌。

有关本地用户的 NTLM 身份验证的详细信息，请参见 Microsoft Windows 文档。

相关信息

启用或禁用本地用户身份验证

如何构建用户访问令牌

当用户映射共享时，将建立经过身份验证的 SMB 会话，并构建用户访问令牌，其中包含有关用户，用户的组成员资格和累积权限以及映射的 UNIX 用户的信息。

除非禁用此功能，否则本地用户和组信息也会添加到用户访问令牌中。构建访问令牌的方式取决于登录用户是本地用户还是 Active Directory 域用户：

- 本地用户登录

  尽管本地用户可以是不同本地组的成员，但本地组不能是其他本地组的成员。本地用户访问令牌由分配给特定本地用户所属组的所有权限组成。

- 域用户登录

  域用户登录时， ONTAP 会获取一个用户访问令牌，该令牌包含用户所属的所有域组的用户 SID 和 SID 。ONTAP 使用域用户访问令牌与用户域组的本地成员资格（如果有）提供的访问令牌以及分配给域用户或其任何域组成员资格的任何直接权限进行联合。

对于本地和域用户登录，还会为用户访问令牌设置主组 RID 。默认RID `Domain Users` (里德513)。您不能更改默认值。

Windows 到 UNIX 和 UNIX 到 Windows 名称映射过程会对本地帐户和域帐户遵循相同的规则。

> 从 UNIX 用户到本地帐户没有隐含的自动映射。如果需要，必须使用现有名称映射命令指定显式映射规则。

在包含本地组的 **SVM** 上使用 **SnapMirror** 的准则

在包含本地组的 SVM 所拥有的卷上配置 SnapMirror 时，应了解相关准则。

您不能在应用于 SnapMirror 复制到另一个 SVM 的文件，目录或共享的 ACE 中使用本地组。如果您使用 SnapMirror 功能为另一个 SVM 上的卷创建 DR 镜像，并且该卷具有本地组的 ACE ，则 ACE 在该镜像上无效。如果将数据复制到其他 SVM ，则数据会有效地跨越到其他本地域。授予本地用户和组的权限仅在最初创建这些用户和组的 SVM 的范围内有效。

删除 **CIFS** 服务器时本地用户和组会发生什么情况

默认的本地用户和组集是在创建 CIFS 服务器时创建的，它们与托管 CIFS 服务器的 Storage Virtual Machine （ SVM ）相关联。SVM 管理员可以随时创建本地用户和组。您需要了解删除 CIFS 服务器时本地用户和组会发生什么情况。

本地用户和组与 SVM 关联；因此，出于安全考虑，删除 CIFS 服务器时不会删除它们。虽然删除 CIFS 服务器时不会删除本地用户和组，但它们是隐藏的。在 SVM 上重新创建 CIFS 服务器之前，您无法查看或管理本地用户和组。

> CIFS 服务器管理状态不会影响本地用户或组的可见性。

如何对本地用户和组使用 **Microsoft** 管理控制台

您可以从 Microsoft 管理控制台查看有关本地用户和组的信息。使用此版本的 ONTAP ，您无法从 Microsoft 管理控制台为本地用户和组执行其他管理任务。

还原准则

如果您计划将集群还原到不支持本地用户和组的 ONTAP 版本，并且正在使用本地用户和组管理文件访问或用户权限，则必须了解某些注意事项。

- 由于安全原因，在将 ONTAP 还原到不支持本地用户和组功能的版本时，不会删除有关已配置的本地用户，组和权限的信息。
- 还原到 ONTAP 的先前主要版本后， ONTAP 在身份验证和凭据创建期间不会使用本地用户和组。
- 不会从文件和文件夹 ACL 中删除本地用户和组。
- 如果文件访问请求取决于因向本地用户或组授予权限而授予的访问权限，则这些请求将被拒绝。

  要允许访问，您必须重新配置文件权限，以允许基于域对象而不是本地用户和组对象进行访问。

什么是本地权限

支持的权限列表

ONTAP 具有一组预定义的受支持权限。默认情况下，某些预定义的本地组已添加其中一些权限。此外，您还可以从预定义组添加或删除权限，或者创建新的本地用户或组，并向您创建的组或现有域用户和组添加权限。

下表列出了 Storage Virtual Machine （ SVM ）上支持的权限，并列出了已分配权限的 BUILTIN 组：

权限名称	默认安全设置	Description
`SeTcbPrivilege`	无	作为操作系统的一部分
`SeBackupPrivilege`	`BUILTIN\Administrators`，`BUILTIN\Backup Operators`	备份文件和目录，覆盖所有 ACL
`SeRestorePrivilege`	`BUILTIN\Administrators`，`BUILTIN\Backup Operators`	还原文件和目录，覆盖任何 ACL 会将任何有效的用户或组 SID 设置为文件所有者
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	获取文件或其他对象的所有权
`SeSecurityPrivilege`	`BUILTIN\Administrators`	管理审核 其中包括查看、转储和清除安全日志。
`SeChangeNotifyPrivilege`	`BUILTIN\Administrators`，`BUILTIN\Backup Operators`，`BUILTIN\Power Users`，`BUILTIN\Users`， `Everyone`	绕过遍历检查 具有此权限的用户无需具有遍历(x)权限即可遍历文件夹、符号链接或接合。

相关信息

- 分配本地权限
- 配置绕过遍历检查

分配权限

您可以直接为本地用户或域用户分配权限。或者，您也可以将用户分配给已分配权限与这些用户所需功能匹配的本地组。

- 您可以为创建的组分配一组权限。

  然后，将用户添加到具有所需权限的组。

- 您还可以将本地用户和域用户分配给默认权限与要授予这些用户的权限匹配的预定义组。

相关信息

- 向本地或域用户或组添加权限
- 从本地或域用户或组中删除权限
- 重置本地或域用户和组的权限
- 配置绕过遍历检查

使用 **BUILTIN** 组和本地管理员帐户的准则

使用 BUILTIN 组和本地管理员帐户时，应牢记一些特定准则。例如，您可以重命名本地管理员帐户，但不能删除此帐户。

- 管理员帐户可以重命名，但无法删除。
- 无法从 BUILTIN\Administrators 组中删除管理员帐户。
- BUILTIN 组可以重命名，但不能删除。

  重命名 BUILTIN 组后，可以使用已知名称创建另一个本地对象；但是，系统会为该对象分配一个新的 RID 。

- 没有本地来宾帐户。

相关信息

预定义的 BUILTIN 组和默认权限

本地用户密码的要求

默认情况下，本地用户密码必须满足复杂性要求。密码复杂度要求与 Microsoft Windows *local security policy* 中定义的要求类似。

密码必须满足以下条件：

- 长度必须至少为六个字符
- 不得包含用户帐户名称
- 必须包含以下四个类别中至少三个类别的字符：
  - 大写英文字符（A 到 Z）
  - 小写英文字符（a 到 z）
  - 基数为 10 位（0 到 9）
  - 特殊字符：

    ~@ # $ % ｛caret｝ & * _ - + = ` \ | （） [ ] ： ； " < > ， .? /

相关信息

为本地 SMB 用户启用或禁用所需的密码复杂度

显示有关 CIFS 服务器安全设置的信息

更改本地用户帐户密码

预定义的 **BUILTIN** 组和默认权限

您可以将本地用户或域用户的成员资格分配给 ONTAP 提供的一组预定义的 BUILTIN 组。预定义的组已分配预定义的权限。

下表介绍了预定义的组：

预定义的 **BUILTIN** 组	默认权限
`BUILTIN\Administrators`第544次 首次创建时、本地 `Administrator` ID为500的帐户将自动成为此组的成员。Storage Virtual Machine (SVM)加入域后、 `domain\Domain Admins` 将组添加到组中。如果SVM离开域、则 `domain\Domain Admins` 组将从组中删除。	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Power Users`547 首次创建时，此组没有任何成员。此组的成员具有以下特征： • 可以创建和管理本地用户和组。 • 无法将自身或任何其他对象添加到中 `BUILTIN\Administrators` 组。	`SeChangeNotifyPrivilege`
`BUILTIN\Backup Operators`第551号 首次创建时，此组没有任何成员。如果出于备份目的打开文件或文件夹，则此组的成员可以覆盖对这些文件或文件夹的读写权限。	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Users`545 首次创建时、此组没有任何成员(除了隐含的 `Authenticated Users` 特殊组)。当SVM加入域时、 `domain\Domain Users` 已将组添加到此组。如果SVM离开域、则 `domain\Domain Users` 已从此组中删除组。	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 此组包括所有用户，包括来宾（但不包括匿名用户）。这是具有隐含成员资格的隐含组。	`SeChangeNotifyPrivilege`

相关信息

使用 BUILTIN 组和本地管理员帐户的准则

支持的权限列表

配置绕过遍历检查

启用或禁用本地用户和组功能

启用或禁用本地用户和组功能概述

在使用本地用户和组访问 NTFS 安全模式数据之前，必须启用本地用户和组功能。此外，如果要使用本地用户进行 SMB 身份验证，则必须启用本地用户身份验证功能。

默认情况下，本地用户和组功能以及本地用户身份验证处于启用状态。如果未启用它们，则必须先启用它们，然后才能配置和使用本地用户和组。您可以随时禁用本地用户和组功能。

除了显式禁用本地用户和组功能之外，如果集群中的任何节点还原到不支持本地用户和组功能的 ONTAP 版本，则 ONTAP 还会禁用此功能。只有当集群中的所有节点都运行支持本地用户和组功能的 ONTAP 版本时，才会启用此功能。

相关信息

修改本地用户帐户

修改本地组

向本地或域用户或组添加权限

启用或禁用本地用户和组

您可以在 Storage Virtual Machine （SVM）上启用或禁用 SMB 访问的本地用户和组。默认情况下，本地用户和组功能处于启用状态。

关于此任务

您可以在配置 SMB 共享和 NTFS 文件权限时使用本地用户和组，也可以选择在创建 SMB 连接时使用本地用户进行身份验证。要使用本地用户进行身份验证，还必须启用本地用户和组身份验证选项。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 执行以下操作之一：

希望本地用户和组 ...	输入命令 ...
enabled	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled true`
已禁用	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-users-and -groups-enabled false`

3. 返回到管理权限级别： `set -privilege admin`

示例

以下示例将在 SVM vs1 上启用本地用户和组功能：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

相关信息

启用或禁用本地用户身份验证

启用或禁用本地用户帐户

启用或禁用本地用户身份验证

您可以为 Storage Virtual Machine （SVM）上的 SMB 访问启用或禁用本地用户身份验证。默认设置为允许本地用户身份验证，当 SVM 无法联系域控制器或您选择不使用域级别访问控制时，此功能非常有用。

开始之前

必须在 CIFS 服务器上启用本地用户和组功能。

关于此任务

您可以随时启用或禁用本地用户身份验证。如果要在创建 SMB 连接时使用本地用户进行身份验证，则还必须启用 CIFS 服务器的本地用户和组选项。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 执行以下操作之一：

本地身份验证的目标位置	输入命令 ...
enabled	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled true`
已禁用	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled false`

3. 返回到管理权限级别： `set -privilege admin`

示例

以下示例将在 SVM vs1 上启用本地用户身份验证：

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

相关信息

本地用户身份验证的工作原理

启用或禁用本地用户和组

管理本地用户帐户

修改本地用户帐户

如果要更改现有用户的全名或问题描述，以及要启用或禁用用户帐户，则可以修改本地用户帐户。如果用户的名称受到影响或出于管理目的需要更改名称，您也可以重命名本地用户帐户。

如果您要 ...	输入命令 ...
修改本地用户的全名	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user -name` *`user_name`* `-full-name text` 如果全名包含空格、则必须使用双引号将其括起来。
修改本地用户的问题描述	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user -name` *`user_name`* `-description text` 如果问题描述包含空格、则必须使用双引号将其括起来。
启用或禁用本地用户帐户	`vserver cifs users-and-groups local-user modify -vserver *vserver_name* -user-name *user_name* -is -account-disabled {true
false}`	重命名本地用户帐户

示例

以下示例将 Storage Virtual Machine （ SVM ，以前称为 Vserver） vs1 上的本地用户 "`CIFS_SERVER\sue` " 重命名为 "`CIFS_SERVER\sue_new` "：

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

启用或禁用本地用户帐户

如果您希望用户能够通过 SMB 连接访问 Storage Virtual Machine （ SVM ）中包含的数据，则可以启用本地用户帐户。如果您不希望本地用户帐户通过 SMB 访问 SVM 数据，也可以禁用该用户帐户。

关于此任务

您可以通过修改用户帐户来启用本地用户。

步骤

1. 执行相应的操作：

如果您要 ...	输入命令 ...
启用用户帐户	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account -disabled false`
禁用用户帐户	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-is-account -disabled true`

更改本地用户帐户密码

您可以更改本地用户的帐户密码。如果用户的密码受到影响或用户忘记了密码，则此功能非常有用。

步骤

1. 通过执行相应的操作更改密码： `vserver cifs users-and-groups local-user set-password -vserver` *`vserver_name`* `-user-name` *`user_name`*

示例

以下示例将为与 Storage Virtual Machine （ SVM ，以前称为 Vserver） vs1 关联的本地用户 "`CIFS_SERVER\sue` " 设置密码：

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

相关信息

为本地 SMB 用户启用或禁用所需的密码复杂度

显示有关 CIFS 服务器安全设置的信息

显示有关本地用户的信息

您可以通过摘要形式显示所有本地用户的列表。如果要确定为特定用户配置了哪些帐户设置，则可以显示该用户的详细帐户信息以及多个用户的帐户信息。此信息可帮助您确定是否需要修改用户的设置，以及对身份验证或文件访问问题进行故障排除。

关于此任务

不会显示有关用户密码的信息。

步骤

1. 执行以下操作之一：

如果您要 ...	输入命令 ...
显示有关 Storage Virtual Machine （ SVM ）上所有用户的信息	`vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
显示用户的详细帐户信息	`vserver cifs users-and-groups local-user show -instance -vserver` *`vserver_name`* `-user-name` *`user_name`*

运行命令时，您还可以选择其他可选参数。有关详细信息，请参见手册页。

示例

以下示例显示了有关 SVM vs1 上所有本地用户的信息：

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name     Description
-------- ---------------------------- ------------- -------------
vs1      CIFS_SERVER\Administrator    James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue              Sue   Jones
```

显示有关本地用户的组成员资格的信息

您可以显示有关本地用户所属的本地组的信息。您可以使用此信息来确定用户对文件和文件夹应具有的访问权限。此信息有助于确定用户应拥有哪些文件和文件夹访问权限，或者解决文件访问问题。

关于此任务

您可以自定义命令，使其仅显示要查看的信息。

步骤

1. 执行以下操作之一：

如果您要 ...	输入命令 ...
显示指定本地用户的本地用户成员资格信息	`vserver cifs users-and-groups local-user show-membership -user-name` *`user_name`*
显示此本地用户所属本地组的本地用户成员资格信息	`vserver cifs users-and-groups local-user show-membership -membership` *`group_name`*
显示与指定 Storage Virtual Machine （ SVM ）关联的本地用户的用户成员资格信息	`vserver cifs users-and-groups local-user show-membership -vserver` *`vserver_name`*
显示指定 SVM 上所有本地用户的详细信息	`vserver cifs users-and-groups local-user show-membership -instance -vserver` *`vserver_name`*

示例

以下示例显示 SVM vs1 上所有本地用户的成员资格信息；用户 "`CIFS_SERVER\Administrator` " 是 "`BUILTIN\Administrators` " 组的成员， "`CIFS_SERVER\sue` " 是 "`CIFS_SERVER\G1` " 组的成员：

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                     Membership
---------- ----------------------------- ------------------------
vs1        CIFS_SERVER\Administrator     BUILTIN\Administrators
           CIFS_SERVER\sue               CIFS_SERVER\g1
```

删除本地用户帐户

如果不再需要本地用户帐户对 CIFS 服务器进行本地 SMB 身份验证或确定对 SVM 中数据的访问权限，则可以从 Storage Virtual Machine （ SVM ）中删除这些帐户。

关于此任务

删除本地用户时，请记住以下几点：

- 文件系统未更改。

  不会调整引用此用户的文件和目录上的 Windows 安全描述符。

- 所有对本地用户的引用都将从成员资格和权限数据库中删除。
- 无法删除众所周知的标准用户，例如管理员。

步骤

1. 确定要删除的本地用户帐户的名称： `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*
2. 删除本地用户： `vserver cifs users-and-groups local-user delete -vserver` *`vserver_name`* `-user-name` *`username_name`*
3. 验证是否已删除此用户帐户： `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

示例

以下示例将删除与 SVM vs1 关联的本地用户 "`CIFS_SERVER\sue` "：

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue             Sue   Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                   Full Name      Description
-------- --------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator   James Smith    Built-in administrator
account
```

管理本地组

修改本地组

您可以通过更改现有本地组的问题描述或重命名组来修改现有本地组。

如果您要 ...	使用命令 ...
修改本地组问题描述	`vserver cifs users-and-groups local-group modify -vserver` *`vserver_name`* `-group-name` *`group_name`* `-description` `text` 如果问题描述包含空格、则必须使用双引号将其括起来。
重命名本地组	`vserver cifs users-and-groups local-group rename -vserver` *`vserver_name`* `-group-name` *`group_name`* `-new-group-name` *`new_group_name`*

示例

以下示例将本地组 "`CIFS_SERVER\engineering` " 重命名为 "`CIFS_SERVER\engineering_new` "：

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

以下示例修改本地组 "`CIFS_SERVER\engineering` " 的问题描述：

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

显示有关本地组的信息

您可以显示在集群或指定 Storage Virtual Machine （ SVM ）上配置的所有本地组的列表。在对 SVM 上所含数据的文件访问问题或 SVM 上的用户权限（特权）问题进行故障排除时，此信息非常有用。

步骤

1. 执行以下操作之一：

所需信息	输入命令 ...
集群上的所有本地组	`vserver cifs users-and-groups local-group show`
SVM 上的所有本地组	`vserver cifs users-and-groups local-group show -vserver` *`vserver_name`*

运行此命令时，您还可以选择其他可选参数。有关详细信息，请参见手册页。

示例

以下示例显示了有关 SVM vs1 上所有本地组的信息：

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                   Description
-------- ---------------------------- ----------------------------
vs1      BUILTIN\Administrators       Built-in Administrators group
vs1      BUILTIN\Backup Operators     Backup Operators group
vs1      BUILTIN\Power Users          Restricted administrative privileges
vs1      BUILTIN\Users                All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

管理本地组成员资格

您可以通过添加和删除本地或域用户，或者添加和删除域组来管理本地组成员资格。如果您希望根据放置在组上的访问控制来控制对数据的访问，或者您希望用户拥有与该组关联的权限，则此功能非常有用。

关于此任务

向本地组添加成员的准则：

- 您不能将用户添加到特殊的 _Everyone 组。
- 本地组必须存在，然后才能向其中添加用户。
- 用户必须存在，然后才能将其添加到本地组。
- 您不能将本地组添加到其他本地组。
- 要将域用户或组添加到本地组， Data ONTAP 必须能够将此名称解析为 SID 。

从本地组中删除成员的准则：

- 您不能从特殊的 _Everyone _ 组中删除成员。
- 要从中删除成员的组必须存在。
- ONTAP 必须能够将要从组中删除的成员的名称解析为相应的 SID 。

步骤

1. 添加或删除组中的成员。

如果您要 ...	然后使用命令 ...
将成员添加到组	`vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` 您可以指定要添加到指定本地组的本地用户，域用户或域组的逗号分隔列表。
从组中删除成员	`vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` 您可以指定要从指定本地组中删除的本地用户，域用户或域组的逗号分隔列表。

以下示例将本地用户 `SMB_SERVER\sue` 和域组`AD_DOM\DOM_eng` 添加到 SVM vs1 上的本地组 `SMB_SERVER\engineering` 中：

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

以下示例将从 SVM vs1 上的本地组 `SMB_SERVER\engineering` 中删除本地用户 `SMB_SERVER\sue` 和 `SMB_SERVER\James`：

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

相关信息

显示有关本地组成员的信息

显示有关本地组成员的信息

您可以显示在集群或指定 Storage Virtual Machine （SVM）上配置的本地组的所有成员的列表。在对文件访问问题或用户权限（权限）问题进行故障排除时，此信息非常有用。

步骤

1. 执行以下操作之一：

要显示的信息	输入命令 ...
集群上所有本地组的成员	`vserver cifs users-and-groups local-group show-members`

要显示的信息	输入命令 ...
SVM 上所有本地组的成员	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

示例

以下示例显示了有关 SVM vs1 上所有本地组的成员的信息：

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- ----------------------------- ------------------------
vs1       BUILTIN\Administrators        CIFS_SERVER\Administrator
                                        AD_DOMAIN\Domain Admins
                                        AD_DOMAIN\dom_grp1
          BUILTIN\Users                 AD_DOMAIN\Domain Users
                                        AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering       CIFS_SERVER\james
```

删除本地组

如果不再需要本地组来确定与该 SVM 关联的数据的访问权限，或者不再需要将 SVM 用户权限（特权）分配给组成员，则可以从 Storage Virtual Machine （ SVM ）中删除该本地组。

关于此任务

删除本地组时，请记住以下几点：

- 文件系统未更改。

  不会调整引用此组的文件和目录上的 Windows 安全描述符。

- 如果该组不存在，则会返回错误。
- 不能删除特殊的 _Everyone 组。
- 无法删除 *BUILTIN\Administrators _ _BUILTIN\Users* 等内置组。

步骤

1. 通过显示SVM上的本地组列表来确定要删除的本地组的名称： `vserver cifs users-and-groups local-group show -vserver vserver_name`
2. 删除本地组： `vserver cifs users-and-groups local-group delete -vserver` *`vserver_name`* `-group-name` *`group_name`*
3. 验证是否已删除此组： `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

示例

以下示例将删除与 SVM vs1 关联的本地组 "`CIFS_SERVER\sales` "：

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ----------------------------- -----------------------------
vs1       BUILTIN\Administrators        Built-in Administrators group
vs1       BUILTIN\Backup Operators      Backup Operators group
vs1       BUILTIN\Power Users           Restricted administrative
privileges
vs1       BUILTIN\Users                 All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- ----------------------------- -----------------------------
vs1       BUILTIN\Administrators        Built-in Administrators group
vs1       BUILTIN\Backup Operators      Backup Operators group
vs1       BUILTIN\Power Users           Restricted administrative
privileges
vs1       BUILTIN\Users                 All users
vs1       CIFS_SERVER\engineering
```

更新本地数据库中的域用户和组名称

您可以将域用户和组添加到 CIFS 服务器的本地组。这些域对象会注册到集群上的本地数据库中。如果重命名域对象，则必须手动更新本地数据库。

关于此任务

您必须指定要更新域名的 Storage Virtual Machine （ SVM ）的名称。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 执行相应的操作：

要更新域用户和组以及 ...	使用此命令 ...
显示成功更新和无法更新的域用户和组	`vserver cifs users-and-groups update-names -vserver` *`vserver_name`*

要更新域用户和组以及 ...	使用此命令 ...
显示已成功更新的域用户和组	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only false`
仅显示无法更新的域用户和组	`vserver cifs users-and-groups update-names -vserver vserver_name -display -failed-only true`
禁止有关更新的所有状态信息	`vserver cifs users-and-groups update-names -vserver vserver_name -suppress -all-output true`

3. 返回到管理权限级别： `set -privilege admin`

示例

以下示例将更新与 Storage Virtual Machine （ SVM ，以前称为 Vserver） vs1 关联的域用户和组的名称。对于上次更新，需要更新一组依赖名称：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin
```

管理本地权限

向本地或域用户或组添加权限

您可以通过添加权限来管理本地或域用户或组的用户权限。添加的权限将覆盖分配给其中任何对象的默认权限。这样可以自定义用户或组的权限，从而增强安全性。

开始之前

要添加权限的本地或域用户或组必须已存在。

关于此任务

向对象添加权限将覆盖该用户或组的默认权限。添加权限不会删除先前添加的权限。

在向本地或域用户或组添加权限时，必须牢记以下几点：

- 您可以添加一个或多个权限。
- 在向域用户或组添加权限时， ONTAP 可能会通过联系域控制器来验证域用户或组。

  如果 ONTAP 无法与域控制器联系，则命令可能会失败。

步骤

1. 向本地或域用户或组添加一个或多个权限： `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. 验证所需权限是否已应用于对象： `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

示例

以下示例将特权 `SeTcbPrivilege` 和 `SeTakeOwnershipPrivilege` 添加到 Storage Virtual Machine （ SVM ，以前称为 Vserver ） vs1 上的用户 "`CIFS_SERVER\sue` " 中：

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege
```

从本地或域用户或组中删除权限

您可以通过删除权限来管理本地或域用户或组的用户权限。这样可以自定义用户和组的最大权限，从而增强安全性。

开始之前

要从中删除权限的本地或域用户或组必须已存在。

关于此任务

从本地或域用户或组删除权限时，必须牢记以下几点：

- 您可以删除一个或多个权限。
- 从域用户或组中删除权限时， ONTAP 可能会通过联系域控制器来验证域用户或组。

  如果 ONTAP 无法与域控制器联系，则命令可能会失败。

步骤

1. 从本地或域用户或组中删除一个或多个权限： `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. 验证是否已从对象中删除所需权限： `vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *name*`

示例

以下示例将从 Storage Virtual Machine （ SVM ，以前称为 Vserver ） vs1 上的用户 "`cifs_server\sue` " 中删除特权 `SeTcbPrivilege` 和 `SeTakeOwnershipPrivilege`：

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- -------------------
vs1       CIFS_SERVER\sue       -
```

重置本地或域用户和组的权限

您可以重置本地或域用户和组的权限。如果您已修改本地或域用户或组的权限，并且不再需要或需要这些修改，则此功能将非常有用。

关于此任务

重置本地或域用户或组的权限会删除该对象的任何权限条目。

步骤

1. 重置本地或域用户或组的权限： `vserver cifs users-and-groups privilege reset-privilege -vserver *vserver_name* -user-or-group-name *name*`

2. 验证是否已对此对象重置权限： `vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *name*`

示例

以下示例将重置 Storage Virtual Machine （ SVM ，以前称为 Vserver） vs1 上用户 "`CIFS_SERVER\sue` " 的权限。默认情况下，普通用户没有与其帐户关联的权限：

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

以下示例将重置组 "`BUILTIN\Administrators` " 的权限，从而有效地删除权限条目：

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ------------------------ -------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

显示有关权限覆盖的信息

您可以显示有关分配给域或本地用户帐户或组的自定义权限的信息。此信息有助于确定是否应用了所需的用户权限。

步骤

1. 执行以下操作之一：

要显示的信息	输入此命令 ...
Storage Virtual Machine （SVM）上所有域和本地用户及组的自定义权限	`vserver cifs users-and-groups privilege show -vserver vserver_name`
SVM 上特定域或本地用户和组的自定义权限	`vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

运行此命令时，您还可以选择其他可选参数。有关详细信息，请参见手册页。

示例

以下命令显示与 SVM vs1 的本地或域用户和组明确关联的所有权限：

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
--------- ---------------------   ---------------
vs1       BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                  SeRestorePrivilege
vs1       CIFS_SERVER\sue         SeTcbPrivilege
                                  SeTakeOwnershipPrivilege
```

配置绕过遍历检查

配置绕过遍历检查概述

绕过遍历检查是一种用户权限（也称为 _privilege _），用于确定用户是否可以遍历路径中的所有目录以访问某个文件，即使用户对遍历的目录没有权限也是如此。您应了解允许或禁止绕过遍历检查时会发生什么情况，以及如何为 Storage Virtual Machine （SVM）上的用户配置绕过遍历检查。

允许或禁止绕过遍历检查时会发生什么情况

- 如果允许，当用户尝试访问某个文件时， ONTAP 在确定是授予还是拒绝访问该文件时不会检查中间目录的遍历权限。
- 如果不允许， ONTAP 将检查文件路径中所有目录的遍历（执行）权限。

  如果任何中间目录不具有 "`X` "（遍历权限），则 ONTAP 将拒绝访问此文件。

配置绕过遍历检查

您可以使用 ONTAP 命令行界面或使用此用户权限配置 Active Directory 组策略来配置绕过遍历检查。

。 `SeChangeNotifyPrivilege` 权限控制是否允许用户绕过遍历检查。

- 通过将其添加到 SVM 上的本地 SMB 用户或组或域用户或组，可以绕过遍历检查。
- 从 SVM 上的本地 SMB 用户或组或域用户或组中删除该文件将禁止绕过遍历检查。

默认情况下， SVM 上的以下 BUILTIN 组有权绕过遍历检查：

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`
- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

如果您不希望允许其中一个组的成员绕过遍历检查，则必须从该组中删除此权限。

在使用命令行界面为 SVM 上的本地 SMB 用户和组配置绕过遍历检查时，必须牢记以下几点：

- 如果要允许自定义本地或域组的成员绕过遍历检查、则必须添加 `SeChangeNotifyPrivilege` 权限。
- 如果要允许单个本地或域用户绕过遍历检查、而该用户不是具有该权限的组的成员、则可以添加 `SeChangeNotifyPrivilege` 权限。
- 您可以通过删除来禁用本地或域用户或组绕过遍历检查 `SeChangeNotifyPrivilege` 随时享受特权。

> 要为指定的本地或域用户或组禁用绕过访问程序检查、还必须删除 `SeChangeNotifyPrivilege` 特权 `Everyone` 组。

相关信息

允许用户或组绕过目录遍历检查

禁止用户或组绕过目录遍历检查

在卷上配置用于 SMB 文件名转换的字符映射

创建 SMB 共享访问控制列表

使用存储级别访问防护确保文件访问安全

支持的权限列表

向本地或域用户或组添加权限

允许用户或组绕过目录遍历检查

如果您希望用户能够遍历路径中的所有目录以查找某个文件、即使该用户对遍历的目录没有权限、则可以添加 `SeChangeNotifyPrivilege` Storage Virtual Machine (SVM)上的本地SMB用户或组的权限。默认情况下，用户可以绕过目录遍历检查。

开始之前

- SVM上必须存在SMB服务器。

- 必须启用本地用户和组SMB服务器选项。
- 要使用的本地或域用户或组 `SeChangeNotifyPrivilege` 要添加的权限必须已存在。

关于此任务

在向域用户或组添加权限时， ONTAP 可能会通过联系域控制器来验证域用户或组。如果 ONTAP 无法与域控制器联系，则此命令可能会失败。

步骤

1. 通过添加启用绕过遍历检查 `SeChangeNotifyPrivilege` 本地或域用户或组的权限： `vserver cifs users-and-groups privilege add-privilege -vserver` *`vserver_name`* `-user-or-group -name` *`name`* `-privileges SeChangeNotifyPrivilege`

   的值 `-user-or-group-name` 参数是本地用户或组、或者域用户或组。

2. 验证指定的用户或组是否已启用绕过遍历检查： `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

示例

以下命令可使属于"`explexe\eng`"组的用户通过添加来绕过目录遍历检查 `SeChangeNotifyPrivilege` 组权限：

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege
```

相关信息

禁止用户或组绕过目录遍历检查

禁止用户或组绕过目录遍历检查

如果您不希望用户遍历路径中的所有目录以访问某个文件、因为该用户对遍历的目录没有权限、则可以删除 `SeChangeNotifyPrivilege` Storage Virtual Machine (SVM)上的本地SMB用户或组的权限。

开始之前

要从中删除权限的本地或域用户或组必须已存在。

关于此任务

从域用户或组中删除权限时， ONTAP 可能会通过联系域控制器来验证域用户或组。如果 ONTAP 无法与域控制器联系，则此命令可能会失败。

步骤

1. 禁止绕过遍历检查： `vserver cifs users-and-groups privilege remove-privilege -vserver *vserver_name* -user-or-group-name *name* -privileges SeChangeNotifyPrivilege`

   此命令将删除 `SeChangeNotifyPrivilege` 使用的值指定的本地或域用户或组的权限 `-user-or-group-name *name*` 参数。

2. 验证指定的用户或组是否已禁用绕过遍历检查： `vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *name*`

示例

以下命令禁止属于 "`example\eng` " 组的用户绕过目录遍历检查：

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ------------------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ------------------------
vs1       EXAMPLE\eng           -
```

相关信息

允许用户或组绕过目录遍历检查

显示有关文件安全性和审核策略的信息

显示有关文件安全性和审核策略概述的信息

您可以显示 Storage Virtual Machine （ SVM ）上卷中包含的文件和目录的文件安全信息。您可以显示有关 FlexVol 卷上审核策略的信息。如果已配置，则可以显示有关 FlexVol 卷上存储级别访问防护和动态访问控制安全设置的信息。

显示有关文件安全性的信息

您可以使用以下安全模式显示应用于卷和 qtree （对于 FlexVol 卷）中数据的文件安全性信息：

- NTFS
- "unix"
- 混合

显示有关审核策略的信息

您可以通过以下 NAS 协议显示有关审核 FlexVol 卷上访问事件的审核策略的信息：

- SMB （所有版本）
- NFSv4.x

显示有关存储级别访问防护（ **SLAG** ）安全性的信息

可以使用以下安全模式对 FlexVol 卷和 qtree 对象应用存储级别访问防护安全性：

- NTFS
- 混合
- UNIX （如果在包含此卷的 SVM 上配置了 CIFS 服务器）

显示有关动态访问控制（ **DAC** ）安全性的信息

可以使用以下安全模式对 FlexVol 卷中的对象应用动态访问控制安全性：

- NTFS
- 混合（如果对象具有 NTFS 有效安全性）

相关信息

使用存储级别访问防护保护文件访问安全

显示有关存储级别访问防护的信息

显示 **NTFS** 安全模式卷上的文件安全性信息

您可以显示 NTFS 安全模式卷上的文件和目录安全性信息，包括安全模式和有效安全模式是什么，应用了哪些权限以及有关 DOS 属性的信息。您可以使用结果验证安全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文件或文件夹安全信息的数据的路径。您可以摘要形式或详细列表形式显示输出。

- 由于 NTFS 安全模式卷和 qtree 在确定文件访问权限时仅使用 NTFS 文件权限以及 Windows 用户和组，因此与 UNIX 相关的输出字段包含仅显示的 UNIX 文件权限信息。
- 对于采用 NTFS 安全模式的文件和文件夹，将显示 ACL 输出。
- 由于可以在卷根或 qtree 上配置存储级别访问防护安全性，因此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 ACL 和存储级别访问防护 ACL 。
- 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。

步骤

1. 使用所需的详细信息级别显示文件和目录安全设置：

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

以下示例显示路径的安全信息 `/vol4` 在SVM VS1中：

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                 Vserver: vs1
                               File Path: /vol4
                       File Inode Number: 64
                          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
```

以下示例显示了路径的安全信息以及展开的掩码 `/data/engineering` 在SVM VS1中：

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

以下示例显示路径为的卷的安全信息、包括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
```

相关信息

显示混合安全模式卷上的文件安全性信息

显示 UNIX 安全模式卷上的文件安全性信息

显示混合安全模式卷上的文件安全性信息

您可以显示混合安全模式卷上的文件和目录安全性信息，包括安全模式和有效安全模式是什么，应用了哪些权限以及有关 UNIX 所有者和组的信息。您可以使用结果验证安全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文件或文件夹安全信息的数据的路径。您可以摘要形式或详细列表形式显示输出。

- 混合安全模式卷和 qtree 可以包含一些使用 UNIX 文件权限的文件和文件夹，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。
- 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 ）的文件和目录，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。
- 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 UNIX 文件权限和存储级别访问防护 ACL 。
- 如果在命令中输入的路径指向具有 NTFS 有效安全性的数据，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。

步骤

1. 使用所需的详细信息级别显示文件和目录安全设置：

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

以下示例显示路径的安全信息 `/projects` 在SVM VS1中、以扩展掩码形式显示。此混合安全模式路径具有 UNIX 有效安全性。

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

                Vserver: vs1
              File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         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: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

以下示例显示路径的安全信息 `/data` 在SVM VS1中。此混合安全模式路径具有 NTFS 有效安全性。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                                 Vserver: vs1
                               File Path: /data
                       File Inode Number: 544
                          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:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                            ALLOW-Everyone-0x1f01ff
                                            ALLOW-Everyone-0x10000000-
OI|CI|IO
```

以下示例显示路径上卷的安全信息 `/datavol5` 在SVM VS1中。此混合安全模式卷的顶层具有 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
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

相关信息

显示NTFS安全模式卷上的文件安全性信息

显示 UNIX 安全模式卷上的文件安全性信息

显示有关 **UNIX** 安全模式卷上的文件安全性的信息

您可以显示 UNIX 安全模式卷上的文件和目录安全性信息，包括安全模式和有效安全模式是什么，应用了哪些权限以及有关 UNIX 所有者和组的信息。您可以使用结果验证安全配

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文件或目录安全信息的数据的路径。您可以摘要形式或详细列表形式显示输出。

- 在确定文件访问权限时， UNIX 安全模式卷和 qtree 仅使用 UNIX 文件权限，模式位或 NFSv4 ACL 。
- 只有具有 NFSv4 安全性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 ）的文件和目录，此字段为空。

- 对于 NFSv4 安全描述符， ACL 输出中的所有者和组输出字段不适用。

  它们仅对 NTFS 安全描述符有意义。

- 由于如果在SVM上配置了CIFS服务器、则UNIX卷或qtree支持存储级别访问防护安全性、因此输出可能包含应用于中指定的卷或qtree的存储级别访问防护安全性的信息 `-path` 参数。

步骤

1. 使用所需的详细信息级别显示文件和目录安全设置：

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

以下示例显示路径的安全信息 `/home` 在SVM VS1中：

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                  Vserver: vs1
                                File Path: /home
                        File Inode Number: 9590
                           Security Style: unix
                          Effective Style: unix
                           DOS Attributes: 10
                   DOS Attributes in Text: ----D---
                  Expanded Dos Attributes: -
                            Unix User Id: 0
                           Unix Group Id: 1
                           Unix Mode Bits: 700
                   Unix Mode Bits in Text: rwx------
                                     ACLs: -
```

以下示例显示路径的安全信息 `/home` 在扩展掩码形式的SVM VS1中：

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                  Vserver: vs1
                                File Path: /home
                        File Inode Number: 9590
                           Security Style: unix
                          Effective Style: unix
                           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: 1
                           Unix Mode Bits: 700
                   Unix Mode Bits in Text: rwx------
                                     ACLs: -
```

相关信息

显示NTFS安全模式卷上的文件安全性信息

显示混合安全模式卷上的文件安全性信息

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。您可以使用结果验证安全配置或对审核问题进行故障排除。

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	`vserver security file-directory show -vserver vserver_name -path path`
作为详细列表	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

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
```

使用命令行界面显示有关 **FlexVol** 卷上 **NFSv4** 审核策略的信息

您可以使用 ONTAP 命令行界面显示有关 FlexVol 卷上 NFSv4 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（ SACL ）的信

息。您可以使用结果验证安全配置或对审核问题进行故障排除。

关于此任务

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

- UNIX 安全模式卷和 qtree 仅对审核策略使用 NFSv4 SACL 。
- 混合安全模式卷中采用 UNIX 安全模式的文件和目录可以应用 NFSv4 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 NFSv4 SACL 。
- 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。
- 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 NFSv4 文件和目录 SACL 以及存储级别访问防护 NTFS SACL 。
- 由于如果在SVM上配置了CIFS服务器、则UNIX卷或qtree支持存储级别访问防护安全性、因此输出可能包含应用于中指定的卷或qtree的存储级别访问防护安全性的信息 `-path` 参数。

步骤

1. 使用所需的详细信息级别显示文件和目录安全设置：

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

以下示例显示路径的安全信息 `/lab` 在SVM VS1中。此 UNIX 安全模式路径具有 NFSv4 SACL 。

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

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

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
```

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

对象	访问类型	访问权限	应用权限的位置
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`

如果您要 ...	使用此命令 ...
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。

为 SMB 共享配置元数据缓存

SMB 元数据缓存的工作原理

通过元数据缓存， SMB 1.0 客户端上的文件属性缓存可以更快地访问文件和文件夹属性。您可以基于每个共享启用或禁用属性缓存。如果启用了元数据缓存，您还可以为缓存条目配置生存时间。如果客户端通过 SMB 2.x 或 SMB 3.0 连接到共享，则无需配置元数据缓存。

启用后， SMB 元数据缓存会将路径和文件属性数据存储一段有限的时间。这样可以提高具有常见工作负载的 SMB 1.0 客户端的 SMB 性能。

对于某些任务， SMB 会创建大量流量，其中可能包括对路径和文件元数据的多个相同查询。您可以改用 SMB 元数据缓存从缓存中提取信息，从而减少冗余查询的数量并提高 SMB 1.0 客户端的性能。

> 元数据缓存虽然不太可能为 SMB 1.0 客户端提供过时的信息。如果您的环境无法承担此风险，则不应启用此功能。

启用 SMB 元数据缓存

您可以通过启用 SMB 元数据缓存来提高 SMB 1.0 客户端的 SMB 性能。默认情况下，SMB 元数据缓存处于禁用状态。

步骤

1. 执行所需的操作：

如果您要 ...	输入命令 ...
创建共享时启用 SMB 元数据缓存	`vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties attributecache`
在现有共享上启用 SMB 元数据缓存	`vserver cifs share properties add -vserver` *`vserver_name`* `-share-name` *`share_name`* `-share-properties attributecache`

相关信息

配置 SMB 元数据缓存条目的生命周期

在现有 SMB 共享上添加或删除共享属性

配置 SMB 元数据缓存条目的生命周期

您可以配置 SMB 元数据缓存条目的生命周期，以优化环境中的 SMB 元数据缓存性能。默认值为10秒。

开始之前

您必须已启用 SMB 元数据缓存功能。如果未启用 SMB 元数据缓存，则不会使用 SMB 缓存 TTL 设置。

步骤

1. 执行所需的操作：

如果要在以下情况下配置 **SMB** 元数据缓存条目的生命周期 ...	输入命令 ...
创建共享	`vserver cifs share -create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-attribute-cache-ttl [integerh][integerm][integers]`
修改现有共享	`vserver cifs share -modify -vserver` *`vserver_name`* `-share-name` *`share_name`* `-attribute-cache-ttl [integerh][integerm][integers]`

您可以在创建或修改共享时指定其他共享配置选项和属性。有关详细信息，请参见手册页。

管理文件锁定

关于协议之间的文件锁定

文件锁定是客户端应用程序用来防止用户访问先前由另一用户打开的文件的方法。ONTAP 锁定文件的方式取决于客户端的协议。

如果客户端是 NFS 客户端，则建议锁定；如果客户端是 SMB 客户端，则必须锁定。

由于 NFS 和 SMB 文件锁定之间的差异， NFS 客户端可能无法访问先前由 SMB 应用程序打开的文件。

当 NFS 客户端尝试访问 SMB 应用程序锁定的文件时，会发生以下情况：

- 在混合卷或NTFS卷中、文件操作(如) `rm`， `rmdir`，和 `mv` 是否可以对NFS应用程序执行发生原因以使其失败。
- SMB 拒绝读取和拒绝写入打开模式分别拒绝 NFS 读取和写入操作。
- 如果文件的写入范围使用独占 SMB 字节锁锁定，则 NFS 写入操作将失败。
- 取消链接
  - 对于NTFS文件系统、支持SMB和CIFS删除操作。

    上次关闭后、此文件将被删除。
  - 不支持NFS取消链接操作。

    不支持此功能、因为需要NTFS和SMB义、并且NFS不支持上次关闭时删除操作。
  - 对于UNIX文件系统、支持取消链接操作。

    之所以支持此功能、是因为需要NFS和UNIX义。
- 重命名
  - 对于NTFS文件系统、如果目标文件是从SMB或CIFS打开的、则可以重命名目标文件。

- 不支持NFS重命名。

  不支持此功能、因为需要NTFS和SMB义。

在 UNIX 安全模式卷中， NFS 取消链接和重命名操作会忽略 SMB 锁定状态并允许访问文件。UNIX 安全模式卷上的所有其他 NFS 操作均遵循 SMB 锁定状态。

ONTAP 如何处理只读位

只读位会逐个文件进行设置，以反映文件是可写（已禁用）还是只读（已启用）。

使用 Windows 的 SMB 客户端可以设置每个文件的只读位。NFS 客户端不会设置每个文件只读位，因为 NFS 客户端不会执行任何使用每个文件只读位的协议操作。

当使用 Windows 的 SMB 客户端创建文件时， ONTAP 可以在该文件上设置只读位。在 NFS 客户端和 SMB 客户端之间共享文件时， ONTAP 还可以设置只读位。NFS 客户端和 SMB 客户端使用某些软件时，需要启用只读位。

要使 ONTAP 对 NFS 客户端和 SMB 客户端之间共享的文件保持适当的读写权限，它会根据以下规则处理只读位：

- NFS 会将启用了只读位的任何文件视为未启用写入权限位。
- 如果 NFS 客户端禁用了所有写入权限位，并且先前至少启用了其中一个位，则 ONTAP 会为该文件启用只读位。
- 如果 NFS 客户端启用任何写入权限位，则 ONTAP 会禁用该文件的只读位。
- 如果启用了文件的只读位，而 NFS 客户端尝试发现文件的权限，则不会将文件的权限位发送到 NFS 客户端；而 ONTAP 是将权限位发送到 NFS 客户端，并屏蔽写入权限位。
- 如果启用了文件的只读位，而 SMB 客户端禁用了只读位，则 ONTAP 将为此文件启用所有者的写入权限位。
- 启用了只读位的文件只能由 root 用户写入。

> 对文件权限的更改会立即在 SMB 客户端上生效，但如果 NFS 客户端启用属性缓存，则可能不会立即在 NFS 客户端上生效。

在处理共享路径组件上的锁定时， ONTAP 与 Windows 有何不同

与 Windows 不同， ONTAP 不会在打开文件时锁定打开文件的路径的每个组件。此行为也会影响 SMB 共享路径。

由于 ONTAP 不会锁定路径的每个组件，因此可以重命名打开的文件或共享上方的路径组件，这可能会导致某些应用程序出现发生原因问题，也可能发生原因会使 SMB 配置中的共享路径无效。这可能发生原因会使此共享无法访问。

为了避免重命名路径组件导致的问题，您可以应用安全设置来防止用户或应用程序重命名关键目录。

显示有关锁定的信息

您可以显示有关当前文件锁定的信息，包括锁定的锁定类型以及锁定状态，字节范围锁定，共享锁定模式，委派锁定和机会锁定的详细信息，以及锁定是使用持久句柄还是持久句柄打开的。

关于此任务

对于通过 NFSv4 或 NFSv4.1 建立的锁定，无法显示客户端 IP 地址。

默认情况下，命令会显示有关所有锁定的信息。您可以使用命令参数显示有关特定 Storage Virtual Machine （SVM）锁定的信息，或者按其他条件筛选命令的输出。

。 `vserver locks show` 命令可显示有关四种类型的锁定的信息：

- 字节范围锁定，仅锁定文件的一部分。
- 共享锁定，用于锁定打开的文件。
- 机会锁，用于控制 SMB 上的客户端缓存。
- 委派，用于通过 NFSv4.x 控制客户端缓存

通过指定可选参数，您可以确定有关每个锁定类型的重要信息。有关详细信息，请参见命令的手册页。

步骤

1. 使用显示有关锁定的信息 `vserver locks show` 命令：

示例

以下示例显示了路径为的文件上的NFSv4锁定的摘要信息 `/vol1/file1`。共享锁定访问模式为 write-deny_none ，而锁定是通过写入委派授予的：

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path                LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1                lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                          delegation  -
               Delegation Type: write
```

以下示例显示路径为的文件上SMB锁定的详细操作锁定和共享锁定信息 `/data2/data2_2/intro.pptx`。对于 IP 地址为 10.3.1.3 的客户端，共享锁定访问模式为 write-deny_none 的文件会授予持久句柄。租用机会锁会授予批量机会锁级别：

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx
```

```
                    Vserver: vs1
                     Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/intro.pptx
                 Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
             Lock Protocol: cifs
                 Lock Type: share-level
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                    Vserver: vs1
                     Volume: data2_2
         Logical Interface: lif2
               Object Path: /data2/data2_2/test.pptx
                 Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
             Lock Protocol: cifs
                 Lock Type: op-lock
   Node Holding Lock State: node3
                Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
```

```
              SMB Open Type: -
          SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

中断锁定

当文件锁定阻止客户端访问文件时，您可以显示有关当前持有的锁定的信息，然后中断特定锁定。可能需要中断锁定的情形示例包括调试应用程序。

关于此任务

。 `vserver locks break` 命令只能在高级权限级别及更高权限级别下使用。命令的手册页包含详细信息。

步骤

1. 要查找解除锁定所需的信息、请使用 `vserver locks show` 命令：

   命令的手册页包含详细信息。

2. 将权限级别设置为高级： `set -privilege advanced`
3. 执行以下操作之一：

如果要通过指定 ... 来中断锁定	输入命令 ...
SVM 名称，卷名称， LIF 名称和文件路径	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
锁定 ID	`vserver locks break -lockid UUID`

4. 返回到管理权限级别： `set -privilege admin`

监控 SMB 活动

显示 SMB 会话信息

您可以显示有关已建立的 SMB 会话的信息，包括 SMB 连接和会话 ID 以及使用会话的工作站的 IP 地址。您可以显示有关会话的 SMB 协议版本和持续可用保护级别的信息，这有助于确定会话是否支持无中断操作。

关于此任务

您可以摘要形式显示 SVM 上所有会话的信息。但是，在许多情况下，返回的输出量很大。您可以通过指定可选参数来自定义输出中显示的信息：

- 您可以使用可选 `-fields` 用于显示有关所选字段的输出的参数。

您可以输入 `-fields ?` 以确定您可以使用哪些字段。

- 您可以使用 `-instance` 用于显示有关已建立SMB会话的详细信息的参数。
- 您可以使用 `-fields` 参数或 `-instance` 参数单独使用或与其他可选参数结合使用。

步骤

1. 执行以下操作之一：

要显示 **SMB** 会话信息的项	输入以下命令 **...**
SVM 上的所有会话的摘要形式	`vserver cifs session show -vserver vserver_name`
指定的连接 ID	`vserver cifs session show -vserver vserver_name -connection-id integer`
指定的工作站 IP 地址	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
指定的 LIF IP 地址	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
在指定节点上	`vserver cifs session show -vserver vserver_name -node {node_name
local}`	指定的 Windows 用户
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	使用指定的身份验证机制
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2
Kerberos	Anonymous}`
使用指定的协议版本	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1

要显示 **SMB** 会话信息的项	输入以下命令 **...**
SMB3	SMB3_1}`  [NOTE] ==== 持续可用的保护和 SMB 多通道仅适用于 SMB 3.0 及更高版本的会话。要查看其在所有符合条件的会话中的状态、应指定此参数并将值设置为 `SMB3` 或更高版本。 ====
具有指定级别的持续可用保护	`vserver cifs session show -vserver vserver_name -continuously-available {No
Yes	Partial}`  [NOTE] ==== 持续可用状态为 `Partial`，这意味着会话至少包含一个打开的持续可用文件，但会话中的某些文件未使用持续可用保护打开。您可以使用 `vserver cifs sessions file show` 命令、用于确定已建立会话中哪些文件未在持续可用的保护下打开。 ====
具有指定的 SMB 签名会话状态	`vserver cifs session show -vserver vserver_name -is-session-signed {true

示例

以下命令显示 SVM vs1 上从 IP 地址为 10.1.1.1 的工作站建立的会话的会话信息：

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID          ID      Workstation      Windows User    Files         Time
----------  ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

以下命令显示 SVM vs1 上具有持续可用保护的会话的详细会话信息。此连接是使用域帐户建立的。

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

以下命令显示 SVM vs1 上使用 SMB 3.0 和 SMB 多通道的会话的会话信息。在此示例中，用户使用 LIF IP 地址从支持 SMB 3.0 的客户端连接到此共享；因此，身份验证机制默认为 NTLMv2 。必须使用 Kerberos 身份验证进行连接，以获得持续可用的保护。

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

相关信息

显示有关打开的 SMB 文件的信息

显示有关打开的 **SMB** 文件的信息

您可以显示有关打开的 SMB 文件的信息，包括 SMB 连接和会话 ID ，托管卷，共享名称和共享路径。您可以显示有关文件的持续可用保护级别的信息，这有助于确定打开的文件是否处于支持无中断操作的状态。

关于此任务

您可以显示有关已建立的 SMB 会话上打开的文件的信息。如果需要确定 SMB 会话中特定文件的 SMB 会话信息，则显示的信息非常有用。

例如、如果您有一个SMB会话、其中一些打开的文件已打开且具有持续可用的保护、而另一些文件未打开且具有持续可用的保护(的值 `-continuously-available` 字段输入 `vserver cifs session show` 命令输出为 `Partial`)、则可以使用此命令确定哪些文件不持续可用。

您可以使用以摘要形式显示Storage Virtual Machine (SVM)上已建立的SMB会话上的所有打开文件的信息 `vserver cifs session file show` 命令、而不带任何可选参数。

但是，在许多情况下，返回的输出量很大。您可以通过指定可选参数来自定义输出中显示的信息。如果您只想查看一小部分打开文件的信息，这将非常有用。

- 您可以使用可选 `-fields` 用于显示所选字段的输出的参数。

  您可以单独使用此参数，也可以与其他可选参数结合使用。

- 您可以使用 `-instance` 用于显示有关打开的SMB文件的详细信息的参数。

  您可以单独使用此参数，也可以与其他可选参数结合使用。

步骤

1. 执行以下操作之一：

如果要显示打开的 **SMB** 文件 ...	输入以下命令 ...
以摘要形式显示在 SVM 上	`vserver cifs session file show -vserver vserver_name`
在指定节点上	`vserver cifs session file show -vserver vserver_name -node {node_name
local}`	指定的文件 ID
`vserver cifs session file show -vserver vserver_name -file-id integer`	指定的 SMB 连接 ID
`vserver cifs session file show -vserver vserver_name -connection-id integer`	指定的 SMB 会话 ID
`vserver cifs session file show -vserver vserver_name -session-id integer`	在指定的托管聚合上
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	在指定卷上
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	指定的 SMB 共享上
`vserver cifs session file show -vserver vserver_name -share share_name`	指定的 SMB 路径上
`vserver cifs session file show -vserver vserver_name -path path`	具有指定级别的持续可用保护

如果要显示打开的 **SMB** 文件 ...	输入以下命令 ...
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== 持续可用状态为 `No`，这意味着这些打开的文件无法从接管和恢复中无系统地恢复。它们也无法从高可用性关系中的合作伙伴之间的常规聚合重新定位中恢复。 ====
具有指定的重新连接状态	`vserver cifs session file show -vserver vserver_name -reconnected {No

您可以使用其他可选参数来细化输出结果。有关详细信息，请参见手册页。

示例

以下示例显示了有关 SVM vs1 上打开的文件的信息：

```
cluster1::> vserver cifs session file show -vserver vs1
Node:       node1
Vserver:    vs1
Connection: 3151274158
Session:    1
File    File      Open Hosting               Continuously
ID      Type      Mode Volume    Share       Available
------- --------- ---- --------- ----------- ------------
41      Regular   r    data      data        Yes
Path: \mytest.rtf
```

以下示例显示了有关 SVM vs1 上文件 ID 82 的已打开 SMB 文件的详细信息：

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                   Node: node1
                Vserver: vs1
                File ID: 82
          Connection ID: 104617
             Session ID: 1
              File Type: Regular
              Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
             CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
             Share Mode: rw
            Range Locks: 1
Continuously Available: Yes
            Reconnected: No
```

相关信息

显示 SMB 会话信息

确定可用的统计信息对象和计数器

在获取有关 CIFS ， SMB ，审核和 BranchCache 哈希统计信息以及监控性能的信息之前，您必须了解哪些对象和计数器可用于获取数据。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 执行以下操作之一：

要确定的内容	输入 ...
哪些对象可用	`statistics catalog object show`
可用的特定对象	`statistics catalog object show object object_name`
哪些计数器可用	`statistics catalog counter show object object_name`

有关哪些对象和计数器可用的详细信息，请参见手册页。

3. 返回到管理权限级别： `set -privilege admin`

示例

以下命令显示与集群中的 CIFS 和 SMB 访问相关的选定统计信息对象的说明，如高级权限级别所示：

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

以下命令显示有关的某些计数器的信息 `cifs` 对象、如高级权限级别所示：

> 此示例不会显示的所有可用计数器 `cifs` 对象；输出被截断。

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    ---------------------------
----------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    ------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                             vserver_1:10.72.205.179
    instance_uuid                                     2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

相关信息

显示统计信息

显示统计信息

您可以显示各种统计信息，包括有关 CIFS 和 SMB ，审核和 BranchCache 哈希的统计信息，以监控性能并诊断问题。

开始之前

您必须已使用收集数据样本 `statistics start` 和 `statistics stop` 命令、然后才能显示有关对象的信息。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 执行以下操作之一：

要显示统计信息的对象	输入 ...
SMB 的所有版本	`statistics show -object cifs`
SMB 1.0	`statistics show -object smb1`
SMB 2.x 和 SMB 3.0	`statistics show -object smb2`
节点的 CIFS 子系统	`statistics show -object nblade_cifs`
多协议审核	`statistics show -object audit_ng`
BranchCache 哈希服务	`statistics show -object hashd`
动态 DNS	`statistics show -object ddns_update`

   有关详细信息，请参见每个命令的手册页。

3. 返回到管理权限级别： `set -privilege admin`

相关信息

确定可用的统计信息对象和计数器

监控 SMB 签名会话统计信息

显示 BranchCache 统计信息

使用统计信息监控自动节点转介活动

"Microsoft Hyper-V 和 SQL Server 的 SMB 配置"

"性能监控设置"