使用 SMB 设置文件访问

ONTAP 9

NetApp
September 12, 2024

目录

使用 SMB 设置文件访问

配置安全模式

安全模式如何影响数据访问

安全模式及其影响

安全模式有四种： UNIX ， NTFS ，混合和统一。每个安全模式对处理数据权限的方式具有不同的影响。您必须了解不同的影响，以确保选择适合您的安全模式。

请务必了解，安全模式并不确定哪些客户端类型可以或不可以访问数据。安全模式仅确定 ONTAP 用于控制数据访问的权限类型以及可以修改这些权限的客户端类型。

例如，如果某个卷使用 UNIX 安全模式，则由于 ONTAP 的多协议性质， SMB 客户端仍可访问数据（前提是它们正确进行身份验证和授权）。但是， ONTAP 使用的是 UNIX 权限，只有 UNIX 客户端才能使用原生工具进行修改。

安全风格	可以修改权限的客户端	客户端可以使用的权限	生成的有效安全模式	可以访问文件的客户端
"unix"	NFS	NFSv3 模式位	"unix"	NFS 和 SMB
		NFSv4.x ACL		
NTFS	SMB	NTFS ACL	NTFS	
混合	NFS 或 SMB	NFSv3 模式位	"unix"	
		NFSv4.ACL		
		NTFS ACL	NTFS	
统一： (仅限无限卷、在ONTAP 9.4及更早版本中。)	NFS 或 SMB	NFSv3 模式位	"unix"	
		NFSv4.1 ACL		
		NTFS ACL	NTFS	

FlexVol卷支持UNIX、NTFS和混合安全模式。混合或统一安全模式时，有效权限取决于上次修改权限的客户端类型，因为用户会逐个设置安全模式。如果修改权限的最后一个客户端是 NFSv3 客户端，则权限为 UNIX NFSv3 模式位。如果最后一个客户端是 NFSv4 客户端，则权限为 NFSv4 ACL 。如果最后一个客户端是 SMB 客户端，则权限为 Windows NTFS ACL 。

统一安全模式仅适用于无限卷，而 ONTAP 9.5 及更高版本不再支持无限卷。有关详细信息，请参见 FlexGroup 卷管理概述。

从ONTAP 9.2开始、 `show-effective-permissions` 参数 `vserver security file-directory` 命令用于显示为Windows或UNIX用户授予的对指定文件或文件夹路径的有效权限。此外、还有可选参数 `-share -name` 用于显示有效共享权限。

ONTAP 最初会设置一些默认文件权限。默认情况下， UNIX ，混合和统一安全模式卷中所有数据的有效安全模式为 UNIX ，有效权限类型为 UNIX 模式位（ 0755 ，除非另有指定），直到客户端按照默认安全模式进行配置为止。默认情况下， NTFS 安全模式卷中所有数据的有效安全模式为 NTFS ，并且具有一个 ACL ，允许对任何人进行完全控制。

设置安全模式的位置和时间

可以在 FlexVol 卷（根卷或数据卷）和 qtree 上设置安全模式。安全模式可以在创建时手动设置，自动继承或稍后更改。

确定要在 **SVM** 上使用的安全模式

为了帮助您确定要在卷上使用的安全模式，您应考虑两个因素。主要因素是管理文件系统的管理员类型。二级因素是访问卷上数据的用户或服务的类型。

在卷上配置安全模式时，应考虑环境的需求，以确保选择最佳安全模式并避免管理权限时出现问题。以下注意事项有助于您做出决定：

安全风格	选择条件
"unix"	• 文件系统由 UNIX 管理员管理。 • 大多数用户都是 NFS 客户端。 • 访问数据的应用程序使用 UNIX 用户作为服务帐户。
NTFS	• 文件系统由 Windows 管理员管理。 • 大多数用户都是SMB客户端。 • 访问数据的应用程序使用 Windows 用户作为服务帐户。
混合	文件系统由 UNIX 和 Windows 管理员管理，用户由 NFS 和 SMB 客户端组成。

安全模式继承的工作原理

如果在创建新的 FlexVol 卷或 qtree 时未指定安全模式，则它会以不同方式继承其安全模式。

安全模式按以下方式继承：

- FlexVol 卷继承其所属 SVM 的根卷的安全模式。
- qtree 继承其所属 FlexVol 卷的安全模式。
- 文件或目录会继承其所在 FlexVol 卷或 qtree 的安全模式。

ONTAP 如何保留 UNIX 权限

当 Windows 应用程序编辑和保存 FlexVol 卷中当前具有 UNIX 权限的文件时， ONTAP 可以保留 UNIX 权限。

当 Windows 客户端上的应用程序编辑和保存文件时，它们会读取文件的安全属性，创建新的临时文件，将这些属性应用于临时文件，然后为临时文件提供原始文件名。

当 Windows 客户端对安全属性执行查询时，它们会收到一个构建的 ACL ，该 ACL 准确表示 UNIX 权限。此构建 ACL 的唯一目的是，在 Windows 应用程序更新文件时保留文件的 UNIX 权限，以确保生成的文件具有相同的 UNIX 权限。ONTAP 不会使用构建的 ACL 设置任何 NTFS ACL 。

使用 **Windows** 安全性选项卡管理 **UNIX** 权限

如果要在 SVM 上操作混合安全模式卷或 qtree 中的文件或文件夹的 UNIX 权限，可以使用 Windows 客户端上的安全性选项卡。或者，您也可以使用可以查询和设置 Windows ACL 的应用程序。

- 修改 UNIX 权限

  您可以使用 Windows 安全性选项卡查看和更改混合安全模式卷或 qtree 的 UNIX 权限。如果您使用 Windows 安全性主选项卡更改 UNIX 权限，则必须先删除要编辑的现有 ACE （此操作会将模式位设置为 0 ），然后再进行更改。或者，您也可以使用高级编辑器更改权限。

  如果使用模式权限，则可以直接更改列出的 UID ， GID 和其他（在计算机上具有帐户的其他所有人）的模式权限。例如，如果显示的 UID 具有 r-x 权限，则可以将 UID 权限更改为 rwx 。

- 将 UNIX 权限更改为 NTFS 权限

  您可以使用 Windows 安全性选项卡将 UNIX 安全对象替换为混合安全模式卷或 qtree 上的 Windows 安全对象，其中文件和文件夹采用 UNIX 有效安全模式。

  您必须先删除列出的所有 UNIX 权限条目，然后才能将其替换为所需的 Windows 用户和组对象。然后，您可以在 Windows 用户和组对象上配置基于 NTFS 的 ACL 。通过删除所有 UNIX 安全对象并仅将 Windows 用户和组添加到混合安全模式卷或 qtree 中的文件或文件夹，可以将文件或文件夹上的有效安全模式从 UNIX 更改为 NTFS 。

  更改文件夹的权限时，默认的 Windows 行为是将这些更改传播到所有子文件夹和文件。因此，如果您不想将安全模式的更改传播到所有子文件夹，子文件夹和文件，则必须将传播选项更改为所需设置。

在 **SVM** 根卷上配置安全模式

您可以配置 Storage Virtual Machine （ SVM ）根卷安全模式，以确定 SVM 根卷上的数据所使用的权限类型。

步骤

1. 使用 `vserver create` 命令 `-rootvolume-security-style` 用于定义安全模式的参数。

   根卷安全模式的可能选项为 `unix`， `ntfs`或 `mixed`。

2. 显示并验证配置，包括您创建的 SVM 的根卷安全模式： `vserver show -vserver vserver_name`

在 FlexVol 卷上配置安全模式

您可以配置 FlexVol 卷安全模式，以确定 Storage Virtual Machine （ SVM ）的 FlexVol 卷上的数据所使用的权限类型。

步骤

1. 执行以下操作之一：

如果 FlexVol 卷 …	使用命令 …
尚不存在	`volume create` 并包括 `-security-style` 用于指定安全模式的参数。
已存在	`volume modify` 并包括 `-security-style` 用于指定安全模式的参数。

   FlexVol卷安全模式的可能选项为 `unix`， `ntfs`或 `mixed`。

   如果在创建 FlexVol 卷时未指定安全模式，则此卷将继承根卷的安全模式。

   有关的详细信息、请参见 `volume create` 或 `volume modify` 命令、请参见 "逻辑存储管理"。

2. 要显示配置，包括您创建的 FlexVol 卷的安全模式，请输入以下命令：

   ```
   volume show -volume volume_name -instance
   ```

在 qtree 上配置安全模式

您可以配置 qtree 卷安全模式，以确定 qtree 上的数据所使用的权限类型。

步骤

1. 执行以下操作之一：

如果 **qtree…**	使用命令 **…**
尚不存在	`volume qtree create` 并包括 `-security -style` 用于指定安全模式的参数。
已存在	`volume qtree modify` 并包括 `-security -style` 用于指定安全模式的参数。

   qtree安全模式的可能选项为 `unix`， `ntfs`或 `mixed`。

   如果在创建qtree时未指定安全模式、则默认安全模式为 `mixed`。

有关的详细信息、请参见 `volume qtree create` 或 `volume qtree modify` 命令、请参见 "逻辑存储管理"。

2. 要显示配置(包括所创建的qtree的安全模式)、请输入以下命令： `volume qtree show -qtree qtree_name -instance`

在 NAS 命名空间中创建和管理数据卷

在 NAS 命名空间中创建和管理数据卷概述

要在 NAS 环境中管理文件访问，您必须管理 Storage Virtual Machine （ SVM ）上的数据卷和接合点。其中包括规划命名空间架构，创建具有或不具有接合点的卷，挂载或卸载卷以及显示有关数据卷和 NFS 服务器或 CIFS 服务器命名空间的信息。

创建具有指定接合点的数据卷

您可以在创建数据卷时指定接合点。生成的卷会自动挂载在接合点，并可立即配置用于 NAS 访问。

开始之前

要创建卷的聚合必须已存在。

> 接合路径中不能使用以下字符： * # " > < | ? \
>
> 此外，接合路径长度不能超过 255 个字符。

步骤

1. 创建具有接合点的卷： `volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path junction_path`

   接合路径必须以根（ / ）开头，并且可以同时包含目录和接合卷。接合路径不需要包含卷的名称。接合路径与卷名称无关。

   指定卷安全模式是可选的。如果未指定安全模式，则 ONTAP 将使用应用于 Storage Virtual Machine （ SVM ）根卷的相同安全模式创建卷。但是，根卷的安全模式可能不是要应用于您创建的数据卷的安全模式。建议您在创建卷时指定安全模式，以最大程度地减少难以解决的文件访问问题。

   接合路径不区分大小写； `/ENG` 与相同 `/eng`。如果创建 CIFS 共享， Windows 会将接合路径视为区分大小写。例如、如果接合为 `/ENG`，则CIFS共享的路径必须以开头 `/ENG`，不是 `/eng`。

   您可以使用许多可选参数自定义数据卷。要了解有关它们的详细信息、请参见的手册页 `volume create` 命令：

2. 验证是否已使用所需的接合点创建卷： `volume show -vserver vserver_name -volume volume_name -junction`

示例

以下示例将在` SVM VS1上创建一个具有接合路径的名为"`home"的卷 `/eng/home`：

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

创建数据卷而不指定接合点

您可以在不指定接合点的情况下创建数据卷。生成的卷不会自动挂载，也不可配置用于 NAS 访问。您必须先挂载卷，然后才能为该卷配置 SMB 共享或 NFS 导出。

开始之前

要创建卷的聚合必须已存在。

步骤

1. 使用以下命令创建不带接合点的卷： `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}`

   指定卷安全模式是可选的。如果未指定安全模式，则 ONTAP 将使用应用于 Storage Virtual Machine （ SVM ）根卷的相同安全模式创建卷。但是，根卷的安全模式可能不是要应用于数据卷的安全模式。建议您在创建卷时指定安全模式，以最大程度地减少难以解决的文件访问问题。

   您可以使用许多可选参数自定义数据卷。要了解有关它们的详细信息、请参见的手册页 `volume create` 命令：

2. 验证是否已在没有接合点的情况下创建卷： `volume show -vserver` *`vserver_name`* `-volume` *`volume_name`* `-junction`

示例

以下示例将在 SVM vs1 上创建一个名为 `sales` 的卷，该卷未挂载在接合点：

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                      Junction                 Junction
Vserver   Volume      Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

挂载或卸载 NAS 命名空间中的现有卷

必须先在 NAS 命名空间上挂载卷，然后才能配置 NAS 客户端对 Storage Virtual Machine （ SVM ）卷中所含数据的访问。如果卷当前未挂载，则可以将其挂载到接合点。您也可以卸载卷。

关于此任务

如果卸载某个卷并使其脱机、则NAS客户端将无法访问该接合点中的所有数据、包括接合点位于已卸载卷的命名空间中的卷中的数据。

> 要停止 NAS 客户端对卷的访问，仅仅卸载卷是不够的。您必须使此卷脱机、或者采取其他步骤确保客户端文件句柄缓存失效。有关详细信息，请参见以下知识库文章： "从 ONTAP 的命名空间中删除卷后， NFSv3 客户端仍可访问该卷"

卸载卷并使其脱机后、卷中的数据不会丢失。此外，在卷上或在已卸载卷内的目录和接合点上创建的现有卷导出策略和 SMB 共享也会保留下来。如果重新挂载卸载的卷， NAS 客户端可以使用现有导出策略和 SMB 共享访问卷中包含的数据。

步骤

1. 执行所需的操作：

如果您要 ...	输入命令 ...
挂载卷	`volume mount -vserver` *`svm_name`* `-volume` *`volume_name`* `-junction-path` *`junction_path`*
卸载卷	`volume unmount -vserver` *`svm_name`* `-volume` *`volume_name`* `volume offline -vserver` *`svm_name`* `-volume` *`volume_name`*

2. 验证卷是否处于所需的挂载状态：

```
volume show -vserver svm_name -volume volume_name -fields state,junction-
path,junction-active
```

示例

以下示例将位于SVM"`VS1`"上名为` ales s的卷挂载到接合点"/sales`"：

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

以下示例将卸载位于SVM"`VS1`"上的名为"`data`"的卷并使其脱机：

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

显示卷挂载和接合点信息

您可以显示有关 Storage Virtual Machine （ SVM ）的已挂载卷以及卷挂载到的接合点的信息。您还可以确定哪些卷未挂载到接合点。您可以使用此信息了解和管理 SVM 命名空间。

步骤

1. 执行所需的操作：

要显示的内容	输入命令 ...
有关 SVM 上已挂载和已卸载卷的摘要信息	`volume show -vserver vserver_name -junction`
有关 SVM 上已挂载和已卸载卷的详细信息	`volume show -vserver vserver_name -volume volume_name -instance`
有关 SVM 上已挂载和已卸载卷的特定信息	a. 如有必要、您可以显示的有效字段 `-fields` 参数： `volume show -fields ?` b. 使用显示所需信息 `-fields` 参数：volume show -vserver vserver-name -fieldname、…

示例

以下示例显示了 SVM vs1 上已挂载和已卸载的卷的摘要：

```
cluster1::> volume show -vserver vs1 -junction
                      Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

以下示例显示了有关 SVM vs2 上卷的指定字段的信息：

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -            -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /            -
node3
```

配置名称映射

配置名称映射概述

ONTAP 使用名称映射将 CIFS 身份映射到 UNIX 身份，将 Kerberos 身份映射到 UNIX 身份，并将 UNIX 身份映射到 CIFS 身份。无论用户是从 NFS 客户端还是从 CIFS 客户端进行连接，它都需要此信息来获取用户凭据并提供正确的文件访问权限。

除了两个例外情况，您无需使用名称映射：

- 您配置的是纯 UNIX 环境，不打算对卷使用 CIFS 访问或 NTFS 安全模式。
- 您可以配置要使用的默认用户。

  在这种情况下，不需要进行名称映射，因为所有客户端凭据都映射到同一默认用户，而不是映射每个客户端凭据。

请注意，您只能对用户使用名称映射，而不能对组使用名称映射。

但是，您可以将一组用户映射到特定用户。例如，您可以将以 SALES 开头或结尾的所有 AD 用户映射到特定 UNIX 用户和用户的 UID 。

名称映射的工作原理

当 ONTAP 必须映射用户的凭据时，它会首先检查本地名称映射数据库和 LDAP 服务器中是否存在现有映射。它是检查一个还是同时检查这两者，以及检查顺序取决于 SVM 的名称服务配置。

- 适用于 Windows 到 UNIX 的映射

  如果未找到映射， ONTAP 将检查小写的 Windows 用户名是否为 UNIX 域中的有效用户名。如果此操作不起作用，则只要配置了默认 UNIX 用户，它就会使用默认 UNIX 用户。如果未配置默认 UNIX 用户，并且 ONTAP 也无法通过这种方式获取映射，则映射将失败并返回错误。

- UNIX 到 Windows 的映射

  如果未找到映射， ONTAP 将尝试查找与 SMB 域中的 UNIX 名称匹配的 Windows 帐户。如果此操作不起作用，则会使用默认 SMB 用户，但前提是已配置此用户。如果未配置默认 CIFS 用户，并且 ONTAP 也无法通过此方式获取映射，则映射将失败并返回错误。

默认情况下，计算机帐户映射到指定的默认 UNIX 用户。如果未指定默认 UNIX 用户，计算机帐户映射将失败。

- 从 ONTAP 9.5 开始，您可以将计算机帐户映射到默认 UNIX 用户以外的用户。
- 在 ONTAP 9.4 及更早版本中，您无法将计算机帐户映射到其他用户。

  即使为计算机帐户定义了名称映射，也会忽略这些映射。

多域搜索 **UNIX** 用户到 **Windows** 用户名映射

在将 UNIX 用户映射到 Windows 用户时， ONTAP 支持多域搜索。系统将搜索所有已发现的受信任域以查找与替换模式匹配的匹配项，直到返回匹配结果为止。或者，您也可以配置首选受信任域列表，该列表将代替发现的受信任域列表使用，并按顺序进行搜索，直到返回匹配结果为止。

域信任如何影响 **UNIX** 用户到 **Windows** 用户名称映射搜索

要了解多域用户名映射的工作原理，您必须了解域信任如何与 ONTAP 配合使用。与 CIFS 服务器主域的 Active Directory 信任关系可以是双向信任，也可以是两种类型的单向信任之一，即入站信任或出站信任。主域是 SVM 上的 CIFS 服务器所属的域。

- _ 双向信任 _

  通过双向信任，两个域相互信任。如果 CIFS 服务器的主域与另一个域具有双向信任，则主域可以对属于受信任域的用户进行身份验证和授权，反之亦然。

  UNIX 用户到 Windows 用户名映射搜索只能在主域和另一个域之间具有双向信任的域上执行。

- 出站信任 _

  对于出站信任，主域信任另一个域。在这种情况下，主域可以对属于出站受信任域的用户进行身份验证和授权。

执行 UNIX 用户到 Windows 用户名映射搜索时，系统会搜索与主域具有出站信任的域。

- *Inbound trust*

  对于入站信任，另一个域信任 CIFS 服务器的主域。在这种情况下，主域无法对属于入站受信任域的用户进行身份验证或授权。

  在执行 UNIX 用户到 Windows 用户名映射搜索时，系统会搜索与主域具有入站信任的域。

如何使用通配符（*）配置名称映射的多域搜索

在 Windows 用户名的域部分使用通配符有助于进行多域名称映射搜索。下表说明了如何在名称映射条目的域部分使用通配符来启用多域搜索：

Pattern	更换	结果
root	• 。 \\ 管理员	UNIX 用户 "`root` " 将映射到名为 "`administrator` " 的用户。系统会按顺序搜索所有受信任域，直到找到第一个名为 "`administrator` " 的匹配用户为止。
*	**	有效的 UNIX 用户将映射到相应的 Windows 用户。系统将按顺序搜索所有受信任域，直到找到具有该名称的第一个匹配用户为止。 模式 ** 仅适用于从 UNIX 到 Windows 的名称映射，而不是相反。

如何执行多域名搜索

您可以选择以下两种方法之一来确定用于多域名搜索的受信任域列表：

- 使用由 ONTAP 编译的自动发现的双向信任列表
- 使用您编译的首选受信任域列表

如果将 UNIX 用户映射到使用通配符用于用户名的域部分的 Windows 用户，则会在所有受信任域中查找此 Windows 用户，如下所示：

- 如果配置了首选受信任域列表，则只会在此搜索列表中按顺序查找映射的 Windows 用户。
- 如果未配置首选受信任域列表，则会在主域的所有双向受信任域中查找 Windows 用户。
- 如果主域没有双向受信任的域，则会在主域中查找用户。

如果 UNIX 用户映射到用户名中没有域部分的 Windows 用户，则会在主域中查找此 Windows 用户。

名称映射转换规则

ONTAP 系统会为每个 SVM 保留一组转换规则。每个规则都包含两部分： *pattern* 和 *replacement* 。转换从相应列表的开头开始，并根据第一个匹配规则执行替换。模式是 UNIX 模式的正则表达式。替换项是一个字符串、其中包含表示模式中的子表达式的转义序列、与UNIX中的情况一样 `sed` 计划。

创建名称映射

您可以使用 `vserver name-mapping create` 命令以创建名称映射。您可以使用名称映射使 Windows 用户能够访问 UNIX 安全模式卷，反之亦然。

关于此任务

对于每个 SVM ， ONTAP 支持每个方向最多 12 ， 500 个名称映射。

步骤

1. 创建名称映射： `vserver name-mapping create -vserver` *`vserver_name`* `-direction {krb-unix|win-unix|unix-win} -position` *`integer`* `-pattern text -replacement` *`text`*

   > 。 `-pattern` 和 `-replacement` 语句可以表达为正则表达式。您也可以使用 `-replacement` 用于使用空替换字符串明确拒绝映射到用户的语句 `" "` (空格字符)。请参见 `vserver name-mapping create` 有关详细信息、请参见手册页。

   创建 Windows 到 UNIX 映射时，在创建新映射时与 ONTAP 系统建立了打开连接的任何 SMB 客户端都必须注销并重新登录才能查看新映射。

示例

以下命令将在名为 vs1 的 SVM 上创建名称映射。此映射是指优先级列表中位置 1 处从 UNIX 到 Windows 的映射。映射会将 UNIX 用户 johnd 映射到 Windows 用户 ENG\JohnDoe 。

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

以下命令会在名为 vs1 的 SVM 上创建另一个名称映射。此映射是指优先级列表中位置 1 处从 Windows 到 UNIX 的映射。此处的模式和替换项包括正则表达式。此映射会将域 ENG 中的每个 CIFS 用户映射到与 SVM 关联的 LDAP 域中的用户。

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

以下命令会在名为 vs1 的 SVM 上创建另一个名称映射。此处的模式将 "` $` " 作为必须转义的 Windows 用户名中的一个元素。映射会将 Windows 用户 ENG\ john$ops 映射到 UNIX 用户 john_ops 。

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

配置默认用户：

您可以配置一个默认用户，以便在用户的所有其他映射尝试均失败或不希望在 UNIX 和 Windows 之间映射单个用户时使用。或者，如果您希望对未映射用户的身份验证失败，则不应配置默认用户。

关于此任务

对于 CIFS 身份验证，如果不希望将每个 Windows 用户映射到单个 UNIX 用户，则可以改为指定默认 UNIX 用户。

对于 NFS 身份验证，如果不希望将每个 UNIX 用户映射到单个 Windows 用户，则可以改为指定一个默认 Windows 用户。

步骤

1. 执行以下操作之一：

如果您要 ...	输入以下命令 ...
配置默认 UNIX 用户	`vserver cifs options modify -default -unix-user` *`user_name`*
配置默认 Windows 用户	`vserver nfs modify -default-win-user` *`user_name`*

用于管理名称映射的命令

您可以使用特定的 ONTAP 命令来管理名称映射。

如果您要 ...	使用此命令 ...
创建名称映射	`vserver name-mapping create`
在特定位置插入名称映射	`vserver name-mapping insert`
显示名称映射	`vserver name-mapping show`
交换两个名称映射的位置 ⓘ 如果使用 IP 限定符条目配置了名称映射，则不允许交换。	`vserver name-mapping swap`

如果您要 ...	使用此命令 ...
修改名称映射	`vserver name-mapping modify`
删除名称映射	`vserver name-mapping delete`
验证名称映射是否正确	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

有关详细信息，请参见每个命令的手册页。

配置多域名称映射搜索

启用或禁用多域名称映射搜索

对于多域名称映射搜索，在配置 UNIX 用户到 Windows 用户名的映射时，您可以在 Windows 名称的域部分使用通配符（*）。通过在名称的域部分中使用通配符（*），ONTAP 可以搜索与包含 CIFS 服务器计算机帐户的域具有双向信任的所有域。

关于此任务

除了搜索所有双向受信任域之外，您还可以配置首选受信任域的列表。配置首选受信任域列表后， ONTAP 将使用首选受信任域列表而不是发现的双向受信任域来执行多域名称映射搜索。

- 默认情况下，多域名称映射搜索处于启用状态。
- 此选项可在高级权限级别下使用。

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：

多域名称映射搜索的目标位置	输入命令 ...
enabled	`vserver cifs options modify -vserver` *`vserver_name`* `-is-trusted-domain-enum-search-enabled true`
已禁用	`vserver cifs options modify -vserver` *`vserver_name`* `-is-trusted-domain-enum-search-enabled false`

3. 返回到管理权限级别： `set -privilege admin`

相关信息

重置和重新发现受信任域

您可以强制重新发现所有受信任域。当受信任域服务器未正确响应或信任关系发生更改时，此功能非常有用。只会发现与主域具有双向信任的域，即包含 CIFS 服务器计算机帐户的域。

步骤

1. 使用重置和重新发现受信任域 `vserver cifs domain trusts rediscover` 命令：

   ```
   vserver cifs domain trusts rediscover -vserver vs1
   ```

相关信息

显示有关已发现的受信任域的信息

显示有关已发现的受信任域的信息

您可以显示有关 CIFS 服务器主域的已发现受信任域的信息，该域是包含 CIFS 服务器计算机帐户的域。如果您希望了解发现了哪些受信任域以及如何在发现的受信任域列表中对这些域进行排序，则此功能非常有用。

关于此任务

仅发现与主域具有双向信任的域。由于主域的域控制器（Domain Controller， DC）按 DC 确定的顺序返回受信任域列表，因此无法预测此列表中域的顺序。通过显示受信任域列表，您可以确定多域名称映射搜索的搜索顺序。

显示的受信任域信息按节点和 Storage Virtual Machine （SVM）分组。

步骤

1. 使用显示有关已发现的受信任域的信息 `vserver cifs domain trusts show` 命令：

   ```
   vserver cifs domain trusts show -vserver vs1
   ```

```
   Node: node1
Vserver: vs1

Home Domain             Trusted Domain
---------------------  ------------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM

   Node: node2
Vserver: vs1

Home Domain             Trusted Domain
---------------------  ------------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM
```

相关信息

重置和重新发现受信任域

在首选受信任域列表中添加，删除或替换受信任域

您可以在SMB服务器的首选受信任域列表中添加或删除受信任域、也可以修改当前列表。如果您配置了首选受信任域列表，则在执行多域名称映射搜索时，系统将使用此列表，而不是发现的双向受信任域。

关于此任务

- 如果要向现有列表添加受信任域，则新列表将与现有列表合并，并在末尾放置新条目系统将按受信任域列表中显示的顺序搜索这些受信任域。
- 如果您要从现有列表中删除受信任域，但未指定列表，则会删除指定 Storage Virtual Machine （ SVM ）的整个受信任域列表。
- 如果修改现有受信任域列表，则新列表将覆盖现有列表。

> 您应在首选受信任域列表中仅输入双向受信任域。即使您可以在首选域列表中输入出站或入站信任域，但在执行多域名称映射搜索时不会使用它们。ONTAP 会跳过单向域的条目，然后转到列表中的下一个双向受信任域。

步骤

1. 执行以下操作之一：

如果要对首选受信任域列表执行以下操作 ...	使用命令 ...
将受信任域添加到列表中	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
从列表中删除受信任域	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`
修改现有列表	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

示例

以下命令会将两个受信任域（ cifs1.example.com 和 cifs2.example.com ）添加到 SVM vs1 使用的首选受信任域列表中：

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

以下命令将从 SVM vs1 使用的列表中删除两个受信任域：

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

以下命令将修改 SVM vs1 使用的受信任域列表。新列表将替换原始列表：

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

相关信息

显示有关首选受信任域列表的信息

显示有关首选受信任域列表的信息

如果启用了多域名称映射搜索，则可以显示有关首选受信任域列表中的受信任域以及这些域的搜索顺序的信息。您可以配置首选受信任域列表，以替代使用自动发现的受信任域列表。

步骤

1. 执行以下操作之一：

要显示以下内容的信息 ...	使用命令 ...
按 Storage Virtual Machine （ SVM ）分组的集群中的所有首选受信任域	`vserver cifs domain name-mapping-search show`
指定 SVM 的所有首选受信任域	`vserver cifs domain name-mapping-search show -vserver` *`vserver_name`*

以下命令显示集群上所有首选受信任域的信息：

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver         Trusted Domains
--------------  ----------------------------------
vs1             CIFS1.EXAMPLE.COM
```

相关信息

在首选受信任域列表中添加，删除或替换受信任域

创建和配置 SMB 共享

创建和配置 SMB 共享概述

在用户和应用程序通过 SMB 访问 CIFS 服务器上的数据之前，您必须创建和配置 SMB 共享， SMB 共享是卷中的一个命名访问点。您可以通过指定共享参数和共享属性来自定义共享。您可以随时修改现有共享。

创建 SMB 共享时， ONTAP 会为共享创建一个默认 ACL ，并为 Everyone 创建具有完全控制权限的 ACL 。

SMB 共享与 Storage Virtual Machine （ SVM ）上的 CIFS 服务器绑定。如果删除了 SVM 或从 SVM 中删除了与之关联的 CIFS 服务器，则会删除 SMB 共享。如果在SVM上重新创建CIFS服务器、则必须重新创建SMB共享。

相关信息

使用 SMB 管理文件访问

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

在卷上配置用于 SMB 文件名转换的字符映射

什么是默认管理共享

在Storage Virtual Machine (SVM)上创建CIFS服务器时、系统会自动创建默认管理共享。您应了解这些默认共享是什么以及如何使用它们。

在创建 CIFS 服务器时， ONTAP 会创建以下默认管理共享：

> 从ONTAP 9.8开始、默认情况下不再创建admin$共享。

- ipc$
- admin$(仅限ONTAP 9.7及更早版本)
- C$

由于以 $ 字符结尾的共享是隐藏共享，因此默认管理共享在 " 我的电脑 " 中不可见，但您可以使用共享文件夹查看它们。

如何使用 **ipc$** 和 **admin$** 默认共享

ipc$ 和 admin$ 共享由 ONTAP 使用， Windows 管理员无法使用这些共享访问驻留在 SVM 上的数据。

- ipc$ 共享

  ipc$ 共享是一种共享命名管道的资源，这些管道对于程序之间的通信至关重要。ipc$ 共享用于远程管理计算机和查看计算机的共享资源。您不能更改 ipc$ 共享的共享设置，共享属性或 ACL 。您也不能重命名或删除 ipc$ 共享。

- admin$共享(仅限ONTAP 9.7及更早版本)

  > 从ONTAP 9.8开始、默认情况下不再创建admin$共享。

  admin$ 共享用于远程管理 SVM 。此资源的路径始终是 SVM 根的路径。您不能更改 admin$ 共享的共享设置，共享属性或 ACL 。您也不能重命名或删除 admin$ 共享。

如何使用 **c$** 默认共享

c$ 共享是一个管理共享，集群或 SVM 管理员可以使用它来访问和管理 SVM 根卷。

以下是 c$ 共享的特征：

- 此共享的路径始终是 SVM 根卷的路径，无法修改。
- c$ 共享的默认 ACL 为管理员 / 完全控制。

  此用户为 BUILTIN\administrator 。默认情况下， BUILTIN\administrator 可以映射到共享，并查看，创建，修改或删除映射的根目录中的文件和文件夹。管理此目录中的文件和文件夹时，应谨慎。

- 您可以更改 c$ 共享的 ACL 。
- 您可以更改 c$ 共享设置和共享属性。
- 您不能删除 c$ 共享。
- SVM 管理员可以通过跨越命名空间接合从映射的 c$ 共享访问 SVM 命名空间的其余部分。
- 可以使用 Microsoft 管理控制台访问 c$ 共享。

相关信息

使用 Windows 安全性选项卡配置高级 NTFS 文件权限

SMB 共享命名要求

在 SMB 服务器上创建 ONTAP 共享时，应牢记 SMB 共享命名要求。

ONTAP 的共享命名约定与 Windows 相同，其中包括以下要求：

- 每个共享的名称对于 SMB 服务器必须是唯一的。
- 共享名称不区分大小写。
- 最大共享名称长度为 80 个字符。
- 支持 Unicode 共享名称。
- 以 $ 字符结尾的共享名称是隐藏的共享。
- 对于ONTAP 9.7及更早版本、系统会自动在每个CIFS服务器上创建admin$、ipc$和c$管理共享、这些共享是保留的共享名称。从ONTAP 9.8开始、不再自动创建admin$共享。
- 创建共享时，不能使用共享名称 ontap_admin$ 。
- 支持包含空格的共享名称：
  - 不能使用空格作为共享名称中的第一个字符或最后一个字符。
  - 必须将包含空格的共享名称用引号括起来。

    单引号被视为共享名称的一部分，不能代替引号。

- 命名 SMB 共享时，支持以下特殊字符：

  ！ @ # $ % & ' _ - 。~ （） { }

- 命名 SMB 共享时不支持以下特殊字符：
  - " / \ : ; _ < > , ? * =

在多协议环境中创建共享时的目录区分大小写要求

如果您在 SVM 中创建共享，并使用 8.3 命名方案来区分名称之间只有大小写差异的目录名称，则必须在共享路径中使用 8.3 名称，以确保客户端连接到所需的目录路径。

在以下示例中，在 Linux 客户端上创建了两个名为 "`testdir` " 和 "`testdir` " 的目录。包含这些目录的卷的接合路径为 `/home`。第一个输出来自 Linux 客户端，第二个输出来自 SMB 客户端。

```
 ls -l
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:24 TESTDIR
```

```
dir

 Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

在向第二个目录创建共享时，必须在共享路径中使用 8.3 名称。在此示例中、第一个目录的共享路径为 `/home/testdir` 第二个目录的共享路径为 `/home/TESTDI~1`。

使用 **SMB** 共享属性

使用 **SMB** 共享属性概述

您可以自定义 SMB 共享的属性。

可用的共享属性如下：

共享属性	**Description**
`oplocks`	此属性指定共享使用机会锁，也称为客户端缓存。
`browsable`	此属性允许 Windows 客户端浏览共享。
`showsnapshot`	此属性指定客户端可以查看和遍历 Snapshot 副本。
`changenotify`	此属性指定共享支持更改通知请求。对于 SVM 上的共享，这是默认的初始属性。
`attributecache`	通过此属性，可以在 SMB 共享上缓存文件属性，从而加快属性访问速度。默认情况下，禁用属性缓存。只有当有客户端通过 SMB 1.0 连接到共享时，才应启用此属性。如果客户端通过 SMB 2.x 或 SMB 3.0 连接到共享，则此共享属性不适用。
`continuously-available`	此属性允许支持它的 SMB 客户端以持久方式打开文件。以这种方式打开的文件不会受到故障转移和交还等中断事件的影响。
`branchcache`	此属性指定共享允许客户端对此共享中的文件请求 BranchCache 哈希。只有在 CIFS BranchCache 配置中将 "`per-share` " 指定为操作模式时，此选项才有用。

共享属性	Description
`access-based-enumeration`	此属性指定已在此共享上启用 _Access Based 枚举 _（ABE）。用户可以根据用户的访问权限查看 ABE 筛选的共享文件夹，从而防止显示用户无权访问的文件夹或其他共享资源。
`namespace-caching`	此属性指定连接到此共享的 SMB 客户端可以缓存 CIFS 服务器返回的目录枚举结果，从而提高性能。默认情况下， SMB 1 客户端不会缓存目录枚举结果。由于默认情况下 SMB 2 和 SMB 3 客户端会缓存目录枚举结果，因此指定此共享属性仅会为 SMB 1 客户端连接提供性能优势。
`encrypt-data`	此属性指定访问此共享时必须使用 SMB 加密。访问 SMB 数据时不支持加密的 SMB 客户端将无法访问此共享。

在现有 **SMB** 共享上添加或删除共享属性

您可以通过添加或删除共享属性来自定义现有 SMB 共享。如果您要更改共享配置以满足环境中不断变化的要求，此功能将非常有用。

开始之前

要修改其属性的共享必须存在。

关于此任务

添加共享属性的准则：

- 您可以使用逗号分隔列表添加一个或多个共享属性。
- 先前指定的任何共享属性仍有效。

  新添加的属性将附加到现有共享属性列表中。

- 如果为已应用于共享的共享属性指定新值，则新指定的值将替换原始值。
- 您不能使用删除共享属性 `vserver cifs share properties add` 命令：

  您可以使用 `vserver cifs share properties remove` 命令以删除共享属性。

删除共享属性的准则：

- 您可以使用逗号分隔列表删除一个或多个共享属性。
- 先前指定但未删除的任何共享属性仍有效。

步骤

1. 输入相应的命令：

如果您要 ...	输入命令 ...
添加共享属性	`vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`
删除共享属性	`vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`

2. 验证共享属性设置：`vserver cifs share show -vserver vserver_name -share-name share_name`

示例

以下命令将添加 `showsnapshot` 将共享属性分配给SVM VS1上名为`shre1`的共享：

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share1  /share1   oplocks      -          Everyone / Full
Control
                             browsable
                             changenotify
                             showsnapshot
```

以下命令将删除 `browsable` SVM VS1上名为`shre2`的共享中的共享属性：

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share2  /share2   oplocks      -          Everyone / Full
Control
                             changenotify
```

相关信息

用于管理 SMB 共享的命令

使用强制组共享设置优化 SMB 用户访问

在从 ONTAP 命令行创建共享以存储具有 UNIX 有效安全性的数据时，您可以指定由该共享中的 SMB 用户创建的所有文件属于同一个组，称为 *force-group* ，该组必须是 UNIX 组数据库中的预定义组。使用强制组可以更轻松地确保属于不同组的 SMB 用户可以访问文件。

只有当共享位于 UNIX 或混合 qtree 中时，指定强制组才有意义。无需为 NTFS 卷或 qtree 中的共享设置强制组，因为这些共享中的文件访问由 Windows 权限而不是 UNIX GID 决定。

如果为共享指定了强制组，则共享的以下内容将变为 true：

- 强制组中访问此共享的 SMB 用户将临时更改为强制组的 GID 。

  通过此 GID ，他们可以访问此共享中无法通过其主 GID 或 UID 正常访问的文件。

- 无论文件所有者的主 GID 如何， SMB 用户创建的此共享中的所有文件都属于同一个强制组。

当 SMB 用户尝试访问 NFS 创建的文件时， SMB 用户的主 GID 将确定访问权限。

强制组不会影响 NFS 用户访问此共享中文件的方式。NFS 创建的文件从文件所有者获取 GID 。访问权限的确定取决于尝试访问文件的 NFS 用户的 UID 和主 GID 。

使用强制组可以更轻松地确保属于不同组的 SMB 用户可以访问文件。例如，如果您要创建一个共享来存储公司的网页并为工程和营销部门的用户授予写入访问权限，则可以创建一个共享并为名为 "`webgroup1` " 的强制组授予写入访问权限。由于使用强制组， SMB 用户在此共享中创建的所有文件均归 "`webgroup1` " 组所有。此外，在访问共享时，系统会自动为用户分配 "`webgroup1` " 组的 GID 。因此，所有用户都可以写入此共享，而无需管理工程和营销部门中用户的访问权限。

相关信息

使用 force-group 共享设置创建 SMB 共享

使用 force-group 共享设置创建 SMB 共享

如果您希望 ONTAP 将访问具有 UNIX 文件安全性的卷或 qtree 上的数据的 SMB 用户视为属于同一 UNIX 组，则可以使用强制组共享设置创建 SMB 共享。

步骤

1. 创建SMB共享： `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path path -force-group-for-create` *`UNIX_group_name`*

   如果为UNC路径 (`\\servername\sharename\filepath`)包含超过256个字符(不包括初始"`\\`")，则Windows属性框中的*Security*选项卡不可用。这是 Windows 客户端问题描述，而不是 ONTAP 问题描述。要避免此问题描述，请勿使用超过 256 个字符的 UNC 路径创建共享。

   如果要在创建共享后删除强制组、则可以随时修改共享并指定空字符串("")作为的值 `-force-group-for-create` 参数。如果通过修改共享来删除 force-group ，则此共享的所有现有连接仍将使用先前设置的 force-group 作为主 GID 。

示例

以下命令将创建一个"`webpages`"共享、此共享可通过中的Web进行访问 `/corp/companyinfo` 将SMB用户创建的所有文件分配给webgroup1组的目录：

```
vserver cifs share create -vserver vs1 -share-name webpages -path
/corp/companyinfo -force-group-for-create webgroup1
```

相关信息

使用强制组共享设置优化 SMB 用户访问

使用 MMC 查看有关 SMB 共享的信息

您可以使用 Microsoft 管理控制台（ MMC ）查看 SVM 上的 SMB 共享信息并执行某些管理任务。在查看共享之前，您需要将 MMC 连接到 SVM 。

关于此任务

您可以使用 MMC 对 SVM 中包含的共享执行以下任务：

- 查看共享
- 查看活动会话
- 查看打开的文件
- 枚举系统中的会话，文件和树连接列表
- 关闭系统中已打开的文件
- 关闭打开的会话
- 创建 / 管理共享

> 上述功能显示的视图是特定于节点的视图，而不是特定于集群的视图。因此，在使用 MMC 连接到 SMB 服务器主机名（即 cifs01.domain.local ）时，系统会根据 DNS 设置方式将您路由到集群中的单个 LIF 。

适用于 ONTAP 的 MMC 不支持以下功能：

- 创建新的本地用户 / 组
- 管理 / 查看现有本地用户 / 组
- 查看事件或性能日志
- 存储
- 服务和应用程序

在不支持此操作的情况下、您可能会遇到这种情况 `remote procedure call failed` 错误。

"常见问题解答：在 ONTAP 中使用 Windows MMC"

步骤

1. 要在任何 Windows 服务器上打开计算机管理 MMC ，请在 * 控制面板 * 中选择 * 管理工具 * > * 计算机管理 * 。

2. 选择 * 操作 * > * 连接到另一台计算机 * 。

   此时将显示选择计算机对话框。

3. 键入存储系统的名称或单击 * 浏览 * 以查找存储系统。
4. 单击 * 确定 * 。

   MMC 连接到 SVM 。

5. 在导航窗格中，单击 * 共享文件夹 * > * 共享 * 。

   SVM 上的共享列表将显示在右侧显示窗格中。

6. 要显示共享的共享属性，请双击该共享以打开 * 属性 * 对话框。
7. 如果无法使用 MMC 连接到存储系统，则可以在存储系统上使用以下命令之一将用户添加到 BUILTIN\Administrators 组或 BUILTIN\Power Users 组：

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

用于管理 SMB 共享的命令

您可以使用 `vserver cifs share` 和 `vserver cifs share properties` 用于管理SMB共享的命令。

如果您要 ...	使用此命令 ...
创建 SMB 共享	`vserver cifs share create`
显示 SMB 共享	`vserver cifs share show`
修改 SMB 共享	`vserver cifs share modify`
删除 SMB 共享	`vserver cifs share delete`
向现有共享添加共享属性	`vserver cifs share properties add`
从现有共享中删除共享属性	`vserver cifs share properties remove`
显示有关共享属性的信息	`vserver cifs share properties show`

有关详细信息，请参见每个命令的手册页。

使用 SMB 共享 ACL 确保文件访问安全

管理 SMB 共享级 ACL 的准则

您可以更改共享级 ACL ，为用户授予对共享的或多或少的访问权限。您可以使用 Windows 用户和组或 UNIX 用户和组配置共享级 ACL 。

默认情况下，创建共享后，共享级 ACL 会为名为 Everyone 的标准组授予读取访问权限。ACL 中的读取访问权限意味着域和所有受信任域中的所有用户都对共享具有只读访问权限。

您可以使用 Windows 客户端上的 Microsoft 管理控制台（ MMC ）或 ONTAP 命令行更改共享级别 ACL 。

使用 MMC 时，请遵循以下准则：

- 指定的用户名和组名必须为 Windows 名称。
- 您只能指定 Windows 权限。

使用 ONTAP 命令行时，请遵循以下准则：

- 指定的用户和组名称可以是 Windows 名称或 UNIX 名称。

  如果在创建或修改 ACL 时未指定用户和组类型，则默认类型为 Windows 用户和组。

- 您只能指定 Windows 权限。

创建 SMB 共享访问控制列表

通过为 SMB 共享创建访问控制列表（ ACL ）来配置共享权限，可以控制用户和组对共享的访问级别。

关于此任务

您可以使用本地或域 Windows 用户或组名称或 UNIX 用户或组名称来配置共享级 ACL 。

在创建新ACL之前、应删除默认共享ACL `Everyone / Full Control`，这会带来安全风险。

在工作组模式下，本地域名为 SMB 服务器名称。

步骤

1. 删除默认共享ACL：`vserver cifs share access-control delete -vserver` *`vserver_name`* `-share` *`share_name`*`-user-or-group Everyone`
2. 配置新 ACL ：

如果要使用配置 **ACL**，请使用 ...	输入命令 ...
Windows 用户	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_domain_name\user_name`* `-permission` *`access_right`*
Windows 组	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_domain_name\group_name`* `-permission` *`access_right`*
UNIX 用户	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type` *`unix-user`* `-user-or-group` *`UNIX_user_name`* `-permission access_right`
UNIX 组	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type` *`unix-group`* `-user-or-group` *`UNIX_group_name`* `-permission access_right`

3. 使用验证应用于共享的ACL是否正确 `vserver cifs share access-control show` 命令：

示例

以下命令提供 `Change` 在"`Svs1.example.coms`"SVM：

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
                 Share       User/Group              User/Group  Access
Vserver          Name        Name                    Type
Permission
---------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\Sales Team     windows     Change
```

以下命令提供 `Read` 对"`vs2.example.com`"SVM：

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                 Share       User/Group                User/Group  Access
Vserver          Name        Name                      Type
Permission
---------------- ----------- --------------------      -----------
-----------
vs2.example.com  c$          BUILTIN\Administrators   windows
Full_Control
vs2.example.com  eng         engineering              unix-group  Read
```

以下命令提供 `Change` 对名为"`Tiger Team`"和的本地Windows组的权限 `Full_Control` 对`Svs1d`"SVM：

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    Tiger Team         windows     Change
vs1            datavol5    Sue Chang          windows     Full_Control
```

用于管理 SMB 共享访问控制列表的命令

您需要了解用于管理 SMB 访问控制列表（ACL）的命令，其中包括创建，显示，修改和删除这些列表。

如果您要 ...	使用此命令 ...
创建新ACL	`vserver cifs share access-control create`
显示 ACL	`vserver cifs share access-control show`
修改 ACL	`vserver cifs share access-control modify`
删除 ACL	`vserver cifs share access-control delete`

使用文件权限确保文件访问安全

使用 Windows 安全性选项卡配置高级 NTFS 文件权限

您可以使用 Windows 属性窗口中的 * Windows 安全性 * 选项卡配置文件和文件夹的标准 NTFS 文件权限。

开始之前

执行此任务的管理员必须具有足够的 NTFS 权限才能更改对选定对象的权限。

关于此任务

通过向与 NTFS 安全描述符关联的 NTFS 随机访问控制列表（ DACL ）添加条目，可以在 Windows 主机上配置 NTFS 文件权限。然后，安全描述符将应用于 NTFS 文件和目录。这些任务由 Windows 图形用户界面自动处理。

步骤

1. 从 Windows 资源管理器的 * 工具 * 菜单中，选择 * 映射网络驱动器 * 。
2. 完成 * 映射网络驱动器 * 对话框：
   a. 选择一个 * 驱动器 * 字母。
   b. 在 * 文件夹 * 框中，键入包含要应用权限的数据的共享的 CIFS 服务器名称以及共享的名称。

      如果CIFS服务器名称为"`CIFS_SERVER`"、而共享名为"`shre1`"、则应键入 `\\CIFS_SERVER\share1`。

      > 您可以为 CIFS 服务器指定数据接口的 IP 地址，而不是 CIFS 服务器名称。

   c. 单击 * 完成 * 。

   您选择的驱动器已挂载并准备就绪，此时将显示 Windows 资源管理器窗口，其中显示共享中包含的文件和文件夹。
3. 选择要为其设置 NTFS 文件权限的文件或目录。
4. 右键单击文件或目录，然后选择 * 属性 * 。
5. 选择 * 安全性 * 选项卡。
   - 安全性 * 选项卡显示设置了 NTFS 权限的用户和组的列表。* 权限 * 框显示了对选定的每个用户或组有效的允许和拒绝权限列表。
6. 单击 * 高级 * 。

   Windows 属性窗口显示有关分配给用户和组的现有文件权限的信息。
7. 单击 * 更改权限 * 。

   此时将打开权限窗口。
8. 执行所需的操作：

如果您要 ...	执行以下操作 ...
为新用户或组设置高级 NTFS 权限	a. 单击 * 添加 * 。 b. 在 * 输入要选择的对象名称 * 框中，键入要添加的用户或组的名称。 c. 单击 * 确定 * 。

如果您要 ...	执行以下操作 ...
更改用户或组的高级 NTFS 权限	a. 在 * 权限条目： * 框中，选择要更改其高级权限的用户或组。 b. 单击 * 编辑 * 。
删除用户或组的高级 NTFS 权限	a. 在 * 权限条目： * 框中，选择要删除的用户或组。 b. 单击 * 删除 * 。 c. 跳至步骤 13 。

如果要为新用户或组添加高级 NTFS 权限，或者更改现有用户或组的 NTFS 高级权限，则会打开 < 对象 > 的权限条目框。

9. 在 * 应用于 * 框中，选择要如何应用此 NTFS 文件权限条目。

   如果要对单个文件设置 NTFS 文件权限，则 * 应用于 * 框不会处于活动状态。* 应用于 * 设置默认为 * 仅此对象 * 。

10. 在 * 权限 * 框中，为要对此对象设置的高级权限选择 * 允许 * 或 * 拒绝 * 框。

    - 要允许指定的访问，请选中 * 允许 * 框。
    - 要不允许指定的访问，请选中 * 拒绝 * 框。 您可以对以下高级权限设置权限：
    - * 完全控制 *

      如果选择此高级权限，则会自动选择所有其他高级权限（允许或拒绝权限）。

    - * 遍历文件夹 / 执行文件 *
    - * 列出文件夹 / 读取数据 *
    - * 读取属性 *
    - * 读取扩展属性 *
    - * 创建文件 / 写入数据 *
    - * 创建文件夹 / 附加数据 *
    - * 写入属性 *
    - * 写入扩展属性 *
    - * 删除子文件夹和文件 *
    - * 删除 *
    - * 读取权限 *
    - * 更改权限 *
    - * 取得所有权 *

    如果任何高级权限框不可选，则是因为权限是从父对象继承的。

11. 如果希望此对象的子文件夹和文件继承这些权限，请选中 * 仅将这些权限应用于此容器中的对象和 / 或容器 * 框。
12. 单击 * 确定 * 。
13. 添加，删除或编辑完 NTFS 权限后，请为此对象指定继承设置：
    - 选中 * 包括此对象父级的可继承权限 * 框。

      这是默认值。
    - 选中 * 将所有子对象权限替换为此对象的可继承权限 * 框。

      如果要对单个文件设置 NTFS 文件权限，则权限框中不存在此设置。

      > 选择此设置时请务必小心。此设置将删除所有子对象的所有现有权限，并将其替换为此对象的权限设置。您可能会无意中删除不希望删除的权限。在混合安全模式卷或 qtree 中设置权限时尤其重要。如果子对象采用 UNIX 有效安全模式，则将 NTFS 权限传播到这些子对象会导致 ONTAP 将这些对象从 UNIX 安全模式更改为 NTFS 安全模式，并且这些子对象上的所有 UNIX 权限将替换为 NTFS 权限。
    - 选择这两个框。
    - 不选择任何一个框。
14. 单击 * 确定 * 关闭 * 权限 * 框。
15. 单击 * 确定 * 以关闭 * 对象 * 的高级安全设置框。

有关如何设置高级 NTFS 权限的详细信息，请参见 Windows 文档。

相关信息

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

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

显示 UNIX 安全模式卷上的文件安全性信息

使用 **ONTAP** 命令行界面配置 **NTFS** 文件权限

您可以使用 ONTAP 命令行界面为文件和目录配置 NTFS 文件权限。这样，您就可以配置 NTFS 文件权限，而无需使用 Windows 客户端上的 SMB 共享连接到数据。

您可以通过向与 NTFS 安全描述符关联的 NTFS 随机访问控制列表（ DACL ）添加条目来配置 NTFS 文件权限。然后，安全描述符将应用于 NTFS 文件和目录。

您只能使用命令行配置 NTFS 文件权限。您不能使用命令行界面配置 NFSv4 ACL 。

步骤

1. 创建NTFS安全描述符。

```
vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
ntfs_security_descriptor_name -owner owner_name -group primary_group_name
-control-flags-raw raw_control_flags
```

2. 将DACL添加到NTFS安全描述符。

```
vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
-rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
{this-folder|sub-folders|files}
```

3. 创建文件/目录安全策略。

```
vserver security file-directory policy create -vserver svm_name -policy-name
policy_name
```

通过 SMB 访问文件时， UNIX 文件权限如何提供访问控制

FlexVol 卷可以采用以下三种安全模式之一： NTFS ， UNIX 或混合。无论安全模式如何，您都可以通过 SMB 访问数据；但是，要以 UNIX 有效安全模式访问数据，需要适当的 UNIX 文件权限。

通过 SMB 访问数据时，在确定用户是否有权执行请求的操作时，会使用多种访问控制：

- 导出权限

  配置 SMB 访问的导出权限是可选的。

- 共享权限
- 文件权限

  以下类型的文件权限可能会应用于用户要执行操作的数据：

  - NTFS
  - UNIX NFSv4 ACL
  - UNIX 模式位

对于设置了 NFSv4 ACL 或 UNIX 模式位的数据，将使用 UNIX 模式权限来确定对数据的文件访问权限。SVM 管理员需要设置适当的文件权限，以确保用户有权执行所需的操作。

> 混合安全模式卷中的数据可能采用 NTFS 或 UNIX 有效安全模式。如果数据采用 UNIX 有效安全模式，则在确定数据的文件访问权限时会使用 NFSv4 权限或 UNIX 模式位。

使用动态访问控制（ DAC ）确保文件访问安全

使用动态访问控制（ DAC ）概述确保文件访问安全

您可以使用动态访问控制来保护访问安全，也可以在 Active Directory 中创建中央访问策略

，并通过已应用的组策略对象（ GPO ）将这些策略应用于 SVM 上的文件和文件夹。您可以配置审核，以便在应用对中央访问策略所做的更改之前，使用中央访问策略暂存事件查看这些更改的影响。

CIFS 凭据的附加项

在动态访问控制之前， CIFS 凭据包括安全主体（用户）的身份和 Windows 组成员资格。通过动态访问控制，凭据中又添加了三种类型的信息：设备标识，设备声明和用户声明：

- 设备标识

  模拟用户的身份信息，但用户登录设备的身份和组成员资格除外。

- 设备声明

  有关设备安全主体的断言。例如，设备声明可能是它是特定 OU 的成员。

- 用户声明

  有关用户安全主体的断言。例如，用户声明可能是其 AD 帐户是特定 OU 的成员。

中央访问策略

通过文件的中央访问策略，组织可以使用用户组，用户声明，设备声明和资源属性集中部署和管理包括条件表达式在内的授权策略。

例如，要访问对业务影响较高的数据，用户必须是全职员工，并且只能从受管设备访问数据。中央访问策略在 Active Directory 中定义，并通过 GPO 机制分发到文件服务器。

具有高级审核功能的中央访问策略暂存

中央访问策略可以是 " `stated` " ，在这种情况下，在文件访问检查期间会以 "`what - if` " 的方式对其进行评估。如果策略有效，会发生什么情况以及这与当前配置有何不同，则会将结果记录为审核事件。通过这种方式，管理员可以使用审核事件日志来研究访问策略更改的影响，然后再实际应用该策略。在评估访问策略更改的影响后，可以通过 GPO 将此策略部署到所需的 SVM 。

相关信息

支持的 GPO

将组策略对象应用于 CIFS 服务器

在 CIFS 服务器上启用或禁用 GPO 支持

显示有关 GPO 配置的信息

显示有关中央访问策略的信息

显示有关中央访问策略规则的信息

配置中央访问策略以保护 CIFS 服务器上的数据安全

显示有关动态访问控制安全性的信息

"SMB 和 NFS 审核和安全跟踪"

支持的动态访问控制功能

如果要在 CIFS 服务器上使用动态访问控制（DAC），则需要了解 ONTAP 如何在 Active Directory 环境中支持动态访问控制功能。

支持动态访问控制

在 CIFS 服务器上启用动态访问控制时， ONTAP 支持以下功能：

功能	注释
声明到文件系统	声明是简单的名称和值对，用于说明有关用户的一些事实。用户凭据包含声明信息、文件上的安全描述符可以执行包括声明检查在内的访问检查。这样，管理员可以更精细地控制谁可以访问文件。
文件访问检查的条件表达式	修改文件的安全参数时、用户可以将任意复杂的条件表达式添加到文件的安全描述符中。条件表达式可以包括对声明的检查。
通过中央访问策略集中控制文件访问	中央访问策略是存储在 Active Directory 中的一种 ACL，可以标记为文件。只有在磁盘上的安全描述符和带标记的中央访问策略的访问检查均允许访问时，才会授予对文件的访问权限。这样，管理员便可以从中央位置（AD）控制对文件的访问，而无需修改磁盘上的安全描述符。
中央访问策略暂存	增加了在不影响实际文件访问的情况下尝试安全更改的功能，方法是 " `staging` " 对中央访问策略的更改，并在审核报告中查看更改的影响。
支持使用 ONTAP 命令行界面显示有关中央访问策略安全性的信息	扩展 `vserver security file-directory show` 命令以显示有关应用的中央访问策略的信息。
包括中央访问策略的安全跟踪	扩展 `vserver security trace` 命令系列、以显示包含应用的中央访问策略相关信息的结果。

不支持动态访问控制

在 CIFS 服务器上启用动态访问控制时， ONTAP 不支持以下功能：

功能	注释
NTFS 文件系统对象的自动分类	这是 ONTAP 不支持的 Windows 文件分类基础架构的扩展。
除中央访问策略暂存之外的高级审核	高级审核仅支持中央访问策略暂存。

对 **CIFS** 服务器使用动态访问控制和中央访问策略时的注意事项

在使用动态访问控制（DAC）和中央访问策略保护 CIFS 服务器上的文件和文件夹时，必须牢记一些注意事项。

如果策略规则为适用场景 **domain\administrator user**，则可以拒绝对 **root** 的 **NFS** 访问

在某些情况下，如果对 root 用户尝试访问的数据应用中央访问策略安全性，则可能会拒绝 NFS 对 root 的访问。如果中央访问策略包含应用于域 \ 管理员且根帐户映射到域 \ 管理员帐户的规则，则会发生问题描述。

您应将规则应用于具有管理权限的组，例如 domain\administrator 组，而不是将规则应用于 domain\administrator 用户。通过这种方式，您可以将 root 映射到域 \ 管理员帐户，而不会使 root 受到此问题描述的影响。

如果在**Active Directory**中找不到应用的中央访问策略、则**CIFS**服务器的**BUILTIN\Administrators**组可以访问资源

CIFS 服务器中包含的资源可能已应用中央访问策略，但当 CIFS 服务器使用中央访问策略的 SID 尝试从 Active Directory 检索信息时， SID 与 Active Directory 中的任何现有中央访问策略 SID 不匹配。在这些情况下， CIFS 服务器会对该资源应用本地默认恢复策略。

本地默认恢复策略允许 CIFS 服务器的 BUILTIN\Administrators 组访问该资源。

启用或禁用动态访问控制概述

默认情况下，用于使用动态访问控制（DAC）保护 CIFS 服务器上的对象的选项处于禁用状态。如果要在 CIFS 服务器上使用动态访问控制，则必须启用此选项。如果您稍后决定不使用动态访问控制来保护存储在 CIFS 服务器上的对象，则可以禁用此选项。

关于此任务

启用动态访问控制后，文件系统可以包含具有与动态访问控制相关的条目的 ACL 。如果禁用了动态访问控制，则会忽略当前的动态访问控制条目，并且不允许输入新条目。

此选项仅在高级权限级别可用。

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：

动态访问控制的目标位置	输入命令 …

enabled	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled true`
已禁用	`vserver cifs options modify -vserver` *`vserver_name`* `-is-dac-enabled false`

3. 返回到管理员权限级别： `set -privilege admin`

相关信息

配置中央访问策略以保护 CIFS 服务器上的数据安全

禁用动态访问控制时，管理包含动态访问控制 ACE 的 ACL

如果您的资源使用动态访问控制 ACE 应用 ACL ，并且您在 Storage Virtual Machine （ SVM ）上禁用了动态访问控制，则必须先删除动态访问控制 ACE ，然后才能管理该资源上的非动态访问控制 ACE 。

关于此任务

禁用动态访问控制后，在删除现有动态访问控制 ACE 之前，您无法删除现有的非动态访问控制 ACE 或添加新的非动态访问控制 ACE 。

您可以使用通常用于管理 ACL 的任何工具来执行这些步骤。

步骤

1. 确定对资源应用了哪些动态访问控制 ACE 。
2. 从资源中删除动态访问控制 ACE 。
3. 根据需要在资源中添加或删除非动态访问控制 ACE 。

配置中央访问策略以保护 CIFS 服务器上的数据安全

要使用中央访问策略保护对 CIFS 服务器上数据的访问，您必须执行几个步骤，包括在 CIFS 服务器上启用动态访问控制（ DAC ），在 Active Directory 中配置中央访问策略，将中央访问策略应用于具有 GPO 的 Active Directory 容器， 并在 CIFS 服务器上启用 GPO 。

开始之前

- 必须将 Active Directory 配置为使用中央访问策略。
- 您必须对 Active Directory 域控制器具有足够的访问权限，才能创建中央访问策略，并创建 GPO 并将其应用于包含 CIFS 服务器的容器。
- 您必须对 Storage Virtual Machine （ SVM ）具有足够的管理访问权限才能执行必要的命令。

关于此任务

中央访问策略已定义并应用于 Active Directory 上的组策略对象（ GPO ）。有关配置中央访问策略和 GPO 的说明，请参见 Microsoft TechNet 库。

"Microsoft TechNet 库"

步骤

1. 如果尚未使用启用动态访问控制、请在SVM上启用它 `vserver cifs options modify` 命令：

   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. 如果尚未使用启用组策略对象(GPO)、请在CIFS服务器上启用它们 `vserver cifs group-policy modify` 命令：

   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. 在 Active Directory 上创建中央访问规则和中央访问策略。
4. 创建组策略对象（ GPO ）以在 Active Directory 上部署中央访问策略。
5. 将 GPO 应用于 CIFS 服务器计算机帐户所在的容器。
6. 使用手动更新应用于CIFS服务器的GPO `vserver cifs group-policy update` 命令：

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. 使用验证是否已将GPO中央访问策略应用于CIFS服务器上的资源 `vserver cifs group-policy show-applied` 命令：

   以下示例显示默认域策略具有两个应用于 CIFS 服务器的中央访问策略：

   ```
   vserver cifs group-policy show-applied
   ```

   ```
   Vserver: vs1
   ----------------------------
       GPO Name: Default Domain Policy
          Level: Domain
         Status: enabled
     Advanced Audit Settings:
         Object Access:
             Central Access Policy Staging: failure
     Registry Settings:
         Refresh Time Interval: 22
         Refresh Random Offset: 8
         Hash Publication Mode for BranchCache: per-share
         Hash Version Support for BranchCache: all-versions
     Security Settings:
         Event Audit and Event Log:
             Audit Logon Events: none
             Audit Object Access: success
             Log Retention Method: overwrite-as-needed
             Max Log Size: 16384
         File Security:
             /vol1/home
   ```

```
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
```

```
        Privilege Rights:
            Take Ownership: usr1, usr2
            Security Privilege: usr1, usr2
            Change Notify: usr1, usr2
        Registry Values:
            Signing Required: false
        Restrict Anonymous:
            No enumeration of SAM accounts: true
            No enumeration of SAM accounts and shares: false
            Restrict anonymous access to shares and named pipes: true
            Combined restriction for anonymous user: no-access
        Restricted Groups:
            gpr1
            gpr2
    Central Access Policy Settings:
        Policies: cap1
                  cap2
 2 entries were displayed.
```

相关信息

显示有关 GPO 配置的信息

显示有关中央访问策略的信息

显示有关中央访问策略规则的信息

启用或禁用动态访问控制

显示有关动态访问控制安全性的信息

您可以显示 NTFS 卷上的动态访问控制（DAC）安全性信息，以及混合安全模式卷上使用 NTFS 有效安全性的数据信息。其中包括有关条件 ACE，资源 ACE 和中央访问策略 ACE 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。

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`

要显示信息的项	输入以下命令 ...
扩展了详细信息	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
其中输出显示有组和用户 SID	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
关于十六进制位掩码转换为文本格式的文件和目录的文件和目录安全性	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

示例

以下示例显示了有关路径的动态访问控制安全信息 `/vol1` 在SVM VS1中：

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
                  File Inode Number: 112
                     Security Style: mixed
                    Effective Style: ntfs
                     DOS Attributes: 10
             DOS Attributes in Text: ----D---
             Expanded Dos Attribute: -
                       Unix User Id: 0
                      Unix Group Id: 1
                     Unix Mode Bits: 777
             Unix Mode Bits in Text: rwxrwxrwx
                               ACLs: NTFS Security Descriptor
                                     Control:0xbf14
                                     Owner:CIFS1\Administrator
                                     Group:CIFS1\Domain Admins
                                     SACL - ACEs
                                        ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                        RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                        POLICY ID-All resources - No Write-
0x0-OI|CI
                                     DACL - ACEs
                                        ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                        ALLOW-Everyone-0x1f01ff-OI|CI
                                        ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

相关信息

显示有关 GPO 配置的信息

显示有关中央访问策略的信息

显示有关中央访问策略规则的信息

动态访问控制的还原注意事项

您应了解还原到不支持动态访问控制（DAC）的 ONTAP 版本时会发生什么情况，以及还原前后必须执行哪些操作。

如果要将集群还原到不支持动态访问控制的 ONTAP 版本，并且在一个或多个 Storage Virtual Machine （SVM）上启用了动态访问控制，则必须在还原之前执行以下操作：

- 您必须在集群上启用动态访问控制的所有 SVM 上禁用动态访问控制。
- 您必须修改包含的集群上的任何审核配置 `cap-staging` 仅使用的事件类型 `file-op` 事件类型。

对于具有动态访问控制 ACE 的文件和文件夹，您必须了解一些重要的还原注意事项并采取相应措施：

- 如果还原集群，则不会删除现有动态访问控制 ACE ；但是，在文件访问检查中将忽略这些 ACE 。
- 由于还原后将忽略动态访问控制 ACE ，因此使用动态访问控制 ACE 的文件将更改对文件的访问。

  这样，用户就可以访问以前无法访问的文件，或者无法访问以前可以访问的文件。

- 您应将非动态访问控制 ACE 应用于受影响的文件，以还原其先前的安全级别。

  可以在还原之前或还原完成后立即执行此操作。

> 由于还原后会忽略动态访问控制 ACE ，因此在将非动态访问控制 ACE 应用于受影响的文件时，您无需删除它们。但是，如果需要，您可以手动将其删除。

从何处查找有关配置和使用动态访问控制和中央访问策略的追加信息

我们还提供了其他资源来帮助您配置和使用动态访问控制和中央访问策略。

您可以在 Microsoft TechNet 库中找到有关如何在 Active Directory 上配置动态访问控制和中央访问策略的信息。

"Microsoft TechNet： 动态访问控制场景概述"

"Microsoft TechNet： 中央访问策略场景"

以下参考资料可帮助您将SMB服务器配置为使用和支持动态访问控制和中央访问策略：

- *在SMB服务器上使用GPO *

  将组策略对象应用于SMB服务器

- 在**SMB**服务器上配置**NAS**审核

  "SMB 和 NFS 审核和安全跟踪"

使用导出策略确保**SMB**访问安全

如何在 **SMB** 访问中使用导出策略

如果在SMB服务器上启用了SMB访问导出策略、则在控制SMB客户端对SVM卷的访问时会使用导出策略。要访问数据，您可以创建一个允许 SMB 访问的导出策略，然后将该策略与包含 SMB 共享的卷相关联。

导出策略应用了一个或多个规则，用于指定允许哪些客户端访问数据以及只读和读写访问支持哪些身份验证协议。您可以配置导出策略，以允许通过 SMB 访问所有客户端，一个子网客户端或特定客户端，并允许在确定对数据的只读和读写访问时使用 Kerberos 身份验证， NTLM 身份验证或 Kerberos 和 NTLM 身份验证进行身份验证。

在处理应用于导出策略的所有导出规则后， ONTAP 可以确定是否授予客户端访问权限以及授予的访问级别。导出规则适用于客户端计算机，而不适用于 Windows 用户和组。导出规则不会取代基于 Windows 用户和组的身份验证和授权。除了共享和文件访问权限之外，导出规则还提供了另一层访问安全性。

您只需将一个导出策略关联到每个卷，即可配置客户端对卷的访问。每个 SVM 可以包含多个导出策略。这样，您可以对包含多个卷的 SVM 执行以下操作：

- 为 SVM 的每个卷分配不同的导出策略，以便对 SVM 中的每个卷进行单个客户端访问控制。
- 为 SVM 的多个卷分配相同的导出策略，以实现相同的客户端访问控制，而无需为每个卷创建新的导出策略。

每个 SVM 至少有一个名为 `default` 的导出策略，该策略不包含任何规则。您不能删除此导出策略，但可以重命名或修改它。默认情况下， SVM 上的每个卷都与默认导出策略相关联。如果在 SVM 上禁用了 `d`访问导出策略，则 `"' 默认 ''` 导出策略对 SMB 访问没有任何影响。

您可以配置规则以提供对 NFS 和 SMB 主机的访问，并将该规则与导出策略关联，然后导出策略可以与包含 NFS 和 SMB 主机都需要访问的数据的卷关联。或者，如果某些卷中只有 SMB 客户端需要访问，则可以为导出策略配置规则，这些规则只允许使用 SMB 协议进行访问，并且仅使用 Kerberos 或 NTLM （或两者）进行只读和写访问身份验证。然后，导出策略将与只需要 SMB 访问的卷相关联。

如果启用了 SMB 的导出策略，并且客户端发出适用导出策略不允许的访问请求，则此请求将失败，并显示权限被拒绝的消息。如果客户端与卷导出策略中的任何规则不匹配，则访问将被拒绝。如果导出策略为空，则会隐式拒绝所有访问。即使共享和文件权限允许访问，也是如此。这意味着，您必须将导出策略配置为在包含 SMB 共享的卷上至少允许以下内容：

- 允许访问所有客户端或相应的部分客户端
- 允许通过 SMB 进行访问
- 允许使用 Kerberos 或 NTLM 身份验证（或这两者）进行适当的只读和写访问

了解相关信息 "配置和管理导出策略"。

导出规则的工作原理

导出规则是导出策略的功能要素。导出规则会根据您配置的特定参数将客户端对卷的访问请求进行匹配，以确定如何处理客户端访问请求。

导出策略必须至少包含一个导出规则，才能访问客户端。如果导出策略包含多个规则，则这些规则将按照它们在导出策略中的显示顺序进行处理。规则顺序由规则索引编号决定。如果某个规则与客户端匹配，则会使用该规则的权限，而不再处理其他规则。如果没有匹配的规则，客户端将被拒绝访问。

您可以使用以下条件配置导出规则以确定客户端访问权限：

- 发送请求的客户端使用的文件访问协议，例如 NFSv4 或 SMB 。
- 客户端标识符，例如主机名或 IP 地址。

的最大大小 `-clientmatch` 字段为4096个字符。

- 客户端用于进行身份验证的安全类型，例如 Kerberos v5 ， NTLM 或 AUTH_SYS 。

如果某个规则指定了多个条件，则客户端必须与所有条件匹配，才能应用此规则。

示例

导出策略包含具有以下参数的导出规则：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

客户端访问请求使用 NFSv3 协议发送，并且客户端的 IP 地址为 10.1.17.37 。

即使客户端访问协议匹配，客户端的 IP 地址也与导出规则中指定的 IP 地址位于不同的子网中。因此，客户端匹配失败，此规则不适用于此客户端。

示例

导出策略包含具有以下参数的导出规则：

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

客户端访问请求使用NFSv4协议发送、客户端的IP地址为10.1.16.54。

客户端访问协议匹配，并且客户端的 IP 地址位于指定子网中。因此，客户端匹配成功，此规则将适用场景此客户端。无论安全类型如何，客户端都可以获得读写访问权限。

示例

导出策略包含具有以下参数的导出规则：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

客户端 1 的 IP 地址为 10.1.16.207 ，使用 NFSv3 协议发送访问请求，并使用 Kerberos v5 进行身份验证。

客户端 2 的 IP 地址为 10.1.16.211 ，使用 NFSv3 协议发送访问请求，并使用 AUTH_SYS 进行身份验证。

这两个客户端的客户端访问协议和 IP 地址匹配。只读参数允许对所有客户端进行只读访问，而不管客户端使用哪种安全类型进行身份验证。因此，这两个客户端都将获得只读访问权限。但是，只有客户端 1 获得读写访问权限，因为它使用经过批准的安全类型 Kerberos v5 进行身份验证。客户端 2 不会获得读写访问权限。

限制或允许通过 SMB 进行访问的导出策略规则示例

这些示例显示了如何在启用了 SMB 访问导出策略的 SVM 上创建导出策略规则来限制或允许通过 SMB 进行访问。

默认情况下， SMB 访问的导出策略处于禁用状态。只有在为 SMB 访问启用了导出策略时，您才需要配置导出策略规则来限制或允许通过 SMB 进行访问。

仅适用于 SMB 访问的导出规则

以下命令会在名为 "`vs1` " 的 SVM 上创建一个导出规则，该规则具有以下配置：

- 策略名称： cifs1
- 索引号： 1
- 客户端匹配：仅匹配 192.168.1.0/24 网络上的客户端
- 协议：仅启用 SMB 访问
- 只读访问：使用 NTLM 或 Kerberos 身份验证的客户端
- 读写访问：使用 Kerberos 身份验证的客户端

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

SMB 和 NFS 访问的导出规则

以下命令会在名为 "` vs1` " 的 SVM 上创建一个导出规则，该规则具有以下配置：

- 策略名称： cifsnfs1.
- 索引编号：2
- 客户端匹配：匹配所有客户端
- 协议： SMB 和 NFS 访问
- 只读访问：对所有客户端
- 读写访问：使用 Kerberos （ NFS 和 SMB ）或 NTLM 身份验证（ SMB ）的客户端
- 映射 UNIX 用户 ID 0 （零）：映射到用户 ID 65534 （通常映射到用户名 nobody ）
- SUID 和 sgid 访问：允许

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule
any -rwrule krb5,ntlm -anon 65534 -allow-suid true
```

仅使用 **NTLM** 进行 **SMB** 访问的导出规则

以下命令会在名为 "`vs1` " 的 SVM 上创建一个导出规则，该规则具有以下配置：

- 策略名称：ntlm1
- 索引号： 1
- 客户端匹配：匹配所有客户端
- 协议：仅启用 SMB 访问
- 只读访问：仅适用于使用 NTLM 的客户端
- 读写访问：仅适用于使用 NTLM 的客户端

> 如果为仅限 NTLM 的访问配置只读选项或读写选项，则必须在客户端匹配选项中使用基于 IP 地址的条目。否则、您将收到 `access denied` 错误。这是因为 ONTAP 在使用主机名检查客户端的访问权限时使用 Kerberos 服务主体名称（ SPN ）。NTLM 身份验证不支持 SPN 名称。

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

启用或禁用 **SMB** 访问导出策略

您可以在 Storage Virtual Machine （ SVM ）上启用或禁用 SMB 访问导出策略。可以选择使用导出策略控制 SMB 对资源的访问。

开始之前

以下是为 SMB 启用导出策略的要求：

- 在为客户端创建导出规则之前，客户端必须在 DNS 中具有 "`PTR` " 记录。
- 如果 SVM 提供对 NFS 客户端的访问权限，并且要用于 NFS 访问的主机名与 CIFS 服务器名称不同，则需要为主机名另外设置一组 "`A` " 和 "`PTR` " 记录。

关于此任务

默认情况下，在 SVM 上设置新的 CIFS 服务器时，不会使用导出策略进行 SMB 访问。如果要根据身份验证协议或客户端 IP 地址或主机名控制访问，则可以为 SMB 访问启用导出策略。您可以随时为 SMB 访问启用或禁用导出策略。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 启用或禁用导出策略：
   - 启用导出策略： `vserver cifs options modify -vserver` *`vserver_name`* `-is -exportpolicy-enabled true`
   - 禁用导出策略： `vserver cifs options modify -vserver` *`vserver_name`* `-is -exportpolicy-enabled false`

3. 返回到管理权限级别： `set -privilege admin`

示例

以下示例支持使用导出策略控制 SMB 客户端对 SVM vs1 上资源的访问：

```
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-exportpolicy
-enabled true

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

使用存储级别访问防护确保文件访问安全

使用存储级别访问防护确保文件访问安全

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

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

存储级别访问防护行为

- 存储级别访问防护适用场景存储对象中的所有文件或所有目录。

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

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

    适用场景存储对象中的每个目录和文件。这是默认设置。

  - 文件安全性

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

  - 目录安全性

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

- 存储级别访问防护用于限制权限。

它不会提供额外的访问权限。

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

  它会在存储对象级别应用，并存储在用于确定有效权限的元数据中。

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

  它只能由存储管理员进行修改。

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

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

- 如果由于存储级别访问防护而拒绝访问，则不会发送 FPolicy 通知。

访问检查的顺序

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

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

使用存储级别访问防护的用例

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

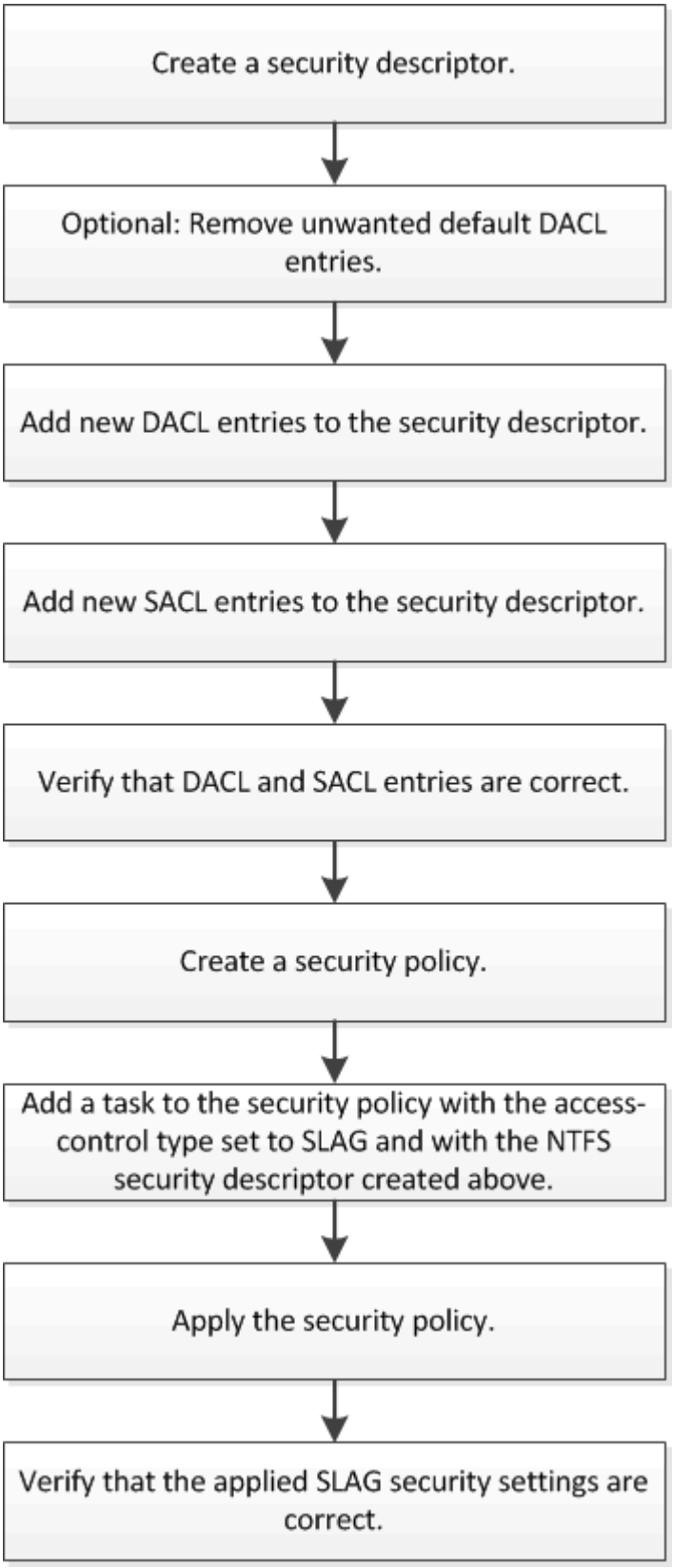
此功能的典型使用情形包括以下情形：

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

用于配置存储级别访问防护的工作流

配置存储级别访问防护（ SLAG ）的工作流使用与配置 NTFS 文件权限和审核策略相同的

ONTAP 命令行界面命令。您无需在指定目标上配置文件和目录访问，而是在指定的 Storage Virtual Machine （SVM）卷上配置 SLAG 。



相关信息

配置存储级别访问防护

配置存储级别访问防护

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

步骤

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

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

   ```
   Vserver: vs1

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

在此示例中，将两个 DACL ACE 添加到安全描述符中：

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

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

在此示例中、将两个SACL Aces添加到安全描述符中：

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

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

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

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

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

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

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

在此示例中、以下命令显示有关安全描述符"`sd1`"的SACL条目的信息：

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

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

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

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

   以下示例将创建一个名为 "`policy1` " 的策略：

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

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

   `vserver security file-directory policy show`

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

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

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

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

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

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

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

   ```
    Vserver: vs1
     Policy: policy1

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

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

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

    已计划应用安全策略的作业。

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

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

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

```
vserver security file-directory show -vserver vs1 -path /datavol1
```

```
                 Vserver: vs1
               File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


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

相关信息

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

用于配置存储级别访问防护的工作流

显示有关存储级别访问防护的信息

正在删除存储级别访问防护

有效的 SLAG 列表

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

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

显示有关存储级别访问防护的信息

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

关于此任务

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

步骤

1. 使用所需的详细信息级别显示存储级别访问防护安全设置：

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

示例

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

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

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


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

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

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

删除存储级别访问防护

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

步骤

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

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

```
                 Vserver: vs1
               File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

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

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

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

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

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

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```