使用命令行界面管理NFS

ONTAP 9

NetApp
April 24, 2024

目录

使用命令行界面管理NFS

NFS参考概述

ONTAP 包括可用于 NFS 协议的文件访问功能。您可以启用 NFS 服务器并导出卷或 qtree 。

您可以在以下情况下执行这些操作步骤：

- 您希望了解ONTAP NFS协议功能的范围。
- 您希望执行不太常见的配置和维护任务、而不是基本NFS配置。
- 您希望使用命令行界面（ CLI ），而不是 System Manager 或自动化脚本编写工具。

了解 NAS 文件访问

命名空间和接合点

命名空间和接合点概述

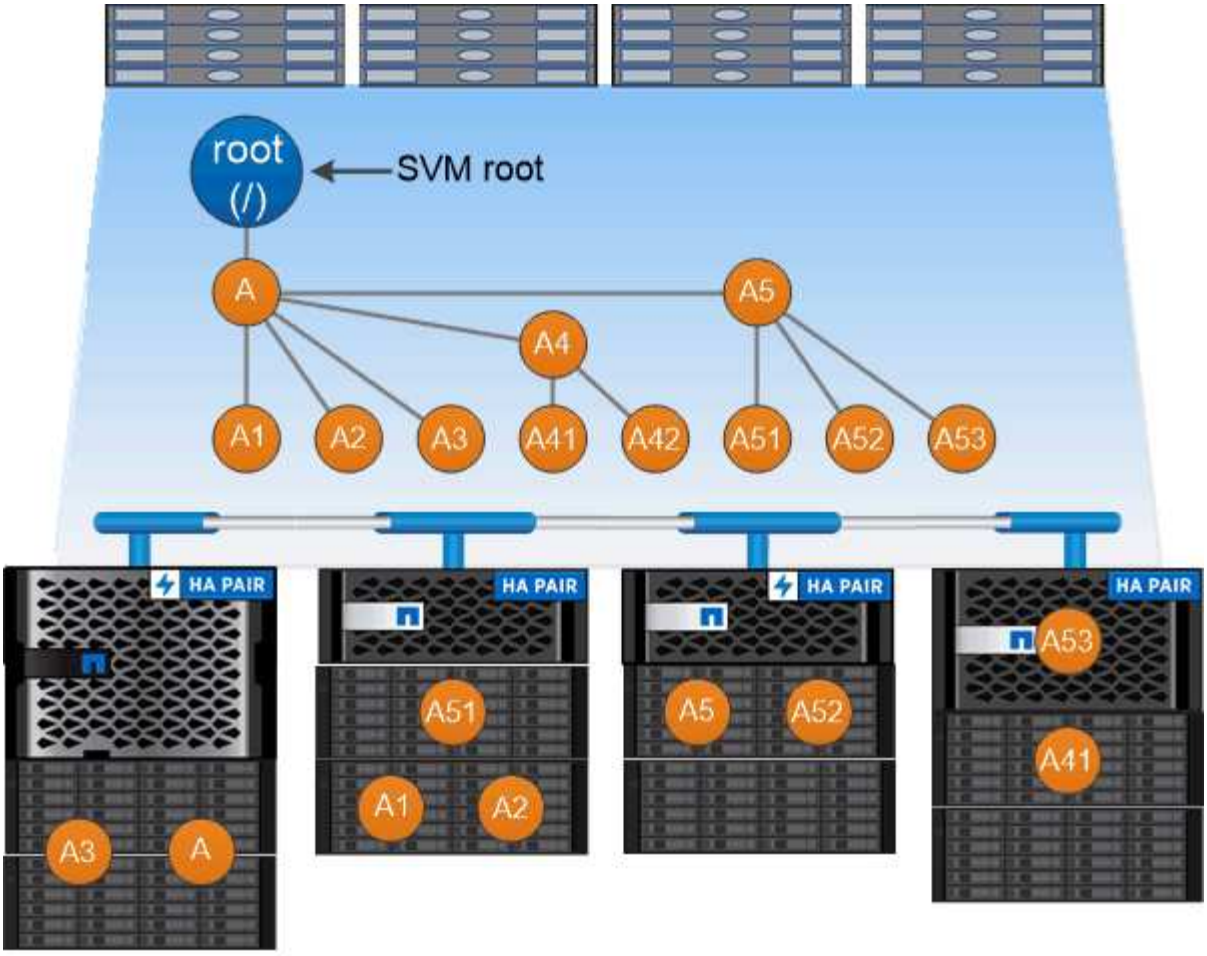
nas_namespaces_ 是指在 *junction points* 处联合在一起的卷的逻辑分组，用于创建单个文件系统层次结构。具有足够权限的客户端可以访问命名空间中的文件，而无需指定文件在存储中的位置。集群中的任何位置都可以驻留未分配的卷。

NAS 客户端不会挂载包含相关文件的每个卷，而是挂载 nfs *export* 或访问 SMB _share 。 _ 导出或共享表示整个命名空间或命名空间中的中间位置。客户端仅访问挂载在其访问点下方的卷。

您可以根据需要向命名空间添加卷。您可以直接在父卷接合下方或卷中的目录上创建接合点。名为"`vol3`"的卷的卷接合路径可能为 `/vol1/vol2/vol3`或 `/vol1/dir2/vol3`，甚至 `/dir1/dir2/vol3`。此路径称为 _junction path…

每个 SVM 都有一个唯一的命名空间。SVM 根卷是命名空间层次结构的入口点。

> 要确保在发生节点中断或故障转移时数据仍然可用，您应为 SVM 根卷创建一个 *load-sharing mirror* 副本。



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

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
```

什么是典型的 **NAS** 命名空间架构

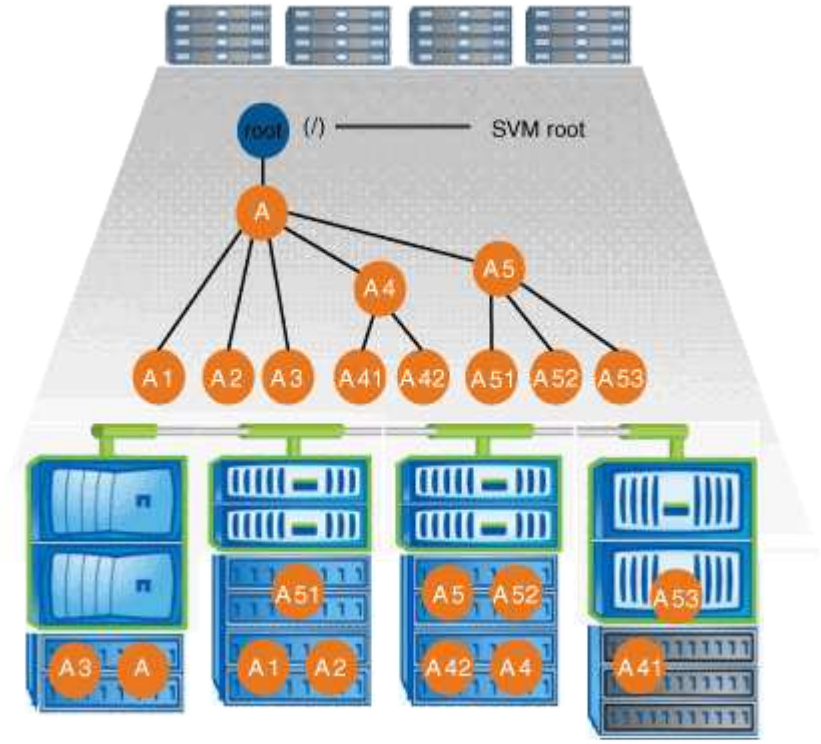
在创建 SVM 名称空间时，您可以使用几种典型的 NAS 命名空间架构。您可以选择符合业务和工作流需求的命名空间架构。

命名空间的顶部始终为根卷，以斜杠（/）表示。根下的命名空间架构分为三个基本类别：

- 一个分支树，与命名空间根只有一个接合点
- 多个分支树，多个接合点指向命名空间的根
- 多个独立卷，每个卷都有一个指向名称空间根的单独接合点

包含单个分支树的命名空间

包含单个分支树的架构在 SVM 命名空间的根上具有一个插入点。单个插入点可以是接合卷，也可以是根下的目录。所有其他卷都挂载在单个插入点（可以是卷或目录）下的接合点处。

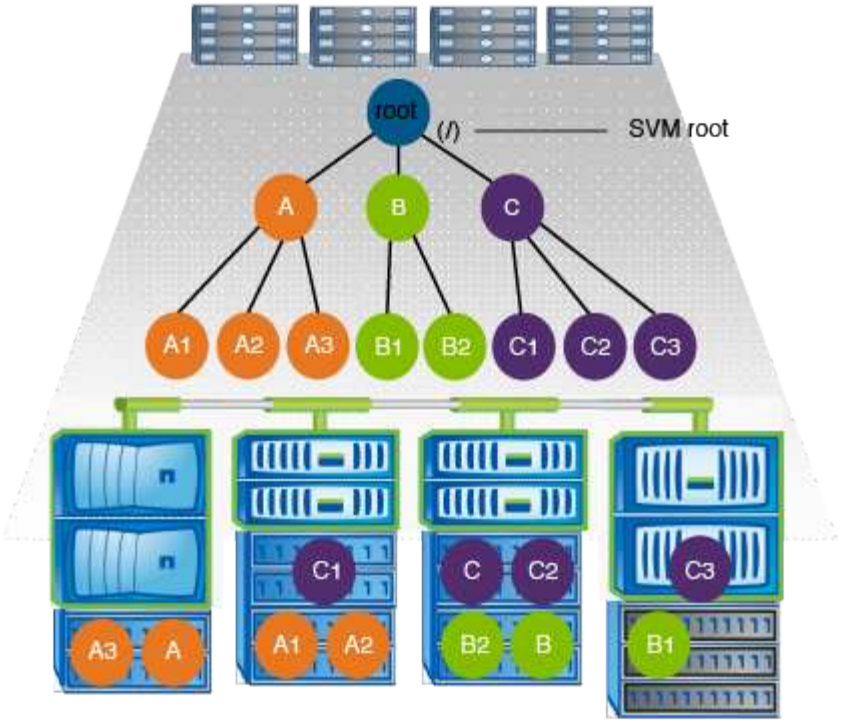


例如，具有上述命名空间架构的典型卷接合配置可能类似于以下配置，其中所有卷都在单个插入点（即名为 `data` 的目录）下接合：

```
                      Junction                        Junction
Vserver Volume        Active   Junction Path          Path Source
------- ------------ -------- --------------------    -----------
vs1     corp1        true     /data/dir1/corp1       RW_volume
vs1     corp2        true     /data/dir1/corp2       RW_volume
vs1     data1        true     /data/data1            RW_volume
vs1     eng1         true     /data/data1/eng1       RW_volume
vs1     eng2         true     /data/data1/eng2       RW_volume
vs1     sales        true     /data/data1/sales      RW_volume
vs1     vol1         true     /data/vol1             RW_volume
vs1     vol2         true     /data/vol2             RW_volume
vs1     vol3         true     /data/vol3             RW_volume
vs1     vs1_root     -        /                      -
```

包含多个分支树的命名空间

包含多个分支树的架构在 SVM 命名空间的根目录中具有多个插入点。插入点可以是接合卷，也可以是根下的目录。所有其他卷都挂载在插入点下方的接合点（可以是卷或目录）。

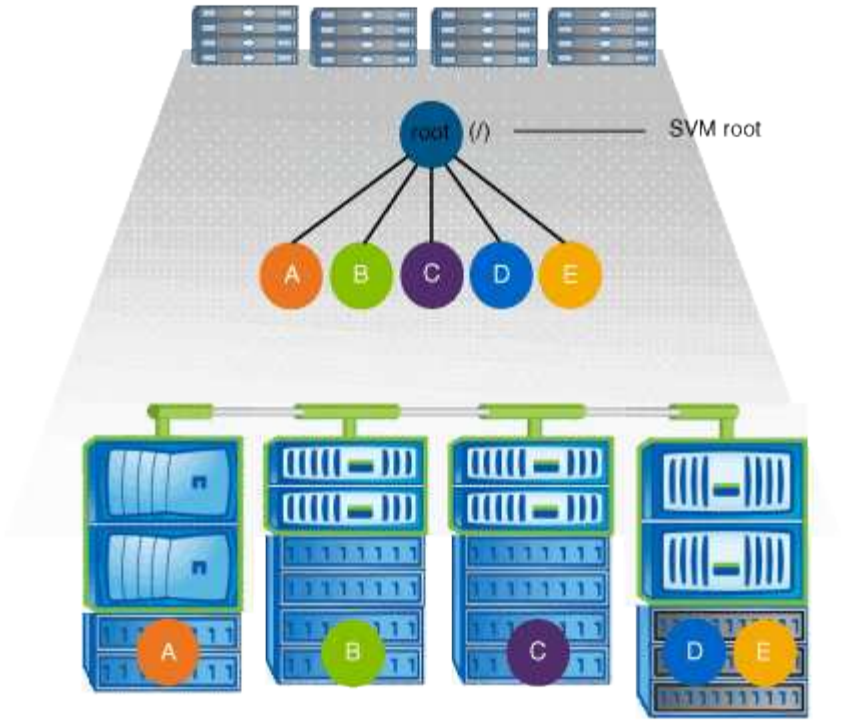


例如，具有上述命名空间架构的典型卷接合配置可能类似于以下配置，其中有三个插入点指向 SVM 的根卷。两个插入点是名为 `data` 和 "`projects` " 的目录。一个插入点是名为 "`audit` " 的接合卷：

```
                      Junction                          Junction
Vserver Volume        Active   Junction Path            Path Source
------- ------------- -------- --------------------     -----------
vs1     audit         true     /audit                   RW_volume
vs1     audit_logs1   true     /audit/logs1             RW_volume
vs1     audit_logs2   true     /audit/logs2             RW_volume
vs1     audit_logs3   true     /audit/logs3             RW_volume
vs1     eng           true     /data/eng                RW_volume
vs1     mktg1         true     /data/mktg1              RW_volume
vs1     mktg2         true     /data/mktg2              RW_volume
vs1     project1      true     /projects/project1       RW_volume
vs1     project2      true     /projects/project2       RW_volume
vs1     vs1_root      -        /                        -
```

包含多个独立卷的命名空间

在具有独立卷的架构中，每个卷都有一个插入点指向 SVM 命名空间的根；但是，卷不会接合到另一个卷下。每个卷都有一个唯一的路径，可以直接在根下接合，也可以在根下的目录下接合。



例如，具有上述命名空间架构的典型卷接合配置可能类似于以下配置，其中有五个插入点指向 SVM 的根卷，每个插入点表示一个卷的路径。

```
                      Junction                          Junction
Vserver Volume        Active   Junction Path            Path Source
------- ------------ -------- --------------------     -----------
vs1     eng           true     /eng                     RW_volume
vs1     mktg          true     /vol/mktg                RW_volume
vs1     project1      true     /project1                RW_volume
vs1     project2      true     /project2                RW_volume
vs1     sales         true     /sales                   RW_volume
vs1     vs1_root      -        /                        -
```

ONTAP 如何控制对文件的访问

ONTAP 如何控制对文件的访问概述

ONTAP 会根据您指定的基于身份验证和基于文件的限制来控制对文件的访问。

当客户端连接到存储系统以访问文件时， ONTAP 必须执行两项任务：

- 身份验证

  ONTAP 必须通过使用可信源验证身份来对客户端进行身份验证。此外，客户端的身份验证类型是一种可用于确定客户端在配置导出策略时是否可以访问数据的方法（对于 CIFS 为可选）。

- Authorization

ONTAP 必须通过将用户凭据与文件或目录上配置的权限进行比较并确定要提供的访问类型（如果有）来授权用户。

要正确管理文件访问控制， ONTAP 必须与 NIS ， LDAP 和 Active Directory 服务器等外部服务进行通信。要使用 CIFS 或 NFS 配置存储系统以进行文件访问，需要根据您在 ONTAP 中的环境设置相应的服务。

基于身份验证的限制

通过基于身份验证的限制，您可以指定哪些客户端计算机以及哪些用户可以连接到 Storage Virtual Machine （ SVM ）。

ONTAP 支持从 UNIX 和 Windows 服务器进行 Kerberos 身份验证。

基于文件的限制

ONTAP 会评估三个安全级别，以确定实体是否有权对 SVM 上的文件和目录执行请求的操作。在评估三个安全级别后，访问权限由有效权限决定。

任何存储对象最多可包含三种类型的安全层：

- 导出（ NFS ）和共享（ SMB ）安全性

  导出并共享对给定 NFS 导出或 SMB 共享的安全适用场景客户端访问。具有管理权限的用户可以管理 SMB 和 NFS 客户端的导出和共享级别安全性。

- 存储级别访问防护文件和目录安全性

  存储级别访问防护安全性适用场景 SMB 和 NFS 客户端对 SVM 卷的访问。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。

  > 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。

- NTFS ， UNIX 和 NFSv4 原生文件级安全性

  表示存储对象的文件或目录具有原生文件级安全性。您可以从客户端设置文件级安全性。无论使用 SMB 还是 NFS 访问数据，文件权限都是有效的。

ONTAP如何处理NFS客户端身份验证

ONTAP 如何处理 **NFS** 客户端身份验证概述

NFS 客户端必须经过适当的身份验证，才能访问 SVM 上的数据。ONTAP 会根据您配置的名称服务检查客户端的 UNIX 凭据，从而对客户端进行身份验证。

当 NFS 客户端连接到 SVM 时， ONTAP 会根据 SVM 的名称服务配置检查不同的名称服务来获取用户的 UNIX 凭据。ONTAP 可以检查本地 UNIX 帐户， NIS 域和 LDAP 域的凭据。必须至少配置其中一个， ONTAP 才能成

功对用户进行身份验证。您可以指定多个名称服务以及 ONTAP 搜索这些服务的顺序。

在采用 UNIX 卷安全模式的纯 NFS 环境中，此配置足以对从 NFS 客户端连接的用户进行身份验证并提供正确的文件访问权限。

如果您使用的是混合、NTFS或统一卷安全模式、则ONTAP必须获取UNIX用户的SMB用户名、以便通过Windows域控制器进行身份验证。这可以通过使用本地UNIX帐户或LDAP域映射单个用户来实现、也可以改用默认SMB用户来实现。您可以指定ONTAP搜索哪些名称服务的顺序、也可以指定默认SMB用户。

ONTAP 如何使用名称服务

ONTAP 使用名称服务获取有关用户和客户端的信息。ONTAP 使用此信息对访问存储系统上的数据或管理存储系统的用户进行身份验证，并在混合环境中映射用户凭据。

配置存储系统时，必须指定希望 ONTAP 用于获取用户凭据进行身份验证的名称服务。ONTAP 支持以下名称服务：

- 本地用户（文件）
- 外部 NIS 域（ NIS ）
- 外部 LDAP 域（ LDAP ）

您可以使用 `vserver services name-service ns-switch` 命令系列、用于为SVM配置源以搜索网络信息以及搜索顺序。这些命令提供与等效的功能 `/etc/nsswitch.conf` 文件。

当 NFS 客户端连接到 SVM 时， ONTAP 会检查指定的名称服务以获取用户的 UNIX 凭据。如果名称服务配置正确，并且 ONTAP 可以获取 UNIX 凭据，则 ONTAP 将成功对用户进行身份验证。

在具有混合安全模式的环境中， ONTAP 可能必须映射用户凭据。您必须为您的环境正确配置名称服务，以使 ONTAP 能够正确映射用户凭据。

ONTAP 还使用名称服务对 SVM 管理员帐户进行身份验证。在配置或修改名称服务切换时，必须牢记这一点，以免意外禁用 SVM 管理员帐户的身份验证。有关SVM管理用户的详细信息、请参见 "管理员身份验证和RBAC"。

ONTAP 如何从 **NFS** 客户端授予 **SMB** 文件访问权限

ONTAP 使用 Windows NT 文件系统（ NTFS ）安全语义来确定 NFS 客户端上的 UNIX 用户是否有权访问具有 NTFS 权限的文件。

为此， ONTAP 会将用户的 UNIX 用户 ID （ UID ）转换为 SMB 凭据，然后使用 SMB 凭据验证用户是否有权访问此文件。SMB 凭据由一个主安全标识符（ SID ）（通常是用户的 Windows 用户名）以及一个或多个与用户所属 Windows 组对应的组 SID 组成。

ONTAP 将 UNIX UID 转换为 SMB 凭据所需的时间可能从数十毫秒到数百毫秒不等，因为此过程涉及到与域控制器联系。ONTAP 会将 UID 映射到 SMB 凭据，并在凭据缓存中输入映射，以缩短转换所导致的验证时间。

NFS 凭据缓存的工作原理

当 NFS 用户请求访问存储系统上的 NFS 导出时， ONTAP 必须从外部名称服务器或本地文件检索用户凭据以对用户进行身份验证。然后， ONTAP 会将这些凭据存储在内部凭据

缓存中，以供日后参考。了解 NFS 凭据缓存的工作原理有助于您处理潜在的性能和访问问题。

如果没有凭据缓存， ONTAP 将必须在 NFS 用户每次请求访问时查询名称服务。在许多用户访问的繁忙存储系统上，这可能会快速导致严重的性能问题，从而导致不必要的延迟，甚至拒绝 NFS 客户端访问。

通过凭据缓存， ONTAP 会检索用户凭据，然后将其存储一段预定的时间，以便在 NFS 客户端发送另一个请求时快速轻松地进行访问。此方法具有以下优势：

- 它可以减少对外部名称服务器（例如 NIS 或 LDAP ）的请求，从而减轻存储系统的负载。
- 它可以减少向外部名称服务器发送的请求，从而减轻这些服务器的负载。
- 它可以在用户进行身份验证之前，消除从外部源获取凭据的等待时间，从而加快用户访问速度。

ONTAP 会将肯定和否定凭据存储在凭据缓存中。肯定凭据表示用户已通过身份验证并获得访问权限。否定凭据表示用户未通过身份验证，并被拒绝访问。

默认情况下， ONTAP 会将肯定凭据存储 24 小时；也就是说，在对用户进行初始身份验证后， ONTAP 会对该用户 24 小时内的任何访问请求使用缓存的凭据。如果用户在 24 小时后请求访问，则此周期将重新开始： ONTAP 丢弃缓存的凭据，并从相应的名称服务源再次获取凭据。如果名称服务器上的凭据在过去 24 小时内发生更改，则 ONTAP 会缓存更新后的凭据，以供未来 24 小时使用。

默认情况下， ONTAP 会将否定凭据存储两个小时；也就是说，在最初拒绝用户访问后， ONTAP 会继续拒绝该用户的任何访问请求两个小时。如果用户在 2 小时后请求访问，则循环将重新开始： ONTAP 再次从相应的名称服务源获取凭据。如果名称服务器上的凭据在过去两小时内发生更改，则 ONTAP 会缓存更新后的凭据，以供未来两小时使用。

在 NAS 命名空间中创建和管理数据卷

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。
- 从ONTAP 9.13.1开始、您可以创建启用了容量分析和活动跟踪的卷。要启用容量或活动跟踪、请问题描述 `volume create` 命令 `-analytics-state` 或 `-activity-tracking-state` 设置为 `on`。

  要了解有关容量分析和活动跟踪的更多信息、请参见 启用文件系统分析。

> 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`，SMB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。
- 从ONTAP 9.13.1开始、您可以创建启用了容量分析和活动跟踪的卷。要启用容量或活动跟踪、请问题描述 `volume create` 命令 `-analytics-state` 或 `-activity-tracking-state` 设置为 `on`。

  要了解有关容量分析和活动跟踪的更多信息、请参见 启用文件系统分析。

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"

卸载卷并使其脱机时，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`* `-fields` *`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
```

配置安全模式

安全模式如何影响数据访问

安全模式及其影响是什么

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`

使用NFS设置文件访问

使用 NFS 概述设置文件访问

要允许客户端使用 NFS 访问 Storage Virtual Machine （ SVM ） 上的文件，您必须完成许多步骤。根据环境的当前配置，还有一些可选的附加步骤。

要使客户端能够使用 NFS 访问 SVM 上的文件，您必须完成以下任务：

1. 在 SVM 上启用 NFS 协议。

   您必须将 SVM 配置为允许客户端通过 NFS 访问数据。

2. 在 SVM 上创建 NFS 服务器。

   NFS 服务器是 SVM 上的一个逻辑实体，可使 SVM 通过 NFS 提供文件。您必须创建 NFS 服务器并指定要允许的 NFS 协议版本。

3. 在 SVM 上配置导出策略。

   您必须配置导出策略，以使卷和 qtree 可供客户端使用。

4. 根据网络和存储环境，为 NFS 服务器配置适当的安全性和其他设置。

   此步骤可能包括配置 Kerberos ， LDAP ， NIS ，名称映射和本地用户。

使用导出策略确保 **NFS** 访问安全

导出策略如何控制客户端对卷或 **qtree** 的访问

导出策略包含一个或多个 *export rules* ，用于处理每个客户端访问请求。此过程的结果将确定客户端是被拒绝还是被授予访问权限，以及访问级别。Storage Virtual Machine （ SVM ）上必须存在具有导出规则的导出策略，客户端才能访问数据。

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

- 为 SVM 的每个卷或 qtree 分配不同的导出策略，以控制单个客户端对 SVM 中每个卷或 qtree 的访问。
- 为 SVM 的多个卷或 qtree 分配相同的导出策略，以实现相同的客户端访问控制，而无需为每个卷或 qtree 创建新的导出策略。

如果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。如果客户端与导出策略中的任何规则不匹配，则会拒绝访问。如果导出策略为空，则会隐式拒绝所有访问。

您可以在运行 ONTAP 的系统上动态修改导出策略。

SVM 的默认导出策略

每个 SVM 都有一个不包含任何规则的默认导出策略。必须存在具有规则的导出策略，客户端才能访问 SVM 上的数据。SVM 中包含的每个 FlexVol 卷都必须与一个导出策略相关联。

创建SVM时、存储系统会自动创建一个名为的默认导出策略 `default` SVM的根卷。您必须为默认导出策略创建一个或多个规则，客户端才能访问 SVM 上的数据。或者，您也可以使用规则创建自定义导出策略。您可以修改和重命名默认导出策略，但不能删除默认导出策略。

在包含的 SVM 中创建 FlexVol 卷时，存储系统会创建该卷，并将该卷与 SVM 根卷的默认导出策略相关联。默认情况下，在 SVM 中创建的每个卷都会与根卷的默认导出策略相关联。您可以对 SVM 中包含的所有卷使用默认导出策略，也可以为每个卷创建唯一的导出策略。您可以将多个卷与同一导出策略相关联。

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。

> 从 ONTAP 9.3 开始，您可以将导出策略配置检查作为后台作业来启用，以便在错误规则列表中记录任何违规。。 `vserver export-policy config-checker` 命令会调用检查程序并显示结果、您可以使用这些结果来验证配置并从策略中删除错误的规则。
>
> 命令仅验证主机名，网络组和匿名用户的导出配置。

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。

管理安全类型未列出的客户端

如果客户端的安全类型未列在导出规则的访问参数中、您可以选择拒绝访问该客户端、也可以改用选项将其映射到匿名用户ID `none` 在访问参数中。

客户端可能使用的安全类型未列在访问参数中，因为它是使用其他安全类型进行身份验证的，或者根本未进行身份验证（安全类型为 AUTH_NONE ）。默认情况下，客户端会自动拒绝访问该级别。但是、您可以添加选项 `none` 访问参数。因此，安全模式未列出的客户端会映射到匿名用户 ID 。。 `-anon` 参数用于确定分配给这些客户端的用户ID。为指定的用户ID `-anon` 参数必须是有效用户、并且已配置您认为适合匿名用户的权限。

的有效值 `-anon` 参数范围从 `0` to `65535`。

分配给的用户**ID** `-anon`	处理客户端访问请求的结果
`0 - 65533`	客户端访问请求将映射到匿名用户 ID ，并根据为此用户配置的权限获得访问权限。
`65534`	客户端访问请求将映射到用户 nobody ，并根据为此用户配置的权限获得访问权限。这是默认值。
`65535`	映射到此 ID 后，来自任何客户端的访问请求都会被拒绝，并且客户端会使用安全类型 AUTH_NONE 显示自己。如果客户端的用户 ID 为 0 ，则在映射到此 ID 时，此客户端发出的访问请求将被拒绝，而此客户端将使用任何其他安全类型显示自己。

使用选项时 `none`，请务必记住，只读参数是首先处理的。为安全类型未列出的客户端配置导出规则时，请考虑以下准则：

只读包括 none	读写包括 none	具有未列出的安全类型的客户端的访问结果
否	否	拒绝
否	是的。	拒绝，因为首先处理只读
是的。	否	以匿名身份只读
是的。	是的。	以匿名身份读写

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 sys,none`
- `-rwrule any`
- `-anon 70`

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。

客户端 3 的 IP 地址为 10.1.16.234 ，使用 NFSv3 协议发送访问请求，并且未进行身份验证（表示安全类型为 AUTH_NONE ）。

所有这三个客户端的客户端访问协议和 IP 地址均匹配。只读参数允许使用自己的用户 ID 并通过 AUTH_SYS 进行身份验证的客户端进行只读访问。只读参数允许使用任何其他安全类型进行身份验证的客户端以用户 ID 为 70 的匿名用户身份进行只读访问。读写参数允许对任何安全类型进行读写访问，但在这种情况下，仅允许已通过只读规则筛选的适用场景客户端。

因此，客户端 1 和 3 只能作为用户 ID 为 70 的匿名用户进行读写访问。客户端 2 使用自己的用户 ID 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 sys,none`
- `-rwrule none`
- `-anon 70`

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。

客户端 3 的 IP 地址为 10.1.16.234 ，使用 NFSv3 协议发送访问请求，并且未进行身份验证（表示安全类型为 AUTH_NONE ）。

所有这三个客户端的客户端访问协议和 IP 地址均匹配。只读参数允许使用自己的用户 ID 并通过 AUTH_SYS 进行身份验证的客户端进行只读访问。只读参数允许使用任何其他安全类型进行身份验证的客户端以用户 ID 为 70 的匿名用户身份进行只读访问。读写参数仅允许以匿名用户身份进行读写访问。

因此，客户端 1 和客户端 3 只能作为用户 ID 为 70 的匿名用户进行读写访问。客户端 2 使用自己的用户 ID 获取只读访问，但被拒绝读写访问。

安全类型如何确定客户端访问级别

客户端使用进行身份验证的安全类型在导出规则中起着特殊的作用。您必须了解安全类型如何确定客户端对卷或 qtree 的访问级别。

三种可能的访问级别如下：

1. 只读
2. 读写
3. 超级用户（对于用户 ID 为 0 的客户端）

由于按安全类型评估访问级别的顺序，因此在导出规则中构建访问级别参数时，必须遵循以下规则：

客户端要获取访问级别 ...	这些访问参数必须与客户端的安全类型匹配 ...
普通用户只读	只读 (`-rorule`)
普通用户读写	只读 (`-rorule`)和读写 (`-rwrule`)
超级用户只读	只读 (`-rorule`)和 `-superuser`
超级用户读写	只读 (`-rorule`)和读写 (`-rwrule`)和 `-superuser`

以下是这三个访问参数中每一个参数的有效安全类型：

- `any`
- `none`
- `never`

  此安全类型不适用于 `-superuser` 参数。

- `krb5`
- `krb5i`
- `krb5p`

- `ntlm`
- `sys`

根据三个访问参数中的每个参数匹配客户端的安全类型时，可能会出现以下三种结果：

客户端的安全类型	然后，客户端 ...
与访问参数中指定的值匹配。	使用自己的用户 ID 获取该级别的访问权限。
与指定的不匹配、但访问参数包括选项 `none`。	获取该级别的访问权限、但作为用户ID由指定的匿名用户 `-anon` 参数。
与指定的不匹配、并且访问参数不包括选项 `none`。	不会获取该级别的任何访问权限。这不适用于 `-superuser` 参数、因为它始终包括 `none` 即使未指定也是如此。

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 sys,krb5`
- `-superuser krb5`

客户端 1 的 IP 地址为 10.1.16.207 ，用户 ID 为 0 ，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 ，用户 ID 为 0 ，使用 NFSv3 协议发送访问请求，并使用 AUTH_SYS 进行身份验证。

客户端 3 的 IP 地址为 10.1.16.234 ，用户 ID 为 0 ，使用 NFSv3 协议发送访问请求，并且未进行身份验证（ AUTH_NONE ）。

客户端访问协议和 IP 地址与所有三个客户端匹配。只读参数允许对所有客户端进行只读访问，而不考虑安全类型。读写参数允许使用自己的用户 ID 并使用 AUTH_SYS 或 Kerberos v5 进行身份验证的客户端进行读写访问。超级用户参数允许超级用户访问用户 ID 为 0 并使用 Kerberos v5 进行身份验证的客户端。

因此，客户端 1 将获得超级用户读写访问权限，因为它与所有三个访问参数匹配。客户端 2 将获得读写访问权限，但不会获得超级用户访问权限。客户端 3 获得只读访问权限，但无超级用户访问权限。

管理超级用户访问请求

在配置导出策略时，您需要考虑在存储系统收到用户 ID 为 0 （即超级用户）的客户端访问请求并相应地设置导出规则时要发生的情况。

在 UNIX 环境中，用户 ID 为 0 的用户称为超级用户，通常称为 root ，他们对系统拥有无限访问权限。由于多种

原因，使用超级用户权限可能会很危险，包括违反系统和数据安全。

默认情况下， ONTAP 会将用户 ID 为 0 的客户端映射到匿名用户。但是、您可以指定 - superuser 用于确定如何根据安全类型处理用户ID为0的客户端的导出规则中的参数。以下是的有效选项 -superuser 参数：

- any
- none

  如果未指定、则此为默认设置 -superuser 参数。

- krb5
- ntlm
- sys

根据、有两种不同的方式处理用户ID为0的客户端 -superuser 参数配置：

如果 **-superuser** 参数和客户端的安全类型	然后，客户端 ...
匹配	获取用户 ID 为 0 的超级用户访问权限。
不匹配	以用户ID由指定的匿名用户身份获取访问 -anon 参数及其分配的权限。这与只读或读写参数指定选项无关 none。

如果客户端使用用户ID 0访问采用NTFS安全模式和的卷 -superuser 参数设置为 none，ONTAP使用匿名用户的名称映射来获取正确的凭据。

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
- -anon 127

客户端1的IP地址为10.1.16.207、用户ID为746、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 ，用户 ID 为 0 ，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。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 不会获得超级用户访问权限。相反、它会映射到匿名、因为 -superuser 未指定参数。这意味着它默

认为 `none` 并自动将用户ID 0映射到匿名。客户端 2 也仅获取只读访问，因为其安全类型与读写参数不匹配。

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`
- `-superuser krb5`
- `-anon 0`

客户端 1 的 IP 地址为 10.1.16.207 ，用户 ID 为 0 ，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 ，用户 ID 为 0 ，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。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。

导出规则允许用户 ID 为 0 的客户端进行超级用户访问。客户端1将获得超级用户访问、因为它与只读和的用户ID和安全类型匹配 `-superuser` parameters客户端2不会获取读写或超级用户访问权限、因为其安全类型与读写参数或不匹配 `-superuser` 参数。而是将客户端 2 映射到匿名用户，在这种情况下，此用户 ID 为 0 。

ONTAP 如何使用导出策略缓存

为了提高系统性能， ONTAP 使用本地缓存来存储主机名和网络组等信息。这样，与从外部源检索信息相比， ONTAP 可以更快地处理导出策略规则。了解什么是缓存以及缓存的用途可以帮助您解决客户端访问问题。

您可以配置导出策略以控制客户端对 NFS 导出的访问。每个导出策略都包含规则，而每个规则都包含参数，用于将规则与请求访问的客户端匹配。其中一些参数要求 ONTAP 与外部源（例如 DNS 或 NIS 服务器）联系，以解析域名，主机名或网络组等对象。

与外部源的这些通信只需很短的时间。为了提高性能， ONTAP 通过将信息存储在多个缓存中的每个节点本地，减少了解析导出策略规则对象所需的时间。

缓存名称	存储的信息类型
访问	客户端到相应导出策略的映射
Name	UNIX 用户名到相应 UNIX 用户 ID 的映射
ID	UNIX 用户 ID 到相应 UNIX 用户 ID 和扩展 UNIX 组 ID 的映射

缓存名称	存储的信息类型
主机	主机名到相应 IP 地址的映射
网络组	网络组到相应成员 IP 地址的映射
showmount	从 SVM 命名空间导出的目录列表

如果在 ONTAP 检索并将环境中外部名称服务器上的信息存储在本地之后更改了这些信息，则缓存现在可能包含过时的信息。尽管 ONTAP 会在特定时间段后自动刷新缓存，但不同的缓存具有不同的到期时间和刷新时间以及算法。

缓存包含过时信息的另一个可能原因是 ONTAP 尝试刷新缓存的信息，但在尝试与名称服务器通信时遇到故障。如果发生这种情况， ONTAP 将继续使用当前存储在本地缓存中的信息，以防止客户端中断。

因此，应该成功的客户端访问请求可能会失败，而应该失败的客户端访问请求可能会成功。在对此类客户端访问问题进行故障排除时，您可以查看并手动刷新某些导出策略缓存。

访问缓存的工作原理

ONTAP 使用访问缓存来存储导出策略规则评估的结果，以供客户端对卷或 qtree 的访问操作使用。这样可以提高性能，因为与每次客户端发送 I/O 请求时执行导出策略规则评估过程相比，从访问缓存中检索信息的速度要快得多。

每当 NFS 客户端发送 I/O 请求以访问卷或 qtree 上的数据时， ONTAP 都必须评估每个 I/O 请求，以确定是授予还是拒绝 I/O 请求。此评估涉及检查与卷或 qtree 关联的导出策略的每个导出策略规则。如果卷或 qtree 的路径涉及跨越一个或多个接合点，则可能需要对路径上的多个导出策略执行此检查。

请注意，此评估适用于从 NFS 客户端发送的每个 I/O 请求，例如读取，写入，列表，复制和其他操作；而不仅仅适用于初始挂载请求。

在 ONTAP 确定适用的导出策略规则并决定允许还是拒绝请求后， ONTAP 会在访问缓存中创建一个条目来存储此信息。

当 NFS 客户端发送 I/O 请求时， ONTAP 会记下客户端的 IP 地址， SVM 的 ID 以及与目标卷或 qtree 关联的导出策略，并首先检查访问缓存中是否存在匹配条目。如果访问缓存中存在匹配的条目， ONTAP 将使用存储的信息来允许或拒绝 I/O 请求。如果不存在匹配条目， ONTAP 将按照上述说明完成评估所有适用策略规则的正常过程。

当前未使用的访问缓存条目不会刷新。这样可以减少与外部名称服务器之间不必要的浪费通信。

从访问缓存中检索信息比对每个 I/O 请求执行整个导出策略规则评估过程要快得多。因此，使用访问缓存可以降低客户端访问检查的开销，从而显著提高性能。

访问缓存参数的工作原理

多个参数用于控制访问缓存中条目的刷新周期。了解这些参数的工作原理后，您可以对其进行修改，以调整访问缓存并平衡性能与存储信息的最新程度。

访问缓存会存储包含一个或多个导出规则的条目，这些规则适用于尝试访问卷或 qtree 的客户端。这些条目会在

刷新之前存储一段时间。刷新时间由访问缓存参数决定，并取决于访问缓存条目的类型。

您可以为单个 SVM 指定访问缓存参数。这样，这些参数就可以根据 SVM 访问要求而有所不同。当前未使用的访问缓存条目不会刷新，从而减少与外部名称服务之间不必要的浪费性通信。

访问缓存条目类型	Description	刷新周期（以秒为单位）
肯定条目	未导致拒绝客户端访问的访问缓存条目。	最小值： 300 最大值： 86 ， 400 默认值： 3,600 。
否定条目	导致客户端访问被拒绝的访问缓存条目。	最小值：60 最大值： 86 ， 400 默认值： 3,600 。

示例

NFS 客户端尝试访问集群上的卷。ONTAP 会将客户端与导出策略规则匹配，并根据导出策略规则配置确定客户端获取访问权限。ONTAP 会将导出策略规则作为肯定条目存储在访问缓存中。默认情况下， ONTAP 会将肯定条目保留在访问缓存中一小时（ 3 ， 600 秒），然后自动刷新该条目以使信息保持最新。

为了防止访问缓存不必要地填满，还提供了一个参数来清除在特定时间段内未用于确定客户端访问的现有访问缓存条目。这 `-harvest-timeout` 参数的允许范围为60到2、592、000秒、默认设置为86、400秒。

从 **qtree** 删除导出策略

如果您决定不再需要将特定导出策略分配给 qtree ，则可以通过修改 qtree 以继承包含卷的导出策略来删除导出策略。您可以使用执行此操作 `volume qtree modify` 命令 `-export-policy` 参数和空名称字符串("")。

步骤

1. 要从 qtree 中删除导出策略，请输入以下命令：

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy ""
   ```

2. 验证是否已相应修改 qtree ：

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

验证 **qtree** 文件操作的 **qtree ID**

ONTAP 可以对 qtree ID 执行可选的额外验证。此验证可确保客户端文件操作请求使用有效的 qtree ID ，并且客户端只能在同一 qtree 内移动文件。您可以通过修改来启用或禁用此验证 `-validate-qtree-export` 参数。默认情况下，此参数处于启用状态。

关于此任务

只有在已将导出策略直接分配给 Storage Virtual Machine （ SVM ）上的一个或多个 qtree 时，此参数才有效。

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：

如果您希望 **qtree ID** 验证为 …	输入以下命令 …
enabled	`vserver nfs modify -vserver vserver_name -validate-qtree-export enabled`
已禁用	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. 返回到管理权限级别：

```
set -privilege admin
```

FlexVol 卷的导出策略限制和嵌套接合

如果您将导出策略配置为在嵌套接合上设置限制性较低的策略，而在更高级别的接合上设置限制性较强的策略，则对较低级别的接合的访问可能会失败。

您应确保较高级别的接合与较低级别的接合相比具有较少限制的导出策略。

将 **Kerberos** 与 **NFS** 结合使用以增强安全性

ONTAP 支持 **Kerberos**

Kerberos 可为客户端 / 服务器应用程序提供强大的安全身份验证。身份验证用于向服务器验证用户和进程身份。在 ONTAP 环境中， Kerberos 在 Storage Virtual Machine （ SVM ）和 NFS 客户端之间提供身份验证。

在 ONTAP 9 中，支持以下 Kerberos 功能：

- Kerberos 5 身份验证与完整性检查（ krb5i ）

  Krb5i 使用校验和验证在客户端和服务器之间传输的每个 NFS 消息的完整性。出于安全原因（例如，确保数据未被篡改）和数据完整性原因（例如，在不可靠的网络上使用 NFS 时，防止数据损坏），这一点非常有用。

- Kerberos 5 身份验证与隐私检查（ krb5p ）

Krb5p 使用校验和对客户端和服务器之间的所有流量进行加密。这种方法更安全，并且会产生更多负载。

- 128 位和 256 位 AES 加密

  高级加密标准（Advanced Encryption Standard， AES）是一种用于保护电子数据安全的加密算法。ONTAP支持使用128位密钥的AES (AES-128)和使用256位密钥的AES (AES-256)对Kerberos进行加密、以增强安全性。

- SVM 级别的 Kerberos 域配置

  现在， SVM 管理员可以在 SVM 级别创建 Kerberos 域配置。这意味着 SVM 管理员无需再依赖集群管理员来配置 Kerberos 域，并且可以在多租户环境中创建单独的 Kerberos 域配置。

使用 **NFS** 配置 **Kerberos** 的要求

在系统上使用 NFS 配置 Kerberos 之前，您必须验证网络和存储环境中的某些项是否已正确配置。

> 配置环境的步骤取决于您使用的客户端操作系统，域控制器， Kerberos， DNS 等的版本和类型。本文档不会介绍如何记录所有这些变量。有关详细信息，请参见每个组件的相应文档。
>
> 有关如何在使用 Windows Server 2008 R2 Active Directory 和 Linux 主机的环境中为 NFSv3 和 NFSv4 设置 ONTAP 和 Kerberos 5 的详细示例，请参见技术报告 4073 。

应首先配置以下项：

网络环境要求

- Kerberos

  您必须使用密钥分发中心（KDC）设置有效的 Kerberos，例如基于 Windows Active Directory 的 Kerberos 或 MIT Kerberos 。

  NFS服务器必须使用 `nfs` 作为其机器主体的主要组件。

- 目录服务

  您必须在环境中使用安全目录服务，例如 Active Directory 或 OpenLDAP，该服务配置为使用基于 SSL/TLS 的 LDAP 。

- NTP

  您必须有一个运行 NTP 的工作时间服务器。为了防止因时间偏差而导致 Kerberos 身份验证失败，必须执行此操作。

- 域名解析（DNS）

  每个 UNIX 客户端和每个 SVM LIF 都必须在正向和反向查找区域下向 KDC 注册正确的服务记录（SRV）。所有参与者都必须可通过 DNS 正确解析。

- 用户帐户

每个客户端在 Kerberos 域中都必须有一个用户帐户。NFS 服务器必须使用 "`NFS` " 作为其计算机主体的主要组件。

NFS客户端要求

- NFS

  必须正确配置每个客户端，以便使用 NFSv3 或 NFSv4 通过网络进行通信。

  客户端必须支持 RFC1964 和 RFC2203 。

- Kerberos

  必须正确配置每个客户端以使用 Kerberos 身份验证，其中包括以下详细信息：

  - 已启用 TGS 通信加密。

    AES-256 可提供最强大的安全性。

  - 启用 TGT 通信最安全的加密类型。
  - 已正确配置 Kerberos 域。
  - 已启用GSS。

    使用计算机凭据时：

  - 请勿运行 `gssd` 使用 `-n` 参数。
  - 请勿运行 `kinit` 以root用户身份。

- 每个客户端都必须使用最新且更新的操作系统版本。

  这样可以为使用 Kerberos 进行 AES 加密提供最佳兼容性和可靠性。

- DNS

  必须正确配置每个客户端，以使用 DNS 进行正确的名称解析。

- NTP

  每个客户端都必须与 NTP 服务器同步。

- 主机和域信息

  每个客户端的 `/etc/hosts` 和 `/etc/resolv.conf` 文件必须分别包含正确的主机名和DNS信息。

- keytab 文件

  每个客户端都必须具有 KDC 中的 keytab 文件。域必须为大写字母。加密类型必须为 AES-256 ，以获得最高安全性。

- 可选：为了获得最佳性能，客户端至少可以使用两个网络接口：一个用于与局域网通信，一个用于与存储网络通信。

- NFS 许可证

  存储系统必须安装有效的 NFS 许可证。

- CIFS许可证

  CIFS 许可证是可选的。只有在使用多协议名称映射时检查 Windows 凭据才需要此功能。在严格的纯 UNIX 环境中不需要此功能。

- SVM

  您必须在系统上至少配置一个 SVM 。

- SVM 上的 DNS

  您必须已在每个 SVM 上配置 DNS 。

- NFS 服务器

  您必须已在 SVM 上配置 NFS 。

- AES 加密

  为了获得最强的安全性，您必须将 NFS 服务器配置为仅允许对 Kerberos 进行 AES-256 加密。

- SMB服务器

  如果您运行的是多协议环境、则必须事先在SVM上配置SMB。多协议名称映射需要SMB服务器。

- Volumes

  您必须具有一个根卷和至少一个数据卷，以供 SVM 使用。

- 根卷

  SVM 的根卷必须具有以下配置：

Name	正在设置 ...
安全风格	"unix"
UID	root 或 ID 0
GID	root 或 ID 0
UNIX 权限	777

  与根卷不同，数据卷可以采用任一安全模式。

- UNIX 组

  SVM 必须配置以下 UNIX 组：

组名称	组 **ID**
守护进程	1.
root	0
pcuser	65534 （在创建 SVM 时由 ONTAP 自动创建）

- UNIX用户

  SVM 必须配置以下 UNIX 用户：

用户名	用户 **ID**	主组 **ID**	**comment**
NFS	500	0	GSS INIT阶段需要此参数 NFS 客户端用户 SPN 的第一个组件用作用户。
pcuser	6554	6554	使用NFS和CIFS多协议时需要此参数 在创建SVM时、ONTAP会自动创建并添加到pcuser组中。
root	0	0	挂载时需要

  如果 NFS 客户端用户的 SPN 存在 Kerberos-UNIX 名称映射，则不需要 NFS 用户。

- 导出策略和规则

  您必须已为导出策略配置根卷和数据卷以及 qtree 所需的导出规则。如果通过Kerberos访问SVM的所有卷、则可以设置导出规则选项 `-rorule`， `-rwrule`，和 `-superuser` 根卷的 `krb5` ， `krb5i``或 `krb5p`。

- Kerberos-UNIX 名称映射

  如果您希望 NFS 客户端用户 SPN 标识的用户具有 root 权限，则必须创建一个映射到 root 的名称。

相关信息

"NetApp 技术报告 4073：《安全统一身份验证》"

"NetApp 互操作性表工具"

"系统管理"

"逻辑存储管理"

指定 NFSv4 的用户 ID 域

要指定用户ID域、您可以设置 `-v4-id-domain` 选项

关于此任务

默认情况下，如果设置了 NIS 域，则 ONTAP 将使用 NIS 域进行 NFSv4 用户 ID 映射。如果未设置 NIS 域，则使用 DNS 域。例如，如果您有多个用户 ID 域，则可能需要设置用户 ID 域。域名必须与域控制器上的域配置匹配。NFSv3 不需要此功能。

步骤

1. 输入以下命令：

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

配置名称服务

ONTAP 名称服务交换机配置的工作原理

ONTAP会将名称服务配置信息存储在一个表中、该表相当于 `/etc/nsswitch.conf` 文件。您必须了解该表的功能以及 ONTAP 如何使用它，以便可以根据您的环境对其进行适当配置。

ONTAP 名称服务切换表可确定 ONTAP 为检索特定类型的名称服务信息而查询的名称服务源。ONTAP 会为每个 SVM 维护一个单独的名称服务切换表。

数据库类型

该表为以下每种数据库类型存储一个单独的名称服务列表：

数据库类型	定义名称服务源 ...	有效源为 ...
主机	将主机名转换为 IP 地址	文件， DNS
组	查找用户组信息	文件， nis ， ldap
密码	查找用户信息	文件， nis ， ldap
网络组	正在查找网络组信息	文件， nis ， ldap
命名映射	正在映射用户名	文件， LDAP

源类型

源用于指定用于检索相应信息的名称服务源。

指定源类型 ...	查找信息的位置	由命令系列管理 ...

文件	本地源文件	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

NIS	在 SVM 的 NIS 域配置中指定的外部 NIS 服务器	`vserver services name-service nis-domain`
ldap	在 SVM 的 LDAP 客户端配置中指定的外部 LDAP 服务器	`vserver services name-service ldap`
DNS	在 SVM 的 DNS 配置中指定的外部 DNS 服务器	`vserver services name-service dns`

即使您计划使用NIS或LDAP进行数据访问和SVM管理身份验证、也仍应包括 `files` 并将本地用户配置为在NIS或LDAP身份验证失败时的回退。

用于访问外部源的协议

要访问外部源的服务器， ONTAP 使用以下协议：

外部名称服务源	用于访问的协议
NIS	UDP
DNS	UDP
LDAP	TCP

示例

以下示例显示了 SVM SVM_1 的名称服务开关配置：

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                 Source
Vserver         Database         Order
--------------- ------------     ---------
svm_1           hosts            files,
                                 dns
svm_1           group            files
svm_1           passwd           files
svm_1           netgroup         nis,
                                 files
```

要查找主机的 IP 地址， ONTAP 首先会查找本地源文件。如果查询未返回任何结果，则接下来会检查 DNS 服务器。

要查找用户或组信息， ONTAP 仅会查找本地源文件。如果查询未返回任何结果，则查找将失败。

要查找网络组信息， ONTAP 首先会查找外部 NIS 服务器。如果查询未返回任何结果，则接下来会检查本地网络组文件。

SVM SVM_1 的表中没有用于名称映射的名称服务条目。因此，默认情况下， ONTAP 仅会查找本地源文件。

相关信息

"NetApp 技术报告 4668 ：《名称服务最佳实践指南》"

使用 **LDAP**

LDAP 概述

通过 LDAP （轻型目录访问协议）服务器，您可以集中维护用户信息。如果您将用户数据库存储在环境中的 LDAP 服务器上，则可以将存储系统配置为在现有 LDAP 数据库中查找用户信息。

- 在为 ONTAP 配置 LDAP 之前，您应验证站点部署是否符合 LDAP 服务器和客户端配置的最佳实践。具体而言，必须满足以下条件：
  - LDAP 服务器的域名必须与 LDAP 客户端上的条目匹配。
  - LDAP 服务器支持的 LDAP 用户密码哈希类型必须包括 ONTAP 支持的类型：
    - 加密（所有类型）和 SHA-1 （ SHA ， SSHA ）。
    - 从 ONTAP 9.8 开始， SHA-2 哈希（ SHA-256 ， SSH/384 ， SHA-512 ， SSHA-256 ， SSHA-384 和 SSHA-512 ）。
  - 如果 LDAP 服务器需要会话安全措施，则必须在 LDAP 客户端中配置这些措施。

    可以使用以下会话安全选项：

    - LDAP 签名（提供数据完整性检查）和 LDAP 签名和签章（提供数据完整性检查和加密）
    - START TLS

    - LDAPS （基于 TLS 或 SSL 的 LDAP ）
  - 要启用签名和签章的 LDAP 查询，必须配置以下服务：
    - LDAP 服务器必须支持 GSSAPI （ Kerberos ） SASL 机制。
    - LDAP 服务器必须在 DNS 服务器上设置 DNS A/AAAA 记录以及 PTR 记录。
    - Kerberos 服务器必须在 DNS 服务器上存在 SRV 记录。
  - 要启用启动 TLS 或 LDAPS ，应考虑以下几点。
    - NetApp 最佳实践是使用 Start TLS ，而不是 LDAPS 。
    - 如果使用 LDAPS ，则必须在 ONTAP 9.5 及更高版本中为 TLS 或 SSL 启用 LDAP 服务器。ONTAP 9.09.4 不支持 SSL 。
    - 必须已在域中配置证书服务器。
  - 要启用 LDAP 转介跟踪（在 ONTAP 9.5 及更高版本中），必须满足以下条件：
    - 这两个域都应配置以下信任关系之一：
      - 双向
      - 单向，主站点信任转介域
      - 父 - 子
    - 必须配置 DNS 以解析所有转介的服务器名称。
    - 在进行身份验证时、域密码应相同 `--bind-as-cifs-server` 设置为true。

> LDAP 转介跟踪不支持以下配置。
>
> - 对于所有 ONTAP 版本：
> - 管理 SVM 上的 LDAP 客户端
> - 对于 ONTAP 9.8 及更早版本（ 9.9.1 及更高版本支持这些功能）：
> - LDAP签名和签章(`-session-security` 选项)
> - 加密TLS连接(`-use-start-tls` 选项)
> - 通过LAPS端口636 (`-use-ldaps-for-ad-ldap` 选项)

- 从ONTAP 9.11.1开始、您可以使用 "用于nsswitch身份验证的LDAP快速绑定。"
- 在 SVM 上配置 LDAP 客户端时，必须输入 LDAP 模式。

  在大多数情况下，默认 ONTAP 模式之一是合适的。但是，如果环境中的 LDAP 模式与这些模式不同，则必须在创建 LDAP 客户端之前为 ONTAP 创建新的 LDAP 客户端模式。有关您的环境要求，请咨询 LDAP 管理员。

- 不支持使用 LDAP 进行主机名解析。

对于追加信息，请参见 "NetApp 技术报告 4835： 《如何在 ONTAP 中配置 LDAP 》"。

LDAP 签名和签章概念

从 ONTAP 9 开始，您可以配置签名和签章，以便对 Active Directory （ AD ）服务器的查

询启用 LDAP 会话安全性。您必须将Storage Virtual Machine (SVM)上的NFS服务器安全设置配置为与LDAP服务器上的安全设置相对应。

签名可使用密钥技术确认 LDAP 有效负载数据的完整性。密封功能对 LDAP 有效负载数据进行加密，以避免以明文形式传输敏感信息。"_LDAP 安全级别 _ " 选项指示 LDAP 流量是需要签名，签名和签章，还是两者都不需要。默认值为 `none`。测试

已使用在SVM上启用SMB流量的LDAP签名和签章 `-session-security-for-ad-ldap` 选项 `vserver cifs security modify` 命令：

LDAPS 概念

您必须了解有关 ONTAP 如何确保 LDAP 通信安全的某些术语和概念。ONTAP 可以使用启动 TLS 或 LDAPS 在 Active Directory 集成的 LDAP 服务器或基于 UNIX 的 LDAP 服务器之间设置经过身份验证的会话。

术语

有关 ONTAP 如何使用 LDAPS 保护 LDAP 通信，您应了解一些特定术语。

- * LDAP *

  （轻型目录访问协议）一种用于访问和管理信息目录的协议。LDAP 用作存储用户，组和网络组等对象的信息目录。LDAP 还提供目录服务，用于管理这些对象并满足 LDAP 客户端的 LDAP 请求。

- * ssl*

  （安全套接字层）一种专为通过 Internet 安全发送信息而开发的协议。ONTAP 9及更高版本支持SSL、但已弃用而改用TLS。

- * TLS *

  （传输层安全性）基于早期 SSL 规范的 IETF 标准跟踪协议。它是 SSL 的后继协议。ONTAP 9.5及更高版本支持TLS。

- * LDAPS （基于 SSL 或 TLS 的 LDAP ） *

  一种使用 TLS 或 SSL 保护 LDAP 客户端与 LDAP 服务器之间通信安全的协议。术语_LDAP over SSL_ 和_LDAP over TLS_有时可以互换使用。ONTAP 9.5及更高版本支持LAPS。

  - 在 ONTAP 9.2-9.8 中，只能在端口 636 上启用 LDAPS 。要执行此操作、请使用 `-use-ldaps-for-ad-ldap` 参数 `vserver cifs security modify` 命令：
  - 从 ONTAP 9.1.1 开始，可以在任何端口上启用 LDAPS ，但端口 636 仍为默认端口。为此、请设置 `-ldaps-enabled` 参数设置为 `true` 并指定所需的 `-port` 参数。有关详细信息，请参见 `vserver services name-service ldap client create` 手册页

  > NetApp 最佳实践是使用 Start TLS ，而不是 LDAPS 。

- * 启动 TL*

  （也称为 *start_tls* ， *STARTTLS _* 和 *_Starttls* ）一种使用 TLS 协议提供安全通信的机制。

ONTAP 使用 STARTTLS 保护 LDAP 通信，并使用默认 LDAP 端口（389）与 LDAP 服务器进行通信。必须将 LDAP 服务器配置为允许通过 LDAP 端口 389 进行连接；否则，从 SVM 到 LDAP 服务器的 LDAP TLS 连接将失败。

ONTAP 如何使用 LDAPS

ONTAP 支持 TLS 服务器身份验证，从而使 SVM LDAP 客户端能够在绑定操作期间确认 LDAP 服务器的身份。启用了 TLS 的 LDAP 客户端可以使用公共密钥加密的标准技术来检查服务器的证书和公有 ID 是否有效以及是否由客户端的可信 CA 列表中列出的证书颁发机构（CA）颁发。

LDAP 支持 STARTTLS 使用 TLS 对通信进行加密。StartTLS 以标准 LDAP 端口（389）上的纯文本连接开头，然后该连接升级到 TLS 。

ONTAP 支持以下功能：

- LDAPS 用于 Active Directory 集成的 LDAP 服务器和 SVM 之间的 SMB 相关流量
- LDAP 流量的 LDAPS ，用于名称映射和其他 UNIX 信息

  可以使用 Active Directory 集成的 LDAP 服务器或基于 UNIX 的 LDAP 服务器来存储 LDAP 名称映射的信息以及其他 UNIX 信息，例如用户，组和网络组。

- 自签名根 CA 证书

  使用 Active Directory 集成的 LDAP 时，在域中安装 Windows Server 证书服务时会生成自签名根证书。使用基于 UNIX 的 LDAP 服务器进行 LDAP 名称映射时，系统会使用适用于该 LDAP 应用程序的方法生成并保存自签名根证书。

默认情况下、LDIPS处于禁用状态。

启用 LDAP RFC2307bis 支持

如果您要使用 LDAP 并需要使用嵌套组成员资格的附加功能，则可以将 ONTAP 配置为启用 LDAP RFC2307bis 支持。

您需要的内容

您必须已为要使用的一个默认 LDAP 客户端模式创建一个副本。

关于此任务

在 LDAP 客户端模式中，组对象使用 memberUid 属性。此属性可以包含多个值，并列出属于该组的用户的名称。在启用了 RFC2307bis 的 LDAP 客户端模式中，组对象使用 uniqueMember 属性。此属性可以包含 LDAP 目录中另一个对象的完整可分辨名称（DN）。这样，您就可以使用嵌套组，因为组可以将其他组作为成员。

用户所属的组不应超过 256 个，包括嵌套组。ONTAP 会忽略超过 256 组限制的任何组。

默认情况下， RFC2307bis 支持处于禁用状态。

> 使用 MS-AD-BIS 模式创建 LDAP 客户端时， ONTAP 会自动启用 RFC2307bis 支持。

对于追加信息，请参见 "NetApp 技术报告 4835：《如何在 ONTAP 中配置 LDAP 》"。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 修改复制的 RFC2307 LDAP 客户端模式以启用 RFC2307bis 支持：

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. 修改模式以匹配 LDAP 服务器中支持的对象类：

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. 修改模式以匹配 LDAP 服务器中支持的属性名称：

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -unique-member-attribute attribute_name
   ```

5. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

LDAP 目录搜索的配置选项

您可以通过配置 ONTAP LDAP 客户端以最适合您的环境的方式连接到 LDAP 服务器来优化 LDAP 目录搜索，包括用户，组和网络组信息。您需要了解默认 LDAP 基础和范围搜索值何时足够，以及在自定义值更合适时需要指定哪些参数。

LDAP 客户端的用户，组和网络组信息搜索选项有助于避免 LDAP 查询失败，从而避免客户端无法访问存储系统。它们还有助于确保搜索尽可能高效，以避免客户端性能问题。

默认基础和范围搜索值

LDAP 基础是 LDAP 客户端用于执行 LDAP 查询的默认基础 DN 。所有搜索，包括用户，组和网络组搜索，均使用基础 DN 完成。如果 LDAP 目录相对较小且所有相关条目都位于同一 DN 中，则此选项适用。

如果未指定自定义基础DN、则默认值为 `root`。这意味着每个查询都会搜索整个目录。尽管这样可以最大限度地提高 LDAP 查询成功的机会，但它效率低下，并会显著降低大型 LDAP 目录的性能。

LDAP 基础范围是 LDAP 客户端用于执行 LDAP 查询的默认搜索范围。所有搜索，包括用户，组和网络组搜索，均使用基础范围完成。它将确定 LDAP 查询是仅搜索命名条目， DN 下一级的条目还是该 DN 下的整个子树。

如果未指定自定义基础范围、则默认值为 `subtree`。这意味着每个查询都会搜索 DN 下的整个子树。尽管这样可以最大限度地提高 LDAP 查询成功的机会，但它效率低下，并会显著降低大型 LDAP 目录的性能。

自定义基础和范围搜索值

您也可以为用户，组和网络组搜索指定单独的基准值和范围值。通过这种方式限制查询的搜索基础和范围可以显

著提高性能，因为它会将搜索限制为 LDAP 目录的较小部分。

如果指定自定义基础值和范围值，则这些值将覆盖用户，组和网络组搜索的常规默认搜索基础和范围。用于指定自定义基础值和范围值的参数可在高级权限级别使用。

LDAP 客户端参数 …	指定自定义 …
`-base-dn`	所有 LDAP 搜索的基础 DN 如果需要，可以输入多个值（例如，如果在 ONTAP 9.5 及更高版本中启用了 LDAP 转介跟踪）。
`-base-scope`	所有 LDAP 搜索的基本范围
`-user-dn`	所有 LDAP 用户搜索的基础 DNS 此参数也适用于适用场景用户名映射搜索。
`-user-scope`	所有 LDAP 用户搜索的基本范围此参数也适用于适用场景用户名映射搜索。
`-group-dn`	所有 LDAP 组搜索的基础 DNS
`-group-scope`	所有 LDAP 组搜索的基础范围
`-netgroup-dn`	所有 LDAP 网络组搜索的基础 DNS
`-netgroup-scope`	所有 LDAP 网络组搜索的基本范围

多个自定义基础 **DN** 值

如果 LDAP 目录结构更复杂，则可能需要指定多个基础 DNS 来搜索 LDAP 目录的多个部分以查找某些信息。您可以为用户，组和网络组 DN 参数指定多个 DNS ，方法是使用分号（；）将其分隔开，并使用双引号（"）将整个 DN 搜索列表括起来。如果 DN 包含分号，则必须在 DN 中的分号前面添加一个转义字符（\）。

请注意，范围适用场景是为相应参数指定的整个 DNS 列表。例如，如果为用户范围指定了一个包含三个不同用户 DNS 和子树的列表，则 LDAP 用户搜索将在整个子树中搜索三个指定 DNS 中的每个 DNS 。

从 ONTAP 9.5 开始，您还可以指定 ldap_referral Chasing ，这样，如果主 LDAP 服务器未返回 LDAP 转介响应，则 ONTAP LDAP 客户端可以将查找请求转介给其他 LDAP 服务器。客户端使用该转介数据从转介数据中所述的服务器检索目标对象。要搜索转介 LDAP 服务器中的对象，可以在 LDAP 客户端配置中将转介对象的基础 DN 添加到基础 DN 中。但是、只有在启用转介跟踪(使用)后、才会查找转介对象 `-referral-enabled true` 选项)。

提高 **LDAP** 目录 **netgroup-by-host** 搜索的性能

如果 LDAP 环境配置为允许按主机搜索网络组，则可以将 ONTAP 配置为利用此功能并按主机执行网络组搜索。这样可以显著加快网络组搜索速度，并减少因网络组搜索期间出现延迟而可能导致的 NFS 客户端访问问题。

您需要的内容

LDAP目录必须包含 `netgroup.byhost` 映射。

DNS 服务器应同时包含 NFS 客户端的正向（A）和反向（PTR）查找记录。

在网络组中指定 IPv6 地址时，必须始终按照 RFC 5952 中的说明缩短和压缩每个地址。

关于此任务

NIS服务器将网络组信息存储在三个单独的映射中、这些映射称为 `netgroup`， `netgroup.byuser`，和 `netgroup.byhost`。的用途 `netgroup.byuser` 和 `netgroup.byhost` 映射用于加快网络组搜索速度。ONTAP 可以在 NIS 服务器上按主机执行网络组搜索，以缩短挂载响应时间。

默认情况下、LDAP目录不具有此类 `netgroup.byhost` 映射为NIS服务器。但是、借助第三方工具、可以导入NIS `netgroup.byhost` 映射到LDAP目录以启用按主机快速网络组搜索。如果您已将LDAP环境配置为允许按主机搜索网络组、则可以使用配置ONTAP LDAP客户端 `netgroup.byhost` 映射名称、DN和搜索范围、以加快按主机搜索网络组的速度。

通过更快地接收按主机搜索网络组的结果， ONTAP 可以在 NFS 客户端请求访问导出时更快地处理导出规则。这样可以减少因网络组搜索延迟问题而导致访问延迟的可能性。

步骤

1. 获取NIS的准确完整可分辨名称 `netgroup.byhost` 映射已导入到LDAP目录。

   映射 DN 可能因用于导入的第三方工具而异。为了获得最佳性能，应指定确切的映射 DN 。

2. 将权限级别设置为高级： `set -privilege advanced`

3. 在Storage Virtual Machine (SVM)的LDAP客户端配置中启用按主机搜索网络组： `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost-dn netgroup-by-host_map_distinguished_name -netgroup-byhost-scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled` {`true` `false`}启用或禁用对LDAP目录的按主机网络组搜索。默认值为 `false`。

   `-netgroup-byhost-dn` `netgroup-by-host_map_distinguished_name` 指定的可分辨名称 `netgroup.byhost` 映射到LDAP目录中。它会覆盖 netgroup-by-host 搜索的基础 DN 。如果不指定此参数，则 ONTAP 将改用基础 DN 。

   `-netgroup-byhost-scope` {`base`|`onelevel` `subtree`}指定按主机搜索网络组的搜索范围。如果未指定此参数、则默认值为 `subtree`。

   如果LDAP客户端配置尚不存在、则可以在使用创建新的LDAP客户端配置时通过指定这些参数来启用按主机进行网络组搜索 `vserver services name-service ldap client create` 命令：

   > 从ONTAP 9.2开始、此字段为 `-ldap-servers` 替换字段 `-servers`。此新字段可以使用 LDAP 服务器的主机名或 IP 地址。

4. 返回到管理权限级别： `set -privilege admin`

示例

以下命令将修改名为"`ldap_corp`"的现有LDAP客户端配置、以使用启用netgroup-by主机搜索 `netgroup.byhost` 映射名为"`nisMapName="netgroup.byHost"、dc=corp、dc=ex例如、dc=com`"和默认搜索范围 `subtree`：

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

完成后

。 `netgroup.byhost` 和 `netgroup` 目录中的映射必须始终保持同步、以避免出现客户端访问问题。

相关信息

"IETF RFC 5952： IPv6 地址文本表示建议"

使用**LDAP**快速绑定进行**nsswitch**身份验证

从ONTAP 9.11.1开始、您可以利用ldap_fast bind_功能(也称为_concurrent bind_)来更快、更简单地处理客户端身份验证请求。要使用此功能、LDAP服务器必须支持快速绑定功能。

关于此任务

如果没有快速绑定、ONTAP 将使用LDAP简单绑定向LDAP服务器对管理员用户进行身份验证。使用此身份验证方法、ONTAP 会向LDAP服务器发送用户或组名称、接收存储的哈希密码、并将服务器哈希代码与本地通过用户密码生成的哈希密码进行比较。如果它们相同、则ONTAP 会授予登录权限。

借助快速绑定功能、ONTAP 仅通过安全连接向LDAP服务器发送用户凭据(用户名和密码)。然后、LDAP服务器会验证这些凭据并指示ONTAP 授予登录权限。

快速绑定的一个优势是、ONTAP 无需支持LDAP服务器支持的每个新哈希算法、因为密码哈希是由LDAP服务器执行的。

"了解如何使用快速绑定。"

您可以使用现有LDAP客户端配置进行LDAP快速绑定。但是、强烈建议为LDAP客户端配置TLS或LDAPS；否则、密码将通过线缆以纯文本形式发送。

要在ONTAP 环境中启用LDAP快速绑定、您必须满足以下要求：

- 必须在支持快速绑定的LDAP服务器上配置ONTAP 管理员用户。
- 必须在名称服务开关(nsswitch)数据库中为LDAP配置ONTAP SVM。
- 必须使用快速绑定为nsswitch身份验证配置ONTAP 管理员用户和组帐户。

步骤

1. 与LDAP管理员确认LDAP服务器支持LDAP快速绑定。
2. 确保已在LDAP服务器上配置ONTAP 管理员用户凭据。
3. 验证是否已为LDAP快速绑定正确配置管理或数据SVM。

a. 要确认LDAP快速绑定服务器已在LDAP客户端配置中列出、请输入：

```
vserver services name-service ldap client show
```

"了解LDAP客户端配置。"

b. 以确认此情况 `ldap` 是为nsswitch配置的源之一 `passwd` 数据库、输入：

```
vserver services name-service ns-switch show
```

"了解nsswitch配置。"

4. 确保管理员用户正在使用nsswitch进行身份验证、并且已在其帐户中启用LDAP快速绑定身份验证。

   - 对于现有用户、输入 `security login modify` 并验证以下参数设置：

     `-authentication-method nsswitch`

     `-is-ldap-fastbind true`

   - 对于新的管理员用户、请参见 "启用LDAP或NIS帐户访问。"

显示**LDAP**统计信息

从 ONTAP 9.2 开始，您可以显示存储系统上 Storage Virtual Machine （SVM）的 LDAP 统计信息，以监控性能并诊断问题。

您需要的内容

- 您必须已在 SVM 上配置 LDAP 客户端。
- 您必须已确定可从中查看数据的 LDAP 对象。

步骤

1. 查看计数器对象的性能数据：

```
statistics show
```

示例

以下示例显示了对象的性能数据 `secd_external_service_op`：

```
cluster::*> statistics show -vserver vserverName -object
secd_external_service_op -instance "vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1"

Object: secd_external_service_op
Instance: vserverName:LDAP (NIS & Name
Mapping):GetUserInfoFromName:1.1.1.1
Start-time: 4/13/2016 22:15:38
End-time: 4/13/2016 22:15:38
Scope: vserverName
Counter                             Value
-------------------------------- --------------------------------
instance_name                       vserverName:LDAP (NIS & Name
                                    Mapping):GetUserInfoFromName:
                                    1.1.1.1
last_modified_time                  1460610787
node_name                           nodeName
num_not_found_responses             1
num_request_failures                1
num_requests_sent                   1
num_responses_received              1
num_successful_responses            0
num_timeouts                        0
operation                           GetUserInfoFromName
process_name                        secd
request_latency                     52131us
```

配置名称映射

配置名称映射概述

ONTAP 使用名称映射将 SMB 身份映射到 UNIX 身份，将 Kerberos 身份映射到 UNIX 身份以及将 UNIX 身份映射到 SMB 身份。无论用户是从 NFS 客户端还是从 SMB 客户端进行连接， IT 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，不打算在卷上使用 SMB 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SMB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SMB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SMB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SMB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SMB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	｛asterisk｝ ｛反斜杠｝ ｛反斜杠｝ 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。
*	｛asterisk｝ ｛反斜杠｝ ｛反斜杠｝ ｛asterisk｝	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 ｛asterisk｝ ｛un斜 杠｝ ｛un斜 杠｝ ｛asterisk｝ 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 注意：如果为名称映射配置了IP限定符条目、则不允许进行交换。	`vserver name-mapping swap`
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。

为 **Windows NFS** 客户端启用访问

ONTAP 支持从 Windows NFSv3 客户端访问文件。这意味着、运行支持NFSv3的Windows操作系统的客户端可以访问集群上NFSv3导出上的文件。要成功使用此功能，您必须正确配置 Storage Virtual Machine （ SVM ）并了解某些要求和限制。

关于此任务

默认情况下， Windows NFSv3 客户端支持处于禁用状态。

开始之前

必须在 SVM 上启用 NFSv3 。

步骤

1. 启用 Windows NFSv3 客户端支持：

   ```
   vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly disabled
   ```

2. 在支持Windows NFSv3客户端的所有SVM上、禁用 `-enable-ejukebox` 和 `-v3-connection-drop` 参数：

   ```
   vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection -drop disabled
   ```

   Windows NFSv3 客户端现在可以在存储系统上挂载导出。

3. 通过指定、确保每个Windows NFSv3客户端都使用硬挂载 `-o mtype=hard` 选项

   这是确保可靠挂载所必需的。

   ```
   mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
   ```

在 NFS 客户端上启用 NFS 导出显示

NFS客户端可以使用 `showmount -e` 命令以查看可从ONTAP NFS服务器导出的列表。这有助于用户确定要挂载的文件系统。

从 ONTAP 9.2 开始，默认情况下， ONTAP 允许 NFS 客户端查看导出列表。在早期版本中、 `showmount` 的选项 `vserver nfs modify` 命令必须显式启用。要查看导出列表，应在 SVM 上启用 NFSv3 。

示例

以下命令显示了名为 vs1 的 SVM 上的 showmount 功能：

```
clusterl : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
------- ---------
vs1    enabled
```

在 NFS 客户端上执行的以下命令显示 IP 地址为 10.63.21.9 的 NFS 服务器上的导出列表：

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix        (everyone)
/unix/unixl  (everyone)
/unix/unix2  (everyone)
/            (everyone)
```

使用NFS管理文件访问

启用或禁用NFSv3

您可以通过修改来启用或禁用NFSv3 `-v3` 选项这样，客户端就可以使用 NFSv3 协议访问文件。默认情况下， NFSv3 处于启用状态。

步骤

1. 执行以下操作之一：

如果您要 …	输入命令 …
启用 NFSv3：	`vserver nfs modify -vserver vserver_name -v3 enabled`
禁用NFSv3	`vserver nfs modify -vserver vserver_name -v3 disabled`

启用或禁用 NFSv4.0

您可以通过修改来启用或禁用NFSv4.0 `-v4.0` 选项这样，使用 NFSv4.0 协议的客户端就可以访问文件。在 ONTAP 9.1.1 中，默认情况下会启用 NFSv4.0 ；在早期版本中，默认情况下会禁用 NFSv4.0 。

步骤

1. 执行以下操作之一：

如果您要 ...	输入以下命令 ...
启用 NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 enabled`
禁用 NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 disabled`

启用或禁用NFSv4.1

您可以通过修改来启用或禁用NFSv4.1 `-v4.1` 选项这样，使用 NFSv4.1 协议的客户端便可访问文件。在 ONTAP 9.1.1 中，默认启用 NFSv4.1 ；在早期版本中，默认禁用 NFSv4.1 。

步骤

1. 执行以下操作之一：

如果您要 ...	输入以下命令 ...
启用NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 enabled`
禁用NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 disabled`

管理NFSv4存储池限制

从ONTAP 9.13开始、管理员可以使NFSv4服务器在达到每个客户端存储池资源限制时拒绝向NFSv4客户端提供资源。如果客户端使用的NFSv4存储池资源过多、则可能会导致其他NFSv4客户端因NFSv4存储池资源不可用而被阻止。

通过启用此功能、客户还可以查看每个客户端的活动存储池资源消耗情况。这样可以更轻松地确定耗尽系统资源的客户端、并可以按客户端设置资源限制。

查看已用存储池资源

。`vserver nfs storepool show` 命令可显示已使用的存储池资源数量。存储池是NFSv4客户端使用的资源池。

步骤

1. 以管理员身份运行 `vserver nfs storepool show` 命令以显示NFSv4客户端的存储池信息。

示例

此示例显示了NFSv4客户端的存储池信息。

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-Ip: 10.0.1.1

Client-Ip Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount

-------------- --------- --------- ---------- ---------- ----------
---------

10.0.2.1          nfs4.1     true    2 1 0 4

10.0.2.2          nfs4.2     true    2 1 0 4

2 entries were displayed.
```

启用或禁用存储池限制控制

管理员可以使用以下命令启用或禁用存储池限制控制。

步骤

1. 以管理员身份执行以下操作之一：

如果您要 ...	输入以下命令 ...
启用存储池限制控制	`vserver nfs storepool config modify -limit-enforce enabled`
禁用存储池限制控制	`vserver nfs storepool config modify -limit-enforce disabled`

查看被阻止的客户端列表

如果启用了存储池限制、则管理员可以查看在达到每个客户端资源阈值时哪些客户端被阻止。管理员可以使用以下命令查看哪些客户端已标记为被阻止的客户端。

步骤

1. 使用 `vserver nfs storepool blocked-client show` 命令以显示NFSv4阻止的客户端列表。

从阻止的客户端列表中删除客户端

达到每个客户端阈值的客户端将断开连接并添加到块-客户端缓存中。管理员可以使用以下命令从块客户端缓存中删除客户端。这样、客户端便可连接到ONTAP NFSv4服务器。

步骤

1. 使用 `vserver nfs storepool blocked-client flush -client-ip <ip address>` 命令以转储存储池已阻止的客户端缓存。
2. 使用 `vserver nfs storepool blocked-client show` 命令以验证客户端是否已从块客户端缓存中删除。

示例

此示例显示一个被阻止的客户端、其IP地址"10.2.1.1"正在从所有节点转储。

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
----------
10.1.1.1

1 entries were displayed.
```

启用或禁用 pNFS

pNFS 允许 NFS 客户端直接并联对存储设备执行读 / 写操作，从而绕过 NFS 服务器作为潜在瓶颈，从而提高性能。要启用或禁用pNFS (并行NFS)、您可以修改 `-v4.1-pnfs` 选项

ONTAP 版本	pNFS 默认值为 ...
9.8或更高版本	已禁用
9.7或更早版本	enabled

您需要的内容

要使用 pNFS ，需要 NFSv4.1 支持。

如果要启用 pNFS ，必须先禁用 NFS 转介。它们不能同时启用。

如果在 SVM 上将 pNFS 与 Kerberos 结合使用，则必须在 SVM 上的每个 LIF 上启用 Kerberos 。

步骤

1. 执行以下操作之一：

如果您要 ...	输入命令 ...
启用 pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled`
禁用 pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled`

相关信息

- NFS中继概述

通过 TCP 和 UDP 控制 NFS 访问

您可以通过修改来启用或禁用通过TCP和UDP对Storage Virtual Machine (SVM)的NFS访问 `-tcp` 和 `-udp` 参数。这样，您可以控制 NFS 客户端是否可以在环境中通过 TCP 或 UDP 访问数据。

关于此任务

这些参数仅适用于 NFS 。它们不会影响辅助协议。例如，如果禁用基于 TCP 的 NFS ，则通过 TCP 的挂载操作仍会成功。要完全阻止 TCP 或 UDP 流量，您可以使用导出策略规则。

> 在为 NFS 禁用 TCP 之前，必须关闭 SnapDiff RPC 服务器，以避免出现命令失败错误。您可以使用命令禁用TCP `vserver snapdiff-rpc-server off -vserver vserver name`。

步骤

1. 执行以下操作之一：

如果您希望 NFS 访问 ...	输入命令 ...
已通过 TCP 启用	`vserver nfs modify -vserver vserver_name -tcp enabled`
已通过 TCP 禁用	`vserver nfs modify -vserver vserver_name -tcp disabled`
通过 UDP 启用	`vserver nfs modify -vserver vserver_name -udp enabled`
已通过UDP禁用	`vserver nfs modify -vserver vserver_name -udp disabled`

控制来自非保留端口的 NFS 请求

您可以通过启用来拒绝来自非保留端口的NFS挂载请求 `-mount-rootonly` 选项要拒绝来自非保留端口的所有NFS请求、您可以启用 `-nfs-rootonly` 选项

关于此任务

默认情况下、是选项 `-mount-rootonly` 为 `enabled`。

默认情况下、是选项 `-nfs-rootonly` 为 `disabled`。

这些选项不适用于空操作步骤。

步骤

1. 执行以下操作之一：

如果您要 …	输入命令 …
允许来自非保留端口的 NFS 挂载请求	`vserver nfs modify -vserver vserver_name -mount -rootonly disabled`
拒绝来自非保留端口的 NFS 挂载请求	`vserver nfs modify -vserver vserver_name -mount -rootonly enabled`
允许来自非保留端口的所有 NFS 请求	`vserver nfs modify -vserver vserver_name -nfs -rootonly disabled`
拒绝来自非保留端口的所有 NFS 请求	`vserver nfs modify -vserver vserver_name -nfs -rootonly enabled`

处理未知 **UNIX** 用户对 **NTFS** 卷或 **qtree** 的 **NFS** 访问

如果 ONTAP 无法识别尝试使用 NTFS 安全模式连接到卷或 qtree 的 UNIX 用户，则无法将该用户显式映射到 Windows 用户。您可以将 ONTAP 配置为拒绝访问此类用户以提高安全性，或者将其映射到默认 Windows 用户以确保所有用户的最低访问级别。

您需要的内容

如果要启用此选项，必须配置默认 Windows 用户。

关于此任务

如果 UNIX 用户尝试访问采用 NTFS 安全模式的卷或 qtree ，则必须先将 UNIX 用户映射到 Windows 用户，以便 ONTAP 能够正确评估 NTFS 权限。但是，如果 ONTAP 无法在已配置的用户信息名称服务源中查找 UNIX 用户的名称，则无法将 UNIX 用户显式映射到特定的 Windows 用户。您可以通过以下方式决定如何处理此类未知 UNIX 用户：

- 拒绝对未知 UNIX 用户的访问。

  这样就要求所有 UNIX 用户都显式映射才能访问 NTFS 卷或 qtree ，从而实现更严格的安全性。

- 将未知 UNIX 用户映射到默认 Windows 用户。

  这样可以确保所有用户都通过默认 Windows 用户获得对 NTFS 卷或 qtree 的最低访问级别，从而降低安全性，但更方便。

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：

如果要为未知 UNIX 用户使用默认 Windows 用户 …	输入命令 …
enabled	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled`
已禁用	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled`

3. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

使用非预留端口挂载 **NFS** 导出的客户端注意事项

。 `-mount-rootonly` 如果存储系统必须支持使用非保留端口挂载NFS导出的客户端、则即使用户以root身份登录、也必须在该存储系统上禁用此选项。此类客户端包括 Hummingbird 客户端和 Solaris NFS/IPv6 客户端。

如果 `-mount-rootonly` 选项处于启用状态时、ONTAP不允许使用非保留端口(即数量超过1、023的端口)的NFS客户端挂载NFS导出。

通过验证域对网络组执行更严格的访问检查

默认情况下， ONTAP 在评估网络组的客户端访问时会执行额外的验证。此附加检查可确保客户端的域与 Storage Virtual Machine （ SVM ）的域配置匹配。否则， ONTAP 将拒绝客户端访问。

关于此任务

当 ONTAP 评估客户端访问的导出策略规则且导出策略规则包含网络组时， ONTAP 必须确定客户端的 IP 地址是否属于该网络组。为此， ONTAP 会使用 DNS 将客户端的 IP 地址转换为主机名，并获取完全限定域名（ FQDN ）。

如果网络组文件仅列出主机的短名称，而主机的短名称存在于多个域中，则来自不同域的客户端可以在不进行此检查的情况下获得访问权限。

为了防止这种情况发生， ONTAP 会将从主机的 DNS 返回的域与为 SVM 配置的 DNS 域名列表进行比较。如果匹配，则允许访问。如果不匹配，则拒绝访问。

默认情况下，此验证处于启用状态。您可以通过修改对其进行管理 `-netgroup-dns-domain-search` 参数、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. 执行所需的操作：

网络组的域验证条件	输入 ...
enabled	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled`
已禁用	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled`

3. 将权限级别设置为 admin ：

   ```
   set -privilege admin
   ```

修改用于 **NFSv3** 服务的端口

存储系统上的 NFS 服务器使用挂载守护进程和网络锁定管理器等服务通过特定的默认网络端口与 NFS 客户端进行通信。在大多数 NFS 环境中，默认端口可以正常工作且不需要修改，但如果要在 NFSv3 环境中使用不同的 NFS 网络端口，则可以这样做。

您需要的内容

更改存储系统上的 NFS 端口要求所有 NFS 客户端都重新连接到系统，因此您应在进行更改之前将此信息传达给用户。

关于此任务

您可以为每个 Storage Virtual Machine （ SVM ）设置 NFS 挂载守护进程，网络锁定管理器，网络状态监控器和 NFS 配额守护进程服务使用的端口。端口号更改会影响通过 TCP 和 UDP 访问数据的 NFS 客户端。

无法更改 NFSv4 和 NFSv4.1 的端口。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 禁用对 NFS 的访问：

```
vserver nfs modify -vserver vserver_name -access false
```

3. 为特定 NFS 服务设置 NFS 端口：

```
vserver nfs modify -vserver vserver_namenfs_port_parameterport_number
```

NFS 端口参数	Description	默认端口
`-mountd-port`	NFS 挂载守护进程	635
`-nlm-port`	网络锁定管理器	4045
`-nsm-port`	网络状态监控器	4046
`-rquotad-port`	NFS 配额守护进程	4049-51

除了默认端口之外，允许的端口号范围为 1024 到 65535 。每个 NFS 服务都必须使用唯一的端口。

4. 启用对 NFS 的访问：

```
vserver nfs modify -vserver vserver_name -access true
```

5. 使用 `network connections listening show` 命令以验证端口号是否更改。
6. 返回到管理权限级别：

```
set -privilege admin
```

示例

以下命令会将名为 vs1 的 SVM 上的 NFS 挂载守护进程端口设置为 1113 ：

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- --------------------------------  ----------------
Node: cluster1-01
Cluster          cluster1-01_clus_1:7700          TCP/ctlopcp
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:1113                       TCP/mount
vs1              data1:1113                       UDP/mount
...
vs1::*> set -privilege admin
```

用于管理NFS服务器的命令

您可以使用特定的 ONTAP 命令来管理 NFS 服务器。

如果您要 ...	使用此命令 ...
创建 NFS 服务器	`vserver nfs create`
显示 NFS 服务器	`vserver nfs show`
修改 NFS 服务器	`vserver nfs modify`
删除 NFS 服务器	`vserver nfs delete`

隐藏 `.snapshot` 列出NFSv3挂载点下的目录 显式访问 `.snapshot` 即使启用了该选项、目录仍被允许。	`vserver nfs` 命令 `-v3-hide-snapshot` 选项已启用

有关详细信息，请参见每个命令的手册页。

对名称服务问题进行故障排除

当客户端因名称服务问题而遇到访问失败时、您可以使用 `vserver services name-service getxxbyyy` 命令系列、用于手动执行各种名称服务查找并检查查找的详细信息和结果、以帮助进行故障排除。

关于此任务

- 对于每个命令，您可以指定以下内容：
  - 要执行查找的节点或 Storage Virtual Machine （ SVM ）的名称。

    这样，您可以测试特定节点或 SVM 的名称服务查找，以缩小潜在名称服务配置问题描述的搜索范围。
  - 是否显示用于查找的源。

    这样，您可以检查是否使用了正确的源。
- ONTAP 会根据配置的名称服务切换顺序选择用于执行查找的服务。
- 这些命令可在高级权限级别下使用。

步骤

1. 执行以下操作之一：

检索…	使用命令 …
主机名的IP地址	`vserver services name-service getxxbyyy getaddrinfo` `vserver services name-service getxxbyyy gethostbyname` (仅限IPv4地址)
按组ID显示组成员	`vserver services name-service getxxbyyy getgrbygid`
按组名称显示组成员	`vserver services name-service getxxbyyy getgrbyname`
用户所属组的列表	`vserver services name-service getxxbyyy getgrlist`

IP地址的主机名	`vserver services name-service getxxbyyy getnameinfo` `vserver services name-service getxxbyyy gethostbyaddr` (仅限IPv4地址)
按用户名显示用户信息	`vserver services name-service getxxbyyy getpwbyname` 您可以通过指定来测试RBAC用户的名称解析 `-use-rbac` 参数为 `true`。
按用户ID显示用户信息	`vserver services name-service getxxbyyy getpwbyuid` 您可以通过指定来测试RBAC用户的名称解析 `-use-rbac` 参数为 `true`。
客户端的网络组成员资格	`vserver services name-service getxxbyyy netgrp`
使用netgroup-by-host搜索的客户端的网络组成员资格	`vserver services name-service getxxbyyy netgrpbyhost`

以下示例显示了通过尝试获取主机acast1.eng.example.com的IP地址来对SVM vs1执行的DNS查找测试：

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

以下示例显示了通过尝试检索UID为501768的用户的用户信息来对SVM vs1执行的NIS查找测试：

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvc2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

以下示例显示了通过尝试检索名为ldap1的用户的用户信息来对SVM vs1执行的LDAP查找测试：

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

以下示例显示了SVM vs1的网络组查找测试、该测试尝试确定客户端dnshost0是否为网络组lnetgroup136的成员：

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. 分析您执行的测试的结果并采取必要的措施。

如果 ...	检查
主机名或 IP 地址查找失败或生成的结果不正确	DNS配置
LOOKUP 查询的源不正确	名称服务开关配置
用户或组查找失败或生成的结果不正确	• 名称服务开关配置 • 源配置(本地文件、NIS域、LDAP客户端) • 网络配置（例如 LIF 和路由）
主机名查找失败或超时，并且 DNS 服务器无法解析 DNS 短名称（例如 host1 ）	用于顶级域(TLD)查询的DNS配置。您可以使用禁用LD查询 `-is-tld-query-enabled false` 选项 `vserver services name-service dns modify` 命令：

相关信息

"NetApp 技术报告 4668 ：《名称服务最佳实践指南》"

验证名称服务连接

从 ONTAP 9.2 开始，您可以检查 DNS 和 LDAP 名称服务器以验证它们是否已连接到 ONTAP 。这些命令可在管理员权限级别使用。

关于此任务

您可以根据需要使用名称服务配置检查程序检查是否存在有效的 DNS 或 LDAP 名称服务配置。此验证检查可以在命令行或 System Manager 中启动。

对于 DNS 配置，所有服务器都经过测试，需要正常运行才能将此配置视为有效。对于 LDAP 配置，只要任何服务器已启动，此配置即有效。除非是、否则名称服务命令将应用配置检查程序 `skip-config-validation` 字段为true (默认值为false)。

步骤

1. 使用相应的命令检查名称服务配置。UI 将显示已配置服务器的状态。

要检查的内容	使用此命令 …
DNS 配置状态	`vserver services name-service dns check`
LDAP配置状态	`vserver services name-service ldap check`

```
cluster1::> vserver services name-service dns check -vserver vs0

Vserver         Name Server     Status  Status Details
--------------  --------------- ------- -------------------------
 vs0            10.11.12.13     up      Response time (msec): 55
 vs0            10.11.12.14     up      Response time (msec): 70
 vs0            10.11.12.15     down    Connection refused.
+-------------------------------------------------------------------+
```

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                    |
| Client Configuration Name: c1                                   |
| LDAP Status: up                                                 |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                  |
```

如果至少有一个已配置的服务器（名称服务器 /ldap-servers ）可访问并提供服务，则配置验证将成功。如果某些服务器无法访问，则会显示警告。

用于管理名称服务切换条目的命令

您可以通过创建，显示，修改和删除名称服务切换条目来管理这些条目。

如果您要 …	使用此命令 …

创建名称服务切换条目	`vserver services name-service ns-switch create`
显示名称服务切换条目	`vserver services name-service ns-switch show`
修改名称服务切换条目	`vserver services name-service ns-switch modify`
删除名称服务切换条目	`vserver services name-service ns-switch delete`

有关详细信息，请参见每个命令的手册页。

相关信息

"NetApp 技术报告 4668：《名称服务最佳实践指南》"

用于管理名称服务缓存的命令

您可以通过修改生存时间（TTL）值来管理名称服务缓存。TTL 值用于确定名称服务信息在缓存中的持久性。

要修改的 TTL 值	使用此命令 ...
UNIX 用户	`vserver services name-service cache unix-user settings`
UNIX 组	`vserver services name-service cache unix-group settings`
UNIX 网络组	`vserver services name-service cache netgroups settings`
主机	`vserver services name-service cache hosts settings`
组成员资格	`vserver services name-service cache group-membership settings`

相关信息

"ONTAP 9命令"

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 注意：如果为名称映射配置了IP限定符条目、则不允许进行交换。	`vserver name-mapping swap`
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。

用于管理本地 **UNIX** 用户的命令

您可以使用特定的 ONTAP 命令来管理本地 UNIX 用户。

如果您要 ...	使用此命令 ...
创建本地 UNIX 用户	`vserver services name-service unix-user create`
从 URI 加载本地 UNIX 用户	`vserver services name-service unix-user load-from-uri`
显示本地 UNIX 用户	`vserver services name-service unix-user show`
修改本地 UNIX 用户	`vserver services name-service unix-user modify`
删除本地 UNIX 用户	`vserver services name-service unix-user delete`

有关详细信息，请参见每个命令的手册页。

用于管理本地 **UNIX** 组的命令

您可以使用特定的 ONTAP 命令来管理本地 UNIX 组。

如果您要 ...	使用此命令 ...
创建本地 UNIX 组	`vserver services name-service unix-group create`

将用户添加到本地 UNIX 组	`vserver services name-service unix-group adduser`
从 URI 加载本地 UNIX 组	`vserver services name-service unix-group load-from-uri`
显示本地 UNIX 组	`vserver services name-service unix-group show`
修改本地 UNIX 组	`vserver services name-service unix-group modify`
从本地 UNIX 组中删除用户	`vserver services name-service unix-group deluser`
删除本地 UNIX 组	`vserver services name-service unix-group delete`

有关详细信息，请参见每个命令的手册页。

本地 **UNIX** 用户，组和组成员的限制

ONTAP 对集群中的最大 UNIX 用户和组数以及用于管理这些限制的命令进行了限制。这些限制可以防止管理员在集群中创建过多的本地 UNIX 用户和组，从而有助于避免性能问题。

本地 UNIX 用户组和组成员的总数存在限制。本地 UNIX 用户有单独的限制。这些限制在集群范围内。每个新限制都设置为默认值，您可以修改该值，但最多不能修改为预先分配的硬限制。

数据库	默认限制	硬限制
本地 UNIX 用户	32、768	这是一项很好的
本地 UNIX 组和组成员	32、768	这是一项很好的

管理本地 **UNIX** 用户和组的限制

您可以使用特定的 ONTAP 命令来管理本地 UNIX 用户和组的限制。集群管理员可以使用这些命令对集群中被认为与本地 UNIX 用户和组数量过多相关的性能问题进行故障排除。

关于此任务

集群管理员可以在高级权限级别使用这些命令。

步骤

1. 执行以下操作之一：

如果您要 ...	使用命令 ...
显示有关本地 UNIX 用户限制的信息	`vserver services unix-user max-limit show`
显示有关本地 UNIX 组限制的信息	`vserver services unix-group max-limit show`
修改本地 UNIX 用户限制	`vserver services unix-user max-limit modify`
修改本地 UNIX 组限制	`vserver services unix-group max-limit modify`

有关详细信息，请参见每个命令的手册页。

用于管理本地网络组的命令

您可以通过以下方式管理本地网络组：从 URI 加载本地网络组，在节点间验证其状态，显示这些网络组并将其删除。

如果您要 ...	使用命令 ...
从 URI 加载网络组	`vserver services name-service netgroup load`
验证节点间网络组的状态	`vserver services name-service netgroup status` 可在高级权限级别及更高权限级别使用。
显示本地网络组	`vserver services name-service netgroup file show`
删除本地网络组	`vserver services name-service netgroup file delete`

有关详细信息，请参见每个命令的手册页。

用于管理 **NIS** 域配置的命令

您可以使用特定的 ONTAP 命令来管理 NIS 域配置。

如果您要 ...	使用此命令 ...
创建 NIS 域配置	`vserver services name-service nis-domain create`
显示NIS域配置	`vserver services name-service nis-domain show`

显示 NIS 域配置的绑定状态	`vserver services name-service nis-domain show-bound`
显示NIS统计信息	`vserver services name-service nis-domain show-statistics` 可在高级权限级别及更高权限级别使用。
清除 NIS 统计信息	`vserver services name-service nis-domain clear-statistics` 可在高级权限级别及更高权限级别使用。
修改 NIS 域配置	`vserver services name-service nis-domain modify`
删除 NIS 域配置	`vserver services name-service nis-domain delete`
为按主机搜索网络组启用缓存	`vserver services name-service nis-domain netgroup-database config modify` 可在高级权限级别及更高权限级别使用。

有关详细信息，请参见每个命令的手册页。

用于管理 **LDAP** 客户端配置的命令

您可以使用特定的 ONTAP 命令来管理 LDAP 客户端配置。

SVM 管理员不能修改或删除集群管理员创建的 LDAP 客户端配置。

如果您要 …	使用此命令 …
创建 LDAP 客户端配置	`vserver services name-service ldap client create`
显示 LDAP 客户端配置	`vserver services name-service ldap client show`
修改 LDAP 客户端配置	`vserver services name-service ldap client modify`
更改 LDAP 客户端绑定密码	`vserver services name-service ldap client modify-bind-password`
删除 LDAP 客户端配置	`vserver services name-service ldap client delete`

有关详细信息，请参见每个命令的手册页。

用于管理 **LDAP** 配置的命令

您可以使用特定的 ONTAP 命令来管理 LDAP 配置。

如果您要 …	使用此命令 …

创建 LDAP 配置	`vserver services name-service ldap create`
显示 LDAP 配置	`vserver services name-service ldap show`
修改 LDAP 配置	`vserver services name-service ldap modify`
删除 LDAP 配置	`vserver services name-service ldap delete`

有关详细信息，请参见每个命令的手册页。

用于管理 **LDAP** 客户端模式模板的命令

您可以使用特定的 ONTAP 命令来管理 LDAP 客户端模式模板。

SVM 管理员不能修改或删除集群管理员创建的 LDAP 客户端模式。

如果您要 …	使用此命令 …
复制现有 LDAP 模式模板	`vserver services name-service ldap client schema copy` 可在高级权限级别及更高权限级别使用。
显示 LDAP 模式模板	`vserver services name-service ldap client schema show`
修改 LDAP 模式模板	`vserver services name-service ldap client schema modify` 可在高级权限级别及更高权限级别使用。
删除 LDAP 模式模板	`vserver services name-service ldap client schema delete` 可在高级权限级别及更高权限级别使用。

有关详细信息，请参见每个命令的手册页。

用于管理 **NFS Kerberos** 接口配置的命令

您可以使用特定的 ONTAP 命令来管理 NFS Kerberos 接口配置。

如果您要 …	使用此命令 …
在 LIF 上启用 NFS Kerberos	`vserver nfs kerberos interface enable`
显示 NFS Kerberos 接口配置	`vserver nfs kerberos interface show`
修改 NFS Kerberos 接口配置	`vserver nfs kerberos interface modify`

在 LIF 上禁用 NFS Kerberos	`vserver nfs kerberos interface disable`

有关详细信息，请参见每个命令的手册页。

用于管理 **NFS Kerberos** 域配置的命令

您可以使用特定的 ONTAP 命令来管理 NFS Kerberos 域配置。

如果您要 **...**	使用此命令 **...**
创建 NFS Kerberos 域配置	`vserver nfs kerberos realm create`
显示 NFS Kerberos 域配置	`vserver nfs kerberos realm show`
修改 NFS Kerberos 域配置	`vserver nfs kerberos realm modify`
删除 NFS Kerberos 域配置	`vserver nfs kerberos realm delete`

有关详细信息，请参见每个命令的手册页。

用于管理导出策略的命令

您可以使用特定的 ONTAP 命令来管理导出策略。

如果您要 …	使用此命令 …
显示有关导出策略的信息	`vserver export-policy show`
重命名导出策略	`vserver export-policy rename`
复制导出策略	`vserver export-policy copy`
删除导出策略	`vserver export-policy delete`

有关详细信息，请参见每个命令的手册页。

用于管理导出规则的命令

您可以使用特定的 ONTAP 命令来管理导出规则。

如果您要 …	使用此命令 …
创建导出规则	`vserver export-policy rule create`

显示有关导出规则的信息	`vserver export-policy rule show`
修改导出规则	`vserver export-policy rule modify`
删除导出规则	`vserver export-policy rule delete`

> 如果您配置了多个与不同客户端匹配的相同导出规则，请确保在管理导出规则时保持同步。

有关详细信息，请参见每个命令的手册页。

配置 NFS 凭据缓存

修改 NFS 凭据缓存生存时间的原因

ONTAP 使用凭据缓存存储 NFS 导出访问的用户身份验证所需的信息，以加快访问速度并提高性能。您可以配置凭据缓存中存储信息的时间长度，以便根据您的环境对其进行自定义。

修改 NFS 凭据缓存生存时间（ TTL ）时，有多种情况可帮助解决问题。您应了解这些情形的含义以及进行这些修改的后果。

reasons

在以下情况下，请考虑更改默认 TTL：

问题描述	补救措施
由于来自 ONTAP 的请求负载较高，您环境中的名称服务器的性能正在下降。	增加缓存的肯定和否定凭据的 TTL ，以减少从 ONTAP 到名称服务器的请求数。
名称服务器管理员进行了更改，以允许访问先前被拒绝的 NFS 用户。	减少缓存的否定凭据的 TTL ，以减少 NFS 用户等待 ONTAP 从外部名称服务器请求新凭据以获得访问权限所需的时间。
名称服务器管理员进行了更改，以拒绝先前允许的 NFS 用户访问。	减少缓存肯定凭据的 TTL ，以缩短 ONTAP 从外部名称服务器请求新凭据的时间，从而使 NFS 用户现在被拒绝访问。

后果

您可以分别修改缓存肯定和否定凭据的时间长度。但是，您应该了解这种做法的优缺点。

如果您 ...	优势是 ...	缺点是 ...
增加肯定凭据缓存时间	ONTAP 向名称服务器发送凭据请求的频率较低，从而减少了名称服务器上的负载。	拒绝访问以前允许访问但不再允许访问的 NFS 用户需要更长时间。
减少肯定凭据缓存时间	拒绝访问先前允许访问但不再允许访问的 NFS 用户所需的时间更短。	ONTAP 会更频繁地向名称服务器发送凭据请求，从而增加名称服务器的负载。
增加否定凭据缓存时间	ONTAP 向名称服务器发送凭据请求的频率较低，从而减少了名称服务器上的负载。	向以前不允许访问但现在允许访问的 NFS 用户授予访问权限需要更长时间。
减少否定凭据缓存时间	为以前不允许访问但现在允许访问的 NFS 用户授予访问权限所需的时间更短。	ONTAP 会更频繁地向名称服务器发送凭据请求，从而增加名称服务器的负载。

为缓存的 **NFS** 用户凭据配置生存时间

您可以通过修改 Storage Virtual Machine （ SVM ）的 NFS 服务器来配置 ONTAP 在其内部缓存中存储 NFS 用户凭据的时间长度（生存时间或 TTL ）。这样，您就可以缓解与名称服务器上的高负载或影响 NFS 用户访问的凭据更改相关的某些问题。

关于此任务

这些参数可在高级权限级别使用。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 执行所需的操作：

要修改缓存的 TTL 的项	使用命令 ...
肯定凭据	`vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live` TTL 以毫秒为单位。从ONTAP 9.10.1及更高版本开始、默认值为1小时(3、600、000毫秒)。 在ONTAP 9.9.1及更早版本中、默认值为24小时(86、400、000毫秒)。 此值的允许范围为 1 分钟（ 60000 毫秒）到 7 天（ 604 ， 800 ， 000 毫秒）。

否定凭据	`vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live` TTL 以毫秒为单位。默认值为 2 小时（ 7 ， 200 ， 000 毫秒）。此值的允许范围为 1 分钟（ 60000 毫秒）到 7 天（ 604 ， 800 ， 000 毫秒）。

3. 返回到管理权限级别：

```
set -privilege admin
```

管理导出策略缓存

刷新导出策略缓存

ONTAP 使用多个导出策略缓存来存储与导出策略相关的信息，以加快访问速度。手动转储导出策略缓存 (`vserver export-policy cache flush`)删除可能过时的信息并强制ONTAP从相应的外部资源检索当前信息。这有助于解决与客户端访问 NFS 导出相关的各种问题。

关于此任务

由于以下原因，导出策略缓存信息可能已过时：

- 最近对导出策略规则进行的更改
- 最近对名称服务器中的主机名记录进行的更改
- 最近对名称服务器中的网络组条目进行的更改
- 从阻止网络组完全加载的网络中断中恢复

步骤

1. 如果未启用名称服务缓存，请在高级权限模式下执行以下操作之一：

要刷新的内容	输入命令 ...
所有导出策略缓存（ showmount 除外）	`vserver export-policy cache flush -vserver vserver_name`
导出策略规则访问缓存	`vserver export-policy cache flush -vserver vserver_name -cache access` 您可以包括可选 `-node` 参数以指定要转储访问缓存的节点。
主机名缓存	`vserver export-policy cache flush -vserver vserver_name -cache host`

要刷新的内容	输入命令 ...
网络组缓存	`vserver export-policy cache flush -vserver vserver_name -cache netgroup` 处理网络组需要大量资源。只有在尝试解析因网络组陈旧而导致的客户端访问问题描述时，才应刷新网络组缓存。
showmount 缓存	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

2. 如果启用了名称服务缓存，请执行以下操作之一：

要刷新的内容	输入命令 ...
导出策略规则访问缓存	`vserver export-policy cache flush -vserver vserver_name -cache access` 您可以包括可选 `-node` 参数以指定要转储访问缓存的节点。
主机名缓存	`vserver services name-service cache hosts forward-lookup delete-all`
网络组缓存	`vserver services name-service cache netgroups ip-to-netgroup delete-all` `vserver services name-service cache netgroups members delete-all` 处理网络组需要大量资源。只有在尝试解析因网络组陈旧而导致的客户端访问问题描述时，才应刷新网络组缓存。
showmount 缓存	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

显示导出策略网络组队列和缓存

ONTAP 在导入和解析网络组时使用网络组队列，并使用网络组缓存存储生成的信息。在对导出策略网络组相关问题进行故障排除时、您可以使用 `vserver export-policy netgroup queue show` 和 `vserver export-policy netgroup cache show` 用于显示网络组队列状态和网络组缓存内容的命令。

步骤

1. 执行以下操作之一：

要显示导出策略网络组 ...	输入命令 ...

队列	`vserver export-policy netgroup queue show`
缓存	`vserver export-policy netgroup cache show -vserver vserver_name`

有关详细信息，请参见每个命令的手册页。

检查客户端 **IP** 地址是否为网络组的成员

在对与网络组相关的NFS客户端访问问题进行故障排除时、您可以使用 `vserver export-policy netgroup check-membership` 命令、以帮助确定客户端IP是否为某个网络组的成员。

关于此任务

通过检查网络组成员资格，您可以确定 ONTAP 是否意识到客户端是或不是网络组的成员。此外，您还可以通过它来了解刷新网络组信息时 ONTAP 网络组缓存是否处于瞬时状态。此信息有助于您了解客户端为何可能会被意外授予或拒绝访问。

步骤

1. 检查客户端IP地址的网络组成员资格： `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

   此命令可返回以下结果：

   - 客户端是网络组的成员。

     这已通过反向查找扫描或按主机搜索网络组来确认。

   - 客户端是网络组的成员。

     已在 ONTAP 网络组缓存中找到此文件。

   - 客户端不是网络组的成员。
   - 由于 ONTAP 当前正在刷新网络组缓存，因此无法确定客户端的成员资格。

     除非这样做，否则不能明确排除成员资格。使用 `vserver export-policy netgroup queue show` 命令以监控网络组的加载、并在完成后重试检查。

示例

以下示例检查 IP 地址为 172.17.16.72 的客户端是否为 SVM vs1 上的网络组 mercury 的成员：

```
 cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
```

优化访问缓存性能

您可以配置多个参数来优化访问缓存，并在性能与存储在访问缓存中的信息的最新程度之间找到适当的平衡。

关于此任务

配置访问缓存刷新周期时，请记住以下几点：

- 值越高意味着条目在访问缓存中的保留时间越长。

  其优势在于性能更好，因为 ONTAP 在刷新访问缓存条目上花费的资源更少。缺点是，如果导出策略规则发生更改，而访问缓存条目因此变得陈旧，则更新这些条目需要的时间会较长。因此，应获取访问权限的客户端可能会被拒绝，而应被拒绝的客户端可能会获得访问权限。

- 值越低意味着 ONTAP 更新访问缓存条目的频率越高。

  其优势在于，条目更新，客户端更有可能被正确授予或拒绝访问。缺点是性能下降，因为 ONTAP 会花费更多资源来刷新访问缓存条目。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 执行所需的操作：

要修改的内容	输入 ...
肯定条目的刷新期限	`vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value`
否定条目的刷新期限	`vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value`
旧条目的超时期限	`vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value`

3. 验证新参数设置：

   ```
   vserver export-policy access-cache config show-all-vservers
   ```

4. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

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。

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Windows访问控制列表(ACL)安全设置、以防止用户或应用程序重命名关键目录。

了解更多信息 "如何防止在客户端访问目录时重命名这些目录"。

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
```

正在中断锁定

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
   ```

FPolicy 首次读取和首次写入筛选器如何与 NFS 配合使用

如果使用将读 / 写操作作为受监控事件的外部 FPolicy 服务器启用了 FPolicy ，则 NFS 客户端在读取 / 写入请求的高流量期间会遇到较长的响应时间。对于 NFS 客户端，在 FPolicy 中使用首次读取和首次写入筛选器可减少 FPolicy 通知的数量并提高性能。

在 NFS 中，客户端通过提取文件句柄对文件执行 I/O 。此句柄可能在服务器和客户端重新启动后仍然有效。因此，客户端可以在不重新检索句柄的情况下缓存句柄并在其上发送请求。在常规会话中，会向文件服务器发送大量读 / 写请求。如果为所有这些请求生成通知，可能会导致以下问题：

- 由于额外的通知处理和较长的响应时间，负载会增加。
- 向 FPolicy 服务器发送大量通知，即使该服务器不受所有通知的影响。

从客户端收到特定文件的第一个读 / 写请求后，将创建一个缓存条目，并增加读 / 写计数。此请求将标记为首次读取 / 写入操作，并生成 FPolicy 事件。在为 NFS 客户端规划和创建 FPolicy 筛选器之前，您应了解 FPolicy 筛选器工作原理的基础知识。

- 首次读取：筛选客户端读取请求以进行首次读取。

  如果对NFS事件使用此筛选器、则会显示 `-file-session-io-grouping-count` 和 `-file-session-io-grouping-duration` 设置用于确定要处理FPolicy的首次读取请求。

- 首次写入：筛选客户端写入请求以进行首次写入。

  如果对NFS事件使用此筛选器、则会显示 `-file-session-io-grouping-count` 和 `-file-session-io-grouping-duration` 设置用于确定要处理FPolicy的首次写入请求。

NFS 服务器数据库中添加了以下选项。

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

修改 NFSv4.1 服务器实施 ID

NFSv4.1 协议包含一个服务器实施 ID ，用于记录服务器域，名称和日期。您可以修改服务器实施 ID 的默认值。更改默认值可能会很有用，例如，在收集使用情况统计信息或对互操作性问题进行故障排除时。有关详细信息，请参见 RFC 5661 。

关于此任务

这三个选项的默认值如下：

选项	选项名称	默认值
NFSv4.1 实施 ID 域	`-v4.1-implementation-domain`	NetApp.com
NFSv4.1 实施 ID 名称	`-v4.1-implementation-name`	集群版本名称
NFSv4.1 实施 ID 日期	`-v4.1-implementation-date`	集群版本日期

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：

要修改 **NFSv4.1** 实施 **ID** 的项	输入命令 **...**
domain	`vserver nfs modify -v4.1 -implementation-domain domain`
Name	`vserver nfs modify -v4.1 -implementation-name name`
Date	`vserver nfs modify -v4.1 -implementation-date date`

3. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

管理 NFSv4 ACL

启用 NFSv4 ACL 的优势

启用 NFSv4 ACL 具有许多优势。

启用 NFSv4 ACL 的优势包括：

- 更精细地控制用户对文件和目录的访问
- 提高 NFS 安全性
- 改进了与 CIFS 的互操作性
- 取消了每个用户 16 个组的 NFS 限制

NFSv4 ACL 的工作原理

使用 NFSv4 ACL 的客户端可以对系统上的文件和目录设置和查看 ACL 。在具有 ACL 的目录中创建新文件或子目录时，新文件或子目录会继承 ACL 中已标记有相应继承标志的所有 ACL 条目（ACE ）。

在根据 NFSv4 请求创建文件或目录时，生成的文件或目录上的 ACL 取决于文件创建请求是包含 ACL 还是仅包含标准 UNIX 文件访问权限，以及父目录是否具有 ACL ：

- 如果请求包含 ACL ，则会使用该 ACL 。
- 如果此请求仅包含标准 UNIX 文件访问权限，但父目录具有 ACL ，则只要父目录的 ACL 中的 ACE 已使用适当的继承标志进行标记，新文件或目录就会继承这些 ACE 。

> 即使如此、也会继承父ACL `-v4.0-acl` 设置为 `off`。

- 如果此请求仅包含标准 UNIX 文件访问权限，并且父目录没有 ACL ，则会使用客户端文件模式设置标准 UNIX 文件访问权限。
- 如果此请求仅包含标准 UNIX 文件访问权限，并且父目录具有不可继承的 ACL ，则只会使用模式位创建新对象。

> 如果 `-chown-mode` 参数已设置为 `restricted` 中的命令 `vserver nfs` 或 `vserver export-policy rule` 系列、文件所有权只能由超级用户更改、即使使用NFSv4 ACL设置的磁盘权限允许非root用户更改文件所有权也是如此。有关详细信息，请参见相关手册页。

启用或禁用修改 **NFSv4 ACL**

当ONTAP接收到 `chmod` 命令时、默认情况下、系统会保留并修改ACL、以反映模式位更改。您可以禁用 `-v4-acl-preserve` 参数以更改要丢弃ACL时的行为。

关于此任务

使用统一安全模式时，此参数还指定客户端为文件或目录发送 chmod ， chgroup 或 chown 命令时是保留还是删除 NTFS 文件权限。

此参数的默认值为 enabled 。

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：

如果您要 …	输入以下命令 …
启用保留和修改现有 NFSv4 ACL （默认）	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
更改模式位时禁用保留并丢弃 NFSv4 ACL	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. 返回到管理权限级别：

```
set -privilege admin
```

ONTAP 如何使用 NFSv4 ACL 来确定是否可以删除文件

为了确定是否可以删除某个文件， ONTAP 将结合使用该文件的删除位和所在目录的 delete_child 位。有关详细信息，请参见 NFS 4.1 RFC 5661 。

启用或禁用 **NFSv4 ACL**

要启用或禁用NFSv4 ACL、您可以修改 `-v4.0-acl` 和 `-v4.1-acl` 选项默认情况下，这些选项处于禁用状态。

关于此任务

。 `-v4.0-acl` 或 `-v4.1-acl` 选项用于控制NFSv4 ACL的设置和查看、而不用于控制在访问检查中强制实施这些ACL。

步骤

1. 执行以下操作之一：

如果您要 …	那么 …
启用 NFSv4.0 ACL	输入以下命令： `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
禁用 NFSv4.0 ACL	输入以下命令： `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
启用NFSv4.1 ACL	输入以下命令： `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`

禁用NFSv4.1 ACL	输入以下命令： `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

修改 NFSv4 ACL 的最大 ACE 限制

您可以通过修改参数来修改每个NFSv4 ACL允许的最大ACL数 `-v4-acl-max-aces`。默认情况下，每个 ACL 的限制设置为 400 个 ACE 。增加此限制有助于确保使用包含 400 个以上 ACE 的 ACL 将数据成功迁移到运行 ONTAP 的存储系统。

关于此任务

增加此限制可能会影响使用 NFSv4 ACL 访问文件的客户端的性能。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 修改 NFSv4 ACL 的最大 ACE 限制：

   ```
   vserver nfs modify -v4-acl-max-aces max_ace_limit
   ```

   的有效范围

   `max_ace_limit` 为 `192` to `1024`.

3. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

管理 NFSv4 文件委派

启用或禁用 NFSv4 读取文件委派

要启用或禁用NFSv4读取文件委派、您可以修改 `-v4.0-read-delegation`或 选项通过启用读取文件委派，您可以消除与打开和关闭文件相关的大量消息开销。

关于此任务

默认情况下，读取文件委派处于禁用状态。

启用读取文件委派的缺点是，服务器及其客户端必须在服务器重新启动，客户端重新启动或发生网络分区后恢复委派。

步骤

1. 执行以下操作之一：

如果您要 …	那么 …
启用 NFSv4 读取文件委派	输入以下命令： `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled`
启用NFSv4.1读取文件委派	输入以下命令： + `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled`
禁用 NFSv4 读取文件委派	输入以下命令： `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled`
禁用NFSv4.1读取文件委派	输入以下命令： `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled`

结果

文件委派选项一经更改即会生效。无需重新启动或重新启动 NFS 。

启用或禁用 **NFSv4** 写入文件委派

要启用或禁用写入文件委派、您可以修改 `-v4.0-write-delegation`或 选项通过启用写入文件委派，除了打开和关闭文件之外，您还可以消除与文件和记录锁定相关的大量消息开销。

关于此任务

默认情况下，写入文件委派处于禁用状态。

启用写入文件委派的缺点是，在服务器重新启动，客户端重新启动或发生网络分区后，服务器及其客户端必须执行其他任务来恢复委派。

步骤

1. 执行以下操作之一：

如果您要 …	那么 …
启用 NFSv4 写入文件委派	输入以下命令： `vserver nfs modify -vserver vserver_name -v4.0-write -delegation enabled`

如果您要 ...	那么 ...
启用NFSv4.1写入文件委派	输入以下命令： `vserver nfs modify -vserver vserver_name -v4.1-write -delegation enabled`
禁用 NFSv4 写入文件委派	输入以下命令： `vserver nfs modify -vserver vserver_name -v4.0-write -delegation disabled`
禁用NFSv4.1写入文件委派	输入以下命令： `vserver nfs modify -vserver vserver_name -v4.1-write -delegation disabled`

结果

文件委派选项一经更改即会生效。无需重新启动或重新启动 NFS 。

配置 **NFSv4** 文件和记录锁定

关于 **NFSv4** 文件和记录锁定

对于 NFSv4 客户端， ONTAP 支持 NFSv4 文件锁定机制，以便在基于租赁的模式下保持所有文件锁定的状态。

"NetApp 技术报告 3580 ：《 NFSv4 增强功能和最佳实践指南： Data ONTAP 实施》"

指定 **NFSv4** 锁定租赁期限

要指定NFSv4锁定租赁期限(即ONTAP不可撤销地向客户端授予锁定的时间段)、您可以修改 `-v4-lease-seconds` 选项较短的租赁期可加快服务器恢复速度，而较长的租赁期则有利于处理大量客户端的服务器。

关于此任务

默认情况下、此选项设置为 `30`。此选项的最小值为 `10`。此选项的最大值是锁定宽限期、您可以使用设置此宽限期 `locking.lease_seconds` 选项

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 输入以下命令：

   ```
   vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
   ```

3. 返回到管理权限级别：

```
set -privilege admin
```

指定 **NFSv4** 锁定宽限期

要指定NFSv4锁定宽限期(即、客户端在服务器恢复期间尝试从ONTAP回收其锁定状态的时间段)、您可以修改 `-v4-grace-seconds` 选项

关于此任务

默认情况下、此选项设置为 `45`。

步骤

1. 将权限级别设置为高级：

```
set -privilege advanced
```

2. 输入以下命令：

```
vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
```

3. 返回到管理权限级别：

```
set -privilege admin
```

NFSv4 转介的工作原理

启用 NFSv4 转介时， ONTAP 会为 NFSv4 客户端提供 "`SVM 内` " 转介。SVM 内转介是指收到 NFSv4 请求的集群节点将 NFSv4 客户端转介到 Storage Virtual Machine （ SVM ）上的另一个逻辑接口（ LIF ）。

从那时起， NFSv4 客户端应访问在目标 LIF 上收到转介的路径。如果原始集群节点确定 SVM 中存在驻留在数据卷所在集群节点上的 LIF ，则会提供此类转介，从而使客户端能够更快地访问数据并避免额外的集群通信。

启用或禁用 **NFSv4** 转介

您可以通过启用选项在Storage Virtual Machine (SVM)上启用NFSv4转介 `-v4-fsid-change` 和 `-v4.0-referrals`或。启用 NFSv4 转介可以加快支持此功能的 NFSv4 客户端的数据访问速度。

您需要的内容

如果要启用 NFS 转介，必须先禁用并行 NFS 。您不能同时启用这两者。

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：

如果您要 ...	输入命令 ...
启用 NFSv4 转介	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled`
禁用 NFSv4 转介	`vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled`
启用NFSv4.1转介	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled`
禁用NFSv4.1转介	`vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled`

3. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

显示NFS统计信息

您可以显示存储系统上 Storage Virtual Machine （ SVM ）的 NFS 统计信息，以监控性能并诊断问题。

步骤

1. 使用 `statistics catalog object show` 命令以确定可从中查看数据的NFS对象。

   ```
   statistics catalog object show -object nfs*
   ```

2. 使用 `statistics start` 和可选 `statistics stop` 用于从一个或多个对象收集数据样本的命令。
3. 使用 `statistics show` 命令以查看示例数据。

示例：监控**NFSv3**性能

以下示例显示了 NFSv3 协议的性能数据。

以下命令将开始收集新样本的数据：

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

以下命令通过指定计数器来显示样本中的数据，这些计数器显示成功的读取和写入请求数与读取和写入请求总数：

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                             Value
    --------------------------- ---------------------------
    read_success                                        40042
    read_total                                          40042
    write_success                                     1492052
    write_total                                       1492052
```

相关信息

"性能监控设置"

显示DNS统计信息

您可以显示存储系统上Storage Virtual Machine (SVM)的DNS统计信息、以监控性能和诊断问题。

步骤

1. 使用 `statistics catalog object show` 命令以确定可从中查看数据的DNS对象。

   ```
   statistics catalog object show -object external_service_op*
   ```

2. 使用 `statistics start` 和 `statistics stop` 用于从一个或多个对象收集数据样本的命令。
3. 使用 `statistics show` 命令以查看示例数据。

监控**DNS**统计信息

以下示例显示了 DNS 查询的性能数据。以下命令将开始收集新样本的数据：

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

以下命令通过指定计数器来显示样本中的数据，这些计数器显示发送的 DNS 查询数与接收，失败或超时的 DNS 查询数：

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            0
    num_requests_sent                                               1
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

以下命令通过指定计数器来显示样本中的数据，这些计数器显示特定服务器上的 DNS 查询收到特定错误的次数：

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                             NXDOMAIN
    server_ip_address                                  10.72.219.109
3 entries were displayed.
```

相关信息

"性能监控设置"

显示NIS统计信息

您可以显示存储系统上Storage Virtual Machine (SVM)的NIS统计信息、以监控性能和诊断问题。

步骤

1. 使用 `statistics catalog object show` 命令以确定可从中查看数据的NIS对象。

   ```
   statistics catalog object show -object external_service_op*
   ```

2. 使用 `statistics start` 和 `statistics stop` 用于从一个或多个对象收集数据样本的命令。
3. 使用 `statistics show` 命令以查看示例数据。

监控 **NIS** 统计信息

以下示例显示了 NIS 查询的性能数据。以下命令将开始收集新样本的数据：

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

以下命令通过指定计数器来显示样本中的数据，这些计数器显示发送的 NIS 查询数与接收，失败或超时的 NIS 查询数：

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                         0
    num_request_failures                                            1
    num_requests_sent                                               2
    num_responses_received                                          1
    num_successful_responses                                        1
    num_timeouts                                                    0
6 entries were displayed.
```

以下命令通过指定计数器来显示样本中的数据，这些计数器显示在特定服务器上收到 NIS 查询特定错误的次数：

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                          YP_NOTFOUND
    server_ip_address                                   10.227.13.221
3 entries were displayed.
```

相关信息

"性能监控设置"

支持基于 **NFS** 的 **VMware vStorage**

ONTAP 支持 NFS 环境中的某些 VMware vStorage APIs for Array Integration （VAAI）功能。

支持的功能

支持以下功能：

- 副本卸载

  使 ESXi 主机可以直接在源数据存储位置和目标数据存储位置之间复制虚拟机或虚拟机磁盘（VMDK），而无需主机参与。这样可以节省 ESXi 主机的 CPU 周期和网络带宽。如果源卷为稀疏卷，则副本卸载可保留空间效率。

- 空间预留

  通过为 VMDK 文件预留空间来保证其存储空间。

限制

基于 NFS 的 VMware vStorage 具有以下限制：

- 在以下情况下，副本卸载操作可能会失败：
  - 在源卷或目标卷上运行 wafliron 时，因为它会暂时使卷脱机
  - 移动源卷或目标卷时
  - 移动源或目标 LIF 时
  - 执行接管或交还操作时
  - 执行切换或切回操作时
- 在以下情况下，由于文件句柄格式不同，服务器端复制可能会失败：

  您尝试将当前或先前已导出 qtree 的 SVM 中的数据复制到从未导出 qtree 的 SVM 。要解决此限制，您可以在目标 SVM 上至少导出一个 qtree 。

相关信息

"Data ONTAP 支持哪些 VAAI 卸载操作？"

启用或禁用基于 **NFS** 的 **VMware vStorage**

您可以使用在Storage Virtual Machine (SVM)上启用或禁用对基于NFS的VMware vStorage的支持 `vserver nfs modify` 命令：

关于此任务

默认情况下，不支持基于 NFS 的 VMware vStorage 。

步骤

1. 显示 SVM 的当前 vStorage 支持状态：

```
vserver nfs show -vserver vserver_name -instance
```

2. 执行以下操作之一：

如果您要 ...	输入以下命令 ...
启用 VMware vStorage 支持	`vserver nfs modify -vserver vserver_name -vstorage enabled`
禁用 VMware vStorage 支持	`vserver nfs modify -vserver vserver_name -vstorage disabled`

完成后

您必须先安装适用于 VMware VAAI 的 NFS 插件，然后才能使用此功能。有关详细信息，请参见 *Installing the NetApp NFS Plug-in for VMware VAAI* 。

相关信息

"NetApp 文档：适用于 VMware VAAI 的 NetApp NFS 插件"

启用或禁用 rquota 支持

ONTAP 支持远程配额协议版本 1 （ rquota v1 ）。使用 rquota 协议， NFS 客户端可以从远程计算机为用户获取配额信息。您可以使用在Storage Virtual Machine (SVM)上启用r配额 `vserver nfs modify` 命令：

关于此任务

默认情况下， rquota 处于禁用状态。

步骤

1. 执行以下操作之一：

如果您要 ...	输入以下命令 ...
为 SVM 启用 rquota 支持	`vserver nfs modify -vserver vserver_name -rquota enable`
禁用 SVM 的 rquota 支持	`vserver nfs modify -vserver vserver_name -rquota disable`

有关配额的详细信息，请参见 "逻辑存储管理"。

通过修改 TCP 传输大小来提高 NFSv3 和 NFSv4 的性能

您可以通过修改 TCP 最大传输大小来提高通过高延迟网络连接到存储系统的 NFSv3 和

NFSv4 客户端的性能。

当客户端通过广域网（ WAN ）或城域网（ man ）等高延迟网络访问存储系统时，如果延迟超过 10 毫秒，则可以通过修改 TCP 最大传输大小来提高连接性能。在低延迟网络（例如局域网（ LAN ））中访问存储系统的客户端，对这些参数的修改几乎没有好处。如果吞吐量提高不会超过延迟影响，则不应使用这些参数。

要确定您的存储环境是否会因修改这些参数而受益，您应首先对性能较差的 NFS 客户端进行全面的性能评估。查看此低性能是否是由于往返延迟过长以及客户端上的请求较小所致。在这种情况下，客户端和服务器无法充分利用可用带宽，因为它们会花费大部分工作周期来等待通过连接传输的小请求和响应。

通过增加 NFSv3 和 NFSv4 请求大小，客户端和服务器可以更有效地使用可用带宽，以便在每个单元时间移动更多数据，从而提高连接的整体效率。

请注意，存储系统和客户端之间的配置可能会有所不同。存储系统和客户端支持传输操作的最大大小为 1 MB 。但是，如果将存储系统配置为支持 1 MB 最大传输大小，但客户端仅支持 64 KB ，则挂载传输大小将限制为 64 KB 或更少。

在修改这些参数之前，您必须了解，在组装和传输大型响应所需的时间段内，它会导致存储系统占用更多内存。存储系统的高延迟连接越多，额外的内存消耗就越多。具有高内存容量的存储系统可能不会受到此更改的影响。内存容量较低的存储系统的性能可能会明显下降。

要成功使用这些参数，需要能够从集群的多个节点检索数据。集群网络固有的延迟可能会增加响应的整体延迟。使用这些参数时，整体延迟往往会增加。因此，延迟敏感型工作负载可能会产生负面影响。

修改 **NFSv3** 和 **NFSv4 TCP** 最大传输大小

您可以修改 `-tcp-max-xfer-size` 可选择为使用NFSv3和NFSv4.x协议的所有TCP连接配置最大传输大小。

关于此任务

您可以分别为每个 Storage Virtual Machine （ SVM ）修改这些选项。

从ONTAP 9开始、 `v3-tcp-max-read-size` 和 `v3-tcp-max-write-size` 选项已过时。您必须使用 `-tcp-max-xfer-size` 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：

如果您要 ...	输入命令 ...
修改 NFSv3 或 NFSv4 TCP 最大传输大小	`vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size`

选项	范围	**Default**
`-tcp-max-xfer-size`	8192 到 1048576 字节	6556字节

> 输入的最大传输大小必须是 4 KB （4096 字节）的倍数。未正确对齐的请求会对性能产生负面影响。

3. 使用 `vserver nfs show -fields tcp-max-xfer-size` 命令以验证所做的更改。
4. 如果任何客户端使用静态挂载，请卸载并重新挂载，以使新参数大小生效。

示例

以下命令会将名为 vs1 的 SVM 上的 NFSv3 和 NFSv4.x TCP 最大传输大小设置为 1048576 字节：

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

配置 **NFS** 用户允许的组 **ID** 数量

默认情况下，在使用 Kerberos （RPCSEC_GSS）身份验证处理 NFS 用户凭据时，ONTAP 最多支持 32 个组 ID 。使用 AUTH_SYS 身份验证时，默认的最大组 ID 数为 16 ，如 RFC 5531 中所定义。如果用户所属的组超过默认组数，则可以将最大值增加到 1 ，024 。

关于此任务

如果用户凭据中的组 ID 超过默认数量，则其余组 ID 将被截断，并且用户在尝试从存储系统访问文件时可能会收到错误。您应将每个 SVM 的最大组数设置为表示环境中最大组数的数字。

下表显示了的两个参数 `vserver nfs modify` 用于确定三个示例配置中组ID最大数量的命令：

Parameters	设置	生成的组 ID 限制

`-extended-groups-limit`
`-auth-sys-extended-groups`
	`32`
	`disabled`
	这些是默认设置。
		RPCSEC_GSS： 32
		AUTH_SYS： 16

`-extended-groups-limit` `-auth-sys-extended-groups`	`256` `disabled`	RPCSEC_GSS：256 AUTH_SYS： 16
`-extended-groups-limit` `-auth-sys-extended-groups`	`512` `enabled`	RPCSEC_GSS：512 auth_SYS：512

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 执行所需的操作：

如果要设置允许的最大辅助组数 ...	输入命令 ...
仅适用于 RPCSEC_GSS ，并保持 AUTH_SYS 设置为默认值 16	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled`
适用于 RPCSEC_GSS 和 AUTH_SYS	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled`

3. 验证 `-extended-groups-limit` 值并验证AUTH _SYS是否正在使用扩展组： `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`
4. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

示例

以下示例将为 AUTH_SYS 身份验证启用扩展组，并将 AUTH_SYS 和 RPCSEC_GSS 身份验证的最大扩展组数设置为 512 。这些更改仅适用于访问名为 vs1 的 SVM 的客户端：

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
------- ------------------------ ---------------------
vs1     enabled                  512

vs1::*> set -privilege admin
```

控制 root 用户对 NTFS 安全模式数据的访问

您可以将 ONTAP 配置为允许 NFS 客户端访问 NTFS 安全模式数据，并允许 NTFS 客户端访问 NFS 安全模式数据。在 NFS 数据存储上使用 NTFS 安全模式时，您必须确定如何处理 root 用户的访问并相应地配置 Storage Virtual Machine （ SVM ）。

关于此任务

当 root 用户访问 NTFS 安全模式数据时，您有两种选择：

- 像任何其他 NFS 用户一样将 root 用户映射到 Windows 用户，并根据 NTFS ACL 管理访问。
- 忽略 NTFS ACL 并提供对 root 的完全访问权限。

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 执行所需的操作：

如果希望 root 用户 …	输入命令 …
映射到 Windows 用户	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled`
绕过 NT ACL 检查	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled`

   默认情况下，此参数处于禁用状态。

   如果启用了此参数，但 root 用户没有名称映射，则 ONTAP 将使用默认的 SMB 管理员凭据进行审核。

3. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

支持的NFS版本和客户端

支持的NFS版本和客户端概述

在网络中使用 NFS 之前，您需要了解 ONTAP 支持哪些 NFS 版本和客户端。

下表说明了ONTAP 默认支持主要和次要NFS协议版本的时间。默认情况下、支持并不表示这是支持该NFS协议的ONTAP 的最早版本。

version	默认情况下处于启用状态
NFSv3	是的。

version	默认情况下处于启用状态
NFSv4.0	是，从 ONTAP 9.9.1 开始
NFSv4.1	是，从 ONTAP 9.9.1 开始
NFSv4.2	是，从 ONTAP 9.9.1 开始
pNFS	否

有关 ONTAP 支持的 NFS 客户端的最新信息，请参见互操作性表。

"NetApp 互操作性表工具"

ONTAP 支持的 NFSv4.0 功能

除了 SPKM3 和 LIPKEY 安全机制之外， ONTAP 还支持 NFSv4.0 中的所有必需功能。

支持以下 NFSv4 功能：

- * 复合 *

  允许客户端在一个远程操作步骤调用（ RPC ）请求中请求多个文件操作。

- * 文件委派 *

  允许服务器将文件控制委派给某些类型的客户端以进行读写访问。

- * 伪 FS*

  NFSv4 服务器用于确定存储系统上的挂载点。NFSv4 中没有挂载协议。

- * 锁定 *

  基于租赁。NFSv4 中没有单独的网络锁定管理器（ Network Lock Manager ， NLM ）或网络状态监控器（ Network Status Monitor ， NSM ）协议。

有关 NFSv4.0 协议的详细信息，请参见 RFC 3530 。

NFSv4 的 ONTAP 支持限制

您应了解 ONTAP 对 NFSv4 的支持存在一些限制。

- 并非每种客户端类型都支持委派功能。
- 在 ONTAP 9.4 及更早版本中，存储系统会拒绝 UTF8 卷以外的卷上具有非 ASCII 字符的名称。

  在 ONTAP 9.5 及更高版本中，使用 utf8mb4 语言设置创建并使用 NFS v4 挂载的卷不再受此限制。

- 所有文件句柄都是永久性的；服务器不提供易失性文件句柄。
- 不支持迁移和复制。
- 只读负载共享镜像不支持 NFSv4 客户端。

  ONTAP 会将 NFSv4 客户端路由到负载共享镜像的源，以实现直接读写访问。

- 不支持命名属性。
- 支持所有建议属性，但以下属性除外：
  - `archive`
  - `hidden`
  - `homogeneous`
  - `mimetype`
  - `quota_avail_hard`
  - `quota_avail_soft`
  - `quota_used`
  - `system`
  - `time_backup`

  ⓘ 但不支持 `quota*` 属性时、ONTAP通过RQUOTA侧带协议支持用户配额和组配额。

ONTAP 支持 NFSv4.1

从 ONTAP 9.8 开始，如果启用了 NFSv4.1 ，则默认情况下可以使用 nconnect 功能。

早期的 NFS 客户端实施仅使用挂载的单个 TCP 连接。在 ONTAP 中，单个 TCP 连接可能会随着 IOPS 的增加而成为瓶颈。但是，启用了 nconnect 的客户端可以具有多个与单个 NFS 挂载关联的 TCP 连接（最多 16 个）。此类 NFS 客户端会以轮循的方式将文件操作多路由到多个 TCP 连接上，从而从可用网络带宽中获得更高的吞吐量。建议仅对 NFSv3 和 NFSv4.1 挂载使用 nConnect 。

请参见 NFS 客户端文档以确认您的客户端版本是否支持 nconnect 。

默认情况下， ONTAP 9.9.1 及更高版本会启用 NFSv4.1 。在早期版本中、您可以通过指定来启用它 `-v4.1` 选项并将其设置为 `enabled` 在Storage Virtual Machine (SVM)上创建NFS服务器时。

ONTAP 不支持 NFSv4.1 目录和文件级委派。

ONTAP支持NFSv4.2

从ONTAP 9.8开始、ONTAP支持NFSv4.2协议、以允许已启用NFSv4.2的客户端访问。

在ONTAP 9.9.1及更高版本中、默认情况下会启用NFSv4.2。在ONTAP 9.8中、需要通过指定手动启用v4.2 `-v4.1` 选项并将其设置为 `enabled` 在Storage Virtual Machine (SVM)上创建NFS服务器时。启用 NFSv4.1 还可以使客户端在挂载为 v4.2 时使用 NFSv4.1 功能。

连续几个ONTAP版本都扩展了对NFSv4.2可选功能的支持。

开头为 ...	**NFSv4.2**的可选功能包括...
ONTAP 9.12.1	• NFS扩展属性 • 稀疏文件 • 空间预留
ONTAP 9.9.1	标记为NFS的强制访问控制(MAC)

NFS v4.2安全标签

从 ONTAP 9.1.1 开始，可以启用 NFS 安全标签。默认情况下，它们处于禁用状态。

对于 NFS v4.2 安全标签， ONTAP NFS 服务器可识别强制访问控制（ MAC ），存储和检索客户端发送的 sec_label 属性。

有关详细信息，请参见 "RFC 7240"。

从ONTAP 9.12.1开始、NDMP转储操作支持NFS v4.2安全标签。如果在早期版本中的文件或目录上遇到安全标签、则转储将失败。

步骤

1. 将权限设置更改为高级：

```
set -privilege advanced
```

2. 启用安全标签：

```
vserver nfs modify -vserver _svm_name_ -v4.2-seclabel enabled
```

NFS扩展属性

从ONTAP 9.12.1开始、默认情况下会启用NFS扩展属性(xattrs)。

扩展属性是定义的标准NFS属性 "RFC 8276" 并在现代NFS客户端中启用。它们可用于将用户定义的元数据附加到文件系统对象、并且对高级安全部署很有兴趣。

NDMP转储操作当前不支持NFS扩展属性。如果文件或目录遇到扩展属性、转储将继续进行、但不会备份这些文件或目录上的扩展属性。

如果需要禁用扩展属性、请使用 `vserver nfs modify -v4.2-xattrs disabled` 命令：

支持并行 **NFS** 的 **ONTAP**

ONTAP 支持并行 NFS （ pNFS ）。pNFS 协议可使客户端直接访问分布在集群多个节点

上的一组文件的数据，从而提高了性能。它可以帮助客户端找到卷的最佳路径。

使用硬挂载

在排除挂载问题时，您需要确保使用的挂载类型正确。NFS 支持两种挂载类型：软挂载和硬挂载。出于可靠性考虑，您应仅使用硬挂载。

您不应使用软挂载，尤其是在可能频繁出现 NFS 超时的情况下。这些超时可能会导致出现争用情况，进而导致数据损坏。

NFS 和 SMB 文件和目录命名依赖关系

NFS和SMB文件及目录命名依赖关系概述

除了 ONTAP 集群和客户端上的语言设置之外，文件和目录命名约定还取决于网络客户端的` 操作系统和文件共享协议。

操作系统和文件共享协议确定以下内容：

- 文件名可以使用的字符
- 文件名区分大小写

ONTAP 支持文件，目录和 qtree 名称中的多字节字符，具体取决于 ONTAP 版本。

文件或目录名称可以使用的字符

如果要从具有不同操作系统的客户端访问文件或目录，则应使用在两个操作系统中均有效的字符。

例如，如果使用 UNIX 创建文件或目录，请勿在名称中使用冒号（：），因为 MS-DOS 文件或目录名称中不允许使用冒号。由于对有效字符的限制因操作系统而异，请参见客户端操作系统的文档，了解有关禁止字符的详细信息。

在多协议环境中，文件和目录名称区分大小写

对于NFS客户端、文件和目录名称区分大小写；对于SMB客户端、文件和目录名称不区分大小写、但保留大小写。您必须了解多协议环境的含义，以及在创建 SMB 共享时指定路径以及访问共享中的数据时可能需要执行的操作。

SMB客户端创建名为的目录时 `testdir`，SMB和NFS客户端都会将文件名显示为 `testdir`。但是、如果SMB用户稍后尝试创建目录名称 `TESTDIR`，则不允许使用该名称，因为SMB客户端当前已存在该名称。如果NFS用户稍后创建一个名为的目录 `TESTDIR`、NFS和SMB客户端显示目录名称的方式不同，如下所示：

- 例如、在NFS客户端上、您可以在创建这两个目录时看到这两个目录名称 `testdir` 和 `TESTDIR`，因为目录名区分大小写。
- SMB 客户端使用 8.3 名称来区分这两个目录。一个目录具有基本文件名。为其他目录分配 8.3 文件名。
  - 在SMB客户端上、您会看到 `testdir` 和 `TESTDI~1`。

- ONTAP将创建 `TESTDI~1` 用于区分这两个目录的目录名称。

  在这种情况下，在 Storage Virtual Machine （ SVM ）上创建或修改共享时，指定共享路径时必须使用 8.3 名称。

同样、对于文件、如果SMB客户端创建 `test.txt`，SMB和NFS客户端都会将文件名显示为 `text.txt`。但是、如果SMB用户稍后尝试创建 `Test.txt`，则不允许使用该名称，因为SMB客户端当前已存在该名称。如果NFS用户稍后创建一个名为的文件 `Test.txt`、NFS和SMB客户端显示文件名的方式不同，如下所示：

- 在NFS客户端上、您会在创建时看到这两个文件名、 `test.txt` 和 `Test.txt`，因为文件名区分大小写。
- SMB 客户端使用 8.3 名称来区分这两个文件。一个文件具有基本文件名。为其他文件分配 8.3 文件名。
  - 在SMB客户端上、您会看到 `test.txt` 和 `TEST~1.TXT`。
  - ONTAP将创建 `TEST~1.TXT` 用于区分这两个文件的文件名。

> 如果已使用vserver cifs character-Mapping命令创建字符映射、则通常不区分大小写的Windows查找可能区分大小写。这意味着、只有在创建了字符映射且文件名正在使用该字符映射的情况下、文件名查找才区分大小写。

ONTAP 如何创建文件和目录名称

ONTAP 会为可从 SMB 客户端访问的任何目录中的文件或目录创建并维护两个名称：原始长名称和 8.3 格式的名称。

对于超过八个字符名称或三个字符扩展名限制的文件或目录名称（对于文件）， ONTAP 将生成 8.3 格式的名称，如下所示：

- 如果原始文件或目录名称超过 6 个字符，则会将其截断为 6 个字符。
- 它会在截断后不再唯一的文件或目录名称后面附加一个颚化符（~ ）和一个数字（ 1 到 5 ）。

  如果由于名称相似而导致数字用尽，则会创建一个与原始名称无关的唯一名称。

- 对于文件，它会将文件扩展名截断为三个字符。

例如、如果NFS客户端创建一个名为的文件 `specifications.html`，则ONTAP创建的8.3格式文件名为 `specif~1.htm`。如果此名称已存在，则 ONTAP 会在文件名末尾使用其他数字。例如、如果NFS客户端创建另一个名为的文件 `specifications_new.html``的8.3格式 `specifications_new.html` 为 `specif~2.htm`。

ONTAP 如何处理多字节文件，目录和 qtree 名称

从 ONTAP 9.5 开始，通过支持 4 字节 UTF-8 编码名称，可以在基本多语言平面（ BMP ）之外创建和显示包含 Unicode 补充字符的文件，目录和树名。在早期版本中，这些补充字符无法在多协议环境中正确显示。

为了支持4字节UTF-8编码名称、为提供了一个新的_utf8mb4_语言代码 `vserver` 和 `volume` 命令系列。

- 您必须通过以下方式之一创建新卷：

- 设置音量 `-language` 显式选项：

  ```
  volume create -language utf8mb4 {…}
  ```

- 继承卷 `-language` 使用选项创建或修改的SVM中的选项：

  ```
  vserver [create|modify] -language utf8mb4 {…}``volume create {…}
  ```

- 如果您使用的是ONTAP 9.6及更早版本、则无法修改现有卷以支持utf8mb4；您必须创建一个新的utf8mb4就绪卷、然后使用基于客户端的复制工具迁移数据。

  如果您使用的是ONTAP 9.7P1或更高版本、则可以根据支持请求修改utf8mb4的现有卷。有关详细信息，请参见 "在ONTAP中创建卷后是否可以更改卷语言？"。

  您可以更新 SVM 以获得 utf8mb4 支持，但现有卷会保留其原始语言代码。

> 当前不支持包含 4 字节 UTF-8 字符的 LUN 名称。

- Unicode 字符数据通常在使用 16 位 Unicode 转换格式（ UTF-16 ）的 Windows 文件系统应用程序和使用 8 位 Unicode 转换格式（ UTF-8 ）的 NFS 文件系统中表示。

  在 ONTAP 9.5 之前的版本中，由 Windows 客户端创建的名称（包括 UTF-16 补充字符）会正确显示给其他 Windows 客户端，但对于 NFS 客户端，这些名称未正确转换为 UTF-8 。同样，对于 Windows 客户端，已创建的 NFS 客户端使用 UTF-8 补充字符的名称也未正确转换为 UTF-16 。

- 在运行 ONTAP 9.4 或更早版本的系统上创建包含有效或无效补充字符的文件名时， ONTAP 将拒绝该文件名并返回无效文件名错误。

  要避免此问题描述，请在文件名中仅使用 BMP 字符并避免使用补充字符，或者升级到 ONTAP 9.5 或更高版本。

qtree 名称中允许使用 Unicode 字符。

- 您可以使用 `volume qtree` 用于设置或修改qtree名称的命令系列或System Manager。
- qtree 名称可以包含 Unicode 格式的多字节字符，例如日语和中文字符。
- 在 ONTAP 9.5 之前的版本中，仅支持 BMP 字符（即，可以用 3 个字节表示的字符）。

> 在 ONTAP 9.5 之前的版本中， qtree 父卷的接合路径可以包含带有 Unicode 字符的 qtree 和目录名称。。 `volume show` 命令可在父卷具有UTF-8语言设置时正确显示这些名称。但是，如果父卷语言不是 UTF-8 语言设置之一，则会使用数字 NFS 备用名称显示接合路径的某些部分。

- 在 9.5 及更高版本中，如果 qtree 位于启用了 utf8mb4 的卷中，则 qtree 名称中支持 4 字节字符。

在卷上配置用于 **SMB** 文件名转换的字符映射

NFS 客户端可以创建包含对 SMB 客户端和某些 Windows 应用程序无效的字符的文件名。您可以为卷上的文件名转换配置字符映射，以使 SMB 客户端能够访问具有 NFS 名称的文件，否则这些名称将无效。

关于此任务

当 SMB 客户端访问 NFS 客户端创建的文件时， ONTAP 将查看该文件的名称。如果此名称不是有效的 SMB 文件名（例如，如果其包含嵌入的冒号 "`：`" 字符），则 ONTAP 将返回为每个文件维护的 8.3 文件名。但是，如果应用程序将重要信息编码为较长的文件名，则会出现此问题。

因此，如果要在不同操作系统上的客户端之间共享文件，则应在文件名中使用在这两个操作系统中均有效的字符。

但是，如果 NFS 客户端创建的文件名包含的字符对于 SMB 客户端无效，则可以定义一个映射，将无效的 NFS 字符转换为 SMB 和某些 Windows 应用程序均可接受的 Unicode 字符。例如，此功能支持 CATIA MCAD 和 Mathematica 应用程序以及具有此要求的其他应用程序。

您可以逐个卷配置字符映射。

在卷上配置字符映射时，必须牢记以下几点：

- 字符映射不会跨接合点应用。

  您必须为每个接合卷显式配置字符映射。

- 您必须确保用于表示无效或非法字符的 Unicode 字符通常不会显示在文件名中；否则，将发生不需要的映射。

  例如，如果您尝试将冒号（：）映射到连字符（ - ），但在文件名中正确使用了连字符（ - ），则尝试访问名为 "`a-b`" 的文件的 Windows 客户端会将其请求映射到 NFS 名称 "`a： b`" （不是所需结果）。

- 应用字符映射后，如果映射仍包含无效的 Windows 字符，则 ONTAP 会回退到 Windows 8.3 文件名。
- 在 FPolicy 通知， NAS 审核日志和安全跟踪消息中，将显示映射的文件名。
- 创建类型为 DP 的 SnapMirror 关系时，源卷的字符映射不会复制到目标 DP 卷上。
- 区分大小写：由于映射的 Windows 名称转换为 NFS 名称，因此，名称的查找遵循 NFS 语义。这包括 NFS 查找区分大小写。这意味着，访问映射共享的应用程序不能依赖 Windows 不区分大小写的行为。但是， 8.3 名称是可用的，不区分大小写。
- 部分映射或无效映射：映射要返回到执行目录枚举（ "dir" ）的客户端的名称后，系统将检查生成的 Unicode 名称是否有效。如果此名称中仍包含无效字符，或者对于 Windows 无效（例如，此名称以 "." 或空白结尾），则会返回 8.3 名称，而不是无效名称。

步骤

1. 配置字符映射：

   ```
   vserver cifs character-mapping create -vserver vserver_name -volume
   volume_name -mapping mapping_text, ...
   ```

   此映射由一个源 - 目标字符对列表组成，并以 "`：`" 分隔。这些字符是使用十六进制数字输入的 Unicode 字符。例如： 3c： E03C 。

   每个的第一个值 `mapping_text` 以冒号分隔的对是要转换的NFS字符的十六进制值、第二个值是SMB使用的Unicode值。映射对必须是唯一的（应存在一对一映射）。

   - 源映射

     下表显示了源映射允许的 Unicode 字符集：

Unicode 字符	打印字符	Description
0x01-0x19	不适用	非打印控制字符
0x5C	\	反斜杠
0x3a	:	冒号
0x2A	*	星号
0x3F	?	问号
0x22	"	引号
0x3C	<	小于
0x3e	>	大于
0x7C	我们可以为您提供	竖线
0xB1	±	加减号

- 目标映射

  您可以在 Unicode 的 "`私有使用区域` " 中指定以下范围内的目标字符： U+E0000…U+F8FF 。

示例

以下命令会为 Storage Virtual Machine （ SVM ） vs1 上名为 `data` 的卷创建字符映射：

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

用于管理用于 SMB 文件名转换的字符映射的命令

您可以通过创建，修改，显示有关 FlexVol 卷上用于 SMB 文件名转换的文件字符映射的信息或删除此类映射来管理字符映射。

如果您要 …	使用此命令 …

创建新的文件字符映射	`vserver cifs character-mapping create`
显示有关文件字符映射的信息	`vserver cifs character-mapping show`
修改现有文件字符映射	`vserver cifs character-mapping modify`
删除文件字符映射	`vserver cifs character-mapping delete`

有关详细信息，请参见每个命令的手册页。