使用NFS管理文件访问

ONTAP 9

NetApp
April 24, 2024

目录

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

如果 ...	检查
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`

如果您要 ...	使用此命令 ...
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`
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`

要刷新的内容	输入命令 ...
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`

要修改 **NFSv4.1** 实施 **ID** 的项	输入命令 **...**
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`
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
```