使用命令行界面配置 NFS

ONTAP 9

NetApp
April 24, 2024

目录

使用命令行界面配置 NFS

使用命令行界面概述 NFS 配置

您可以使用 ONTAP 9 命令行界面命令配置 NFS 客户端对新的或现有的 Storage Virtual Machine （ SVM ）中新卷或 qtree 中所含文件的访问权限。

如果要按以下方式配置对卷或 qtree 的访问，请使用以下过程：

- 您希望使用 ONTAP 当前支持的任何 NFS 版本： NFSv3 ， NFSv4 ， NFSv4.1 ， NFSv4.2 或 NFSv4.1 与 pNFS 。
- 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。

  要使用 System Manager 配置 NAS 多协议访问，请参见 "使用 NFS 和 SMB 为 Windows 和 Linux 配置 NAS 存储"。

- 您希望使用最佳实践，而不是浏览每个可用选项。

  有关命令语法的详细信息，请参见 CLI 帮助和 ONTAP 手册页。

- UNIX 文件权限将用于保护新卷的安全。
- 您拥有集群管理员权限，而不是 SVM 管理员权限。

如果要了解有关ONTAP NFS协议功能范围的详细信息、请参见 "NFS参考概述"。

在 ONTAP 中执行此操作的其他方法

要执行以下任务，请执行以下操作 …	请参见 …
重新设计的 System Manager （适用于 ONTAP 9.7 及更高版本）	"使用 NFS 为 Linux 服务器配置 NAS 存储"
System Manager 经典版（适用于 ONTAP 9.7 及更早版本	"NFS 配置概述"

NFS 配置工作流

配置 NFS 包括评估物理存储和网络要求，然后选择特定于您的目标的工作流—配置对新的或现有 SVM 的 NFS 访问，或者向已完全配置 NFS 访问的现有 SVM 添加卷或 qtree 。

准备

评估物理存储要求

在为客户端配置 NFS 存储之前，您必须确保现有聚合中有足够的空间来容纳新卷。如果没有，您可以向现有聚合添加磁盘或创建所需类型的新聚合。

步骤

1. 显示现有聚合中的可用空间：

   ```
   storage aggregate show
   ```

   如果聚合具有足够的空间，请在工作表中记录其名称。

   ```
   cluster::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
   --------- -------- --------- ----- ------- ------ ------ -----------
   aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                             normal
   aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                             normal
   6 entries were displayed.
   ```

2. 如果没有具有足够空间的聚合、请使用向现有聚合添加磁盘 `storage aggregate add-disks` 命令、或者使用创建新聚合 `storage aggregate create` 命令：

相关信息

"ONTAP 概念"

评估网络连接要求

在向客户端提供 NFS 存储之前，您必须验证网络配置是否正确，以满足 NFS 配置要求。

您需要的内容

必须配置以下集群网络对象：

- 物理和逻辑端口
- 广播域
- 子网（如果需要）
- IP 空间（除默认 IP 空间外，根据需要）
- 故障转移组（根据需要，除每个广播域的默认故障转移组外）
- 外部防火墙

步骤

1. 显示可用的物理和虚拟端口：

   ```
   network port show
   ```

   - 如果可能，您应使用数据网络速度最快的端口。
   - 数据网络中的所有组件都必须具有相同的 MTU 设置，才能获得最佳性能。

2. 如果您计划使用子网名称为 LIF 分配 IP 地址和网络掩码值，请验证子网是否存在且具有足够的可用地址：

   ```
   network subnet show
   ```

   子网包含属于同一第 3 层子网的 IP 地址池。可使用创建子网 `network subnet create` 命令：

3. 显示可用 IP 空间：

   ```
   network ipspace show
   ```

   您可以使用默认 IP 空间或自定义 IP 空间。

4. 如果要使用 IPv6 地址，请验证是否已在集群上启用 IPv6 ：

   ```
   network options ipv6 show
   ```

   如果需要、您可以使用启用IPv6 `network options ipv6 modify` 命令：

确定在何处配置新的 **NFS** 存储容量

在创建新的 NFS 卷或 qtree 之前，您必须先确定是将其置于新的还是现有的 SVM 中，以及 SVM 需要多少配置。此决定将决定您的工作流。

选项

- 如果要在新 SVM 或已启用但未配置 NFS 的现有 SVM 上配置卷或 qtree ，请完成 " 配置对 SVM 的 NFS 访问 " 和 " 将 NFS 存储添加到启用了 NFS 的 SVM " 中的步骤。

  配置对 SVM 的 NFS 访问

  将NFS存储添加到启用了NFS的SVM

  如果满足以下条件之一，您可以选择创建新的 SVM ：

  - 首次在集群上启用 NFS 。
  - 集群中的现有 SVM 不希望启用 NFS 支持。
  - 一个集群中有一个或多个启用了 NFS 的 SVM ，您希望在一个隔离的命名空间中使用另一个 NFS 服务器（多租户情形）。 您还应选择此选项，以便在已启用但未配置 NFS 的现有 SVM 上配置存储。如果您创建了用于 SAN 访问的 SVM ，或者在创建 SVM 时未启用任何协议，则可能会出现这种情况。

  在 SVM 上启用 NFS 后，继续配置卷或 qtree 。

- 如果要在已完全配置为可进行 NFS 访问的现有 SVM 上配置卷或 qtree ，请完成 " 将 NFS 存储添加到启用

了 NFS 的 SVM" 中的步骤。

将 NFS 存储添加到启用了 NFS 的 SVM

用于收集 **NFS** 配置信息的工作表

通过 NFS 配置工作表，您可以收集为客户端设置 NFS 访问所需的信息。

您应根据决定在何处配置存储来完成工作表的一个或两个部分：

如果要配置对 SVM 的 NFS 访问，应完成这两个部分。

- 配置对 SVM 的 NFS 访问
- 向启用了 NFS 的 SVM 添加存储容量

如果要向启用了NFS的SVM添加存储容量、则应仅完成以下操作：

- 向启用了 NFS 的 SVM 添加存储容量

有关参数的详细信息，请参见命令手册页。

配置对 **SVM** 的 **NFS** 访问

- 用于创建 SVM* 的参数

您可以在中提供这些值 `vserver create` 命令。

字段	Description	您的价值
`-vserver`	您为新 SVM 提供的名称，可以是完全限定域名（FQDN），也可以遵循在集群中强制实施唯一 SVM 名称的其他约定。	
`-aggregate`	集群中具有足够空间来容纳新 NFS 存储容量的聚合的名称。	
`-rootvolume`	为 SVM 根卷提供的唯一名称。	
`-rootvolume-security-style`	对 SVM 使用 UNIX 安全模式。	`unix`
`-language`	在此工作流中使用默认语言设置。	`C.UTF-8`
`ipspace`	IP 空间是 Storage Virtual Machine（SVM）所在的不同 IP 地址空间。	

- 用于创建 NFS 服务器的参数 *

您可以在中提供这些值 `vserver nfs create` 命令。

如果要启用 NFSv4 或更高版本，则应使用 LDAP 来提高安全性。

字段	Description	您的价值
`-v3`，`-v4.0`，`-v4.1`，`-v4.1-pnfs`	根据需要启用 NFS 版本。 ONTAP 9.8及更高版本也支持v4.2 `v4.1` 已启用。	
`-v4-id-domain`	ID 映射域名。	
`-v4-numeric-ids`	支持数字所有者 ID （已启用或已禁用）。	

- 用于创建 LIF* 的参数

您可以在中提供这些值 `network interface create` 命令。

如果您使用的是 Kerberos ，则应在多个 LIF 上启用 Kerberos 。

字段	Description	您的价值
`-lif`	为新 LIF 提供的名称。	
`-role`	在此工作流中使用数据 LIF 角色。	`data`
`-data-protocol`	在此工作流中仅使用 NFS 协议。	`nfs`
`-home-node`	LIF返回到的节点 `network interface revert` 命令将在LIF上运行。	
`-home-port`	LIF返回到的端口或接口组 `network interface revert` 命令将在LIF上运行。	
`-address`	集群上要由新 LIF 用于数据访问的 IPv4 或 IPv6 地址。	
`-netmask`	LIF 的网络掩码和网关。	

`-subnet`	IP 地址池。已使用、而不是 `-address` 和 `-netmask` 自动分配地址和网络掩码。	
`-firewall-policy`	在此工作流中使用默认数据防火墙策略。	`data`

- 用于 DNS 主机名解析的参数 *

您可以在中提供这些值 `vserver services name-service dns create` 命令。

字段	Description	您的价值
`-domains`	最多五个 DNS 域名。	
`-name-servers`	每个 DNS 名称服务器最多三个 IP 地址。	

名称服务信息

- 用于创建本地用户的参数 *

如果要创建本地用户、请使用提供以下值 `vserver services name-service unix-user create` 命令：如果要通过从统一资源标识符（ Uniform Resource Identifier， URI ）加载包含 UNIX 用户的文件来配置本地用户，则无需手动指定这些值。

	用户名 (`-user`)	用户 ID (`-id`)	组 ID (`-primary-gid`)	全名 (`-full-name`)
示例	johnm	123.	100	John Miller
1.				
2.				
3.				
…				
不包括				

- 用于创建本地组的参数 *

如果要创建本地组、请使用提供以下值 `vserver services name-service unix-group create` 命令：如果要通过从 URI 加载包含 UNIX 组的文件来配置本地组，则无需手动指定这些值。

	组名称 (-name)	组 ID (-id)
示例	工程	100
1.		
2.		
3.		
…		
不包括		

- 用于 NIS* 的参数

您可以在中提供这些值 `vserver services name-service nis-domain create` 命令：

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

字段	Description	您的价值
`-domain`	SVM 将用于名称查找的 NIS 域。	
`-active`	活动的 NIS 域服务器。	`true` 或 `false`
`-servers`	ONTAP 9.0 和 9.1： NIS 域配置使用的一个或多个 NIS 服务器 IP 地址。	
`-nis-servers`	ONTAP 9.2： 域配置所使用的 NIS 服务器的 IP 地址和主机名列表，以英文逗号分隔。	

LDAP 的 * 参数 *

您可以在中提供这些值 `vserver services name-service ldap client create` 命令：

您还需要自签名根CA证书 `.pem` 文件

> 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。

字段	Description	您的价值
-vserver	要为其创建 LDAP 客户端配置的 SVM 的名称。	
-client-config	为新 LDAP 客户端配置分配的名称。	
-servers	ONTAP 9.0 和 9.1： 一个或多个 LDAP 服务器，按 IP 地址列出，以逗号分隔。	
-ldap-servers	ONTAP 9.2： LDAP 服务器的 IP 地址和主机名列表，以英文逗号分隔。	
-query-timeout	使用默认值 3 秒。	3
-min-bind-level	最小绑定身份验证级别。默认值为 anonymous。必须设置为 sasl 如果配置了签名和签章。	
-preferred-ad-servers	一个或多个首选 Active Directory 服务器，按 IP 地址列出，以逗号分隔。	
-ad-domain	Active Directory 域。	
-schema	要使用的模式模板。您可以使用默认模式或自定义模式。	
-port	使用默认LDAP服务器端口 389 。	389
-bind-dn	绑定用户可分辨名称。	
-base-dn	基本可分辨名称。默认值为 "" (root)。	
-base-scope	使用默认的基本搜索范围 subnet 。	subnet
-session-security	启用 LDAP 签名或签名和签章。默认值为 none。	
-use-start-tls	启用基于 TLS 的 LDAP 。默认值为 false。	

- 用于 Kerberos 身份验证的参数 *

您可以在中提供这些值 `vserver nfs kerberos realm create` 命令：根据您使用 Microsoft Active Directory 作为密钥分发中心（ Key Distribution Center ， KDC ）服务器，还是使用 MIT 或其他 UNIX KDC 服务器，某些值会有所不同。

字段	Description	您的价值
`-vserver`	要与 KDC 通信的 SVM 。	
`-realm`	Kerberos 域。	
`-clock-skew`	客户端和服务器之间允许的时钟偏差。	
`-kdc-ip`	KDC IP 地址。	
`-kdc-port`	KDC 端口号。	
`-adserver-name`	仅限 Microsoft KDC： AD 服务器名称。	
`-adserver-ip`	仅限 Microsoft KDC： AD 服务器 IP 地址。	
`-adminserver-ip`	仅限 UNIX KDC： 管理服务器 IP 地址。	
`-adminserver-port`	仅限 UNIX KDC： 管理服务器端口号。	
`-passwordserver-ip`	仅限 UNIX KDC： 密码服务器 IP 地址。	
`-passwordserver-port`	仅限 UNIX KDC： 密码服务器端口。	
`-kdc-vendor`	KDC 供应商。	{`Microsoft` 我们可以为您提供 `Other`}
`-comment`	任何所需注释。	

您可以在中提供这些值 `vserver nfs kerberos interface enable` 命令：

字段	Description	您的价值

`-vserver`	要为其创建 Kerberos 配置的 SVM 的名称。	
`-lif`	要启用 Kerberos 的数据 LIF 。您可以在多个 LIF 上启用 Kerberos 。	
`-spn`	服务主体名称（ SPN ）	
`-permitted-enc-types`	基于NFS的Kerberos允许的加密类型； `aes-256` 建议使用、具体取决于客户端功能。	
`-admin-username`	用于直接从 KDC 检索 SPN 机密密钥的 KDC 管理员凭据。密码为必填项	
`-keytab-uri`	如果您没有 KDC 管理员凭据，则为 KDC 中包含 SPN 密钥的 keytab 文件。	
`-ou`	使用域为 Microsoft KDC 启用 Kerberos 时，要在其中创建 Microsoft Active Directory 服务器帐户的组织单位（ OU ）。	

向启用了 **NFS** 的 **SVM** 添加存储容量

- 用于创建导出策略和规则的参数 *

您可以在中提供这些值 `vserver export-policy create` 命令：

字段	Description	您的价值
`-vserver`	要托管新卷的 SVM 的名称。	
`-policyname`	为新导出策略提供的名称。	

您可以使用为每个规则提供以下值 `vserver export-policy rule create` 命令：

字段	Description	您的价值
`-clientmatch`	客户端匹配规范。	
`-ruleindex`	导出规则在规则列表中的位置。	
`-protocol`	在此工作流中使用 NFS 。	`nfs`

`-rorule`	只读访问的身份验证方法。	
`-rwrule`	读写访问的身份验证方法。	
`-superuser`	用于超级用户访问的身份验证方法。	
`-anon`	匿名用户映射到的用户 ID 。	

您必须为每个导出策略创建一个或多个规则。

-ruleindex	**-clientmatch**	**-rorule**	**-rwrule**	**-superuser**	**-anon**
示例	0.0.0.0/0 ，@rootaccess_netgroup	任意	krb5.	系统	6554
1.					
2.					
3.					
…					
不包括					

用于创建卷的 * 参数 *

您可以在中提供这些值 `volume create` 命令。

字段	Description	您的价值
`-vserver`	要托管新卷的新 SVM 或现有 SVM 的名称。	
`-volume`	为新卷提供的唯一描述性名称。	
`-aggregate`	集群中具有足够空间来容纳新 NFS 卷的聚合的名称。	
`-size`	为新卷的大小提供的整数。	
`-user`	设置为卷根所有者的用户的名称或 ID 。	

`-group`	设置为卷根所有者的组的名称或 ID 。	
`--security-style`	对此工作流使用 UNIX 安全模式。	`unix`
`-junction-path`	根（/）下要挂载新卷的位置。	
`-export-policy`	如果您计划使用现有导出策略，则可以在创建卷时输入其名称。	

用于创建 qtree* 的 * 参数

您可以在中提供这些值 `volume qtree create` 命令。

字段	Description	您的价值
`-vserver`	包含 qtree 的卷所在 SVM 的名称。	
`-volume`	要包含新 qtree 的卷的名称。	
`-qtree`	为新 qtree 提供的唯一描述性名称，不超过 64 个字符。	
`-qtree-path`	格式的qtree路径参数 `/vol/volume_name/qtree_name\>` 可以指定、而不是将卷和qtree指定为单独的参数。	
`-unix-permissions`	可选： qtree 的 UNIX 权限。	
`-export-policy`	如果您计划使用现有导出策略，则可以在创建 qtree 时输入其名称。	

配置对 SVM 的 NFS 访问

创建 SVM：

如果集群中尚未至少有一个 SVM 来为 NFS 客户端提供数据访问，则必须创建一个 SVM 。

开始之前

- 从ONTAP 9.13.1开始、您可以为Storage VM设置最大容量。您还可以在SVM接近阈值容量级别时配置警报。有关详细信息，请参见 管理SVM容量。

步骤

1. 创建 SVM：

   `vserver create -vserver vserver_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style unix -language C.UTF-8 -ipspace ipspace_name`

   - 对使用UNIX设置 `-rootvolume-security-style` 选项
   - 使用默认C.UTF-8 `-language` 选项
   - 。 `ipspace` 设置是可选的。

2. 验证新创建的 SVM 的配置和状态：

   `vserver show -vserver vserver_name`

   。 `Allowed Protocols` 字段必须包含NFS。您可以稍后编辑此列表。

   。 `Vserver Operational State` 字段必须显示 `running` 状态。如果显示 `initializing` 状态、表示某些中间操作(如创建根卷)失败、您必须删除SVM并重新创建它。

示例

以下命令将在 IP 空间 ipspaceA 中创建用于数据访问的 SVM：

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

以下命令显示已创建根卷为1 GB的SVM、并且此SVM已自动启动并位于中 `running` 状态。根卷具有一个默认导出策略，该策略不包含任何规则，因此根卷在创建时不会导出。

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                                Vserver Type: data
                             Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                 Root Volume: root_vs1
                                   Aggregate: aggr1
                                  NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
                Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                         Vserver Admin State: running
                   Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                           Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                        Disallowed Protocols: -
                            QoS Policy Group: -
                                 Config Lock: false
                                IPspace Name: ipspaceA
```

> 从ONTAP 9.13.1开始、您可以设置自适应QoS策略组模板、以便为SVM中的卷应用吞吐量下限和上限限制。只有在创建SVM之后、才能应用此策略。要了解有关此过程的更多信息、请参见 设置自适应策略组模板。

验证是否已在 **SVM** 上启用 **NFS** 协议

在 SVM 上配置和使用 NFS 之前，必须验证是否已启用此协议。

关于此任务

此操作通常在SVM设置期间完成、但如果您在设置期间未启用此协议、则可以稍后使用启用它 `vserver add-protocols` 命令：

> 创建 LIF 后，您不能在该 LIF 中添加或删除协议。

您还可以使用在SVM上禁用协议 `vserver remove-protocols` 命令：

步骤

1. 检查 SVM 当前已启用和禁用的协议：

```
vserver show -vserver vserver_name -protocols
```

您也可以使用 `vserver show-protocols` 命令以查看集群中所有SVM上当前已启用的协议。

2. 如有必要，启用或禁用协议：
   - 启用NFS协议：
     `vserver add-protocols -vserver vserver_name -protocols nfs`
   - 禁用协议：
     `vserver remove-protocols -vserver vserver_name -protocols protocol_name [,protocol_name,…]`
3. 确认已启用和禁用的协议已正确更新：

```
vserver show -vserver vserver_name -protocols
```

示例

以下命令显示 SVM vs1 上当前已启用和禁用（允许和不允许）的协议：

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       -----------------------   ------------------------
vs1.example.com   nfs                       cifs, fcp, iscsi, ndmp
```

以下命令可通过添加来允许通过NFS进行访问 `nfs` 到SVM VS1上已启用的协议列表：

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

打开 **SVM** 根卷的导出策略

SVM 根卷的默认导出策略必须包含一条规则，允许所有客户端通过 NFS 进行开放访问。如果没有此规则，则会拒绝所有 NFS 客户端访问 SVM 及其卷。

关于此任务

创建新的 SVM 时，系统会自动为 SVM 的根卷创建默认导出策略（称为 default ）。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。

您应验证默认导出策略中的所有 NFS 客户端是否均可访问，然后通过为单个卷或 qtree 创建自定义导出策略来限制对单个卷的访问。

步骤

1. 如果您使用的是现有 SVM ，请检查默认根卷导出策略：

```
vserver export-policy rule show
```

命令输出应类似于以下内容：

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                    Vserver: vs1.example.com
                                Policy Name: default
                                 Rule Index: 1
                            Access Protocol:  nfs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                             RO Access Rule: any
                             RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                    Superuser Security Types: any
                Honor SetUID Bits in SETATTR: true
                   Allow Creation of Devices: true
```

如果存在允许开放访问的规则，则此任务将完成。如果没有，请继续执行下一步。

2. 为 SVM 根卷创建导出规则：

   `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`

   如果SVM仅包含受Kerberos保护的卷、则可以设置导出规则选项 `-rorule`， `-rwrule`，和 `-superuser` 根卷的 `krb5` 或 `krb5i`。例如：

   `-rorule krb5i -rwrule krb5i -superuser krb5i`

3. 使用验证规则创建 `vserver export-policy rule show` 命令：

结果

现在，任何 NFS 客户端都可以访问在 SVM 上创建的任何卷或 qtree 。

创建 **NFS** 服务器

在确认NFS在集群上已获得许可后、您可以使用 `vserver nfs create` 命令以在SVM上创建NFS服务器并指定其支持的NFS版本。

关于此任务

可以将 SVM 配置为支持一个或多个 NFS 版本。如果您支持 NFSv4 或更高版本：

- NFSv4 用户 ID 映射域名在 NFSv4 服务器和目标客户端上必须相同。

  只要 NFSv4 服务器和客户端使用相同的名称，它不一定需要与 LDAP 或 NIS 域名相同。

- 目标客户端必须支持 NFSv4 数字 ID 设置。
- 出于安全原因，您应在 NFSv4 部署中使用 LDAP 提供名称服务。

开始之前

必须已将 SVM 配置为允许 NFS 协议。

步骤

1. 验证 NFS 是否已在集群上获得许可：

   ```
   system license show -package nfs
   ```

   如果不是，请联系您的销售代表。

2. 创建 NFS 服务器：

   ```
   vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0
   {enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids
   {enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
   ```

   您可以选择启用 NFS 版本的任意组合。如果要支持pNFS、则必须同时启用这两者 `-v4.1` 和 `-v4.1-pnfs` 选项

   如果启用 v4 或更高版本，还应确保正确设置以下选项：

   - `-v4-id-domain`

     此可选参数用于指定 NFSv4 协议定义的用户名和组名称字符串形式的域部分。默认情况下，如果设置了 NIS 域，则 ONTAP 将使用 NIS 域；否则，将使用 DNS 域。您必须提供一个与目标客户端使用的域名匹配的值。

   - `-v4-numeric-ids`

     此可选参数用于指定是否在 NFSv4 所有者属性中启用对数字字符串标识符的支持。默认设置为 enabled ，但您应验证目标客户端是否支持该设置。

   您可以稍后使用启用其他NFS功能 `vserver nfs modify` 命令：

3. 验证 NFS 是否正在运行：

   ```
   vserver nfs status -vserver vserver_name
   ```

4. 验证是否已根据需要配置 NFS ：

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

示例

以下命令会在 SVM vs1 上创建一个 NFS 服务器，并启用 NFSv3 和 NFSv4.0 ：

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id
-domain my_domain.com
```

以下命令用于验证名为 vs1 的新 NFS 服务器的状态和配置值：

```
vs1::> vserver nfs status -vserver vs1
The NFS server is running on Vserver "vs1".

vs1::> vserver nfs show -vserver vs1

                              Vserver: vs1
                  General NFS Access: true
                                NFS v3: enabled
                              NFS v4.0: enabled
                         UDP Protocol: enabled
                         TCP Protocol: enabled
                 Default Windows User: -
                  NFSv4.0 ACL Support: disabled
    NFSv4.0 Read Delegation Support: disabled
   NFSv4.0 Write Delegation Support: disabled
            NFSv4 ID Mapping Domain: my_domain.com
...
```

创建 LIF

LIF 是指与物理或逻辑端口关联的 IP 地址。如果组件出现故障，则 LIF 可以故障转移到或迁移到其他物理端口，从而继续与网络通信。

您需要的内容

- 底层物理或逻辑网络端口必须已配置为管理端口 `up` 状态。
- 如果您计划使用子网名称为 LIF 分配 IP 地址和网络掩码值，则此子网必须已存在。

  子网包含属于同一第 3 层子网的 IP 地址池。它们是使用创建的 `network subnet create` 命令：

- 用于指定 LIF 处理的流量类型的机制已发生更改。对于 ONTAP 9.5 及更早版本， LIF 使用角色指定要处理的流量类型。从 ONTAP 9.6 开始， LIF 使用服务策略指定要处理的流量类型。

关于此任务

- 您可以在同一网络端口上创建 IPv4 和 IPv6 LIF 。
- 如果您使用的是 Kerberos 身份验证，请在多个 LIF 上启用 Kerberos 。
- 如果集群中有大量LIF、则可以使用验证集群上支持的LIF容量 `network interface capacity show` 命令以及每个节点上支持的LIF容量 `network interface capacity details show` 命令(在高级权限级别)。
- 从 ONTAP 9.7 开始，如果同一子网中已存在 SVM 的其他 LIF ，则无需指定 LIF 的主端口。ONTAP 会自动在与已在同一子网中配置的其他 LIF 位于同一广播域的指定主节点上选择一个随机端口。

从 ONTAP 9.4 开始，支持 FC-NVMe 。如果要创建 FC-NVMe LIF ，应注意以下事项：

- 创建 LIF 的 FC 适配器必须支持 NVMe 协议。

- FC-NVMe 可以是数据 LIF 上的唯一数据协议。
- 必须为支持 SAN 的每个 Storage Virtual Machine （ SVM ）配置一个 LIF 处理管理流量。
- NVMe LIF 和命名空间必须托管在同一节点上。
- 每个 SVM 只能配置一个处理数据流量的 NVMe LIF 。

步骤

1. 创建 LIF：

   ```
   network interface create -vserver vserver_name -lif lif_name -role data -data
   -protocol nfs -home-node node_name -home-port port_name {-address IP_address
   -netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
   -revert {true|false}
   ```

选项	Description
• ONTAP 9.5 及更早版本 *	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`
• ONTAP 9.6 及更高版本 *	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`

   - 。 `-role` 使用服务策略创建LIF时不需要参数(从ONTAP 9.6开始)。
   - 。 `-data-protocol` 必须在创建LIF时指定参数、如果不销毁并重新创建数据LIF、则以后无法修改此参数。

     。 `-data-protocol` 使用服务策略创建LIF时不需要参数(从ONTAP 9.6开始)。

   - `-home-node` 是LIF返回到的节点 `network interface revert` 命令将在LIF上运行。

     您还可以使用指定LIF是否应自动还原到主节点和主端口 `-auto-revert` 选项

   - `-home-port` 是LIF返回到的物理或逻辑端口 `network interface revert` 命令将在LIF上运行。
   - 您可以使用指定IP地址 `-address` 和 `-netmask` 选项、或者使用启用从子网分配 `-subnet_name` 选项
   - 使用子网提供 IP 地址和网络掩码时，如果使用网关定义了子网，则在使用该子网创建 LIF 时，系统会自动向 SVM 添加指向该网关的默认路由。
   - 如果您手动分配 IP 地址（而不使用子网），则在其他 IP 子网上存在客户端或域控制器时，可能需要配置指向网关的默认路由。。 `network route create` 手册页包含有关在SVM中创建静态路由的信息。

- 。 `-firewall-policy` 选项中、使用相同的默认值 `data` 作为LIF角色。

  如果需要，您可以稍后创建和添加自定义防火墙策略。

  > 从ONTAP 9.10.1开始、防火墙策略已弃用、并完全替换为LIF服务策略。有关详细信息，请参见 "为 LIF 配置防火墙策略"。

- `-auto-revert` 用于指定在启动、更改管理数据库状态或建立网络连接等情况下、数据LIF是否自动还原到其主节点。默认设置为 `false`，但您可以将其设置为 `false` 具体取决于您环境中的网络管理策略。

2. 使用验证是否已成功创建LIF `network interface show` 命令：
3. 验证配置的 IP 地址是否可访问：

要验证 ...	使用 ...
IPv4 地址	`network ping`
IPv6地址	`network ping6`

4. 如果使用的是 Kerberos ，请重复步骤 1 到 3 以创建其他 LIF 。

   必须在每个 LIF 上单独启用 Kerberos 。

示例

以下命令将使用创建LIF并指定IP地址和网络掩码值 `-address` 和 `-netmask` 参数：

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

以下命令将创建一个 LIF ，并从指定子网（名为 client1_sub ）分配 IP 地址和网络掩码值：

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

以下命令显示 cluster-1 中的所有 LIF 。数据 LIF datalif1 和 datalif3 配置了 IPv4 地址，而 datalif4 配置了 IPv6 地址：

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

以下命令显示如何创建分配给的NAS数据LIF `default-data-files` 服务策略：

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

启用 DNS 以进行主机名解析

您可以使用 `vserver services name-service dns` 命令以在SVM上启用DNS、并将其配置为使用DNS进行主机名解析。主机名可使用外部 DNS 服务器进行解析。

您需要的内容

站点范围的 DNS 服务器必须可用于主机名查找。

您应配置多个 DNS 服务器，以避免单点故障。。 `vserver services name-service dns create` 如果仅输入一个DNS服务器名称、则命令会发出警告。

关于此任务

网络管理指南 _ 包含有关在 SVM 上配置动态 DNS 的信息。

步骤

1. 在 SVM 上启用 DNS：

   `vserver services name-service dns create -vserver` *`vserver_name`* `-domains` *`domain_name`* `-name-servers` *`ip_addresses`* `-state enabled`

   以下命令将在 SVM vs1 上启用外部 DNS 服务器：

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   > 从ONTAP 9.2开始、 `vserver services name-service dns create` 命令会执行自动配置验证、如果ONTAP无法联系到名称服务器、则会报告错误消息。

2. 使用显示DNS域配置 `vserver services name-service dns show` 命令：

   以下命令显示集群中所有 SVM 的 DNS 配置：

   ```
   vserver services name-service dns show
                                                  Name
   Vserver           State     Domains              Servers
   ----------------- --------- -------------------- -------------
   cluster1          enabled   example.com          192.0.2.201,
                                                    192.0.2.202
   vs1.example.com   enabled   example.com          192.0.2.201,
                                                    192.0.2.202
   ```

   以下命令显示 SVM vs1 的详细 DNS 配置信息：

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
          Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. 使用验证名称服务器的状态 `vserver services name-service dns check` 命令：

   - `vserver services name-service dns check` 命令从ONTAP 9.2开始可用。

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
--------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

配置名称服务

配置名称服务概述

根据存储系统的配置， ONTAP 需要能够查找主机，用户，组或网络组信息，以便能够正确访问客户端。您必须配置名称服务，以使 ONTAP 能够访问本地或外部名称服务来获取此信息。

您应使用 NIS 或 LDAP 等名称服务在客户端身份验证期间便于进行名称查找。为了提高安全性，最好尽可能使用 LDAP ，尤其是在部署 NFSv4 或更高版本时。如果外部名称服务器不可用，您还应配置本地用户和组。

名称服务信息必须在所有源上保持同步。

配置名称服务切换表

您必须正确配置名称服务切换表，以使 ONTAP 能够查询本地或外部名称服务以检索主机，用户，组，网络组或名称映射信息。

您需要的内容

您必须已根据环境情况确定要用于主机，用户，组，网络组或名称映射的名称服务。

如果您计划使用网络组，则网络组中指定的所有 IPv6 地址都必须按照 RFC 5952 中的说明进行缩短和压缩。

关于此任务

请勿包含未使用的信息源。例如、如果您的环境未使用NIS、请勿指定 `-sources nis` 选项

步骤

1. 将必要的条目添加到名称服务切换表：

   `vserver services name-service ns-switch create -vserver` *`vserver_name`* `-database` *`database_name`* `-sources` *`source_names`*

2. 验证名称服务切换表是否包含所需顺序的预期条目：

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

   如果要进行任何更正、必须使用 `vserver services name-service ns-switch modify` 或 `vserver services name-service ns-switch delete` 命令

示例

以下示例将在名称服务切换表中为 SVM vs1 创建一个新条目，以便使用本地网络组文件和外部 NIS 服务器按此顺序查找网络组信息：

```
cluster::> vserver services name-service ns-switch create -vserver vs1
-database netgroup -sources files,nis
```

完成后

- 您必须配置为 SVM 指定的名称服务以提供数据访问。
- 如果您删除了 SVM 的任何名称服务，则还必须将其从名称服务切换表中删除。

  如果无法从名称服务切换表中删除名称服务，则客户端对存储系统的访问可能无法按预期工作。

配置本地 **UNIX** 用户和组

配置本地 **UNIX** 用户和组概述

您可以在 SVM 上使用本地 UNIX 用户和组进行身份验证和名称映射。您可以手动创建 UNIX 用户和组，也可以通过统一资源标识符（ Uniform Resource Identifier ， URI ）加载包含 UNIX 用户或组的文件。

默认情况下，集群中本地 UNIX 用户组和组成员的组合上限为 32 ， 768 。集群管理员可以修改此限制。

创建本地 **UNIX** 用户

您可以使用 `vserver services name-service unix-user create` 命令以创建本地UNIX用户。本地 UNIX 用户是指您在 SVM 上创建的 UNIX 用户，该用户作为 UNIX 名称服务选项，用于处理名称映射。

步骤

1. 创建本地 UNIX 用户：

`vserver services name-service unix-user create -vserver vserver_name -user user_name -id integer -primary-gid integer -full-name full_name`

`-user user_name` 指定用户名。用户名长度不能超过 64 个字符。

`-id integer` 指定您分配的用户ID。

`-primary-gid integer` 指定主组ID。此操作会将用户添加到主组。创建用户后，您可以手动将该用户添加到任何所需的其他组。

示例

以下命令会在名为 vs1 的 SVM 上创建一个名为 johnm （全名为 "John Miller" ）的本地 UNIX 用户。用户的 ID 为 123 ，主组 ID 为 100 。

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

从 URI 加载本地 UNIX 用户

除了在SVM中手动创建单个本地UNIX用户之外、您还可以通过统一资源标识符(URI)将本地UNIX用户列表加载到SVM中、从而简化此任务。（`vserver services name-service unix-user load-from-uri`）。

步骤

1. 创建一个包含要加载的本地 UNIX 用户列表的文件。

   文件必须包含UNIX中的用户信息 `/etc/passwd` 格式：

   `user_name: password: user_ID: group_ID: full_name`

   命令将丢弃的值 *`password`* 字段以及后面字段的值 *`full_name`* 字段 (*`home_directory`* 和 *`shell`*）。

   支持的最大文件大小为 2.5 MB 。

2. 验证此列表是否不包含任何重复信息。

   如果此列表包含重复条目，则加载此列表将失败并显示错误消息。

3. 将文件复制到服务器。

   存储系统必须可通过 HTTP ， HTTPS ， FTP 或 FTPS 访问此服务器。

4. 确定文件的 URI 。

   此 URI 是您为存储系统提供的地址，用于指示文件的位置。

5. 从 URI 将包含本地 UNIX 用户列表的文件加载到 SVM 中：

`vserver services name-service unix-user load-from-uri -vserver vserver_name -uri {ftp|http|ftps|https}://uri -overwrite {true|false}`

`-overwrite {true false}`指定是否覆盖条目。默认值为 `false`。

示例

以下命令将从URI加载本地UNIX用户列表 `ftp://ftp.example.com/passwd` 到名为VS1的SVM中。SVM 上的现有用户不会被 URI 中的信息覆盖。

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

创建本地 UNIX 组

您可以使用 `vserver services name-service unix-group create` 命令创建SVM的本地UNIX组。本地 UNIX 组用于本地 UNIX 用户。

步骤

1. 创建本地 UNIX 组：

   `vserver services name-service unix-group create -vserver vserver_name -name group_name -id integer`

   `-name group_name` 指定组名称。组名称长度不能超过 64 个字符。

   `-id integer` 指定您分配的组ID。

示例

以下命令会在名为 vs1 的 SVM 上创建一个名为 eng 的本地组。此组的 ID 为 101 。

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

将用户添加到本地 UNIX 组

您可以使用 `vserver services name-service unix-group adduser` 命令将用户添加到SVM本地的补充UNIX组。

步骤

1. 将用户添加到本地 UNIX 组：

`vserver services name-service unix-group adduser -vserver vserver_name -name group_name -username user_name`

`-name group_name` 指定除用户的主组之外要将用户添加到的UNIX组的名称。

示例

以下命令会将名为 max 的用户添加到名为 vs1 的 SVM 上名为 eng 的本地 UNIX 组：

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

从 **URI** 加载本地 **UNIX** 组

除了手动创建单个本地UNIX组之外、您还可以使用从统一资源标识符(uniual resource ID标识 符、URI)将本地UNIX组列表加载到SVM中 `vserver services name-service unix-group load-from-uri` 命令：

步骤

1. 创建一个包含要加载的本地 UNIX 组列表的文件。

   文件必须包含UNIX中的组信息 `/etc/group` 格式：

   `group_name: password: group_ID: comma_separated_list_of_users`

   命令将丢弃的值 *`password`* 字段。

   支持的最大文件大小为1 MB。

   组文件中每行的最大长度为 32 ， 768 个字符。

2. 验证此列表是否不包含任何重复信息。

   此列表不得包含重复条目，否则加载此列表将失败。如果SVM中已存在条目、则必须设置 `-overwrite` 参数设置为 `true` 使用新文件覆盖所有现有条目、或者确保新文件不包含与现有条目重复的任何条目。

3. 将文件复制到服务器。

   存储系统必须可通过 HTTP ， HTTPS ， FTP 或 FTPS 访问此服务器。

4. 确定文件的 URI 。

   此 URI 是您为存储系统提供的地址，用于指示文件的位置。

5. 从 URI 将包含本地 UNIX 组列表的文件加载到 SVM 中：

   `vserver services name-service unix-group load-from-uri -vserver` *`vserver_name`* `-uri {ftp|http|ftps|https}://`*`uri`* `-overwrite {true|false}`

   `-overwrite true false`}指定是否覆盖条目。默认值为 `false`。如果将此参数指定为 `true`，ONTAP将使用您正在加载的文件中的条目替换指定SVM的整个现有本地UNIX组数据库。

示例

以下命令将从URI加载本地UNIX组的列表 `ftp://ftp.example.com/group` 到名为VS1的SVM中。SVM上的现有组不会被 URI 中的信息覆盖。

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

使用网络组

使用网络组概述

您可以使用网络组进行用户身份验证，并在导出策略规则中匹配客户端。您可以通过外部名称服务器(LDAP或NIS)提供对网络组的访问权限、也可以使用将网络组从统一资源标识符(URI)加载到SVM中 `vserver services name-service netgroup load` 命令：

您需要的内容

在使用网络组之前，您必须确保满足以下条件：

- 网络组中的所有主机，无论源（ NIS ， LDAP 或本地文件）如何，都必须同时具有正向（ A ）和反向（ PTR ） DNS 记录，才能提供一致的正向和反向 DNS 查找。

  此外，如果客户端的 IP 地址具有多个 PTR 记录，则所有这些主机名都必须是网络组的成员并具有相应的 A 记录。

- 网络组中所有主机的名称，无论其源（ NIS ， LDAP 或本地文件）如何，都必须拼写正确，并使用正确的大小写。网络组中使用的主机名大小写不一致可能导致意外行为，例如导出检查失败。
- 网络组中指定的所有 IPv6 地址都必须按照 RFC 5952 中的说明进行缩短和压缩。

  例如， 2011： hu9： 0： 0： 0： 0： 3： 1 必须缩短为 2011： hu9：： 3： 1 。

关于此任务

使用网络组时，您可以执行以下操作：

- 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。
- 您可以使用 `vserver services name-service getxxbyyy netgrp` 命令以检查客户端是否属于网络组。

  系统将根据配置的名称服务切换顺序选择用于执行查找的底层服务。

将网络组加载到 **SVM** 中

在导出策略规则中匹配客户端的方法之一是使用网络组中列出的主机。除了使用存储在外部名称服务器中的网络组之外、您还可以将网络组从统一资源标识符(URI)加载到SVM中（`vserver services name-service netgroup load`）。

您需要的内容

在加载到 SVM 之前，网络组文件必须满足以下要求：

- 该文件必须使用用于填充 NIS 的正确网络组文本文件格式。

  ONTAP 会在加载网络组文本文件格式之前对其进行检查。如果文件包含错误，则不会加载该文件，并且会显示一条消息，指示您必须在该文件中执行的更正。更正错误后，您可以将网络组文件重新加载到指定的 SVM 中。

- 网络组文件中主机名中的任何字母字符都应小写。
- 支持的最大文件大小为5 MB。
- 支持的嵌套网络组的最大级别为 1000 。
- 在网络组文件中定义主机名时，只能使用主 DNS 主机名。

  为了避免导出访问问题，不应使用 DNS CNAME 或轮循记录定义主机名。

- 网络组文件中三个组的用户和域部分应保留为空，因为 ONTAP 不支持它们。

  仅支持主机 /IP 部分。

关于此任务

ONTAP 支持按主机搜索本地网络组文件。加载网络组文件后， ONTAP 会自动创建 netgroup.byHost 映射以启用按主机搜索网络组。在处理导出策略规则以评估客户端访问时，这可以显著加快本地网络组搜索的速度。

步骤

1. 从 URI 将网络组加载到 SVM：

   `vserver services name-service netgroup load -vserver` *`vserver_name`* `-source {ftp|http|ftps|https}://`*`uri`*

   加载网络组文件并构建 netgroup.byHost 映射可能需要几分钟的时间。

   如果要更新网络组，您可以编辑该文件并将更新后的网络组文件加载到 SVM 中。

示例

以下命令会通过HTTP URL将网络组定义加载到名为VS1的SVM中 `http://intranet/downloads/corp-netgroup`：

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

验证网络组定义的状态

将网络组加载到SVM后、您可以使用 `vserver services name-service netgroup status` 命令以验证网络组定义的状态。这样，您就可以确定支持 SVM 的所有节点上的网络组定义是否一致。

步骤

1. 将权限级别设置为高级：

```
set -privilege advanced
```

2. 验证网络组定义的状态：

   ```
   vserver services name-service netgroup status
   ```

   您可以在更详细的视图中显示追加信息。

3. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

示例

设置权限级别后，以下命令将显示所有 SVM 的网络组状态：

```
vs1::> set -privilege advanced

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

vs1::*> vserver services name-service netgroup status
Virtual
Server    Node            Load Time           Hash Value
--------- --------------- -------------------
--------------------------------
vs1
          node1           9/20/2006 16:04:53
e6cb38ec1396a280c0d2b77e3a84eda2
          node2           9/20/2006 16:06:26
e6cb38ec1396a280c0d2b77e3a84eda2
          node3           9/20/2006 16:08:08
e6cb38ec1396a280c0d2b77e3a84eda2
          node4           9/20/2006 16:11:33
e6cb38ec1396a280c0d2b77e3a84eda2
```

创建 **NIS** 域配置

如果您的环境使用网络信息服务(Network Information Service、NIS)提供名称服务、则必须使用为SVM创建NIS域配置 `vserver services name-service nis-domain create` 命令：

您需要的内容

在 SVM 上配置 NIS 域之前，所有已配置的 NIS 服务器都必须可用且可访问。

如果计划使用 NIS 进行目录搜索，则 NIS 服务器中的映射每个条目不能超过 1 ， 024 个字符。请勿指定不符合此限制的 NIS 服务器。否则，依赖于 NIS 条目的客户端访问可能会失败。

关于此任务

您可以创建多个 NIS 域。但是、您只能使用设置为的 `active`。

如果NIS数据库包含 `netgroup.byhost` 地图、ONTAP可以使用它加快搜索速度。。 `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。从ONTAP 9.7开始、为NIS `netgroup.byhost` 可以使用缓存条目 `vserver services name-service nis-domain netgroup-database` 命令

不支持使用NIS进行主机名解析。

步骤

1. 创建 NIS 域配置：

   ```
   vserver services name-service nis-domain create -vserver vs1 -domain
   domain_name -active true -servers IP_addresses
   ```

   最多可以指定 10 个 NIS 服务器。

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

2. 验证是否已创建域：

   ```
   vserver services name-service nis-domain show
   ```

示例

以下命令将在 SVM vs1 上为 NIS 域 nisdomain 创建 NIS 域配置并使其处于活动状态，并且 NIS 服务器的 IP 地址为 192.0.2.180 ：

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -active true -nis-servers 192.0.2.180
```

使用 **LDAP**

LDAP 使用概述

如果在您的环境中使用 LDAP 提供名称服务，则需要与 LDAP 管理员一起确定要求和适当的存储系统配置，然后将 SVM 作为 LDAP 客户端启用。

从 ONTAP 9.10.1 开始，默认情况下， Active Directory 和名称服务 LDAP 连接均支持 LDAP 通道绑定。只有在启用了 Start-TLS 或 LDAPS 且会话安全设置为 sign 或 seal 的情况下， ONTAP 才会尝试使用 LDAP 连接进行通道绑定。要禁用或重新启用与名称服务器的LDAP通道绑定、请使用 `-try-channel-binding` 参数 `ldap client modify` 命令：

有关详细信息，请参见 "2020 年 Windows 的 LDAP 通道绑定和 LDAP 签名要求"。

- 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。
    - 当 -bind-as-cifs-server 设置为 true 时，域密码应相同以进行身份验证。

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)

- 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。

有关详细信息 ...

- "NetApp 技术报告 4835：《如何在 ONTAP 中配置 LDAP 》"
- "在 SVM 上安装自签名根 CA 证书"

创建新的 **LDAP** 客户端模式

如果环境中的 LDAP 模式与 ONTAP 默认值不同，则必须在创建 LDAP 客户端配置之前为 ONTAP 创建新的 LDAP 客户端模式。

关于此任务

大多数 LDAP 服务器都可以使用 ONTAP 提供的默认模式：

- MS-AD-BIS （大多数 Windows 2012 及更高版本 AD 服务器的首选架构）
- AD-IDMU （ Windows 2008 ， Windows 2012 及更高版本的 AD 服务器）
- AD-SFU （ Windows 2003 及更早版本的 AD 服务器）
- RFC-2307 （ UNIX LDAP 服务器）

如果需要使用非默认 LDAP 模式，则必须在创建 LDAP 客户端配置之前创建该模式。在创建新模式之前，请咨询 LDAP 管理员。

无法修改 ONTAP 提供的默认 LDAP 模式。要创建新模式，请创建一个副本，然后相应地修改该副本。

步骤

1. 显示现有 LDAP 客户端模式模板以确定要复制的模板：

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

2. 将权限级别设置为高级：

```
set -privilege advanced
```

3. 为现有 LDAP 客户端模式创建副本：

```
vserver services name-service ldap client schema copy -vserver vserver_name
-schema existing_schema_name -new-schema-name new_schema_name
```

4. 修改新架构并根据您的环境对其进行自定义：

```
vserver services name-service ldap client schema modify
```

5. 返回到管理权限级别：

```
set -privilege admin
```

创建 **LDAP** 客户端配置

如果您希望ONTAP访问您环境中的外部LDAP或Active Directory服务、则需要先在存储系统上设置LDAP客户端。

您需要的内容

Active Directory域解析列表中前三个服务器之一必须已启动并提供数据。否则，此任务将失败。

> 有多个服务器、其中在任意时间点有两个以上的服务器停机。

步骤

1. 请咨询LDAP管理员以确定的适当配置值 `vserver services name-service ldap client create` 命令：

   a. 指定与 LDAP 服务器的基于域或基于地址的连接。

      - `-ad-domain` 和 `-servers` 选项不能同时使用。

        - 使用 `-ad-domain` 选项以在Active Directory域中启用LDAP服务器发现。

          - 您可以使用 `-restrict-discovery-to-site` 用于将LDAP服务器发现限制为指定域的CIFS默认站点的选项。如果使用此选项、则还需要使用指定CIFS默认站点 `-default-site`。

        - 您可以使用 `-preferred-ad-servers` 此选项可按IP地址在逗号分隔列表中指定一个或多个首选Active Directory服务器。创建客户端后、您可以使用修改此列表 `vserver services name-service ldap client modify` 命令：

        - 使用 `-servers` 可选择通过IP地址在逗号分隔列表中指定一个或多个LDAP服务器(Active Directory或UNIX)。

          > - `-servers` 选项在ONTAP 9.2中已弃用。从ONTAP 9.2开始、 `-ldap-servers` 字段将取代 `-servers` 字段。此字段可以使用LDAP服务器的主机名或IP地址。

   b. 指定默认或自定义 LDAP 模式。

      大多数 LDAP 服务器都可以使用 ONTAP 提供的默认只读模式。除非另有要求，否则最好使用这些默认

模式。如果是，您可以通过复制默认模式（默认模式为只读）并修改副本来创建自己的模式。

默认模式：

- MS-AD-BIS

  此模式基于 RFC-2307bis ，是大多数标准 Windows 2012 及更高版本 LDAP 部署的首选 LDAP 模式。

- `AD-IDMU`

  此模式基于适用于 UNIX 的 Active Directory 身份管理，适用于大多数 Windows 2008 ， Windows 2012 及更高版本的 AD 服务器。

- `AD-SFU`

  此模式基于适用于 UNIX 的 Active Directory 服务，适用于大多数 Windows 2003 及更早版本的 AD 服务器。

- `RFC-2307`

  根据 RFC-2307 （使用 LDAP 作为网络信息服务的方法 _ ），此模式适用于大多数 UNIX AD 服务器。

c. 选择绑定值。

- `-min-bind-level {anonymous|simple|sasl}` 指定最低绑定身份验证级别。

  默认值为 **`anonymous`**。

- `-bind-dn` *`LDAP_DN`* 指定绑定用户。

  对于 Active Directory 服务器，您必须在帐户（域 \ 用户）或主体（ user@domain.com ）表单中指定用户。否则，您必须以可分辨名称（ CN=user ， DC=domain ， DC=com ）形式指定用户。

- `-bind-password` *`password`* 指定绑定密码。

d. 如果需要，选择会话安全选项。

如果 LDAP 服务器需要，您可以启用 LDAP 签名和签章或基于 TLS 的 LDAP 。

- `--session-security {none|sign|seal}`

  您可以启用签名 (`sign`、数据完整性)、签名和签章 (`seal``数据完整性和加密)、或者两者都不是`none`，无签名或签章)。默认值为 `none`。

  您还应设置 `-min-bind-level {sasl}`，除非您希望绑定身份验证回退到 **`anonymous`** 或 **`simple`** 签名和签章绑定失败时。

- `-use-start-tls {true|false}`

  如果设置为 **`true`** 如果LDAP服务器支持此功能、则LDAP客户端将使用加密TLS连接连接到该服务器。默认值为 **`false`**。要使用此选项，您必须安装 LDAP 服务器的自签名根 CA 证书。

> 如果Storage VM已将SMB服务器添加到域中、并且LDAP服务器是SMB服务器主域的域控制器之一、则可以修改 `-session-security-for-ad-ldap` 选项 `vserver cifs security modify` 命令：

e. 选择端口，查询和基本值。

建议使用默认值，但您必须向 LDAP 管理员确认这些值适合您的环境。

- `-port` *`port`* 指定LDAP服务器端口。

  默认值为 `389`。

如果您计划使用 Start TLS 来保护 LDAP 连接，则必须使用默认端口 389 。启动 TLS 以 LDAP 默认端口 389 上的纯文本连接开头，然后该连接升级到 TLS 。如果更改此端口，则启动 TLS 将失败。

- `-query-timeout` *`integer`* 指定查询超时(以秒为单位)。

  允许的范围为 1 到 10 秒。默认值为 `3` 秒。

- `-base-dn` *`LDAP_DN`* 指定基础DN。

  如果需要，可以输入多个值（例如，如果启用了 LDAP 转介跟踪）。默认值为 `""` (root)。

- `-base-scope` {`base`|`onelevel`|`subtree`}指定基本搜索范围。

  默认值为 `subtree`。

- `-referral-enabled` {`true`|`false`}指定是否启用LDAP转介跟踪。

  从 ONTAP 9.5 开始，如果主 LDAP 服务器返回 LDAP 转介响应，指示转介的 LDAP 服务器上存在所需记录，则 ONTAP LDAP 客户端可以将查找请求转介给其他 LDAP 服务器。默认值为 **`false`**。

要搜索转介 LDAP 服务器中的记录，必须在 LDAP 客户端配置中将转介记录的基础 DN 添加到基础 DN 中。

2. 在Storage VM上创建LDAP客户端配置：

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```

> 创建LDAP客户端配置时、必须提供Storage VM名称。

3. 验证是否已成功创建 LDAP 客户端配置：

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

示例

以下命令将为Storage VM VS1创建一个名为ldap1的新LDAP客户端配置、以便与适用于LDAP的Active Directory服务器配合使用：

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

以下命令将为Storage VM VS1创建一个名为ldap1的新LDAP客户端配置、以便与需要签名和签章的LDAP的Active Directory服务器配合使用、并且LDAP服务器发现仅限于指定域的特定站点：

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

以下命令将为Storage VM VS1创建一个名为ldap1的新LDAP客户端配置、以便与需要LDAP转介跟踪的LDAP Active Directory服务器配合使用：

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

以下命令通过指定基础DN来修改Storage VM VS1的LDAP客户端配置ldap1：

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

以下命令通过启用转介跟踪来修改Storage VM VS1的LDAP客户端配置ldap1：

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

将 **LDAP** 客户端配置与 **SVM** 关联

要在SVM上启用LDAP、必须使用 `vserver services name-service ldap create` 命令将LDAP客户端配置与SVM关联。

您需要的内容

- LDAP 域必须已存在于网络中，并且必须可供 SVM 所在的集群访问。
- SVM 上必须存在 LDAP 客户端配置。

步骤

1. 在SVM上启用LDAP：

   `vserver services name-service ldap create -vserver` *`vserver_name`* `-client-config` *`client_config_name`*

   > 从ONTAP 9.2开始、 `vserver services name-service ldap create` 命令会执行自动配置验证、并在ONTAP无法联系名称服务器时报告错误消息。

   以下命令将在 vs1" SVM 上启用 LDAP ，并将其配置为使用 "ldap1" LDAP 客户端配置：

   ```
   cluster1::> vserver services name-service ldap create -vserver vs1
   -client-config ldap1 -client-enabled true
   ```

2. 使用 vserver services name-service ldap check 命令验证名称服务器的状态。

   以下命令将验证 SVM vs1. 上的 LDAP 服务器。

   ```
   cluster1::> vserver services name-service ldap check -vserver vs1

   | Vserver: vs1                                                |
   | Client Configuration Name: c1                               |
   | LDAP Status: up                                             |
   | LDAP Status Details: Successfully connected to LDAP server
   "10.11.12.13".                                              |
   ```

   从 ONTAP 9.2 开始，可以使用 name service check 命令。

在名称服务切换表中验证 **LDAP** 源

您必须验证 SVM 的名称服务切换表中是否正确列出了名称服务的 LDAP 源。

步骤

1. 显示当前名称服务切换表内容：

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

以下命令显示 SVM My_SVM 的结果：

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                  Source
Vserver         Database          Order
--------------- ------------      ---------
My_SVM          hosts             files,
                                  dns
My_SVM          group             files,ldap
My_SVM          passwd            files,ldap
My_SVM          netgroup          files
My_SVM          namemap           files
5 entries were displayed.
```

`namemap` 指定要搜索名称映射信息的源及其顺序。在纯 UNIX 环境中，不需要此条目。只有同时使用 UNIX 和 Windows 的混合环境才需要名称映射。

2. 更新 `ns-switch` 根据需要输入：

要更新 **ns-switch** 条目的项	输入命令 **...**
用户信息	`vserver services name-service ns-switch modify -vserver` *`vserver_name`* `-database passwd -sources ldap,files`
组信息	`vserver services name-service ns-switch modify -vserver` *`vserver_name`* `-database group -sources ldap,files`
网络组信息	`vserver services name-service ns-switch modify -vserver` *`vserver_name`* `-database netgroup -sources ldap,files`

将 **Kerberos** 与 **NFS** 结合使用可增强安全性

将 **Kerberos** 与 **NFS** 结合使用以增强安全性的概述

如果在您的环境中使用 Kerberos 进行强身份验证，则需要与 Kerberos 管理员一起确定要求和适当的存储系统配置，然后将 SVM 作为 Kerberos 客户端启用。

您的环境应符合以下准则：

- 在为 ONTAP 配置 Kerberos 之前，您的站点部署应遵循 Kerberos 服务器和客户端配置的最佳实践。
- 如果需要 Kerberos 身份验证，请尽可能使用 NFSv4 或更高版本。

  NFSv3 可与 Kerberos 结合使用。但是，只有在 NFSv4 或更高版本的 ONTAP 部署中，才会充分发挥

Kerberos 的全部安全优势。

- 要提高冗余服务器访问能力，应在使用同一 SPN 的集群中多个节点上的多个数据 LIF 上启用 Kerberos 。
- 在 SVM 上启用 Kerberos 时，必须根据 NFS 客户端配置在卷或 qtree 的导出规则中指定以下安全方法之一。
  - `krb5` (Kerberos v5协议)
  - `krb5i` (使用校验和进行完整性检查的Kerberos v5协议)
  - `krb5p` (具有隐私服务的Kerberos v5协议)

除了 Kerberos 服务器和客户端之外，还必须为 ONTAP 配置以下外部服务以支持 Kerberos ：

- 目录服务

  您应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 。请勿使用 NIS ，因为其请求会以明文形式发送，因此不安全。

- 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。

验证 **Kerberos** 配置的权限

Kerberos 要求为 SVM 根卷以及本地用户和组设置某些 UNIX 权限。

步骤

1. 显示 SVM 根卷上的相关权限：

   `volume show -volume` *`root_vol_name`*`-fields user,group,unix-permissions`

   SVM 的根卷必须具有以下配置：

名称	正在设置 ...
UID	root 或 ID 0
GID	root 或 ID 0
UNIX 权限	755

   如果未显示这些值、请使用 `volume modify` 命令进行更新。

2. 显示本地 UNIX 用户：

```
vserver services name-service unix-user show -vserver vserver_name
```

SVM 必须配置以下 UNIX 用户：

用户名	用户 **ID**	主组 **ID**	**comment**
NFS	500	0	GSS 初始化阶段需要此项。 NFS 客户端用户 SPN 的第一个组件用作用户。 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。
root	0	0	挂载时需要。

如果未显示这些值、则可以使用 `vserver services name-service unix-user modify` 命令进行更新。

3. 显示本地 UNIX 组：

```
vserver services name-service unix-group show -vserver vserver _name
```

SVM 必须配置以下 UNIX 组：

组名称	组 **ID**
守护进程	1.
root	0

如果未显示这些值、则可以使用 `vserver services name-service unix-group modify` 命令进行更新。

创建 **NFS Kerberos** 域配置

如果您希望 ONTAP 访问环境中的外部 Kerberos 服务器，则必须先将 SVM 配置为使用现有 Kerberos 域。为此、您需要收集Kerberos KDC服务器的配置值、然后使用 `vserver nfs kerberos realm create` 命令以在SVM上创建Kerberos域配置。

您需要的内容

集群管理员应已在存储系统，客户端和 KDC 服务器上配置 NTP ，以避免出现身份验证问题。客户端和服务器之间的时间差异（时钟偏差）是常见的身份验证失败发生原因。

步骤

1. 请咨询Kerberos管理员以确定要为提供的适当配置值 `vserver nfs kerberos realm create` 命令：
2. 在 SVM 上创建 Kerberos 域配置：

   ```
   vserver nfs kerberos realm create -vserver vserver_name -realm realm_name
   {AD_KDC_server_values |AD_KDC_server_values} -comment "text"
   ```

3. 验证是否已成功创建 Kerberos 域配置：

   ```
   vserver nfs kerberos realm show
   ```

示例

以下命令将为 SVM vs1 创建一个 NFS Kerberos 域配置，该配置使用 Microsoft Active Directory 服务器作为 KDC 服务器。Kerberos 域为 AUTH.EXAMPLE.COM 。Active Directory 服务器名为 AD-1 ，其 IP 地址为 10.10.8.14 。允许的时钟偏差为 300 秒（默认值）。KDC 服务器的 IP 地址为 10.10.8.14 ，其端口号为 88 （默认值）。"Microsoft Kerberos config" 是注释。

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

以下命令将为使用 MIT KDC 的 SVM vs1 创建 NFS Kerberos 域配置。Kerberos 域为 SECURITY.EXAMPLE.COM 。允许的时钟偏差为 300 秒。KDC 服务器的 IP 地址为 10.10.9.1 ，端口号为 88 。KDC 供应商为 "Other" ，表示 UNIX 供应商。管理服务器的 IP 地址为 10.10.9.1 ，端口号为 749 （默认值）。密码服务器的 IP 地址为 10.10.9.1 ，端口号为 464 （默认值）。"UNIX Kerberos config" 是注释。

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

配置 **NFS Kerberos** 允许的加密类型

默认情况下， ONTAP 支持以下 NFS Kerberos 加密类型： DES ， 3DES ， AES-128 和 AES-256 。您可以使用为每个SVM配置允许的加密类型、以满足特定环境的安全要求 `vserver nfs modify` 命令 `-permitted-enc-types` 参数。

关于此任务

为了最大程度地实现客户端兼容性， ONTAP 默认同时支持弱 DES 和强 AES 加密。例如，这意味着，如果您要提高安全性，并且您的环境支持此安全性，则可以使用此操作步骤禁用 DES 和 3DES ，并要求客户端仅使用 AES 加密。

您应使用可用的最强加密。对于 ONTAP ，即 AES-256 。您应向 KDC 管理员确认您的环境支持此加密级别。

- 在 SVM 上完全启用或禁用 AES （AES-128 和 AES-256 ）会造成中断，因为它会销毁原始 DES 主体 /keytab 文件，从而要求在 SVM 的所有 LIF 上禁用 Kerberos 配置。

  在进行此更改之前，您应验证 NFS 客户端是否不依赖于 SVM 上的 AES 加密。

- 启用或禁用 DES 或 3DES 不需要对 LIF 上的 Kerberos 配置进行任何更改。

步骤

1. 启用或禁用所需的允许加密类型：

要启用或禁用的项	请按照以下步骤操作 ...
DES 或 3DES	a. 配置SVM的NFS Kerberos允许的加密类型： `vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`* 使用逗号分隔多种加密类型。 b. 验证更改是否成功： `vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`

AES-128或AES-256	a. 确定启用了Kerberos的SVM和LIF：
	`vserver nfs kerberos interface show`
	
	b. 在要修改NFS Kerberos允许的加密类型的SVM上的所有SVM上禁用Kerberos：
	`vserver nfs kerberos interface disable -lif` *`lif_name`*
	
	c. 配置SVM的NFS Kerberos允许的加密类型：
	`vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`*
	
	使用逗号分隔多种加密类型。
	
	d. 验证更改是否成功：
	`vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`
	
	e. 在SVM上的所有SVM上重新启用Kerberos：
	`vserver nfs kerberos interface enable -lif` *`lif_name`* `-spn` *`service_principal_name`*
	
	f. 验证是否已在所有生命周期管理器上启用Kerberos：
	`vserver nfs kerberos interface show`

在数据 **LIF** 上启用 **Kerberos**

您可以使用 `vserver nfs kerberos interface enable` 命令以对数据LIF启用Kerberos。这样， SVM 就可以对 NFS 使用 Kerberos 安全服务。

关于此任务

如果您使用的是 Active Directory KDC ，则所使用的任何 SPN 的前 15 个字符必须在域或域中的 SVM 之间是唯一的。

步骤

1. 创建 NFS Kerberos 配置：

   ```
   vserver nfs kerberos interface enable -vserver vserver_name -lif
   logical_interface -spn service_principal_name
   ```

   ONTAP 需要 KDC 中 SPN 的机密密钥才能启用 Kerberos 接口。

   对于 Microsoft KDC ，将联系 KDC ，并在命令行界面上发出用户名和密码提示以获取机密密钥。如果需要在Kerberos域的其他OU中创建SPN、则可以指定可选 `-ou` 参数。

   对于非 Microsoft KDC ，可以使用以下两种方法之一获取机密密钥：

如果您 ...	您还必须在命令中包含以下参数 ...
拥有 KDC 管理员凭据，以便直接从 KDC 检索密钥	`-admin-username` *kdc_admin_username*
没有 KDC 管理员凭据，但具有包含此密钥的 KDC 中的 keytab 文件	`-keytab-uri` {ftp-http} ：//*uri*

2. 验证是否已在 LIF 上启用 Kerberos ：

   ```
   vserver nfs kerberos-config show
   ```

3. 重复步骤 1 和 2 ，在多个 LIF 上启用 Kerberos 。

示例

以下命令将在逻辑接口 ves03-d1 上为名为 vs1 的 SVM 创建并验证 NFS Kerberos 配置，并在 OU lab2ou 中使用 SPN NFS/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM ：

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
        Logical
Vserver Interface Address       Kerberos  SPN
------- --------- -------       --------- -------------------------------
vs0     ves01-a1
                  10.10.10.30   disabled  -
vs2     ves01-d1
                  10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

向启用了 NFS 的 SVM 添加存储容量

将存储容量添加到启用了 NFS 的 SVM 概述中

要向启用了 NFS 的 SVM 添加存储容量，必须创建一个卷或 qtree 以提供存储容器，并为此容器创建或修改导出策略。然后，您可以从集群验证 NFS 客户端访问，并测试客户端系统的访问。

您需要的内容

- 必须在 SVM 上完全设置 NFS 。
- SVM 根卷的默认导出策略必须包含允许访问所有客户端的规则。
- 必须完成对名称服务配置的所有更新。
- 必须完成对 Kerberos 配置的任何添加或修改。

创建导出策略

在创建导出规则之前，您必须创建一个导出策略来存放这些规则。您可以使用 `vserver export-policy create` 命令以创建导出策略。

步骤

1. 创建导出策略

   `vserver export-policy create -vserver` *`vserver_name`* `-policyname` *`policy_name`*

   策略名称最长可为 256 个字符。

2. 验证是否已创建导出策略：

   `vserver export-policy show -policyname` *`policy_name`*

示例

以下命令将在名为 vs1 的 SVM 上创建并验证是否已创建名为 exp1 的导出策略：

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
---------------  -------------------
vs1              exp1
```

向导出策略添加规则

如果没有规则，导出策略将无法提供客户端对数据的访问。要创建新的导出规则，您必须标识客户端并选择客户端匹配格式，选择访问和安全类型，指定匿名用户 ID 映射，选择规则索引编号，然后选择访问协议。然后、您可以使用 `vserver export-policy rule create` 命令将新规则添加到导出策略中。

您需要的内容

- 要添加导出规则的导出策略必须已存在。
- 必须在数据 SVM 上正确配置 DNS ，并且 DNS 服务器必须具有适用于 NFS 客户端的正确条目。

  这是因为 ONTAP 使用数据 SVM 的 DNS 配置对某些客户端匹配格式执行 DNS 查找，如果导出策略规则匹配失败，则可能会阻止客户端数据访问。

- 如果您要使用 Kerberos 进行身份验证，则必须已确定 NFS 客户端使用以下哪种安全方法：
  - `krb5` (Kerberos V5协议)
  - `krb5i` (使用校验和进行完整性检查的Kerberos V5协议)
  - `krb5p` (具有隐私服务的Kerberos V5协议)

关于此任务

如果导出策略中的现有规则满足客户端匹配和访问要求，则无需创建新规则。

如果要使用Kerberos进行身份验证、并且SVM的所有卷都通过Kerberos进行访问、则可以设置导出规则选项 `-rorule`， `-rwrule`，和 `-superuser` 根卷的 `krb5`， `krb5i``或 `krb5p`。

步骤

1. 确定新规则的客户端和客户端匹配格式。

   。 `-clientmatch` option用于指定应用此规则的客户端。可以指定一个或多个客户端匹配值；多个值的规范必须用逗号分隔。您可以使用以下任意格式指定匹配项：

客户端匹配格式	示例
域名前面带有 "." 字符	`.example.com` 或 `.example.com,.example.net,...`
主机名	`host1` 或 `host1,host2, ...`
IPv4 地址	`10.1.12.24` 或 `10.1.12.24,10.1.12.25, ...`
IPv4 地址，子网掩码以位数表示	`10.1.12.10/4` 或 `10.1.12.10/4,10.1.12.11/4,...`
带有网络掩码的 IPv4 地址	`10.1.16.0/255.255.255.0` 或 `10.1.16.0/255.255.255.0,10.1.17.0/255.255.255.0,...`
点格式的 IPv6 地址	`::1.2.3.4` 或 `::1.2.3.4,::1.2.3.5,...`
IPv6地址、子网掩码以位数表示	`ff::00/32` 或 `ff::00/32,ff::01/32,...`
一个网络组，其网络组名称前面带有 @ 字符	`@netgroup1` 或 `@netgroup1,@netgroup2,...`

您还可以组合使用各种类型的客户端定义、例如、 `.example.com,@netgroup1`。

指定 IP 地址时，请注意以下事项：

- 不允许输入 IP 地址范围，例如 10.1.12.10-10.1.12.70 。

  此格式的条目将被解释为文本字符串，并被视为主机名。

- 在导出规则中指定单个 IP 地址以精细管理客户端访问时，请勿指定动态分配（例如 DHCP ）或临时分配（例如 IPv6 ）的 IP 地址。

  否则，当客户端的 IP 地址发生更改时，客户端将失去访问权限。

- 不允许输入带有网络掩码的 IPv6 地址，例如 ff： 12/ff：： 00 。

2. 为客户端匹配选择访问和安全类型。

   您可以为使用指定安全类型进行身份验证的客户端指定以下一种或多种访问模式：

   - `-rorule` (只读访问)
   - `-rwrule` (读写访问)
   - `-superuser` (root访问权限)

> 只有当导出规则也允许对特定安全类型进行只读访问时，客户端才能获得该安全类型的读写访问权限。如果只读参数对于安全类型的限制性比读写参数更强，则客户端可能无法获得读写访问权限。超级用户访问也是如此。

您可以为一个规则指定多种安全类型的逗号分隔列表。将安全类型指定为 `any` 或 `never`，请勿指定任何其他安全类型。从以下有效安全类型中进行选择：

当安全类型设置为 ...	匹配的客户端可以访问导出的数据 ...
`any`	始终，无论传入的安全类型如何。
`none`	如果单独列出，则具有任何安全类型的客户端将被授予匿名访问权限。如果与其他安全类型一起列出，则具有指定安全类型的客户端将被授予访问权限，而具有任何其他安全类型的客户端将被授予匿名访问权限。
`never`	从不，无论传入的安全类型如何。
`krb5`	如果通过 Kerberos 5 进行身份验证。 仅身份验证：每个请求和响应的标头都已签名。
`krb5i`	如果通过 Kerberos 5i 进行身份验证。 身份验证和完整性：每个请求和响应的标头和正文均已签名。
`krb5p`	如果使用Kerberos 5p进行身份验证。 身份验证，完整性和隐私：对每个请求和响应的标题和正文进行签名，并对 NFS 数据有效负载进行加密。
`ntlm`	如果通过 CIFS NTLM 进行身份验证。
`sys`	如果通过 NFS AUTH_SYS 进行身份验证。

建议的安全类型为 `sys`或者，如果使用`Kerberos`， `krb5`， `krb5i`或 `krb5p`。

如果要将Kerberos与NFSv3结合使用、则导出策略规则必须允许 `-rorule` 和 `-rwrule` 访问 `sys` 除了 `krb5`。这是因为需要允许 Network Lock Manager （ NLM ）访问导出。

3. 指定匿名用户 ID 映射。

   。 `-anon` option用于指定映射到用户ID为0 (零)的客户端请求的UNIX用户ID或用户名、此用户ID或用户名通常与用户名root相关联。默认值为 `65534`。NFS 客户端通常会将用户 ID 65534 与用户名 nobody 相关联（也称为 *root squash* ）。在 ONTAP 中，此用户 ID 与用户 pcuser 关联。要禁止用户ID为0的任何客户端访问、请指定值 `65535`。

4. 选择规则索引顺序。

   。 `-ruleindex` option用于指定规则的索引编号。规则将根据其在索引编号列表中的顺序进行评估；索引编

号较低的规则将首先进行评估。例如，索引编号为 1 的规则会在索引编号为 2 的规则之前进行评估。

如果要添加 ...	那么 ...
导出策略的第一个规则	输入 ... `1`。
导出策略的其他规则	a. 显示策略中的现有规则： `vserver export-policy rule show -instance -policyname` *`your_policy`* b. 根据新规则的评估顺序为其选择索引编号。

5. 选择适用的NFS访问值：{`nfs`|`nfs3`|`nfs4`} 。

   `nfs` 匹配任何版本、 `nfs3` 和 `nfs4` 仅匹配这些特定版本。

6. 创建导出规则并将其添加到现有导出策略：

   `vserver export-policy rule create -vserver` *`vserver_name`* `-policyname` *`policy_name`* `-ruleindex` *`integer`* `-protocol {nfs|nfs3|nfs4} -clientmatch { text |` *`"text,text,…"`* `} -rorule` *`security_type`* `-rwrule` *`security_type`* `-superuser` *`security_type`* `-anon` *`user_ID`*

7. 显示导出策略的规则以验证新规则是否存在：

   `vserver export-policy rule show -policyname` *`policy_name`*

   命令将显示该导出策略的摘要，包括应用于该策略的规则列表。ONTAP 会为每个规则分配一个规则索引编号。知道规则索引编号后，您可以使用它显示有关指定导出规则的详细信息。

8. 验证是否已正确配置应用于导出策略的规则：

   `vserver export-policy rule show -policyname` *`policy_name`* `-vserver` *`vserver_name`* `-ruleindex` *`integer`*

示例

以下命令将在名为 RS1 的导出策略中的 SVM vs1 上创建导出规则并验证此创建过程。此规则的索引编号为 1 。此规则与域 eng.company.com 和 netgroup @netgroup1 中的任何客户端匹配。此规则将启用所有 NFS 访问。它允许使用 AUTH_SYS 进行身份验证的用户进行只读和读写访问。除非使用 Kerberos 进行身份验证，否则使用 UNIX 用户 ID 0 （零）的客户端将被匿名化。

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname exp1
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5

vs1::> vserver export-policy rule show -policyname nfs_policy
Virtual      Policy         Rule    Access    Client           RO
Server       Name           Index   Protocol  Match            Rule
------------ -------------- ------  --------  ---------------- ------
vs1          exp1           1       nfs       eng.company.com, sys
                                               @netgroup1

vs1::> vserver export-policy rule show -policyname exp1 -vserver vs1
-ruleindex 1

                                     Vserver: vs1
                                 Policy Name: exp1
                                  Rule Index: 1
                             Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
                              RO Access Rule: sys
                              RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
                    Superuser Security Types: krb5
                Honor SetUID Bits in SETATTR: true
                   Allow Creation of Devices: true
```

以下命令将在名为 expol2 的导出策略中的 SVM vs2 上创建导出规则并验证此创建过程。此规则的索引编号为21。此规则会将客户端与网络组 dev_netgroup_main 中的成员匹配。此规则将启用所有 NFS 访问。它允许使用 AUTH_SYS 进行身份验证的用户进行只读访问，并要求对读写和 root 访问进行 Kerberos 身份验证。除非使用 Kerberos 进行身份验证，否则使用 UNIX 用户 ID 0 （零）的客户端将被拒绝进行 root 访问。

```
vs2::> vserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5

vs2::> vserver export-policy rule show -policyname nfs_policy
Virtual   Policy       Rule    Access    Client               RO
Server    Name         Index   Protocol  Match                Rule
-------- ------------ ------  --------  ------------------   ------
vs2       expol2       21       nfs      @dev_netgroup_main   sys

vs2::> vserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21

                                   Vserver: vs2
                               Policy Name: expol2
                                Rule Index: 21
                            Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
                                            @dev_netgroup_main
                             RO Access Rule: sys
                             RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
                    Superuser Security Types: krb5
                Honor SetUID Bits in SETATTR: true
                   Allow Creation of Devices: true
```

创建卷或 qtree 存储容器

创建卷

您可以使用创建卷并指定其接合点和其他属性 `volume create` 命令：

关于此任务

卷必须包含 *junction path* ，才能使其数据可供客户端使用。您可以在创建新卷时指定接合路径。如果在创建卷时未指定接合路径、则必须使用_mount_在SVM命名空间中挂载此卷 `volume mount` 命令：

开始之前

- 应设置并运行NFS。
- SVM安全模式必须为UNIX。
- 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. 创建具有接合点的卷：

   `volume create -vserver svm_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number -group group_name_or_number -junction-path junction_path [-policy export_policy_name]`

   的选项 `-junction-path` 包括：

   - 直接位于root下、例如、 `/new_vol`

     您可以创建一个新卷并指定将其直接挂载到 SVM 根卷。

   - 在现有目录下、例如、 `/existing_dir/new_vol`

     您可以创建一个新卷并指定将其挂载到现有层次结构中的现有卷，以目录的形式表示。

     例如、如果要在新目录(在新卷下的新层次结构中)中创建卷、 `/new_dir/new_vol` 然后，必须先创建一个与SVM根卷连接的新父卷。然后，您将在新父卷的接合路径（新目录）中创建新的子卷。

     如果您计划使用现有导出策略、则可以在创建卷时指定此策略。您也可以稍后使用添加导出策略 `volume modify` 命令：

2. 验证是否已使用所需的接合点创建卷：

   `volume show -vserver svm_name -volume volume_name -junction`

示例

以下命令将在 SVM vs1.example.com 和聚合 aggr1 上创建一个名为 users1 的新卷。新卷可通过访问 `/users`。此卷的大小为 750 GB ，其卷保证类型为 volume （默认值）。

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                          Junction                 Junction
Vserver           Volume  Active   Junction Path   Path Source
----------------- ------- -------- --------------- -----------
vs1.example.com   users1  true     /users          RW_volume
```

以下命令会在 SVM vs1.example.com 和聚合 "aggr1" 上创建一个名为 "home4" 的新卷。目录 `/eng/` 已位于VS1 SVM的命名空间中、新卷可通过访问 `/eng/home`，将成为的主目录 `/eng/` 命名空间。此卷的大小为750 GB、其卷保证类型为 `volume` (默认情况下)。

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

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

创建 **qtree**

您可以使用创建一个qtree以包含您的数据、并指定其属性 `volume qtree create` 命令：

您需要的内容

- 要包含新 qtree 的 SVM 和卷必须已存在。
- SVM 安全模式必须为 UNIX ，并且 NFS 应设置并运行。

步骤

1. 创建 qtree：

   `volume qtree create -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `} -security-style unix [-policy` *`export_policy_name`*`]`

   您可以将卷和qtree指定为单独的参数、也可以采用格式指定qtree路径参数 `/vol/`*`volume_name`*`/`*`_qtree_name`*。

   默认情况下， qtree 会继承其父卷的导出策略，但可以将其配置为使用自己的导出策略。如果您计划使用现有导出策略，则可以在创建 qtree 时指定该策略。您也可以稍后使用添加导出策略 `volume qtree modify` 命令：

2. 验证是否已使用所需的接合路径创建 qtree：

   `volume qtree show -vserver` *`vserver_name`* `{ -volume` *`volume_name`* `-qtree` *`qtree_name`* `| -qtree-path` *`qtree path`* `}`

示例

以下示例将在SVM vs1.example.com上创建一个名为qt01的qtree、此qtree具有接合路径 `/vol/data1`：

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style unix
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                    Security Style: unix
                       Oplock Mode: enable
                  Unix Permissions: ---rwxr-xr-x
                           Qtree Id: 2
                      Qtree Status: normal
                     Export Policy: default
        Is Export Policy Inherited: true
```

使用导出策略确保 NFS 访问安全

使用导出策略确保 NFS 访问安全

您可以使用导出策略将对卷或 qtree 的 NFS 访问限制为与特定参数匹配的客户端。配置新存储时，您可以使用现有策略和规则，向现有策略添加规则或创建新策略和规则。您还可以检查导出策略的配置

> 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验证配置并从策略中删除错误的规则。这些命令仅验证主机名、网络组和匿名用户的导出配置。

管理导出规则的处理顺序

您可以使用 `vserver export-policy rule setindex` 命令以手动设置现有导出规则的索引编号。这样，您可以指定 ONTAP 将导出规则应用于客户端请求的优先级。

关于此任务

如果新索引编号已在使用中，则该命令会在指定位置插入规则并相应地对列表重新排序。

步骤

1. 修改指定导出规则的索引编号：

   `vserver export-policy rule setindex -vserver` *`virtual_server_name`* `-policyname` *`policy_name`* `-ruleindex` *`integer`* `-newruleindex` *`integer`*

示例

以下命令会将 SVM vs1 上名为 RS1 的导出策略中索引编号为 3 的导出规则的索引编号更改为 2：

```
vs1::> vserver export-policy rule setindex -vserver vs1
-policyname rs1 -ruleindex 3 -newruleindex 2
```

为卷分配导出策略

SVM 中包含的每个卷都必须与一个导出策略相关联，该导出策略包含导出规则，客户端可以通过这些规则访问卷中的数据。

关于此任务

您可以在创建卷时或创建卷后随时将导出策略与卷关联。您可以将一个导出策略与卷关联，但一个策略可以与多个卷关联。

步骤

1. 如果在创建卷时未指定导出策略，请为此卷分配一个导出策略：

   ```
   volume modify -vserver vserver_name -volume volume_name -policy
   export_policy_name
   ```

2. 验证是否已将此策略分配给卷：

   ```
   volume show -volume volume_name -fields policy
   ```

示例

以下命令会将导出策略 nfs_policy 分配给 SVM vs1 上的卷 vol1 并验证分配情况：

```
cluster::> volume modify -v1server vs1 -volume vol1 -policy nfs_policy

cluster::>volume show -volume vol -fields policy
vserver volume       policy
------- ------------ ----------------
vs1     vol1         nfs_policy
```

为 **qtree** 分配导出策略

您还可以导出卷上的特定 qtree ，使其可供客户端直接访问，而不是导出整个卷。您可以通过为 qtree 分配导出策略来导出 qtree 。您可以在创建新 qtree 时分配导出策略，也可以通过修改现有 qtree 来分配导出策略。

您需要的内容

导出策略必须存在。

关于此任务

默认情况下，如果在创建时未另行指定， qtree 将继承包含卷的父导出策略。

您可以在创建 qtree 时或在创建 qtree 之后随时将导出策略与 qtree 相关联。您可以将一个导出策略与 qtree 关联，但一个策略可以与多个 qtree 关联。

步骤

1. 如果在创建 qtree 时未指定导出策略，请为此 qtree 分配一个导出策略：

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

2. 验证是否已将此策略分配给 qtree：

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

示例

以下命令会将导出策略 nfs_policy 分配给 SVM vs1 上的 qtree qt1 并验证分配情况：

```
cluster::> volume modify -v1server vs1 -qtree-path /vol/vol1/qt1 -policy
nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
------- ------ ----- -------------
vs1     data1  qt01  nfs_policy
```

从集群验证 NFS 客户端访问

您可以通过在 UNIX 管理主机上设置 UNIX 文件权限来为选定客户端授予对共享的访问权限。您可以使用检查客户端访问 `vserver export-policy check-access` 命令、根据需要调整导出规则。

步骤

1. 在集群上、使用检查客户端对导出的访问权限 `vserver export-policy check-access` 命令：

   以下命令将检查 IP 地址为 1.2.3.4 的 NFSv3 客户端对卷 Home2 的读 / 写访问权限。命令输出显示卷使用导出策略 `exp-home-dir` 而且访问被拒绝。

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
-type read-write
                                          Policy    Policy     Rule
Path                     Policy           Owner     Owner Type Index  Access
------------------------ ------------- --------- ---------- ------
----------
/                        default       vs1_root  volume          1 read
/eng                     default       vs1_root  volume          1 read
/eng/home2               exp-home-dir  home2     volume          1 denied

3 entries were displayed.
```

2. 检查输出以确定导出策略是否按预期工作以及客户端访问是否按预期进行。

   具体而言，您应验证卷或 qtree 使用的导出策略以及客户端因此具有的访问类型。

3. 如有必要，请重新配置导出策略规则。

测试客户端系统的 NFS 访问

在验证对新存储对象的 NFS 访问之后，您应登录到 NFS 管理主机并从 SVM 读取数据并向 SVM 写入数据来测试配置。然后，您应在客户端系统上以非 root 用户身份重复此过程。

您需要的内容

- 客户端系统必须具有先前指定的导出规则允许的 IP 地址。
- 您必须具有 root 用户的登录信息。

步骤

1. 在集群上，验证托管新卷的 LIF 的 IP 地址：

   `network interface show –vserver svm_name`

2. 以 root 用户身份登录到管理主机客户端系统。
3. 将目录更改为挂载文件夹：

   `cd /mnt/`

4. 使用 SVM 的 IP 地址创建并挂载新文件夹：

   a. 创建新文件夹：
      `mkdir /mnt/folder`

   b. 将新卷挂载到此新目录：
      `mount -t nfs -o hard IPAddress:/volume_name /mnt/folder`

c. 将目录更改为新文件夹：
   `cd folder`

   以下命令将创建一个名为 test1 的文件夹，并在 test1 挂载文件夹的 192.0.2.130 IP 地址处挂载 vol1 卷，然后更改为新的 test1 目录：

```
host# mkdir /mnt/test1
host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. 创建一个新文件，验证该文件是否存在并向其写入文本：

   a. 创建测试文件：
      `touch filename`

   b. 验证文件是否存在：
      `ls -l filename`

   c. 输入 ...
      `cat > filename`

      键入一些文本，然后按 Ctrl+D 将文本写入测试文件。

   d. 显示测试文件的内容。
      `cat filename`

   e. 删除测试文件：
      `rm filename`

   f. 返回到父目录：
      `cd ..`

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. 以 root 用户身份，在挂载的卷上设置所需的任何 UNIX 所有权和权限。

7. 在导出规则中标识的 UNIX 客户端系统上，以现在有权访问新卷的授权用户之一身份登录，然后重复步骤 3 至 5 中的过程，以验证是否可以挂载卷并创建文件。

从何处查找追加信息

成功测试 NFS 客户端访问后，您可以执行其他 NFS 配置或添加 SAN 访问。协议访问完成后，您应保护 Storage Virtual Machine （ SVM ）的根卷。

NFS配置

您可以使用以下信息和技术报告进一步配置 NFS 访问：

- "NFS 管理"

  介绍如何使用 NFS 配置和管理文件访问。

- "NetApp 技术报告 4067 ：《 NFS 最佳实践和实施指南》"

  可作为 NFSv3 和 NFSv4 操作指南，简要介绍 ONTAP 操作系统，重点介绍 NFSv4 。

- "NetApp 技术报告 4073 ：《安全统一身份验证》"

  介绍如何将 ONTAP 配置为与基于 UNIX 的 Kerberos 版本 5 （ krb5 ）服务器结合使用以进行 NFS 存储身份验证，并将 Windows Server Active Directory （ AD ）配置为 KDC 和轻量级目录访问协议（ LDAP ）身份提供程序。

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

  介绍在连接到运行 ONTAP 的系统的 AIX ， Linux 或 Solaris 客户端上实施 NFSv4 组件时应遵循的最佳实践。

网络配置

您可以使用以下信息和技术报告进一步配置网络功能和名称服务：

- "NFS 管理"

  介绍如何配置和管理 ONTAP 网络。

- "NetApp 技术报告 4182 ：《集群模式 Data ONTAP 配置的以太网存储设计注意事项和最佳实践》"

  介绍 ONTAP 网络配置的实施，并提供常见网络部署场景和最佳实践建议。

- "NetApp 技术报告 4668 ：《名称服务最佳实践指南》"

  介绍如何配置 LDAP ， NIS ， DNS 和本地文件配置以进行身份验证。

SAN 协议配置

如果要提供或修改对新 SVM 的 SAN 访问，可以使用 FC 或 iSCSI 配置信息，此信息可用于多个主机操作系统。

根卷保护

在 SVM 上配置协议后，您应确保其根卷受到保护：

- "数据保护"

  介绍如何创建负载共享镜像以保护 SVM 根卷，这是适用于已启用 NAS 的 SVM 的 NetApp 最佳实践。此外，还介绍如何通过从负载共享镜像提升 SVM 根卷来快速从卷故障或丢失中恢复。

ONTAP 导出与 7- 模式导出有何不同

ONTAP 导出与 7- 模式导出有何不同

如果您不熟悉ONTAP如何实施NFS导出、可以比较7-模式和ONTAP导出配置工具以及7-模式示例 `/etc/exports` 具有集群模式策略和规则的文件。

在ONTAP中、没有 `/etc/exports` file和no `exportfs` 命令：而是必须定义导出策略。通过导出策略，您可以像在 7- 模式中一样控制客户端访问，但也可以提供其他功能，例如可以对多个卷重复使用相同的导出策略。

相关信息

"NFS 管理"

"NetApp 技术报告 4067 ：《 NFS 最佳实践和实施指南》"

7- 模式和 ONTAP 中的导出比较

ONTAP 中的导出定义和使用方式与 7- 模式环境中不同。

不同之处	7- 模式	ONTAP
如何定义导出	导出在中进行定义 `/etc/exports` 文件	导出可通过在 SVM 中创建导出策略来定义。一个 SVM 可以包含多个导出策略。
导出范围	• 导出将应用于指定的文件路径或 qtree 。 • 您必须在中创建单独的条目 `/etc/exports` 对于每个文件路径或qtree。 • 只有在中定义导出后、这些导出才会持久保留 `/etc/exports` 文件	• 导出策略适用于整个卷，包括卷中包含的所有文件路径和 qtree 。 • 如果需要，可以将导出策略应用于多个卷。 • 所有导出策略都会在系统重新启动后保持不变。

隔离（为特定客户端指定对相同资源的不同访问权限）	要为特定客户端提供对单个导出资源的不同访问权限、必须在中列出每个客户端及其允许的访问权限 `/etc/exports` 文件	导出策略由多个单独的导出规则组成。每个导出规则都定义资源的特定访问权限，并列出具有这些权限的客户端。要为特定客户端指定不同的访问权限，您必须为每组特定访问权限创建一个导出规则，列出具有这些权限的客户端，然后将这些规则添加到导出策略中。
名称别名	定义导出时，您可以选择使导出名称与文件路径名称不同。您应使用 `-actual` 参数 `/etc/exports` 文件	您可以选择使导出卷的名称与实际卷名称不同。为此、您必须在SVM命名空间中使用自定义接合路径名称挂载卷。 默认情况下，卷会使用其卷名称进行挂载。要自定义卷的接合路径名称，您需要将其卸载，重命名并重新挂载。

ONTAP 导出策略示例

您可以查看导出策略示例，以更好地了解导出策略在 ONTAP 中的工作原理。

7- 模式导出的 ONTAP 实施示例

以下示例显示了中显示的7-模式导出 `/etc/export` 文件：

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

要将此导出复制为集群模式导出策略，您必须创建一个包含三个导出规则的导出策略，然后将此导出策略分配给卷 vol1 。

规则	Element	价值
规则 1.	`-clientmatch` (客户端规范)	`@readonly_netgroup`
`-ruleindex`(导出规则在规则列表中的位置)	`1`	`-protocol`
`nfs`	`-rorule`(允许只读访问)	`sys` (客户端使用AUTH _ SYS进行身份验证)
`-rwrule`(允许读写访问)	`never`	`-superuser`(允许超级用户访问)

规则	Element	价值
none(root用户_squ希_到anon)	第2条	-clientmatch
@rootaccess_netgroup	-ruleindex	2
-protocol	nfs	-rorule
sys	-rwrule	sys
-superuser	sys	第3条
-clientmatch	@readwrite_netgroup1,@readwrite_netgroup2	-ruleindex
3	-protocol	nfs
-rorule	sys	-rwrule
sys	-superuser	none

1. 创建名为 exp_vol1 的导出策略：

```
vserver export-policy create -vserver NewSVM -policyname exp_vol1
```

2. 在基本命令中使用以下参数创建三个规则：
   - 基本命令：
     `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1`
   - 规则参数：
     ```
     -clientmatch @readonly_netgroup -ruleindex 1 -protocol nfs -rorule sys
     -rwrule never -superuser none
     -clientmatch @rootaccess_netgroup -ruleindex 2 -protocol nfs -rorule sys
     -rwrule sys -superuser sys
     -clientmatch @readwrite_netgroup1,@readwrite_netgroup2 -ruleindex 3
     -protocol nfs -rorule sys -rwrule sys -superuser none
     ```
3. 将此策略分配给卷 vol1 ：

```
volume modify -vserver NewSVM -volume vol1 -policy exp_vol1
```

7- 模式导出的整合示例

以下示例显示了7-模式 `/etc/export` 文件、其中每一行对应10个qtrees：

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```

在ONTAP中、每个qtree需要两个策略之一：一个策略包含一个规则 `-clientmatch host1519s`，或包含规则的 `-clientmatch host2057s`。

1. 创建两个名为 exp_vol1q1 和 exp_vol1q2 的导出策略：
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q1`
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q2`
2. 为每个策略创建一个规则：
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q1 -clientmatch host1519s -rwrule sys -superuser sys`
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q2 -clientmatch host1519s -rwrule sys -superuser sys`
3. 将策略应用于 qtree：
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_1472 -export -policy exp_vol1q1`
   - [接下来的 4 个 qtree…]
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_2237 -export -policy exp_vol1q2`
   - [接下来的 4 个 qtree…]

如果稍后需要为这些主机添加其他 qtree ，则可以使用相同的导出策略。