



配置对 **SVM** 的 **NFS** 访问

ONTAP 9

NetApp
April 24, 2024

目录

- 配置对 SVM 的 NFS 访问..... 1
 - 创建 SVM : 1
 - 验证是否已在 SVM 上启用 NFS 协议..... 2
 - 打开 SVM 根卷的导出策略..... 3
 - 创建 NFS 服务器 4
 - 创建 LIF 6
 - 启用 DNS 以进行主机名解析 9
 - 配置名称服务 11
 - 将 Kerberos 与 NFS 结合使用可增强安全性 27

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 vservice_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 vservice_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 vservice_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 true 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 elc -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 elc -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
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is 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
```

Vserver	State	Domains	Name 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::> vsserver services name-service unix-group adduser -vsserver 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(unial resource ID 标识符、URI)将本地UNIX组列表加载到SVM中 vsserver 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：

```
vsserver services name-service unix-group load-from-uri -vsserver vsserver_name  
-uri {ftp|http|https|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|https|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	<code>vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files</code>
组信息	<code>vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files</code>
网络组信息	<code>vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files</code>

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	<div>a. 配置SVM的NFS Kerberos允许的加密类型： <code>vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types</code> 使用逗号分隔多种加密类型。</div> <div>b. 验证更改是否成功： <code>vserver nfs show -vserver vserver_name -fields permitted-enc- types</code></div>

要启用或禁用的项	请按照以下步骤操作 ...
AES-128或AES-256	<p>a. 确定启用了Kerberos的SVM和LIF： <code>vserver nfs kerberos interface show</code></p> <p>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： <code>vserver nfs kerberos interface disable -lif lif_name</code></p> <p>c. 配置SVM的NFS Kerberos允许的加密类型： <code>vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types</code></p> <p>使用逗号分隔多种加密类型。</p> <p>d. 验证更改是否成功： <code>vserver nfs show -vserver vserver_name -fields permitted-enc-types</code></p> <p>e. 在SVM上的所有SVM上重新启用Kerberos： <code>vserver nfs kerberos interface enable -lif lif_name -spn service_principal_name</code></p> <p>f. 验证是否已在所有生命周期管理器上启用Kerberos： <code>vserver nfs kerberos interface show</code></p>

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 <i>kdc_admin_username</i>
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} : <i>//uri</i>

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
-spns 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.
```

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。