使用NFS设置文件访问

ONTAP 9

NetApp
April 24, 2024

目录

使用NFS设置文件访问

使用 NFS 概述设置文件访问

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

要使客户端能够使用 NFS 访问 SVM 上的文件，您必须完成以下任务：

1. 在 SVM 上启用 NFS 协议。

   您必须将 SVM 配置为允许客户端通过 NFS 访问数据。

2. 在 SVM 上创建 NFS 服务器。

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

3. 在 SVM 上配置导出策略。

   您必须配置导出策略，以使卷和 qtree 可供客户端使用。

4. 根据网络和存储环境，为 NFS 服务器配置适当的安全性和其他设置。

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

使用导出策略确保 NFS 访问安全

导出策略如何控制客户端对卷或 qtree 的访问

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

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

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

如果客户端发出适用导出策略不允许的访问请求，则此请求将失败，并显示权限被拒绝的消息。如果客户端与导出策略中的任何规则不匹配，则会拒绝访问。如果导出策略为空，则会隐式拒绝所有访问。

您可以在运行 ONTAP 的系统上动态修改导出策略。

SVM 的默认导出策略

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

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

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

导出规则的工作原理

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

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

您可以使用以下条件配置导出规则以确定客户端访问权限：

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

  的最大大小 `-clientmatch` 字段为4096个字符。

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

如果某个规则指定了多个条件，则客户端必须与所有条件匹配，才能应用此规则。

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

示例

导出策略包含具有以下参数的导出规则：

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

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

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

示例

导出策略包含具有以下参数的导出规则：

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

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

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

示例

导出策略包含具有以下参数的导出规则：

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

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

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

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

管理安全类型未列出的客户端

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

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

的有效值 `-anon` 参数范围从 `0` to `65535`。

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

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

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

示例

导出策略包含具有以下参数的导出规则：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

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

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

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

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

的匿名用户身份进行只读访问。读写参数允许对任何安全类型进行读写访问，但在这种情况下，仅允许已通过只读规则筛选的适用场景客户端。

因此，客户端 1 和 3 只能作为用户 ID 为 70 的匿名用户进行读写访问。客户端 2 使用自己的用户 ID 获得读写访问权限。

示例

导出策略包含具有以下参数的导出规则：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule none`
- `-anon 70`

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

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

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

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

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

安全类型如何确定客户端访问级别

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

三种可能的访问级别如下：

1. 只读
2. 读写
3. 超级用户（对于用户 ID 为 0 的客户端）

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

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

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

以下是这三个访问参数中每一个参数的有效安全类型：

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

  此安全类型不适用于 `-superuser` 参数。

- `krb5`
- `krb5i`
- `krb5p`
- `ntlm`
- `sys`

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

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

示例

导出策略包含具有以下参数的导出规则：

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

客户端 1 的 IP 地址为 10.1.16.207 ，用户 ID 为 0 ，使用 NFSv3 协议发送访问请求，并使用 Kerberos v5 进行

身份验证。

客户端 2 的 IP 地址为 10.1.16.211 ，用户 ID 为 0 ，使用 NFSv3 协议发送访问请求，并使用 AUTH_SYS 进行身份验证。

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

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

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

管理超级用户访问请求

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

在 UNIX 环境中，用户 ID 为 0 的用户称为超级用户，通常称为 root ，他们对系统拥有无限访问权限。由于多种原因，使用超级用户权限可能会很危险，包括违反系统和数据安全。

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

- `any`
- `none`

  如果未指定、则此为默认设置 `-superuser` 参数。

- `krb5`
- `ntlm`
- `sys`

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

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

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

示例

导出策略包含具有以下参数的导出规则：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

客户端1的IP地址为10.1.16.207、用户ID为746、使用NFSv3协议发送访问请求、并使用Kerberos v5进行身份验证。

客户端 2 的 IP 地址为 10.1.16.211 ，用户 ID 为 0 ，使用 NFSv3 协议发送访问请求，并使用 AUTH_SYS 进行身份验证。

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

客户端 2 不会获得超级用户访问权限。相反、它会映射到匿名、因为 `-superuser` 未指定参数。这意味着它默认为 `none` 并自动将用户ID 0映射到匿名。客户端 2 也仅获取只读访问，因为其安全类型与读写参数不匹配。

示例

导出策略包含具有以下参数的导出规则：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

客户端 1 的 IP 地址为 10.1.16.207 ，用户 ID 为 0 ，使用 NFSv3 协议发送访问请求，并使用 Kerberos v5 进行身份验证。

客户端 2 的 IP 地址为 10.1.16.211 ，用户 ID 为 0 ，使用 NFSv3 协议发送访问请求，并使用 AUTH_SYS 进行身份验证。

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

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

ONTAP 如何使用导出策略缓存

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

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

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

缓存名称	存储的信息类型
访问	客户端到相应导出策略的映射
Name	UNIX 用户名到相应 UNIX 用户 ID 的映射
ID	UNIX 用户 ID 到相应 UNIX 用户 ID 和扩展 UNIX 组 ID 的映射
主机	主机名到相应 IP 地址的映射
网络组	网络组到相应成员 IP 地址的映射
showmount	从 SVM 命名空间导出的目录列表

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

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

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

访问缓存的工作原理

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

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

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

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

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

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

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

访问缓存参数的工作原理

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

访问缓存会存储包含一个或多个导出规则的条目，这些规则适用于尝试访问卷或 qtree 的客户端。这些条目会在刷新之前存储一段时间。刷新时间由访问缓存参数决定，并取决于访问缓存条目的类型。

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

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

示例

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

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

从 qtree 删除导出策略

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

步骤

1. 要从 qtree 中删除导出策略，请输入以下命令：

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

2. 验证是否已相应修改 qtree ：

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

验证 qtree 文件操作的 qtree ID

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

关于此任务

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

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

2. 执行以下操作之一：

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

3. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

FlexVol 卷的导出策略限制和嵌套接合

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

您应确保较高级别的接合与较低级别的接合相比具有较少限制的导出策略。

将 Kerberos 与 NFS 结合使用以增强安全性

ONTAP 支持 Kerberos

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

在 ONTAP 9 中，支持以下 Kerberos 功能：

- Kerberos 5 身份验证与完整性检查（ krb5i ）

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

- Kerberos 5 身份验证与隐私检查（ krb5p ）

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

- 128 位和 256 位 AES 加密

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

- SVM 级别的 Kerberos 域配置

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

使用 NFS 配置 Kerberos 的要求

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

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

应首先配置以下项：

网络环境要求

- Kerberos

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

  NFS服务器必须使用 `nfs` 作为其机器主体的主要组件。

- 目录服务

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

- NTP

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

- 域名解析（ DNS ）

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

- 用户帐户

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

NFS客户端要求

- NFS

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

  客户端必须支持 RFC1964 和 RFC2203 。

- Kerberos

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

  - 已启用 TGS 通信加密。

    AES-256 可提供最强大的安全性。

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

    使用计算机凭据时：

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

- 每个客户端都必须使用最新且更新的操作系统版本。

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

- DNS

  必须正确配置每个客户端，以使用 DNS 进行正确的名称解析。

- NTP

  每个客户端都必须与 NTP 服务器同步。

- 主机和域信息

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

- keytab 文件

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

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

存储系统要求

- NFS 许可证

  存储系统必须安装有效的 NFS 许可证。

- CIFS许可证

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

- SVM

  您必须在系统上至少配置一个 SVM 。

- SVM 上的 DNS

  您必须已在每个 SVM 上配置 DNS 。

- NFS 服务器

  您必须已在 SVM 上配置 NFS 。

- AES 加密

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

- SMB服务器

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

- Volumes

  您必须具有一个根卷和至少一个数据卷，以供 SVM 使用。

- 根卷

  SVM 的根卷必须具有以下配置：

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

  与根卷不同，数据卷可以采用任一安全模式。

- UNIX 组

  SVM 必须配置以下 UNIX 组：

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

- UNIX用户

  SVM 必须配置以下 UNIX 用户：

用户名	用户 **ID**	主组 **ID**	**comment**
NFS	500	0	GSS INIT阶段需要此参数 NFS 客户端用户 SPN 的第一个组件用作用户。

用户名	用户 ID	主组 ID	comment
pcuser	6554	6554	使用NFS和CIFS多协议时需要此参数 在创建SVM时、ONTAP会自动创建并添加到pcuser组中。
root	0	0	挂载时需要

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

- 导出策略和规则

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

- Kerberos-UNIX 名称映射

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

相关信息

"NetApp 技术报告 4073：《安全统一身份验证》"

"NetApp 互操作性表工具"

"系统管理"

"逻辑存储管理"

指定 NFSv4 的用户 ID 域

要指定用户ID域、您可以设置 `-v4-id-domain` 选项

关于此任务

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

步骤

1. 输入以下命令：

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

配置名称服务

ONTAP 名称服务交换机配置的工作原理

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

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

数据库类型

该表为以下每种数据库类型存储一个单独的名称服务列表：

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

源类型

源用于指定用于检索相应信息的名称服务源。

指定源类型 ...	查找信息的位置	由命令系列管理 ...

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

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

指定源类型 ...	查找信息的位置	由命令系列管理 ...
DNS	在 SVM 的 DNS 配置中指定的外部 DNS 服务器	`vserver services name-service dns`

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

用于访问外部源的协议

要访问外部源的服务器， ONTAP 使用以下协议：

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

示例

以下示例显示了 SVM SVM_1 的名称服务开关配置：

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

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

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

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

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

相关信息

"NetApp 技术报告 4668 ：《名称服务最佳实践指南》"

使用 LDAP

LDAP 概述

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

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

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

LDAP 转介跟踪不支持以下配置。

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

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

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

- 不支持使用 LDAP 进行主机名解析。

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

LDAP 签名和签章概念

从 ONTAP 9 开始，您可以配置签名和签章，以便对 Active Directory （ AD ）服务器的查询启用 LDAP 会话安全性。您必须将Storage Virtual Machine (SVM)上的NFS服务器安全设置配置为与LDAP服务器上的安全设置相对应。

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

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

LDAPS 概念

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

术语

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

- * LDAP *

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

- * ssl*

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

- * TLS *

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

- * LDAPS （基于 SSL 或 TLS 的 LDAP ） *

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

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

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

- * 启动 TL*

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

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

ONTAP 如何使用 LDAPS

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

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

ONTAP 支持以下功能：

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

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

- 自签名根 CA 证书

  使用 Active Directory 集成的 LDAP 时，在域中安装 Windows Server 证书服务时会生成自签名根证书。使

用基于 UNIX 的 LDAP 服务器进行 LDAP 名称映射时，系统会使用适用于该 LDAP 应用程序的方法生成并保存自签名根证书。

默认情况下、LDIPS处于禁用状态。

启用 **LDAP RFC2307bis** 支持

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

您需要的内容

您必须已为要使用的一个默认 LDAP 客户端模式创建一个副本。

关于此任务

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

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

默认情况下， RFC2307bis 支持处于禁用状态。

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

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

步骤

1. 将权限级别设置为高级：

   ```
   set -privilege advanced
   ```

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

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

3. 修改模式以匹配 LDAP 服务器中支持的对象类：

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

4. 修改模式以匹配 LDAP 服务器中支持的属性名称：

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

5. 返回到管理权限级别：

   ```
   set -privilege admin
   ```

LDAP 目录搜索的配置选项

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

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

默认基础和范围搜索值

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

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

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

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

自定义基础和范围搜索值

您也可以为用户，组和网络组搜索指定单独的基准值和范围值。通过这种方式限制查询的搜索基础和范围可以显著提高性能，因为它会将搜索限制为 LDAP 目录的较小部分。

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

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

`-netgroup-dn`	所有 LDAP 网络组搜索的基础 DNS
`-netgroup-scope`	所有 LDAP 网络组搜索的基本范围

多个自定义基础 **DN** 值

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

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

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

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

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

您需要的内容

LDAP目录必须包含 `netgroup.byhost` 映射。

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

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

关于此任务

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

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

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

步骤

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

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

2. 将权限级别设置为高级： `set -privilege advanced`
3. 在Storage Virtual Machine (SVM)的LDAP客户端配置中启用按主机搜索网络组： `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost-dn netgroup-by-host_map_distinguished_name -netgroup-byhost-scope netgroup-by-host_search_scope`

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

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

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

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

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

4. 返回到管理权限级别： `set -privilege admin`

示例

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

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

完成后

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

相关信息

"IETF RFC 5952： IPv6 地址文本表示建议"

使用**LDAP**快速绑定进行**nsswitch**身份验证

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

关于此任务

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

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

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

"了解如何使用快速绑定。"

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

要在ONTAP 环境中启用LDAP快速绑定、您必须满足以下要求：

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

步骤

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

   a. 要确认LDAP快速绑定服务器已在LDAP客户端配置中列出、请输入：

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

      "了解LDAP客户端配置。"

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

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

   "了解nsswitch配置。"

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

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

     ```
     -authentication-method nsswitch
     ```

   `-is-ldap-fastbind true`

   - 对于新的管理员用户、请参见 "启用LDAP或NIS帐户访问。"

显示**LDAP**统计信息

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

您需要的内容

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

步骤

1. 查看计数器对象的性能数据：

```
statistics show
```

示例

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

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

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

配置名称映射

配置名称映射概述

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

除了两个例外情况，您无需使用名称映射：

- 您配置的是纯 UNIX 环境，不打算在卷上使用 SMB 访问或 NTFS 安全模式。
- 您可以配置要使用的默认用户。

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

请注意，您只能对用户使用名称映射，而不能对组使用名称映射。

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

名称映射的工作原理

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

- 适用于 Windows 到 UNIX 的映射

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

- UNIX 到 Windows 的映射

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

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

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

  即使为计算机帐户定义了名称映射，也会忽略这些映射。

多域搜索 **UNIX** 用户到 **Windows** 用户名映射

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

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

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

- _ 双向信任 _

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

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

- 出站信任 _

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

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

- *Inbound trust*

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

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

如何使用通配符（ * ）配置名称映射的多域搜索

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

Pattern	更换	结果
root	｛asterisk｝ ｛反斜杠｝ ｛反斜杠｝ 管理员	UNIX 用户 "`root` " 将映射到名为 "`administrator` " 的用户。系统会按顺序搜索所有受信任域，直到找到第一个名为 "`administrator` " 的匹配用户为止。

Pattern	更换	结果
*	｛asterisk｝ ｛反斜杠｝ ｛反斜杠｝ ｛asterisk｝	有效的 UNIX 用户将映射到相应的 Windows 用户。系统将按顺序搜索所有受信任域，直到找到具有该名称的第一个匹配用户为止。 模式 ｛asterisk｝ ｛un斜 杠｝ ｛un斜 杠｝ ｛asterisk｝ 仅适用于从 UNIX 到 Windows 的名称映射，而不是相反。

如何执行多域名搜索

您可以选择以下两种方法之一来确定用于多域名搜索的受信任域列表：

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

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

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

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

名称映射转换规则

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

创建名称映射

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

关于此任务

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

步骤

1. 创建名称映射：

```
vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-
unix|unix-win} -position integer -pattern text -replacement text
```

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

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

示例

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

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

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

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

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

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

配置默认用户：

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

关于此任务

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

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

Windows 用户。

步骤

1. 执行以下操作之一：

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

用于管理名称映射的命令

您可以使用特定的 ONTAP 命令来管理名称映射。

如果您要 …	使用此命令 …
创建名称映射	`vserver name-mapping create`
在特定位置插入名称映射	`vserver name-mapping insert`
显示名称映射	`vserver name-mapping show`
交换两个名称映射的位置 注意：如果为名称映射配置了IP限定符条目、则不允许进行交换。	`vserver name-mapping swap`
修改名称映射	`vserver name-mapping modify`
删除名称映射	`vserver name-mapping delete`
验证名称映射是否正确	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

有关详细信息，请参见每个命令的手册页。

为 Windows NFS 客户端启用访问

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

关于此任务

默认情况下， Windows NFSv3 客户端支持处于禁用状态。

开始之前

必须在 SVM 上启用 NFSv3 。

步骤

1. 启用 Windows NFSv3 客户端支持：

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

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

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

   Windows NFSv3 客户端现在可以在存储系统上挂载导出。

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

   这是确保可靠挂载所必需的。

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

在 NFS 客户端上启用 NFS 导出显示

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

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

示例

以下命令显示了名为 vs1 的 SVM 上的 showmount 功能：

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

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

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