使用导出策略确保 NFS 访问安全

ONTAP 9

NetApp
April 24, 2024

目录

使用导出策略确保 NFS 访问安全

导出策略如何控制客户端对卷或 qtree 的访问

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

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

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

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

您可以在运行 ONTAP 的系统上动态修改导出策略。

SVM 的默认导出策略

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

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

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

导出规则的工作原理

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

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

您可以使用以下条件配置导出规则以确定客户端访问权限：

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

的最大大小 `-clientmatch` 字段为4096个字符。

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

如果某个规则指定了多个条件，则客户端必须与所有条件匹配，才能应用此规则。

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

示例

导出策略包含具有以下参数的导出规则：

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

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

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

示例

导出策略包含具有以下参数的导出规则：

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

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

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

示例

导出策略包含具有以下参数的导出规则：

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

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

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

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

管理安全类型未列出的客户端

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

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

的有效值 `-anon` 参数范围从 `0` to `65535`。

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

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

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

示例

导出策略包含具有以下参数的导出规则：

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

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

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

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

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

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

示例

导出策略包含具有以下参数的导出规则：

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

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

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

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

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

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

安全类型如何确定客户端访问级别

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

三种可能的访问级别如下：

1. 只读
2. 读写
3. 超级用户（对于用户 ID 为 0 的客户端）

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

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

以下是这三个访问参数中每一个参数的有效安全类型：

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

  此安全类型不适用于 `-superuser` 参数。

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

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

客户端的安全类型	然后，客户端 ...
与访问参数中指定的值匹配。	使用自己的用户 ID 获取该级别的访问权限。

客户端的安全类型	然后，客户端 ...
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。