使用导出策略确保SMB访问安全

ONTAP 9

NetApp
April 24, 2024

目录

使用导出策略确保SMB访问安全

如何在 SMB 访问中使用导出策略

如果在SMB服务器上启用了SMB访问导出策略、则在控制SMB客户端对SVM卷的访问时会使用导出策略。要访问数据，您可以创建一个允许 SMB 访问的导出策略，然后将该策略与包含 SMB 共享的卷相关联。

导出策略应用了一个或多个规则，用于指定允许哪些客户端访问数据以及只读和读写访问支持哪些身份验证协议。您可以配置导出策略，以允许通过 SMB 访问所有客户端，一个子网客户端或特定客户端，并允许在确定对数据的只读和读写访问时使用 Kerberos 身份验证， NTLM 身份验证或 Kerberos 和 NTLM 身份验证进行身份验证。

在处理应用于导出策略的所有导出规则后， ONTAP 可以确定是否授予客户端访问权限以及授予的访问级别。导出规则适用于客户端计算机，而不适用于 Windows 用户和组。导出规则不会取代基于 Windows 用户和组的身份验证和授权。除了共享和文件访问权限之外，导出规则还提供了另一层访问安全性。

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

- 为 SVM 的每个卷分配不同的导出策略，以便对 SVM 中的每个卷进行单个客户端访问控制。
- 为 SVM 的多个卷分配相同的导出策略，以实现相同的客户端访问控制，而无需为每个卷创建新的导出策略。

每个 SVM 至少有一个名为 `default` 的导出策略，该策略不包含任何规则。您不能删除此导出策略，但可以重命名或修改它。默认情况下， SVM 上的每个卷都与默认导出策略相关联。如果在 SVM 上禁用了 d**访问导出策略，则 "' 默认 '** '导出策略对 SMB 访问没有任何影响。

您可以配置规则以提供对 NFS 和 SMB 主机的访问，并将该规则与导出策略关联，然后导出策略可以与包含 NFS 和 SMB 主机都需要访问的数据的卷关联。或者，如果某些卷中只有 SMB 客户端需要访问，则可以为导出策略配置规则，这些规则只允许使用 SMB 协议进行访问，并且仅使用 Kerberos 或 NTLM （或两者）进行只读和写访问身份验证。然后，导出策略将与只需要 SMB 访问的卷相关联。

如果启用了 SMB 的导出策略，并且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。如果客户端与卷导出策略中的任何规则不匹配，则访问将被拒绝。如果导出策略为空，则会隐式拒绝所有访问。即使共享和文件权限允许访问，也是如此。这意味着，您必须将导出策略配置为在包含 SMB 共享的卷上至少允许以下内容：

- 允许访问所有客户端或相应的部分客户端
- 允许通过 SMB 进行访问
- 允许使用 Kerberos 或 NTLM 身份验证（或这两者）进行适当的只读和写访问

了解相关信息 "配置和管理导出策略"。

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。

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。

限制或允许通过 SMB 进行访问的导出策略规则示例

这些示例显示了如何在启用了 SMB 访问导出策略的 SVM 上创建导出策略规则来限制或允许通过 SMB 进行访问。

默认情况下， SMB 访问的导出策略处于禁用状态。只有在为 SMB 访问启用了导出策略时，您才需要配置导出策略规则来限制或允许通过 SMB 进行访问。

仅适用于 SMB 访问的导出规则

以下命令会在名为 "`vs1` " 的 SVM 上创建一个导出规则，该规则具有以下配置：

- 策略名称： cifs1
- 索引号： 1
- 客户端匹配：仅匹配 192.168.1.0/24 网络上的客户端
- 协议：仅启用 SMB 访问
- 只读访问：使用 NTLM 或 Kerberos 身份验证的客户端
- 读写访问：使用 Kerberos 身份验证的客户端

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

SMB 和 NFS 访问的导出规则

以下命令会在名为 "` vs1` " 的 SVM 上创建一个导出规则，该规则具有以下配置：

- 策略名称： cifsnfs1.
- 索引编号：2
- 客户端匹配：匹配所有客户端
- 协议： SMB 和 NFS 访问
- 只读访问：对所有客户端

- 读写访问：使用 Kerberos （ NFS 和 SMB ）或 NTLM 身份验证（ SMB ）的客户端
- 映射 UNIX 用户 ID 0 （零）：映射到用户 ID 65534 （通常映射到用户名 nobody ）
- SUID 和 sgid 访问：允许

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule
any -rwrule krb5,ntlm -anon 65534 -allow-suid true
```

仅使用 **NTLM** 进行 **SMB** 访问的导出规则

以下命令会在名为 "`vs1` " 的 SVM 上创建一个导出规则，该规则具有以下配置：

- 策略名称：ntlm1
- 索引号： 1
- 客户端匹配：匹配所有客户端
- 协议：仅启用 SMB 访问
- 只读访问：仅适用于使用 NTLM 的客户端
- 读写访问：仅适用于使用 NTLM 的客户端

> 如果为仅限 NTLM 的访问配置只读选项或读写选项，则必须在客户端匹配选项中使用基于 IP 地址的条目。否则、您将收到 `access denied` 错误。这是因为 ONTAP 在使用主机名检查客户端的访问权限时使用 Kerberos 服务主体名称（ SPN ）。NTLM 身份验证不支持 SPN 名称。

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

启用或禁用 **SMB** 访问导出策略

您可以在 Storage Virtual Machine （ SVM ）上启用或禁用 SMB 访问导出策略。可以选择使用导出策略控制 SMB 对资源的访问。

开始之前

以下是为 SMB 启用导出策略的要求：

- 在为客户端创建导出规则之前，客户端必须在 DNS 中具有 "`PTR` " 记录。
- 如果 SVM 提供对 NFS 客户端的访问权限，并且要用于 NFS 访问的主机名与 CIFS 服务器名称不同，则需要为主机名另外设置一组 "`A` " 和 "`PTR` " 记录。

关于此任务

默认情况下，在 SVM 上设置新的 CIFS 服务器时，不会使用导出策略进行 SMB 访问。如果要根据身份验证协议或客户端 IP 地址或主机名控制访问，则可以为 SMB 访问启用导出策略。您可以随时为 SMB 访问启用或禁用

导出策略。

步骤

1. 将权限级别设置为高级： `set -privilege advanced`
2. 启用或禁用导出策略：
   - 启用导出策略： `vserver cifs options modify -vserver *vserver_name* -is -exportpolicy-enabled true`
   - 禁用导出策略： `vserver cifs options modify -vserver *vserver_name* -is -exportpolicy-enabled false`
3. 返回到管理权限级别： `set -privilege admin`

示例

以下示例支持使用导出策略控制 SMB 客户端对 SVM vs1 上资源的访问：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```