配置绕过遍历检查

ONTAP 9

NetApp
April 24, 2024

目录

配置绕过遍历检查

配置绕过遍历检查概述

绕过遍历检查是一种用户权限（也称为 _privilege _ ），用于确定用户是否可以遍历路径中的所有目录以访问某个文件，即使用户对遍历的目录没有权限也是如此。您应了解允许或禁止绕过遍历检查时会发生什么情况，以及如何为 Storage Virtual Machine （ SVM ）上的用户配置绕过遍历检查。

允许或禁止绕过遍历检查时会发生什么情况

- 如果允许，当用户尝试访问某个文件时， ONTAP 在确定是授予还是拒绝访问该文件时不会检查中间目录的遍历权限。
- 如果不允许， ONTAP 将检查文件路径中所有目录的遍历（执行）权限。

  如果任何中间目录不具有 "`X` "（遍历权限），则 ONTAP 将拒绝访问此文件。

配置绕过遍历检查

您可以使用 ONTAP 命令行界面或使用此用户权限配置 Active Directory 组策略来配置绕过遍历检查。

。 `SeChangeNotifyPrivilege` 权限控制是否允许用户绕过遍历检查。

- 通过将其添加到 SVM 上的本地 SMB 用户或组或域用户或组，可以绕过遍历检查。
- 从 SVM 上的本地 SMB 用户或组或域用户或组中删除该文件将禁止绕过遍历检查。

默认情况下， SVM 上的以下 BUILTIN 组有权绕过遍历检查：

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`
- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

如果您不希望允许其中一个组的成员绕过遍历检查，则必须从该组中删除此权限。

在使用命令行界面为 SVM 上的本地 SMB 用户和组配置绕过遍历检查时，必须牢记以下几点：

- 如果要允许自定义本地或域组的成员绕过遍历检查、则必须添加 `SeChangeNotifyPrivilege` 权限。
- 如果要允许单个本地或域用户绕过遍历检查、而该用户不是具有该权限的组的成员、则可以添加 `SeChangeNotifyPrivilege` 权限。
- 您可以通过删除来禁用本地或域用户或组绕过遍历检查 `SeChangeNotifyPrivilege` 随时享受特权。

> 要为指定的本地或域用户或组禁用绕过访问程序检查、还必须删除 `SeChangeNotifyPrivilege` 特权 `Everyone` 组。

相关信息

允许用户或组绕过目录遍历检查

禁止用户或组绕过目录遍历检查

在卷上配置用于 SMB 文件名转换的字符映射

创建 SMB 共享访问控制列表

使用存储级别访问防护确保文件访问安全

支持的权限列表

向本地或域用户或组添加权限

允许用户或组绕过目录遍历检查

如果您希望用户能够遍历路径中的所有目录以查找某个文件、即使该用户对遍历的目录没有权限、则可以添加 `SeChangeNotifyPrivilege` Storage Virtual Machine (SVM)上的本地SMB用户或组的权限。默认情况下，用户可以绕过目录遍历检查。

开始之前

- SVM上必须存在SMB服务器。
- 必须启用本地用户和组SMB服务器选项。
- 要使用的本地或域用户或组 `SeChangeNotifyPrivilege` 要添加的权限必须已存在。

关于此任务

在向域用户或组添加权限时， ONTAP 可能会通过联系域控制器来验证域用户或组。如果 ONTAP 无法与域控制器联系，则此命令可能会失败。

步骤

1. 通过添加启用绕过遍历检查 `SeChangeNotifyPrivilege` 本地或域用户或组的权限： `vserver cifs users-and-groups privilege add-privilege -vserver` *`vserver_name`* `-user-or-group -name` *`name`* `-privileges SeChangeNotifyPrivilege`

   的值 `-user-or-group-name` 参数是本地用户或组、或者域用户或组。

2. 验证指定的用户或组是否已启用绕过遍历检查： `vserver cifs users-and-groups privilege show -vserver` *`vserver_name`* `-user-or-group-name` *`name`*

示例

以下命令可使属于"`explexe\eng`"组的用户通过添加来绕过目录遍历检查 `SeChangeNotifyPrivilege` 组权限：

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege
```

相关信息

禁止用户或组绕过目录遍历检查

禁止用户或组绕过目录遍历检查

如果您不希望用户遍历路径中的所有目录以访问某个文件、因为该用户对遍历的目录没有权限、则可以删除 `SeChangeNotifyPrivilege` Storage Virtual Machine (SVM)上的本地SMB用户或组的权限。

开始之前

要从中删除权限的本地或域用户或组必须已存在。

关于此任务

从域用户或组中删除权限时， ONTAP 可能会通过联系域控制器来验证域用户或组。如果 ONTAP 无法与域控制器联系，则此命令可能会失败。

步骤

1. 禁止绕过遍历检查： `vserver cifs users-and-groups privilege remove-privilege -vserver *vserver_name* -user-or-group-name *name* -privileges SeChangeNotifyPrivilege`

   此命令将删除 `SeChangeNotifyPrivilege` 使用的值指定的本地或域用户或组的权限 `-user-or-group-name *name*` 参数。

2. 验证指定的用户或组是否已禁用绕过遍历检查： `vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *name*`

示例

以下命令禁止属于 "`example\eng` " 组的用户绕过目录遍历检查：

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ------------------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ------------------------
vs1       EXAMPLE\eng           -
```

相关信息

允许用户或组绕过目录遍历检查