



配置绕过遍历检查 ONTAP 9

NetApp
April 24, 2024

目录

- 配置绕过遍历检查..... 1
 - 配置绕过遍历检查概述..... 1
 - 允许用户或组绕过目录遍历检查..... 2
 - 禁止用户或组绕过目录遍历检查..... 3

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

cluster1::> vservers cifs users-and-groups privilege show -vservers 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: `vservers cifs users-and-groups privilege remove-privilege -vservers vservers_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: `vservers cifs users-and-groups privilege show -vservers vservers_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](#)

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。