



## 未经授权的 Windows 用户访问 Unix 安全样式卷

[https://kb-cn-stage.netapp.com/on-prem/ontap/da/NAS/NAS-KBs/Unauthorized\\_Windows\\_User\\_Acces...](https://kb-cn-stage.netapp.com/on-prem/ontap/da/NAS/NAS-KBs/Unauthorized_Windows_User_Acces...)

Updated: Wed, 22 Apr 2026 09:26:32 GMT

### 适用于

- ONTAP 9
- CIFS

### 问题

即使权限被修改后，没有权限的用户仍能够访问具有 Unix 安全样式的 CIFS 共享并执行操作。

1. 收集所涉及的文件夹或文件的文件 [目录显示](#) 输出：

```
vserver security file-directory show -vserver <vserver> -path <Path>
```

```
cluster1::*> vserver security file-directory show -vserver svm0 -path /home0 Vserver: svm0 File Path: /home0/  
File Inode Number: 13918 Security Style: unix Effective Style: unix DOS Attributes: 10 DOS Attributes in Text: ---  
-D--- Expanded Dos Attributes: - UNIX User Id: 1010 UNIX Group Id: 111 UNIX Mode Bits: 770 UNIX Mode Bits  
in Text: rwxrwxrwx ACLs: -
```

2. 捕获启用了跟踪允许标志的 `sectrace` 以观察成功结果并检查 Windows 会话权限以识别正在使用的 Unix 用户。

'NetApp provides no representations or warranties regarding the accuracy or reliability or serviceability of any information or recommendations provided in this publication or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS and the use of this information or the implementation of any recommendations or techniques herein is a customers responsibility and depends on the customers ability to evaluate and integrate them into the customers operational environment. This document and the information

Node	Index	Filter Details	Reason
cluster1-01	1	Access is denied by UNIX permissions	permissions while opening existing file or directory. Access is not granted for: "Synchronize", "Write DAC", "Read Control", "Delete", "Write Attributes", "Delete Child", "Execute", "Write EA", "Read EA", "Append", "Write", "Read" Protocol: cifs Volume: - Share: home0 Path: /home0 Win-User: DEMO\user1 UNIX-User: pcuser Session-ID: 10652701968591486984

示例：

```
cifs session show -node * -vserver svm0 -session-id 10652701968591486984 -show-win-unix-creds
```

Vserver: svm0

```
Node: cluster1-01
Session ID: 10652701968591486984
Connection ID: 1489010350
Incoming Data LIF IP Address: 10.216.29.119
Workstation IP Address: 10.216.29.238
Authentication Mechanism: Kerberos
User Authenticated as: domain-user
Windows User: DEMO\user1
UNIX User: pcuser
Open Shares: 1
Open Files: 3
Open Other: 0
Connected Time: 2d 17h 43m 34s
Idle Time: 2d 16h 37m 3s
```

```
Protocol Version: SMB3_1
Continuously Available: No
Is Session Signed: false
NetBIOS Name: -
SMB Encryption Status: unencrypted
Large MTU Enabled: true
Connection Count: 1
Windows UNIX Credentials:
UNIX UID: pcuser <> Windows User: DEMO\user1 (Windows Domain User)

GID: pcuser
Supplementary GIDs:
pcuser

Windows Membership:
DEMO\Group Policy Creator Owners (Windows Domain group)
DEMO\Domain Users (Windows Domain group)
Authentication authority asserted identity (Windows Well known group)
BUILTIN\Users (Windows Alias)
User is also a member of Everyone, Authenticated Users, and Network Users

Privileges (0x22b7):
SeChangeNotifyPrivilege
```

### 3. 获取 CIFS 共享属性

```
cluster1-01::> cifs share show -vserver scoa -share-name audit
```

```
Vserver: svm0
Share: home0
CIFS Server NetBIOS Name: svm0
Path: /home0
Share Properties: oplocks
browsable
changenotify
show-previous-versions
Symlink Properties: symlinks
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment:
Share ACL: Authenticated Users/ Full Control
File Attribute Cache Lifetime: -
```

Volume Name: home  
Offline Files: manual  
Vscan File-Operations Profile: standard  
Maximum Tree Connections on Share: 4294967295  
UNIX Group for File Create: allowtestgroup