NetApp Knowledge Base

Troubleshooting CIFS or SMB access denied

https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/ONTAP_OS/Troubleshoot…

Updated: Thu, 19 Nov 2020 08:09:44 GMT

Applies to

- CIFS
- SMB

Issue

Access denied to a file or folder attempting to be accessed through the CIFS SMB protocol.

Cause

There are many potential causes. The information that follows is designed to help identify the cause more easily to quickly resolve it.

Solution

Note: It is recommended that all command line input and resulting console output be recorded in a text file for later review. Providing this in a technical support case notes may significantly improve time to resolution. Throughout this guide, commands with diagnostic and advances privilege levels are used. Exercise all due caution when running these commands as erroneous inputs might have unexpected consequences.

There have been some basic assumptions made about the environment. They are as follows:

- Connectivity to the Domain is functional and the time between the SVM, Domain Controller and clients are in sync
- The SVM is running
- CIFS is licensed and running on the SVM
- The CIFS Protocol is enabled on data LIFs

Share And Export Policy Access Permissions

The first step in validating access to a file or folder over CIFS (SMB protocol) is to make sure the user has share-level access to that file or folder. Once this is confirmed, validate there are no export policy's restricting access to the CIFS share.

Complete the following steps.

1. Confirm share path and permissions
   Check if the desired path is shared from the SVM, by running the cifs share show command.
   In the below example, verify the path /files is shared, and verify the ACL entry to which it is shared to.
   ```
   cluster::> cifs share show -vserver svm1
   ```

```
Vserver        Share         Path             Properties Comment  ACL
-------------- ------------- ---------------- ---------- -------- -----------
svm1           admin$        /                browsable  -        -
svm1           c$            /                oplocks    -        BUILTIN\Administrators / Full Control
                                                browsable
                                                changenotify
                                                show-previous-versions
svm1           ipc$          /                browsable  -        -
svm1           Public        /files           oplocks    -        Everyone / Full Control
                                                browsable
                                                changenotify
                                                show-previous-versions
4 entries were displayed.
```

In the above example, it is seen that the path /files are shared as "Public" to the "Everyone" group with "Full Control" permissions. Make sure that the user you are trying to validate has access to this share is a member of the group "Everyone".

Note: The default share-level acl is EveryoneFull Control.

2. Check to see if the export policy is enabled on the Vserver for CIFS.

   It is highly possible that an export policy exists, but is not enabled for CIFS. On a later version of ONTAP, the default for the Vserver is to have an export policy created but, not enabled for CIFS.

   Run the `cifs options show` command at the advanced privilege level to see if the export policy is enabled for CIFS.

   In the below example (after going to the advanced privilege level), you can see that Vserver svm1 has export polices enabled for CIFS.

   ```
   cluster::> set -privilege advanced
   ```

   ```
   Warning: These advanced commands are potentially dangerous; use them only when directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

   ```
   cluster::*> cifs options show -vserver svm1 -fields is-exportpolicy-enabled
   ```

   ```
   vserver is-exportpolicy-enabled
   ------- ----------------------
   svm1    true
   ```

   Note: If export policies are not enabled on the Vserver for CIFS, you can proceed to the next section.

3. Check for the existence of an export policy on the vserver

   Typically export policies are used to control access to folders and files for NFS clients. However, they can

also be used to restrict access to CIFS folder and files as well. Run the `vserver export-policy show` command to see if an export policy exists.

In the below example, you are looking to see if the veserver svm1 has any policy's applied.

```
cluster::*> vserver export-policy show -vserver svm1
```

```
Vserver          Policy Name
---------------  -------------------
svm1             default
```

Note: If an export policy does not exist you can proceed to the next section.

4. If an export policy exists and is enabled for CIFS, you must check to see if this policy has a rule which can restrict access to the CIFS share path.

   Run the `vserver export-policy rule show` command to examine all of the rules that exist within the export policy.

   In the below example, it is seen that the rule could be applying to the user that is attempting to access the CIFS share. This is because the protocol is set to "cifs".

```
vserver policyname ruleindex protocol clientmatch rorule rwrule anon  superuser
------- ---------- --------- -------- ----------- ------ ------ ----- ---------
svm1    default    1         cifs     0.0.0.0/0   never  never  65534 none
```

   In this case, it is obvious that the first rule is preventing access to the file or folder due to the read only rule and read write being set to 'never'.
   If you think that an export policy rule might be causing an issue, a simple test would be to create a wide-open export policy rule.

   Example of creating a wide open export policy and rule, and assigning the volume files to it.

```
cluster::*> export-policy create-vserver svm1 -policyname wide_open
cluster::*> export-policy rule create -vserver svm1 -policyname wide_open
-clientmatch 0.0.0.0/0 -protocol any -rorule any -rwrule any -superuser
any
cluster::*> vol modify -vserver svm1 -volume files -policy wide_open
```

```
Volume modify successful on volume files of Vserver svm1.
```

   Note: If you have verified that the export policy rules are not preventing access continue to the next section.

5. If you determine that an export policy is preventing CIFS access to the file or folder then you need to delete that export rule. **However, you must also be sure that the rule is not providing access to other client types (like NFS) before you delete the rule**.

   Run the `vserver export-policy rule delete` command to remove the export rule that is preventing CIFS access.

   In the below example, we are deleting the 1st rule in the default policy that we noted was set to 'never' for RO and RW in the Step 4 above.

   ```
   cluster::*> vserver export-policy rule delete -vserver svm1 -policyname
   default -ruleindex 1
   ```

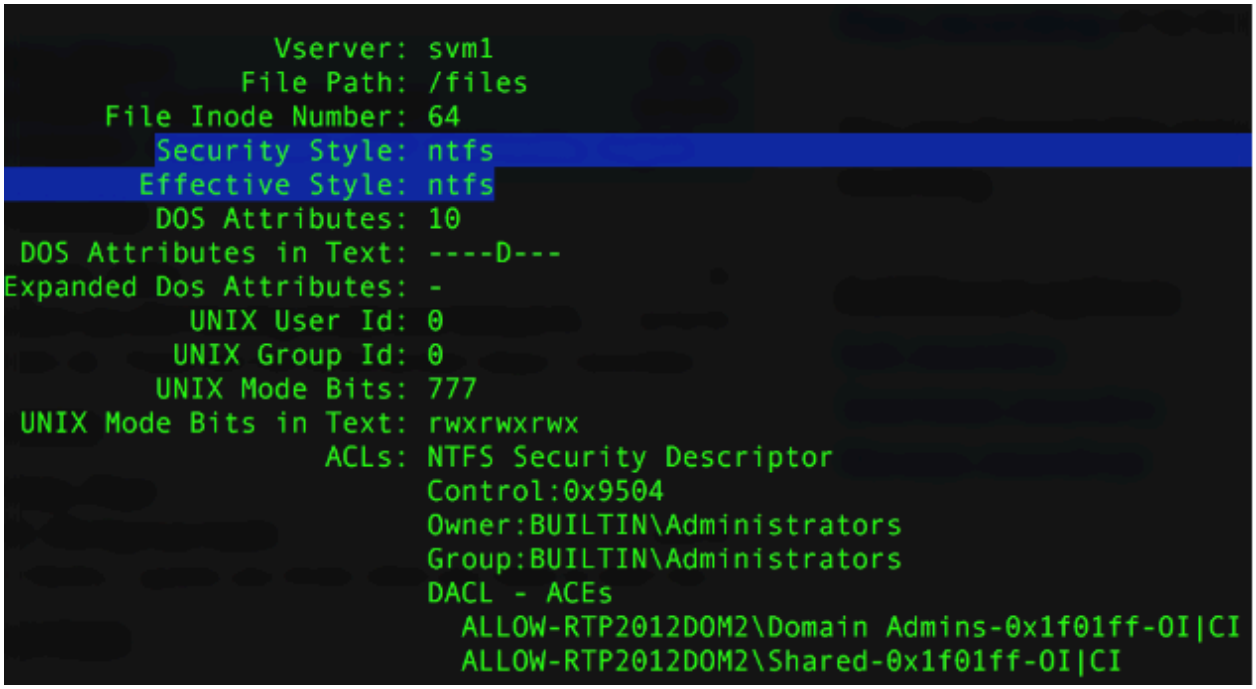
   ```
   Warning: The last rule in the export-policy "default" is being deleted. All volumes and qtrees using this policy will become inaccessible.
   Do you want to continue? {y|n}: y
   ```

File Permissions

1. Determine the security style of the file or folder you are trying to access.

   Run the `vserver security file-directory show` command on the Vserver and file or folder path and note the "security" and "effective security" style.
   In the following example, it is seen that both the "security" and "effective security" style are NTFS.

   ```
   cluster::*> vserver security file-directory show -vserver svm1 -path
   /files
   ```



Depending on the effective style (NTFS / UNIX), proceed to the appropriate section below.

Note: When the security style is mixed or unified, the effective permissions depend on the client type that last modified the permissions because users set the security style on an individual basis. If the last client that modified permissions was an NFSv3 client, the permissions are UNIX NFSv3 mode bits. If the last client was an NFSv4 client, the permissions are NFSv4 ACLs. If the last client was an SMB client, the permissions are Windows NTFS ACLs.

NTFS Security Style

Note: Start in diag mode

```
::>set diag y
```

Once you have determined that there is not a share or export issue, and the effective security style is NTFS, perform the following steps:

Method 1 - Security Trace (sectrace)

1. Begin by using sectrace to determine the reason for access denied.

   An additional troubleshooting tool for permission issues is security trace.
   It is possible to create a security trace filter on the Vserver and user Windows account being used to see what is causing access denied.

In the following example, create a filter on the Windows account 'user'.

```
cluster::*> vserver sectrace filter create -vserver svm1 -index 1 -trace-
allow no -windows-name rtp2012dom2\user
cluster::*> vserver sectrace filter show
```

```
Vserver  Index    Client-IP           Path          Trace-Allow Windows-Name
-------- -----  --------------  --------------------  ----------- -------------
svm1       1    -               -                        no      rtp2012dom2\
                                                                  user
```

Note: Attempt to reproduce the access denied issue after this step.

```
cluster::*> vserver sectrace trace-result show
```

```
  Index      Filter Details                  Reason
-- -----  -------------------------  ------------------------------
    1    Security Style: NTFS and   Access is denied. The
         NT ACL                     requested permissions are not
                                    granted by the ACE while
                                    opening existing file or
                                    directory. Access is not
                                    granted for: "Read
                                    Attributes", "Read"
         Share: Public
         Path: /
         Win-User: rtp2012dom2\user
         UNIX-User: pcuser
         Session-ID: 70889472884578714l5
```

Note: Be sure to delete the trace after you are done troubleshooting.
`cluster::*>vserver sectrace filter delete -index 1`
(Best practice for performance reasons are to delete *all sectrace filters* once troubleshooting is completed)

From the above example output, it is seen that the user account `rtp2012dom2\user` does not have even basic "read" access.
This indicates that the user account needs to be added to the appropriate group (or file/folder directly) for the path in question.

Method 2 Analyze DACL's (Discretionary Access Control List)

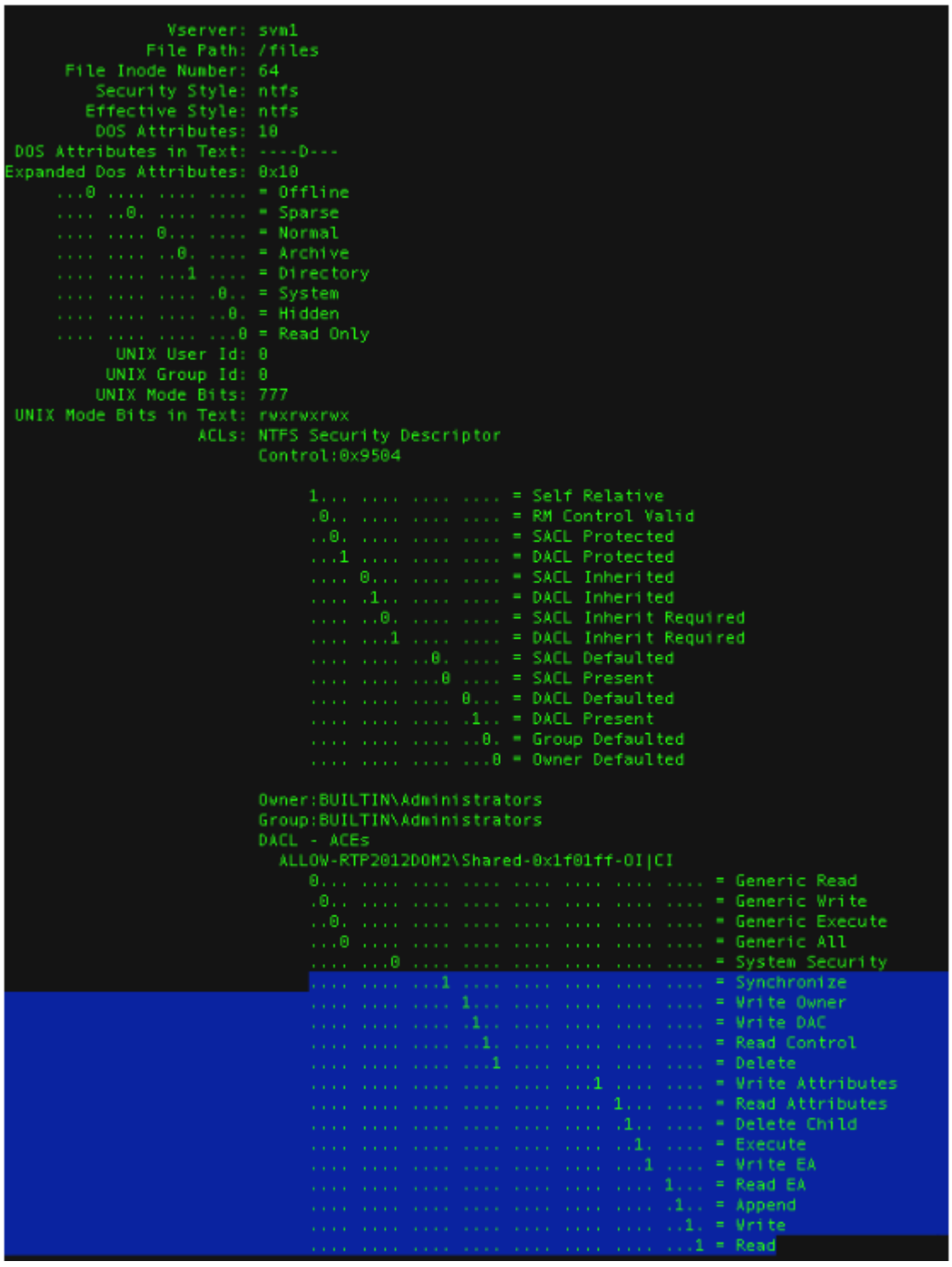
If `sectrace` does not indicate the possible issue, then try the following more advanced steps to help determine

the cause of the access denied issue.

1. Determine the DACL's that will either specify allow or deny for the path in question by running the `vserver security file-directory show` command

   The **DACL** section of the output can show you which users or groups have allow or deny access.In the following example, it is seen that the user or groups "`RTP2012DOM2Shared`" have access in 14 different areas including Read, Write, and Execute.

   ```
   cluster::*> vserver security file-directory show -vserver svm1 -path
   /files -expand-mask true
   ```



In the above example the “1’s” indicate that access has been granted in that area.

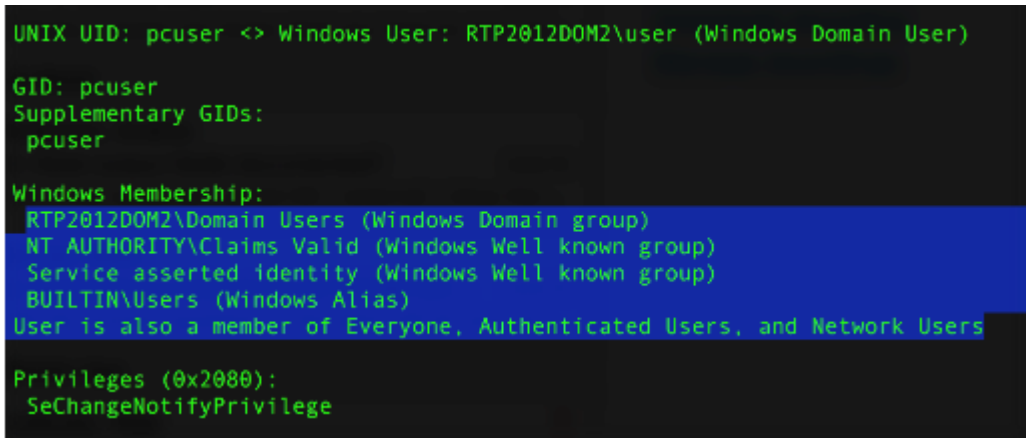
Note: If the Windows account name with either "ALLOW" or "DENY' is not seen, then the account will either need to be a member of a group that has an "ALLOW" or it will have to be directly added to the ACL

of the file/folder.

2. Determine Windows account group membership by running the `diag secd authentication show-creds` command

   The " **Windows Membership"** section will show the groups in which the account is a member.

   In the below example, the Windows user account " `rtp2012dom2\user`" is not a member of the " `RTP2012DOM2Shared`" groups.
   `cluster::*>diag secd authentication show-creds -node node01  -vserver svm1 -win-name rtp2012dom2\user`

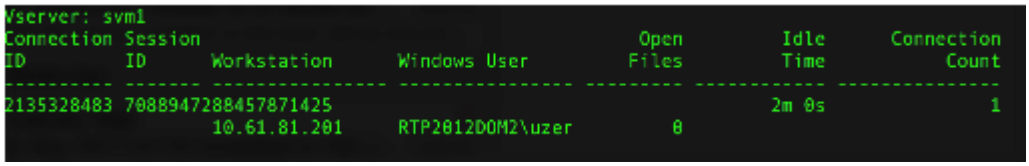


   At this point it is likely that the reason for the access denied message is due to the Windows account "user" not being a member of the "Shared" group.
   If adding the user account to the appropriate group (or directly to the file/folder if needed) does not resolve the issue proceed to the next step.

3. Verify the Windows account is actually the one being used to authenticate by running the `cifs session show` command

   There might be a misunderstanding about which account is being used to authenticate to the file/folder.

   In the following example, it is seen that the Windows account "user" is not present, and instead "uzer" is being used, which is indicating that the wrong account may have been used.



   In this example, the user should either switch to using the "user" account, or add the user account "uzer" to the appropriate group (or file/folder directly).

Note: If there are many CIFS sessions being displayed, it is possible to filter the output to the client IP address that is being used to access the path.

UNIX Security Style

Note: On UNIX Security Style, the preferred method is to use Security Trace (sectrace), which is described on the section above.

To manually diagnose, follow the instructions below.

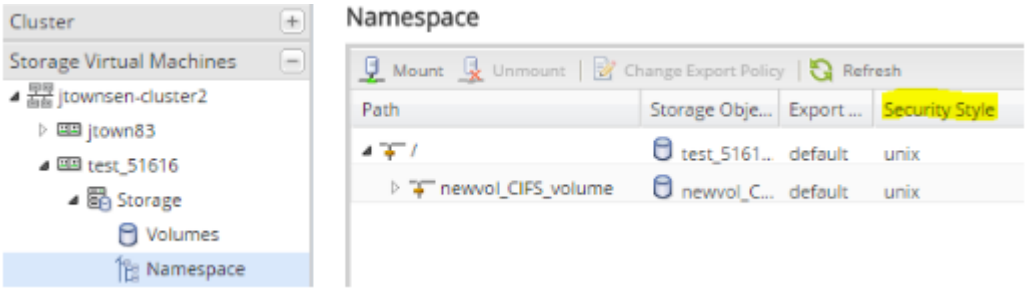
Start in diag mode:

```
::> set diag
Y
```

Filer Permissions

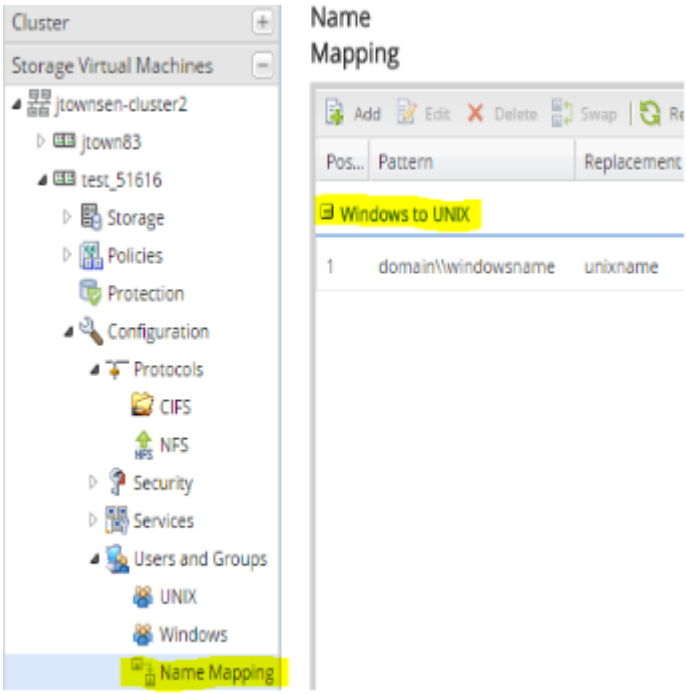
1. Confirm security style of the volume containing the object being accessed.

```
::> vol show -vserver <vserver> -volume <vol> -fields security-style,unix-permissions,junction-path
```



2. NTFS security style volume
   A. Check the usermapping of the Windows user: `::*> diag secd name-mapping show -node <node> -vserver <vserver> -direction win-unix -name <windows name>`
   B. If mapping to an unexpected user, verify the name-mapping source/configuration
      a. Note if unexpectedly name mapping to unix-user “pcuser” then name mapping may not be configured or working properly.
      b. `::> vserver services name-service ns-switch show -vserver <vserver> -database passwd,group,namemap`
      c. If name mapping uses source file, check the name mapping configuration
         I. `::> vserver name-mapping show -vserver <vserver> -direction win-unix`

II. To view local (file) name mappings through System Manager:



d. If name mapping use source LDAP:

I. Ensure name-mappings have been properly configured within LDAP.

II. Perform LDAP Troubleshooting Steps if necessary

3. If name mapping succeeds, convert username to UID.

A. Check the UID and GID's for the username

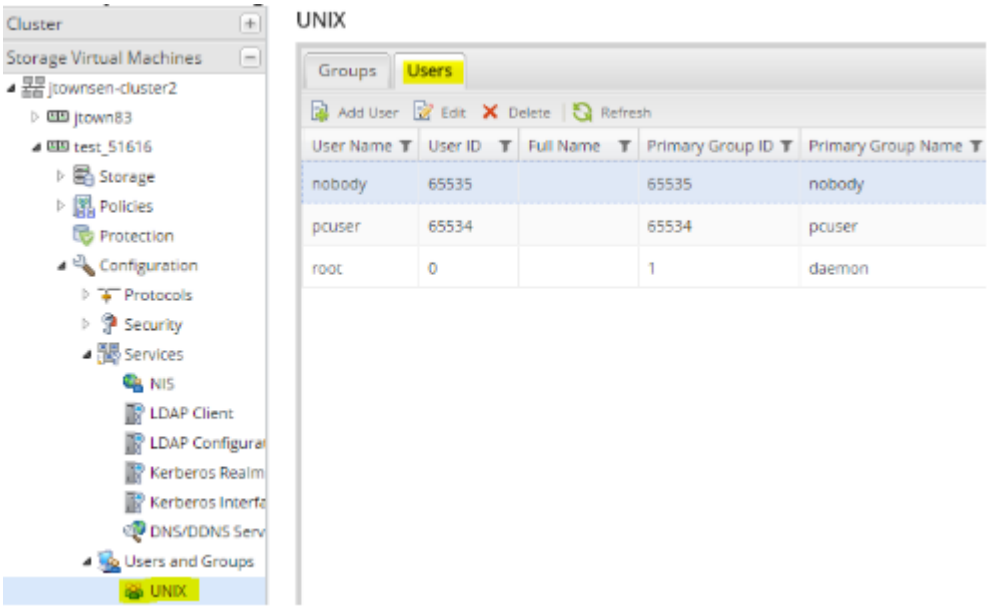
a. `::*> diag secd authentication show-creds -node <node> -vserver <vserver> -unix-user-name <user> -list-id true`

B. If the UID/GID does not show as expected, using the following command previously run, check the sources for user lookup called "passwd"

a. `::> vserver services name-service ns-switch show -vserver <vserver> -database passwd,group,namemap`

I. Case File:

i. Check existence of local UNIX User and its primary group ID:
`::> vserver services unix-user show -vserver <vserver>`
Or via system manager:

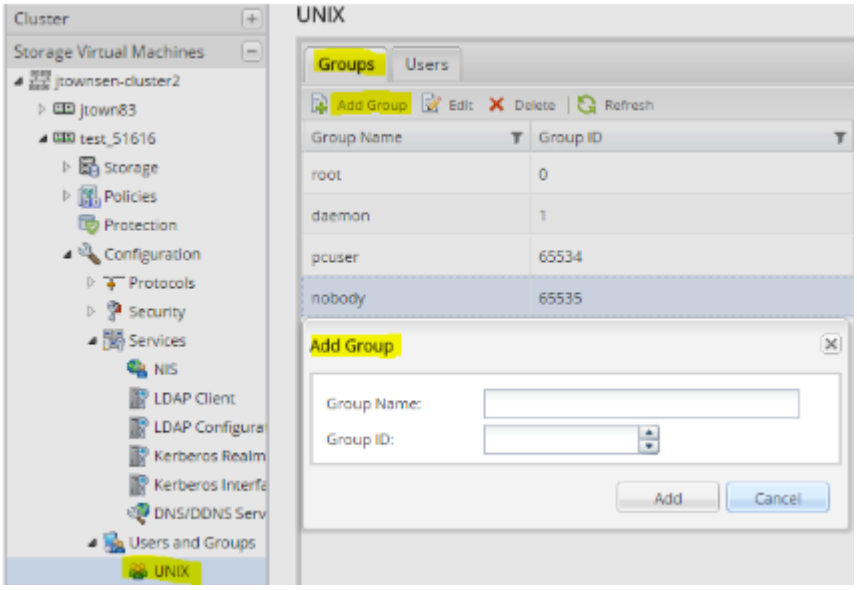


II. Add local unix-user if not present `::> vserver services unix-user create -user <name> -id <uid> -vserver <vserver> -primary-gid <gid>`

Note: System Manager will not show the user's secondary groups

III. If user is not part of an expected secondary group, inspect groups/members and create/add accordingly:

```
::> vserver services unix-group create -vserver <vserver> -name
<group name> -id <gid>
```



```
::> vserver services unix-group adduser -vserver <vserver> -name <group name> -username <username>
```

Note: System Manager cannot be used to add users to groups

b. Case NIS:
   I. Ensure that users and groups have been added to the NIS server
   II. Perform NIS troubleshooting steps if necessary.
c. Case LDAP:
   I. Ensure users and groups have been added to the LDAP server
   II. Perform LDAP troubleshooting steps if necessary
d. Checking/Modifying NFS permissions
   I. For details on Mode bits see section **How Unix Permissions Work**
   II. Check UNIX permissions from the storage controller:
      i. `vserver security file-directory show -vserver <vserver> -path <junction-path>`
         a. Ensure “security style” and “effective style” are UNIX.
         b. Ensure unix-user id (owner) is expected.
            i. If unexpected, access through a Linux user with appropriate permissions and use “chown” command to change ownership of the file/directory.
               - Example: `chown <new owner name> <file/directory>`
         c. Ensure UNIX-group is expected
            i. If unexpected, access via a Linux user with appropriate permissions and run the “`chgrp`” command to change group for the file/directory
            Example: `chgrp <new group name> <file/directory>`
         d. Ensure UNIX permissions are expected. See “How Unix Permissions Work” for details.
            i. If permissions are incorrect modify them with a Windows user with appropriate permissions using the Windows Security tab.
      ii. Alternately access using a Linux user with appropriate permissions and run the “`chmod`” command to change group to the desired mode bit combination.
      `chmod <mode_bits> <file>`
      Example for full control: `chmod 777 file`

How UNIX Permissions Work

Every file has a set of UNIX permissions, which are used when a file has UNIX-style security. These include the owning UID, the owning GID, and separate Read, Write, and Execute permissions for each of three categories of users: the owner, group members, and everyone else ('other'). These are displayed by the Windows security tab or 'ls' as rwxrwxrwx with the order being owner, group and other.

This example rwxrwxrwx provides read, write, and execute permissions to the owner, group, and all other UNIX-users.

Another example rwx-r-x--- provides read, write and execute permission to the owner, read and execute permissions to the associated group, and no permissions to anyone else.

Each specific permission can also be represented in binary.

- Execute = 1 or binary 001 if execute permission is allowed
- Read = 2 or binary 010 if read permission is allowed
- Write = 4 or binary 100 if write permission is allowed

These numbers are added up and can also be displayed in an octal number 0-7 to show permissions.
The following table displays the permissions provided by each octal value.

7	Read/write/execute
6	Read and write
5	Read and execute
4	Read
3	Write and execute
2	Write
1	Execute
0	No permissions

For more information about UNIX permissions, see UNIX permissions help.

NIS Troubleshooting

1. Confirm that NIS settings are correct
   `nis show -vserver <vserver>`
2. Determine if there are any errors reported in the EMS event log and take the specified corrective action
   `event log show -messagename *nis*`
   `event route show -messagename <EMS event name> -instance`
   Example

```
::> event route show -messagename nis.server.not.available -instance
```

Message Name: `nis.server.not.available`
Severity: ERROR
Corrective Action: From a UNIX (R) workstation, make sure that the NIS server is responding to requests. Also make sure that the portmapper on the NIS server is responding to requests. Make sure that there are no networking issues stopping the cluster from communicating with this NIS server.
Description: This message occurs when none of the NIS servers configured for a Storage Virtual Machine can be contacted.

3. Check network connectivity using the steps outlined the section Network Connectivity Checking.

LDAP Troubleshooting

1. Confirm that LDAP settings are correct:
   ```
   ldap show -vserver <vserver>
   ldap client show -client-config <config>
   ```
2. Determine if there are any errors reported in the EMS event log and take the specified corrective action
   ```
   event log show -messagename *ldap*
   event route show -messagename <EMS event name>
   ```

   Example
   ```
   ::> event route show -messagename secd.ldap.noServers -instance
   ```
   Message Name: `secd.ldap.noServers`
   Severity: ERROR
   Corrective Action: From a LDAP client workstation, make sure that all configured LDAP servers are responding to requests. Make sure that there are no networking issues stopping the cluster from communicating with the configured LDAP servers. Also, make sure that the portmapper running on the LDAP server is working correctly.
   Description: This message occurs when none of the configured Lightweight Directory Access Protocol (LDAP) servers are accepting connections.

3. Check network connectivity using the steps outlined in the **Network Connectivity Checking** section.

Network Connectivity Checking

SVM LIFs

Checking connectivity for the LIFs owned by an SVM are based almost entirely on basic networking principles, such as subneting and routing. It is important to understand whether the LIF is in the same network as a particular destination, and whether it can figure out how to get there.

```
network interface show – check the IP of each LIF and which node/port it
resides on
cluster::> network interface show -vserver Svm
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
Svm
            Svm_lif1        up/up    172.18.162.6/16    node01
                                                                   e0c     true
            Svm_admin
                         up/up    172.18.162.14/24   node02
                                                                   e0d     true

network route show – check the destination route and which gateway will be
used.
cluster::> network route show -vserver Svm
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
Svm
                    0.0.0.0/0       10.113.52.1     30
                    0.0.0.0/0       172.18.162.1    20
```

Troubleshooting

- Are the LIFs in the same network as the gateway?
  - If the gateway is 10.10.30.1, the LIF must be in one of these networks:
    - 10/8 (10.x.x.x, netmask 255.0.0.0)
    - 10.10/16 (10.10.x.x netmask 255.255.0.0)
    - 10.10.30/24 (10.10.30.x netmask 255.255.255.0)
- Are there multiple gateways per Vserver?
  - Ensure that if a Vserver has multiple gateways, each gateway has a different metric
  - Gateways with the lower metric have greater priority (the SVM will try that route first)

Ping and Traceroute

Ping and Traceroute are used to test network connectivity. Ping can verify that the source is able to reach the destination, while traceroute will show which routers the packet must pass through to get to the destination. For

IPv6 networks, use ping6 or traceroute6.

Ping and Traceroute are not good indicators for whether a protocol will succeed, such as NFS, CIFS, DNS or LDAP. They can only determine whether the packet can get from point A to point B. Keeping this in mind, ICMP traffic must be allowed by the destination and for all devices in-between. Otherwise, failures may be seen for either command regardless of network state.

The following commands should always be run with -lif, unless checking connectivity for the Node Management LIFs.

- `network ping | network ping6`
- `network traceroute | network traceroute6`

Ping

ping success

```
cluster::> network ping -lif test3 -vserver Svm -destination 172.18.162.1
172.18.162.1 is alive

cluster::> network ping -lif test3 -vserver Svm -destination 172.18.162.1 -v
true -show-detail true
PING 172.18.162.1 (172.18.162.1) from 172.18.162.22: 56 data bytes
 to 172.18.162.22 64 bytes from 172.18.162.1: icmp_seq=0 ttl=128 time=1.815 ms
```

ping failure

```
cluster::> network ping -lif test -vserver Svm -destination 8.8.8.8
no answer from 8.8.8.8

cluster::> network ping -lif test -vserver Svm -destination 8.8.8.8 -v true
-show-detail true
ping: sendto: No route to host
```

Tracereoute

```
cluster::> network traceroute -lif test3 -vserver Svm -destination 8.8.8.8
```

An asterisk may be displayed in the traceroute output. In most cases, traceroute defaults to waiting 5 seconds per query. If a device does not respond within 5 seconds, an asterisk is displayed. The default is also 3 queries per hop (device).
With traceroute, the goal is for the destination to have 0 asterisks for queries to that device. If each query

becomes an asterisk before reaching the destination, communication cannot proceed to the next hop. If the traceroute returns Time Exceeded or ICMP Time Exceeded, there are too many hops between the source and destination.

Firewalls

For this aspect of troubleshooting, the firewall is on the client or is a device external to both the client and SVM. A command, such as "netstat –an" can provide a simple overview of these aspects. For NFS, the primary concern is whether a related service is in the LISTEN state for its well-known port.

It is also important to note that the firewall in this section is external to Data ONTAP. Data ONTAP has a firewall internal to itself for management protocols, such as SSH, NDMP, or NTP. In clustered Data ONTAP 8.3, the following firewall policies may be applied to LIFs:

Firewall policy	Default service protocols	Default access	LIFs applied to
mgmt	DNS, HTTP, HTTPS, NDMP, NDMPS, NTP, SNMP, SSH	0.0.0.0/0	Cluster management, SVM management, and node management LIFs
intercluster	HTTPS, NDMP, NDMPS	0.0.0.0/0	All intercluster LIFs
data	DNS, NDMP, NDMPS	0.0.0.0/0	All data LIFs

Data ONTAP's firewall is not applied to a data protocol, such as NFS. If a data protocol is displaying symptoms of a firewall blocking the port, such as Connection Refused messages, it is be more important to confirm that the data LIFs have a data protocol and that SVMs have the same data protocol.

```
cluster::> network interface show –vserver Svm -fields data-protocol
vserver lif                  data-protocol
------- -------------------- -------------
Svm     svm_lif1             nfs,cifs

cluster::> vserver show –vserver Svm -fields allowed-protocols
vserver allowed-protocols
------- ----------------------
Svm     nfs,cifs,ndmp

cluster::> vserver show –vserver Svm -fields disallowed-protocols
vserver disallowed-protocols
```

```
------- --------------------
Svm     fcp,iscsi
```

If Data ONTAP's firewall is suspect, check for ipfiler.ReachedMaxStates in the EMS event log.

```
cluster::> event route show -messagename ipfilter.ReachedMaxStates -instance
                                    Message Name: ipfilter.ReachedMaxStates
                                        Severity: NOTICE
                                Corrective Action: (NONE)
                                     Description: This message occurs when the
ipfilter firewall fails to create a new dynamic state entry for a 'keep-state'
rule because the number of dynamic state entries has reached the maximum
allowed value of 4013. The 'keep-state' rule is used by the firewall to keep
track of whether a connection is established. States are maintained by firewall
for TCP, UDP, and ICMP packets. This message occurs at most once every 60
seconds; it lists the most recent connections to reach the limit.
```

Services and Ports

Service	Port
RPC-Portmapper (NIS)*	111
LDAP	389
DNS	53
Kerberos	88

Note: NIS servers dynamically select a privileged port during startup and register with the RPC-Portmapper service. Data ONTAP will query RPC-Portmapper running on port 111 to discover the actual service port.

Additional Information

Add your text here.