NetApp Knowledge Base

Troubleshooting Access Denied or Mount Hung from NFS client for clustered Data ONTAP

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

Updated: Wed, 31 Aug 2022 14:30:03 GMT

Applies to

ONTAP 9

Description

This guide intends to provide a set of troubleshooting procedures to assist with identifying the cause of an NFS mount hang or access denied response.

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 may significantly improve time to resolution.

Throughout this guide, commands with diagnostic and advances privilege levels are used. Exercise all with due caution when running these commands as erroneous inputs might have unexpected consequences.

Common Causes of Access Denied or Hang

There are many causes of NFS mounts that fail with access denied or continually re-attempt and appear to hang. The following list describes the most common causes that have been observed. The following section will provide troubleshooting strategies that will enable you to quickly identify and remediate the cause of the issue.

- Export rule does not exist for the client's IP or hostname
- Mount attempts prior to provisioning the name services including netgroup or DNS entries results in negative entry in access cache
- DNS resolution of client IP to name does not match netgroup or the hostname specified in the export rule
- Missing or incorrect DNS search domains
- DNS, NIS or LDAP server timeouts
- Missing DNS PTR record
- Hostname specified in export rules is not fully qualified and ends with a dot (.), also known as a rooted name
- DNS, NIS or LDAP servers are unreachable due to network connectivity – firewall policies or route configurations
- Lack of `netgroup.byhost` maps in NIS or LDAP
- Netgroups with hostnames that will not resolve in DNS
- Netgroup hostname case sensitivity for local files and some remote services including NIS and LDAP
- NFSv4 mounts or NFSv3 auth=null require user mapping only if there is an NTFS volume in the path

Procedure

Confirm NFS is enabled

```
Cluster1::> vserver nfs show

Virtual  General
Server   Access  v3       v4.0     v4.1     UDP      TCP
-------- ------- -------- -------- -------- -------- --------
svm1     true    enabled  enabled  disabled enabled  enabled
```

```
svm2     true    enabled  disabled disabled enabled  enabled
```

Troubleshoot NFS Mount Access Denied or Hang

- Verify if an export rule exists that allows the client to gain access using the check-access command:
  - `Cluster1::> vserver export-policy check-access -vserver <vserver> -volume <volume> -client-ip <clientIP> -auth <auth_type> -proto <proto> -access-type <type>`

NFS check-access succeeds:

1. If the `check-access` command succeeds:
   - All of the export policies in the junction-path will be listed in check-access output:
     (in diag privilage level) `Cluster1::> nblade access-cache show -node <node> -vserver <vserver> -policy <policy> -address <address>`
   - If a negative access entry exists, clear the entry and reattempt the mount:
     (in diag privilage level) `Cluster1::> nblade access-cache flush -vserver <vserver> -node <node> -policy <policy> -address <clientIP>`
2. If `check-access` succeeds, the mount fails with NFSv4 or NFSv3 using `auth_null`
   - Attempt to mount the root of the Vserver from the client
     The root of the Vserver has the junction-path '/'
     For example:
     - `mount <filerIP>:/ <mount point`
   - If this succeeds, '`cd`' directory by directory on the client until you get access-denied, and record the path.
   - For the directory that gives you access-denied from the previous step, determine the following:
     1. Is the security style of the directory NTFS or Unix?
        `Cluster1::> vserver security file-directory show -vserver <vserver> -path <path>`
        - If the security style of the directory is NTFS confirm the following:
          1. Usermapping and credential access correct:
             (in diag privilege level) `Cluster1::*> secd authentication show-creds -node <node> -vserver <vserver> -uid <clientUID>`
          2. Permissions from the 'vserver security file-directory show' grant the user determined from the 'secd authentication show-creds' to the directory:
             `Cluster1::> vserver security file-directory show -vserver <vserver> -path <path>`
     2. If the directory is Unix, confirm that the UID of the client should have access. This can be determined from the Vserver security file-directory show output:
        (in diag privilege level) `Cluster1::> vserver security file-directory`

`show -vserver <vserver> -path <path>`

3. If the Unix user is root, determine if the client has root access in the export-policy by vserver export-policy rule show:
   `Cluster1::> vserver export-policy rule show -vserver <vserver> -policyname <policy name>`
4. If NFSv4, confirm that ID mapping is working correctly:
   How to configure NFSv4 in Cluster-Mode
   If this is a newly created volume, or ls-mirrors have not updated, update `ls-mirror-set`
   - How do LS mirrors affect NAS access when new volumes are added?
     To PUSH the scheduled LS Mirror job appreciate that this is a function of the SOURCE PATH: i. Example: `Cluster1::> snapmirror update-ls-set -source-path cm2244a-cn://vs_cifs/vs2_root`
   - Issue with mounting new NFS vol from Vserver without schedule for LS Mirror
   - Unable to mount a volume using NFS in clustered Data ONTAP 8.2

NFS check-access command fails:

1. Run the `event log show` command to determine if any name services errors have occurred:
   `Cluster1::> event log show -message-name *nis*,*dns*,*ldap*`
2. List the export rules on the denying policy that reports access failure.
   `Cluster1::> vserver export-policy rule show -vserver <vserver> -policyname <policy name>`
3. Confirm that there is a rule listed that grants this client access, if it does not exist, then create a rule.
   `Cluster1::> vserver export-policy rule create`

If there is an export-policy rule that should grant access

1. If the rule is by IP or subnet
   - Confirm that the IP and netmask encompass the client's IP
   - For a rule for all hosts (0.0.0.0), confirm that there is a /0 at the end to encompass all hosts
2. If the export policy rule is by hostname:
   - Confirm that the hostname in the rule resolves to the expected IP
     (in diag privilege level) `Cluster::*> vserver services name-service getxxbyyy gethostbyname -node <node> -vserver <vserver> -hostname <hostnname>`
     If this resolves to the wrong IP, move to the Name Services Troubleshooting section below.
3. If the export policy rule is by DNS domain name
   - Confirm that the rule for the domain name is prepended with a '.' to indicate that it is a domain.
     - If not, edit the rule to reflect the correct syntax.
4. Confirm if the client IP resolves to the correct hostname by checking the PTR record in DNS:
   (in diag privilage level) `Cluster::> vserver services name-service getxxbyyy gethostbyaddr -node <node> -vserver <vserver> -ipaddress <clientip>`

If this does not resolve to the correct hostname, move to the Name Services Troubleshooting section below.

5. If the export policy rule is by netgroup:
    1. Confirm the name service source(s) being used
       `Cluster::> ns-switch show -vserver <vserver> -database netgroup`
    2. If LDAP is one of the sources, determine if `netgroup.byhost` is enabled
       `Cluster::> ldap client show -client-config jason.local -fields is-netgroup-byhost-enabled`
        1. If the netgroup source is files, NIS, or LDAP with `netgroup.byhost` enabled:
            - Confirm that client resolves with `netgroup.byhost` lookup
              (in diag privilage level) `Cluster::> getxxbyyy netgrpbyhost -node <node> -vserver <vserver> -netgroup <netgroup> -client <ip>`
            - If the source is LDAP with without `netgroup.byhost` enabled
              Confirm that the client is in the netgroup with a netgroup lookup.
              (in diag privilage level) `Cluster::>getxxbyyy netgrp -node <node> -vserver <vserver> -netgroup <netgroup> -client <ip>`
    3. If the client did appear in the previous netgroup lookup, clear the netgroup cache and re-run the appropriate check-access command:
       `Cluster::>export-policy cache flush -vserver <vserver> -cache netgroup`
    4. If the client did not appear in the netgroup with the `getxxbyyy` command:
       Confirm that the client IP resolves to the correct hostname
       (in diag privilage level) `Cluster::>getxxbyyy gethostbyaddr -node <node> -vserver <vserver> -ipaddress <clientip>`
    5. If the IP does not resolve correctly, move to the Name Services Troubleshooting section below.
    6. If the IP resolve correctly, confirm that the name matches the entry in the netgroup file

If it was determined that the netgroup lookup would be `netgroup.byhost`, not only must the name match; however, it is case sensitive.

If it was determined that the netgroup lookup would not use the byhost functionality, case is not sensitive; however, it is best to match case.

1. If the hostname does not match the entry in netgroup (does not exist or is mistyped), update the netgroup.
2. If the netgroup source is Files, ensure a current copy of the netgroup files is uploaded to the controller.
3. Clear the current netgroup cache:
   `export-policy cache flush -vserver trusts -cache netgroup`
4. Clear the Access Cache:
   (in diag privilage level) `Cluster::>nblade access-cache flush -vserver <vserver> -node <node> -policy <policy> -address <clientIP>`
5. Reattempt the check-access operation

If the hostname matches what is in the netgroup, clear the secd netgroup caches by running the following commands::

- (in diag privilage level) `Cluster1::*>secd cache clear -node <node> -vserver <vserver> -cache-name netgroup-ip`
- (in diag privilage level) `Cluster1::*>secd cache clear -node <node> -vserver <vserver> -cache-name netgroup-host`
- (in diag privilage level) `Cluster1::*>secd cache clear -node <node> -vserver <vserver> -cache-name ldap netgroupname-to-member`

Name Services Troubleshooting

Name services troubleshooting for DNS, NIS and LDAP all follow the same steps:

1. Verify the SVM or vserver configuration
2. Determine if the name service has the correct entries
3. Verify network connectivity

DNS Troubleshooting

1. Confirm if the DNS settings are correct:
   `Cluster1::> vserver services name-service dns show -vserver <vserver>`
2. Determine if there are any errors reported in the EMS event log and take the specified corrective action
   `Cluster1::> event log show -message-name *dns*`
   `Cluster1::> event route show -message-name <EMS event name> -instance`

   For example:
   ```
   Cluster1::> event route show -message-name dns.server.timed.out -instance
   Message Name: dns.server.timed.out
   Severity: WARNING
   Corrective Action: Make sure that the DNS server is up and running and that
   there are no networking issues preventing the Vserver from communicating
   with the DNS server.
   Description: This message occurs when the DNS server fails to respond to a
   query and timeout occurs.
   ```
3. Check network connectivity using the steps outlined the section Network Connectivity Checking.
4. If troubleshooting `getxxbyyy gethostbyname`, investigate the DNS server to ensure it has the correct A record for this client
5. If troubleshooting `getxxbyyy gethostbyaddr`, investigate the DNS server to ensure it has the correct PTR record for this client.

DNS Statistics

Statistics for DNS communications can be viewed per SVM and are useful for determining overall response times for DNS lookups. It is typical to expect DNS average round trip times (RTT) to closely match the network

latency; however, unusually large RTTs can be observed when the DNS servers are heavily loaded, or there is packet loss between the SVM LIFs and the DNS servers. In `priv advanced` mode, run the `dns info` command to view the descriptive statistics:

```
cluster1::*> dns info

Node: node_a

          Name     Average   Minimum   Maximum    Total      Num  Host Not
Timed   Other  Format  Servfail  NotImp  Refused
Vserver   Server  RTT (us)  RTT (us)  RTT (us)  RTT (s)  Queries     Found
Out  Errors  Errors    Errors  Errors   Errors
--------  ------  --------  --------  --------  -------  -------  --------
-----  ------  ------  --------  ------  -------
my_svm     10.61.81.53    0         0         0        0        0
0      0       0       0         0       0        0
cluster    10.61.79.2   828       411       7646        0      880
878      0       0       0         0       0        0
```

On 9.0 and later, the DNS statistic can be found in Counter Manager under the object external_service_op

```
Cluster1::>  statistics start -object external_service_op -sample-id
dns_sample1
```

For more information about collection DNS statistics, see document: Displaying DNS statistics

```
Cluster::*> dns show
                                                                  Name
Vserver         State     Domains                                 Servers
--------------- --------- --------------------------------------- ----------------
cluster1        enabled   demo.netapp.com                         192.168.0.253
```

NIS Troubleshooting

1. Confirm if the NIS settings are correct:
   `Cluster::> 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 -message-name *nis*`
   `event route show -message-name <EMS event name> -instance`

For example:

```
::> event route show -message-name 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

NIS Statistics

Statistics for NIS communications can be viewed per SVM and are useful for determining overall response times for NIS lookups. It is typical to expect NIS average round trip times (RTT) to closely match the network latency; however, unusually large RTTs can be observed when the NIS servers are heavily loaded, or there is packet loss between the SVM LIFs and the NIS servers. In `priv advanced` mode, run the `nis info` command to view the descriptive statistics.

```
Cluster1::*> nis info
  (nis-domain)

Node: node_a

        NIS     Number of    Total   Minimum   Maximum   Average    Number of
Entry Not
Vserver Server YP Lookups  RTT (s)  RTT (us)  RTT (us)  RTT (us)
Retransmits      Found
------  ------ ----------  -------  --------  --------  --------  -----------
---------
my_svm  10.60.252.15    0        0         0         0         0
0          0
```

On 9.1 there is no nis info use nis show.

LDAP Troubleshooting

1. Confirm if the NIS settings are correct:

```
Cluster1::> ldap show -vserver <vserver>
Cluster1::>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:
```
Cluster1::> event log show -message-name *ldap*
Cluster1::> event route show –messagename <EMS event name>
```

For example:
```
Cluster1::> event route show -message-name 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 the section Network Connectivity Checking.

LDAP Statistics

(in diag privilege level) `Cluster1::*>  diag secd connections show -node node2 -vserver SVM`

```
[ Cache: LDAP (NIS & Name Mapping)/<no key> ]
 Queue> Waiting: 0, Max Waiting: 1, Wait Timeouts: 0, Avg Wait: 0.00ms
 Performance> Hits: 4, Misses: 1, Failures: 0, Avg Retrieval: 0.60ms

+ Rank: 01 - Server: 10.228.225.120 (10.228.225.120)
         Connected through the 10.63.21.9 interface, 0.0 mins ago
         Used 5 time(s), and has been available for 2 secs
         RTT in ms: mean=8.60, min=2, max=22, med=4, dev=7.58 (0.0 mins of
data)
```

Name Services Troubleshooting Cluster Shell commands

The `getxxbyyy` command is used for querying name service. When used in conjunction with `-show-source true`, the command displays the `ns-switch` source that is being used for the `query`. `getXXbyYY` is an advanced privilege command, and has the following query types:

1. `getaddrinfo |gethostbyname`: Convert hostname to IPv4/6
```
cluster::*> getxxbyyy getaddrinfo -node node01 -vserver Svm -hostname
support.netapp.com -show-source true
Source used for lookup: DNS
Host name: support.netapp.com
Canonical Name: support.netapp.com
```

```
IPv4: 216.240.21.18
IPv6: 2620:10a:4005:c000::a78:2d11
```

2. `getnameinfo | gethostbyaddr`: Convert IP address to hostname

```
cluster::*> getxxbyyy getnameinfo -node node01 -vserver Svm -ipaddress
216.240.21.18 -show-source true
Source used for lookup: DNS
IP address: 216.240.21.18
Host name: support.netapp.com
```

3. `getgrbygid`: Get group info as members by GID

```
cluster::*> getxxbyyy getgrbygid -node node01 -vserver Svm -groupID 1000
-show-source true
Source used for lookup: Files
name: wheatley
gid: 1000
gr_mem:
```

4. `getgrbyname`: Get group members by name

```
cluster::*> getxxbyyy getgrbyname -node node01 -vserver Svm -groupname
daemon -show-source true
Source used for lookup: Files
name: daemon
gid: 1
gr_mem:
```

5. `getgrlist`: Get groups to which a user belongs

```
cluster::*> getxxbyyy getgrlist -node node01 -vserver Svm -username root
-show-source true
Source used for lookup: Unknown
pw_name: root
Groups: 0

cluster::*> getxxbyyy getgrlist -node node01 -vserver Svm -username user1
-show-source true
Source used for lookup: Files
pw_name: user1
Groups: 1000
```

6. `getpwdbyname | getpwbyuid`: Get a user's info by name | uid

```
cluster::*> getxxbyyy getpwbyname -node node01 -vserver Svm -username user1
-show-source true
Source used for lookup: Files
```

```
pw_name: user1
pw_passwd: *
pw_uid: 1000
pw_gid: 1000
pw_gecos:
pw_dir:
pw_shell:

cluster::*> getxxbyyy getpwbyuid -node node01 -vserver Svm -userID 60001
-show-source true
Source used for lookup: Files
pw_name: dubsquash
pw_passwd: *
pw_uid: 60001
pw_gid: 60001
pw_gecos:
pw_dir:
pw_shell:
```

7. `netgrp | netgrpbyhost:` Check netgroup membership using the netgroup | `netgroup.byhost` API

```
cluster::*> getxxbyyy netgrp -node node01 -vserver Svm -netgroup group1
-client myclient -show-source true
Source used for lookup: NIS
myclient is a member of group1


cluster::*> getxxbyyy netgrpbyhost -node node01 -vserver Svm -netgroup
group1 -clientIP 172.18.162.242 -show-source true
Success
Hostname resolved to: myclient.netapp.com
Source used for lookup: NIS


cluster::*> getxxbyyy netgrpbyhost -node node01 -vserver Svm -netgroup
group2 -clientIP 172.18.162.242 -show-source true
netgroup not found in netgroup.byhost lookup in all the configured sources
Hostname resolved to: myclient.netapp.com
Source used for lookup: Unknown
```

EMS Events

The Event Manager System (EMS) records system events that often point to the source of the problem. Users might subscribe to events as well as view events for the entire cluster. For more information on configuring notifications, see Technical Report 4303 Logging in Clustered Data ONTAP.

Users might view the event log by running the `event log show` command and might view specific events description and corrective action by running the following command:
`event route show –messagename <message_name> -instance`

The following events are a short selection those most commonly associated with exports and name services configuration issues:

- **AccessCache.NearLimits:** This message occurs when the access cache module is near its limit for entries or export rules.
- **AccessCache.ReachedLimits:** This message occurs when the access cache module reaches its limit for the entries or export rules.
- **dns.server.timed.out:** This message occurs when the Domain Name Service (DNS) server fails to look up a service name.
- **exports.hostname.notFound**
- **exports.host.data.notFound**
- **exports.host.clus.notFound**
- **exports.host.notFound**: This message occurs when the forward lookup record mapping a host name to its IP address is not found in the configured name servers in a Vserver. This record must be present to evaluate the export-policy rule that has a host name in its clientmatch entry.
- **exports.hostname.transient**
- **exports.host.transient**
- **exports.host.data.transient**
- **exports.host.clus.transient:** This message occurs when a host named in a clientmatch entry of an export-policy rule is not resolved to an IP address using the configured name servers in a data Vserver.
- **export.dns.config:** This message occurs when a name service lookup request finds that DNS is configured as an ns-switch source for hosts, but DNS is not configured for the Vserver.
- **exports.dom.clus.notFound**
- **exports.dom.notFound:** This message occurs when the reverse lookup record mapping an IP to its hostname cannot be found in the configured name servers.
- **exports.dom.data.transient**
- **exports.dom.clus.transient**
- **exports.dom.transient**: This message occurs when reverse lookup of the IP address of a client using the configured name servers in a data Vserver is unsuccessful for an export-policy rule that uses the domain name in clientmatch.

- **exports.netgroup.dnsNoPtrRec**: This message occurs when the reverse lookup record mapping an IP address to its hostname cannot be found in the configured name servers. This record must be present to evaluate the membership of a hostname in the netgroup named in the clientmatch of an export-policy rule.
- **exports.netgroup.notFound**: This message occurs when a netgroup named in a clientmatch of an export-policy rule is not found in the configured name servers.
- **exports.netgroup.partial**: This message occurs when partial netgroup results are returned by the name services because of errors in the netgroup mapping.
- **exports.ngbh.allFailed**: This message occurs when a netgroup by host request fails because all ns-switch sources for the netgroup database have returned connection errors and files are unusable as a source.
- **Nblade.exportAccessIndeterm**: This message occurs when client access cannot be evaluated because of an error while matching the client against export rules.
- **netgroup.files.missing**: This message occurs when a netgroup lookup request finds that files is specified as a ns-switch source, but a netgroup file cannot be found
- **netgroup.ldap.byhost.missing**: This message occurs when netgroup.byhost is disabled in the Lightweight Directory Access Protocol (LDAP) client configuration on the storage system, and LDAP is configured as an ns-switch source for the Vserver. Enabling netgroup.byhost enables mount operations to succeed faster when the netgroup size is large.
- **netgroup.ldap.config**: This message occurs when a netgroup lookup request finds that Lightweight Directory Access Protocol (LDAP) is specified as a ns-switch source, but LDAP is not configured for the Vserver. Netgroup lookups using LDAP will not function.
- **netgroup.nis.byhost.decode**: This message occurs when the netgroup.byhost remote procedure call to the Network Information Service (NIS) server returns a response that cannot be decoded.
- **netgroup.nis.byhost.missing**: This message occurs when the netgroup.byhost map is not configured on the Network Information Service (NIS) server and NIS is configured as a ns-switch source for the Vserver. Enabling netgroup.byhost enables mount operations to succeed faster when the netgroup size is large.
- **netgroup.nis.config**: This message occurs when a netgroup lookup request finds that Network Information Service (NIS) is specified as a ns-switch source, but NIS is not configured for the Vserver. Netgroup lookups using NIS will not function.
- **nis.server.not.available**: This message occurs when none of the NIS servers configured for a Storage Virtual Machine can be contacted.
- **secd.authsys.lookup.failed**: This message occurs when the incoming UNIX user ID (UID) that tries to mount or access a mount point cannot be looked up in any of the name-services (NIS, LDAP, file).
- **secd.dns.server.timed.out**: This message occurs when the DNS server fails to respond to a query and timeout occurs.
- **secd.dns.srv.lookup.failed**: This message occurs when the Domain Name Service (DNS) server fails to look up a service name.
- **secd.ldap.query.timed.out**: This message indicates that the Lightweight Directory Access Protocol (LDAP) server is not responding to requests in the expected time frame.
- **secd.ldap.noServers**: This message occurs when the server could not establish a TCP connection to a Network Information Service (NIS) server.
- **secd.ldap.connectFailure**: This message occurs when the server could not establish a TCP connection to a Network Information Service (NIS) server.

- **secd.netgroup.ldap.badFilter**: This message occurs if the filter for searching the Lightweight Directory Access Protocol (LDAP) server is found to be invalid. The typical reason for this issue is incorrect LDAP client configuration or a bad netgroup name. Searching for the current netgroup is skipped, so all hosts in the netgroup might not be authorized.
- **secd.ldap.slowServer**: This message indicates that the Lightweight Directory Access Protocol (LDAP) server is not responding to requests in the expected time frame.
- **secd.nfsAuth.problem**: This message occurs when an NFS authorization attempt fails.
- **secd.noNetgroupFile**: This message occurs when trying to process a netgroup in an export policy while the Vserver 'ns-switch' option is set exclusively to 'file' but no netgroup file is loaded. Client requests cannot be processed until a netgroup file is loaded or another name service is added to the Vserver 'ns-switch' option.
- **secd.nis.noServers**: This message occurs when none of the configured Network Information Service (NIS) servers are accepting connections.
- **secd.nis.connectFailure:** This message occurs when the server could not establish a TCP connection to a Network Information Service (NIS) server.
- **secd.nis.slowServer**: This message occurs when the server could not establish a TCP connection to a Network Information Service (NIS) server.
- **secd.unexpectedFailure**: This message occurs when the security daemon captures an unexpected failure. This is a generic event indicating many possible different failures with name services. The event is posted with a long description indicating the specific detail of the unexpected failure.

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 node/port on which it resides

```
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

1. 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)
2. 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 attempt 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 might 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 might 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. The `netstat -an` command 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 might 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 would 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 suspected, check for `ipfiler.ReachedMaxStates` in the EMS event log.

```
cluster::> event route show -message-name 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

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

Additional Information

- Error messages such as `access denied by server while mounting` are common indicators of export policy rule violations