Abstract

This troubleshooting guide helps you troubleshoot issues in your physical networking environment. If you are unable to connect to a node, the problem might be related to your InfiniBand switch, down or unstable interfaces, the configuration of the node and its network interfaces, routing, or client connectivity.

September 26, 2017
Contents and overview

1. Follow these steps.

   - Before you begin
     [Page 3]

2. Perform troubleshooting steps in order.

   - Start troubleshooting / Problem assessment
     [Page 4]
   - Routing and client connectivity
     [Page 10]
   - Check the cluster network configuration
     [Page 16]
   - Test connectivity between the cluster and the gateway
     [Page 20]
   - Troubleshoot connections to the external network
     [Page 22]

3. Appendixes

   - Appendix A
     If you need further assistance
   - Appendix B
     How to use this flowchart
   - Appendix C
     Example output
   - Appendix D
     Example output
   - Appendix E
     Example output

Note
Follow all of these steps, in order, until you reach a resolution.

Before you begin

**CAUTION!**
If the node, subnet, or pool that you are working on goes down during the course of troubleshooting and you do not have any other way to connect to the cluster, you could experience data unavailability.

Therefore, make sure that you have more than one way to connect to the cluster before you start this troubleshooting process. The best method is to have a serial console connection available. This way, if you are unable to connect through the network, you will still be able to connect to the cluster physically.

For specific requirements and instructions for making a physical connection to the cluster, see [article 304071](http://bit.ly/isidocfeedback) on the EMC Online Support site.

Before you begin troubleshooting, confirm that you can connect through either another subnet or pool, or that you have physical access to the cluster.

---

**Configure screen logging through SSH**

We recommend that you configure screen logging to log all session input and output during your troubleshooting session. This log file can be shared with Isilon Technical Support, if you require assistance at any point during troubleshooting.

**Note:** The screen session capability does not work in OneFS 7.1.0.6 and 7.1.1.2. If you are running either of these versions, you can configure logging by using your local SSH client’s logging feature.

1. Open an SSH connection to the cluster and log in by using the root account.
   
   **Note:** If the cluster is in compliance mode, use the compadmin account to log in. All compadmin commands must be preceded by the `sudo` prefix.

2. Change the directory to `/ifs/data/Isilon_Support` by running the following command:

   ```
   cd /ifs/data/Isilon_Support
   ```

3. Run the following command to capture all input and output from the session:

   ```
   screen -L
   ```

   This will create a file named `screenlog.0` that will be appended to during your session.

4. Perform troubleshooting.
Start troubleshooting / Problem assessment

Introduction
Start troubleshooting here. For an overview of the conventions used in this flowchart, see Appendix B: How to use this flowchart.

If you have not done so already, log in to the cluster and configure logging through SSH, as described on Page 3.

Note
Throughout this troubleshooting guide, we will refer to the node that you cannot connect to as "the problem node."

If there are multiple problem nodes, choose one of the problem nodes and perform all of the troubleshooting steps on that same node.

Can you ping the problem node from a client?
Yes

Can the client ping another node in the cluster?
Yes → Go to Page 5
No → Go to Page 7

Note the page number that you are currently on. Upload log files and contact Isilon Technical Support, as instructed in Appendix A.
OPTIONAL WORKAROUND

If the problem affects a single node that is in production and is affecting users, you can perform a workaround to suspend the node in SmartConnect so that clients trying to connect will be given access to a working node. If the problem node is in multiple pools, you might need to run this command for every pool that contains this node.

To perform this workaround, you need to know the subnet and pool that contain the problem node. If you do not know these things, see the instructions on Page 6.

To perform the workaround, run the following command, where <LNN> is the logical node number of the problem node.

OneFS 8.0.0 and later

    isi network pools sc-suspend-nodes <groupnet_name>.<subnet_name>.<pool_name> <LNN>

For example, the following command suspends node 2:

    isi network pools sc-suspend-nodes groupnet0.subnet0.pool. 2

OneFS 7.2.1 and earlier

    isi networks modify pool --name=<subnet>:<pool> --sc-suspend-node <LNN>

For example:

    isi networks modify pool --name=subnet0:pool0 --sc-suspend-node 2

After you run the command, continue troubleshooting.

IMPORTANT: After the problem is resolved, remember to end the suspension of the node by running the following command:

OneFS 8.0.0 and later

    isi network pools sc-resume-nodes <groupnet_name>.<subnet_name>.<pool_name> <LNN>

OneFS 7.2.1 and earlier

    isi networks modify pool --name=<subnet>:<pool> --sc-resume-node <LNN>
Problem assessment (3)

You could have arrived here from:
- Page 5 - Problem assessment (2)

---

**DETERMINE THE IP ADDRESS, AND SUBNET:POOL OF THE PROBLEM NODE**

Run the following command for your version of OneFS:

**OneFS 8.0.0 and later**

```bash
isi network pools list -v
```

**OneFS 7.2.1 and later**

```bash
isi networks list pools -v
```

Example output is shown in Appendix E. Look at the Ranges for each listed subnet:pool and find which range contains the IP address of the problem node.

In the example output, if the IP address of the problem node is 10.1.1.3, the subnet:pool would be subnet0:pool0.

---

Go back to Page 5
Run the following command:

```
isi status -q
```

Look in the **Health** DASR column for the problem node and see if the node reports as `D--` (Down).

See Appendix C for example output.

---

**IDENTIFY THE IP ADDRESS OF THE PROBLEM NODE**

From the output of the `isi status -q` command that you just ran, identify the IP address of the problem node. You will use this later.

---

**Is the problem node down?**

Yes

Note the page number that you are currently on. Upload log files and contact Isilon Technical Support, as instructed in Appendix A.

No

Go to Page 8
Problem assessment (5)

You could have arrived here from:

- Page 7 - Problem assessment (4)

---

Did you previously remove the problem node from the IP address pool?

- Yes
  - Either add the node back to the original IP address pool, or create a separate subnet and test pool and add the problem node to the test subnet or pool.
  
  **Note:**
  If you are not able to work in a production environment, use a test subnet or pool. A test subnet or pool will enable you to make changes without affecting your production environment.

- No
  - Go to Page 9
Problem assessment (6)

You could have arrived here from:
- Page 8 - Problem assessment (5)

Did you receive any of the following alerts or events on the cluster:
- Aggregate network link {ifname} error, interface(s) down: {phys_ifaces}
- External network link {ifname} down
- Multiple external network problems detected

If yes, this indicates a problem outside the cluster. Go to Page 22.

If no, go to Page 10.
Routing and client connectivity

Ping the problem node from the node itself

Try to connect to the problem node through an external interface by using an SSH client such as PuTTY.

If that fails, connect to a different node in the cluster and then open an SSH connection to the problem node through the internal network by running the following command, where `<cluster name>` is the name of the cluster and `<LNN>` is the logical node number of the problem node:

```
ssh <cluster name>-<LNN>
```

If you are still unable to connect, try to connect to the problem node via a serial cable. For instructions, see *Isilon: How to connect to the management port of a node*, 304071.

Ping from the problem node to the node itself by using the IP address you identified on *Page 7* as the IP address you cannot connect to:

```
ping <IP address>
```

Did the ping succeed?

- Yes
  - Go to Page 11

- No
  - Note the page number that you are currently on. Upload log files and contact Isilon Technical Support, as instructed in *Appendix A*.
Routing and client connectivity (2)

Ping another node from the problem node

You could have arrived here from:
- Page 9 - Problem assessment (6)
- Page 10 - Ping the problem node from itself

Ping another node IP address in the same subnet. To see a list of the external IP addresses of all pool members, run the following command for your version of OneFS:

**OneFS 8.0.0 and later**

isi network interfaces list

**OneFS 7.2.1 and earlier**

isi networks list interfaces --wide

Then run the following command to ping the node:

```
ping <external IP address>
```

Did the ping succeed?

- **Yes**
  - Go to Page 12

- **No**
  - The interface is up, but it cannot ping to another node on the same subnet. The issue is on your external network. Contact your networking team.

Gather the Isilon configuration details to provide to your networking team by running the following commands for your version of OneFS:

**OneFS 8.0.0 and later**

isi network subnets list -v

isi network pools list -v

**OneFS 7.2.1 and earlier**

isi networks list subnets -v

isi networks list pools -v

End troubleshooting
Routing and client connectivity (3)

Determine the subnet

Determine the subnet that contains the IP address of the problem node by running the following command for your version of OneFS:

OneFS 8.0.0 and later

isi network pools list -v

OneFS 7.2.1 and earlier

isi networks list pools -v

See Appendix E for example output from both commands.

Look at the Ranges for each listed subnet and find which range contains the IP address of the problem node. In the example output, if the IP address of the problem node is 10.1.1.3, the subnet would be subnet0.
Routing and client connectivity (4)

Ping the subnet gateway from the problem node

DETERMINE THE SUBNET GATEWAY

Determine the subnet gateway of the problem node by running the following command for your version of OneFS:

**OneFS 8.0.0 and later**

isi network subnets list

**OneFS 7.2.1 and earlier**

isi networks list subnets

The command returns one line for every subnet and looks similar to the following. In the **Name** column, find the subnet that you determined in the previous step. The subnet gateway is listed in the **Gateway:Prio** column. In this example, where the subnet is subnet0, the subnet gateway is 10.1.1.1.

<table>
<thead>
<tr>
<th>Name</th>
<th>Subnet</th>
<th>Gateway:Prio</th>
<th>SC Service Pools</th>
</tr>
</thead>
<tbody>
<tr>
<td>subnet0</td>
<td>10.1.1.0/22</td>
<td>10.1.1.1:1</td>
<td>0.0.0.0</td>
</tr>
</tbody>
</table>

From the node: Ping the node's subnet gateway by running the following command, where `<subnet gateway>` is the IP address of the subnet gateway that you determined in the previous step:

```
ping -c3 <subnet gateway>
```

For example, using the output above, you would run:

```
ping -c3 10.1.1.1
```

Did the ping succeed?

Yes

Go to Page 14

No

Go to Page 15
Routing and client connectivity (5)
Ping the subnet gateway from the client

From the client that cannot connect to the node, ping the same subnet gateway of the node that you pinged on the previous page:

```
ping <subnet gateway>
```

Did the ping succeed?

- Yes:
  - This indicates a network configuration issue.
  - Gather routing table information by running the following command:
    ```
    netstat -rn
    ```
  - Note the page number that you are currently on.
  - Upload log files and contact Isilon Technical Support, as instructed in Appendix A.

- No:
  - This indicates an issue with your external network.
  - Contact your networking team for assistance.

End troubleshooting
Routing and client connectivity (6)

Ping the subnet gateway from the client (2)

From the client that cannot connect to the node, ping the same subnet gateway of the node:

ing <subnet gateway>

Did the ping succeed?

Yes

Go to Page 16

No

This indicates an issue with your external network. Contact your networking team for assistance.

End troubleshooting
Check the cluster network configuration

You could have arrived here from:
- Page 15 - Ping the subnet gateway from the client

Page 16

Compare your cluster network configuration to the "Networking" section of the OneFS Web Administration Guide for your version of OneFS to make sure the cluster is set up correctly.

Is your cluster configured correctly?

No

Configure your cluster according to the best practices in the "Networking" section of the OneFS Web Administration Guide.

Is your original issue resolved?

No

End troubleshooting.

Yes

Ask your local network administrator to confirm that the VLAN tag numbers are the same on both the subnet for the cluster and the switch ports that connect to that physical interface. Record the VLAN tag numbers in case you need to contact Isilon Technical Support.

Go to Page 17

Is your cluster configured correctly?

Yes

End troubleshooting.

16 - EMC Isilon Customer Troubleshooting Guide: Clients Cannot Connect to a Node

For links to all Isilon customer troubleshooting guides, visit the Customer Troubleshooting - Isilon Info Hub. We appreciate your help in improving this document. Submit your feedback at http://bit.ly/isi-docfeedback.
Check the cluster network configuration (2)

Verify the subnet and the external IP address

From the OneFS command-line interface of the problem node, run the following command:

```
ifconfig
```

Using the `ifconfig` output, confirm that the cluster external network IP addresses are configured correctly:

- **For 1 GbE connections**, make sure that the subnet mask is correct and that the external network IP address is configured on interface `em0, em1, em2, em3, igb0, igb1, igb2, or igb3`.

- **For 10 GbE connections**, make sure that the subnet mask is correct and that the external network IP address is configured on interface `cxgb0, cxgb1, ix0, or ix1`.

For additional information, see How to map OneFS Flexnet single and aggregate interface designations to BSD interface designations, 304455.

Are the subnet mask and external network IP address configured correctly?

- **No** → Go to Page 18
- **Yes**

Is the client connectivity issue resolved now?

- **No** → Go to Page 19
- **Yes**

End troubleshooting

---

For links to all Isilon customer troubleshooting guides, visit the Customer Troubleshooting - Isilon Info Hub. We appreciate your help in improving this document. Submit your feedback at http://bit.ly/si-docfeedback.
Check the cluster network configuration (3)

Reconfigure external networking

You could have arrived here from:

- Page 17 - Verify the subnet and the external network IP address

Reconfigure your external networking to provide external access. Refer to the "Configuring an external network" section of the OneFS Web Administration Guide for your version of OneFS.

Is the client connectivity issue resolved now?

Yes

End troubleshooting

No

Go to Page 19
Check the cluster network configuration (4)

Get the name of the problem interface

Determine the name of the problem interface by running the following command, where `<nodeIP>` is the IP address of the problem node:

```
ifconfig | egrep '((RUNNING|<nodeIP>)' | grep -Bl inet
```

The output is two lines of text, preceded by the name of the problem interface. In this example, the interface is `igb0`.

```
igb0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
      inet 10.1.1.3 netmask 0xfffffc00 broadcast 10.1.3.255 zone 1
```

Go to Page 20
Test connectivity between the cluster and the gateway

Open two SSH connections to the same node that you have been using (one to watch the packet capture and the other to ping the subnet gateway) and log on by using the root account.

**From the first SSH window**, run the following command, where `<problem interface>` is the name of the problem interface that you determined on the previous page, and `<subnet gateway>` is the IP address of the subnet gateway that you determined from the `isi networks list subnets` command on **Page 13**.

```
tcpdump -n -i <problem interface> icmp or arp and host <subnet gateway>
```

For example:
```
tcpdump -n -i igb0 icmp or arp and host 10.1.1.1
```

**From the second SSH window**, run the following command to ping the subnet gateway, where `<subnet gateway>` is the same subnet gateway that is used in the first SSH window:

```
ping -c3 <subnet gateway>
```

Monitor the first SSH window to verify that both the request and the response are visible in the packet capture. See **Appendix D** for an example of the tcpdump output.
Test connectivity between the cluster and the gateway (2)

In the first window, do you see both the request and the response?

Yes

End the capture by pressing CTRL+C.

Connectivity between the cluster and the gateway has been confirmed. This indicates that the issue is outside the gateway.

Your local networking team should address this issue.

Provide a copy of the tcpdump output to your network team.

End troubleshooting

No

End the capture by pressing CTRL+C.

There might be an issue with the cables, SFP module, or port.

Go to Page 22
Troubleshoot connections to the external network

Verify the interface and cable type

You could have arrived here from:

- Page 9 - Problem assessment (6)
- Page 21 - Test connectivity between the cluster and the gateway

Is the problem interface 1 GbE or 10 GbE?

1 GbE

Go to Page 23

10 GbE

Is the cable that is connected to the problem interface copper or fiber-optic?

Copper

Go to Page 23

Fiber-optic

Go to Page 24

Note
Detachable SFP modules are used only for 10 GbE connections using a fiber-optic cable.
Troubleshoot connections to the external network (2)

Replace the copper cable

You could have arrived here from:
- Page 22 - Verify the interface and cable type

Replace the cable from the down interface. Make sure that the cable is not kinked or folded, and that it is loosely draped.

Can you connect to the node now?

Yes
- End troubleshooting.

No
- Go to Page 27

For links to all Isilon customer troubleshooting guides, visit the Customer Troubleshooting - Isilon Info Hub. We appreciate your help in improving this document. Submit your feedback at http://bit.ly/isi-docfeedback.
Troubleshoot connections to the external network (3)

Verify the fiber-optic cable is correct

Check the cables that you are using on the problem interface. Isilon fiber-optic cables connected to SFP modules require the following:

- Connector ends must be either LC-LC or LC-SC.
- The cable must be multimode optical fiber, either aqua or orange. We recommend aqua because it is optimized for Isilon usage (10 Gb laser-optimized 50/125 micrometer).

For more information about correct cable types, see Isilon: How to choose the type of fiber cable for a 10 Gb SFP module, article 471787.

Are you using the correct type of cable?

No

Go to Page 25

Yes

Go to Page 26

Not sure

Note the page number that you are currently on. Upload log files and contact Isilon Technical Support, as instructed in Appendix A.
Troubleshoot connections to the external network (4)

Replace the incorrect fiber-optic cable and SFP module

You could have arrived here from:
- Page 24 - Verify the fiber-optic cable is correct

Replace the incorrect cable with a cable of the correct type.

You might also need to replace the SFP module. Check the SFP module that you are using in the problem interface. The correct type of SFP module is an 850 nm wavelength SX SFP module. See the picture on this page.

Contact your sales representative for assistance.

Is the client connectivity issue resolved now?

Yes

End troubleshooting

No

Go to Page 27

Correct SFP module: 850 nm wavelength SX
Troubleshoot connections to the external network (5)

Replace the fiber-optic cable

You could have arrived here from:
- [Page 24 - Verify the fiber-optic cable is correct]

Replace the cable with a different cable of the correct type.

As a test, you may swap the cable from the problem interface with a cable of the correct type from a known good interface. If the cable is at fault, the known good interface should go down, and the problem interface should come up and stay up.

**Note:** Do not replace the SFP module at this time. If needed, we'll test the SFP module later.

Is the client connectivity issue resolved now?

- **Yes**
  - The original cable is bad. Discard the bad cable and use a cable of the correct type.
  - End troubleshooting

- **No**
  - Go to [Page 27]

The original cable is bad. Discard the bad cable and use a cable of the correct type.
Troubleshoot connections to the external network (6)

Check for an empty port on the network switch

You could have arrived here from:

- Page 23 - Replace the copper cable
- Page 25 - Replace the incorrect fiber-optic cable and SFP module
- Page 26 - Replace the fiber-optic cable

Is there an empty port on the external network switch that the node can be connected to?

Yes

- Go to Page 29

No

- Go to Page 28
Troubleshoot connections to the external network (7)

Swap ports on the external network switch

Why swap ports?
This step helps to determine whether the issue is caused by the cable or the port. If the cable is moved to a working port and the issue persists, the issue is with the cable. If the cable is moved and the issue does not persist, the issue is with the port.

Using the new cable, swap ports on the switch with the port of a known good interface, and then check both ports.

A "known good interface" can be any port on the switch that has a working node connected to it.

Does the nonworking port stay off, and does the known good port come on and stay on?

Yes

Return the known good connection to its previous state. Designate the nonworking port as "bad," following your local site practices, and do not use the port.

Make another connection on the switch for the node, or explore options for replacing the switch.

End troubleshooting.

No

Go to Page 30

You could have arrived here from:

- Page 27 - Check for an empty port on the network switch
Troubleshoot connections to the external network (8)

Move the cable on the external network switch

You could have arrived here from:
- Page 27 - Check for an empty port on the network switch

Take the new cable and move it to an empty port on the switch.

Run the following command several times and note the output in the status row of the down or intermittent interface over time:

```plaintext
ifconfig
```

Is the status active, and does it stay active (meaning that it does not change to no carrier)? See example output in the note box on this page.

- Yes
  - Designate the nonworking port as "bad," following your local site practices, and do not use the port.
  - End troubleshooting.
- No
  - Go to Page 30

---

**Example output**
The status is active, indicating that the interface is up and connected:

```
em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
  options=19b<RXCSUM, TXCSUM, VLAN_MTU, VLAN_HWTAGGING, VLAN_HWCSUM, TSO4>
  ether 68:05:ca:14:1c:e9
  media: Ethernet autoselect (1000baseTX <full-duplex>)
  status: active
```
Troubleshoot connections to the external network (9)

Check for an SFP module

You could have arrived here from:
- Page 28 - Swap ports on the external network switch
- Page 29 - Move the cable on the external network switch

Is the problem interface 10 GbE with a fiber-optic cable attached?

Yes

Check the SFP module you are using in the problem interface. The correct type of module is an 850 nm wavelength SX SFP module.

- See the picture on this page.

No

Note the page number that you are currently on.
Upload log files and contact Isilon Technical Support, as instructed in Appendix A.

Are you using the correct SFP module?

Yes

Go to Page 32

No

Go to Page 31
Troubleshoot connections to the external network (10)

Replace the SFP module

Replace the SFP module with one of the correct type.
Contact your Isilon sales representative for assistance.

Is the issue resolved?

Yes
End troubleshooting

No
Note the page number that you are currently on. Upload log files and contact Isilon Technical Support, as instructed in Appendix A.
Swap the SFP module

Swap the down SFP module with a known good SFP module (ideally, from the same node, if possible, to minimize production impact; however you can use an SFP module from any node).

**Note:** The interface with the known good SFP module will also go down during the swap. This test will take less than 5 minutes, but you might want to schedule this during a low-production time.

Is the client connectivity issue resolved now?

Yes

The original SFP module is either the wrong type or is no longer working.

Contact your Isilon sales representative to order a new SFP module.

No

End troubleshooting

Note the page number that you are currently on. Upload log files and contact Isilon Technical Support, as instructed in Appendix A.
Appendix A: If you need further assistance

Contact Isilon Technical Support

If you need to contact Isilon Technical Support during troubleshooting, reference the page or step that you need help with. This information and the log file will help Isilon Technical Support staff resolve your case more quickly.

Upload node log files and the screen log file to Isilon Technical Support

1. When troubleshooting is complete, in the command-line interface, type `exit` to end your screen session.
2. Gather and upload the node log set and include the SSH screen log file by using the command appropriate for your method of uploading files. If you are not sure which method to use, use FTP.

   **ESRS:**
   ```bash
   isi_gather_info --esrs --local-only -f /ifs/data/Isilon_Support/screenlog.0
   ```

   **FTP:**
   ```bash
   isi_gather_info --ftp --local-only -f /ifs/data/Isilon_Support/screenlog.0
   ```

   **HTTP:**
   ```bash
   isi_gather_info --http --local-only -f /ifs/data/Isilon_Support/screenlog.0
   ```

   **SMTP:**
   ```bash
   isi_gather_info --email --local-only -f /ifs/data/Isilon_Support/screenlog.0
   ```

   **SupportIQ:**
   Copy and paste the following command.
   **Note:** When you copy and paste the command into the command-line interface, it will appear on multiple lines (exactly as it appears on the page), but when you press `Enter`, the command will run as it should.
   ```bash
   isi_gather_info --local-only -f /ifs/data/Isilon_Support/screenlog.0 --noupload \ 
   --symlink /var/crash/SupportIQ/upload/ftp
   ```

3. If you receive a message that the upload was unsuccessful, refer to article 304567 on the EMC Online Support site for directions on how to upload files over FTP.
Appendix B: How to use this flowchart

Introduction
Describes what the section helps you to accomplish.

You could have arrived here from:
- Page 4 - Start Troubleshooting

Directional arrows indicate the path through the process flow.

Yes

Process step

Optional process step

End point

No

Process step with command:
command xyz

Go to Page #

Decision diamond

Note
Provides context and additional information. Sometimes a note is linked to a process step with a colored dot.

CAUTION!
Caution boxes warn that a particular step needs to be performed with great care, to prevent serious consequences.

Document Shape
Calls out supporting documentation for a process step. When possible, these shapes contain links to the reference document. Sometimes linked to a process step with a colored dot.

For links to all Isilon customer troubleshooting guides, visit the Customer Troubleshooting - Isilon Info Hub. We appreciate your help in improving this document. Submit your feedback at http://bit.ly/isi-docfeedback.
### Example output of `isi status -q`

Cluster Name: mycluster  
Cluster Health: [ ATTN]  
Cluster Storage:  
HDD: 238T (243T Raw)  
SSD Storage: 0 (0 Raw)  

VHS Size: 5.7T  
Used: 6.1G (< 1%)  
Avail: 238T (> 99%)  

<table>
<thead>
<tr>
<th>ID</th>
<th>IP Address</th>
<th>DASR</th>
<th>In</th>
<th>Out</th>
<th>Total</th>
<th>Used / Size</th>
<th>Used / Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.1.1.2</td>
<td>OK</td>
<td>765K</td>
<td>800K</td>
<td>1.6M</td>
<td>2.0G/81T(&lt; 1%)</td>
<td>L3: 2.2T</td>
</tr>
<tr>
<td>2</td>
<td>10.1.1.3</td>
<td>OK</td>
<td>0</td>
<td>24</td>
<td>24</td>
<td>2.0G/81T(&lt; 1%)</td>
<td>L3: 2.2T</td>
</tr>
<tr>
<td>3</td>
<td>10.1.1.4</td>
<td>-A--</td>
<td>0</td>
<td>16</td>
<td>16</td>
<td>2.0G/81T(&lt; 1%)</td>
<td>L3: 2.2T</td>
</tr>
</tbody>
</table>

Cluster Totals:  
|                | 765K| 800K| 1.6M| 238T(< 1%) | L3: 6.5T        |

Health Fields:  
- D = Down  
- A = Attention  
- S = Smartfailed  
- R = Read-Only
Appendix D: Example output

You could have arrived here from:

- Page 20 - Test connectivity between the cluster and the gateway

**Example output from**

tcpdump -n -i <problem interface> icmp or arp and host <subnet gateway>

```
cluster-2# tcpdump -n -i em1 icmp or arp and host 10.1.1.1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on em1, link-type EN10MB (Ethernet), capture size 300 bytes
03:40:27.489203 IP 10.1.1.3 > 10.1.1.1: ICMP echo request, id 60584, seq 0, length 64
03:40:27.489358 arp who-has 10.1.1.3 tell 10.1.1.1
03:40:27.489398 arp reply 10.1.1.3 is-at 00:0c:29:0f:fc:a1
03:40:27.489424 IP 10.1.1.1 > 10.1.1.3: ICMP echo reply, id 60584, seq 0, length 64
03:40:28.508960 IP 10.1.1.1 > 10.1.1.3: ICMP echo reply, id 60584, seq 1, length 64
03:40:28.508973 IP 10.1.1.3 > 10.1.1.1: ICMP echo request, id 60584, seq 1, length 64
```
Appendix E: Example output

You could have arrived here from:
- Page 6 - Problem assessment (3)
- Page 12 - Routing and client connectivity (3)

**Example output of isi networks pools list -v**

```
ID: groupnet0.subnet0.pool0
  Groupnet: groupnet0
  Subnet: subnet0
  Name: pool0
  Rules: rule0
  Access Zone: System
  Allocation Method: static
  Aggregation Mode: lacp
  SC Suspended Nodes: -
    Description: Default ext-1 pool
    Ifaces: 1:ext-1, 2:ext-1, 3:ext-1
    IP Ranges: 100.225.158.01-100.225.158.043
  Rebalance Policy: auto
  SC Auto Unsuspend Delay: 0
  SC Connect Policy: round_robin
  SC Zone: System
  SC DNS Zone Aliases: -
  SC Failover Policy: round_robin
  SC Subnet: subnet0
  SC TTL: 0
  Static Routes: -
```

**Example output of isi networks pools list -v**

```
subnet0:pool0 - Default ext-1 pool
  In Subnet: subnet0
  Allocation: Static
  Ranges: 1
    10.1.1.2-10.1.1.40
  Pool Membership: 1
    1:ext-1 (up)
  Aggregation Mode: Link Aggregation Control Protocol (LACP)
  Access Zone: System (1)
  SmartConnect:
    Suspended Nodes : None
    Auto Unsuspend ... 0
    Zone : N/A
    Time to Live : 0
    Service Subnet : N/A
    Connection Policy: Round Robin
```
For links to all Isilon customer troubleshooting guides, visit the Customer Troubleshooting - Isilon Info Hub. We appreciate your help in improving this document. Submit your feedback at http://bit.ly/isi-docfeedback.