SAN Configuration Guide
Chapter 1. Deciding whether to use the SAN Configuration Guide

This guide describes supported FC-NVMe, FC, and iSCSI topologies for connecting host computers to nodes, and lists supported limits for SAN components.

You should use this guide under the following circumstances:

If you want to create a basic SAN configuration using best practices, you should choose among the following documentation:

- FC configuration for Windows
  - FC express configuration for Windows
- FC configuration for ESX
  - FC express configuration for ESXi using VSC
- FC configuration for Red Hat Enterprise Linux
  - FC express configuration for Red Hat Enterprise Linux
- iSCSI configuration for Windows
  - iSCSI express configuration for Windows
- iSCSI configuration for ESX
  - iSCSI express configuration for EESXi using VSC
- iSCSI configuration for Red Hat Enterprise Linux
  - iSCSI express configuration for Red Hat Enterprise Linux

If you require additional configuration or conceptual information, you should choose among the following documentation:

- Basic SAN host provisioning including how to configure and manage LUNs, igroups, and targets in iSCSI networks and FC fabrics.
  - SAN Administration Guide
- Conceptual background for SAN host provisioning
  - ONTAP concepts
- Command reference
  - ONTAP Command man pages
Chapter 2. Considerations for iSCSI configurations

You should consider several things when setting up your iSCSI configuration.

- You can set up your iSCSI configuration with HA pairs.
  
  Direct connect or the use of Ethernet switches is supported for connectivity. You must create LIFs for both types of connectivity.

- You should configure one management LIF for every storage virtual machine (SVM) supporting SAN.

- Selective LUN mapping (SLM) limits the paths that are being utilized in accessing the LUNs owned by an HA pair.
  
  This is the default behavior for LUNs created with ONTAP releases.

- HA pairs are defined as the reporting nodes for the Active/Optimized and the Active/Unoptimized paths that will be used by the host in accessing the LUNs through ALUA.

- It is recommended that all SVMs in iSCSI configurations have a minimum of two LIF’s per node in separate Ethernet networks for redundancy and MPIO across multiple paths.

- You need to create one or more iSCSI paths from each node in an HA pair, using logical interfaces (LIFs) to allow access to LUNs that are serviced by the HA pair.
  
  If a node fails, LIFs do not migrate or assume the IP addresses of the failed partner node. Instead, the MPIO software, using ALUA on the host, is responsible for selecting the appropriate paths for LUN access through LIFs.

- VLANs offer specific benefits, such as increased security and improved network reliability that you might want to leverage in iSCSI.

Ways to configure iSCSI SAN hosts with HA pairs

You can configure the iSCSI SAN hosts to connect to dual-node or multi-node configurations by using either one or multiple IP switches. You should determine whether you want a single-switch configuration that is not completely redundant or a multi-switch configuration that is completely redundant.

You can configure iSCSI SAN hosts with HA pairs on direct-attached, single-network, or multi-network environments. HA pairs can have multiple iSCSI connections to each switch, but multipathing software that supports ALUA is required on each host. If there are multiple hosts, you can configure each host with a different operating system by checking the Lenovo Storage Interoperability Center (LSIC).

https://datacentersupport.lenovo.com/lsic

Direct-attachment

In a direct-attached configuration, one or more hosts are directly connected to the controllers.
Single-network HA pairs
In single-network HA pair configurations, one switch connects the HA pair to one or more hosts. Because there is a single switch, this configuration is not fully redundant.

Multi-network HA pairs
In multi-network HA pair configurations, two or more switches connect the HA pair to one or more hosts. Because there are multiple switches, this configuration is fully redundant.
Benefits of using VLANs in iSCSI configurations

A VLAN consists of a group of switch ports grouped together into a broadcast domain. A VLAN can be on a single switch or it can span multiple switch chassis. Static and dynamic VLANs enable you to increase security, isolate problems, and limit available paths within your IP network infrastructure.

When you implement VLANs in large IP network infrastructures, you derive the following benefits:

- Increased security. VLANs enable you to leverage existing infrastructure while still providing enhanced security because they limit access between different nodes of an Ethernet network or an IP SAN.
- Improved Ethernet network and IP SAN reliability by isolating problems.
- Reduction of problem resolution time by limiting the problem space.
- Reduction of the number of available paths to a particular iSCSI target port.
- Reduction of the maximum number of paths used by a host.

Having too many paths slows reconnect times. If a host does not have a multipathing solution, you can use VLANs to allow only one path.

Static VLANs

Static VLANs are port-based. The switch and switch port are used to define the VLAN and its members.

Static VLANs offer improved security because it is not possible to breach VLANs using media access control (MAC) spoofing. However, if someone has physical access to the switch, replacing a cable and reconfiguring the network address can allow access.

In some environments, it is easier to create and manage static VLANs than dynamic VLANs. This is because static VLANs require only the switch and port identifier to be specified, instead of the 48-bit MAC address. In addition, you can label switch port ranges with the VLAN identifier.
Dynamic VLANs

Dynamic VLANs are MAC address-based. You can define a VLAN by specifying the MAC address of the members you want to include.

Dynamic VLANs provide flexibility and do not require mapping to the physical ports where the device is physically connected to the switch. You can move a cable from one port to another without reconfiguring the VLAN.
Chapter 3. Considerations for FC-NVMe configurations

Beginning with ONTAP 9.4, the non-volatile memory express (NVMe) protocol is available for SAN environments. FC-NVMe allows you to run NVMe over an existing FC network with an AFA system. FC-NVMe uses the same physical setup and zoning practice as traditional FC networks but allows for greater bandwidth, increased IOPs and reduced latency than FC-SCSI.

- Beginning in ONTAP 9.6, volume move with mapped namespaces is supported.
  
  Volume move with mapped namespaces is not supported in ONTAP 9.5 or 9.4.

- Beginning in ONTAP 9.6, namespaces support 512 byte blocks and 4096 byte blocks.

  4096 is the default value. 512 should only be used if the host operating system does not support 4096 byte blocks.

- You can set up your FC-NVMe configuration with HA pairs using a single fabric or multifabric.

- NVMe is supported on AFA platforms that have 32G FC ports.

- Beginning with ONTAP 9.5 multipath HA pair failover/giveback is supported for NVMe configurations.

  Path failover/giveback is not supported in ONTAP 9.4.

- NVMe can be the only data protocol on the storage virtual machine (SVM).

- FC-NVMe can be the only data protocol on data LIFs.

- LUNs and namespaces cannot be mixed on the same volume.

- You should configure one management LIF for every SVM supporting SAN.

- The use of heterogeneous FC switch fabrics is not supported, except in the case of embedded blade switches.

  Specific exceptions are listed on Lenovo Storage Interoperability Center (LSIC).

- Cascade, partial mesh, full mesh, core-edge, and director fabrics are all industry-standard methods of connecting FC switches to a fabric, and all are supported.

  A fabric can consist of one or multiple switches, and the storage controllers can be connected to multiple switches.

The following applies only to nodes running ONTAP 9.4:

- NVMe LIFs and namespaces must be hosted on the same node.

- The NVMe service must be created before the NVMe LIF is created.

The following ONTAP features are not supported by NVMe configurations:

- NVMe namespace move

- NVMe namespaces (Copy on Demand)

- Creating namespaces on a volume transitioned from Data ONTAP.

- Sync

- Virtual Storage Console

- Application Aware (AppDM/Balanced Placement)

See Lenovo press for a complete list of NVMe limits.
Chapter 4. Considerations for FC configurations

You should be aware of several things when setting up your FC configuration.

- You can set up your FC configuration with HA pairs using a single fabric or multifabric.
- You should configure two FC data LIFs per node.
  
  This creates redundancy and protects against loss of data access.
- You should configure one management LIF for every storage virtual machine (SVM) supporting SAN.
- Multiple hosts, using different operating systems, such as Windows or Linux, can access the storage solution at the same time.

  Hosts require that a supported multipathing solution be installed and configured. Supported operating systems and multipathing solutions can be verified on the Lenovo Storage Interoperability Center (LSIC).
- ONTAP supports dual, or multiple node solutions that are connected to multiple physically independent storage fabrics; a minimum of two are recommended for SAN solutions.
  
  This provides redundancy at the fabric and storage system layers. Redundancy is particularly important because these layers typically support many hosts.
- The use of heterogeneous FC switch fabrics is not supported, except in the case of embedded blade switches.

  Specific exceptions are listed on the Lenovo Storage Interoperability Center (LSIC).
- Cascade, partial mesh, full mesh, core-edge, and director fabrics are all industry-standard methods of connecting FC switches to a fabric, and all are supported.

  A fabric can consist of one or multiple switches, and the storage controllers can be connected to multiple switches.

Ways to configure FC & FC-NVMe SAN hosts with HA pairs

You can configure FC and FC-NVMe SAN hosts to connect to HA pairs through one or more fabrics. You cannot directly attach FC or FC-NVMe SAN hosts to HA pairs without using a switch.

You can configure FC and FC-NVMe SAN hosts with single fabric HA pairs or with multifabric HA pairs. The FC target port numbers (0a, 0c, 0d, 1a, 1b) in the illustrations are examples. The actual port numbers vary depending on the model of your storage node and whether you are using expansion adapters.

Single-fabric HA pairs

In single-fabric HA pair configurations, there is one fabric connecting both controllers in the HA pair to one or more hosts. Because the hosts and controllers are connected through a single switch, single-fabric HA pairs are not fully redundant.

All platforms that support FC configurations support single-fabric HA pair configurations.
Multifabric HA pairs

In multifabric HA pairs, there are two or more switches connecting HA pairs to one or more hosts. For simplicity, the following multifabric HA pair figure shows only two fabrics, but you can have two or more fabrics in any multifabric configuration:
### FC switch configuration best practices

For best performance, you should consider certain best practices when configuring your FC switch.

A fixed link speed setting is the best practice for FC switch configurations, especially for large fabrics because it provides the best performance for fabric rebuilds and can significantly save time. Although autonegotiation provides the greatest flexibility, FC switch configuration does not always perform as expected, and it adds time to the overall fabric-build sequence.

All of the switches that are connected to the fabric must support N_Port ID virtualization (NPIV) and must have NPIV enabled. ONTAP uses NPIV to present FC targets to a fabric. For details about which environments are supported, see Lenovo Storage Interoperability Center (LSIC).

### Supported number of FC hop counts

The maximum supported FC hop count between a host and storage system depends on the switch supplier and storage system support for FC configurations.

The hop count is defined as the number of switches in the path between the initiator (host) and target (storage system). Cisco also refers to this value as the diameter of the SAN fabric.

<table>
<thead>
<tr>
<th>Switch supplier</th>
<th>Supported hop count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brocade</td>
<td>7 for FC</td>
</tr>
<tr>
<td>Cisco</td>
<td>7 for FC</td>
</tr>
</tbody>
</table>

### Managing systems with FC adapters

Commands are available to manage onboard FC adapters and FC adapter cards. These commands can be used to configure the adapter mode, display adapter information, and change the speed.

Most storage systems have onboard FC adapters that can be configured as initiators or targets. You can also use FC adapter cards configured as initiators or targets. Initiators connect to back-end disk shelves. Targets connect only to FC switches. Both the FC target HBA ports and the switch port speed should be set to the same value and should not be set to auto.

### Commands for managing FC adapters

You can use FC commands to manage FC target adapters, FC initiator adapters, and onboard FC adapters for your storage controller. The same commands are used to manage FC adapters for the FC protocol and the FC-NVMe protocol.

FC initiator adapter commands work only at the node level. You must use the `run -node node_name` command before you can use the FC initiator adapter commands.

#### Commands for managing FC target adapters

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display FC adapter information on a node</td>
<td>network fcp adapter show</td>
</tr>
<tr>
<td>Modify FC target adapter parameters</td>
<td>network fcp adapter modify</td>
</tr>
<tr>
<td>Display FC protocol traffic information</td>
<td>run -node node_name sysstat -f</td>
</tr>
<tr>
<td>Display how long the FC protocol has been running</td>
<td>run -node node_name uptime</td>
</tr>
</tbody>
</table>
If you want to... Use this command...

Display adapter configuration and status run -node node_name sysconfig -v adapter

Verify which expansion cards are installed and whether there are any configuration errors run -node node_name sysconfig -ac

View a man page for a command man command_name

Commands for managing FC initiator adapters

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display information for all initiators and their adapters in a node</td>
<td>run -node node_name storage show adapter</td>
</tr>
<tr>
<td>Display adapter configuration and status</td>
<td>run -node node_name sysconfig -v adapter</td>
</tr>
<tr>
<td>Verify which expansion cards are installed and whether there are any configuration errors</td>
<td>run -node node_name sysconfig -ac</td>
</tr>
</tbody>
</table>

Commands for managing onboard FC adapters

<table>
<thead>
<tr>
<th>If you want to...</th>
<th>Use this command...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the status of the onboard FC ports</td>
<td>run -node node_name system hardware unified-connect show</td>
</tr>
</tbody>
</table>

Configuring FC adapters for initiator mode

You can configure individual FC ports of onboard adapters and certain FC adapter cards for initiator mode. Initiator mode is used to connect the ports to tape drives, tape libraries, or third-party storage with Foreign LUN Import (FLI).

Before you begin

- LIFs on the adapter must be removed from any port sets of which they are members.
- All LIF’s from every storage virtual machine (SVM) using the physical port to be modified must be migrated or destroyed before changing the personality of the physical port from target to initiator.

About this task

Each onboard FC port can be individually configured as an initiator or a target. Ports on certain FC adapters can also be individually configured as either a target port or an initiator port, just like the onboard FC ports. A list of adapters that can be configured for target mode is available in the Lenovo press.

Note: FC-NVMe does support initiator mode.

Step 1. Remove all LIFs from the adapter:

    network interface delete -vserver SVM_name -lif LIF_name,LIF_name

Step 2. Take your adapter offline:

    network fcp adapter modify -node node_name -adapter adapter_port -status-admin down

    If the adapter does not go offline, you can also remove the cable from the appropriate adapter port on the system.

Step 3. Change the adapter from target to initiator:

    system hardware unified-connect modify -t initiator adapter_port

Step 4. Reboot the node hosting the adapter you changed.
Configuring FC adapters for target mode

You can configure individual FC ports of onboard adapters and certain FC adapter cards for target mode. Target mode is used to connect the ports to FC initiators.

About this task

Each onboard FC port can be individually configured as an initiator or a target. Ports on certain FC adapters can also be individually configured as either a target port or an initiator port, just like the onboard FC ports. A list of adapters that can be configured for target mode is available in the Lenovo press.

The same steps are used when configuring FC adapters for the FC protocol and the FC-NVMe protocol. However, only certain FC adapters support FC-NVMe. See Lenovo press for a list of adapters that support the FC-NVMe protocol.

Step 1. Take the adapter offline:
node run -node node_name storage disable adapter -d adapter_port
If the adapter does not go offline, you can also remove the cable from the appropriate adapter port on the system.

Step 2. Change the adapter from initiator to target:
  system hardware unified-connect modify -t target adapter_port

Step 3. Reboot the node hosting the adapter you changed.

Step 4. Verify that the target port has the correct configuration:
  network fcp adapter show -node node_name

Step 5. Bring your adapter online:
  network fcp adapter modify -node node_name -adapter adapter_port -state up

Displaying information about an FC target adapter

You can use the network fcp adapter show command to display system configuration and adapter information for any FC adapter in the system.

Step 1. Display information about the FC adapter by using the network fcp adapter show command.

Example

The output displays system configuration information and adapter information for each slot that is used.

network fcp adapter show -instance -node node1 -adapter 0a

Changing the FC adapter speed

You should set your adapter target port speed to match the speed of the device to which it connects, instead of using autonegotiation. A port that is set to autonegotiation can take longer time to reconnect after a takeover/giveback or other interruption.

Before you begin

All LIFs that use this adapter as their home port must be offline.
About this task

Because this task encompasses all storage virtual machines (SVMs) and all LIFs in a cluster, you must use the -home-port and -home-lif parameters to limit the scope of this operation. If you do not use these parameters, the operation applies to all LIFs in the cluster, which might not be desirable.

Step 1. Take all of the LIFs on this adapter offline:
   `network interface modify -vserver * -lif * { -home-node node1 -home-port 0c } -status-admin down`

Step 2. Take the adapter offline:
   `network fcp adapter modify -node node1 -adapter 0c -state down`
   If the adapter does not go offline, you can also remove the cable from the appropriate adapter port on the system.

Step 3. Determine the maximum speed for the port adapter:
   `fcp adapter show -instance`
   You cannot modify the adapter speed beyond the maximum speed.

Step 4. Change the adapter speed:
   `network fcp adapter modify -node node1 -adapter 0c -speed 16`

Step 5. Bring the adapter online:
   `network fcp adapter modify -node node1 -adapter 0c -state up`

Step 6. Bring all of the LIFs on the adapter online:
   `network interface modify -vserver * -lif * { -home-node node1 -home-port 0c } -status-admin up`

Supported FC ports

The number of onboard FC ports and CNA/UTA2 ports configured for FC varies based on the model of the controller. FC ports are also available through supported FC target expansion adapters or additional UTA2 cards configured with FC SFP+ adapters.

Onboard FC, UTA, and UTA2 ports

- Onboard ports can be individually configured as either target or initiator FC ports.
- The number of onboard FC ports differs depending on controller model.

   The Lenovo press contains a complete list of onboard FC ports on each controller model.

Target expansion adapter FC ports

- Available target expansion adapters differ depending on controller model.

   The Lenovo press contains a complete list of target expansion adapters for each controller model.

- The ports on some FC expansion adapters are configured as initiators or targets at the factory and cannot be changed.

   Others can be individually configured as either target or initiator FC ports, just like the onboard FC ports. A complete list is available in Lenovo press.

Port configuration options for the 4XC7A14394 adapter

By default the 4XC7A14394 adapter is configured in FC target mode, but you can configure its ports as either 10 Gb Ethernet ports or as 16 Gb FC initiator or target ports, this will require different SFP+ adapters.

Port pairs connected to the same ASIC must be configured in the same mode.

In FC mode, the 4XC7A14394 adapter behaves just like any existing FC device with speeds up to 16 Gbps. In CNA mode, you can use the 4XC7A14394 adapter for concurrent NIC traffic sharing the same 10 GbE port.
How to prevent loss of connectivity when using the 4XC7A14397 adapter

You can prevent loss of connectivity during a port failure by configuring your system with redundant paths to separate 4XC7A14397 HBAs.

The 4XC7A14397 HBA is a 4-port, 16 Gb FC adapter consisting of two 2-port pairs. The 4XC7A14397 adapter can be configured as target mode or initiator mode. Each 2-port pair is supported by a single ASIC (for example, Port 1 and Port 2 on ASIC 1 and Port 3 and Port 4 on ASIC 2). Both ports on a single ASIC must be configured to operate in the same mode, either target mode or initiator mode. If an error occurs with the ASIC supporting a pair, both ports in the pair go offline.

To prevent this loss of connectivity, you configure your system with redundant paths to separate 4XC7A14397 HBAs, or with redundant paths to ports supported by different ASICs on the HBA.

Supported port configurations for 4XC7A14394 adapter

The FC target mode is the default configuration for 4XC7A14394 adapter ports. However, ports on this adapter can be configured as either 10-Gb Ethernet ports or as 16-Gb FC ports.

When configured for Ethernet, 4XC7A14394 adapters support concurrent NIC target traffic on the same 10-GBE port. When configured for FC, each two-port pair that shares the same ASIC can be individually configured for FC target or FC initiator mode. This means that a single 4XC7A14394 adapter can support FC target mode on one two-port pair and FC initiator mode on another two-port pair.

Configuring the ports

To configure the unified target adapter (4XC7A14394), you must configure the two adjacent ports on the same chip in the same personality mode.

Step 1. Configure the ports as needed for Fibre Channel (FC) or Converged Network Adapter (CNA) using the `system node hardware unified-connect modify` command.

Step 2. Attach the appropriate cables for FC or 10 Gb Ethernet.

Step 3. Verify that you have the correct SFP+ installed:

   `network fcp adapter show -instance -node -adapter`

   For CNA, you should use a 10Gb Ethernet SFP. For FC, you should either use an 8 Gb SFP or a 16 Gb SFP, based on the FC fabric being connected to.

Changing the UTA2 port from CNA mode to FC mode

You should change the UTA2 port from Converged Network Adapter (CNA) mode to Fibre Channel (FC) mode to support the FC initiator and FC target mode. You should change the personality from CNA mode to FC mode when you need to change the physical medium that connects the port to its network.

Step 1. Take the adapter offline:

   `network fcp adapter modify -node node_name -adapter adapter_name -status-admin down`

Step 2. Change the port mode:

   `ucadmin modify -node node_name -adapter adapter_name -mode fcp`

Step 3. Reboot the node, and then bring the adapter online:

   `network fcp adapter modify -node node_name -adapter adapter_name -status-admin up`

Step 4. Notify your admin or VIF manager to delete or remove the port, as applicable:

   If the port is used as a home port of a LIF, is a member of an interface group (ifgrp), or hosts VLANs, then an admin should do the following:

   1. Move the LIFs, remove the port from the ifgrp, or delete the VLANs, respectively.
2. Manually delete the port by running the **network port delete** command.

   If the **network port delete** command fails, the admin should address the errors, and then run the command again.

If the port is not used as the home port of a LIF, is not a member of an ifgrp, and does not host VLANs, then the VIF manager should remove the port from its records at the time of reboot.

If the VIF manager does not remove the port, then the admin must remove it manually after the reboot by using the **network port delete** command.

**Example**

```
net-f8040-34::> network port show

Node: net-f8040-34-01

<table>
<thead>
<tr>
<th>Port</th>
<th>IPspace</th>
<th>Broadcast Domain</th>
<th>Link</th>
<th>MTU</th>
<th>Admin/Oper</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>e0i</td>
<td>Default</td>
<td>Default</td>
<td>down</td>
<td>1500</td>
<td>auto/10</td>
<td>-</td>
</tr>
<tr>
<td>e0f</td>
<td>Default</td>
<td>Default</td>
<td>down</td>
<td>1500</td>
<td>auto/10</td>
<td>-</td>
</tr>
</tbody>
</table>

...  

net-f8040-34::> ucadmin show

<table>
<thead>
<tr>
<th>Node</th>
<th>Adapter</th>
<th>Current Mode</th>
<th>Current Type</th>
<th>Pending Mode</th>
<th>Pending Type</th>
<th>Admin</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>net-f8040-34-01</td>
<td>0e</td>
<td>cna</td>
<td>target</td>
<td>-</td>
<td>-</td>
<td>offline</td>
<td></td>
</tr>
<tr>
<td>net-f8040-34-01</td>
<td>0f</td>
<td>cna</td>
<td>target</td>
<td>-</td>
<td>-</td>
<td>offline</td>
<td></td>
</tr>
</tbody>
</table>

...  

net-f8040-34::> network interface create -vs net-f8040-34 -lif m -role node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1 -netmask 255.255.255.0

net-f8040-34::> network interface show -fields home-port, curr-port

<table>
<thead>
<tr>
<th>vserver lif</th>
<th>home-port</th>
<th>curr-port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster net-f8040-34-01_clus1 m</td>
<td>e0a</td>
<td>e0a</td>
</tr>
<tr>
<td>Cluster net-f8040-34-01_clus2 m</td>
<td>e0b</td>
<td>e0b</td>
</tr>
<tr>
<td>Cluster net-f8040-34-01_clus3 m</td>
<td>e0c</td>
<td>e0c</td>
</tr>
<tr>
<td>Cluster net-f8040-34-01_clus4 m</td>
<td>e0d</td>
<td>e0d</td>
</tr>
<tr>
<td>net-f8040-34_cluster_mgmt m</td>
<td>eOM</td>
<td>eOM</td>
</tr>
<tr>
<td>net-f8040-34 m</td>
<td>e0e</td>
<td>e0i</td>
</tr>
<tr>
<td>net-f8040-34</td>
<td>net-f8040-34-01_mgmt1 m</td>
<td>eOM</td>
</tr>
</tbody>
</table>

7 entries were displayed.

net-f8040-34::> ucadmin modify local 0e fc

Warning: Mode on adapter 0e and also adapter 0f will be changed to fc.
Do you want to continue? (y/n): y
Any changes will take effect after rebooting the system. Use the "system node reboot" command to reboot.

net-f8040-34::> reboot local (system node reboot)

Warning: Are you sure you want to reboot node "net-f8040-34-01"?
```
Step 5. Verify that you have the correct SFP+ installed: network fcp adapter show -instance -node -adapter

For CNA, you should use a 10Gb Ethernet SFP. For FC, you should either use an 8 Gb SFP or a 16 Gb SFP, before changing the configuration on the node.

Changing the CNA/UTA2 target adapter optical modules
You should change the optical modules on the unified target adapter (CNA/UTA2) to support the personality mode you have selected for the adapter.

Step 1. Verify the current SFP+ used in the card. Then, replace the current SFP+ with the appropriate SFP+ for the preferred personality (FC or CNA).
Step 2. Remove the current optical modules from the 4XC7A14394 adapter.
Step 3. Insert the correct modules for your preferred personality mode (FC or CNA) optics.
Step 4. Verify that you have the correct SFP+ installed: network fcp adapter show -instance -node -adapter

Supported SFP+ modules and Cisco-branded Copper (Twinax) cables are listed in the Lenovo press.

Viewing adapter settings
To view the settings for your unified target adapter (4XC7A14394), you must run the system hardware unified-connect show command to display all modules on your controller.

Step 1. Boot your controller without the cables attached.
Step 2. Run the system hardware unified-connect show command to see the port configuration and modules.
Step 3. View the port information before configuring the CNA and ports.

FC target port supported speeds
FC target ports can be configured to run at different speeds. You should set the target port speed to match the speed of the device to which it connects. All target ports used by a given host should be set to the same speed. FC target ports can be used for FC-NVMe configurations in the exact same way they are used for FC configurations.

You should set the target port speed to match the speed of the device to which it connects instead of using autonegotiation. A port that is set to autonegotiation can take longer to reconnect after a takeover/giveback or other interruption.

You can configure onboard ports and expansion adapters to run at the following speeds. Each controller and expansion adapter port can be configured individually for different speeds as needed.

<table>
<thead>
<tr>
<th>4 Gb ports</th>
<th>8 Gb ports</th>
<th>16 Gb ports</th>
<th>32 Gb ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 4 Gb</td>
<td>• 8 Gb</td>
<td>• 16 Gb</td>
<td>• 32 Gb</td>
</tr>
<tr>
<td>• 2 Gb</td>
<td>• 4 Gb</td>
<td>• 8 Gb</td>
<td>• 16 Gb</td>
</tr>
<tr>
<td>• 1 Gb</td>
<td>• 2 Gb</td>
<td>• 4 Gb</td>
<td>• 8 Gb</td>
</tr>
</tbody>
</table>

Note: UTA2 ports can use an 8 Gb SFP+ adapter to support 8, 4, and 2 Gb speeds, if required.
**FC Target port configuration recommendations**

For best performance and highest availability, you should use the recommended FC target port configuration.

The following table shows the preferred port usage order for onboard FC and FC-NVMe target ports. For expansion adapters, the FC ports should be spread so that they do not use the same ASIC for connectivity. The preferred slot order is listed in the *Lenovo press* for the version of ONTAP software used by your controller.

FC-NVMe is supported on the following models:
- AFA DM7000F

**Note:** The AFA DM7000F onboard ports do not support FC-NVMe.

<table>
<thead>
<tr>
<th>Controller</th>
<th>Port pairs with shared ASIC</th>
<th>Number of target ports: Preferred ports</th>
</tr>
</thead>
</table>
| DM7000H and AFA DM7000F | 0g+0h | 1: 0g  
2: 0g, 0h |
| DM3000H, DM5000H, AFA DM5000F and AFA DM5000F | 0c+0d, 0e+0f | 1: 0c  
2: 0c, 0e  
3: 0c, 0e, 0d  
4: 0c, 0e, 0d, 0f |
Chapter 5. Fibre Channel zoning

An FC or FC-NVMe zone is a logical grouping of one or more ports within a fabric. For devices to be able see each other, connect, create sessions with one another, and communicate, both ports need to have a common zone membership. Single initiator zoning is recommended.

Reasons for zoning

- Zoning reduces or eliminates crosstalk between initiator HBAs.
  
  This occurs even in small environments and is one of the best arguments for implementing zoning. The logical fabric subsets created by zoning eliminate crosstalk problems.

- Zoning reduces the number of available paths to a particular FC or FC-NVMe port and reduces the number of paths between a host and a particular LUN that is visible.
  
  For example, some host OS multipathing solutions have a limit on the number of paths they can manage. Zoning can reduce the number of paths that an OS multipathing driver sees. If a host does not have a multipathing solution installed, you need to verify that only one path to a LUN is visible by using either zoning in the fabric or a combination of Selective LUN Mapping (SLM) and portsets in the SVM.

- Zoning increases security by limiting access and connectivity to end-points that share a common zone.
  
  Ports that have no zones in common cannot communicate with one another.

- Zoning improves SAN reliability by isolating problems that occur and helps to reduce problem resolution time by limiting the problem space.

Recommendations for zoning

- You should implement zoning any time, if four or more hosts are connected to a SAN or if SLM is not implemented on the nodes to a SAN.

- Although World Wide Node Name zoning is possible with some switch vendors, World Wide Port Name zoning is required to properly define a specific port and to use NPIV effectively.

- You should limit the zone size while still maintaining manageable.
  
  Multiple zones can overlap to limit size. Ideally, a zone is defined for each host or host cluster.

- You should use single-initiator zoning to eliminate crosstalk between initiator HBAs.

World Wide Name-based zoning

Zoning based on World Wide Name (WWN) specifies the WWN of the members to be included within the zone. When zoning in ONTAP, you must use World Wide Port Name (WWPN) zoning.

WWPN zoning provides flexibility because access is not determined by where the device is physically connected to the fabric. You can move a cable from one port to another without reconfiguring zones.

For Fibre Channel paths to storage controllers running ONTAP, be sure the FC switches are zoned using the WWPNs of the target logical interfaces (LIFs), not the WWPNs of the physical ports on the node. For more information on LIFs, see the ONTAP Network Management Guide.

Network Management Guide
**Individual zones**

In the recommended zoning configuration, there is one host initiator per zone. The zone consists of the host initiator port and one or more target LIFs on the storage nodes that are providing access to the LUNs up to the desired number of paths per target. This means that hosts accessing the same nodes cannot see each other's ports, but each initiator can access any node.

You should add all LIF’s from the storage virtual machine (SVM) into the zone with the host initiator. This allows you to move volumes or LUNs without editing your existing zones or creating new zones.

For Fibre Channel paths to nodes running ONTAP, be sure that the FC switches are zoned using the WWPNs of the target logical interfaces (LIFs), not the WWPNs of the physical ports on the node. The WWPNs of the physical ports start with “50” and the WWPNs of the LIFs start with “20”.

**Single-fabric zoning**

In a single-fabric configuration, you can still connect each host initiator to each storage node. Multipathing software is required on the host to manage multiple paths. Each host should have two initiators for multipathing to provide resiliency in the solution.

Each initiator should have a minimum of one LIF from each node that the initiator can access. The zoning should allow at least one path from the host initiator to the HA pair of nodes in the cluster to provide a path for LUN connectivity. This means that each initiator on the host might only have one target LIF per node in its zone configuration. If there is a requirement for multipathing to the same node or multiple nodes in the cluster, then each node will have multiple LIFs per node in its zone configuration. This enables the host to still access its LUNs if a node fails or a volume containing the LUN is moved to a different node. This also requires the reporting nodes to be set appropriately.

Single-fabric configurations are supported, but are not considered highly available. The failure of a single component can cause loss of access to data.

In the following figure, the host has two initiators and is running multipathing software. There are two zones:

**Note:** The naming convention used in this figure is just a recommendation of one possible naming convention that you can choose to use for your ONTAP solution.

- Zone 1: HBA 0, LIF_1, and LIF_3
- Zone 2: HBA 1, LIF_2, and LIF_4

If the configuration included more nodes, the LIFs for the additional nodes would be included in these zones.
In this example, you could also have all four LIFs in each zone. In that case, the zones would be as follows:

- Zone 1: HBA 0, LIF_1, LIF_2, LIF_3, and LIF_4
- Zone 2: HBA 1, LIF_1, LIF_2, LIF_3, and LIF_4

**Note:** The host operating system and multipathing software have to support the number of supported paths that are being used to access the LUNs on the nodes. To determine the number of paths used to access the LUNs on nodes, see the SAN configuration limits section.

### Dual-fabric HA pair zoning

In dual-fabric configurations, you can connect each host initiator to each cluster node. Each host initiator uses a different switch to access the cluster nodes. Multipathing software is required on the host to manage multiple paths.

Dual-fabric configurations are considered high availability because access to data is maintained if a single component fails.

In the following figure, the host has two initiators and is running multipathing software. There are two zones. SLM is configured so that all nodes are considered as reporting nodes.

**Note:** The naming convention used in this figure is just a recommendation of one possible naming convention that you can choose to use for your ONTAP solution.

- Zone 1: HBA 0, LIF_1, LIF_3, LIF_5, and LIF_7
- Zone 2: HBA 1, LIF_2, LIF_4, LIF_6, and LIF_8

Each host initiator is zoned through a different switch. Zone 1 is accessed through Switch 1. Zone 2 is accessed through Switch 2.
Each initiator can access a LIF on every node. This enables the host to still access its LUNs if a node fails. SVMs have access to all iSCSI and FC LIFs on every node in a clustered solution based on the setting for Selective LUN Map (SLM) and the reporting node configuration. You can use SLM, portsets, or FC switch zoning to reduce the number of paths from an SVM to the host and the number of paths from an SVM to a LUN.

If the configuration included more nodes, the LIFs for the additional nodes would be included in these zones.

Note: The host operating system and multipathing software have to support the number of paths that is being used to access the LUNs on the nodes.

### Zoning restrictions for Cisco FC switches

When using Cisco FC switches, a single fabric zone must not contain more than one target LIF for the same physical port. If multiple LIFs on the same port are in the same zone, then the LIF ports might fail to recover from a connection loss.

Regular FC switches are used for the FC-NVMe protocol in the exact same way they are used for the FC protocol.

- Multiple LIFs for the FC protocols, can share physical ports on a node as long as they are in different zones.
- FC-NVMe cannot share the same physical port.
- FC and FC-NVMe can share the same 32 Gb physical port.
- Cisco FC switches require each LIF on a given port to be in a separate zone from the other LIFs on that port.
- A single zone can have both FC LIFs. A zone can contain a LIF from every target port in the cluster, but be careful to not exceed the host’s path limits and verify the SLM configuration.
- LIFs on different physical ports can be in the same zone.
- Cisco switches require that LIFs be separated.
Though not required, separating LIFs is recommended for all switches
Chapter 6. Requirements for shared SAN configurations

Shared SAN configurations are defined as hosts that are attached to both ONTAP storage systems and other vendors' storage systems. Accessing ONTAP storage systems and other vendors' storage systems from a single host is supported as long as several requirements are met.

For all of the host operating systems, it is a best practice to use separate adapters to connect to each vendor's storage systems. Using separate adapters reduces the chances of conflicting drivers and settings. For connections to an ONTAP storage system, the adapter model, BIOS, firmware, and driver must be listed as supported in the Lenovo Storage Interoperability Center (LSIC).

You should set the required or recommended timeout values and other storage parameters for the host. You must always install the Lenovo software or apply the Lenovo settings last.

- For ESX, you should apply host settings by using Virtual Storage Console for VMware vSphere.
- For Linux, you should apply the values from the Linux Host Utilities version that is listed in the Lenovo Storage Interoperability Center (LSIC) for your configuration.
- For Windows, you should install either the Data ONTAP DSM for Windows MPIO or the Windows Host Utilities version that is listed in the Lenovo Storage Interoperability Center (LSIC) for your configuration.
Chapter 7. Host support for multipathing

ONTAP always uses Asymmetric Logical Unit Access (ALUA) for both FC and iSCSI paths. Be sure to use host configurations that support ALUA for FC and iSCSI protocols.

Beginning with ONTAP 9.5 multipath HA pair failover/giveback is supported for NVMe configurations using Asynchronous Namespace Access (ANA). In ONTAP 9.4, NVMe only supports one path from host to target. The application host needs to manage path failover to its high availability (HA) partner.

For information about which specific host configurations support ALUA or ANA, see the Lenovo Storage Interoperability Center (LSIC) and the Host Utilities Installation and Setup Guide for your host operating system.

When host multipathing software is required

If there is more than one path from the storage virtual machine (SVM) logical interfaces (LIFs) to the fabric, multipathing software is required. Multipathing software is required on the host any time the host can access a LUN through more than one path.

The multipathing software presents a single disk to the operating system for all paths to a LUN. Without multipathing software, the operating system could treat each path as a separate disk, which can lead to data corruption.

Your solution is considered to have multiple paths if you have any of the following:

- A single initiator port in the host attaching to multiple SAN LIFs in the SVM
- Multiple initiator ports attaching to a single SAN LIF in the SVM
- Multiple initiator ports attaching to multiple SAN LIFs in the SVM

Multipathing software is recommended in HA configurations. In addition to Selective LUN Map, using FC switch zoning or portsets to limit the paths used to access LUNs is recommended.

Multipathing software is also known as MPIO (multipath I/O) software.

Recommended number of paths from host to nodes in cluster

You should not exceed more than eight paths from your host to each node in your cluster, paying attention to the total number of paths that can be supported for the host OS and the multipathing used on the host.

You should have a minimum of two paths per LUN connecting to each reporting node through Selective LUN Map (SLM) being used by the storage virtual machine (SVM) in your cluster. This eliminates single points of failure and enables the system to survive component failures.

If you have four or more nodes in your cluster or more than four target ports being used by the SVMs in any of your nodes, you can use the following methods to limit the number of paths that can be used to access LUNs on your nodes so that you do not exceed the recommended maximum of eight paths.

- SLM
  SLM reduces the number of paths from the host to LUN to only paths on the node owning the LUN and the owning node’s HA partner. SLM is enabled by default.
- Portsets for iSCSI
• FC igroup mappings from your host
• FC switch zoning
Chapter 8. Configuration limits for FC and iSCSI configurations

Configuration limits are available for FC and iSCSI configurations. In some cases, theoretical limits might be higher, but the published limits are tested and supported.

Accessing SAN and NVMe configuration limits

You should use the tested and supported maximum configuration limits established for each storage controller in your SAN environment. For reliable operations, you should not exceed the tested and supported limits.

About this task

Current SAN node limits, configuration limits for your specific platforms and ONTAP versions supported by each platform can be accessed in the Lenovo press. Host operating systems supported for your specific version of ONTAP, platforms, and protocols are available in the Lenovo Storage Interoperability Center (LSIC).

SAN limits are impacted by the following:

- The maximum number of nodes within a cluster is determined by the platform that supports the fewest number of nodes.
  - If any node in the cluster is configured for FC, FC-NVMe, or iSCSI, the cluster is limited to the SAN node limits.
- The cluster limits for nodes with mixed controller types are based on the node with the lowest limits.
- 8-node limits are the maximum limits for all SAN nodes.
  - 10-node and 12-node clusters in a SAN environment must adhere to 8-node limits. In such cases, the cluster limits are the node limits multiplied by eight, rather than 10 or 12.
- The maximum number of LUNs and the number of host HBAs that can connect to an FC port are limited by the available queue depth on the FC target ports.

Storage limits for Cloud Volumes ONTAP are documented in the Cloud Volumes ONTAP Release Notes.

Step 1. Connect to Lenovo press.

Step 2. Select your platform type.

For FC or iSCSI, click Platforms → Hybrid

For FC-NVMe, click Platforms → All-Flash Array (AFA)

Step 3. Select your version of ONTAP from the list. Stat with OS is the default selection. Use this option to get the correct limits for your platform and your ONTAP version.

Step 4. Select the platforms for which you need SAN limits.

Step 5. Under Choose Your Specifications, deselect Select All.

Step 6. Scroll down and select the limits you need to view.

Select SAN Limits to display limits for FC or iSCSI.
Select **NVMe/FC Limits** to display limits for FC-NVMe.

---

### SAN configuration requirement for FlexVol volumes

Volumes containing LUNs must be FlexVol volumes. SAN protocols can only be used with storage virtual machines (SVMs). Infinite Volumes are not supported for SAN.

In this document, “volume” always means “FlexVol volume”.

---

### Determining the number of supported nodes for SAN configurations

The number of nodes per cluster supported by ONTAP varies depending on your version of ONTAP, the storage controller models in your cluster, and the protocol of your cluster nodes.

**About this task**

If any node in the cluster is configured for FC, FC-NVMe, or iSCSI, that cluster is limited to the SAN node limits. Node limits based on the controllers in your cluster are listed in Lenovo press.

**Step 1.** Go to Lenovo press.

**Step 2.** Click **Platforms** in the upper left (next to the Home button) and select the platform type.

**Step 3.** Select the check box next to your version of ONTAP. A new column is displayed for you to choose your platforms.

**Step 4.** Select the check boxes next to the platforms used in your solution.

**Step 5.** Unselect the Select All check box in the Choose Your Specifications column.

**Step 6.** Select the Max Nodes per Cluster (NAS/SAN) check box.

**Step 7.** Click Show Results.

---

### Determining the number of supported hosts per cluster in FC and FC-NVMe configurations

The maximum number of SAN hosts that can be connected to a cluster varies greatly based upon your specific combination of multiple cluster attributes, such as the number of hosts connected to each cluster node, initiators per host, sessions per host, and nodes in the cluster.

**About this task**

For FC and FC-NVMe configurations, you should use the number of initiator-target nexuses (ITNs) in your system to determine whether you can add more hosts to your cluster.

An ITN represents one path from the host’s initiator to the storage system's target. The maximum number of ITNs per node in FC and FC-NVMe configurations is 2,048. As long as you are below the maximum number of ITNs, you can continue to add hosts to your cluster.

To determine the number of ITNs used in your cluster, perform the following steps for each node in the cluster.

**Step 1.** Identify all the LIFs on a given node.

**Step 2.** Run the following command for every LIF on the node:

```bash
fcp initiator show -fields wwpn, lif
```

The number of entries displayed at the bottom of the command output represents your number of ITNs for that LIF.
Step 3. Record the number of ITNs displayed for each LIF.

Step 4. Add the number of ITNs for each LIF on every node in your cluster.
This total represents the number of ITNs in your cluster.

Determining the supported number of hosts in iSCSI configurations

The maximum number of SAN hosts that can be connected in iSCSI configurations varies greatly based on your specific combination of multiple cluster attributes, such as the number of hosts connected to each cluster node, initiators per host, logins per host, and nodes in the cluster.

About this task

The number of hosts that can be directly connected to a node or that can be connected through one or more switches depends on the number of available Ethernet ports. The number of available Ethernet ports is determined by the model of the controller and the number and type of adapters installed in the controller. The number of supported Ethernet ports for controllers and adapters is available in the Lenovo press.

For all multi-node cluster configurations, you must determine the number of iSCSI sessions per node to know whether you can add more hosts to your cluster. As long as your cluster is below the maximum number of iSCSI sessions per node, you can continue to add hosts to your cluster. The maximum number of iSCSI sessions per node varies based on the types of controllers in your cluster.

Step 1. Identify all of the target portal groups on the node.

Step 2. Check the number of iSCSI sessions for every target portal group on the node:

```
iscsi session show -tpgroup tpgroup
```

The number of entries displayed at the bottom of the command output represents your number of iSCSI sessions for that target portal group.

Step 3. Record the number of iSCSI sessions displayed for each target portal group.

Step 4. Add the number of iSCSI sessions for each target portal group on the node.
The total represents the number of iSCSI sessions on your node.

FC switch configuration limits

Fibre Channel switches have maximum configuration limits, including the number of logins supported per port, port group, blade, and switch. The switch vendors document their supported limits.

Each FC logical interface (LIF) logs into an FC switch port. The total number of logins from a single target on the node equals the number of LIFs plus one login for the underlying physical port. Do not exceed the switch vendor’s configuration limits for logins or other configuration values. This also holds true for the initiators being used on the host side in virtualized environments with NPIV enabled. Do not exceed the switch vendor’s configuration limits for logins for either the target or the initiators being used in the solution.

Brocade switch limits

You can find the configuration limits for Brocade switches in the Brocade Scalability Guidelines.

Cisco Systems switch limits

You can find the configuration limits for Cisco switches in the Cisco Configuration Limits guide for your version of Cisco switch software.
Calculating queue depth

You might need to tune your FC queue depth on the host to achieve the maximum values for ITNs per node and FC port fan-in. The maximum number of LUNs and the number of HBAs that can connect to an FC port are limited by the available queue depth on the FC target ports.

About this task

Queue depth is the number of I/O requests (SCSI commands) that can be queued at one time on a storage controller. Each I/O request from the host’s initiator HBA to the storage controller’s target adapter consumes a queue entry. Typically, a higher queue depth equates to better performance. However, if the storage controller’s maximum queue depth is reached, that storage controller rejects incoming commands by returning a QFULL response to them. If a large number of hosts are accessing a storage controller, you should plan carefully to avoid QFULL conditions, which significantly degrade system performance and can lead to errors on some systems.

In a configuration with multiple initiators (hosts), all hosts should have similar queue depths. Because of the inequality in queue depth between hosts connected to the storage controller through the same target port, hosts with smaller queue depths are being deprived of access to resources by hosts with larger queue depths.

The following general recommendations can be made about “tuning” queue depths:

- For small to mid-size systems, use an HBA queue depth of 32.
- For large systems, use an HBA queue depth of 128.
- For exception cases or performance testing, use a queue depth of 256 to avoid possible queuing problems.
- All hosts should have the queue depths set to similar values to give equal access to all hosts.
- To avoid performance penalties or errors, the storage controller target FC port queue depth must not be exceeded.

Step 1. Count the total number of FC initiators in all of the hosts that connect to one FC target port.

Step 2. Multiply by 128.

If the result is less than 2,048, set the queue depth for all initiators to 128.

Example

You have 15 hosts with one initiator connected to each of two target ports on the storage controller. 15 × 128 = 1,920. Because 1,920 is less than the total queue depth limit of 2,048, you can set the queue depth for all of your initiators to 128.

If the result is greater than 2,048, go to step Step 3 on page 32.

Example

You have 30 hosts with one initiator connected to each of two target ports on the storage controller. 30 × 128 = 3,840. Because 3,840 is greater than the total queue depth limit of 2,048, you should choose one of the options under step Step 3 on page 32 for remediation.

Step 3. Choose one of the following options to add more hosts to the storage controller.

Option 1:
1. Add more FC target ports.
2. Redistribute your FC initiators.
3. Repeat steps Step 1 1 on page 32 and Step 2 2 on page 32.

Example

The desired queue depth of 3,840 exceeds the available queue depth per port. To remedy this, you can add a two-port FC target adapter to each controller, then rezone your FC switches so that 15 of your 30 hosts connect to one set of ports, and the remaining 15 hosts connect to a second set of ports. The queue depth per port is then reduced to $15 \times 128 = 1,920$.

Option 2:

1. Designate each host as “large” or “small” based on its expected I/O need.
2. Multiply the number of large initiators by 128.
3. Multiply the number of small initiators by 32.
4. Add the two results together.
5. If the result is less than 2,048, set the queue depth for large hosts to 128 and the queue depth for small hosts to 32.
6. If the result is still greater than 2,048 per port, reduce the queue depth per initiator until the total queue depth is less than or equal to 2,048.

   Note: To estimate the queue depth needed to achieve a certain I/O per second throughput, use this formula: Needed queue depth = (Number of I/O per second) × (Response time)

For example, if you need 40,000 I/O per second with a response time of 3 milliseconds, the needed queue depth = $40,000 \times (.003) = 120$.

The maximum number of hosts that you can connect to a target port is 64, if you decide to limit the queue depth to the basic recommendation of 32. However, if you decide to have a queue depth of 128, then you can have a maximum of 16 hosts connected to one target port. The larger the queue depth, the fewer hosts that a single target port can support. If your requirement is such that you cannot compromise on the queue depth, then you should get more target ports.

Example

The desired queue depth of 3,840 exceeds the available queue depth per port. You have 10 “large” hosts that have high storage I/O needs, and 20 “small” hosts that have low I/O needs. Set the initiator queue depth on the large hosts to 128 and the initiator queue depth on the small hosts to 32.

Your resulting total queue depth is $(10 \times 128) + (20 \times 32) = 1,920$.

Example

You can spread the available queue depth equally across each initiator.

Your resulting queue depth per initiator is $2,048 \div 30 = 68$.

Setting queue depths on VMware hosts

Use the `esxcli module` command to change the HBA timeout settings. Manually updating the `esx.conf` file is not recommended.
To set maximum queue depth for a QLogic HBA

Step 1. Log on to the service console as the root user.

Step 2. Use the `vmload_mod -l` command to verify which QLogic HBA module is currently loaded.

Step 3. For a single instance of a Qlogic HBA, run the following command:

```
# esxcfg-module -s ql2xmaxqdepth=64 qla2300_707
```

**Note:** This example uses qla2300_707 module. Use the appropriate module based on the output of `vmload_mod -l`.

Step 4. Save your changes using the following command:

```
#/usr/sbin/esxcfg-boot -b
```

Step 5. Reboot the server using the following command:

```
#reboot
```

Step 6. Confirm the changes using the following commands:

a. `#esxcfg-module -g qla2300_707`

b. `qla2300_707 enabled = 1 options = 'ql2xmaxqdepth=64'`

To change the queue depth of an Emulex HBA

Step 1. Log on to the service console as the root user.

Step 2. Use the `vmload_mod -l grep lpfcdd` command to verify which Emulex HBA is currently loaded.

Step 3. For a single instance of an Emulex HBA, enter the following command:

```
# esxcfg-module -s lpfc0_lun_queue_depth=16 lpfcdd_7xx
```

**Note:** Depending on the model of the HBA, the module can be either lpfcdd_7xx or lpfcdd_732.

The above command uses the lpfcdd_7xx module. You should use the appropriate module based on the outcome of `vmload_mod -l`.

Running this command will set the LUN queue depth to 16 for the HBA represented by lpfc0.

Step 4. For multiple instances of an Emulex HBA, run the following command:

```
a esxcfg-module -s "lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16" lpfcdd_7xx
```

The LUN queue depth for lpfc0 and the LUN queue depth for lpfc1 is set to 16.

Step 5. Enter the following command: `#esxcfg-boot -b`

Step 6. Reboot using `#reboot`.

Setting queue depths on Windows hosts

On Windows hosts, you can use the LPUTILNT utility to update the queue depth for Emulex HBAs and the SANsurfer HBA manager utility to update the queue depths for QLogic HBAs.

To update Emulex HBA queue depths

Step 1. Run the LPUTILNT utility located in the `C:\WINNT\system32` directory.

Step 2. Select **Drive Parameters** from the menu on the right side.

Step 3. Scroll down and double-click **QueueDepth**.

**Note:** If you are setting **QueueDepth** greater than 150, the following Windows Registry value also need to be increased appropriately: `HKEY_LOCAL_MACHINESYSTEM\CurrentControlSet\Services\lpxnds\Parameters\Device\NumberOfRequests`

To update Qlogic HBA queue depths

Step 1. Run the SANsurfer HBA manager utility.

Step 2. Click on **HBA port → Settings**.
Step 3. Click Advanced HBA port settings in the list box.
Step 4. Update the Execution Throttle parameter.

**Setting queue depths on Linux hosts**

You can change the queue depth of Emulex HBAs and QLogic HBAs on Linux hosts.

**Updating Emulex HBA queue depths on a Linux host**

You can update the queue depths of an Emulex HBA on a Linux host. To make the updates persistent across reboots, you must then create a new RAM disk image and reboot the host.

Step 1. Identify the queue depth parameters to be modified:
```
modinfo lpfc|grep queue_depth
```
The list of queue depth parameters with their description is displayed. Depending on your operating system version, you can modify one or more of the following queue depth parameters:

- `lpfc_lun_queue_depth`: Maximum number of FC commands that can be queued to a specific LUN (uint)
- `lpfc_hba_queue_depth`: Maximum number of FC commands that can be queued to an lpfc HBA (uint)
- `lpfc_tgt_queue_depth`: Maximum number of FC commands that can be queued to a specific target port (uint)

The `lpfc_tgt_queue_depth` parameter is applicable only for Red Hat Enterprise Linux 7.x systems, SUSE Linux Enterprise Server 11 SP4 systems and 12.x systems.

Step 2. Update the queue depths by adding the queue depth parameters to the `/etc/modprobe.conf` file for a Red Hat Enterprise Linux 5.x system and to the `/etc/modprobe.d/scsi.conf` file for a Red Hat Enterprise Linux 6.x or 7.x system, or a SUSE Linux Enterprise Server 11.x or 12.x system. Depending on your operating system version, you can add one or more of the following commands:

- `options lpfc lpfc_hba_queue_depth=new_queue_depth`
- `options lpfc lpfc_lun_queue_depth=new_queue_depth`
- `options lpfc lpfc_target_queue_depth=new_queue_depth`

Step 3. Create a new RAM disk image, and then reboot the host to make the updates persistent across reboots.
For more information, see the *System Administration Reference Guide* for your version of Linux operating system.

Step 4. Verify that the queue depth values are updated for each of the queue depth parameter that you have modified:
```
cat /sys/class/scsi_host/host_number/lpfc_lun_queue_depth
cat /sys/class/scsi_host/host_number/lpfc_target_queue_depth
cat /sys/class/scsi_host/host_number/lpfc_hba_queue_depth
```

**Example**
```
root@localhost ~]$ cat /sys/class/scsi_host/host5/lpfc_lun_queue_depth
30
```
The current value of the queue depth is displayed.

**Updating QLogic HBA queue depths on a Linux host**

You can update the device queue depth of a QLogic driver on a Linux host. To make the updates persistent across reboots, you must then create a new RAM disk image and reboot the host. You can use the QLogic HBA management GUI or command-line interface (CLI) to modify the QLogic HBA queue depth.
About this task

This task shows how to use the QLogic HBA CLI to modify the QLogic HBA queue depth

Step 1. Identify the device queue depth parameter to be modified:

```
modinfo qla2xxx | grep ql2xmaxqdepth
```

You can modify only the ql2xmaxqdepth queue depth parameter, which denotes the maximum queue depth that can be set for each LUN. The default value is 32.

Example

```
root@localhost ~]# modinfo qla2xxx | grep ql2xmaxqdepth
parm:           ql2xmaxqdepth:Maximum queue depth to set for each LUN. Default is 32. (int)
```

Step 2. Update the device queue depth value:

If you want to make the modifications persistent, perform the following steps:

1. Update the queue depths by adding the queue depth parameter to the `/etc/modprobe.conf` file for a Red Hat Enterprise Linux 5.x system and to the `/etc/modprobe.d/scsi.conf` file for a Red Hat Enterprise Linux 6.x or 7.x system, or a SUSE Linux Enterprise Server 11.x or 12.x system:
   
   ```
   options qla2xxx ql2xmaxqdepth=new_queue_depth
   ```

2. Create a new RAM disk image, and then reboot the host to make the updates persistent across reboots.

   For more information, see the System Administration Reference Guide for your version of Linux operating system.

If you want to modify the parameter only for the current session, run the following command:

```
echo new_queue_depth > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

Example

In the following example, the queue depth is set to 64 by adding the following line to the `/etc/modprobe.d/scsi.conf` file.

```
options qla2xxx ql2xmaxqdepth=64
```

In the following example, the queue depth is set to 128.

```
echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

Step 3. Verify that the queue depth values are updated:

```
cat /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

The current value of the queue depth is displayed.

Step 4. Modify the QLogic HBA queue depth by updating the firmware parameter Execution Throttle from the QLogic HBA BIOS.

a. Log in to the QLogic HBA management CLI:

   ```
   /opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli
   ```

b. From the main menu, select the Adapter Configuration option.

Example

```
[root@localhost ~]# /opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli
Using config file: /opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli.cfg
Installation directory: /opt/QLogic_Corporation/QConvergeConsoleCLI
Working dir: /root
```
QConvergeConsole

CLI - Version 2.2.0 (Build 15)

Main Menu

1: Adapter Information
2: Adapter Configuration
3: Adapter Updates
4: Adapter Diagnostics
5: Monitoring
6: FabricCache CLI
7: Refresh
8: Help
9: Exit

Please Enter Selection: 2

c. From the list of adapter configuration parameters, select the HBA Parameters option.

Example

1: Adapter Alias
2: Adapter Port Alias
3: HBA Parameters
4: Persistent Names (udev)
5: Boot Devices Configuration
6: Virtual Ports (NPIV)
7: Target Link Speed (iiDMA)
8: Export (Save) Configuration
9: Generate Reports
10: Personality
11: FEC

(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)

Please Enter Selection: 3

d. From the list of HBA ports, select the required HBA port.

Example

Fibre Channel Adapter Configuration

HBA Model QLE2562 SN: BFD1524C78510
1: Port 1: WWPN: 21-00-00-24-FF-8D-98-E0 Online
2: Port 2: WWPN: 21-00-00-24-FF-8D-98-E1 Online

HBA Model QLE2672 SN: RFE1241G81915
3: Port 1: WWPN: 21-00-00-0E-1E-09-B7-62 Online
4: Port 2: WWPN: 21-00-00-0E-1E-09-B7-63 Online

(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)

Please Enter Selection: 1

The details of the HBA port are displayed.

e. From the HBA Parameters menu, select the Display HBA Parameters option to view the current value of the Execution Throttle option.
The default value of the Execution Throttle option is 65535.

Example

HBA Parameters Menu

********************************************************************************
HBA : 2 Port: 1
SN : BFD01524C78510

Chapter 8. Configuration limits for FC and iSCSI configurations 37
1: Display HBA Parameters
2: Configure HBA Parameters
3: Restore Defaults

(P or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
Please Enter Selection: 1

--------------------------------------------------------------------------------
HBA Instance 2: QLE2562 Port 1 WWPN 21-00-00-24-FF-8D-98-E0 PortID 03-07-00
Link: Online
--------------------------------------------------------------------------------
Connection Options: 2 - Loop Preferred, Otherwise Point-to-Point
Data Rate: Auto
Frame Size: 2048
Hard Loop ID: 0
Loop Reset Delay (seconds): 5
Enable Host HBA BIOS: Enabled
Enable Hard Loop ID: Disabled
Enable FC Tape Support: Enabled
Operation Mode: 0 - Interrupt for every I/O completion
Interrupt Delay Timer (100us): 0
Execution Throttle: 65535
Login Retry Count: 8
Port Down Retry Count: 30
Enable LIP Full Login: Enabled
Link Down Timeout (seconds): 30
Enable Target Reset: Enabled
LUNs Per Target: 128
Out Of Order Frame Assembly: Disabled
Enable LR Ext. Credits: Disabled
Enable Fabric Assigned WWN: N/A

Press <Enter> to continue:
f. Press Enter to continue.
g. From the HBA Parameters menu, select the Configure HBA Parameters option to modify the HBA parameters.
h. From the Configure Parameters menu, select the Execute Throttle option and update the value of this parameter.

Example

Configure Parameters Menu

================================================================================
HBA        : 2 Port: 1
SN         : 8FD1524C78510
HBA Model  : QLE2562
HBA Desc.  : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version : 8.01.02
WWPN       : 21-00-00-24-FF-8D-98-E0
WWNN       : 20-00-00-24-FF-8D-98-E0
Link       : Online
================================================================================
4: Enable HBA Hard Loop ID
5: Hard Loop ID
6: Loop Reset Delay (seconds)
7: Enable BIOS
8: Enable Fibre Channel Tape Support
9: Operation Mode
10: Interrupt Delay Timer (100 microseconds)
11: Execution Throttle
12: Login Retry Count
13: Port Down Retry Count
14: Enable LIP Full Login
15: Link Down Timeout (seconds)
16: Enable Target Reset
17: LUNs per Target
18: Enable Receive Out Of Order Frame
19: Enable LR Ext. Credits
20: Commit Changes
21: Abort Changes

(p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
Please Enter Selection: 11
Enter Execution Throttle [1-65535] [65535]: 65500

i. Press Enter to continue.

j. From the Configure Parameters menu, select the Commit Changes option to save the changes.

k. Exit the menu.
Chapter 9. Considerations for SAN configurations in a MetroCluster environment

You must be aware of certain considerations when using SAN configurations in a MetroCluster environment.

- Two-node, four-node, and eight-node MetroCluster configurations do not support front-end FC fabric “routed” vSAN configurations.
- Two-node, four-node, and eight-node MetroCluster configurations support SAN protocols.
- When using SAN client configurations, you must check whether any special considerations for MetroCluster configurations are included in the notes that are provided in the Lenovo Storage Interoperability Center (LSIC).
- The NVMe protocol is not supported on MetroCluster configurations.
Chapter 10.  Where to find additional information

You can learn more about the tasks and concepts described in this guide in Lenovo’s extensive documentation library.

The following documentation is available:

• **SAN Administration Guide** Describes how to configure and manage NVMe, iSCSI, and FC protocols, including configuration of LUNs, igroups, and targets.

• **System Administration Guide** Describes general system administration of a cluster, including the CLI interface, cluster access, and node management.

• **ONTAP Command man pages** Describes ONTAP commands in reference format.
Appendix A. Contacting Support

You can contact Support to obtain help for your issue.

You can receive hardware service through a Lenovo Authorized Service Provider. To locate a service provider authorized by Lenovo to provide warranty service, go to https://datacentersupport.lenovo.com/serviceprovider and use filter searching for different countries. For Lenovo support telephone numbers, see https://datacentersupport.lenovo.com/supportphonelist for your region support details.
Appendix B. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document is not an offer and does not provide a license under any patents or patent applications. You can send inquiries in writing to the following:

Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.
Trademarks

LENOVO, LENOVO logo, and THINKSYSTEM are trademarks of Lenovo. All other trademarks are the property of their respective owners. © 2021 Lenovo.