

Summary

This article is intended as a “how to” guide to allow for successful deployment of Nimble Storage iSCSI connectivity to Cisco UCS.

Nimble Storage / Cisco UCS connectivity checklist:

- 1) [Determine UCS operation mode](#) – Knowledge of this setting will affect the network topology decisions in the next step.
- 2) [Determine the UCS network topology](#) that will be employed with the Nimble Storage array. Pay particular attention to determining if you need a single iSCSI subnet or if you need dual subnets for network diversity.
- 3) Based on the network topology example you chose in the previous step, implement the correct [VLAN / LAN connectivity](#) in the UCSM LAN tab.
- 4) Determine if you want to use Jumbo frames. There are several steps involved in applying Jumbo frames. The first is to understand your network topology (See [step2](#)). Also realize that by default QoS only allows the standard 1500 MTU size. This limitation still applies even if you have the Nimble Storage array and the host OS negotiate to a jumbo frame MTU. You must define the MTU value in the QoS policy to allow for jumbo frames. The first step is to [Configure QoS Policy for Jumbo Frames](#). The next step is to [Apply the QoS policy with Jumbo Frames](#). Also note that there are additional QoS steps needed if you are using a network topology that utilizes an upstream switch in the iSCSI data path ([Upstream switch QoS configuration for Jumbo Frames](#)).
- 5) [Create, configure, and apply a Flow Control Policy](#) - This determines how a LAN segment will handle congestion control using send and receive pause frames.
- 6) [Configure the appropriate Network Control Policy](#) – This setting will determine how the UCS failover policies behave in the event of a network Uplink or Appliance port failure.
- 7) Determine how you want to deploy the blade Service Profiles:
 - a. Deploy Service Profiles individually. This is the most flexible, but it also requires the most administration. This type of deployment is typically done in an environment with just a few blades.
 - b. (Non SANboot hosts): Create an updating Service Profile template. Then deploy Service Profiles from that template. Note: This method will not work if the blade requires an OS to SANboot. This is because it requires a unique target boot LUN entry per Service Profile. An updating template would update the boot entry for all hosts to be the same.

- c. (SANboot hosts): Create updating [vNIC templates](#). Implement a [LAN Connectivity Policy](#) that utilizes these vNIC templates. Finally create an initial [Service Profile template](#) with the LAN Connectivity Policy you just created. This method will allow you to deploy Service Profiles from a template and also dynamically update parameters on vNICs while still employing a unique target boot LUN for each blade.
- 8) Additional Service Profile settings are required for iSCSI SANboot: If you only have a few hosts then manual configuration makes more sense. However, if you have several hosts, then setting up pools will save on future administrative tasks and resource tracking.
- a. Manual setup for IP addresses, iqn initiator name, and MAC addresses, for every host blade Service Profile.
or
 - b. Setup pools for [IP addresses](#), [MAC addresses](#), and [iqn initiator](#).
 - c. Create [iSCSI vNIC template](#) to bind to the physical vNICs in the service profile.
 - d. Create and apply an [iSCSI Adapter policy](#). This will determine the timeout values for iSCSI boot connections.
 - e. Create and apply a [Boot Policy](#) for iSCSI sanboot. This determines the boot device order.
 - f. From the Nimble GUI configure an [iSCSI initiator group](#).
 - g. From the Nimble GUI [create the boot volume](#) for the host OS and apply the iSCSI initiator group.
 - h. Determine and configure the [static iqn entry](#) needed to identify the boot volume.
- Note: these IPs, MACs, and iqn names are used for the initial configuration for an iSCSI iBFT SANboot operation. Once the OS has booted the iBFT boot parameters are passed to the host OS, but still requires MPIO to be properly setup on each host.

Part II) Troubleshooting common issues:

- 1) Problems with [Twin-AX connectivity](#)
- 2) [Network connectivity issues](#).
- 3) [SANboot "Initialize error 1"](#)
- 4) ["Policy reference AuthProfileName does not resolve to named policy"](#)
- 5) [ENM source pinning error](#)
- 6) [Wrong version of firmware / UCSM / BIOS / driver](#)
- 7) [Discovery IP address](#)

Part III) Sample upstream switch configurations:

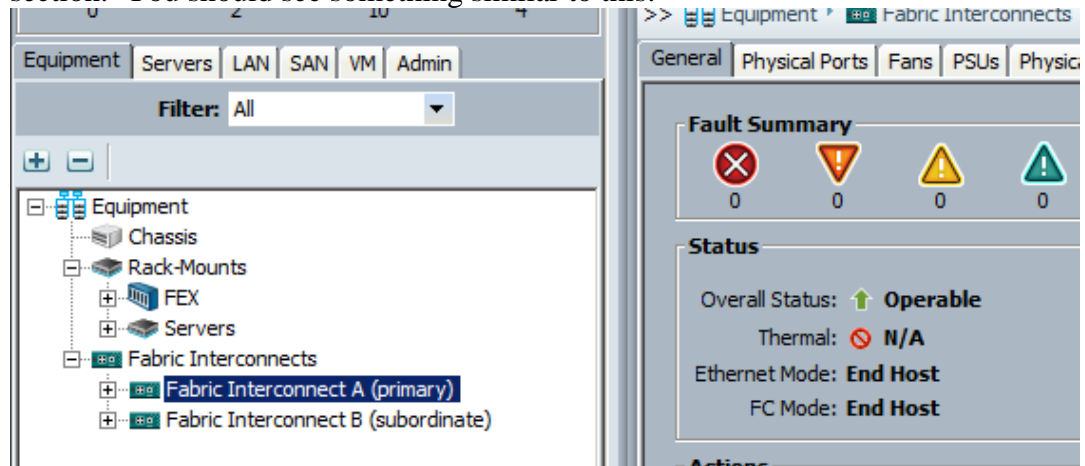
- 1) Standard etherchannel configuration:
- 2) VPC configuration with multiple upstream switches

Appendix A: Configuration Details

Determine UCS operation mode. → [#TOP](#)

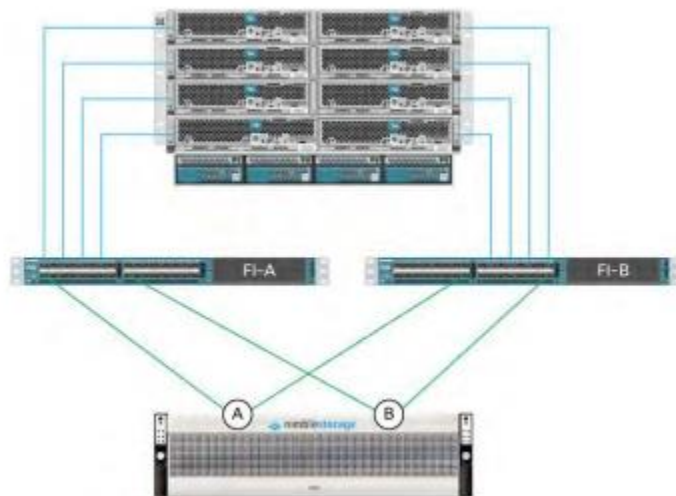
UCS operation mode determines how the Fabric Interconnects forward network traffic. Note that in this case we are only interested in the Ethernet operation mode. In Ethernet Switching mode, the FIs behave as a standard network switch and forwards traffic accordingly. However in Ethernet End-host mode the FIs behave as if the switch is a host. Ethernet End-host mode is the most common setting. Therefore portfast is an appropriate setting for any upstream switch connectivity to the FIs. This is an important consideration to avoid spanning tree loops and proper network convergence. To confirm which mode you in currently perform the following steps from the UCSM GUI:

- Go to the Equipment tab
- Expand the Fabric Interconnects section
- Select one of the Fabric Interconnects and observe the details in the General section. You should see something similar to this:



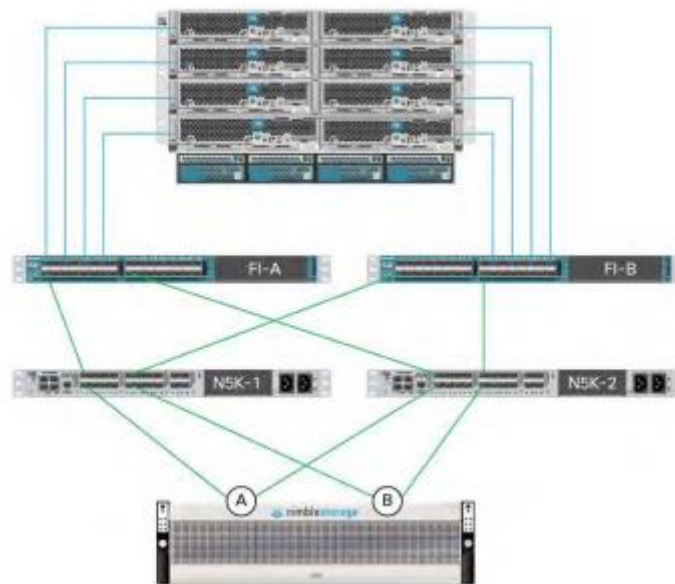
Determine UCS network topology: [#TOP](#)

Example1: Direct attach via Appliance ports (Dual subnets)



In this case Nimble Storage is directly connected to the Cisco Fabric Interconnects (FIs) as Appliance ports. Appliance ports are essentially untagged traffic bound for one specific VLAN in the UCS environment. In the below graphic each Nimble Controller uses one interface to connect to FI-A and the other to FI-B (for example tg1 connections from both controllers to FI-A and tg2 to FI-B). In addition there needs to be two separate VLANs (and associated subnet) for iSCSI connectivity. One VLAN will be specific to FI-A and the other will be specific to FI-B. The VLANs should exist only on a single FI and do not allow failover between the FIs. Each UCS blade server profile will in turn need to have a presence on each iSCSI VLAN. This is accomplished by creating a specific vNIC and assigning it a native VLAN of each of the iSCSI VLANs created previously. The host OS will have an IP presence in these subnets and in turn manage MPIO connectivity via these paths.

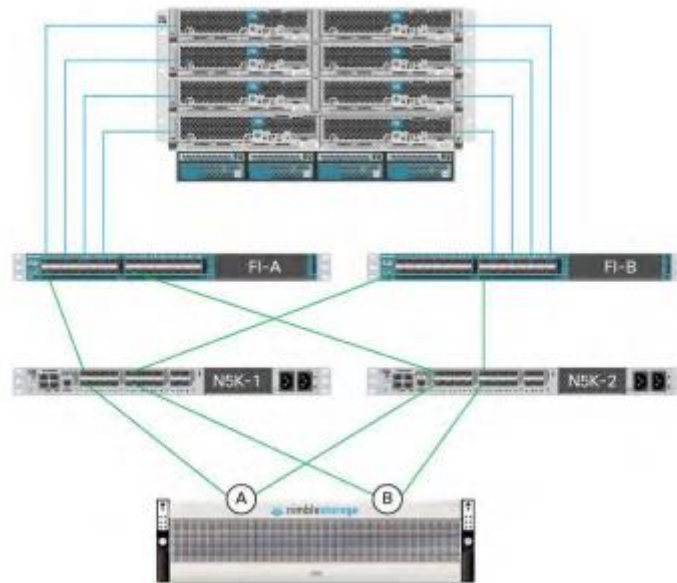
Example 2) Connectivity to one or more upstream access switches. (Single iSCSI VLAN)



The Nimble array can be connected to one or more upstream switches. The upstream switch (Nexus 5K in the below example) will need to configure the connections to the Nimble array as non-tagged access ports. The connectivity from the UCS FIs to the Nexus 5K will be of type “Network” or “Uplink”. Pay particular attention to the Native VLAN setting for these ports. If you are only going to trunk the iSCSI VLAN on the “Network Ports”, then set the Native VLAN to be the iSCSI VLAN. However, if you are trunking multiple VLANs over this Network port, then do not set the native VLAN to be the iSCSI VLAN to let the traffic remain “VLAN tagged”.

** If desired you can additionally use UCS pinning to specify which path to a given FI a host will take. This is a legacy mechanism for MPIO traffic, but will work when you have a single subnet for iSCSI connectivity. Note: using UCS interface pinning is not a substitute for host based MPIO requirements.

Example 3) Connectivity to one or more upstream access switches. (Multiple iSCSI VLANs)



This topology is physically identical to example 2. However in some cases it is desirable to have multiple VLANs for further redundancy. As in example 2 the Nimble Storage array is connected to the upstream switch (Nexus 5Ks in this example) as non-tagged access ports or as trunk ports with a native VLAN as the iSCSI subnet for that switch.

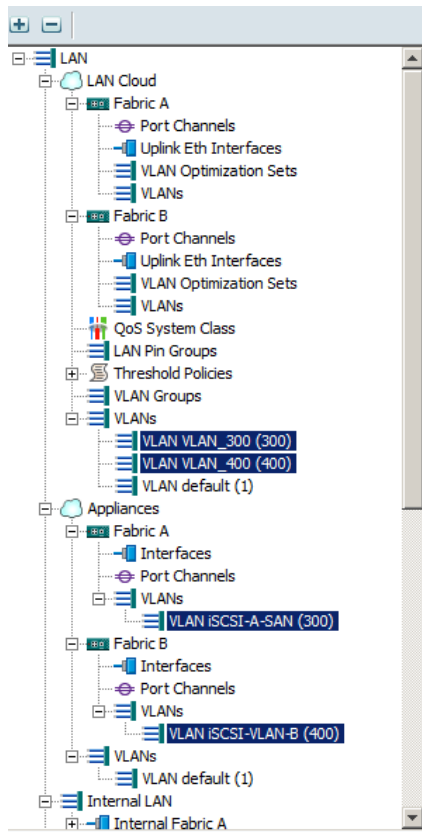
There needs to be two separate VLANs (and associated subnet) for iSCSI connectivity. One VLAN will be specific to N5K-1 and the other will be to N5K-2. Each UCS server profile will in turn need to have a presence on each iSCSI VLAN. This is accomplished by creating a specific vNIC and assigning it a native VLAN of each of the iSCSI VLANs created previously. The host OS will have an IP presence in these subnets and in turn manage MPIO connectivity via these paths. Note: you do NOT want to additionally add any type of UCS interface pinning if you are using multiple iSCSI subnets as this can have unpredictable results.

VLAN / LAN connectivity → [#TOP](#)

Example 1, Appliance ports (dual subnets)

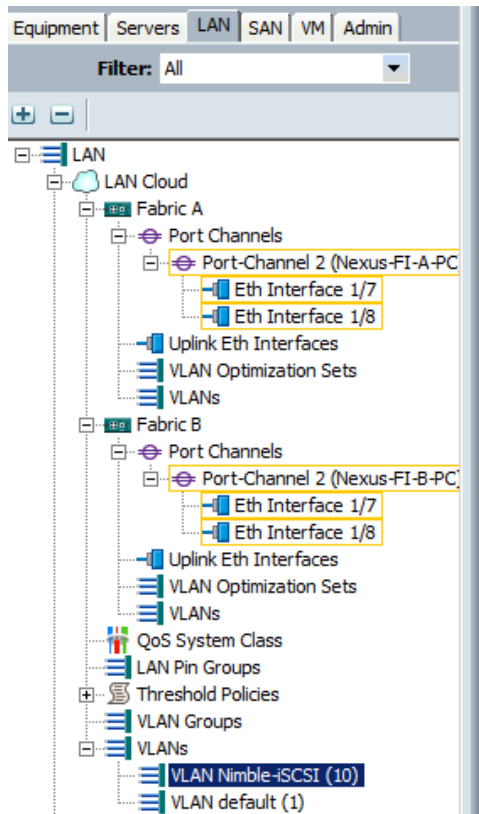
Create Appliance ports for any Nimble Storage data port directly connected to the FI.

Create VLANs that look similar to the below example. Note how in this example in the LAN Cloud section the 300 and 400 VLANs are in the general section. However in the Appliances section VLAN 300 is only in FI-A and VLAN 400 is only in FI-B. Interfaces 1/7 and 1/8 in the Appliance section represent the connections from the Nimble Storage controllers.



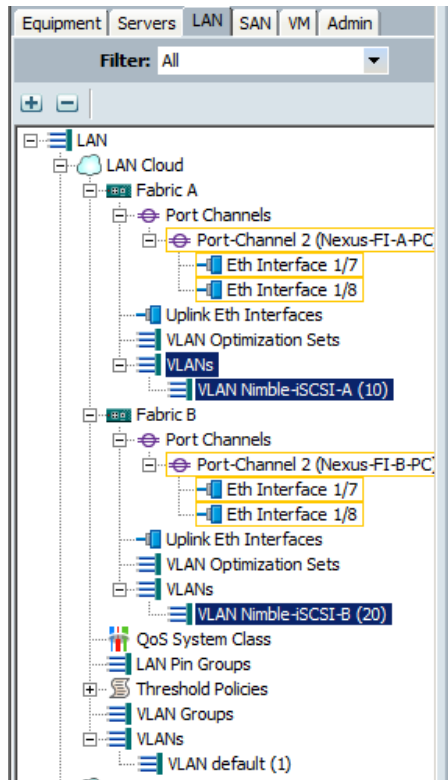
Example 2) Connectivity to one or more upstream access switches. (Single iSCSI VLAN)

Create a single VLAN configuration that look similar to the below example. Note how the VLAN exists in the global section and is NOT configured as the Native VLAN. Also note that there are port-channels setup for the Network uplink ports which go to the upstream Nexus switch. This is not required but usually desired for network redundancy. The port-channel configuration also requires additional configuration with the upstream switch for either standard port channels or a virtual port channel (vpc).



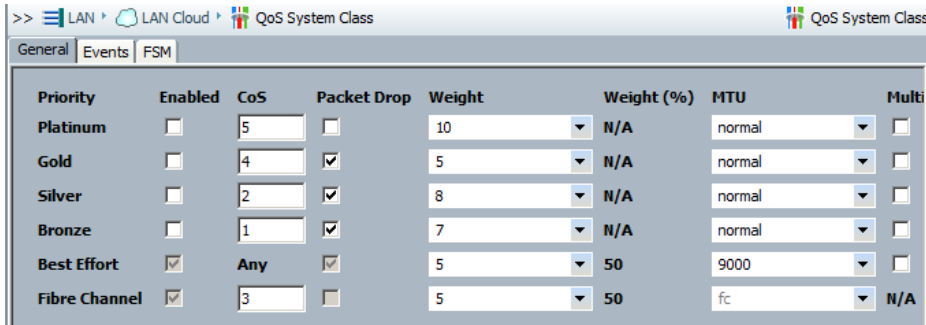
Example 3) Connectivity to one or more upstream access switches. (Multiple iSCSI VLANs)

In order to implement the above changes, you need to create a dual VLAN configuration that look similar to the below example. Also note that there are port-channels setup for the Network uplink ports which go to the upstream Nexus switch. This is not required but usually desired for network redundancy. The port-channel configuration also requires additional configuration with the upstream switch for either standard port channels or a virtual port channel (vpc).



Configure QoS policy for Jumbo Frames → [#TOP](#)

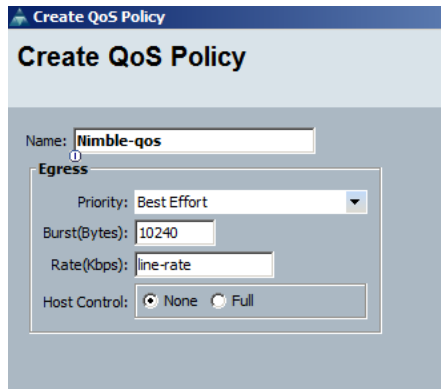
- Step 1** In the Navigation pane, click the LAN tab.
- Step 2** In the LAN tab > Select LAN cloud > QoS System class
- Step 3** Determine the Class of Service (CoS) you want to use for your iSCSI traffic. However note that if you are using uplink ports via a Nexus 5K, then you will in effect be using the “Best Effort” CoS.
Note: You should only enable the CoS types that you are actually using. Otherwise there will be wasted resources that could potentially lead to a performance bottleneck.
- Step 4** Increase the MTU of the CoS that you will be using to a value of 9000 and select Save Changes. The QoS system class settings are now applied.



Priority	Enabled	CoS	Packet Drop	Weight	Weight (%)	MTU	Multi
Platinum	<input type="checkbox"/>	5	<input type="checkbox"/>	10	N/A	normal	<input type="checkbox"/>
Gold	<input type="checkbox"/>	4	<input checked="" type="checkbox"/>	5	N/A	normal	<input type="checkbox"/>
Silver	<input type="checkbox"/>	2	<input checked="" type="checkbox"/>	8	N/A	normal	<input type="checkbox"/>
Bronze	<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	7	N/A	normal	<input type="checkbox"/>
Best Effort	<input checked="" type="checkbox"/>	Any	<input checked="" type="checkbox"/>	5	50	9000	<input type="checkbox"/>
Fibre Channel	<input checked="" type="checkbox"/>	3	<input type="checkbox"/>	5	50	fc	N/A

Step 5 Next we need to create a custom QoS policy.

- While still in the LAN tab, navigate to the Policies section.
- Expand the root section and look for the QoS policies. Right click and select "Create QoS Policy".
- Name the QoS policy and select the appropriate CoS type appropriate for iSCSI traffic (See step 4 above). Save changes and the custom QoS policy is now created. Reference this graphic:



Create QoS Policy

Name:

Egress

Priority:

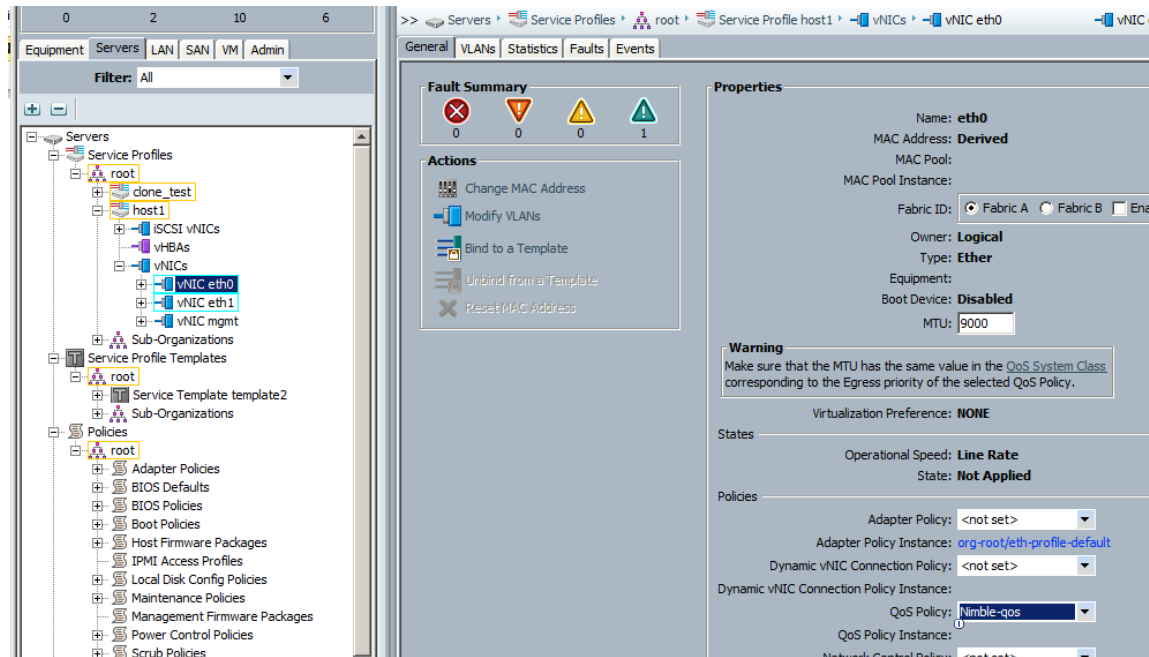
Burst(Bytes):

Rate(Kbps):

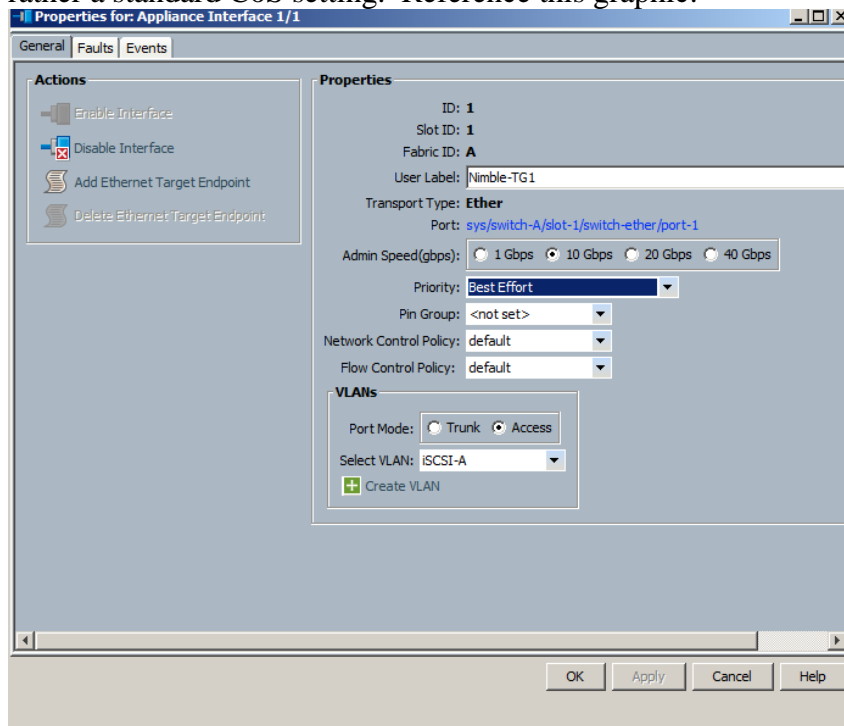
Host Control: ☒ None ☐ Full

Applying the QoS policy with Jumbo Frames → [#TOP](#)

- Go to the Server Profile, select the physical vNIC to be used with iSCSI traffic. Change the QoS policy for the vNIC. Also be sure to update the MTU size to reflect Jumbo Frames (9000). Note that this second step isn't actually a QoS setting, but rather the setting on the physical interface when the card is initialized during the boot up sequence. Repeat this for every vNIC that will carry iSCSI traffic. Reference this graphic:



- b) If using Appliance ports, navigate to the Equipment tab then to the Fabric Interconnect section. Select one of the Appliance ports. Right click and select “Show Navigator” followed by selecting “Show Interface”. You will verify that the QoS policy is set to the proper CoS setting. Note that the custom QoS policy we created earlier is not used, but rather a standard CoS setting. Reference this graphic:



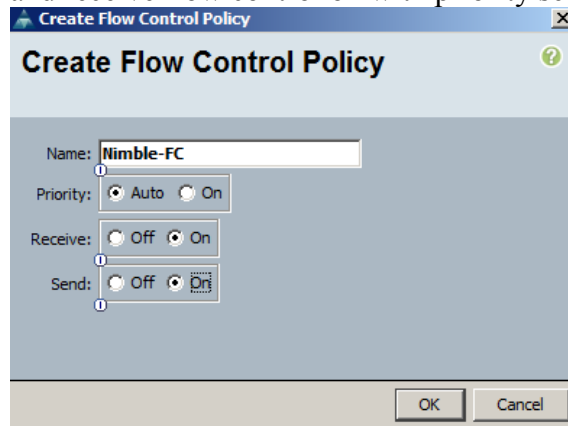
Upstream switch QoS configuration for Jumbo Frames → [#TOP](#)

Required steps for enabling Jumbo frames via QoS policy on Nexus 5K switch:

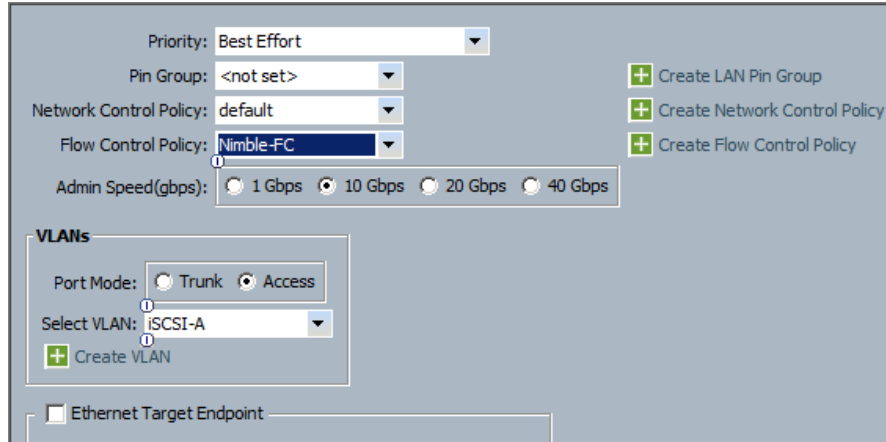
```
switch(config)#policy-map type network-qos jumbo
switch(config-pmap-nq)#class type network-qos class-default
switch(config-pmap-c-nq)#mtu 9216
switch(config-pmap-c-nq)#exit
switch(config-pmap-nq)#exit
switch(config)#system qos
switch(config-sys-qos)#service-policy type network-qos jumbo
```

Create, Configure, and apply a flow control policy: → [#TOP](#)

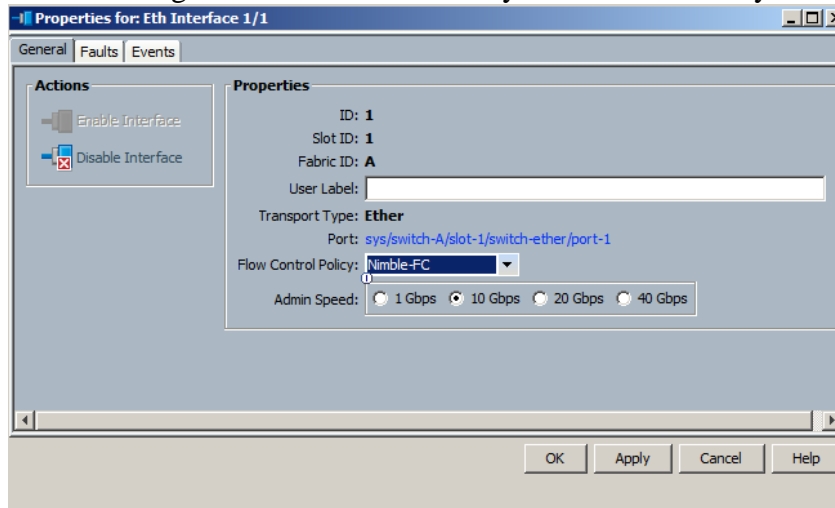
- a. Navigate to LAN -> Flow Control Policies.
- b. Right click and select “Create Flow Control Policy”
- c. Select which options you want and select OK. Typically it is desired to turn send and receive flow control on with priority set to “Auto”. Reference this graphic:



- d. For any UCS Appliance ports do the following:
 - i. Navigate to the Equipment tab -> Fabric Interconnects -> Select an appliance port.
 - ii. Apply the newly created Flow control policy to the port. Repeat this step for every Appliance port on both Fabric Interconnects. Reference this graphic:



- e. For any UCS Network Uplink ports do the following:
- Select the Equipment tab-> Fabric Interconnects -> Network Uplink ports -> Navigate
 - Change the Flow Control Policy to match the newly created policy.



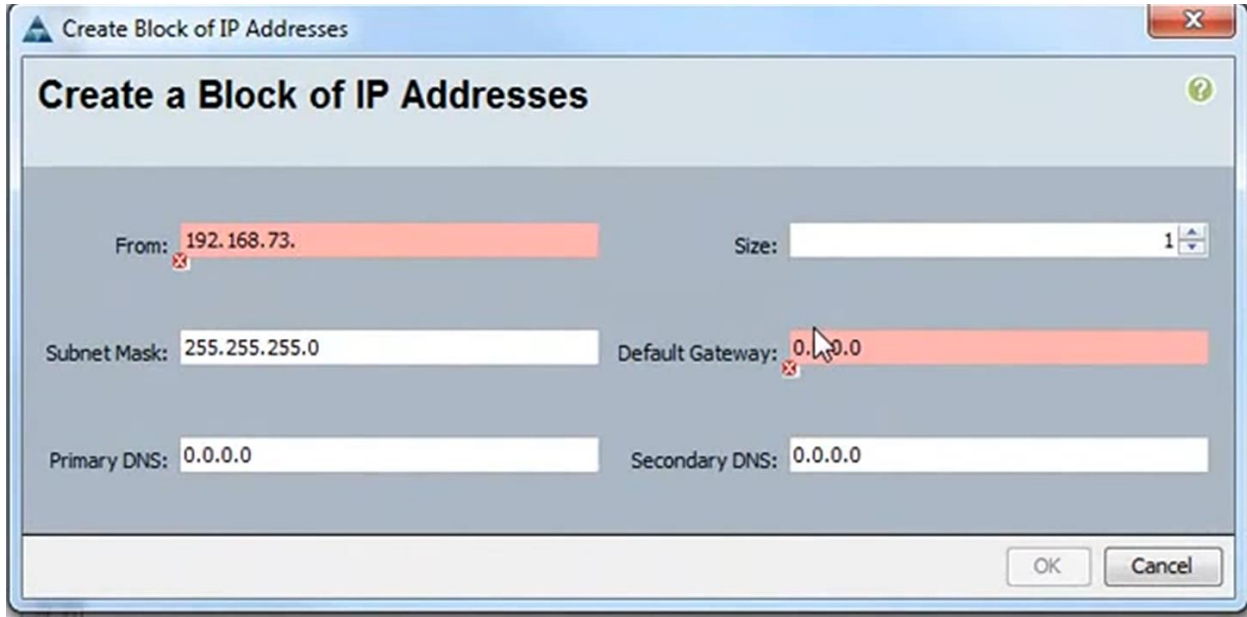
Configure the appropriate Network Control Policy → [#TOP](#)

- Go to the LAN tab -> “Network Control Policy”-> default
- Set the “Action on Uplink” fail is set to “warning”. This will ensure that UCS will not failover from one FI to the other in the event of a link down. It is preferable to use this setting and let the host OS MPIO do all path management in the event of a link down.

Create an IP Pool: → [#TOP](#)

- Step 1** In the Navigation pane, click the LAN tab.
- Step 2** In the LAN tab, expand LAN > Pools > *Organization_Name* .
- Step 3** Right-click IP Pools and select Create IP Pool.
- Step 4** Name the IP Pool

- Step 5** Define the Assignment Order (Default or Sequential)
- Step 6** Click Next
- Step 7** In the Add IP Blocks page of the Create IP Pool wizard, Click Add.
- Step 8** Define the first IP in the block of IPs (i.e. From)
- Step 9** Define the number of IPs in the pool (i.e. Size)
- Step 10** Define the Subnet Mask
- Step 11** Define the Default Gateway.

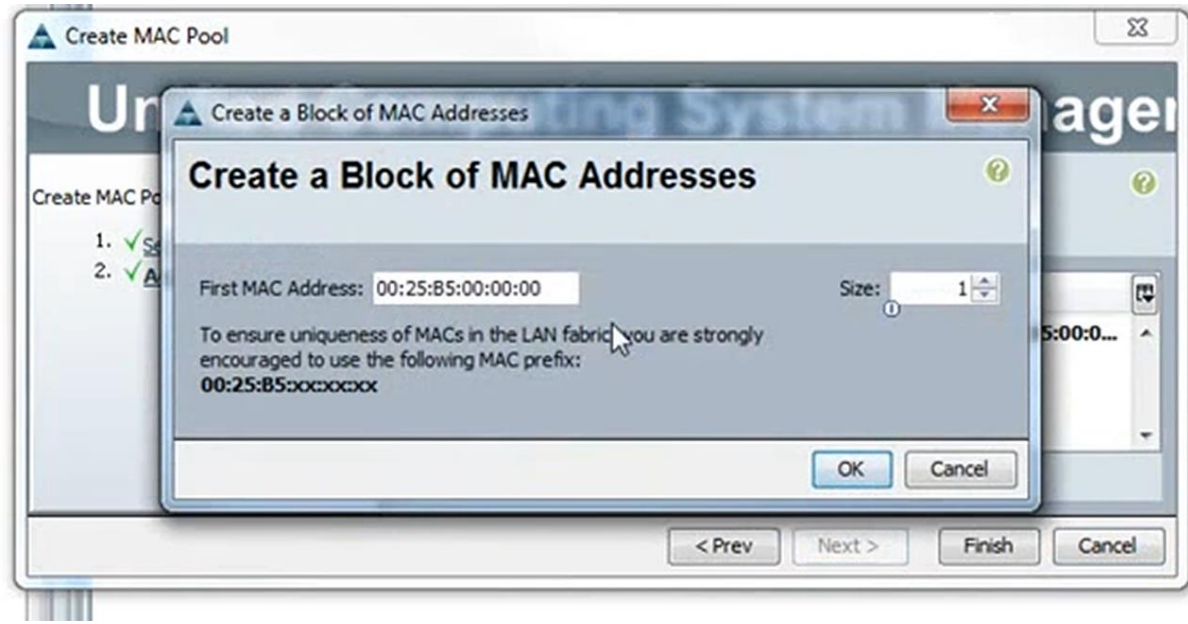


Create a MAC Pool: → [#TOP](#)

Procedure:

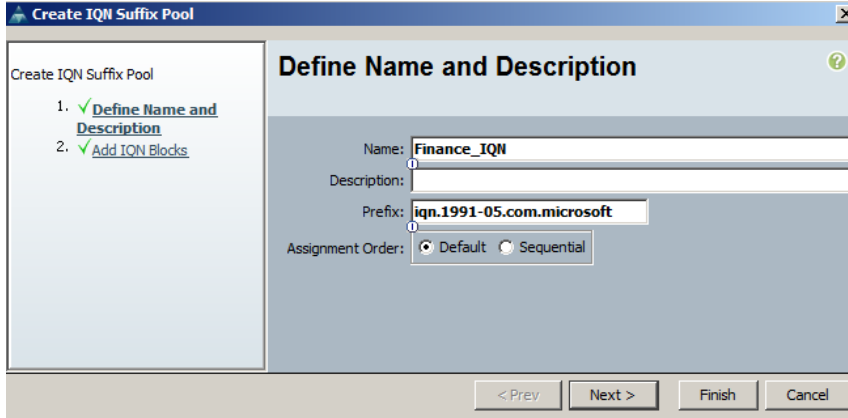
- Step 1** In the Navigation pane, click the LAN tab.
- Step 2** In the LAN tab, expand LAN > Pools.
- Step 3** Expand the node for the organization where you want to create the pool.
- Step 4** Right-click MAC Pools and select Create MAC Pool.
- Step 5** In the first page of the Create MAC Pool wizard:
 - a. Name the MAC Pool (i.e. iSCSI MAC Pool)
 - b. Click Next.
- Step 6** In the second page of the Create MAC Pool wizard:
 - a. Click Add.

- b. In the Create a Block of MAC Addresses page, enter the first MAC address in the pool and the number of MAC addresses to include in the pool.
- c. Click OK.
- d. Click Finish.



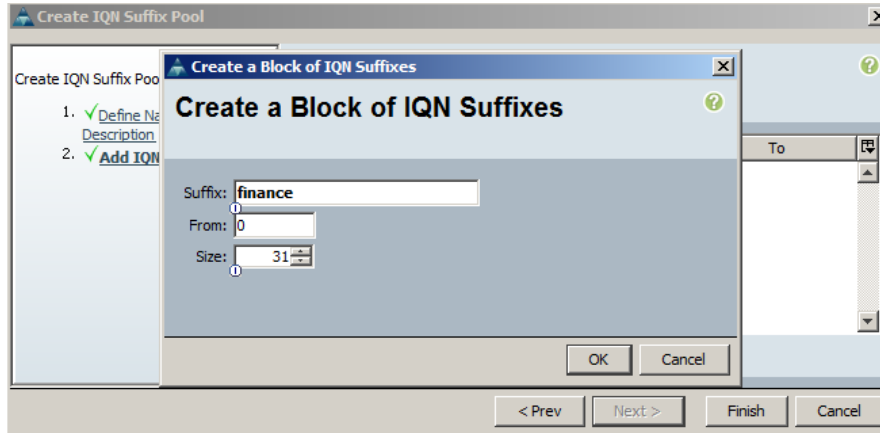
Create an IQN pool: → [#TOP](#)

- Step 1** In the Navigation pane, click the SAN tab.
- Step 2** In the SAN tab, expand SAN > Pools > *Organization_Name* > IQN Pools
- Step 3** Right-click IQN Pool and select Create IQN Suffix pool.
- Step 4** Select a name of the IQN pool and choose a Prefix. The prefix should have the standard iqn format as illustrated below. Select Next.



The 'Create IQN Suffix Pool' dialog box is shown. It has a left sidebar with a progress indicator showing two steps: '1. Define Name and Description' (checked) and '2. Add IQN Blocks'. The main area is titled 'Define Name and Description' and contains the following fields: 'Name' (Finance_IQN), 'Description' (empty), 'Prefix' (iqn.1991-05.com.microsoft), and 'Assignment Order' (radio buttons for 'Default' and 'Sequential', with 'Default' selected). At the bottom are buttons for '< Prev', 'Next >', 'Finish', and 'Cancel'.

Step 6 Select Add to add a new set of suffix blocks for iqn assignment. Note that the suffix piece of the iqn is a specific identifier to indicate an organizational group or set of hosts. Be sure to use the size to indicate how many hosts you want to connect.



The 'Create a Block of IQN Suffixes' dialog box is shown. It has a left sidebar with a progress indicator showing two steps: '1. Define Name and Description' (checked) and '2. Add IQN Blocks' (checked). The main area is titled 'Create a Block of IQN Suffixes' and contains the following fields: 'Suffix' (finance), 'From' (0), and 'Size' (31). At the bottom are buttons for 'OK' and 'Cancel'. The main dialog box also has buttons for '< Prev', 'Next >', 'Finish', and 'Cancel'.

Step 7 Verify that the pool is successfully created with no errors.

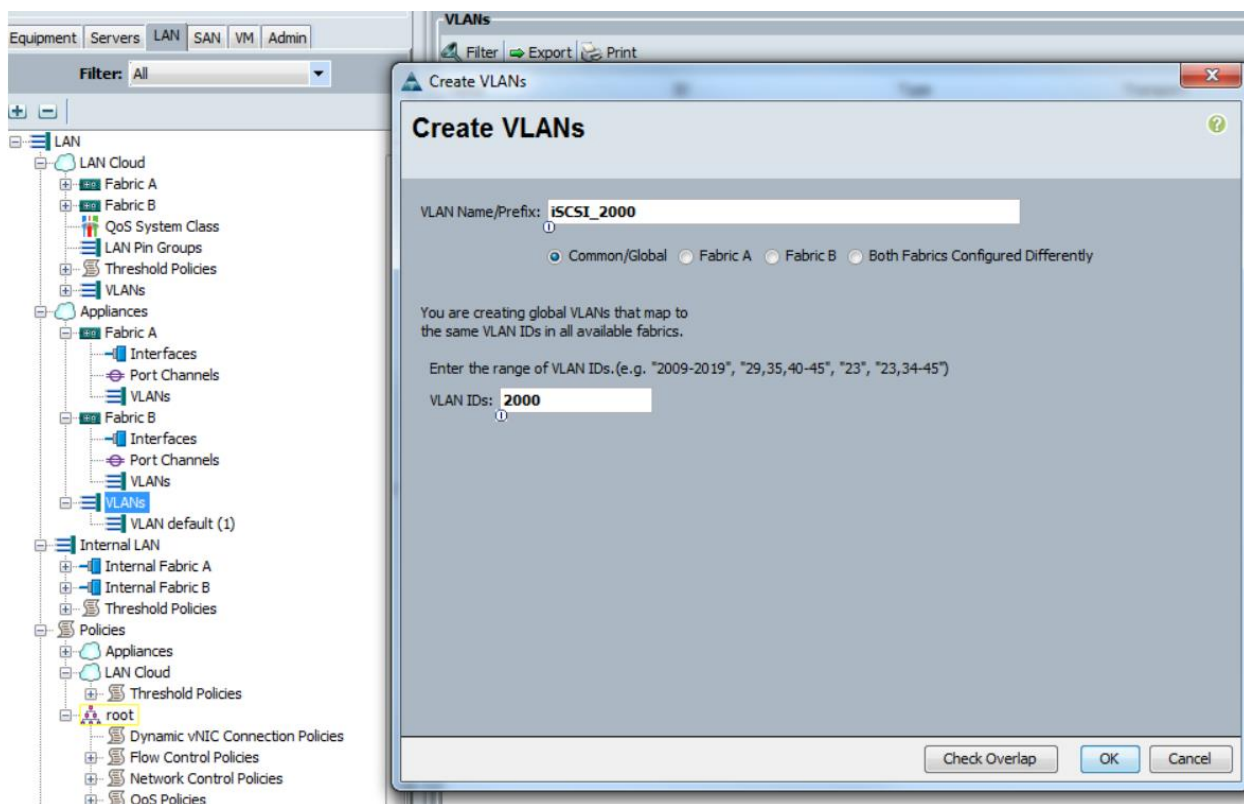
Create an Appliance VLAN: → [#TOP](#)

Procedure:

- Step 1** In the Navigation pane, click the LAN tab.
- Step 2** In the LAN tab, expand LAN > Appliances > VLANS.
- Step 3** Right click on VLANS and select Create VLANs.
- Step 4** Name the VLAN (i.e. iSCSI VLAN)

Step 5 Enter a VLAN ID

Step 6 Click OK



1) Configure Appliance Ports & Bind the Appliance Ports to the Appliance VLAN: → #TOP

Procedure: (Repeat this step on each Fabric Interconnect. The array will need two ports per controller.)

Step 1 In the Navigation pane, click the Equipment tab.

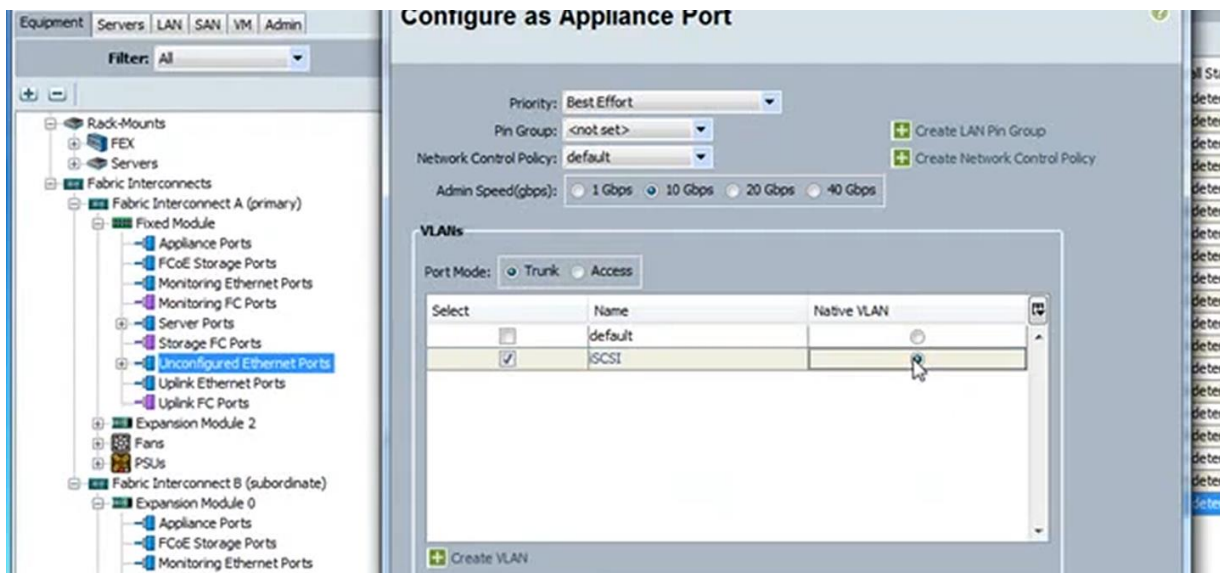
Step 2 On the Equipment tab, expand Equipment > Fabric Interconnects > *Fabric_Interconnect_Name*.

Step 3 Depending upon the location of the ports you want to configure, expand one of the following:

- Fixed Module
- Expansion Module

Step 4 Click on the ports under Unconfigured Ethernet Ports.

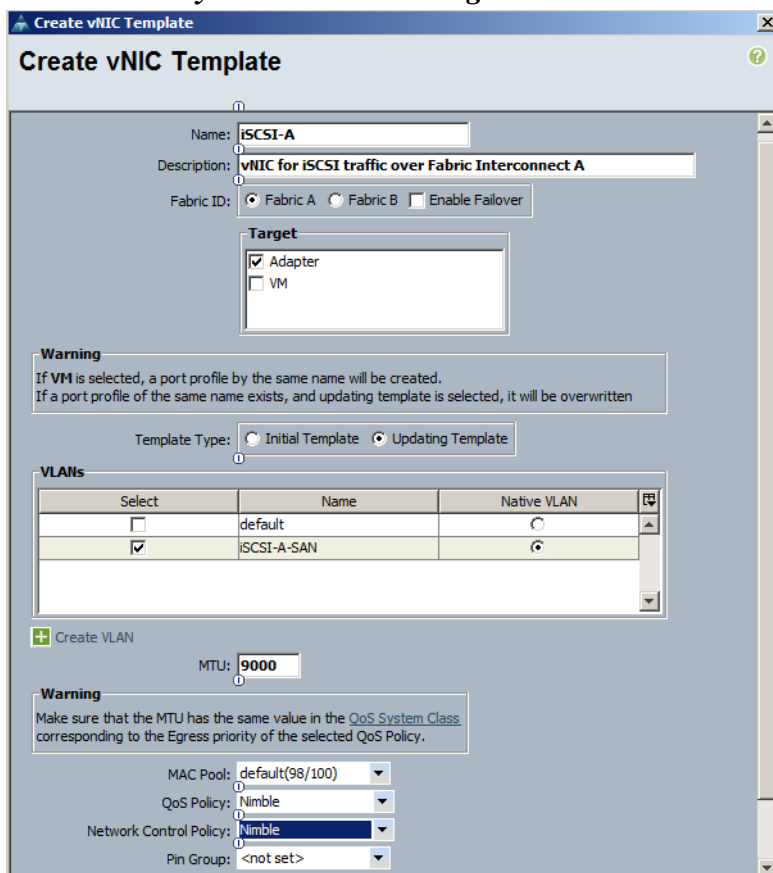
- Step 5** Right-click the selected port and choose Configure as Appliance Port.
- Step 6** If the Cisco UCS Manager GUI displays a confirmation dialog box, click Yes.
- Step 7** In the Configure as Appliance Port dialog box, complete the following fields:
- Set the Priority to Gold.
 - Set the Admin Speed to 10Gbps.
- Step 8** In the VLANs area, do the following:
- In the Port Mode field, click Trunk.
 - Select the check box in the iSCSI VLAN row.
 - Select the radio button to designate the iSCSI VLAN as the native VLAN.
- Step 9** Click OK.



Creating vNIC Templates → [#TOP](#)

Procedure: Do the below procedure a minimum of three times. The first time create a management vNIC template. Then create two vNIC templates for iSCSI connectivity (with diverse paths to FI-A and FI-B).

- Step 1** In the Navigation pane, click the LAN tab.
- Step 2** In the LAN tab, expand LAN > Policies > Root.
- Step 3** Right click on vNIC Templates and select Create vNIC Templates.
- Step 4** Name the vNIC template (i.e. Management / iSCSI-A / iSCSI-B).
- Step 5** Next to Fabric ID, choose Enable Failover. (Note you only want to enable failover for management traffic, do not enable this for iSCSI vNICs)
- Step 6** In the Template Type field, select Updating Template.
- Step 7** Select the appropriate VLAN(s) that you want to use. Note in this example the vNIC uses only the Native (untagged) traffic.
- Step 7** Select the iSCSI MAC Pool from the MAC Pool drop down menu.
- Step 8** Choose MTU size. Note: if you choose a MTU size over 1500 (Jumbo frames) be sure that the QoS Policy is set correctly to honor this.
- Step 9** Select the desired [QoS](#) and [NCP](#) policies.
- Step 10** Select OK to save.
- Note:** *If any of these parameters need to change, this can be accomplished on the fly because it is an updating template. Just be sure that the affected hosts are ready to receive the change.*



Create vNIC Template

Name:

Description:

Fabric ID: ☒ Fabric A ☐ Fabric B ☐ Enable Failover

Target:
☒ Adapter
☐ VM

Warning
If VM is selected, a port profile by the same name will be created.
If a port profile of the same name exists, and updating template is selected, it will be overwritten

Template Type: ☐ Initial Template ☒ Updating Template

VLANs

Select	Name	Native VLAN
<input type="checkbox"/>	default	<input type="radio"/>
<input checked="" type="checkbox"/>	ISCSI-A-SAN	<input checked="" type="radio"/>

[+ Create VLAN](#)

MTU:

Warning
Make sure that the MTU has the same value in the [QoS System Class](#) corresponding to the Egress priority of the selected QoS Policy.

MAC Pool:

QoS Policy:

Network Control Policy:

Pin Group:

Create iSCSI Adapter Policy: → [#TOP](#)

Procedure:

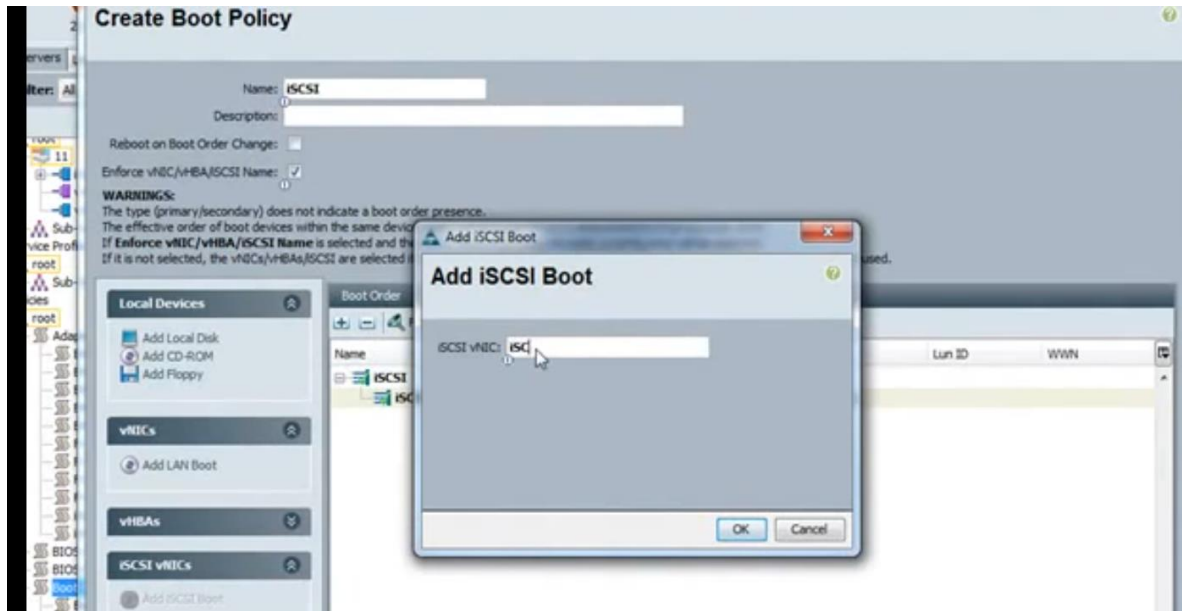
- Step 1** In the Navigation pane, click the Servers tab.
- Step 2** In the Servers tab, expand Servers > Policies > *Organization_Name*.
- Step 3** Right click on Adapter Policies and select Create iSCSI Adapter Policies.
- Step 4** Name the Adapter Policy (i.e. iSCSI) and leave the rest of the defaults.
- Step 5** Click OK



Create a Boot Policy for iSCSI SANboot: → [#TOP](#)

Procedure: (Repeat this step in order to create a boot policy associated with each Fabric Interconnect – i.e. iSCSI-A Boot Policy bound to iSCSI-A vNIC Template and iSCSI-B Boot Policy bound to iSCSI-B vNIC Template.)

- Step 1** In the Navigation pane, click the Servers tab.
- Step 2** In the Servers tab, expand Servers > Policies > *Organization_Name*.
- Step 3** Right click on Boot Policy and select Create Boot Policy.
- Step 4** Name the Boot Policy (e.g. Nimble-SANboot).
- Step 5** Add a CDROM to allow for installation media.
- Step 6** Click Add iSCSI Boot.
- Step 7** Type iSCSI vNIC Template name (i.e. iSCSI-A) in the field. (*Note this has to be the actual name of the iSCSI vNIC interface in the Service Profile*)
- Step 8** Repeat the step 7 and add the iSCSI-B iSCSI vNIC template.
- Step 9** Click OK to save changes.



Create iSCSI Initiator Group in Nimble GUI: → [#TOP](#)

Procedure:

- Step 1** Log into the Nimble GUI.
- Step 2** Click Manage.
- Step 3** Select Initiator Groups from the drop down.
- Step 4** Once in the Initiator Groups tab, click New Initiator Group.
- Step 5** Name the Initiator Group.
- Step 6** Click Add Initiator.
- Step 7** Add IQNs from the iSCSI host that will be associated with this Initiator Group. These IQNs can be collected from UCS manager. Go to the Service Profile under the Boot Order Tab. Click Set Boot Parameters for each Boot Policy. The IQN name is listed there.
- Step 8** Click OK

Create a iSCSI Boot Performance Policy on the Nimble array:

→ [#TOP](#)

Procedure:

- Step 1** Log into the Nimble GUI.
- Step 2** Click Manage.
- Step 3** Select Performance Policy from the drop down.
- Step 4** Once in the Performance Policy tab, click New Performance Policy.
- Step 5** Name the Performance Policy (i.e. iBoot_host name).
- Step 6** Set the block size to 4K.
- Step 7** Select the checkboxes for Caching and Compression.
- Step 8** Click OK

Create a boot volume on the Nimble Array: → [#TOP](#)

Procedure:

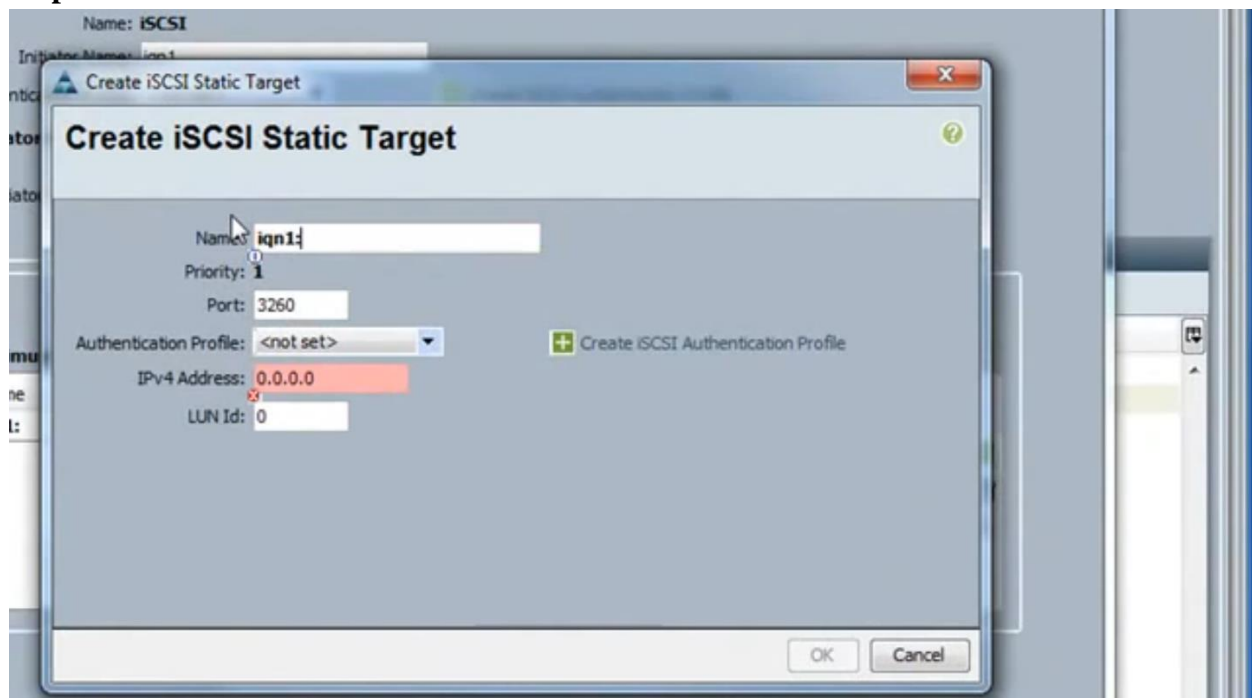
- Step 1** Log into the Nimble GUI.
- Step 2** Click Volumes.
- Step 3** Click New Volume.
- Step 4** Name the Volume
- Step 5** Select the newly created iSCSI Boot Performance Policy (optional, see previous step)
- Step 6** Click Limit Access
- Step 7** Select the newly created Initiator Group for the Host
- Step 8** Select Allow Multiple Initiator Access (*Very important as you will have multiple initiators accessing this boot LUN from the same host*)
- Step 9** Set the capacity of the volume appropriate to the OS.
- Step 10** Click next
- Step 11** For the Protection Policy, select None.
- Step 12** Click Finish

Set Static IQN for iSCSI Boot Parameters: → [#TOP](#)

Procedure: (Repeat process for each vNIC – iSCSI-A & iSCSI-B.)

- Step 1** SSH into the Nimble array.

- Step 2** Pull a list of the volumes on the Nimble array. Use command: `vol --list`.
- Step 3** Pull the information for the iSCSI boot volume. Use command: `vol --info Volume Name | grep iqn`
- Step 4** Copy the IQN name of the iSCSI Target.
- Step 5** Return to UCS Manager.
- Step 6** In Boot Policy tab, select Set iSCSI Boot Parameters.
- Step 7** Name the iSCSI target.
- Step 8** Select the iSCSI Static Target Interface radio button.
- Step 9** Click the “+” button to add a static target.
- Step 10** Paste the IQN name of the Nimble array in the Name field (from Step 4)
- Step 11** Enter the Discovery IP of the Nimble array in the IPv4 field.
- Step 12** Click OK



Creating and applying a LAN Connectivity Policy → [#TOP](#)

Procedure: A LAN Connectivity Policy defines the number of Ethernet vNICs, iSCSI vNICs, and the associated VLANs. This is then in turn applied to an individual Service Profile or a Service Profile template. Below is a procedure on a typical policy defined for an iSCSI boot host.

- Step 1** In the UCSM navigation menu select the LAN tab.
- Step 2** Under the Policies section right click on LAN Connectivity policy to create. Fill in the name and description of the new LAN connectivity policy.

Step 3 Select Add to add the first vNIC




Create LAN Connectivity Policy

Name:

Description:

Click **Add** to specify one or more vNICs that the server should use to connect to the LAN.

Name	MAC Address
------	-------------

 Delete  Add  Modify

Step 4 Fill in the name of the interface.

Step 5 Select the “Use vNIC template” check box


Step 6 From the drop down menu select the desired vNIC template. In the example below the mgmt template was used.

Step 7 Select the appropriate adapter performance profile

Create vNIC


Name:

Use vNIC Template: ☒

 Create vNIC Template

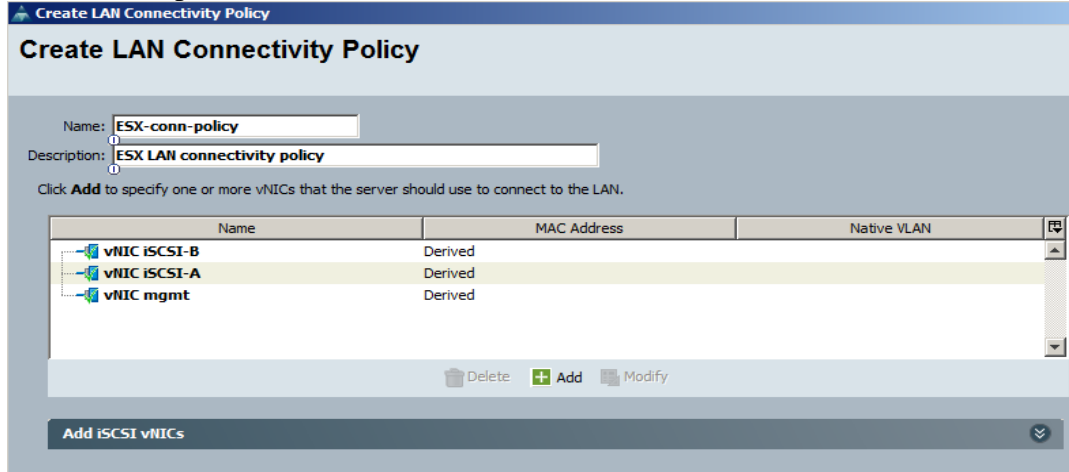
vNIC Template:

Adapter Performance Profile

Adapter Policy: 

Step 8 Select OK. Continue to add vNICs using the vNIC templates. You should have a

minimum of 1 management vNIC and 2 iSCSI vNICs (one for each Fabric Interconnect path).









Create LAN Connectivity Policy

Name:

Description:

Click **Add** to specify one or more vNICs that the server should use to connect to the LAN.

Name	MAC Address	Native VLAN
 vNIC iSCSI-B	Derived	
 vNIC iSCSI-A	Derived	
 vNIC mgmt	Derived	

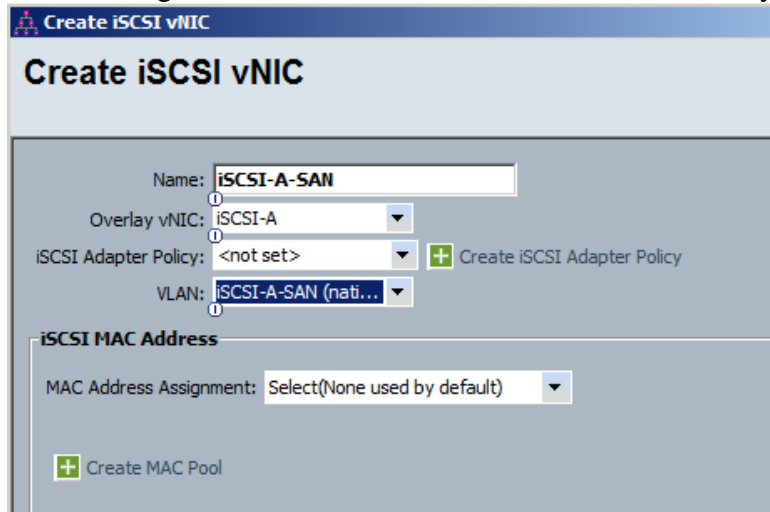
 Delete  Add  Modify

Add iSCSI vNICs

Step 9 Select the “Add iSCSI vNICs” drop down arrow.

Step 10 Select Add to bring up the “Create iSCSI vNIC” menu.


Step 11 Select a Name, overlay vNIC, and select the appropriate VLAN. Note you do not need to assign a new MAC address as it will be inherited by the overlay vNIC.



Create iSCSI vNIC

Name:


Overlay vNIC:

iSCSI Adapter Policy: 

VLAN:

iSCSI MAC Address

MAC Address Assignment:

 Create MAC Pool




Step 12 Example of finished setup:




Create LAN Connectivity Policy

Name:



Description:




Click **Add** to specify one or more vNICs that the server should use to connect to the LAN.

Name	MAC Address	Native VLAN
 vNIC iSCSI-B	Derived	
 vNIC iSCSI-A	Derived	
 vNIC mgmt	Derived	

 Delete  Add  Modify

Add iSCSI vNICs

Name	Overlay vNIC Name	iSCSI Adapter Policy	MAC Add
 iSCSI vNIC iSCSI-B-SAN	iSCSI-B		Derived
 iSCSI vNIC iSCSI-A-SAN	iSCSI-A		Derived

 Add  Delete  Modify

Step 13 Select OK. The LAN connectivity policy is now ready to be applied.



Step 14 To apply the LAN connectivity policy:

- Navigate to either an individual Service Profile or Service Profile template.
- Select the Network tab
- Select the LAN connectivity dropdown box and Save Changes.

>> Servers > Service Profile Templates > root > Service Template BootFromSAN > Service Template BootFromSA

General Storage Network iSCSI vNICs Boot Order Policies Events FSM

Actions

-  Change Dynamic vNIC Connection Policy
-  Modify vNIC/vHBA Placement

Dynamic vNIC Connection Policy

Nothing Selected


vNIC/vHBA Placement Policy

Nothing Selected

LAN Connectivity Policy

LAN Connectivity Policy:

LAN Connectivity Policy Instance:

 Create LAN Connectivity Policy

vNICs

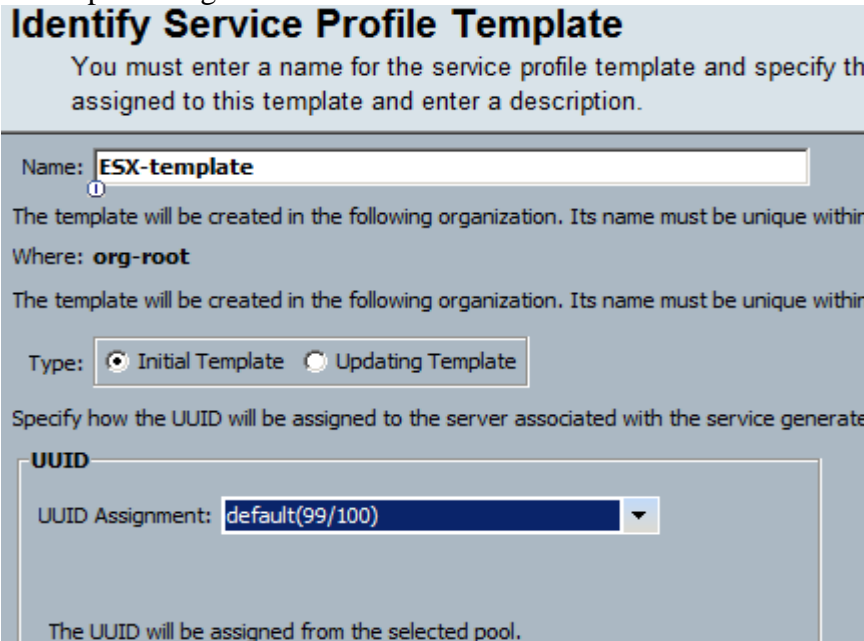
Creating a Service Profile Template → [#TOP](#)

Note: There are two types of Service Profile templates (initial and updating). For any iSCSI SANboot hosts you will need to use an initial template. Updating Service Profile templates do not allow unique LUN boot entries.

Step 1 In the UCSM navigation menu select the Servers tab.

Step 2 Right click on Service Profile templates and select “Create Service Profile Template”

Step 3 Select a name and choose the “initial template” radio button. Select a UUID server pool assignment and then select “Next”.





Step 4 On the next screen, select the “Use Connectivity Policy” radio button.



Step 5 Select the LAN Connectivity Policy dropdown box and select the policy you created [here](#):


Step 6 In the initiator name section select the drop down for the IQN pool you created [here](#) and select Next.

Networking
Optionally specify LAN configuration information.

Dynamic vNIC Connection Policy: Select a Policy to use (no Dynamic vNIC Policy by default)   Create Dynamic vNIC Connection Policy

How would you like to configure LAN connectivity? ☐ Simple ☐ Expert ☐ No vNICs ☒ Use Connectivity Policy



LAN Connectivity Policy: ESX-conn-policy   Create LAN Connectivity Policy

Initiator Name
Initiator Name Assignment: IQN-Pool(100/100) 

- Step 7** On the next page in the question “How would you like to configure SAN connectivity”. Select “no vHBAs”. Then Next.

Storage
Optionally specify disk policies and SAN configuration information.

Select a local disk configuration policy.

Local Storage: Select Local Storage Policy to use   Create Local Disk Configuration Policy

If nothing is selected, the default Local Storage configuration policy will be assigned to this service profile.

How would you like to configure SAN connectivity? ☐ Simple ☐ Expert ☒ No vHBAs ☐ Use Cor

This server associated with this service profile will not be connected to a storage area network.

- Step 8** Select Next to skip the zoning section as it does not apply.
- Step 9** Confirm the vNIC / vHBA placement is similar to the following and select “Next”. Note that the management port is the first PCI device discovered. This configuration is required to prevent issues with SANboot installs (such as ESX) as first PCI device discovered will become the management port.




vNIC/vHBA Placement

Specify how vNICs and vHBAs are placed on physical network adapters

vNIC/vHBA Placement specifies how vNICs and vHBAs are placed on physical network adapters (mezzanine) in a server hardware configuration independent way.

Select Placement: Let System Perform Placement + Create Placement Policy

System will perform automatic placement of vNICs and vHBAs based on PCI order.

Name	Address	Order
 vNIC mgmt	Derived	1
 vNIC iSCSI-B	Derived	2
 vNIC iSCSI-A	Derived	3

Step 10 Select a [boot policy](#) and then select “Next”. The example below shows a boot from SAN configuration.

Server Boot Order

Optionally specify the boot policy for this service profile template.

Select a boot policy.

Boot Policy: Nimble-SANboot + Create Boot Policy

Name: **Nimble-SANboot**

Description:





Reboot on Boot Order Change: **No**

Enforce vNIC/vHBA/iSCSI Name: **Yes**

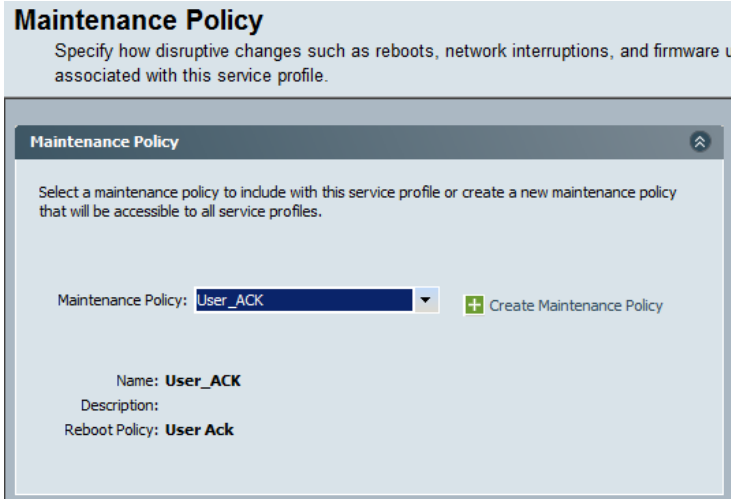
WARNING:
The type (primary/secondary) does not indicate a boot order presence.
The effective order of boot devices within the same device class (LAN/Storage/iSCSI) is determined by PCIe bus scan order.
If **Enforce vNIC/vHBA/iSCSI Name** is selected and the vNIC/vHBA/iSCSI does not exist, a config error will be reported.
If it is not selected, the vNICs/vHBAs/iSCSI are selected if they exist, otherwise the vNIC/vHBA/iSCSI with the lowest PCIe bus scan order is used.

Boot Order

+ Add - Remove Filter Export Print

Name	Order	vNIC/vHBA/iSCSI vNIC	Type	Lun ID	WWN
 CD-ROM	1				
 iSCSI	2				
 iSCSI		iSCSI-A	Primary		
 iSCSI		iSCSI-B	Secondary		

Step 11 Choose a server maintenance policy. Make sure to use one that requires acknowledgement prior to rebooting a host. This setting will undoubtedly save you an unplanned reboot in the future.





Maintenance Policy

Specify how disruptive changes such as reboots, network interruptions, and firmware updates are handled for the service profiles associated with this service profile.

Maintenance Policy

Select a maintenance policy to include with this service profile or create a new maintenance policy that will be accessible to all service profiles.

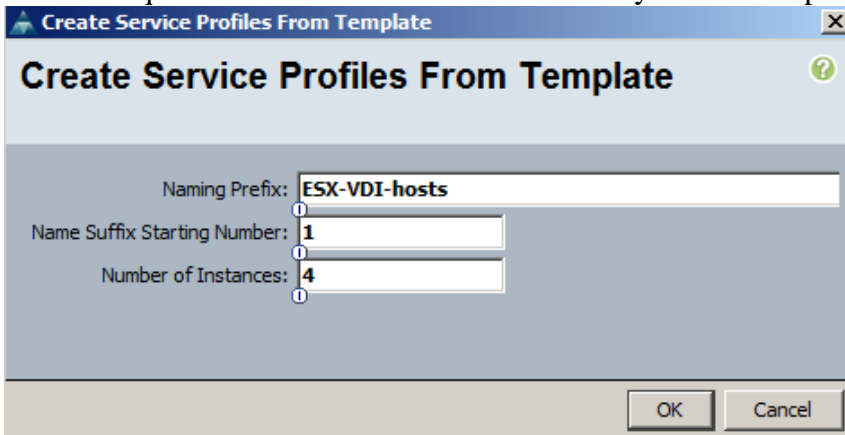
Maintenance Policy: **User_ACK**   Create Maintenance Policy

Name: **User_ACK**
Description:
Reboot Policy: **User Ack**

Step 12 At this point go ahead and select the finish button to save the SP template. There are other additional parameters that could be configured such as Adapter firmware, BIOS levels, power policy upon creation, etc.. These are not required, but might be useful to know about.

Deploying Service Profiles from a Template → [#TOP](#).

- Step 1** In the UCSM navigation menu select the Servers tab.
- Step 2** Navigate to the Service Profile templates that you want to use.
- Step 3** Right click on the entry and select “Create Service Profiles from Template”
- Step 4** You will be presented with a dialog box. Enter the name of the Service Profiles that you want to use. Then enter the starting number and the total of Service Profiles required. Select OK and this will create your Service profiles.



Create Service Profiles From Template

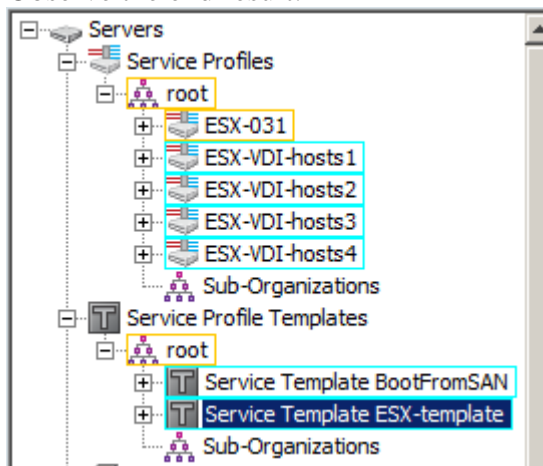
Naming Prefix: **ESX-VDI-hosts**

Name Suffix Starting Number: **1**

Number of Instances: **4**

OK Cancel

Step 5 Observe the end result:



Appendix B: Troubleshooting details

Problems with Twin-AX connectivity: → [Troubleshooting](#)

The Cisco part for a Twin-AX 3 meter cable (SFP-H10GB-CU3M) has several versions. There was a known issue with an earlier version of this cable 37-0961-01. However with 37-0961-02 and higher are supposed to be compatible with the MSA SFF-8431 spec. We know for certain that the 37-0961-02 cable works perfectly fine. Problems with the early manufactured 37-0961-03 version (Manufactured in early 2013) have also been observed. More current versions of the 37-0961-03 cable have not shown these problems.

Network connectivity issues → [Troubleshooting](#)

- 1) Start with verifying the [network topology](#) as well as the [VLAN / LAN connectivity](#)
- 2) Look for things like the native VLAN setting in the LAN Cloud section. Most likely you do not want your iSCSI network to be the Native VLAN.
- 3) Verify that the iSCSI vNIC is going to the correct Fabric Interconnect. Keep in mind that a Fabric Interconnect will be a separate broadcast domain in the case of dual subnets.

SANboot “Initialize error 1” → [Troubleshooting](#)

Unfortunately this error can mean a lot of different things. Start with these steps:

- 1) Login to the Fabric Interconnect via SSH using the UCSM login.
 - a. Determine which mac addresses are present. “show mac address-table”. This can also be filtered by VLAN. Verify if you see both the blade MAC address as well

as the MAC address from the array's data ports. Keep in mind that you may also need to do this on the upstream Nexus switch if it is in the data path.

- b. Run the following command set to determine iSCSI connectivity. Note that the iSCSI connectivity will change upon blade boot up:
 - i. connect adapter x/y/z (chassis ID / Server ID / Adapter Number)
 - ii. connect
 - iii. attach-mcp
 - iv. iscsi_get_config

Note if you see any login errors:

- 2) From the Nimble CLI tail the dsd.log file to see if you get any iSCSI session requests.
 - a. If you get a request, but it is denied, then this could be an ACL issue (such as multi-initiator bit or a typo in the initiator group).
 - b. If you do not get a request then this is a network / config issue.

“Policy reference AuthProfileName does not resolve to named policy”

→Troubleshooting

This is due to a Cisco bug indicating that a CHAP configuration is not present. This error can be ignored. Reference: <https://tools.cisco.com/bugsearch/bug/CSCui43905>

ENM source pinning error →Troubleshooting

This error can cause an interface to go offline. This is known to occur due to two different causes. The first is that there needs to be at least 1 uplink port that is active. This is still required even if you are using Appliance ports for iSCSI connectivity. The second cause is that if you are using Appliance ports you must represent a VLAN in both the Appliance ports section and the LAN Cloud section. This VLAN can have different names in each location, but MUST be the same VLAN id#. This is not two instances of the same VLAN, but rather two access ports for the same VLAN.

Wrong version of firmware / UCSM / BIOS / driver →Troubleshooting

Always reference the Cisco HCL to make sure the UCS and blade configuration is up to date: <http://www.cisco.com/c/en/us/support/servers-unified-computing/unified-computing-system/products-technical-reference-list.html>

Note: it is very common in ESX to be running the wrong version of driver on a fresh install. This can cause issues with iSCSI discovery and MPIO failover. You can confirm this by running the following command via SSH in the command prompt:

esxcli software vib list | grep enic

Note that as of this writing the current version of enic driver for ESX 5.x is 2.1.2.38.

Discovery IP address → [Troubleshooting](#)

Note that with SANboot of any type you should not be using the discovery IP address. Instead you should use one of the Data IP addresses. In SANboot you do not do a discovery at all, but rather use a static entry to define connectivity to the boot LUN.

However once the OS is online, then it is appropriate to use the iSCSI discovery IP address.

Also note that the discovery IP address can be on any subnet as long as the host has a route to it. It is only used for LUN discovery and will not tear down sessions to the target data IPs if the discovery ip address happens to become unavailable. This would of course prevent new LUNs from being dynamically discovered during this time.

Appendix C: Configuration Details

Sample Etherchannel Configuration. → [#TOP](#)

Procedure: Configure the below syntax on connection to a Fabric Interconnect.

```
Cisco4500A# show run int te1/1/2
interface TenGigabitEthernet1/1/2
description To Fabric A
switchport trunk native vlan 300
switchport trunk allowed vlan 1,300
switchport mode trunk
channel-group 4 mode active    <<<<< Note: channel-group 4 mode "on" will NOT work.
end
```

```
Cisco4500A#show run int po4
Building configuration...
```

Current configuration : 162 bytes

!

```
interface Port-channel4
description To Fabric A
switchport
switchport trunk native vlan 300
switchport trunk allowed vlan 1,300
switchport mode trunk
end
```

(End of document)