REFERENCE ARCHITECTURE

# FlashStack Direct Attached Configuration —UCSM

Deployment Guide for FlashStack configured without Nexus or MDS networking components with UCS Manager.

# Contents

**Introduction** 3

**Considerations for Running in a Direct-Attached Model** 3

Management Functionality 3

Differences in Functionality 3

**Connection Diagram** 4

**Architecture Infrastructure Components** 5

**Mounting External Storage to VMware on HyperFlex, Nutanix, or vSAN Clusters** 5

**Configuration Guide—Pure Storage FlashArray** 6

Port Configuration—Fiber Channel Interfaces 6

Port Configuration—Ethernet Interfaces & VIFs 6

**Configuration Guide—UCSM** 7

UCS Pools, VLAN/VSAN, and Policies Configuration 7

Create IP Pools 8

Create MAC Pools 9

Create IQN Pools 10

Create WWNN Pools 10

Create UUID Suffix Pools 12

Appliance Interface Configuration—Ethernet 16

Storage FC Interface Configuration—Fiber Channel 17

vNIC/vHBA Templates and LAN/SAN Connectivity Policies 17

Boot Policy—Fiber Channel 23

Boot Policy—iSCSI 24

**UCS Service Profile Templates** 25

**Deployment of VMware vSphere** 27

Boot from SAN Connectivity 27

FlashArray Host Connectivity 28

vSphere Host Connectivity 29

**Conclusion** 30

## Introduction

FlashStack® from Pure Storage® deployed in a direct-attached configuration can extend the usability of the FlashStack platform into a smaller, more economical form factor.

When FlashStack leverages this direct-attached model, it can deliver a fully functional converged infrastructure with reduced rack space and power consumption requirements in private cloud environments.

This document aims to showcase the ease of deploying a consolidated FlashStack environment with VMware vSphere running both iSCSI and Fiber Channel connected storage in a direct-attach model while leveraging UCS Manager for the configuration.

## Considerations for Running in a Direct-Attached Model

Running a FlashStack environment with a direct-attached model is a perfectly viable configuration to choose, rather than leveraging Nexus or MDS networking components for the connection between the compute to storage components.

FlashStack running in a direct-attached model with Boot from SAN may be a more suitable infrastructure design within an environment for dedicated workloads and ROBO sites, or for environments where a customer is looking to utilize minimal power, rack space, and cooling.

There are some differences in management and functionality when running a direct-attached configuration rather than traditional networking, which the customer should be aware of.

### Management Functionality

Within a UCSM (UCS Managed) environment running in a direct-attached architecture, configuration details are managed and controlled at the policy and port levels. Still, the configuration for ethernet and fiber channel ports is less flexible when connected directly to a Fabric Interconnect port than when connected to a Nexus or MDS switch.

Troubleshooting the configuration and connectivity between the UCS FIs and the Pure Storage FlashArray™ may be slightly more difficult due to a lack of some advanced troubleshooting commands or monitoring functionality. However, if proper configuration steps are followed, basic command-line interaction should provide more than enough detail to verify interface details and validate connectivity.

### Differences in Functionality

The major differences in functionality with a direct-attach configuration revolve around some functionality lost when using a Fabric Interconnect as the switching fabric.

The primary differences in functionality for the configuration of a FlashStack in a direct-attached model relate to the specific details of the port configurations that serve as the cabling between the fabric interconnects and the storage array. For the configuration of ethernet ports, whether individual ports or port channels are leveraged, it is recommended to define specific ethernet target endpoints for the storage array ports connected to the FIs. For the configuration of fiber channel ports, storage ports can only be configured as individual links, so the infrastructure cannot leverage port channels for direct connections to the storage array ports due to the lack of an MDS switch.

Customers might reach some performance limitations when the ethernet and fiber channel ports between the FIs and storage array are fully saturated. These limitations were not fully tested and documented, as performance was not a focus of this document. It is best to engage your partner when designing the environment to assist in a design that will meet the performance needs of the specific environment and workloads.

There may also be limitations in full monitoring of the environment when comparing this direct-attached model to an environment using a full ethernet or fiber channel fabric, primarily when looking at port-level specifics/counters or alerting for thresholds/bottlenecks, but this is more specific to the monitoring tool/suite used within the customer environment; it is recommended to investigation the specifics from the relevant vendor.

## Connection Diagram

Other considerations exist for using only the fabric interconnects for connectivity within your environment to ensure optimal performance, reliability, and scalability.

In this documentation, we will use the same physical hardware with the below cabling layout for both the UCSM configuration of FlashStack in a direct-attached model.

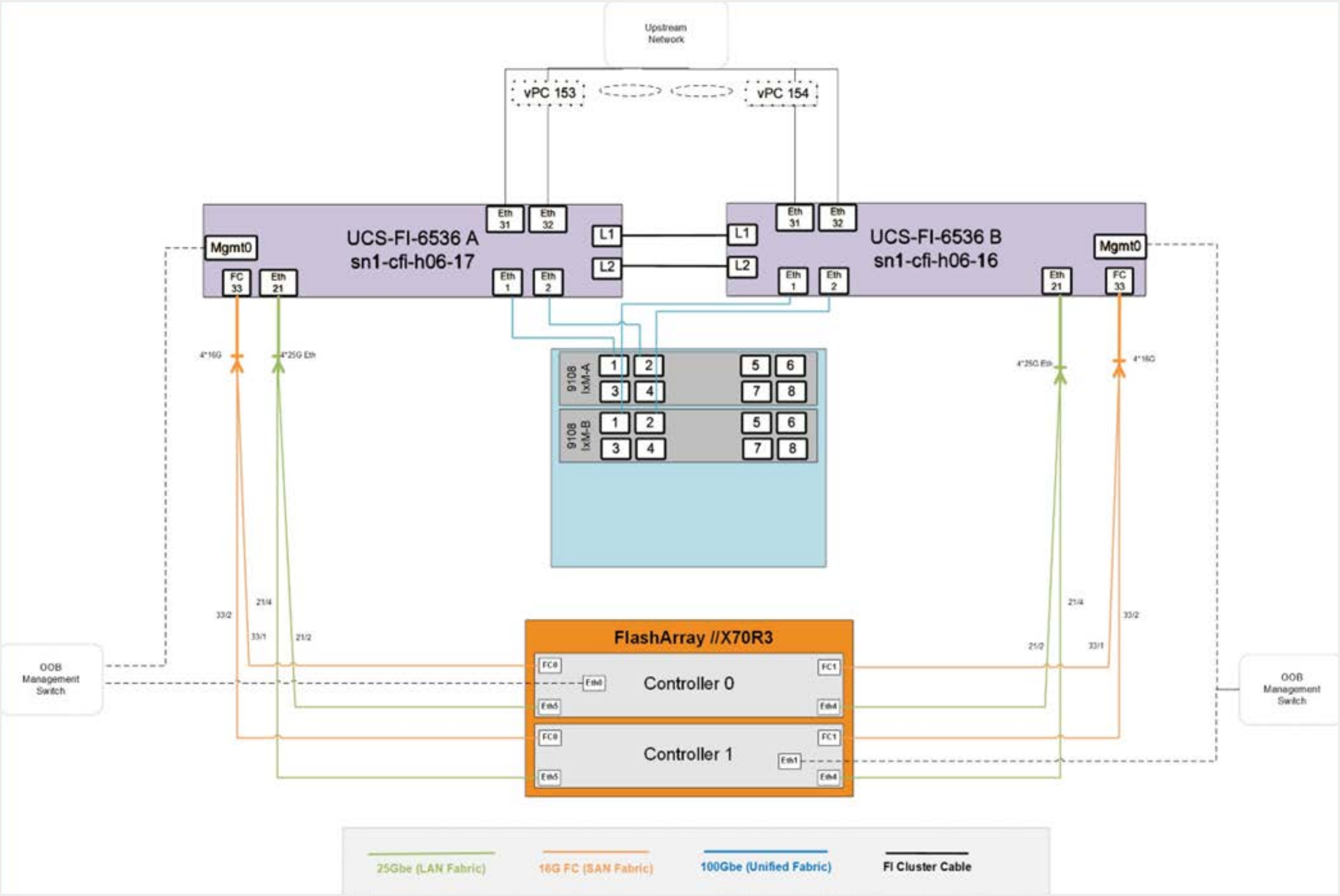


**FIGURE 1** Diagram of physical connections within the lab environment used for this document.

## Architecture Infrastructure Components

This section lists the components used to build the configuration of a direct-attached FlashStack.

| Infrastructure Component | Model/Version |
|---|---|
| Storage | FlashArray//XR3 (running Purity 6.4.5) |
| Networking | Cisco UCS 6536 |
| Compute (Chassis) | Cisco UCSX 9508 (UCSM Mode) |
| Compute (Nodes) | Cisco UCS X210c M6 Compute Node |
| Hypervisor | VMware ESXi, 7.0.3, 21424296 (7.0 U3l) |
| PowerShell Modules (UCS) | Cisco.UCS.Common 3.0.4.4<br>Cisco.UCSManager 3.0.3.3 |

**TABLE 1** All infrastructure components and models or versions used within the documented FlashStack deployment in direct-attached configuration.

In our test setup, VMware vSphere hypervisors were deployed on 6 Cisco UCS X210C M6 compute nodes, each leveraging dual 24-core, 2.4 GHz Intel Xeon Gold 6312U processors and 2TB of DDR4-3200 DIMMs. Service profiles were created using service profile templates to configure the following scenarios:

- Three servers providing vNICs configured for direct-attached iSCSI connectivity and iSCSI Boot from SAN
- Three servers providing vHBAs configured for direct-attached Fiber Channel connectivity and FC Boot from SAN

## Mounting External Storage to VMware on HyperFlex, Nutanix, or vSAN Clusters

There is a specific use case that we want to be sure to highlight outside of leveraging FlashStack in a direct-attached model, which is the capability of adding external storage to VMware hosts specifically running within Hyperflex, Nutanix, and vSAN clusters (if Nutanix or vSAN hosts are Cisco UCS managed by an FI).

The principles covered in this guide can also be used for VMware hosts running in Hyperflex and Nutanix clusters. The same configurations of LAN and SAN policies will allow for the connectivity for iSCSI and Fiber Channel storage to be directly attached to a pair of UCS Fabric Interconnects.

Customers should be aware that the same considerations for connectivity from earlier in this document apply in both scenarios, but this direct-attach functionality gives the ability to access a Pure Storage FlashArray and mount the volumes as VMFS datastores. When using VMware as the hypervisor, customers can now simply vMotion workloads from the datastores backed by HX and AOS storage systems to Pure Storage FlashArray.

Cisco HyperFlex supports the capability of connecting external storage to a cluster, but the Cisco UCS documentation (link) only covers how to configure the Fabric Interconnect switching mode, so this guide expands on how to perform the configuration for both iSCSI and Fiber Channel access, as these policy configurations would be the same for standard UCS and Hyperflex.

For a more in-depth walkthrough of adding a Pure Storage FlashArray to a vSAN cluster, covering iSCSI and vVols specifically, there is a multi-part blog from Jase McCarty which goes into much more detail about the VMware portion of adding the FlashArray storage to the cluster (part 1, part 2, part 3)

Be aware that Nutanix does not recommend connecting 3rd party storage devices, so any customer should verify with Nutanix support as to any potential support impacts or caveats for their environment, before configuring this setup.

## Configuration Guide—Pure Storage FlashArray

This section will cover the configuration of the Pure Storage FlashArray such that basic network connectivity is online, a nd so that both fiber channel and iSCSI details are configured and available before being needed for the UCS Policies later in this guide.

### Port Configuration—Fiber Channel Interfaces

Each fiber channel interface on the FlashArray should be enabled under 'Settings' > 'Network' so the ports are ready for connectivity once the appropriate configuration is set on the UCS FIs.

**NOTE:** This page is also where the WWNs for each interface are found for use in the Boot from SAN configuration for fiber channel later.

### Port Configuration—Ethernet Interfaces & VIFs

Each of our physical ethernet ports on the FlashArray should be enabled under 'Settings' > 'Network' so that the ports are ready for connectivity once the appropriate configuration is set on the UCS FIs.

For our direct connectivity from the FlashArray to the UCS FIs, we will use Subnets with VLAN Interfaces that match the VLAN IDs we have defined for our environment.

We will create a subnet with a VLAN interface for each data path (A and B) and will then attach sub-interfaces from each of our physical ethernet interfaces to connect to these subnets with VLANs.

1. To create a subnet on the FlashArray, navigate to the Network Settings page of the FlashArray (*'Settings' > 'Network'*).
2. Click the "+" icon in the 'Subnets' area of the page.
3. In the Create Subnet pop-up that appears, enter the following details:
   a. *Name*: This field is the name of the subnet used within the FlashArray; it is suggested that the data path is included (A or B)
   b. *Enabled*: This field is set by default, and it should remain enabled
   c. *Prefix*: This field is the prefix for the network subnet in CIDR notation, which defaults to /24
   d. *VLAN*: this field will tag the VLAN to be used on the sub-interface that is attached to this subnet; this ID will match the details that we have defined for our environment
   e. *Gateway*: This field is the gateway for your network subnet; this is not required in our direct attach configuration
   f. *MTU*: This field sets the MTU to be used by the sub-interfaces that inherit this setting from the subnet; the general recommendation is to use the standard MTU of 9000 for iSCSI connectivity to FlashArray
4. Click "Create" to finish the creation of a subnet for the FlashArray.
5. Repeat steps 1-4 again to create a second subnet with the appropriate details of the second data path.
6. Once the two subnets are created, interfaces can be added to them by clicking the "Add Interface" button under the 'Interfaces' column of the subnet.
7. In the Add Interface of Subnet '%Subnet Name%' pop-up that appears, click the dropdown menu for "Name" and select the appropriate physical ethernet interface which is directly connected to the UCS FIs for the data path of the subnet

   **NOTE:** The interfaces in the dropdown menu will be listed with this name format: ct#:eth#:#### with these details - (controller #):(physical interface #):(subnet VLAN ID)
8. Once the correct sub-interface has been picked from the menu, click "Save" to add the interface to the subnet.
9. Repeat steps 6-8 to add interfaces to each subnet so that a minimum of two sub-interfaces, connected to two separate physical interfaces, are configured to provide redundant connectivity from the FlashArray to the UCS FIs.

**NOTE:** The Connections page ('Health' > 'Connections') is where the IQN for the FlashArray is found for use in the Boot from SAN configuration for iSCSI later.

## Configuration Guide—UCSM

As this document is focused on running FlashStack in a direct-attach mode, there are some portions of the configuration of a UCSM environment which are covered within Cisco Validated Designs and UCS documentation, and will not be covered within this document.

The list of UCSM configuration details not covered by this document is listed below, broken out by UCSM navigation tab:

| Configuration Tab | Policies Not Covered in this Guide |
|---|---|
| Admin Tab | Fault Policies, User Management, Key Management, Communication Management |
| Equipment Tab | Firmware Management, Equipment Policies |
| Server Tab | Various policies—Adapter, BIOS, Host Firmware, IPMI/Redfish Access, KVM Management, Maintenance, Power Control, Serial over LAN, Server Pool, iSCSI Authentication, vMedia |
| LAN Tab | Various policies—Dynamic vNIC Connection, LACP, Multicast, QOS, VMQ Connection |
| Storage Tab | Storage Policy |
| Chassis Tab | Chassis Maintenance Policy |

**TABLE 2** All configuration policies not covered within the guide, listed by UCSM tab.

This document will cover the other requisite policies & templates to be configured for the deployment of FlashStack in a direct-attach mode, with the example of running ESXi hosts, as it is a common deployment for customer environments.

## UCS Pools, VLAN/VSAN, and Policies Configuration

Before we can create our templates used for vNICs, VHBAs, and Service Profiles, we need to create our pools, VLANs, VSANs, and policies used by these template objects. We will create these objects in groups such that similar configuration steps follow each other, in an order for each stage to build upon previous steps.

### Identifier Pools

We will first create our pools of identifiers to be consumed by our policies and vNIC/vHBA templates.

For the configuration of Pools within the LAN tab, this is how the filtered view of all pools under the LAN tab will appear:

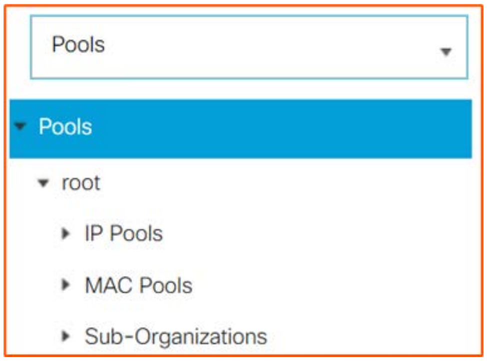
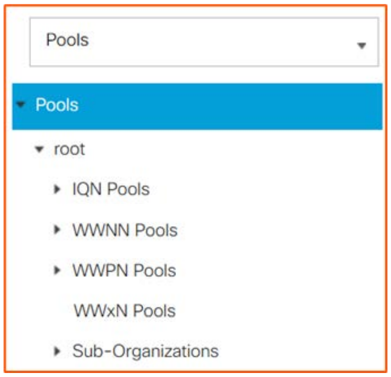


**FIGURE 2** Filtering the view to Pools within the LAN tab

For the configuration of Pools within the LAN tab, this is how the filtered view of all pools under the LAN tab will appear:



Pools

- Pools
  - root
    - IQN Pools
    - WWNN Pools
    - WWPN Pools
    - WWxN Pools
    - Sub-Organizations

**FIGURE 3** Filtering the view to Pools within SAN tab

## Create IP Pools

These same steps will be followed to create all IP Pools that are necessary for the environment, which may include Outband KVM Access (Out of band using UCS FI management network), Inband KVM Access, and iSCSI Initiators. If you are configuring iSCSI for the environment, it is recommended to configure one IP Pool for each data path (A and B).

**NOTE:** Best practices dictate the creation of distinct IP address pools for adapters on each distinct data path (A & B) with an IP range that is distinct and easily identifiable for any required troubleshooting if iSCSI is being configured for your environment.

1. In the Cisco UCS Manager, click on the **LAN** tab in the left navigation pane.
2. Select the **Pools** filter at the top of the navigation pane to only view Pools. Expand the navigation to the UCS Org you are creating the pool under (typically 'root' upon initial deployment).
3. Once you have expanded the Org that will contain your IP Pool, you can either right-click the **IP Pools** subtab and click Create IP Pool, or you can expand the **IP Pools** tab and press the "Add" button in the main navigation area.
4. In the **Create IP Pool** pop-up that appears, enter the Name of the pool (required), Description of the pool (optional), and the Assignment Order (required). Click "Next".
5. In the **Add IPv4 Blocks** subtab, click the "Add" button in the main navigation area. In the **Create Block of IPv4 Addresses** pop-up that appears, enter the following details:
   a. *From*: This field is your starting IPv4 address
   b. *Size*: This field is the size of your IP blocks—the quantity of IP addresses contained in the pool
   c. *Subnet Mask*: This field is the subnet mask for your network subnet
   d. *Default Gateway*: This field is the default gateway for your network subnet
   e. *Primary DNS/Secondary DNS*: These fields are for your primary and secondary DNS IP addresses (optional)
6. Once all details are entered in the **Create Block of IPv4 Addresses** pop-up, click "OK" to add your IPv4 IP block. Click "Next" to accept your IPv4 blocks.
7. If you require IPv6 blocks, follow the same direction as step 5 above to create an IPv6 block.
8. Click "Finish" in the **Create IP Pool** pop-up to complete your **IP Pool** creation.

**NOTE:** If inband management is required for your environment, you should follow the configuration steps within the Cisco UCS Manager Administration Management Guide.

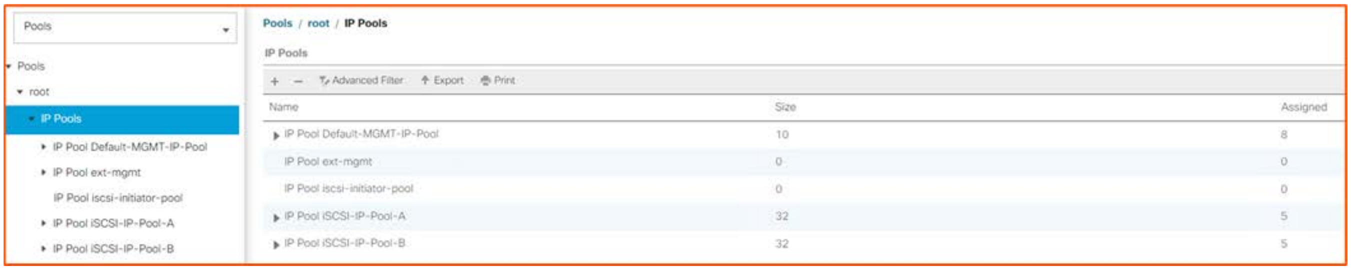
## Create MAC Pools

These same steps will be followed to create all MAC Pools that are necessary for each vNIC adapter that will be used within the environment.

**NOTE:** Best practices dictate the creation of distinct MAC address pools for adapters on each distinct data path (A & B) with a range that is distinct and easily identifiable for any required troubleshooting.

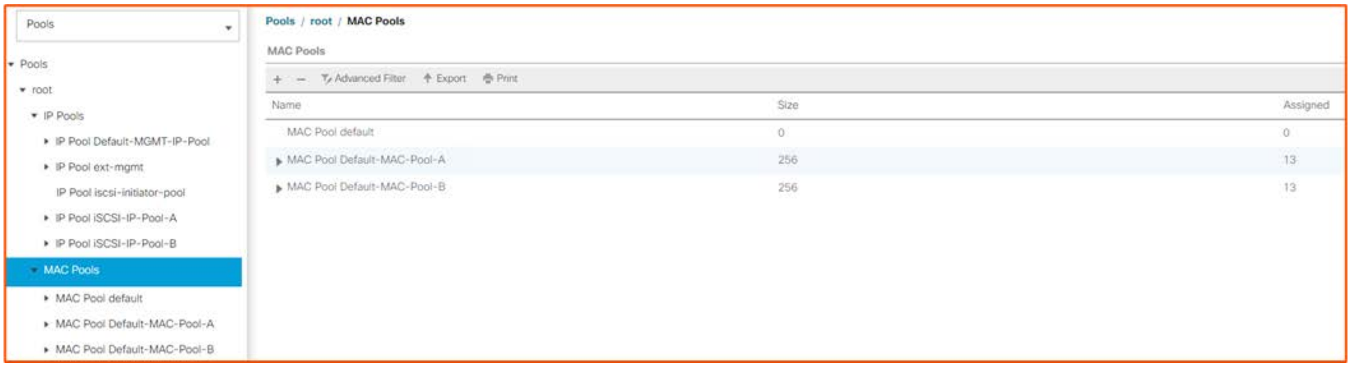
1. In the Cisco UCS Manager, click on the **LAN** tab in the left navigation pane.
2. Select the **Pools** filter at the top of the navigation pane to only view Pools. Expand the navigation to the UCS Org that you are creating the pool under (typically 'root' upon initial deployment).
3. Once you have expanded the Org that will contain your MAC Pool, you can either right-click the **MAC Pools** subtab and click **Create MAC Pool**, or you can expand the MAC Pools tab and press the "Add" button in the main navigation area.
4. In the **Create MAC Pool** pop-up that appears, enter the Name of the pool (required), Description of the pool (optional), and the Assignment Order (required). Click "Next".
5. In the **Add MAC Addresses** subtab, click the "Add" button in the main navigation area. In the **Create Block of MAC Addresses** pop-up that appears, enter the following details:
   a. *First MAC Address*: This field is your starting MAC address
   b. *Size*: This field is the size of your MAC Address pool—the quantity of MAC addresses contained in the pool
6. Best practices require the use of the following MAC prefix: 00:25:B5:xx:xx:xx
7. Once all details are entered in the **Create Block of MAC Addresses** pop-up, click "OK" to add your MAC Address block.
8. Click "Finish" in the **Create MAC Pool** pop-up to complete your MAC Pool creation.

Once the IP and MAC Pools have been created, the pools under the LAN tab should look similar to these pools:



| Name | Size | Assigned |
|---|---|---|
| IP Pool Default-MGMT-IP-Pool | 10 | 8 |
| IP Pool ext-mgmt | 0 | 0 |
| IP Pool iscsi-initiator-pool | 0 | 0 |
| IP Pool iSCSI-IP-Pool-A | 32 | 5 |
| IP Pool iSCSI-IP-Pool-B | 32 | 5 |

**FIGURE 4** IP Pools within LAN tab


Pools
Pools
root
IP Pools
IP Pool Default-MGMT-IP-Pool
IP Pool ext-mgmt
IP Pool iscsi-initiator-pool
IP Pool iSCSI-IP-Pool-A
IP Pool iSCSI-IP-Pool-B
MAC Pools
MAC Pool default
MAC Pool Default-MAC-Pool-A
MAC Pool Default-MAC-Pool-B
Pools / root / MAC Pools
MAC Pools
+ − Advanced Filter Export Print

| Name | Size | Assigned |
|---|---|---|
| MAC Pool default | 0 | 0 |
| MAC Pool Default-MAC-Pool-A | 256 | 13 |
| MAC Pool Default-MAC-Pool-B | 256 | 13 |

**FIGURE 5** MAC Pools within LAN tab

## Create IQN Pools

If iSCSI is being utilized within the environment, these same steps will be followed to create all IQN Pools which are necessary for each server profile connected to iSCSI within the environment.

1. In the Cisco UCS Manager, click on the **SAN** tab in the left navigation pane.
2. Select the **Pools** filter at the top of the navigation pane to only view Pools. Expand the navigation to the UCS Org that you are creating the pool under (typically 'root' upon initial deployment).
3. Once you have expanded the Org that will contain your IQN Pool, you can either right-click the IQN Pools subtab and click **Create IQN Suffix Pool**, or you can expand the IQN Pools tab and press the "Add" button in the main navigation area.
4. In the **Create IQN Pool** pop-up that appears, enter the Name of the pool (required), Description of the pool (optional), Prefix of the pool (required), and the Assignment Order (required). Click "Next".

   **NOTE:** IQN prefixes must match the following pattern: iqn.yyyy-mm.naming-authority

5. In the **Add IQN Blocks** subtab, click the "Add" button in the main navigation area. In the Create a Block of IQN Suffixes pop-up that appears, enter the following details:

   a. *Suffix*: This field is attached to the IQN prefix for the pool

   b. *From*: This field is the starting IQN

   c. *Size*: This field is the size of the IQN block—the quantity of IQNs contained in the pool

6. Once all details are entered in the Create WWN Block pop-up, click "OK" to add your WWN block.
7. Click "Finish" in the Create WWNN Pool pop-up to complete your WWNN Pool creation.

## Create WWNN Pools

These same steps will be followed to create all WWNN Pools which are necessary for each server profile with an vHBA adapter that will be used within the environment.

1. In the Cisco UCS Manager, click on the **SAN** tab in the left navigation pane.
2. Select the **Pools** filter at the top of the navigation pane to only view Pools. Expand the navigation to the UCS Org that you are creating the pool under (typically 'root' upon initial deployment).
3. Once you have expanded the Org that will contain your WWNN Pool, you can either right-click the **WWNN Pools** subtab and click **Create WWNN Pool**, or you can expand the **WWNN Pools** tab and press the "Add" button in the main navigation area.
4. In the **Create WWNN Pool** pop-up that appears, enter the Name of the pool (required), Description of the pool (optional), and the Assignment Order (required). Click "Next".
5. In the **Add WWNN Blocks** subtab, click the "Add" button in the main navigation area. In the **Create WWN Block** pop-up that appears, enter the following details:

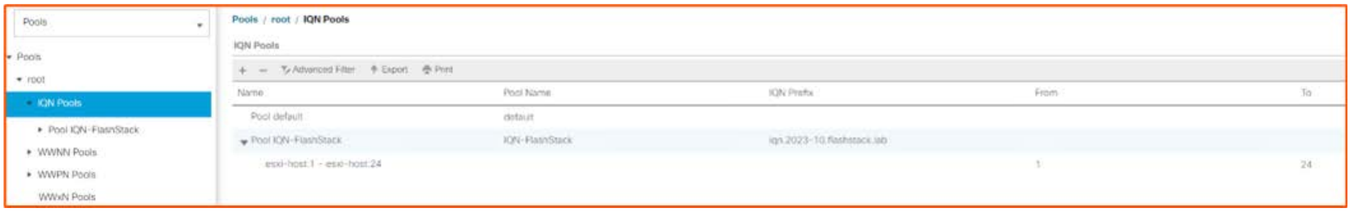
   a. *From*: This field is the starting WWN

   b. *Size*: This field is the size of the WWN block—the number of WWNs contained in the pool

   **NOTE:** Best practices require the use of the following WWN prefix: 20:00:00:25:B5:xx:xx:xx

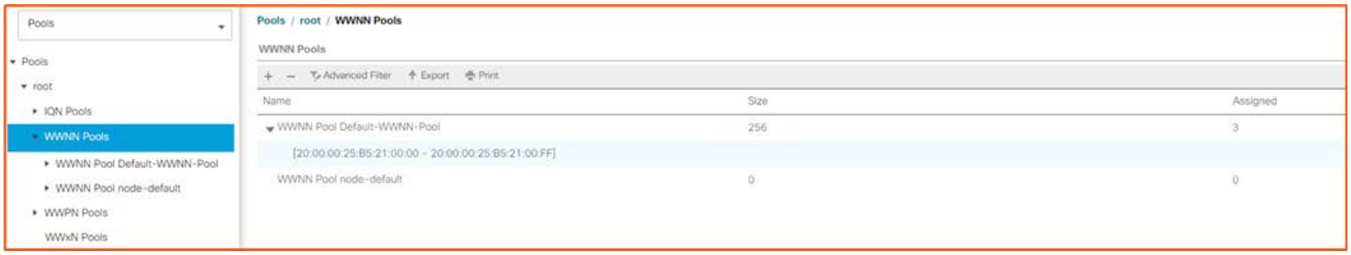
6. Once all details are entered in the **Create WWN Block** pop-up, click "OK" to add your WWN block.
7. Click "Finish" in the **Create WWNN Pool** pop-up to complete your WWNN Pool creation.

Once the IQN, WWNN, and WWPN Pools have been created, the pools under the SAN tab should look similar to these pools:



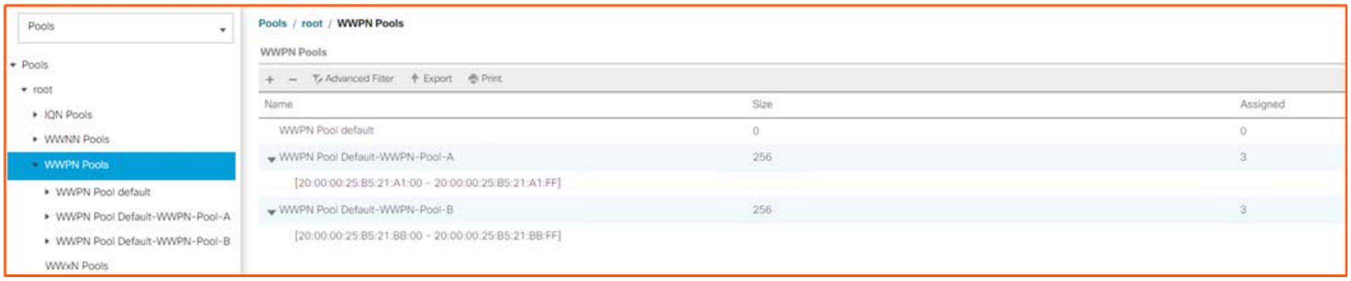
| Name | Pool Name | IQN Prefix | From | To |
|---|---|---|---|---|
| Pool default | default | | | |
| Pool IQN-FlashStack | IQN-FlashStack | iqn.2023-10.flashstack.lab | | |
| esxi-host:1 - esxi-host:24 | | | 1 | 24 |

**FIGURE 6** IQN Pools within the SAN tab



| Name | Size | Assigned |
|---|---|---|
| WWNN Pool Default-WWNN-Pool | 256 | 3 |
| [20:00:00:25:B5:21:00:00 - 20:00:00:25:B5:21:00:FF] | | |
| WWNN Pool node-default | 0 | 0 |

**FIGURE 7** WWNN Pools within the SAN tab


Pools
Pools
root
IQN Pools
WWNN Pools
WWPN Pools
WWPN Pool default
WWPN Pool Default-WWPN-Pool-A
WWPN Pool Default-WWPN-Pool-B
WWxN Pools
Pools / root / WWPN Pools
WWPN Pools
+ − Advanced Filter Export Print

| Name | Size | Assigned |
|---|---|---|
| WWPN Pool default | 0 | 0 |
| WWPN Pool Default-WWPN-Pool-A | 256 | 3 |
| [20:00:00:25:B5:21:A1:00 - 20:00:00:25:B5:21:A1:FF] | | |
| WWPN Pool Default-WWPN-Pool-B | 256 | 3 |
| [20:00:00:25:B5:21:BB:00 - 20:00:00:25:B5:21:BB:FF] | | |

**FIGURE 8** WWPN Pools within the SAN tab

## Create UUID Suffix Pools

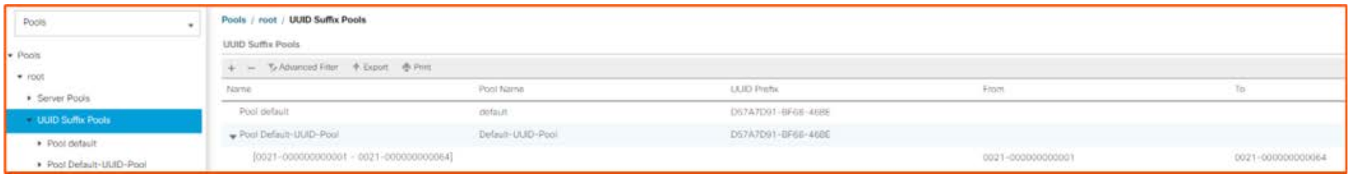
These same steps will be followed to create all UUID Suffix Pools which are necessary for each server profile that will be used within the environment.

1. In the Cisco UCS Manager, click on the **Servers** tab in the left navigation pane.
2. Select the **Pools** filter at the top of the navigation pane to only view Pools. Expand the navigation to the UCS Org that you are creating the pool under (typically 'root' upon initial deployment).
3. Once you have expanded the Org that will contain your UUID Suffix Pool, you can either right-click the **UUID Suffix Pools** subtab and click **Create UUID Suffix Pool**, or you can expand the **UUID Suffix Pools** tab and press the "Add" button in the main navigation area.
4. In the **Create UUID Suffix Pool** pop-up that appears, enter the Name of the pool (required), Description of the pool (optional), Prefix (required), and Assignment Order (required). Click "Next".
5. In the **Add UUID Blocks** subtab, click the "Add" button in the main navigation area. In the **Create a Block of UUID Suffixes** pop-up that appears, enter the following details:

   a. *From*: This field is the starting UUID suffix

   b. *Size*: This field is the size of the UUID block—the quantity of UUIDs contained in the pool
6. Once all details are entered in the **Create a Block of UUID Suffixes** pop-up, click "OK" to add your UUID block.
7. Click "Finish" in the **Create UUID Suffix Pool** pop-up to complete your UUID Pool creation.

Once the UUID Pool has been created, the pools under the Server tab should look similar to this pool:



| Name | Pool Name | UUID Prefix | From | To |
|---|---|---|---|---|
| Pool default | default | D57A7D91-BF66-468E | | |
| Pool Default-UUID-Pool | Default-UUID-Pool | D57A7D91-BF66-468E | | |
| [0021-000000000001 - 0021-000000000064] | | | 0021-000000000001 | 0021-000000000064 |

**FIGURE 9** UUID Pool within the Server tab

### VLAN Creation

These same steps will be followed to create all VLANs that are necessary for the environment, which includes all VLANs required to pass upstream network traffic. If iSCSI is being configured for your environment, two additional non-routable VLANs with unique VLAN IDs should be created to carry iSCSI traffic for each data path (A&B).

For the configuration of VLANs within the LAN tab, this is how the filtered view of the LAN Cloud under the LAN tab will appear:

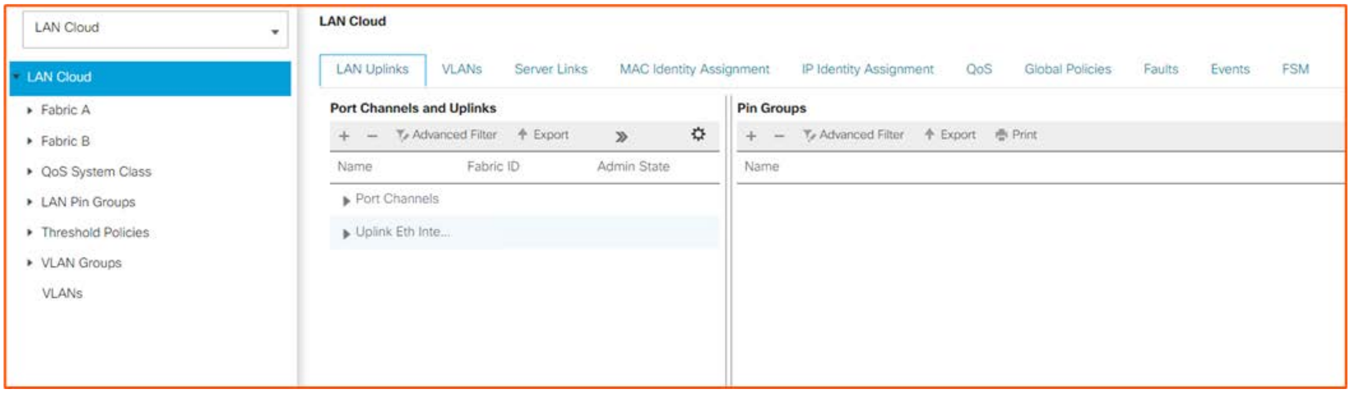


**FIGURE 10** Filtering the view to LAN Cloud within the LAN tab

**NOTE:** Best practices dictate that network VLANS should be matching for all vNIC templates connecting to hosts within your environment. There is an exception for creating dedicated NICs for iSCSI to be provided with a distinct data path (A & B) if iSCSI is being configured for direct-attached connectivity within your environment.

1. In the Cisco UCS Manager, click on the **LAN** tab in the left navigation pane.
2. Select the **LAN Cloud** filter at the top of the navigation pane to view only the LAN Cloud for the entire environment
3. Once you can see the **VLANs** subtab, you can either right-click the subtab and click **Create VLANs**, or you can expand the **VLANs** tab and press the "Add" button in the main navigation area.
4. In the **Create VLANs** pop-up that appears, enter the Name/Prefix of the VLAN (required), Multicast policy of the VLAN (optional), Fabric ID for the VLAN (required), the VLAN ID (required), and the Sharing Type (required). Click "Check Overlap".

   **NOTE:** The Fabric ID for each VLAN should be 'Common/Global', and sharing should remain as 'None' during VLAN creation. Once the VLAN is created, if you look at the info for each VLAN, the Fabric ID will then be listed as 'Dual'.

5. In the **Check Overlap** popup, confirm that no overlapping VLANs appear in the main display area and click "OK".
6. Once you have confirmed your VLAN does not overlap with an existing VLAN, click "OK" to add the VLAN.

**NOTE:** If iSCSI is being configured for your environment, ensure that you create two additional VLANs with unique names and IDs, one for each data path to be used for the appliance ports and iSCSI vNIC templates.

### VSAN Creation

If you are using fiber channel connectivity within your environment, these same steps will be followed to create the VSANs that are necessary for the environment. Each VSAN should be configured with unique VSAN IDs to carry FC traffic for each data path (A&B).

For the configuration of VSANs within the SAN tab, this is how the filtered view of the SAN Cloud under the SAN tab will appear:

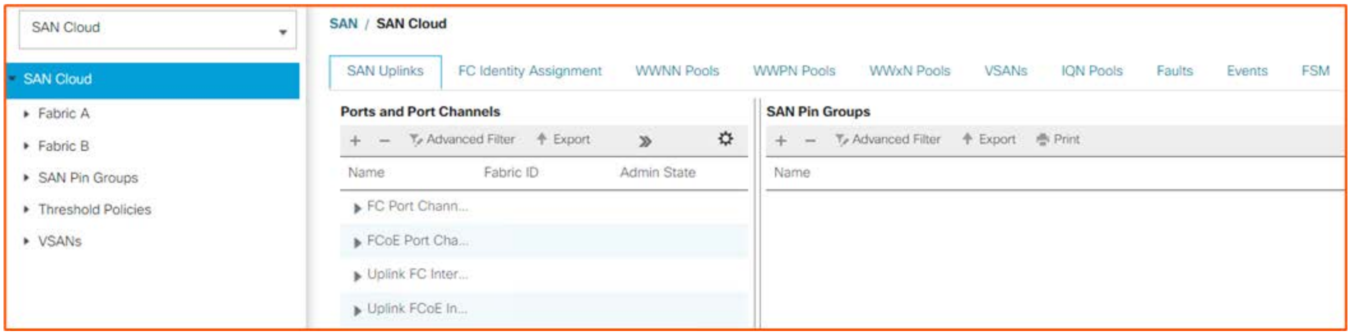


**FIGURE 11** Filtering the view to SAN Cloud within the SAN tab

1. In the Cisco UCS Manager, click on the **SAN** tab in the left navigation pane.
2. Select the **SAN Cloud** filter at the top of the navigation pane to only view the SAN Cloud for the entire environment.
3. Once you can see the **VSANs** subtab, you can either right-click the subtab and click **Create VSANs**, or you can expand the **VSANs** tab and press the "Add" button in the main navigation area.
4. In the **Create Storage VSANs** pop-up that appears, enter the Name of the VSAN (required), FC Zoning of the VSAN (required), Fabric ID for the VLAN (required), the VSAN ID (required), and the FCoE VLAN ID (required). Click "OK" to add the VSAN.

**NOTE:** Ensure that you are not connected to an upstream FC/FCOE switch where you are enabling FC Zoning. Also ensure that you create two VSANs with unique names and IDs, one for each data path to be used for the appliance ports and vHBA templates.

### Network Control Policy

One of the final policies that should be configured for our network connectivity is the Network Control Policy, which allows both Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) to be enabled on vNICs for the environment.

1. In the Cisco UCS Manager, click on the **LAN** tab in the left navigation pane.
2. Select the **Policies** filter at the top of the navigation pane to only view Pools. Expand the navigation to the UCS Org that you are creating the pool under (typically 'root' upon initial deployment).
3. Once you have expanded the Org that will contain your Network Control Policy, you can either right-click the **Network Control Policies** subtab and click **Create Network Control Policy**, or you can expand the **Network Control Policies** tab and press the "Add" button in the main navigation area.

4. In the **Create Network Control Policy** pop-up that appears, enter the following details:
    a. *Name*: This field is the name of the Network Control Policy
    b. *Description*: This field is the name of the Network Control Policy
    c. *CDP*: This will enable/disable CDP—set this to 'Enabled'
    d. *MAC Register Mode*: This will control which VLAN the MAC address will register on—set this to 'Only Native VLAN'
    e. *Action on Uplink Fail*: This controls how the VIF will handle the loss of an uplink port in end-host mode—set this to 'Link Down'
    f. *MAC Security*: This controls if forged MAC addresses are allowed/denied when sent from server to FI; default Is 'allowed', set as appropriate for your environment.
    g. *LLDP Area*: This options will set if LLDP packets are enabled/disabled on an interface; set at 'Enabled' for transmit & receive.
5. Once all details are entered in the **Create Network Control Policy** pop-up, click "OK" to create your Network Control Policy.

### UCS Storage Ports Configuration

Before we can create our configuration components within the UCS environment, we must enable the physical interfaces within the UCSM environment to provide connectivity for our data paths between the FlashArray and the UCS FIs. The following steps will be followed to configure the server, network uplink, and storage appliance ports.

For the configuration of Fabric Interconnects within the Equipment tab, this is how the filtered view of the FIs under the Equipment tab will appear:

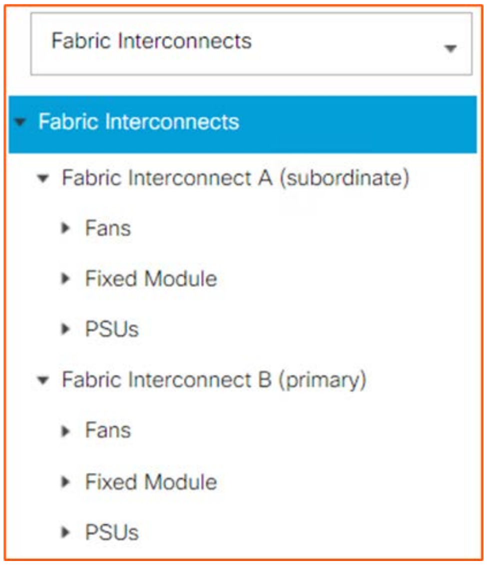


**FIGURE 12** Filtering the view to Fabric Interconnects within the Equipment tab

## Appliance Interface Configuration—Ethernet

These same steps will be followed to create an Appliance Interface that will allow for direct-attach connectivity between the FlashArray and the UCS FIs.

1. In the Cisco UCS Manager, click on the Equipment tab in the left navigation pane.
2. Select the **Fabric Interconnects** filter at the top of the navigation pane to view only the Fabric Interconnects configuration for the environment.
3. Once you have can see the Fabric A and Fabric B items, expand either one of these items to see the 'Fixed Module' item, then expand that to see the 'Ethernet Ports' item.
4. With the **Ethernet Ports** item selected, find the appropriate port number for your environment. Right-clicked on item for the port number and click "Configure as Appliance Port".
5. In the **Configure as Appliance Port** notification that appears, confirm that the correct port number is displayed in the notification, and click "Yes" to configure it as an appliance port.
6. In the **Configure as Appliance Port** pop-up that appears, enter the following details:
    a. *Priority*: This field is the QoS priority assigned to the interface; select 'Platinum'

    b. *Pin Group*: Leave this field as '<not set>'

    c. *Network Control Policy*: Select the Network Control Policy that was created earlier to allow CDP/LLDP

    d. *Flow Control Policy*: This field can remain as 'default'

    e. *Admin Speed(gbps)*: This field should be set to the appropriate speed for your physical interfaces & transceivers

    f. *VLANs*: Set the port mode to 'Trunk', and select the VLANs for both the "dummy" trunk native VLAN and the iSCSI VLAN defined in the configuration details for the environment

    **NOTE:** Ensure that you are selecting the correct VLANs for the physical uplink for the A or B data path. Each appliance port should have only the trunk and appropriate iSCSI VLAN to be used for one specific data path.

    g. *Native VLAN*: Set this to the "dummy" trunk native VLAN defined in the configuration details for the environment

    h. *Ethernet Target Endpoint*: Enter the name and MAC address for the physical interface of FlashArray to which this port of the UCS FI is directly attached
7. Repeat steps 4-6 for all physical interfaces on Fabric Interconnect A which need to be configured as Appliance Ports, then repeat the steps for all interfaces on Fabric Interconnect B which need to be configured as Appliance Ports.
8. Click "OK" to close the **NAS Appliance Manager** pop-up and save the configuration of the Appliance Ports.

## Storage FC Interface Configuration—Fiber Channel

These same steps will be followed to create an Appliance Interface that will allow for direct-attach connectivity between the FlashArray and the UCS FIs.

1. In the Cisco UCS Manager, click on the **Equipment** tab in the left navigation pane.
2. Select the **Fabric Interconnects** filter at the top of the navigation pane to view only the Fabric Interconnects configuration for the environment.
3. Once you can see the Fabric A and Fabric B items, expand either one of these items to see the 'Fixed Module' item, then expand that to see the 'FC Ports' item.
4. With the **FC Ports** item selected, find the appropriate port number for your environment. Right-click on the item for the port number and click "Configure as FC Storage Port".
5. In the **Configure as FC Storage Port** notification that appears, confirm that the correct port number is displayed in the notification, and click "Yes" to configure it as an appliance port.
6. Repeat steps 3-5 to set all physical interfaces on Fabric Interconnect A, which need to be configured as FC Storage Ports, then repeat the steps for all interfaces on Fabric Interconnect B, which need to be configured as FC Storage Ports.
7. Navigate to the first port configured as an **FC Storage Port**. In the main window, look for the 'VSAN' drop-down, and select the appropriate VSAN created for the data path of the particular fabric interconnect
8. Repeat step 7 for all ports configured as **FC Storage Ports** to set the correct VSAN ID for the port.

## vNIC/vHBA Templates and LAN/SAN Connectivity Policies

Next, we will configure vNIC and vSAN templates which will provide the relevant ethernet and finer channel networking details for the vNICs and vHBAs that are used in our LAN and SAN connectivity policies for the service profile templates.

### vNIC Template

These same steps will be followed to create each vNIC template necessary for the environment, which includes host Ethernet vNICs and iSCSI vNICs.

**NOTE:** Best practices using separate iSCSI vNICs, with one on each distinct data path (A & B) with an VLAN ID that is distinct per data path.

1. In the Cisco UCS Manager, click on the **LAN** tab in the left navigation pane.
2. Select the **Policies** filter at the top of the navigation pane to only view Policies. Expand the navigation to the UCS Org that you are creating the pool under (typically 'root' upon initial deployment).
3. Once you have expanded the Org that will contain your vNIC template, you can either right-click the vNIC Templates subtab and click **Create vNIC Template**, or you can expand the vNIC Templates tab and press the "Add" button in the main navigation area.
4. In the **Create vNIC Template** pop-up that appears, enter the following details:

   a. *Name*: This is the name for the vNIC template; it is recommended to include the usage such as 'ETH' or 'iSCSI', along with the data path that the vNIC provides.

   b. *Description*: This field is the description for the vNIC template; it is recommended to be verbose about any details that someone should be aware of when using the vNIC template, including VLAN IDs or VLAN Groups used.

   c. *Fabric ID*: This selection is to set the fabric data path for the vNIC (A or B) and determine if failover is allowed. Failover is not recommended for this use case.

   d. *Redundancy Type*: This field controls whether or not two vNIC templates will share configurations; it is recommended that either the A path or B path vNIC templates are chosen to be set as 'Primary Template' for redundancy type, with the opposing data path to be chosen as the 'Secondary Template' for redundancy type.

   e. *Target*: These checkboxes control which vNIC type this template is allowed to create; choose 'Adapter' for template type

   f. *Template Type*: This selection is to set the option for updates to the template to apply to created vNICs; select 'Updating Template' for all vNIC templates

   g. *VLANs*: Click the 'Select' box for each VLAN that should be added to your vNIC template, and click the radio button for the "Native VLAN" for any vNICs with multiple VLANs available for access.

   **NOTE:** For traditional vNIC templates, all VLANs should match the A & B data paths, which is one of the major reasons for using the primary/secondary redundancy type. For iSCSI vNICs, these templates should include only the iSCSI VLAN for each distinct data path with these VLANs set as the Native VLAN (e.g. iSCSI vNIC Template 'iSCSI-vNIC-A' should have only VLAN 'iSCSI-VLAN-A', which is also set as Native VLAN)

   h. *CDN Source*: This selection is for Consistent Device Naming; select 'vNIC Name'

   i. *MTU*: This selection is for the MTU size of the network connection; select appropriate value for the environment

   **NOTE:** The general recommendation is to use the standard MTU of 9000 for iSCSI connectivity to FlashArray.

   j. *MAC Pool*: Select the MAC Pool that was created earlier for the data path (A or B)

   k. *Network Control Policy*: Select the Network Control Policy that was created earlier to allow CDP/LLDP

5. Once all details are entered in the **Create vNIC Template** pop-up, click "OK" to create a vNIC template.

   **NOTE:** Once all vNIC templates are created, there should be at minimum two vNIC templates—one for each data path (A and B)—for standard Ethernet connectivity to hosts, with one set at 'Primary Template' and the peer set at 'Secondary Template' for the redundancy type. If iSCSI is also being used in this environment, then there should be a second pair of vNIC templates dedicated to iSCSI connectivity.

### vHBA Template

If fiber channel connectivity is to be used within the environment, these same steps will be followed to create each vHBA template, which is necessary for the environment.

**NOTE:** Best practices using paired vHBA templates, with one on each distinct data path (A & B) with both VSAN and FCoE VLAN ID that are distinct per data path.

1. In the Cisco UCS Manager, click on the **SAN** tab in the left navigation pane.
2. Select the **Policies** filter at the top of the navigation pane to only view Policies. Expand the navigation to the UCS Org that you are creating the pool under (typically 'root' upon initial deployment).
3. Once you have expanded the Org that will contain your vHBA template, you can either right-click the vHBA Templates subtab and click **Create vHBA Template**, or you can expand the vHBA Templates tab and press the "Add" button in the main navigation area.
4. In the **Create vHBA Template** pop-up that appears, enter the following details:

    a. *Name*: This is the name for the vHBA template; it is recommended to include the data path that the vHBA provides.

    b. *Description*: This field is the description for the vHBA template; it is recommended to be verbose about any details that someone should be aware of when using the vHBA template, including VSAN IDs used.

    c. *Fabric ID*: This selection is to set the fabric data path for the vHBA (A or B).

    d. *Redundancy Type*: This field controls whether or not two vHBA templates will share configurations; it is recommended that either the A path or B path vHBA templates are chosen to be set as 'Primary Template' for redundancy type, with the opposing data path to be chosen as the 'Secondary Template' for redundancy type.

    e. *VSAN*: This option is to set the VSAN used for data traffic for the vHBA

    f. *Template Type*: This selection is to set the option for updates to the template to apply to created vHBA; select 'Updating Template' for all vHBA templates

    g. *WWPN Pool*: Select the WWPN Pool that was created earlier for the data path (A or B)

5. Once all details are entered in the Create vHBA Template pop-up, click "OK" to create a vHBA template.

**NOTE:** There should be at least one vHBA template for each data path (A/B) for fiber channel connectivity for hosts, with one set at 'Primary Template' and the peer set at 'Secondary Template' for the redundancy type.

### LAN Connectivity Policy—Base vNICs for iSCSI or Fiber Channel Connectivity

These steps will cover creation of a LAN Connectivity Policy that can be used to provide ethernet connectivity (via vNICs) for service profiles using either iSCSI or fiber channel for data connectivity. If iSCSI is required, follow these steps in addition to the next configuration section.

**NOTE:** If you will have service profiles that require iSCSI connectivity, and others that do not require iSCSI connectivity, it is recommended to create two LAN Connectivity Policies for each connectivity use case.

1. In the Cisco UCS Manager, click on the **LAN** tab in the left navigation pane.
2. Select the **Policies** filter at the top of the navigation pane to only view Policies. Expand the navigation to the UCS Org that you are creating the pool under (typically 'root' upon initial deployment).
3. Once you have expanded the Org that will contain your **LAN Connectivity Policy**, you can either right-click the LAN Connectivity Policies subtab and click **Create LAN Connectivity Policy**, or you can expand the LAN Connectivity Policies tab and press the "Add" button in the main navigation area.
4. In the **Create LAN Connectivity Policy** pop-up that appears, enter the Name of the policy (required) and description of the policy (optional), then click "Add" in the main area to add a vNIC.

   **NOTE:** It is recommended to name the LAN Connectivity Policy to clearly identify if iSCSI connectivity is provided or not.

5. In the Create vNIC pop-up that appears, enter the following details:

   a. *Name*: This is the name for the vNIC being created; it is recommended to include your use such as 'ETH' or 'iSCSI', along with the data path that the vNIC provides.

   b. *Use vNIC Template*: Check this box to hide the options for manually creating a vNIC; select the vNIC template for your first data path.

   c. *Redundancy Pair*: Check this box to also set the peer vNIC to be created using the secondary template.

   d. *vNIC Template*: This selection is to set the vNIC template that is being created and named in this pop-up; select the appropriate vNIC template from the drop-down menu.

   e. *Peer Name*: This is the name for the peer vNIC being created; it is recommended to include your use such as 'ETH' or 'TRUNK', along with the data path that the vNIC provides.

   f. *Adapter Policy*: This selection is to set the performance profile for the vNICs that are being created in your LAN connectivity policy; select the appropriate built-in adapter policy.

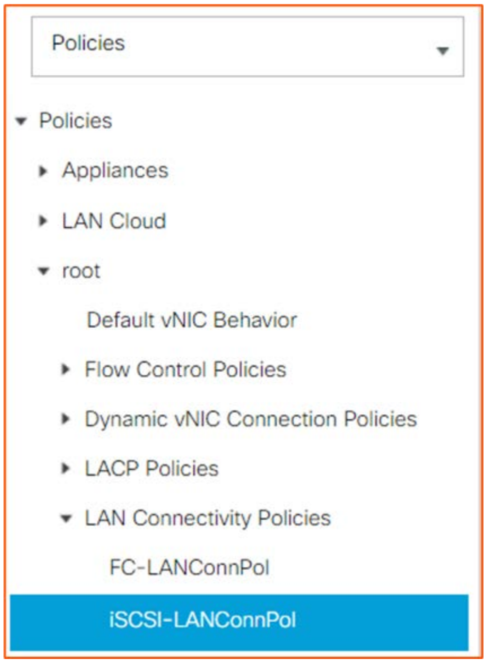
   **NOTE:** For an ESXi deployment that is being covered in this guide, it is recommended to provision 2 sets of peer vNICs (2 for A path, and 2 for B path) so that if any interruption of a single data path does not alert for loss of network redundancy. If the configuration was done with failover enabled for each vNIC template, then creating 4 vNICs is not necessary.

6. Once all details are entered in the Create vNIC Template pop-up, click "OK" to add the vNICs to your LAN Connectivity Policy.
7. Once you have created all the necessary vNICs in Create LAN Connectivity Policy pop-up, click "OK" to create the policy.

### LAN Connectivity Policy—iSCSI vNICs Only for iSCSI or Connectivity

If you are using iSCSI within the environment, follow these steps to add the two additional iSCSI vNICs used for iSCSI data traffic.

For the updating of the previously created LAN Connectivity Policy, this is how the filtered view of the LAN Connectivity Policies under the LAN tab will appear:



Policies

- Policies
  - Appliances
  - LAN Cloud
  - root
    - Default vNIC Behavior
    - Flow Control Policies
    - Dynamic vNIC Connection Policies
    - LACP Policies
    - LAN Connectivity Policies
      - FC-LANConnPol
      - iSCSI-LANConnPol

**FIGURE 13** Expanding the view to previously created LAN Connectivity Policy within LAN tab

1. In the Cisco UCS Manager, open the **LAN Connectivity Policies** subtab and locate the LAN Connectivity Policy was created previously for your iSCSI connectivity.
2. Click on the name of the iSCSI LAN Connectivity Policy in either the left navigation tab, or within the main tab, to edit this existing policy.
3. In the **LAN Connectivity Policy** details that appear in the main tab, look for the upper section displaying the current vNICs, then click "Add" in the main area to create additional vNICs for the existing policy.
4. Create two additional vNICs using step 5 from the above section "LAN Connectivity Policy—Base vNICs for iSCSI or Fiber Channel". These two additional vNICs should be created with the vNIC templates which were created for connectivity to the iSCSI VLANs for each data path.
5. Click "Save Changes" to modify your **LAN Connectivity Policy** for the new vNICs to be available for the iSCSI configuration as the next step.
6. Once the additional vNICs have been created from the iSCSI vNIC templates and are configured for your policy (these will no longer be bold), click "Add iSCSI vNICs" to expand the iSCSI vNICs details.
7. Next, click "Add" below the iSCSI vNIC area to add iSCSI vNICs to the existing policy.

8. In the Create iSCSI vNIC pop-up that appears, enter the following details:
   a. *Name*: This is the name for the iSCSI vNIC being created; it is recommended to include 'iSCSI', along with the data path that the iSCSI vNIC provides.
   b. *Overlay vNIC*: This selection is to set the vNIC that is being used tp provide the iSCSI connectivity; select the newly created vNIC for your first data path.
   c. *iSCSI Adapter Policy*: Select 'default' for the adapter policy.
   d. *VLAN*: This selection is to set the VLAN that the iSCSI vNIC will use for the direct-attached connectivity to the FlashArray. Ensure that the correct VLAN is selected whichi was configured for the direct connect for your data path (A or B) to the array.
   e. *MAC Address Assignment*: Select the MAC Pool that was created earlier for the data path (A or B).
9. Repeat steps 7 & 8 above to create an iSCSI vNIC for the other data path. At a minimum, there should be one iSCSI vNIC created for each data path, as these vNICs will used the direct-attached appliance uplinks from the Fis to the FlashArray.
10. Click "Save Changes" to modify your **LAN Connectivity Policy** for the new iSCSI vNICs to be added to the policy.

### SAN Connectivity Policy—Fiber Channel

These steps will cover creation of a SAN Connectivity Policy that can be used to provide ethernet connectivity (via vHBAs) for service profiles using fiber channel for data connectivity.

1. In the Cisco UCS Manager, click on the **SAN** tab in the left navigation pane.
2. Select the **Policies** filter at the top of the navigation pane to only view Policies. Expand the navigation to the UCS Org that you are creating the pool under (typically 'root' upon initial deployment).
3. Once you have expanded the Org that will contain your SAN Connectivity Policy, you can either right-click the SAN Connectivity Policies subtab and click **Create SAN Connectivity Policy**, or you can expand the SAN Connectivity Policies tab and press the "Add" button in the main navigation area.
4. In the **Create SAN Connectivity Policy** pop-up that appears, enter the Name of the policy (required), the description of the policy (optional), the WWNN Pool to be used for the policy, then click “Add” in the main area to add a vHBA.
5. In the Create vHBA pop-up that appears, enter the following details:
   a. *Name*: This is the name for the vHBA being created; it is recommended to include with the data path that the vHBA provides.
   b. *Use vHBA Template*: Check this box to hide the options for manually creating a vHBA; select the vHBA template for your first data path.
   c. *Redundancy Pair*: Check this box to also set the peer vHBA to be created using the secondary template.
   d. *vHBA Template*: This selection is to set the vHBA template that is being created and named in this pop-up; select the appropriate vHBA template from the drop-down menu.
   e. *Peer Name*: This is the name for the peer vHBA being created; it is recommended to include the data path that the vHBA provides.
   f. *Adapter Policy*: This selection is to set the performance profile for the vHBA that are being created in your SAN connectivity policy; select the appropriate built-in adapter policy.
6. Once all details are entered in the **Create vHBA Template** pop-up, click "OK" to add the vHBAs to your SAN Connectivity Policy.
7. Once you have created all the necessary vHBAs in the **Create SAN Connectivity Policy** pop-up, click "OK" to create the policy.

## Boot Policy—Fiber Channel

These steps will cover the configuration of a boot policy for Boot from SAN leveraging the fiber channel connected vHBAs on the service profile. This boot policy will only work if you have configured the fiber channel requirements (VSANs, vHBA Templates, and a SAN Connectivity Policy).

1. In the Cisco UCS Manager, click on the **Servers** tab in the left navigation pane.
2. Select the **Policies** filter at the top of the navigation pane to only view Policies. Expand the navigation to the UCS Org that you are creating the pool under (typically 'root' upon initial deployment).
3. Once you have expanded the Org that will contain your Boot Policy, you can either right-click the **Boot Policies** subtab and click **Create Boot Policy**, or you can expand the Boot Policies tab and press the "Add" button in the main navigation area.
4. In the **Create Boot Policy** pop-up that appears, enter the Name of the policy (required), the description of the policy (optional), click the box to select the options for both 'Reboot on Boot Order Change' and 'Enforce vNIC/vHBA/iSCSI Name', and set the boot mode to 'Uefi'. Click the box to select the option for both 'Boot Security' if necessary for the environment.

   **NOTE:** It is not recommended to use 'Legacy' boot mode, unless you have a specific requirement for the system not to be UEFI-enabled.

5. In the subtabs for boot options on the bottom left, click "Local Devices" to expand the boot options menu, then look under the 'Add CD/DVD' section and click "Add Remote CD/DVD" to allow for the remote KVM to mount installation media.
6. In the subtabs for boot options on the bottom left, click "vHBAs" to expand the appropriate SAN Boot Options.
7. Click **Add SAN Boot**, and in the Add SAN Boot pop-up that appears, click the radio button to set the type to 'Primary'. Once this option if set, a dialog box will appear for 'vHBA', and the name of one of the vHBAs created in the SAN Connectivity Profile should be entered here.
8. Highlight the new SAN Primary object created in the Boot Order on the main window, and then click "Add SAN Boot Target" from the vHBAs menu on the left.
9. In the **Add SAN Boot** pop-up that appears, enter the following details:
   a. *Boot Target LUN*: This is the LUN ID of the volume the service profile will boot from; set this as '1'.
   b. *Boot Target WWPN*: Enter the WWPN of the first physical adapter on the FlashArray which is connected to the data path for this specific vHBA.
   c. *Type*: This option is to set the address as the first or second to be defined for the boot device; select 'Primary'.
10. Click "OK" to add the SAN Boot Target to the Boot Order.
11. Repeat steps 7 & 8 to add another SAN Boot Target. This time, the Add SAN Boot Target pop-up that appears will already have the type set to 'Secondary'. For the 'Boot Target WWPN', enter the WWPN of the second physical adapter on the FlashArray which is connected to the same data path as the vHBA.
12. At the **Create Boot Policy** pop-up, click "Add SAN Boot" again. This time, the Add SAN Boot pop-up that appears will already have the type set to 'Secondary'. In the 'vHBA' dialog, enter the name of the second vHBA created in the SAN Connectivity Profile.
13. Highlight the new SAN Secondary object created in the Boot Order on the main window, and then click "Add SAN Boot Target" from the vHBAs menu on the left.

14. In the **Add SAN Boot** pop-up that appears, enter the following details:
    a. *Boot Target LUN*: This is the LUN ID of the volume that the service profile will boot from; leave this as '1'.
    b. *Boot Target WWPN*: Enter the WWPN of the first physical adapter on the FlashArray which is connected to the data path for this specific vHBA.
    c. *Type*: This option is to set the address as the first or second to be defined for the boot device; select 'Primary'.
15. Click "OK" to add the SAN Boot Target to the Boot Order.
16. Repeat steps 12 & 13 to add another SAN Boot Target. This time, the **Add SAN Boot Target** pop-up that appears will already have the type set to 'Secondary'. For the 'Boot Target WWPN', enter the WWPN of the second physical adapter on the FlashArray which is connected to the same data path as the vHBA.
17. Once you have created the Remote CD/DVD, 2 SAN Boot, and 2 SAN Boot Target objects in the **Create Boot Policy** pop-up, click "OK" to create the policy.

## Boot Policy—iSCSI

These steps will cover the configuration of a boot policy for Boot from SAN leveraging the iSCSI connected vNICs on the service profile. This boot policy will only work if you have configured the iSCSI requirements (VLANs, vNIC Templates, and a LAN Connectivity Policy including iSCSI vNICs).

1. In the Cisco UCS Manager, click on the Servers tab in the left navigation pane.
2. Select the Policies filter at the top of the navigation pane to only view Policies. Expand the navigation to the UCS Org that you are creating the pool under (typically 'root' upon initial deployment).
3. Once you have expanded the Org that will contain your Boot Policy, you can either right-click the Boot Policies subtab and click Create Boot Policy, or you can expand the Boot Policies tab and press the "Add" button in the main navigation area.
4. In the Create Boot Policy pop-up that appears, enter the Name of the policy (required), the description of the policy (optional), click the box to select the options for both 'Reboot on Boot Order Change' and 'Enforce vNIC/vHBA/iSCSI Name', and set the boot mode to 'Uefi'. Click the box to select the option for both 'Boot Security' if necessary for the environment.

   **NOTE:** It is not recommended to use 'Legacy' boot mode, unless you have a specific requirement for the system not to be UEFI-enabled.

5. In the subtabs for boot options on the bottom left, click "Local Devices" to expand the boot options menu, then look under the 'Add CD/DVD' section and click "Add Remote CD/DVD" to allow for the remote KVM to mount installation media.
6. In the subtabs for boot options on the bottom left, click "iSCSI vNICs" to expand the appropriate iSCSI Boot Options
7. Click "Add iSCSI Boot", and in the Add iSCSI Boot pop-up that appears, enter the name of first iSCSI vNIC created in the LAN Connectivity Profile.
8. Click "Add iSCSI Boot" again, and in the Add iSCSI Boot pop-up that appears, enter the name of second iSCSI vNIC created in the LAN Connectivity Profile.

   **NOTE:** The name of the iSCSI vNICs should be entered here, not the overlay vNIC.

9. Once you have created the Remote CD/DVD and 2 iSCSI Boot objects in the Create Boot Policy pop-up, click "OK" to create the policy.

## UCS Service Profile Templates

These steps will cover all configuration options for service profile templates which can provide iSCSI and/or fiber channel connectivity, if all of the prerequisite components and policies have been created. Be aware that additional configuration is required to set the iSCSI Boot Parameters during the creation of the service profile template, which is found on the 'Server Boot Order' tab listed below.

For the configuration of Service Profile Templates within the Server tab, this is how the filtered view of the Service Profile Templates under the Server tab will appear:

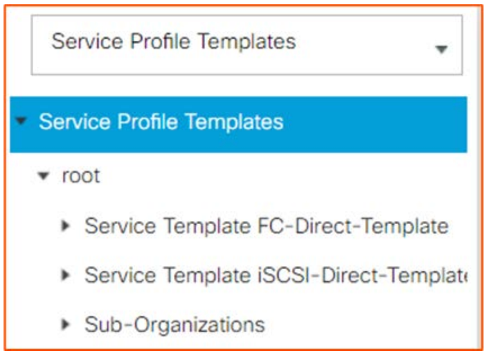

Service Profile Templates
Service Profile Templates
root
Service Template FC-Direct-Template
Service Template iSCSI-Direct-Templat
Sub-Organizations

**FIGURE 14** Filtering the view to Service Profile Templates within Server tab

1. In the Cisco UCS Manager, click on the Servers tab in the left navigation pane.
2. Select the Service Profile Templates filter at the top of the navigation pane to only view Service Profile Templates. Expand the navigation to the UCS Org you are creating the pool under (typically 'root' upon initial deployment).
3. Once you have expanded the Org that will contain your Service Profile Template, you can either right-click the Service Profile Templates subtab and click Create Service Profile Template, or you can expand the Service Profile Templates tab and press the "Add" button in the main navigation area.
4. In the Create Service Profile Templates pop-up that appears, we begin in the 'Identify Service Profile Template' tab. Enter the Name of the template (required), select the radio button to set the type as 'Updating Template', and set the UUID Assignment to the UUID Pool that was configured earlier. Click 'Next' to proceed to the next tab.
5. Next, the configuration moves to the 'Storage Provisioning' tab. We will skip all options on this tab, as we are configuring only Boot from SAN for these service profile templates.
6. Next, the configuration moves to the 'Networking' tab. Select the radio button for 'Use Connectivity Policy' and select the appropriate LAN Connectivity Policy which was configured earlier. If this template is built with a LAN Connectivity Policy is providing iSCSI connectivity, then the 'Initiator Name Assignment' dropdown should be set to the IQN Pool which was created earlier.
7. Next, the configuration moves to the 'SAN Connectivity' tab. If this template will provide fiber channel connectivity, select the radio button for 'Use Connectivity Policy', then the SAN Connectivity Policy' dropdown should be set to the policy created earlier. If this template will not provide fiber channel connectivity, select the radio button for 'No vHBAs'.
8. Next, the configuration moves to the 'Zoning' tab. We will skip all options on this tab, as we are not configuring vHBA Initiator Groups.

9. Next, the configuration moves to the'vNIC/vHBA Placement' tab. For the 'Select Placement' dropdown, the default of "Let System Perform Placement" is preferred since we are not configuring dynamic vNICs/vHBAs in these service profile templates.
10. Next, the configuration moves to the 'vMedia' Policy tab. We will skip all options on this tab, as we are not configuring vMedia Policies in these service profile templates.
11. Next, the configuration moves to the 'Server Boot Order' tab. Select the appropriate boot policy for Boot from SAN via iSCSI or fiber channel to be used by the template.
12. If iSCSI Boot from SAN is being configured for this template, once you have set your Boot Policy, expand the iSCSI option under boot order to set your iSCSI Boot Parameters for each iSCSI boot object.
    a. The drop-down menu for 'Initiator Name Assignment' should be set to your IQN pool, and the Initiator Address should be set to the iSCSI IP Pool for the data path if the iSCSI vNIC.
    b. Click "Add" to create an iSCSI Static Target, and in this pop-up menu, you will need to enter an iSCSI target name (IQN of the FlashArray), along with the IP address of the virtual interface on the FlashArray connected to the FI on the same data path as your iSCSI vNIC.
    c. Repeat this step to create a second iSCSI Static Target for the Primary iSCSI boot option.
    d. Continue these same steps to create two iSCSI Static Targets for the Secondary iSCSI boot option using the appropriate details for the other data path.
13. Next, the configuration moves to the 'Maintenance Policy' tab. For the 'Maintenance Policy' dropdown, selecting the "default" policy is acceptable.

    **NOTE:** While not covered in this guide, creating a Maintenance Policy which opts for "User Ack" or "On Next Reboot" as the Reboot Policy is preferred in most environments.

14. Next, the configuration moves to the 'Server Assignment' tab. For the 'Pool Assignment' dropdown, the default of "Assign Later" is preferred since we are not configuring server pools. For the 'Host Firmware Package' dropdown, the default policy is acceptable.

    **NOTE:** The user can create a Host Firmware Package if it is necessary to assign or upgrade to a specific host firmware version. This can also be assigned to the template in the future to handle firmware upgrades.

15. Next, the configuration moves to the 'Operational Policies' tab. The user should select the appropriate policies for the template, with the recommended minimum configurations for policies including these dropdown menus: 'BIOS Profile', 'External IPMI/Redfish Management Configuration', and 'Management IP Address'.
16. Click "Finish" to create your Service Profile Template.

## Deployment of VMware vSphere

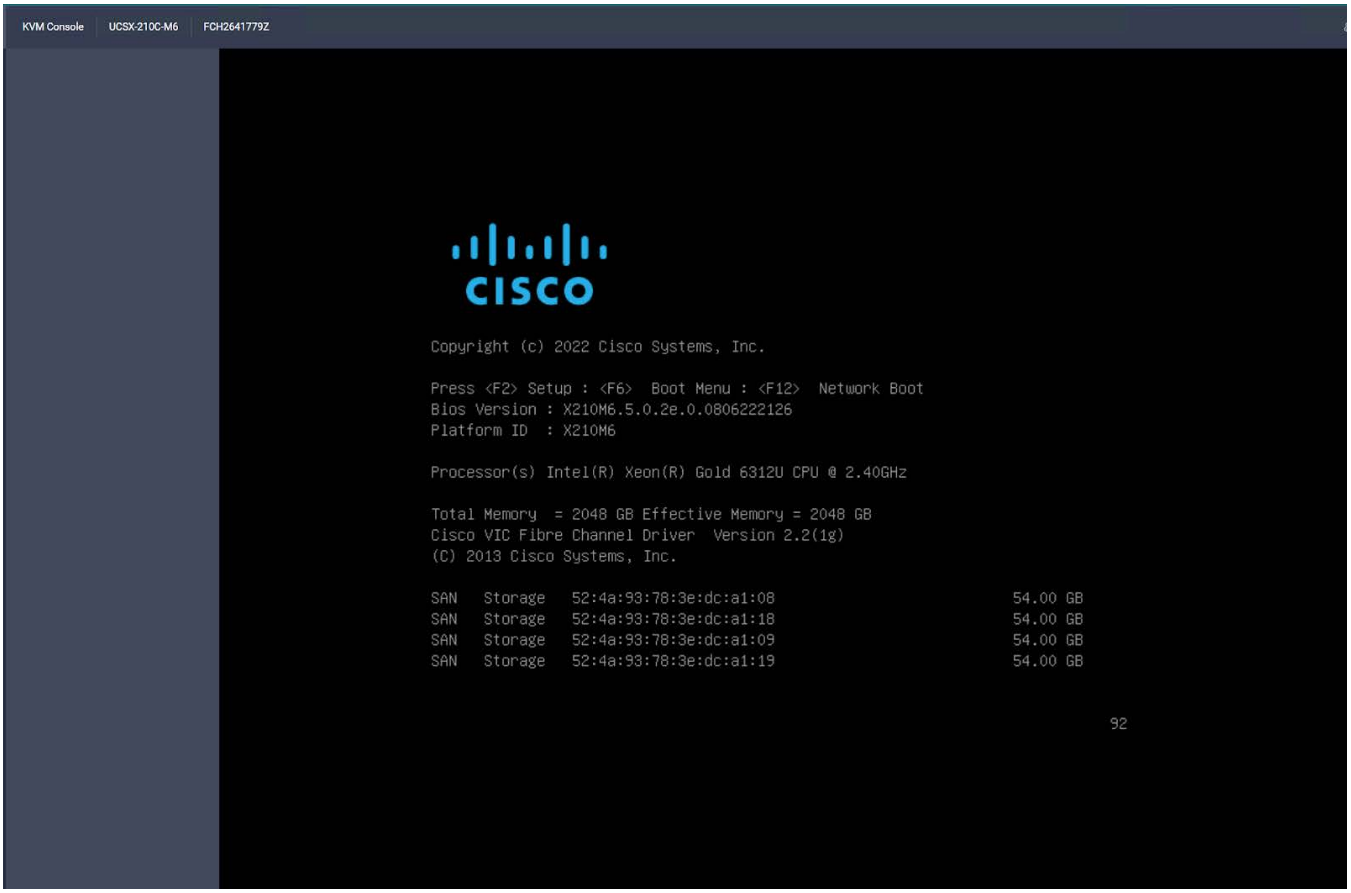
Once the above configuration sections have been completed, we can create Service Profiles from the newly created UCS Service Profile templates. After the Service Profiles have been created and associated with servers, the creation of hosts, host groups (if necessary), and volumes will need to be completed within the FlashArray.

The steps for the creation of service profiles from template are not covered within this document with screenshots, as these follow the standard steps contained within any Cisco Validated Design and Cisco UCS documentation; likewise, the steps for creating these objects on the FlashArray follow the standard steps contained within any Cisco Validated Design and Pure Storage documentation.

### Boot from SAN Connectivity

Once we have booted the servers with our associated service profiles, we will see similar connections at server boot, and within the Pure Storage FlashArray connection details.

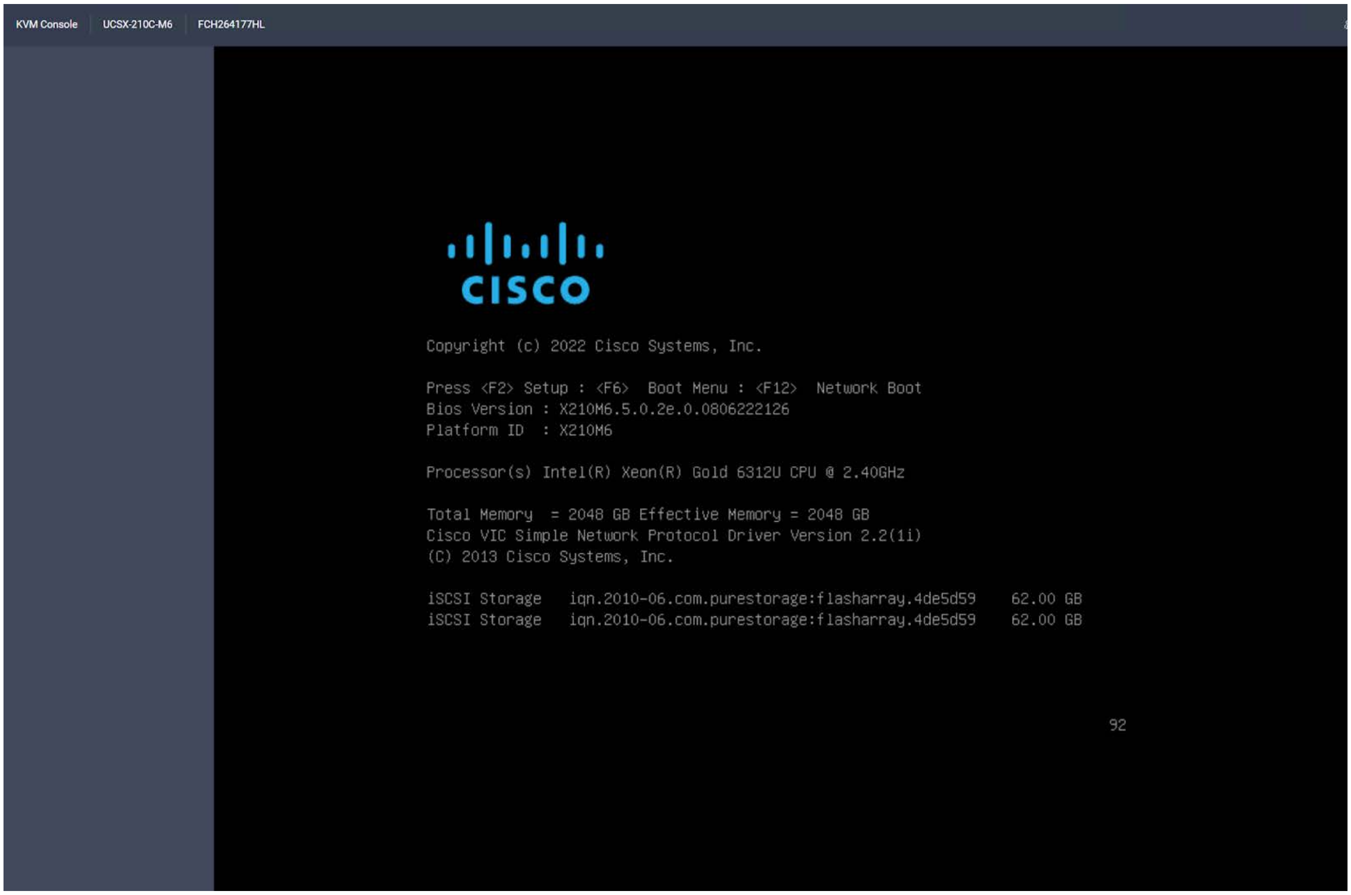
When we boot our Service Profile configured for Fiber Channel Boot from SAN, we can see the storage connection after the VIC has loaded the driver and scanned the vHBA:



```
Copyright (c) 2022 Cisco Systems, Inc.

Press <F2> Setup : <F6>  Boot Menu : <F12>  Network Boot
Bios Version : X210M6.5.0.2e.0.0806222126
Platform ID  : X210M6

Processor(s) Intel(R) Xeon(R) Gold 6312U CPU @ 2.40GHz

Total Memory  = 2048 GB Effective Memory = 2048 GB
Cisco VIC Fibre Channel Driver  Version 2.2(1g)
(C) 2013 Cisco Systems, Inc.

SAN   Storage   52:4a:93:78:3e:dc:a1:08                     54.00 GB
SAN   Storage   52:4a:93:78:3e:dc:a1:18                     54.00 GB
SAN   Storage   52:4a:93:78:3e:dc:a1:09                     54.00 GB
SAN   Storage   52:4a:93:78:3e:dc:a1:19                     54.00 GB

                                                                    92
```

**FIGURE 15** View of connected storage during boot of Service Profile configured for Fiber Channel Boot from SAN

When we boot our Service Profile configured for iSCSI Boot from SAN, we can see the storage connection after the VIC has loaded the driver and scanned the iSCSI vNIC:

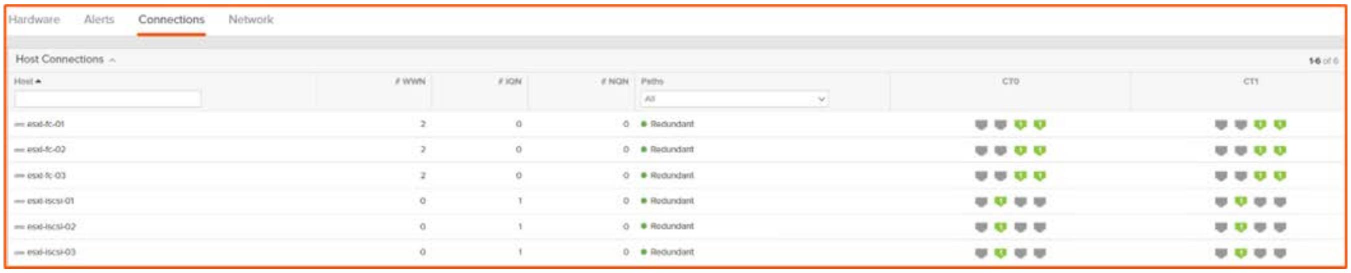


```
Copyright (c) 2022 Cisco Systems, Inc.

Press <F2> Setup : <F6>  Boot Menu : <F12>  Network Boot
Bios Version : X210M6.5.0.2e.0.0806222126
Platform ID  : X210M6

Processor(s) Intel(R) Xeon(R) Gold 6312U CPU @ 2.40GHz

Total Memory  = 2048 GB Effective Memory = 2048 GB
Cisco VIC Simple Network Protocol Driver Version 2.2(1i)
(C) 2013 Cisco Systems, Inc.

iSCSI Storage   iqn.2010-06.com.purestorage:flasharray.4de5d59    62.00 GB
iSCSI Storage   iqn.2010-06.com.purestorage:flasharray.4de5d59    62.00 GB

                                                                       92
```

**FIGURE 16** View of connected storage during boot of Service Profile configured for iSCSI Boot from SAN

## FlashArray Host Connectivity

When we log into our Pure Storage FlashArray, we can see our redundant connections for all servers, which are configured for Fiber Channel and iSCSI Boot from SAN:



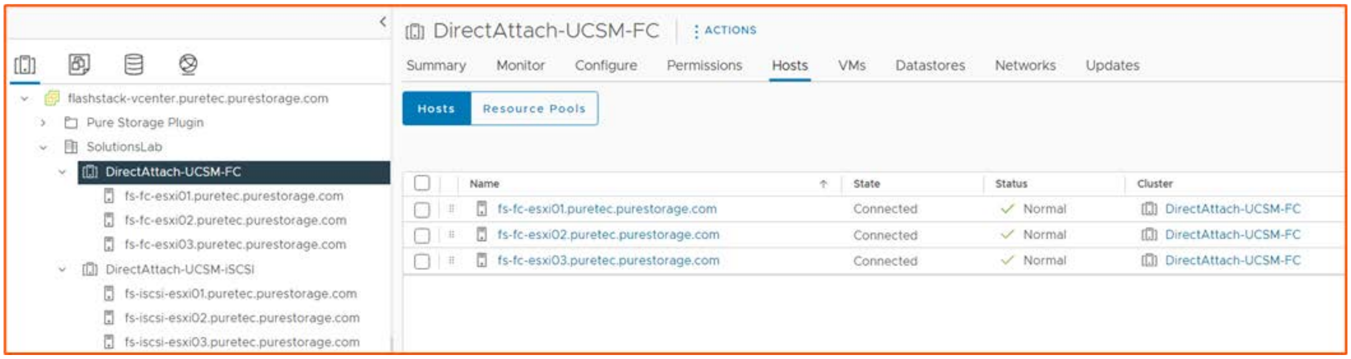
| Host ▴ | # WWN | # IQN | # NQN | Paths | CT0 | CT1 |
|---|---|---|---|---|---|---|
| | | | | All | | |
| esxi-fc-01 | 2 | 0 | 0 | ● Redundant | ■ ■ 🟩 🟩 | ■ ■ 🟩 🟩 |
| esxi-fc-02 | 2 | 0 | 0 | ● Redundant | ■ ■ 🟩 🟩 | ■ ■ 🟩 🟩 |
| esxi-fc-03 | 2 | 0 | 0 | ● Redundant | ■ ■ 🟩 🟩 | ■ ■ 🟩 🟩 |
| esxi-iscsi-01 | 0 | 1 | 0 | ● Redundant | ■ 🟩 ■ ■ | ■ 🟩 ■ ■ |
| esxi-iscsi-02 | 0 | 1 | 0 | ● Redundant | ■ 🟩 ■ ■ | ■ 🟩 ■ ■ |
| esxi-iscsi-03 | 0 | 1 | 0 | ● Redundant | ■ 🟩 ■ ■ | ■ 🟩 ■ ■ |

**FIGURE 17** View of host connections within Pure Storage FlashArray for FC & iSCSI Boot from SAN service profiles

## vSphere Host Connectivity

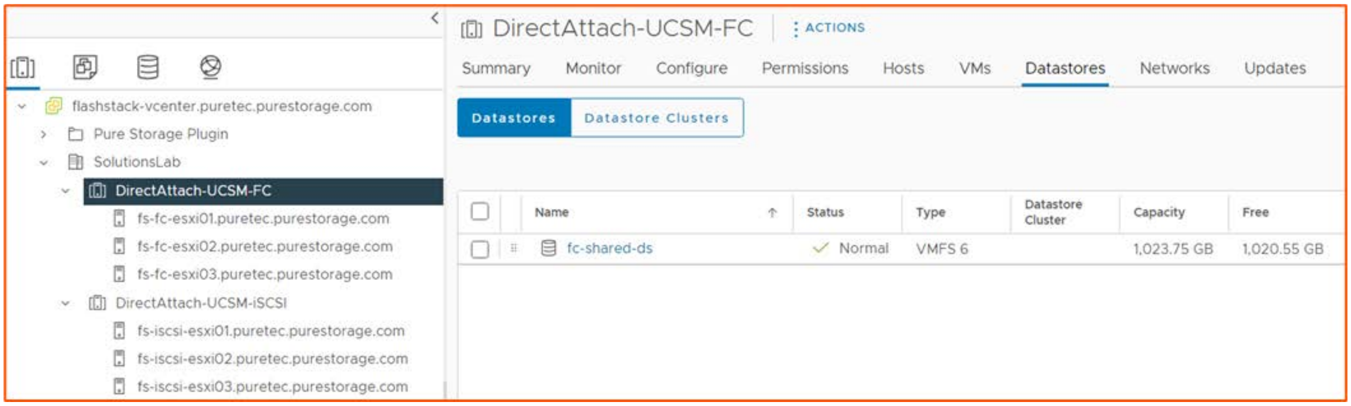
To demonstrate host and storage connectivity, after the hosts were booted successfully, vSphere ESXi is installed. Clusters are then configured with a FlashArray host group for the FC and iSCSI service profiles, and each cluster is mapped to a shared volume used as a VMFS datastore.

### Fiber Channel Cluster Hosts & Datastore


flashstack-vcenter.puretec.purestorage.com
Pure Storage Plugin
SolutionsLab
DirectAttach-UCSM-FC
fs-fc-esxi01.puretec.purestorage.com
fs-fc-esxi02.puretec.purestorage.com
fs-fc-esxi03.puretec.purestorage.com
DirectAttach-UCSM-iSCSI
fs-iscsi-esxi01.puretec.purestorage.com
fs-iscsi-esxi02.puretec.purestorage.com
fs-iscsi-esxi03.puretec.purestorage.com
DirectAttach-UCSM-FC
ACTIONS
Summary
Monitor
Configure
Permissions
Hosts
VMs
Datastores
Networks
Updates
Hosts
Resource Pools

| Name | State | Status | Cluster |
|---|---|---|---|
| fs-fc-esxi01.puretec.purestorage.com | Connected | ✓ Normal | DirectAttach-UCSM-FC |
| fs-fc-esxi02.puretec.purestorage.com | Connected | ✓ Normal | DirectAttach-UCSM-FC |
| fs-fc-esxi03.puretec.purestorage.com | Connected | ✓ Normal | DirectAttach-UCSM-FC |

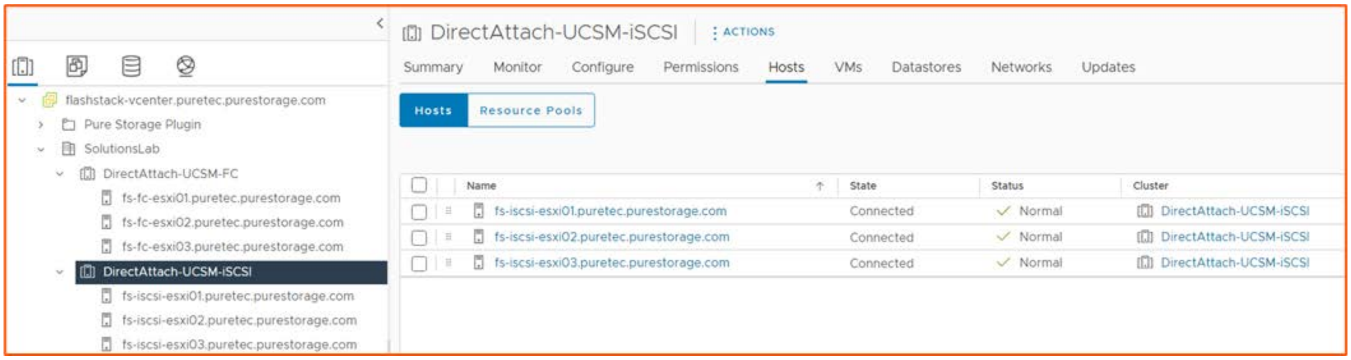
**FIGURE 18** View of hosts within vSphere cluster for Fiber Channel service profiles


flashstack-vcenter.puretec.purestorage.com
Pure Storage Plugin
SolutionsLab
DirectAttach-UCSM-FC
fs-fc-esxi01.puretec.purestorage.com
fs-fc-esxi02.puretec.purestorage.com
fs-fc-esxi03.puretec.purestorage.com
DirectAttach-UCSM-iSCSI
fs-iscsi-esxi01.puretec.purestorage.com
fs-iscsi-esxi02.puretec.purestorage.com
fs-iscsi-esxi03.puretec.purestorage.com
DirectAttach-UCSM-FC
ACTIONS
Summary
Monitor
Configure
Permissions
Hosts
VMs
Datastores
Networks
Updates
Datastores
Datastore Clusters

| Name | Status | Type | Datastore Cluster | Capacity | Free |
|---|---|---|---|---|---|
| fc-shared-ds | ✓ Normal | VMFS 6 | | 1,023.75 GB | 1,020.55 GB |

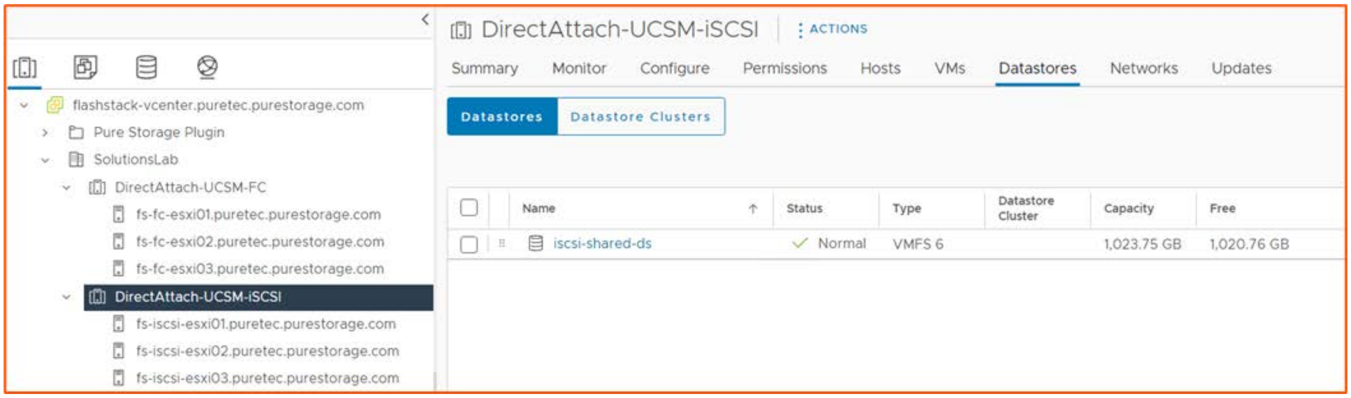
**FIGURE 19** View of datastore within vSphere cluster for Fiber Channel service profiles

### iSCSI Cluster Hosts & Datastore


DirectAttach-UCSM-iSCSI
ACTIONS
Summary
Monitor
Configure
Permissions
Hosts
VMs
Datastores
Networks
Updates
Hosts
Resource Pools
flashstack-vcenter.puretec.purestorage.com
Pure Storage Plugin
SolutionsLab
DirectAttach-UCSM-FC
fs-fc-esxi01.puretec.purestorage.com
fs-fc-esxi02.puretec.purestorage.com
fs-fc-esxi03.puretec.purestorage.com
DirectAttach-UCSM-iSCSI
fs-iscsi-esxi01.puretec.purestorage.com
fs-iscsi-esxi02.puretec.purestorage.com
fs-iscsi-esxi03.puretec.purestorage.com

| Name ↑ | State | Status | Cluster |
|---|---|---|---|
| fs-iscsi-esxi01.puretec.purestorage.com | Connected | ✓ Normal | DirectAttach-UCSM-iSCSI |
| fs-iscsi-esxi02.puretec.purestorage.com | Connected | ✓ Normal | DirectAttach-UCSM-iSCSI |
| fs-iscsi-esxi03.puretec.purestorage.com | Connected | ✓ Normal | DirectAttach-UCSM-iSCSI |

**FIGURE 20** View of hosts within vSphere cluster for iSCSI service profiles


DirectAttach-UCSM-iSCSI
ACTIONS
Summary
Monitor
Configure
Permissions
Hosts
VMs
Datastores
Networks
Updates
Datastores
Datastore Clusters
flashstack-vcenter.puretec.purestorage.com
Pure Storage Plugin
SolutionsLab
DirectAttach-UCSM-FC
fs-fc-esxi01.puretec.purestorage.com
fs-fc-esxi02.puretec.purestorage.com
fs-fc-esxi03.puretec.purestorage.com
DirectAttach-UCSM-iSCSI
fs-iscsi-esxi01.puretec.purestorage.com
fs-iscsi-esxi02.puretec.purestorage.com
fs-iscsi-esxi03.puretec.purestorage.com

| Name ↑ | Status | Type | Datastore Cluster | Capacity | Free |
|---|---|---|---|---|---|
| iscsi-shared-ds | ✓ Normal | VMFS 6 | | 1,023.75 GB | 1,020.76 GB |

**FIGURE 21** View of datastores within vSphere cluster for iSCSI service profiles

## Conclusion

Flexibility, performance, reliability, and ease of management are critical needs of any IT customer. When running FlashStack in a direct-attached model, these needs can be met while providing a fully functional converged infrastructure with reduced rack space and power consumption requirements in private cloud deployments.

FlashStack can meet the needs of any workload needed by a customer, while giving the flexibility to upgrade and expand their environment as needed. With the capability to do this in a reduced footprint in regards to both power and cost, FlashStack truly becomes the platform to deliver more potential to all customers from the smallest to largest scale.

purestorage.com

800.379.PURE

PURESTORAGE®
Uncomplicate Data Storage, Forever