PURESTORAGE®
Uncomplicate Data Storage, Forever

REFERENCE ARCHITECTURE

FlashStack Direct Attached Configuration —IMM

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

Contents

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 an IMM (Intersight Managed Mode)environment running in a direct-attached architecture, configuration details are managed and controlled at the policy level. 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 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.

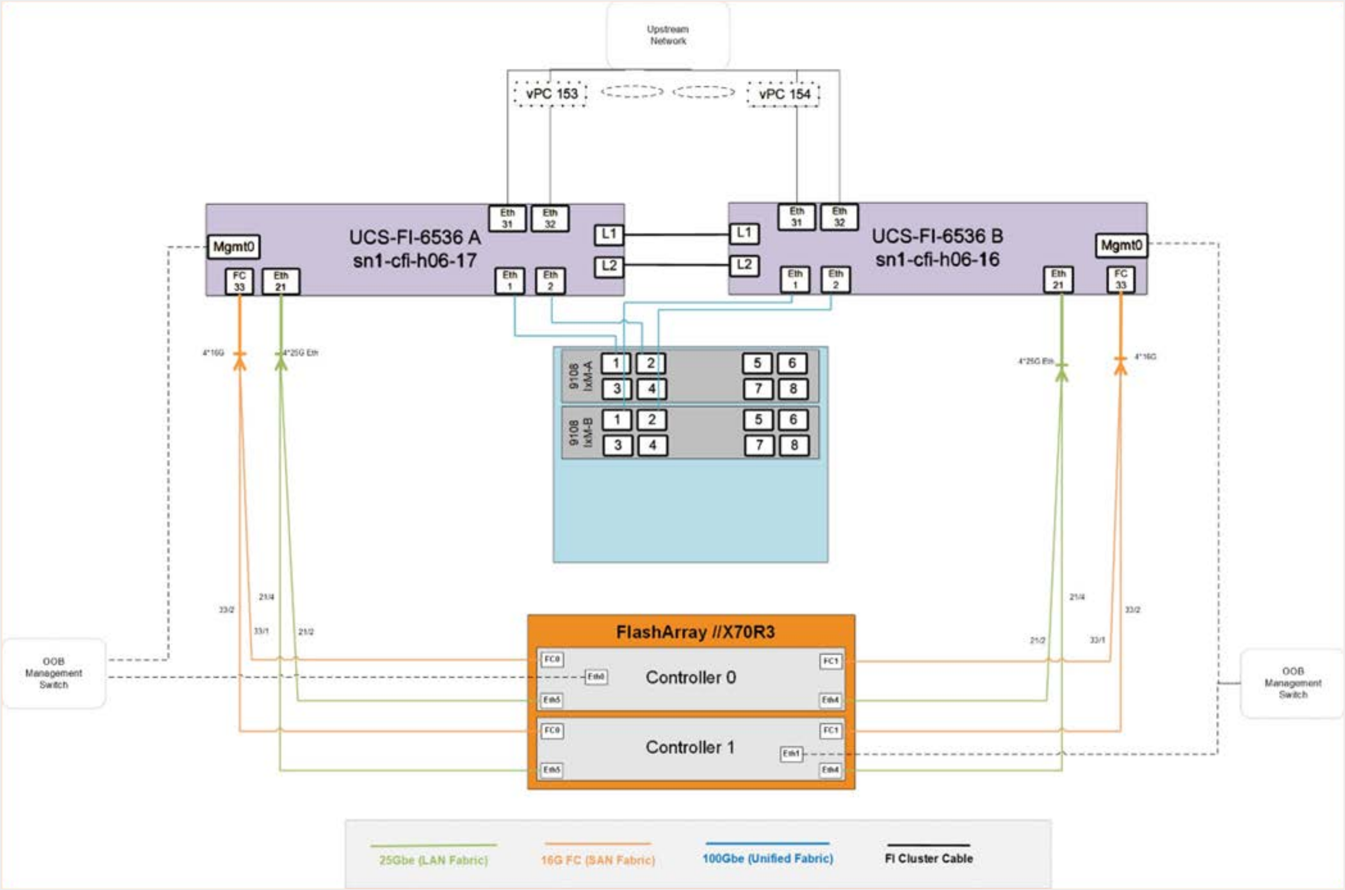


FIGURE 1 Diagram of physical connections within the lab environment used for this document.

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 (IMM Mode)
Compute (Nodes)	Cisco UCS X210c M6 Compute Node
Hypervisor	VMware ESXi, 7.0.3, 21424296 (7.0 U3l)

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 Storage FlashArray such that basic network connectivity is online, and 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—IMM

As this document is focused on running FlashStack in a direct-attach mode, there are some portions of the configuration of an Intersight environment which will not be covered within this document as they are covered within Cisco Validated Designs, UCS documentation, and the Pure Storage X-Series Deployment Guide.

The list of IMM configuration details not covered by this document is listed below, broken out by Intersight Platform Type:

Platform Type	Policies Not Covered in this Guide
UCS Domain	Multicast, Syslog, SNMP, System QoS, NTP
UCS Server	BIOS, Firmware, Power, Thermal, Virtual Media, Serial over LAN, Syslog, Storage

TABLE 2 All configuration policies not covered within the guide, listed by Intersight Platform type.

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.

Before we can create our policies used for the UCS Domain and UCS Server configurations, we need to create our pools and other core policies used by these platform and template objects.

The creation of these objects is documented in groups such that similar configuration steps follow each other for each stage to build upon previous steps.

Identifier Pools Configuration

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

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 troubleshooting required, if iSCSI is being configured for your environment

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane and click "Pools". Next, click the "Create Pool" button in the main tab, click the radio button for 'IP' and click "Start".
2. The Create IP Pool wizard appears and starts in the General tab. Select the Organization that will contain your IP Pool, enter the Name of the pool (required), Tags for the pool (optional), and Description of the pool (optional). Click "Next".
3. In the IPv4 Pools tab of the wizard, the 'Configure IPv4 Pool' option is enabled by default. In the main navigation area, enter the following details:
   a. Netmask: This field is the subnet mask for your network subnet
   b. Gateway: This field is the default gateway for your network subnet (optional)
   c. Primary DNS/Secondary DNS: These fields are for your primary & secondary DNS IP addresses (optional)
   d. (IP Blocks) From: This field is your starting IPv4 address
   e. (IP Blocks) Size: This field is the size of your IP blocks—the number of IP addresses contained in the pool

4. Once all details are entered in the pool details area, click "Next" to the IPv4 pool.
5. If IPv6 blocks are required, follow the same direction as step 5 as above to create an IPv6 block. If IPv6 blocks are not required, deselect 'Configure IPv6 Pool'.
6. Click "Create" in the Create IP Pool wizard to complete your IP Pool creation.

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 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 troubleshooting required

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane and click "Pools". Next, click the "Create Pool" button in the main tab, click the radio button for 'MAC' and click "Start".
2. The Create MAC Pool wizard appears and starts in the General tab. Select the Organization that will contain your MAC Pool, enter the Name of the pool (required), Tags for the pool (optional), and Description of the pool (optional). Click "Next".
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.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".
4. In the Pool Details tab of the wizard, enter the following details:

   a. MAC Blocks: 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
   NOTE: Intersight requires the use of the following MAC prefix: 00:25:B5:xx:xx:xx

1. Once all details are entered in the MAC Blocks section, click "Create" to complete your MAC Pool creation.

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 Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane and click "Pools". Next, click the "Create Pool" button in the main tab, click the radio button for 'IQN' and click "Start".
2. The Create IQN Pool wizard appears and starts in the General tab. Select the Organization that will contain your IQN Pool, enter the Name of the pool (required), Tags for the pool (optional), and Description of the pool (optional). Click "Next".
3. In the Pool Details tab of the wizard, enter the following details:

   a. Prefix: This field is the text of the IQN prefix for the pool
   NOTE: IQN prefixes must match the following pattern: iqn.yyyy-mm.naming-authority

   b. Suffix: This field is text of the IQN suffix to be added for the pool

   c. From: This field is the starting IQN

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

1. Once all details are entered in the Pool Details section, click "Create" to complete your IQN Pool creation.

Create WWNN Pools

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

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane and click "Pools". Next, click the "Create Pool" button in the main tab, click the radio button for 'WWNN' and click "Start".
2. The Create WWNN Pool wizard appears and starts in the General tab. Select the Organization that will contain your WWNN Pool, enter the Name of the pool (required), Tags for the pool (optional), and Description of the pool (optional). Click "Next".
3. In the Pool Details tab of the wizard, enter the following details:

   a. From: This field is the starting WWN

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

   NOTE: Intersight requires the use of the following WWN prefix: 20:00:00:25:B5:xx:xx:xx

4. Once all details are entered in the Pool Details section, click "Create" to complete your WWNN Pool creation.

Create WWPN Pools

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

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

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane and click "Pools". Next, click the "Create Pool" button in the main tab, click the radio button for 'WWPN' and click "Start".
2. The Create WWPN Pool wizard appears and starts in the General tab. Select the Organization that will contain your WWPN Pool, enter the Name of the pool (required), Tags for the pool (optional), and Description of the pool (optional). Click "Next".
3. In the Pool Details tab of the wizard, enter the following details:

   a. From: This field is the starting WWN

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

   NOTE: Intersight requires the use of the following WWN prefix: 20:00:00:25:B5:xx:xx:xx

4. Once all details are entered in the Pool Details section, click "Create" to complete your WWPN Pool creation.

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 Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane and click "Pools". Next, click the "Create Pool" button in the main tab, click the radio button for 'WWNN' and click "Start".
2. The Create WWNN Pool wizard appears and starts in the General tab. Select the Organization that will contain your WWNN Pool, enter the Name of the pool (required), Tags for the pool (optional), and Description of the pool (optional). Click "Next".
3. In the Pool Details tab of the wizard, enter the following details:
    a. Prefix: This field is the text of the UUID prefix for the pool
    b. From: This field is the starting UUID suffix
    c. Size: This field is the size of the UUID block—the quantity of UUIDs contained in the pool
4. Once all details are entered in the Pool Details section, click "Create" to complete your UUID Pool creation.

Core Policies Configuration

We will now create the policies that will provide the ethernet and fiber channel connectivity to be consumed by our UCS Domain and UCS Server profiles.

Create System QoS Policy

This policy provides the configuration to prioritize network traffic based on the importance of the network for a UCS Domain profile.

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for 'System QoS' and click "Start".
2. The Create System QoS Policy wizard appears and starts in the General tab. Select the Organization that will contain the System QoS policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Click "Next".
3. In the Policy Details tab of the wizard, change the MTU value to ‘9216’ for the Best Effort class and leave the rest of the settings at their defaults.
4. Once all details are entered in the Policy Details section, click "Create" to complete the System QoS Policy creation.

Create VLAN Policy

These steps will be followed to create a VLAN Policy to define all VLANs used within a UCS Domain.

NOTE: For a configuration including iSCSI, although there are iSCSI VLANs defined for each distinct data path (A or B), we will define all VLANs within the VLAN policy, and control access for uplinks and vNICs through Ethernet Network Group Policies.

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for 'VLAN' and click "Start".
2. The Create VLAN Policy wizard appears and starts in the General tab. Select the Organization that will contain the VLAN policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Click "Next".
3. In the Policy Details tab of the wizard, click the "Add VLANs" button and enter the following details:
    a. Name/Prefix: This field is the text name or prefix for the VLAN (required)

    b. VLAN IDs: This field is the ID of the VLAN (required)

    NOTE: While VLAN ranges are allowed in this field, it is recommended to create a VLAN for each distinct VLAN ID.

    c. Auto Allow on Uplinks: This field allows the VLAN to be auto allowed on uplinks; deselect this so that Ethernet Network Groups can be leveraged for VLAN restrictions

    d. Multicast Policy: This guide does not walkthrough this policy, and a policy should be created to meet the network requirements of your environment
4. Once you have filled in all details for the VLAN, click "Add" to add the VLAN.
5. Repeat steps 3 & 4 for all VLANs necessary for the UCS environment.
6. Click "Set Native VLAN ID" and enter the ID of the native VLAN for the environment.
7. Once all details are entered in the Policy Details section, click "Create" to complete the VLAN Policy creation.

Create Ethernet Network Group Policy

These same steps will be followed to create all Ethernet Network Group Policies which are necessary for the environment, as these provide the configuration to include all VLANs to either pass upstream network traffic, or to grant VLAN access to the vNICs. 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).

NOTE: For a configuration without iSCSI, only one Ethernet Network Group Policy is required to provision all VLANs for both upstream network traffic, and allowing VLAN access to all vNICs. For a configuration including iSCSI, three Ethernet Network Group Policies are required. One policy will provision all VLANs for upstream network traffic, and the other two will allow VLAN access to vNICs for each distinct data path (A or B).

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for 'Ethernet Network Group' and click "Start".
2. The Create Ethernet Network Group Policy wizard appears and starts in the General tab. Select the Organization that will contain the Ethernet Network Group policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Click "Next".

3. In the Policy Details tab of the wizard, enter the following details:

    a. Native VLAN: This field is the ID of the VLAN for untagged traffic on uplink/vNIC

    b. Allowed VLANs: This field is the list of comma-separated IDs of all VLAN for untagged traffic on uplink/vNIC
    NOTE: Ensure that you are entering the correct Native VLAN IDs, and that all VLANs re included for the policy to be applied to uplinks. For the policy used for iSCSI vNICS, include all production VLANs and ONLY the iSCSI VLAN for each distinct data path (A or B).

4. Once all details are entered in the Policy Details section, click "Create" to complete the Ethernet Network Group Policy creation.

Create VSAN Policy

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

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for 'VSAN' and click "Start".
2. The Create VSAN Policy wizard appears and starts in the General tab. Select the Organization that will contain the VSAN policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Click "Next".
3. In the Policy Details tab of the wizard, click the "Add VSAN" button and enter the following details:

    a. Name: This field is the text name for the VSAN (required)

    b. VSAN Scope: This field controls the usage of the VSAN ID; select 'Storage'

    c. VSAN ID: This field is the ID of the VSAN (required)

    d. FCoE VLAN ID: This field is the FCoE VLAN ID that the VSAN will use (required)

4. Once you have filled in all details for the VLAN, click "Add" to add the VSAN.
5. Once all details for a single VSAN are entered in the Policy Details section, click "Create" to complete the VSAN Policy creation.
6. Repeat steps 3-5 to create another VSAN Policy for the opposite data path for the UCS environment.

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.

Create Port Policy

The final policy to configure for our UCS Domain profile is the port policy, which defines all FI connectivity within your environment. Follow these steps to create two Port Policies to configure the FIs for each data path (A or B).

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for 'Port' and click "Start".
2. The Create Port Policy wizard appears and starts in the General tab. Select the Organization that will contain the VSAN policy, enter the Name of the policy (required), the Fabric Interconnect Switch Model for the UCS Domain (required), Tags for the policy (optional), and the Description of the policy (optional). Click "Next".
3. Next, the wizard brings up the Unified Port tab. Drag the slider to the right to select the number of fibre channel ports to be used on the FIs (maximum of 16 ports on 6454/64108 FIs, or 4 ports on 6536 FIs). Click "Next".
4. Next, the wizard brings up the Breakout Options tab. The main window displays the list of Ethernet ports first. Click the checkbox for any ports that need to be set to any specific breakout type (4×10G or 4×25G), then click the “Configure” button and choose the correct Ethernet breakout option. Click ‘Set’ to configure the Ethernet breakouts. Continue for any additional breakouts that need to be configured.
5. If you are configuring a UCS Domain on 6536 FIs, click the ‘Fibre Channel’ option at the top of the main window. Click the checkbox for any ports that need to be set to any specific breakout type (4×8G, 4×16G, or 4×32G), then click the “Configure” button and choose the correct Fibre Channel breakout option. Click ‘Set’ to configure the Fibre Channel breakouts. Continue for any additional breakouts that need to be configured.
6. Once all of the Ethernet and Fibre Channel breakouts have been set, click "Next".
7. Next, the wizard brings up the Port Roles tab, and will start with ‘Port Roles’ in the main window. We will configure ports roles in groups based on their functionality.
8. For Ethernet uplink ports, click the checkbox for each of the FI ports and click “Configure”. In the Configure Port menu, select ‘Ethernet Uplink ' from the dropdown menu as the port role. In the new options that appear, set the Admin Speed for your ports, select the Ethernet Network Group policy for your uplinks, and click “Save”.
9. For Ethernet links to chassis, click the checkbox for each of the FI ports and click “Configure”. In the Configure Port menu, select ‘Server' from the dropdown menu as the port role. In the new options that appear, leave ‘Auto Negotiation’ enabled, and click “Save”.
10. For Fibre Channel ports directly connected to the FlashArray, click the checkbox for each of the FI ports and click “Configure”. In the Configure Port menu, select ‘Ethernet Uplink ' from the dropdown menu as the port role. In the new options that appear, set correct VSAN ID for the port policy being created (either A or B), and click “Save”.
11. Once all port roles have been configured, click "Save" to complete the Port Policy creation.
12. Repeat all these steps to create another Port Policy for the opposite data path for the UCS domain.

UCS Domain Profile

Now that all appropriate policies have been created, we can create our UCS Domain profile and deploy it.

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane, and click "Profiles". Next, click the "UCS Domain Profiles" tab and click the “Create UCS Domain Profile".
2. The Create UCS Domain Profile wizard appears and starts in the General tab. Select the Organization that will contain the UCS Domain profile, enter the Name of the profile (required), Tags for the profile (optional), and Description of the profile (optional). Click "Next".
3. Next, the wizard brings up the UCS Domain Assignment tab. Click the radio button for any Fabric Interconnect pair that has been claimed into Intersight, or click “Assign Later” to assign the profile after creation. Click "Next".
4. Next, the wizard brings up the VLAN & VSAN Configuration tab. The main window displays options for the VLAN and VSAN configuration policies to be selected for Fabric Interconnect A and B. Click the ‘Select Policy’ option for the appropriate configuration option (either VLAN or VSAN) for each Fabric Interconnect, and select the appropriate policy for the specific data path (A or B) of the Fabric Interconnect.
5. Once the VLAN and VSAN policies on each Fabric Interconnect have been set, click "Next".

   NOTE: In most environments, the VLAN policy will be the same for A and B data paths/FIs, but the VSAN policy will always be different for A and B data paths/FIs.
6. Next, the wizard brings up the Ports Configuration tab. The main window displays options for the Ports Configuration policies to be selected for Fabric Interconnect A and B. Click the ‘Select Policy’ button for each Fabric Interconnect, and select the appropriate Port policy for the specific data path (A or B) of the Fabric Interconnect, then click “Next”.
7. Next, the wizard brings up the UCS Domain Configuration tab. The main window displays options for the policies to be assigned to the UCS Domain. Click the ‘Select Policy’ button for each policy object, and select the appropriate policy for the UCS Domain. Only a System QOS policy is required to be set for the UCS Domain.
8. Once all of the UCS Domain management and network policies have been selected, click "Next" to complete the UCS Domain Profile creation.

NOTE: If you did not assign the UCS Domain Profile to a pair of Fabric Interconnects during the profile creation wizard, edit the policy to the FI pair now.

Policy Creation—UCS Server Profile and Template

We will now create the policies that will be consumed by our server profile templates.

Create IMC Access Policy

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for 'IMC Access' and click "Start".
2. The Create IMC Access Policy wizard appears and starts in the General tab. Select the Organization that will contain the IMC Access policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Click "Next".
3. In the Policy Details tab of the wizard, click the "UCS Server (FI-Attached)" button, enable either the In-Band or Out-of-Band configuration option, enter the VLAN ID of the network to be used for KVM Access, select IPv4 or IPv6 address configuration, and finally select the IP Pool that was created earlier for KVM Access. Click "Create" to complete the IMC Access creation.

Create IPMI Over LAN Policy

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for 'IPMI over LAN' and click "Start".
2. The Create IPMI over LAN Policy wizard appears and starts in the General tab. Select the Organization that will contain the IPMI over LAN policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Click "Next".
3. In the Policy Details tab of the wizard, click the "UCS Server (FI-Attached)" button, enable the "Enable IPMI Over LAN' option, and set the privilege level to 'admin'. Click "Create" to complete the IPMI over LAN policy creation.

Create Local User Policy

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for 'Local User' and click "Start".
2. The Create Local User Policy wizard appears and starts in the General tab. Select the Organization that will contain the Local User policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Click "Next".
3. In the Policy Details tab of the wizard, click the "UCS Server (FI-Attached)" button, set your required settings for the Password Properties options, and click "Add New User".
4. Click the '+' button next to "New User" in the lower portion of the main navigation screen. Enter the user name for the local user, select the role for the user, and enter the password for the local user, along with the password confirmation. Click "Create" to complete the Local User policy creation.

Create Virtual Media Policy

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for 'Virtual Media' and click "Start".
2. The Create Virtual Media Policy wizard appears and starts in the General tab. Select the Organization that will contain the Virtual Media policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Click "Next".
3. In the Policy Details tab of the wizard, click the "UCS Server (FI-Attached)" button, and enable the "Enable Virtual Media' option. Click "Create" to complete the Virtual Media policy creation.

Create Virtual KVM Policy

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for 'Virtual KVM' and click "Start".
2. The Create Virtual KVM Policy wizard appears and starts in the General tab. Select the Organization that will contain the Virtual KVM policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Click "Next".
3. In the Policy Details tab of the wizard, click the "UCS Server (FI-Attached)" button, and enable the "Enable Virtual KVM' option. Leave other settings at defaults. Click "Create" to complete the Virtual KVM policy creation.

Create Ethernet Adapter Policy

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for 'Ethernet Adapter' and click "Start".
2. The Create Ethernet Adapter Policy wizard appears and starts in the General tab. Select the Organization that will contain the Ethernet Adapter policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Click "Next".
3. In the Policy Details tab of the wizard, click the "UCS Server (FI-Attached)" button, and leave other settings at defaults. Click "Create" to complete the Ethernet Adapter policy creation.

Create Fiber Channel Adapter Policy

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for 'Fiber Channel Adapter' and click "Start".
2. The Create Fiber Channel Adapter Policy wizard appears and starts in the General tab. Select the Organization that will contain the Fiber Channel Adapter policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Click "Next".
3. In the Policy Details tab of the wizard, click the "UCS Server (FI-Attached)" button, and leave other settings at defaults. Click "Create" to complete the Fiber Channel Adapter policy creation.

Create Ethernet QoS Policy

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for 'Ethernet QoS' and click "Start".
2. The Create Ethernet QoS Policy wizard appears and starts in the General tab. Select the Organization that will contain the Ethernet QoS policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Click "Next".
3. In the Policy Details tab of the wizard, click the “UCS Server (FI-Attached)” button, change the “MTU, Bytes” value to ‘9216’ and leave the rest of the settings at their defaults.
4. Once all details are entered in the Policy Details section, click "Create" to complete the Ethernet QoS Policy creation.

Create Fiber Channel QoS Policy

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for Fiber Channel QoS' and click "Start".
2. The Create Fiber Channel QoS Policy wizard appears and starts in the General tab. Select the Organization that will contain the Fiber Channel QoS policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Click "Next".
3. In the Policy Details tab of the wizard, click the “UCS Server (FI-Attached)” button, and leave all settings at their defaults.
4. Once all details are entered in the Policy Details section, click "Create" to complete the Fiber Channel QoS Policy creation.

iSCSI Policies

If you are using iSCSI connectivity within your environment, the following policies must be created for the environment: iSCSI Adapter, iSCSI Boot, and iSCSI Target.

Create iSCSI Adapter Policy

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane, and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for 'iSCSI Adapter’ and click "Start".
2. The Create iSCSI Adapter Policy wizard appears and starts in the General tab. Select the Organization that will contain the iSCSI Adapter policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Click "Next".
3. In the Policy Details tab of the wizard, accept the default configurations, although the timers can be adjusted if necessary. Click "Create" to complete the iSCSI Adapter Policy creation.

Create iSCSI Static Target Policy

These steps will be followed to create all iSCSI Static Targets for iSCSI Boot from SAN. There should be a minimum of 1 static target for each data path (both A and B).

NOTE: It is recommended to create 4 Static targets to have 1 boot target for each controller of the FlashArray on each data path.

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane, and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for 'iSCSI Static Target' and click "Start".
2. The Create iSCSI Static Target Policy wizard appears and starts in the General tab. Select the Organization that will contain the iSCSI Static Target policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Click "Next".
3. In the Policy Details tab of the wizard, enter the following details:
    a. Target Name: This field is the IQN of the FlashArray (required)
    b. IP Address: This field is the IP address of the interface on the FlashArray connected to the FI on the same data path as your iSCSI vNIC
    c. Port: This field is the port number of the iSCSI target (default is ‘3260’)
    d. LUN ID: This field is the LUN ID of the volume the server profile will boot from; set this as '1'.
4. Once the iSCSI target details have been entered, click "Create" to complete the iSCSI Static Target policy creation.
5. Repeat steps 1-4 to create the additional policies for the other iSCSI Static Targets.

Create iSCSI Boot Policy

These steps will be followed to create all policies for iSCSI Boot from SAN. There should be a boot policy for each data path (both A and B).

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane, and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for 'iSCSI Boot’ and click "Start".
2. The Create iSCSI Boot Policy wizard appears and starts in the General tab. Select the Organization that will contain the iSCSI Boot policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Click "Next".
3. In the Policy Details tab of the wizard, click the “Static” button and select the primary target for the data path, select the iSCSI Adapter policy that was created earlier, and finally select the IP Pool that was created earlier for iSCSI initiators. Click "Create" to complete the iSCSI Boot Policy creation.
4. Repeat steps 1-4 to create another iSCSI Boot policy for the other data path.

Fiber Channel Policies

If you are using FC connectivity within your environment, the following policies must be created for the environment: Fiber Channel Network and FC Zone.

Create Fiber Channel Network Policy

These steps will be followed to create network policies to specify the fiber channel VSAN ID for each data path (both A and B).

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane, and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for 'Fiber Channel Network' and click "Start".
2. The Create Fiber Channel Network Policy wizard appears and starts in the General tab. Select the Organization that will contain the Fiber Channel Network policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Click "Next".
3. In the Policy Details tab of the wizard, click the “UCS Server (FI-Attached)” button and enter the VSAN ID for the data path. Click "Create" to complete the Fiber Channel Network Policy creation.
4. Repeat steps 1-4 to create another Fiber Channel Network policy for the other data path.

Create FC Zone Policy

These steps will be followed to create all FC Zones for fiber channel Boot from SAN. There should be 1 FC zone created for each data path.

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane, and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for 'FC Zone' and click "Start".
2. The Create FC Zone Policy wizard appears and starts in the General tab. Select the Organization that will contain the FC Zone policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Click "Next".
3. In the Policy Details tab of the wizard, ensure that ‘Single Initiator Single Target’ is selected, then click the “Add Target” button.
4. In the Add Target pop-up of the wizard, enter the following details:
   a. Name: This field is the name of the FC target (required)
   b. WWPN: This field is the WWPN of the interface on the FlashArray connected to the FI on the same data path as your FC port
   c. Switch ID: This field sets the Fabric Interconnect/data path for the FC zone (A or B)
   d. VSAN ID: This field is the VSAN ID for the data path
5. Repeat steps 3-4 to create any additional fiber channel targets for the data path. Click "Create" to complete the FC Zone Policy creation.
6. Repeat steps 1-5 to create another FC Zone policy for the other data path.

Create Connectivity Policies

Create LAN Connectivity Policy—FC

These steps will be followed to create the LAN connectivity for server profiles using FC storage connectivity (without iSCSI adapters).

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane, and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for 'LAN Connectivity' and click "Start".
2. The Create LAN Connectivity Policy wizard appears and starts in the General tab. Select the Organization that will contain the LAN Connectivity policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Set the Target Platform as 'UCS Server (FI-Attached)'. Click "Next".
3. In the Policy Details tab of the wizard, click on 'Pool' in the IQN section. Under the vNIC Configuration section, click 'Auto vNIC Placement'.
4. Click "Add vNIC" to create a vNIC in the LAN Connectivity policy.
5. In the Add vNIC pop-up of the wizard, enter the following details:
   a. Name: This field is the name of the vNIC (required)
   b. MAC Pool: Select the MAC pool that was created earlier
   c. Switch ID: This field sets the Fabric Interconnect/data path for the FC zone (A or B)
   d. Ethernet Network Group Policy: Select the Ethernet Network Group Policy pool that was created earlier (matching the Switch ID)
   e. Ethernet Network Control Policy: Select the Ethernet Network Group Policy pool that was created earlier
   f. Ethernet QoS Policy: Select the Ethernet QoS Policy pool that was created earlier

a. Ethernet Adapter Policy: Select the Ethernet Adapter Policy pool that was created earlier

6. Click "Add" to add the vNIC to the LAN Connectivity policy.
7. Repeat steps 4-6 to create additional vNICs for ethernet connectivity.
8. Click "Create" to complete the LAN Connectivity Policy creation.

NOTE: It is recommended to create multiple vNICs for ethernet connectivity on each data path.

Create LAN Connectivity Policy—iSCSI

These steps will be followed to create the LAN connectivity for server profiles using iSCSI storage connectivity.

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane, and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for 'LAN Connectivity' and click "Start".
2. The Create LAN Connectivity Policy wizard appears and starts in the General tab. Select the Organization that will contain the LAN Connectivity policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Set the Target Platform as 'UCS Server (FI-Attached)'. Click "Next".
3. In the Policy Details tab of the wizard, click on 'Pool' in the IQN section. Under the vNIC Configuration section, click 'Auto vNIC Placement'.
4. Click "Add vNIC" to create a vNIC in the LAN Connectivity policy.
5. In the Add vNIC pop-up of the wizard, enter the following details:
   a. Name: This field is the name of the vNIC (required)
   b. MAC Pool: Select the MAC pool that was created earlier
   c. Switch ID: This field sets the Fabric Interconnect/data path for the FC zone (A or B)
   d. Ethernet Network Group Policy: Select the Ethernet Network Group Policy that was created earlier (matching the Switch ID)
   e. Ethernet Network Control Policy: Select the Ethernet Network Group Policy that was created earlier
   f. Ethernet QoS Policy: Select the Ethernet QoS Policy that was created earlier
   g. Ethernet Adapter Policy: Select the Ethernet Adapter Policy that was created earlier
6. Click "Add" to add the vNIC to the LAN Connectivity policy.
7. Repeat steps 4-6 to create additional vNICs for ethernet connectivity.
8. Repeat steps 4-6 to create additional iSCSI vNICs for iSCSI connectivity. In the Add vNIC pop-up of the wizard, be sure to select the iSCSI Boot Policy (matching the Switch ID)
9. Click "Create" to complete the LAN Connectivity Policy creation.

NOTE: It is recommended to create multiple vNICs for both ethernet and iSCSI connectivity on each data path.

Create SAN Connectivity Policy—FC

These steps will be followed to create the SAN connectivity for server profiles using FC storage connectivity.

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane, and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for 'SAN Connectivity' and click "Start".
2. The Create SAN Connectivity Policy wizard appears and starts in the General tab. Select the Organization that will contain the SAN Connectivity policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Set the Target Platform as 'UCS Server (FI-Attached)'. Click "Next".
3. In the Policy Details tab of the wizard, click 'Auto vHBAs Placement'. Under the WWNN section, select the WWNN Pool which was created earlier.
4. Click "Add vHBA" to create a vHBA in the SAN Connectivity policy.
5. In the Add vHBA pop-up of the wizard, enter the following details:
   a. Name: This field is the name of the vHBA (required)
   b. vHBA Type: Select 'fc-initiator' as the interface type
   c. WWPN Pool: Select the WWPN pool that was created earlier
   d. Switch ID: This field sets the Fabric Interconnect/data path for the FC zone (A or B)
   e. Fiber Channel Network Policy: Select the Fiber Channel Network Policy that was created earlier (matching the Switch ID)
   f. Fiber Channel QoS Policy: Select the Fiber Channel QoS Policy that was created earlier
   g. Fiber Channel Adapter Policy: Select the Fiber Channel Adapter Policy that was created earlier
   h. FC Zone Policy: Select the FC Zone Policy that was created earlier (matching the Switch ID)
6. Click "Add" to add the vHBA to the SAN Connectivity policy.
7. Repeat steps 4-6 to create additional vHBAs for fiber channel connectivity.
8. Click "Create" to complete the SAN Connectivity Policy creation.

NOTE: It is recommended to create multiple vHBAs for fiber channel connectivity on each data path.

Create Boot Order Policies

Create Boot Order Policy—FC

These steps will be followed to create the boot order configuration for server profiles using FC Boot from SAN.

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane, and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for 'Boot Order' and click "Start".
2. The Create Boot Order Policy wizard appears and starts in the General tab. Select the Organization that will contain the Boot Order policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Click "Next".
3. In the Policy Details tab of the wizard, click the "UCS Server (FI-Attached)" button and select the boot mode for the policy.
4. Click the dropdown arrow next to the "Add Boot Device" and select SAN Boot. Repeat this step to add 4 SAN boot devices in total.
5. Click the dropdown arrow next to the "Add Boot Device" and select Virtual Media.
6. In the Virtual Media boot device, enter the device name for the boot device and set the sub-type as 'KVM MAPPED DVD'
7. In the first SAN boot device, enter the following details:
    a. Device Name: This field is the name of the boot device (required)
    b. LUN: This field is the LUN ID of the volume the server profile will boot from; set this as '1'.
    c. Interface Name: This field is the name of the vHBA to be used for connecting to the boot device (required)
    d. Target WWPN: This field is the WWPN of the interface on the FlashArray connected to the FI on the same data path as your FC port
8. Repeat step 7 to set the details for the next SAN boot devices using the same vHBA for the first Switch ID/data path targeting the next WWPN on the FlashArray.
9. Repeat step 7 to set the details for the remaining SAN boot devices using the same vHBA for the second Switch ID/data path targeting the appropriate WWPNs on the FlashArray.
10. Click "Create" to complete the Boot Order Policy creation.

NOTE: It is recommended to create 4 SAN Boot devices to have 1 boot target for each controller of the FlashArray on each data path.

Create Boot Order Policy—iSCSI

These steps will be followed to create the boot order configuration for server profiles using iSCSI Boot from SAN.

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane, and click "Policies". Next, click the "Create Policy" button in the main tab, click the radio button for ‘Boot Order’ and click "Start".
2. The Create Boot Order Policy wizard appears and starts in the General tab. Select the Organization that will contain the Boot Order policy, enter the Name of the policy (required), Tags for the policy (optional), and Description of the policy (optional). Click "Next".
3. In the Policy Details tab of the wizard, click the “UCS Server (FI-Attached)” button and select the boot mode for the policy.
4. Click the dropdown arrow next to the “Add Boot Device” and select iSCSI Boot. Repeat this step to add another iSCSI boot device.
5. Click the dropdown arrow next to the “Add Boot Device” and select Virtual Media.
6. In the Virtual Media boot device, enter the device name for the boot device and set the sub-type as ‘KVM MAPPED DVD’
7. In the first iSCSI boot device, enter the following details:
   a. Device Name: This field is the name of the boot device (required)
   b. Interface Name: This field is the name of the iSCSI to be used for connecting to the boot device (required)
8. Repeat step 7 to set the details for the remaining iSCSI boot device using the iSCSI vNIC for the second Switch ID/data path targeting the FlashArray.
9. Click "Create" to complete the Boot Order Policy creation.

NOTE: It is recommended to create 2 iSCSI Boot devices to have 1 boot target on each data path.

UCS Server Profile Templates

These steps will cover all configuration options for server profile templates which can provide iSCSI and/or fiber channel connectivity, if all of the prerequisite policies have been created.

1. In Intersight, go to the Infrastructure Service page, click to expand the Configure menu tab in the left navigation pane, and click "Templates” and click the “Create UCS Server Profile Template".
2. The Create UCS Server Profile Template wizard appears and starts in the General tab. Select the Organization that will contain the UCS Server Profile Template, enter the Name of the template (required), Tags for the template (optional), and Description of the template (optional). Set the Target Platform as ‘UCS Server (FI-Attached)’ and click "Next".
3. Next, the wizard brings up the Compute Configuration tab. Select the UUID pool then select the BIOS and Boot Order policies that were previously created, based on if the Boot from SAN will use FC or iSCSI storage. Click "Next".
4. Next, the wizard brings up the Management Configuration tab. Select the policies created earlier for IMC Access, Local User, and Virtual KVM, then click "Next".
5. Next, the wizard brings up the Storage Configuration tab. Do not select any policies on this tab, then click “Next”.
6. Next, the wizard brings up the Network Configuration tab. If you will be using iSCSI, set the policy for LAN connectivity to the policy created for iSCSI access. If you will be using FC, set the policy for SAN connectivity to the policy created for FC access. Click “Next”.
7. Review the policies chosen for all configuration tabs to ensure they are correct for your usage. Once you have checked the policy configuration, click “Derive Profiles” to clone server profiles from the template now, or click "Close" to complete the UCS Server Profile Template creation without creating server profiles.

Deployment of VMware vSphere

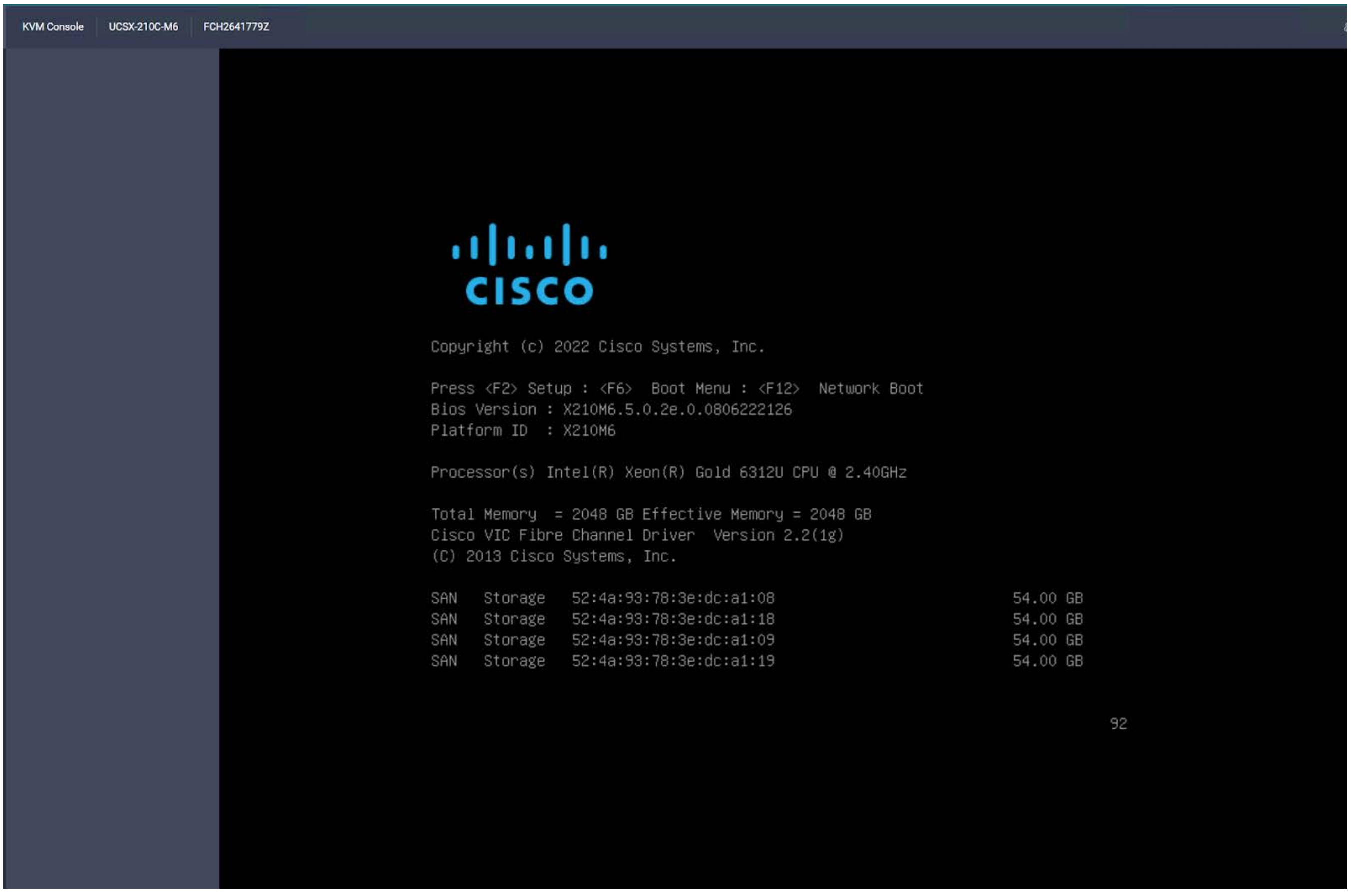
Once the above configuration sections have been completed, we can create Server Profiles from the newly created IMM Server Profile templates. After the Server Profiles have been created and associated with servers, the creation of hosts, host groups (if necessary), and volumes will need to be completed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

The steps for the creation of Server Profiles from the 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 Server Profiles, we will see similar connections at server boot, and within the Pure Storage FlashArray connection details.

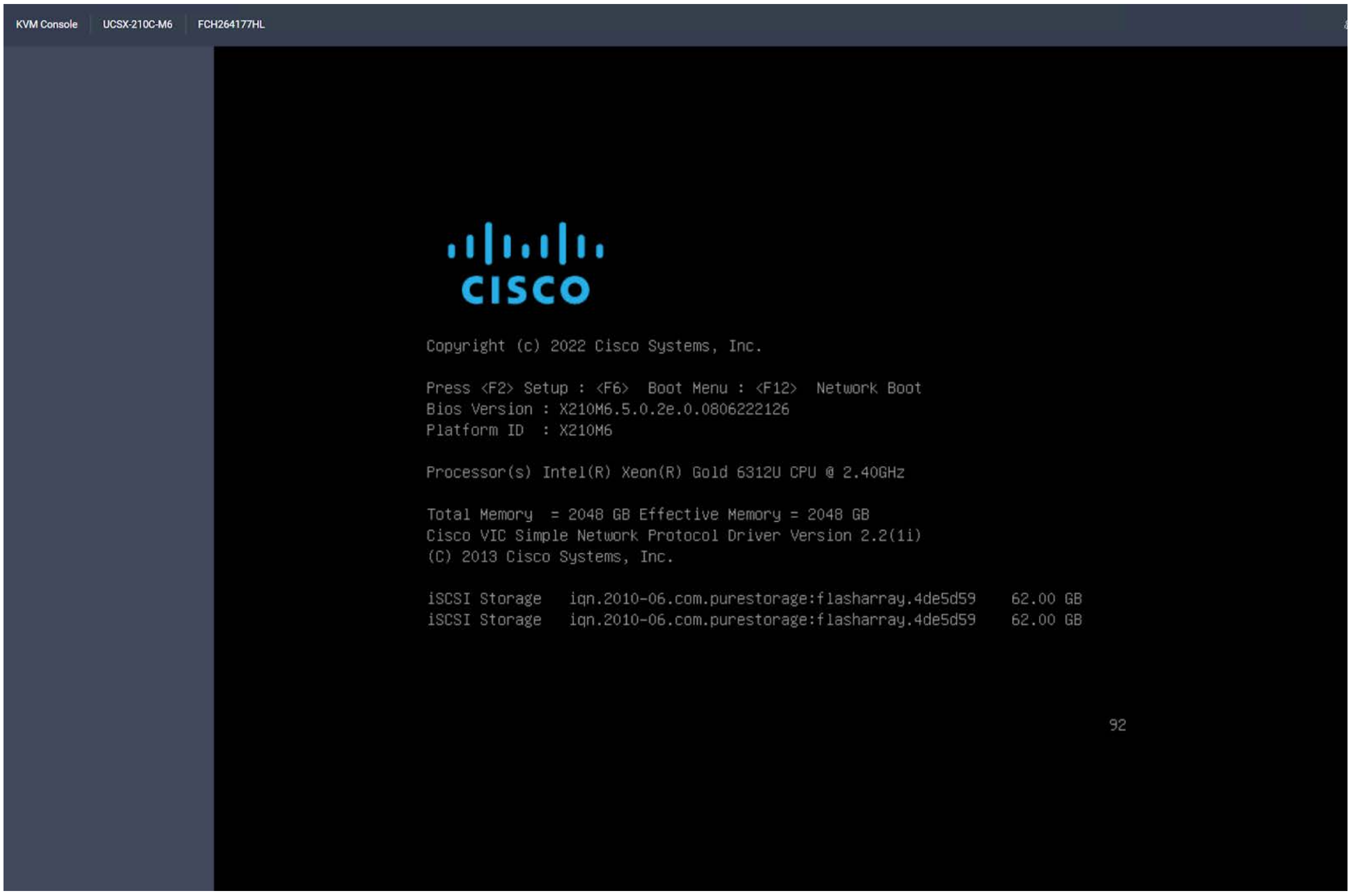
When we boot our Server Profile configured for Fiber Channel Boot from SAN, we can see the storage connection after the VIC has loaded the driver and scanned the vHBA:



```
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 2 View of connected storage during boot of Server Profile configured for Fiber Channel Boot from SAN

When we boot our Server 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:

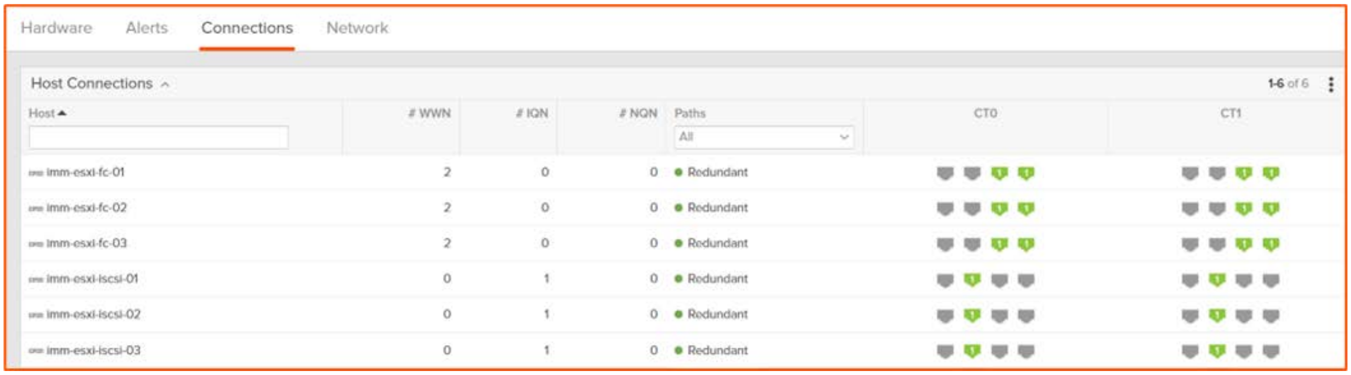


```
Copyright (c) 2022 Cisco Systems, Inc.

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 3 View of connected storage during boot of Server Profile configured for iSCSI Boot from SAN

FlashArray Host Connectivity

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



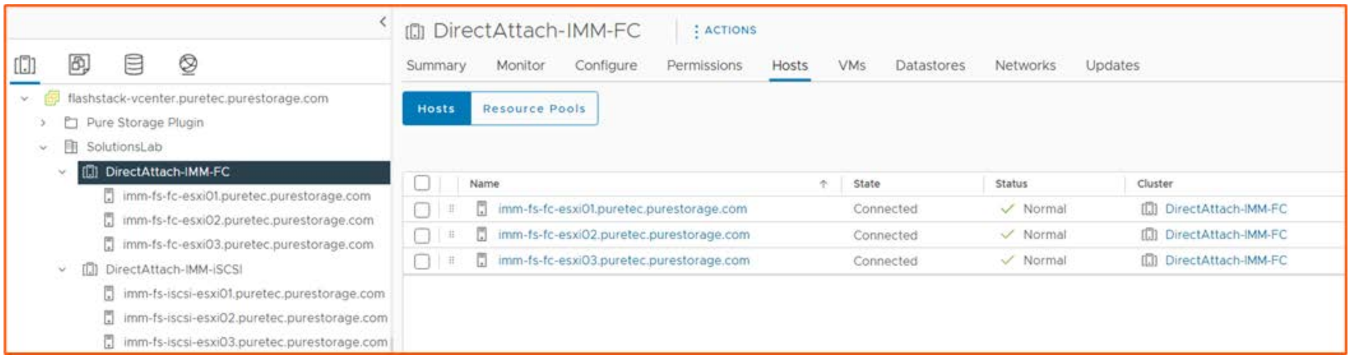
Host ▲	# WWN	# IQN	# NQN	Paths	CT0	CT1
imm-esxi-fc-01	2	0	0	● Redundant	■ ■ 🟩 🟩	■ ■ 🟩 🟩
imm-esxi-fc-02	2	0	0	● Redundant	■ ■ 🟩 🟩	■ ■ 🟩 🟩
imm-esxi-fc-03	2	0	0	● Redundant	■ ■ 🟩 🟩	■ ■ 🟩 🟩
imm-esxi-iscsi-01	0	1	0	● Redundant	■ 🟩 ■ ■	■ 🟩 ■ ■
imm-esxi-iscsi-02	0	1	0	● Redundant	■ 🟩 ■ ■	■ 🟩 ■ ■
imm-esxi-iscsi-03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

FIGURE 4 View of host connections within FlashArray for FC & iSCSI Boot from SAN service profiles

vSphere Host Connectivity

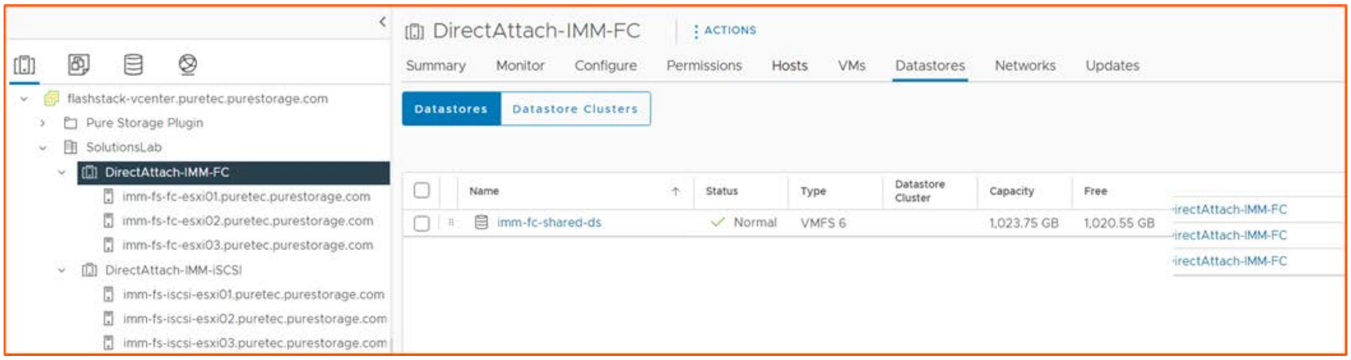
To demonstrate host and storage connectivity, after the hosts were booted successfully, vSphere ESXi is installed. Clusters are then configured with a FlashArray host group for the FC and iSCSI service profiles, and each cluster is mapped to a shared volume used as a VMFS datastore.

Fiber Channel Cluster Hosts & Datastore


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

□	Name ↑	State	Status	Cluster
□	imm-fs-fc-esxi01.puretec.purestorage.com	Connected	✓ Normal	DirectAttach-IMM-FC
□	imm-fs-fc-esxi02.puretec.purestorage.com	Connected	✓ Normal	DirectAttach-IMM-FC
□	imm-fs-fc-esxi03.puretec.purestorage.com	Connected	✓ Normal	DirectAttach-IMM-FC

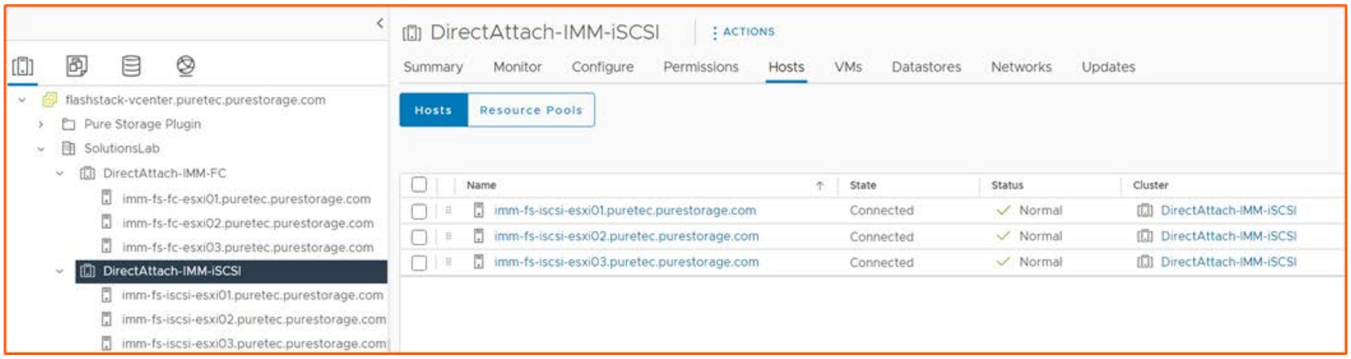
FIGURE 5 View of hosts within vSphere cluster for Fiber Channel service profiles


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

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

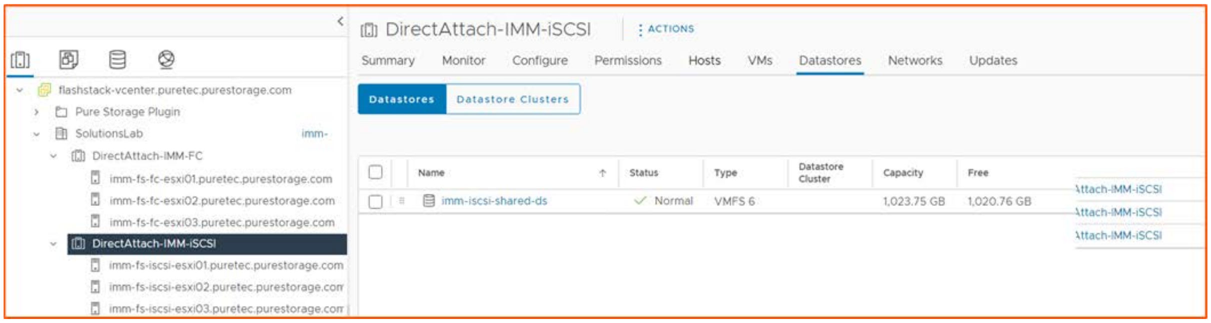
FIGURE 6 View of datastore within vSphere cluster for Fiber Channel service profiles

iSCSI Cluster Hosts & Datastore


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

Name	State	Status	Cluster
imm-fs-iscsi-esxi01.puretec.purestorage.com	Connected	✓ Normal	DirectAttach-IMM-iSCSI
imm-fs-iscsi-esxi02.puretec.purestorage.com	Connected	✓ Normal	DirectAttach-IMM-iSCSI
imm-fs-iscsi-esxi03.puretec.purestorage.com	Connected	✓ Normal	DirectAttach-IMM-iSCSI

FIGURE 7 View of hosts within vSphere cluster for iSCSI service profiles


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

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

FIGURE 8 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.