WHITE PAPER

FlashArray Direct-attach Connectivity for Cisco UCS X-Series

Deployment Guide for Cisco UCS X-Series with Intersight Managed Mode and UCS Manager

Contents

Introduction

This white paper presents a streamlined architecture for deploying Pure Storage® FlashArray™ directly with Cisco UCS Fabric Interconnects, enabling efficient file services—such as Network File System (NFS) and Server Message Block (SMB)—within a Unified Computing System (UCS) compute environment.

By eliminating the need for intermediary network switches, this direct-attach model reduces infrastructure complexity, lowers power and rack footprint, and accelerates deployment time. It provides an ideal foundation for private cloud environments that demand consolidated file services with simplified management and strong performance.

The solution supports both Intersight Managed Mode (IMM) and UCS Manager (UCSM), offering operational flexibility to suit various enterprise management strategies. While this model simplifies deployment and management within a single UCS domain, it's important to note that FlashArray File Services connectivity is inherently confined to that domain—unlike traditional designs with external switches that enable shared storage across multiple UCS domains.

This white paper outlines the implementation details of this topology and highlights considerations for planning and deploying a direct-attach configuration within your UCS environment.

Considerations for Running in Direct-attach Mode

The implementation operates a FlashStack® environment in a direct-attach configuration to validate NFS and SMB protocols on the Pure Storage FlashArray. This setup eliminates the need for intermediate Cisco Nexus switches, providing a simplified and cost-effective alternative for connecting compute and high-performance file storage.

The Pure Storage FlashArray delivers consistent high availability, operational simplicity, and exceptional throughput for data-intensive, file-based applications such as centralized user shares, application data repositories, and home directories.

Design Considerations

In Cisco UCSM direct-attach environments, network policies and port configurations are centrally managed via Fabric Interconnects. Direct FlashArray connectivity, without top-of-rack (ToR) switches, introduces a critical design consideration: **scalability and resource sharing across UCS domains**.

- **Single UCS domain confinement**: A direct-attached FlashArray is limited to providing storage services within a single UCS domain. Its resources cannot be directly shared with servers in separate UCS domains.
- **Scalability trade-off**: While simplifying single-domain networking, this design restricts broader sharing. Multi-domain resource sharing typically requires external ToR switches (for example, Cisco Nexus) for a common network fabric.

When considering a direct-attached FlashArray for file services, it is important to assess current and future multi-UCS domain sharing requirements. For FlashArray File Services (NFS and SMB), the trade-offs are generally manageable. Adhering to validated design practices—including proper port channeling, Link Aggregation Control Protocol (LACP), virtual local-area network (VLAN) tagging, and interface-to-workload mapping—allows effective monitoring and maintenance. UCS command-line interface (CLI) tools and FlashArray real-time metrics provide sufficient operational insight for robust performance, offering a balanced trade-off between architectural simplicity and operational control.

Ethernet Port Configuration and Topology Constraints

In a direct-attach model, Ethernet ports on UCS Fabric Interconnects must be explicitly configured as appliance ports to connect with the FlashArray. Unlike traditional Nexus-based topologies, port channeling is supported but requires precise LACP configuration and policy alignment between the Fabric Interconnects and FlashArray.

- VLANs must be manually defined at both ends (UCS Fabric Interconnects and FlashArray) to ensure proper network segmentation and traffic isolation for NFS and SMB services.
- While removing external switching reduces complexity, it also reduces flexibility—especially when scaling or adding more uplinks or arrays.

Connectivity Diagram

Figure 1 shows the physical connections between the FlashArray and Cisco UCS Fabric Interconnects in the reference architecture.

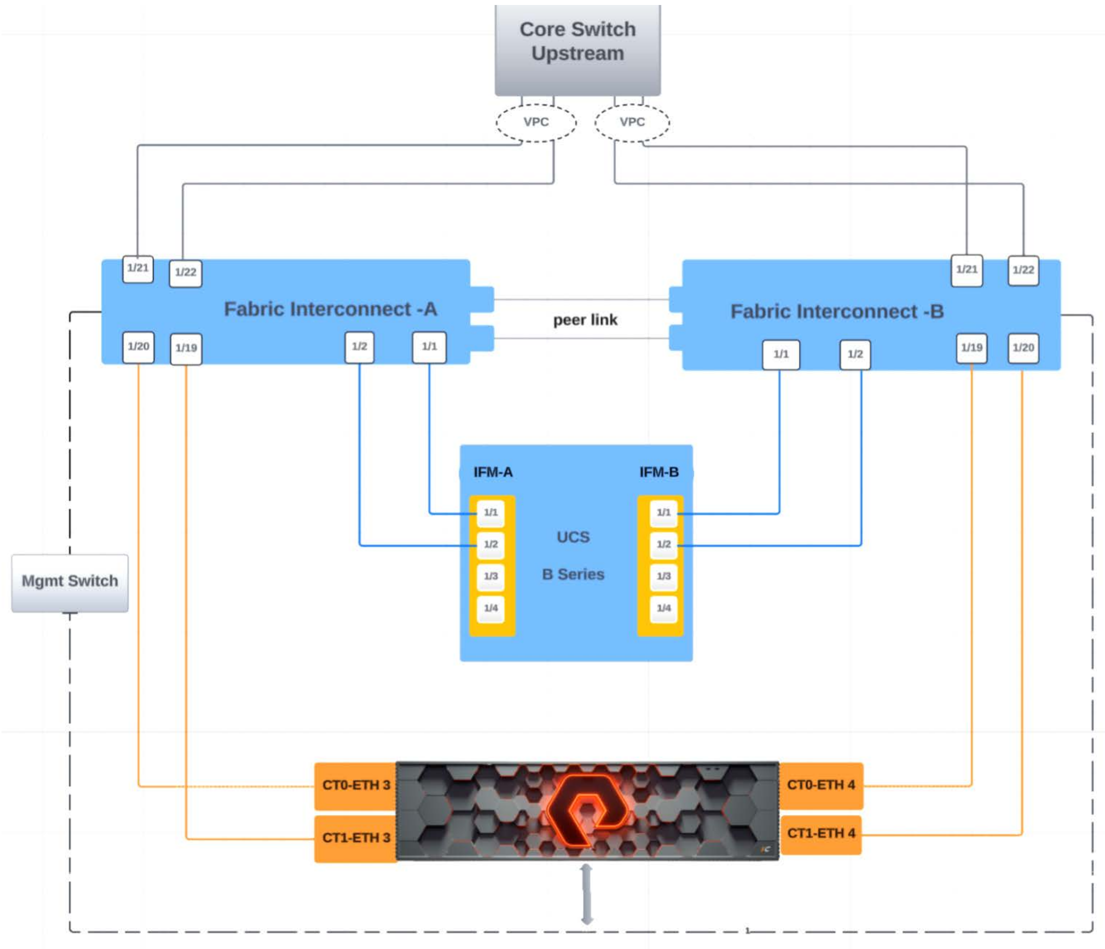

FIGURE 1 Diagram of physical connections between FlashArray and Cisco UCS Fabric Interconnects

Infrastructure Components

Table 1 lists the components used to build the configuration of a direct-attached FlashStack.

Infrastructure Component	Model	Version
Storage	FlashArray//X™, FlashArray//XL™, FlashArray//C™, FlashArray//E™	Purity//FA 6.6.0 or later
Fabric Interconnects	Cisco UCS 6536	-
Compute Chassis	Cisco UCS X9508	-
Intelligent Fabric Module (IFM)	Cisco UCS 9108 IFM	-
Compute Nodes	Cisco UCS X210c, X410c, X215c	M6 or later
Linux Operating System	Bare metal	-
Windows Operating System	Bare metal	-

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

Configuration Guide: Pure Storage FlashArray

In high-performance storage environments, multiple network paths are critical to maximizing throughput, availability, and fault tolerance. When connecting the Pure Storage FlashArray to upstream network components—such as Cisco UCS Fabric Interconnects (FI-A and FI-B)—via multiple physical links, it's essential to logically aggregate these links to ensure optimal performance and reliability. Technologies such as link aggregation groups (LAGs) and LACP play a key role in achieving these objectives.

This network topology is designed to deliver high availability, redundant data paths, and enhanced aggregate bandwidth for FlashArray File Services (NFS and SMB). By leveraging dual Fabric Interconnects and properly configured LAGs with LACP, the architecture minimizes single points of failure and ensures consistent performance under varying workloads.

Figure 2 outlines the key infrastructure components in a direct-attached FlashArray deployment, highlighting their roles in enabling resilient client access, load balancing, and operational efficiency across file storage services.

Component	Description
FI-A / FI-B	Fabric Interconnects A and B serve as top-of-rack switches or upstream network aggregation points in UCS-managed environments.
LAG1 / LAG2	Link Aggregation Groups that logically combine multiple physical Ethernet connections into a single interface, enhancing both redundancy and throughput.
ct0.eth4/eth5 ct1.eth4/eth5	Physical Ethernet interfaces on the FlashArray controllers. ct0 and ct1 represent the primary and secondary controllers, respectively. These ports establish uplinks to the fabric.
lacp0 / lacp1	Link Aggregation Control Protocol instances corresponding to LAG1 and LAG2. LACP automatically negotiates, monitors, and maintains the health of the aggregated links.
Virtual Interface (VIP)	A floating IP/interface used by FlashArray File Services to provide uninterrupted client connectivity. Enables automatic failover between controllers.
Primary / Secondary Controllers	Active/Standby controller architecture. The primary controller handles client traffic during normal operation, while the secondary seamlessly takes over in failure scenarios.
FA File Services	The file services layer on FlashArray supporting NFS and SMB protocols. Designed for resilient, high-performance file sharing across enterprise workloads.

FIGURE 2 Key infrastructure components in a direct-attached FlashArray deployment

To deliver high availability, scalability, and performance for NFS and SMB file services, the FlashArray is deployed in direct-attach mode with Cisco UCS Fabric Interconnects (Figure 3). The following subsections outline the critical networking elements and architecture that enable this solution.

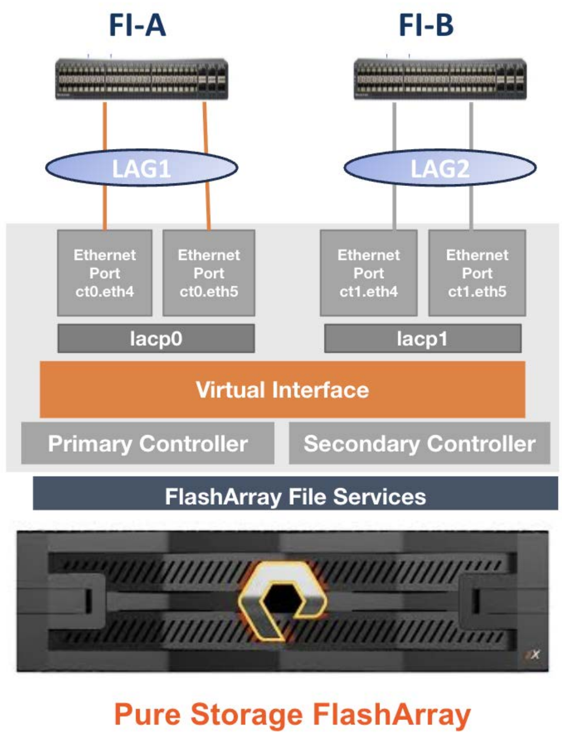

FIGURE 3 FlashArray deployment with Cisco UCS Fabric Interconnects

Physical Port Connectivity

The Pure Storage FlashArray is designed with dual controllers to ensure uninterrupted service:

- **ct0 (primary controller)**: connected to Fabric Interconnect A (FI-A) via ct0.eth5 and ct0.eth4
- **ct1 (secondary controller)**: connected to Fabric Interconnect B (FI-B) via ct1.eth5 and ct1.eth4

Link Aggregation Groups

To optimize link usage and ensure failover protection, LAGs are implemented:

- **LAG1:** combines ct0.eth4 and ct0.eth5, connected to FI-A
- **LAG2**: combines ct1.eth4 and ct1.eth5, connected to FI-B

LAGs provide the following benefits:

- **Redundancy**: maintains connectivity if a physical link fails
- **Increased bandwidth**: allows load distribution across multiple active links

Enabling Link Aggregation Control Protocol

To simplify and strengthen the LAG configuration, LACP is enabled:

- **lacp0**: manages LAG1 (ct0 to FI-A)
- **lacp1**: manages LAG2 (ct1 to FI-B)

LACP provides the following benefits:

- Automates negotiation of link bundling
- Ensures only healthy and active links participate in data forwarding
- Reduces administrative complexity

Virtual Interface Abstraction

A **virtual interface** sits above the physical and aggregated interfaces, abstracting controller-level details from clients.

Key functions include:

- **Client-facing endpoint**: NFS and SMB traffic targets the virtual IP (VIP)
- **Failover capability**: in a controller failure, the VIP is automatically reassigned to the secondary controller

Active/Standby Controller Model

FlashArray File Services operates on an **active/standby architecture:**

- **Active controller (primary):** handles all active file service traffic
- **Standby controller (secondary):** takes over upon active node failure

Failover is automatic and seamless, preserving both availability and performance.

Pure Storage FlashArray Network Configuration Details

This section outlines the configuration of Pure Storage FlashArray network connectivity to support high-performance file data services.

Use Case: File Services over Direct-attached Ethernet (NFS/SMB)

The Pure Storage FlashArray is deployed in a direct-attach topology using high-throughput Ethernet links to Cisco UCS Fabric Interconnects (FI-A and FI-B). This configuration is optimized for enterprise-grade NFS and SMB workloads, offering:

- High availability through dual-path connectivity
- Enhanced bandwidth using LAGs
- Seamless client access via a virtual interface

The following subsection details the physical port layout, LAG/LACP setup, and interface abstraction required for reliable and scalable file services deployment with FlashArray.

Port Configuration: Ethernet and Virtual Interfaces

Each of the physical Ethernet ports on the Pure Storage FlashArray should be enabled so that the ports are ready for connectivity once the appropriate configuration is set on the UCS Fabric Interconnects.

For direct connectivity from the FlashArray to the UCS Fabric Interconnects, 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 subinterfaces 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 FlashArray Network Settings page (**Settings > Network**).
2. Click the **+** icon in the Subnets area.
3. In the Create Subnet pop-up window that appears, enter the following details:
   - **Name**: the name of the subnet used within the FlashArray; it is recommended to include the data path (A or B)
   - **Enabled**: set by default and should remain enabled
   - **Prefix**: the prefix for the network subnet in Classless Inter-Domain Routing (CIDR) notation, which defaults to **/24**
   - **VLAN**: tags the VLAN to be used on the subinterface attached to this subnet; this ID will match the details we have defined for our environment
   - **Gateway**: the gateway for your network subnet; not required in our direct-attach configuration
   - **MTU**: sets the MTU to be used by the subinterfaces that inherit this setting from the subnet; the general recommendation is to use the standard MTU of **9000**

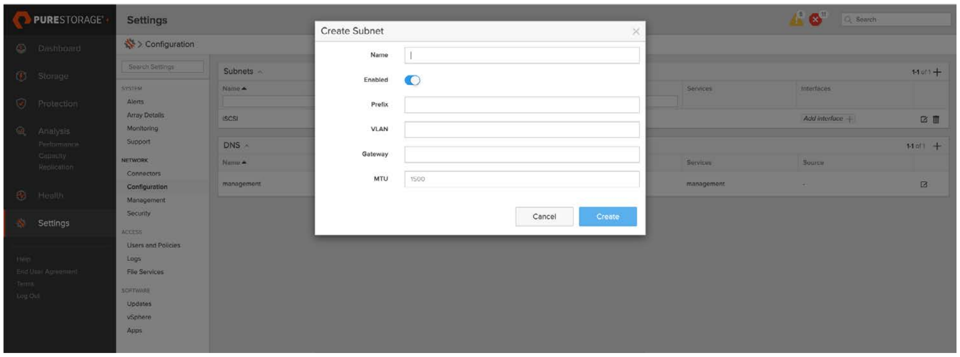

FIGURE 4 Create subnet

4. Click **Create** to finish the creation of a subnet for the FlashArray.
5. Repeat steps 1–4 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 window that appears, click the **Name** drop-down menu and select the physical Ethernet interface that is directly connected to the UCS Fabric Interconnects for the data path of the subnet.

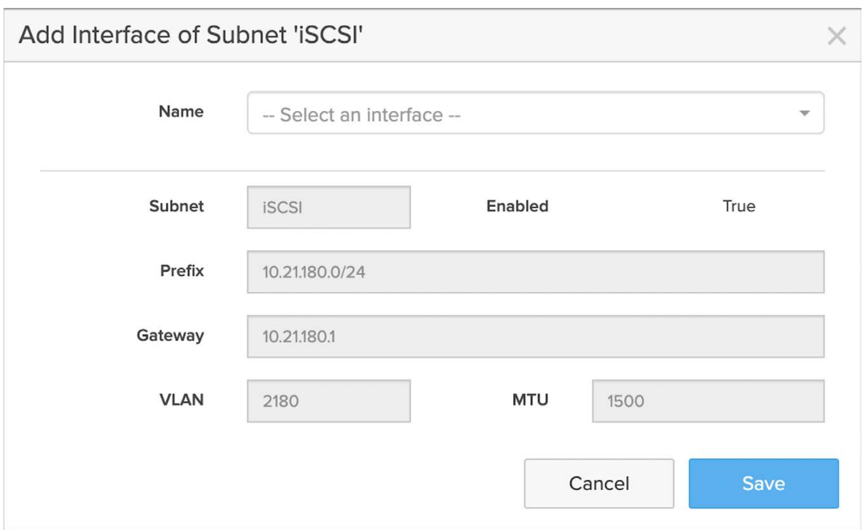

FIGURE 5 Add interface of subnet

NOTE: The interfaces in the drop-down menu are listed with the following name format: ct#:eth#:#### (controller #, physical interface #, and subnet VLAN ID, respectively).

8. Once the correct subinterface 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 subinterfaces, connected to two separate physical interfaces, are configured to provide redundant connectivity from the FlashArray to the UCS Fabric Interconnects.

Configuration Guide: Cisco Intersight Managed Mode

To enable direct-attach connectivity between Cisco UCS Fabric Interconnects and the Pure Storage FlashArray in IMM, specific configurations must be performed to correctly classify the ports and ensure efficient and reliable data access.

1. **Log in to Cisco Intersight console:** Access the Cisco Intersight console using your credentials. Ensure you have the appropriate permissions to configure policies and manage Fabric Interconnects.
2. **Navigate to the Policies section:** In the left-hand navigation panel, go to **Policies > Create Policy**. Here, you'll define the connectivity behavior for the Fabric Interconnects.

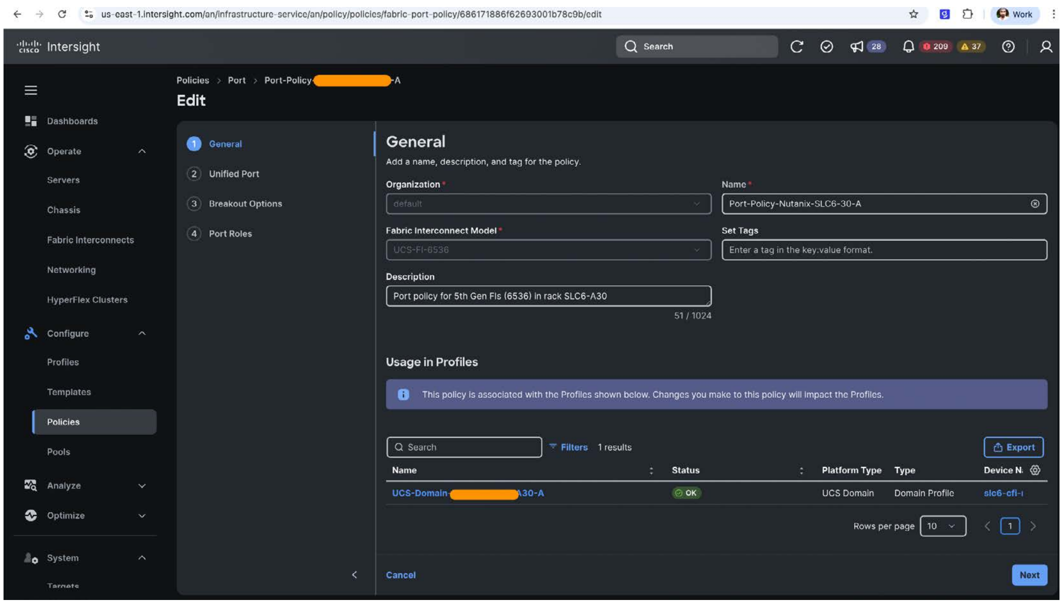

FIGURE 6 Navigate to Policies section of Cisco Intersight console

3. **Create or edit a port policy:** Under the Port Policies section, either create a new port policy or edit an existing one that is associated with your UCS domain profile. This policy will define the role and configuration of each port on the Fabric Interconnect.
4. **Configure appliance ports on the Fabric Interconnect:** Within the port policy, locate the ports on the Fabric Interconnects (typically on the uplink side) that you intend to use for connecting directly to the FlashArray. These ports must be configured as appliance ports. To do this, select one of the relevant ports, right-click on it, and choose **Configure as Appliance Port**. Repeat for each port.

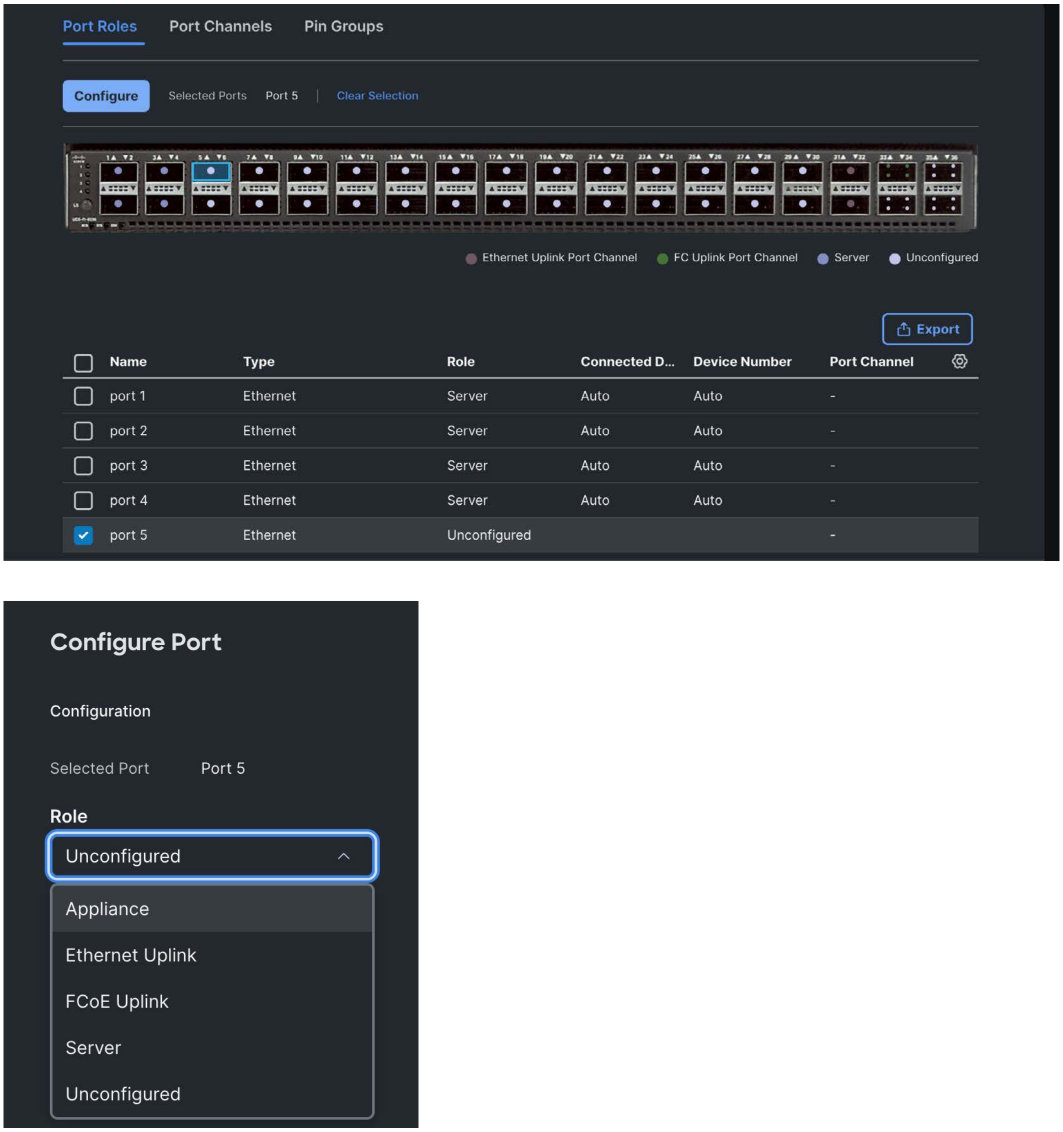

FIGURE 7 Configure appliance ports of Fabric Interconnect

Configuration Guide: Cisco UCS Manager

Because this white paper focuses on running FlashStack in direct-attach mode, there are some portions of the configuration of a UCSM environment that are not covered (see Cisco Validated Designs and UCS documentation for additional configuration details).

The UCSM configuration policies not covered in this white paper are listed in Table 2, broken down by UCSM navigation tabs.

Configuration Tab	Policies Not Covered in this Guide
Admin	Fault policies, user management, key management, communication management
Equipment	Firmware management, equipment policies
Server	Various policies—adapter, BIOS, host firmware, IPMI/Redfish access, KVM management, maintenance, power control, Serial over LAN, Server Pool, iSCSI authentication, vMedia
LAN	Various policies—dynamic vNIC connection, LACP, Multicast, QoS, VMQ connection
Storage	Storage policy
Chassis	Chassis maintenance policy

TABLE 2 All configuration policies not covered in this white paper, listed by UCSM tab

UCS Storage Port 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 UCS Fabric Interconnects. The following steps walk through configuring the server, network uplink, and storage appliance ports.

For the configuration of Fabric Interconnects, Figure 8 shows how the filtered view of the Fabric Interconnects under the Equipment tab will appear.

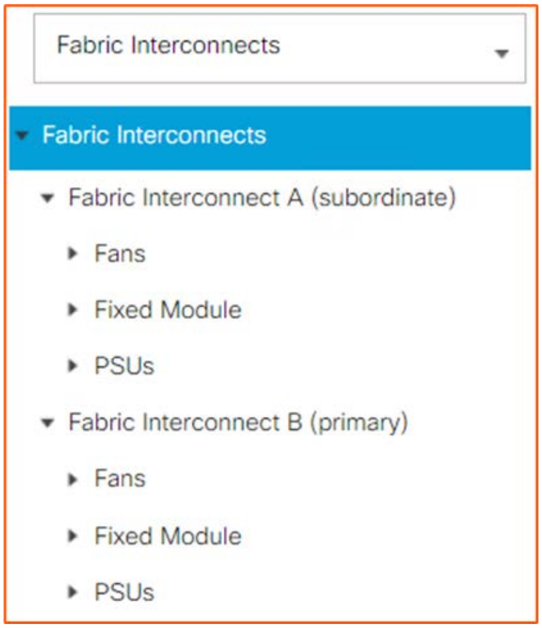

FIGURE 8 Filtering the view to Fabric Interconnects within the Equipment tab

First, the ports on the Fabric Interconnects need to be assigned as appliance ports. Select a port that needs to be assigned, right-click on it (**Port 33** is selected in Figure 9), and choose **Configure as Appliance Port**. Repeat for the remaining ports.

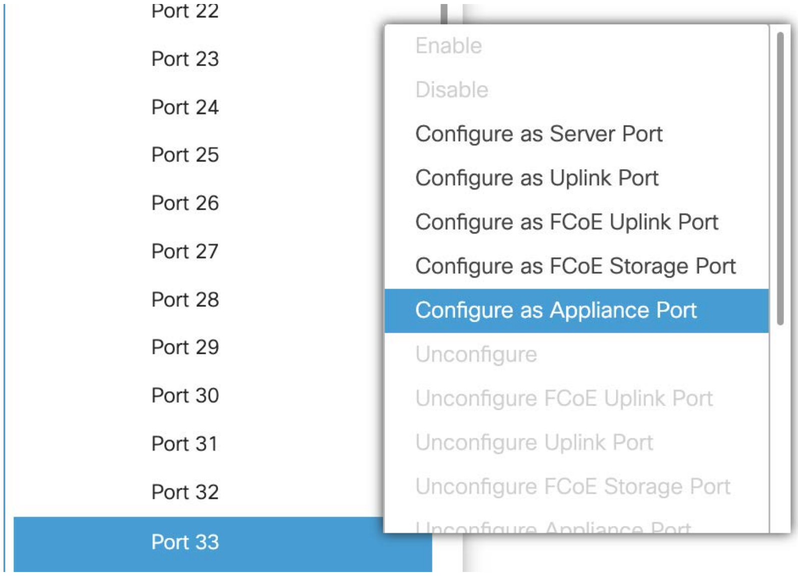

FIGURE 9 Configure ports as appliance ports

Unlike a server port, the appliance port requires some additional configuration. Appliance ports use their own special appliances VLAN cloud, which is separate from the standard LAN cloud. You can either make the clouds as you configure the ports or prepare them ahead of time.

Create individual port channel for each FI in Cisco UCS

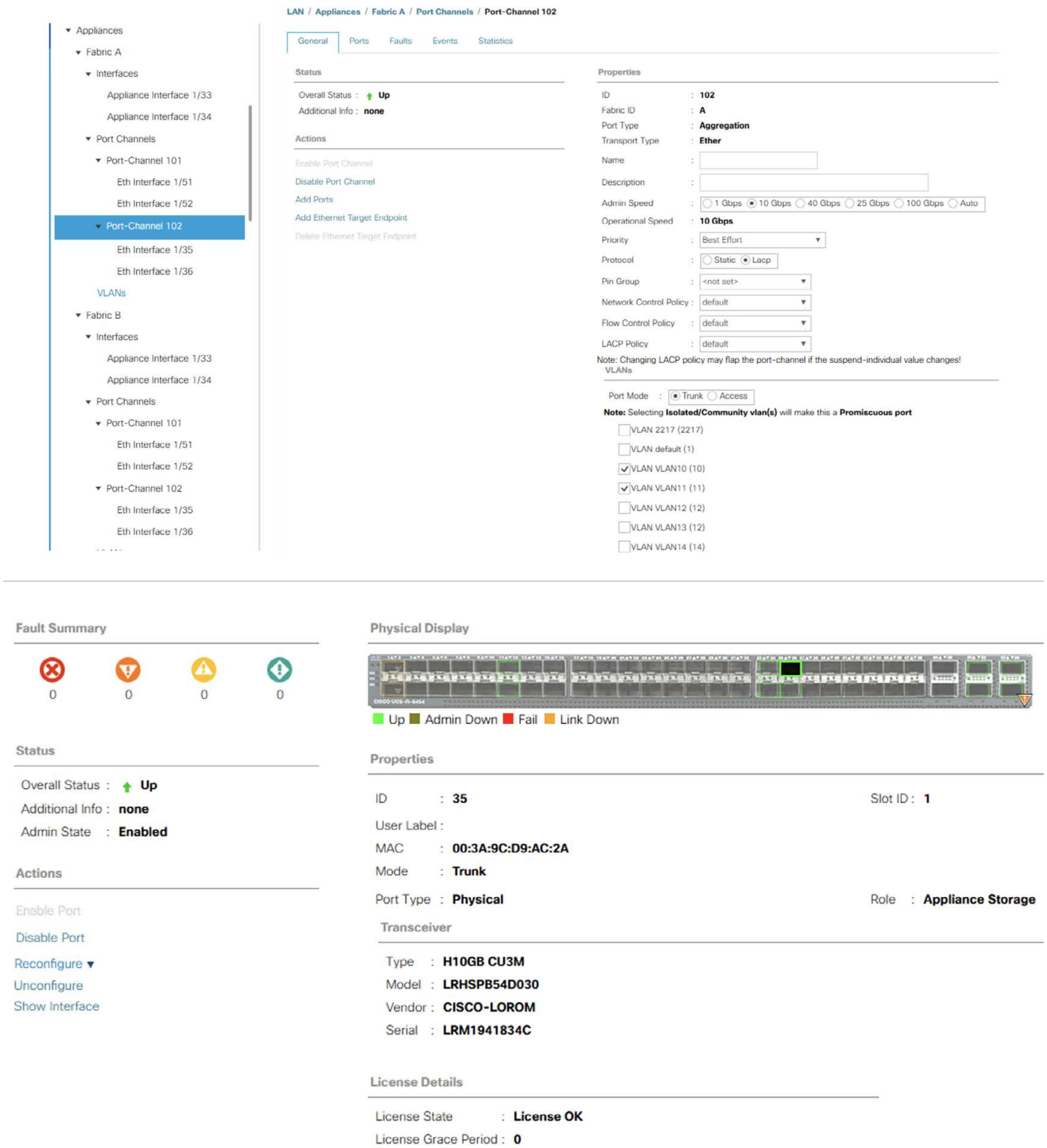

FIGURE 10 Create appliances VLAN cloud

Assigning VLANs for FlashArray Storage Traffic on Cisco UCS

1. Log in to UCS Manager.
2. Open the UCS Manager graphical user interface (GUI)—typically via the cluster IP of the Fabric Interconnects.
3. Create VLANs for different storage protocols:
   - Navigate to **LAN > VLANs**.
   - Create separate VLANs for each FlashArray protocol (for example, VLAN 100 – NFS, VLAN 101 – SMB)
   - Ensure that these VLANs are non-native and not configured as default VLANs.
4. Assign VLANs to the appliance port:
   - Navigate to **LAN > Appliances**.
   - Locate the previously configured appliance port (for example, Eth1/10, Eth1/11).
   - Select the appliance port.
   - In the VLANs tab, click **Add VLAN**.
   - Associate VLAN 100, 101, and 102 to the selected port.
   - Set the native VLAN correctly if needed for fallback traffic.

Note: Appliance ports bypass UCS server management and are intended for external systems (for example, network-attached storage or S3 storage). These ports do not participate in UCS pinning or server vNIC policies.

Enable Jumbo Frames for Performance (Optional)

1. Navigate to **LAN > Policies > MTU Policies**.
2. Create a new MTU policy (for example, JumboFrames-9000).
3. Set **MTU size** to **9000 bytes**.
4. Apply the MTU policy to the VLANs.
5. Navigate back to **LAN > VLANs**.
6. For each VLAN (100, 101, 102), edit the VLAN configuration. Under MTU Policy, select and apply **JumboFrames-9000**.

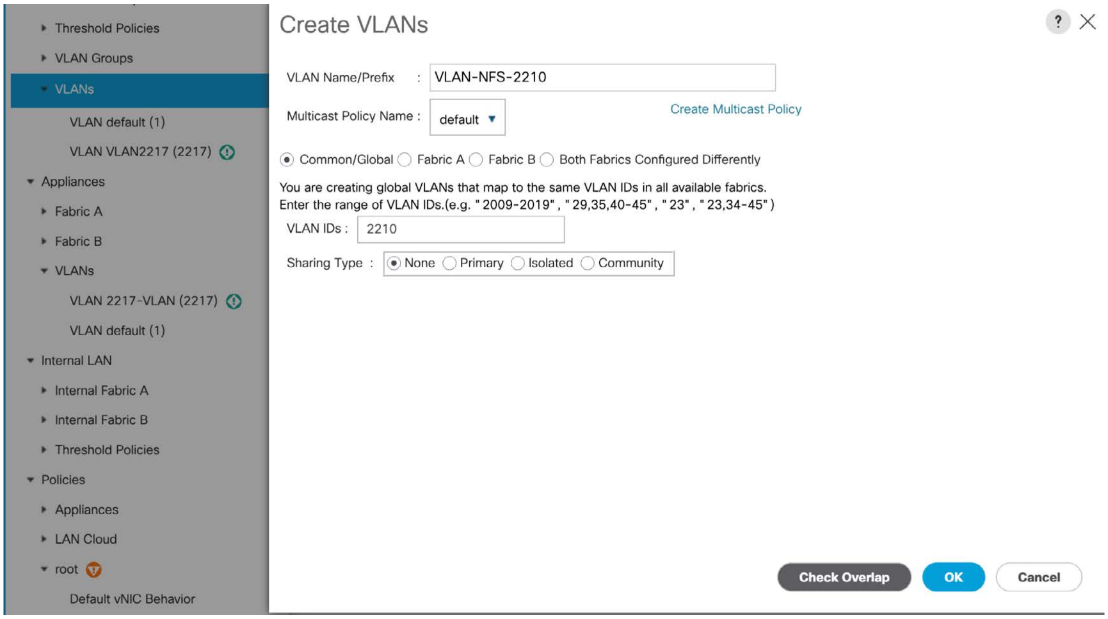

FIGURE 11 Enable jumbo frames (optional)

Appliance Interface Configuration: Ethernet

The same steps used previously will be followed to create an appliance interface that will allow for direct-attach connectivity between the FlashArray and UCS Fabric Interconnects.

1. **Navigate to the Equipment section:** In the Cisco UCS Manager, click the **Equipment** tab in the left navigation pane.
2. **Filter to Fabric Interconnects**: Select the **Fabric Interconnects** filter at the top of the navigation pane to view only the Fabric Interconnects configuration.
3. **Locate Ethernet ports**: Once Fabric A and Fabric B are visible, expand either one to see the fixed module. Then, expand the fixed module to view the Ethernet ports.
4. **Configure appliance port**: With **Ethernet Ports** selected, locate the required port number for your environment. Right-click on the desired port and click **Configure as Appliance Port**.
5. **Confirm appliance port selection:** In the Configure as Appliance Port notification, ensure the correct port number is shown. Click **Yes** to proceed.
6. **Enter appliance port configuration details**: In the pop-up window, enter the following:
   - **Priority**: Select **Platinum** (QoS priority).
   - **Pin Group**: Leave as **<not set>**.
   - **Network Control Policy**: Select the policy created earlier (for Cisco Discovery Protocol/Link Layer Discovery Protocol).
   - **Flow Control Policy**: Leave as **default**.
   - **Admin Speed (Gbps)**: Set to match your physical interface and transceiver specifications.
   - **VLANs**:
     - Set port mode to **Trunk**.
     - Select VLANs, including the dummy trunk native VLAN. The iSCSI VLAN is defined for your environment.
   - **Native VLAN**: Set to the dummy trunk native VLAN.
   - **Ethernet Target Endpoint**: Enter the name and MAC address of the FlashArray interface this UCS Fabric Interconnect port connects to.
7. **Repeat steps for all required ports**: Repeat steps 4–6 for all necessary physical interfaces on Fabric Interconnect A. Then, repeat the same process for Fabric Interconnect B.
8. **Finalize configuration**: Click **OK** to close the NAS Appliance Manager pop-up window and save the configuration.

Failover Test Summary: Ensuring High Availability of FlashArray File Services

To validate the resiliency and high availability of the Pure Storage FlashArray File Services environment, a series of controlled failover scenarios was executed. These tests simulate real-world events and demonstrate the ability of the FlashArray to maintain file service continuity through its redundant architecture and automated failover mechanisms. The following types of tests were performed:

1. Controller reboot (ct0/ct1)
2. Fabric Interconnect (FI) reboot

The flow of these tests and their respective outcomes are detailed in the following subsections.

Controller Reboot (ct0/ct1)

Purpose

To validate complete hardware-level failover from one controller to the other.

Method

- The active FlashArray controller (for example, ct0) was deliberately rebooted.
- All network links (including LAGs) and file services were observed during the transition.
- The standby controller (ct1) remained active and monitored for takeover.

Expected Behavior

- The **VIP** associated with file services **automatically migrated** to the standby controller.
- LAG/LACP interfaces re-established traffic flow through the active controller.
- **Client sessions experienced minimal or no disruption,** with reconnections handled at the protocol level.
- NFS and SMB shares remained accessible without administrative intervention.

This ensures the **continuity of storage services** even during disruptive controller-level events.

Fabric Interconnect Reboot

Purpose

To verify the behavior of the direct-attached FlashArray configuration during a **Fabric Interconnect reboot,** with a focus on **upstream redundancy, LACP stability, and failover across UCS Fabrics.**

Method

- Initiated a **controlled reboot** of either **FI-A** or **FI-B** while ensuring that the corresponding connected FlashArray controller (for example, ct0 or ct1) remained fully operational.
- Ensured storage interfaces from the FlashArray were directly connected to each Fabric Interconnect via **individual port channels** (LAGs).
- Monitored storage traffic routing and link-state behavior during and after the reboot.
- Validated that LACP reconvergence occurred on the surviving path without manual reconfiguration.

Expected Behavior

- A **brief interruption** (sub-second to a few seconds) in traffic was observed due to the loss of link connectivity through the rebooted Fabric Interconnect.
- **Client-side access** to storage (NFS/SMB shares or iSCSI sessions) resumed automatically once traffic rerouted through the alternate Fabric Interconnect and corresponding LAG interface.
- This behavior aligns with UCS architecture, where Fabric Interconnects in IMM **do not operate as traditional switches** (that is, no virtual port channel–like behavior). Instead, each **Fabric Interconnect functions independently**, with LAGs terminating on each fabric.
- Upon reboot completion, the system **automatically re-established dual-path redundancy.**

This validates the system's ability to sustain **continuous access to storage** despite upstream disruptions and confirms the **resilience of port channel configurations in UCS IMM.**

	Test Cases	Purpose	Method	Expected Behavior
▸1	▸Controller Reboot (ct0 / ct1)	▸To verify complete hardware-level failover from one controller to another.	▸Intentionally rebooted the active controller (e.g., ct0). - Observed automatic migration of file services and LAG interfaces to standby controller (ct1). - VIP reassigned to the newly active controller (ct1)	▸- VIP migrated automatically to the active controller. - Minimal to no client disruption. - LACP maintained traffic via healthy paths.
▸2	▸Fabric Interconnect (FI) Reboot	▸To test redundancy of upstream connectivity and validate LAG/LACP resiliency between FI-A and FI-B.	▸- Rebooted either FI-A or FI-B while FlashArray remained online. - Each FlashArray controller had dual connections to both FIs. - Observed LACP behavior and traffic rerouting.	▸- Brief packet drops occurred, as expected. - Interfaces tied to failed FI removed from LAG. - Traffic rerouted via alternate FI. - System auto-reconverged and resumed normal operations.

FIGURE 12 Test outcomes

Conclusion

Direct connectivity of NFS and SMB file services to Cisco UCS Fabric Interconnects provides a simplified and high-performance storage solution. By understanding the limitations and best practices outlined in this white paper, IT teams can design a scalable and efficient direct-attached storage architecture with Pure Storage FlashArray that meets their workload demands.

With the capability to deliver this in a reduced footprint for both power and cost, the FlashArray solution truly becomes a powerful platform, delivering more potential to customers from the smallest to largest scale.

Additional Resources

- Visit the Pure Storage FlashArray product page.
- Review the Pure Storage FlashStack Compatibility Matrix. This interoperability list requires a support login from Pure Storage.

ID3121-01-en-08/25