



The bridge to possible

White paper
Cisco public

FlexPod Datacenter with Cisco UCS X-Series and Cisco Intersight

June 11, 2021

Contents

Executive summary	4
Solution overview	5
Introduction	5
Audience	5
Purpose of this document	5
What's new in this release?	5
Solution summary	6
Technology overview	6
FlexPod Datacenter	6
Cisco Unified Compute System X-Series	7
Cisco Intersight	13
Cisco Nexus Switching Fabric	15
Cisco MDS 9132T 32G Multilayer Fabric Switch	15
Cisco DCNM-SAN	16
NetApp AFF A-Series Storage	16
VMware vSphere 7.0	19
Cisco Intersight Assist device connector for VMware vCenter and NetApp ONTAP	19
Solution design	21
Design requirements	21
Physical topology	21
Logical topology	25
Compute system connectivity	28
Cisco Nexus Ethernet connectivity	28
Cisco MDS SAN connectivity - Fibre Channel design only	30
Cisco UCS X-Series configuration - Cisco Intersight Managed Mode	31
NetApp AFF A400 - Server Virtual Machine (SVM) design	37
VMware vSphere - ESXi design	39
Cisco Intersight Integration with VMware vCenter and NetApp storage	41
Deployment hardware and software	50
Hardware and software revisions	50

Summary	51
Appendix	52
Compute	52
Network	52
Storage	52
Virtualization	52

Executive summary

The FlexPod Datacenter solution is a validated approach for deploying Cisco® and NetApp technologies and products to build shared private and public cloud infrastructure. Cisco and NetApp have partnered to deliver a series of FlexPod solutions that enable strategic data-center platforms. The success of the FlexPod solution is driven through its ability to evolve and incorporate both technology and product innovations in the areas of management, compute, storage, and networking. This document covers the design details of incorporating the Cisco X-Series modular platform into the FlexPod Datacenter and the ability to manage and orchestrate FlexPod components from the cloud using Cisco Intersight. Some of the key advantages of integrating Cisco UCS X-Series into the FlexPod infrastructure are:

- **Simpler and programmable infrastructure:** infrastructure as a code delivered through a single partner integrable open API
- **Power and cooling innovations:** higher power headroom and lower energy loss due to a 54V DC power delivery to the chassis
- **Better airflow:** midplane-free design with fewer barriers, therefore lower impedance
- **Fabric innovations:** PCIe/Compute Express Link (CXL) topology for heterogeneous compute and memory composability
- **Innovative cloud operations:** continuous feature delivery and no need for maintaining on-premise virtual machines supporting management functions
- **Built for investment protections:** design ready for future technologies such as liquid cooling and high-Wattage CPUs; CXL-ready

In addition to the compute-specific hardware and software innovations, the integration of the Cisco Intersight cloud platform with VMware vCenter and NetApp Active IQ Unified Manager delivers monitoring, orchestration, and workload optimization capabilities for different layers (virtualization and storage) of the FlexPod infrastructure. The modular nature of the Cisco Intersight platform also provides an easy upgrade path to additional services, such as workload optimization and Kubernetes.

Customers interested in understanding FlexPod design and deployment details, including the configuration of various elements of design and associated best practices, should refer to Cisco Validated Designs for FlexPod, at <https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html>.

Solution overview

Introduction

The Cisco Unified Compute System (UCS) X-Series is a brand-new modular compute system, configured and managed from the cloud. It is designed to meet the needs of modern applications and to improve operational efficiency, agility, and scale through an adaptable, future-ready, modular design. The Cisco Intersight platform is a Software-as-a-Service (SaaS) infrastructure lifecycle management platform that delivers simplified configuration, deployment, maintenance, and support.

Powered by the Cisco Intersight cloud-operations platform, the Cisco UCS X-Series enables the next-generation cloud-operated FlexPod infrastructure that not only simplifies data-center management but also allows the infrastructure to adapt to the unpredictable needs of modern applications as well as traditional workloads. With the Cisco Intersight platform, customers get all the benefits of SaaS delivery and the full lifecycle management of Intersight-connected distributed servers and integrated NetApp storage systems across data centers, remote sites, branch offices, and edge environments.

Audience

The intended audience of this document includes but is not limited to IT architects, sales engineers, field consultants, professional services, IT managers, partner engineering, and customers who want to take advantage of an infrastructure built to deliver IT efficiency and enable IT innovation.

Purpose of this document

This document provides design guidance around incorporating the Cisco Intersight-managed UCS X-Series platform within FlexPod Datacenter infrastructure. The document introduces various design elements and covers various considerations and best practices for a successful deployment. The document also highlights the design and product requirements for integrating virtualization and storage systems to Cisco Intersight to deliver a true cloud-based integrated approach to infrastructure management.

What's new in this release?

The following design elements distinguish this version of FlexPod from previous models:

- Integration with Cisco UCS X-Series
- Managing Cisco UCS X-Series from the cloud using Cisco Intersight
- Integration of Cisco Intersight with NetApp Active IQ Unified Manager for storage monitoring and orchestration
- Integration of Cisco Intersight with VMware vCenter for interacting with, monitoring, and orchestrating the virtual environment

Solution summary

The FlexPod Datacenter solution with Cisco UCS X-Series and Cisco Intersight offers the following key benefits:

- Simplified cloud-based management of the solution components
- Hybrid-cloud-ready, policy-driven modular design
- Highly available and scalable platform with flexible architecture that supports various deployment models
- Cooperative support model and Cisco Solution Support
- Easy to deploy, consume, and manage architecture, which saves time and resources required to research, procure, and integrate off-the-shelf components
- Support for component monitoring, solution orchestration, and workload optimization

Like all other FlexPod solution designs, FlexPod Datacenter with Cisco UCS X-Series and Intersight is configurable according to demand and usage. Customers can purchase exactly the infrastructure they need for their current application requirements and can then scale up by adding more resources to the FlexPod system or scale out by adding more FlexPod instances. By moving the management from the fabric interconnects into the cloud, the solution can respond to the speed and scale of customer deployments with a constant stream of new capabilities delivered from Intersight software-as-a-service model at cloud-scale.

Technology overview

FlexPod Datacenter

FlexPod Datacenter architecture is built using the following infrastructure components for compute, network, and storage:

- Cisco Unified Computing System (Cisco UCS)
- Cisco Nexus® and Cisco MDS switches
- NetApp All Flash FAS (AFF) storage systems

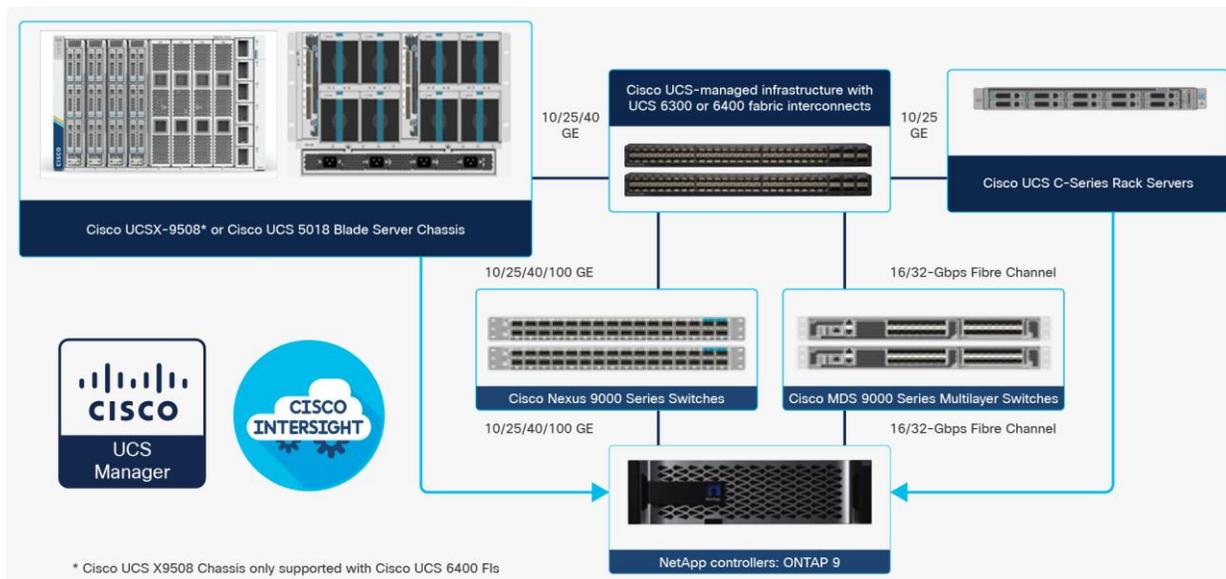


Figure 1.

FlexPod Datacenter components

All the FlexPod components have been integrated so that customers can deploy the solution quickly and economically while eliminating many of the risks associated with researching, designing, building, and deploying similar solutions from the foundation. One of the main benefits of FlexPod is its ability to maintain consistency at scale. Each of the component families shown in [Figure 1](#) (Cisco UCS, Cisco Nexus, Cisco MDS, and NetApp controllers) offers platform and resource options to scale up or scale out the infrastructure while supporting the same features.

The FlexPod Datacenter solution with Cisco UCS X-Series and Intersight uses following hardware components:

- Cisco UCS X9508 Chassis with up to eight Cisco UCS X210c M6 Compute Nodes
- Fourth-generation Cisco UCS 6454 Fabric Interconnects to support 10GbE, 25GbE, and 100GbE connectivity from various components
- High-speed Cisco NX-OS-based Nexus 93180YC-FX3 switching design to support up to 100GE connectivity
- NetApp AFF A400 end-to-end NVMe storage with high-speed Ethernet and (optional) Fibre Channel connectivity

The software components consist of:

- Cisco Intersight platform to deploy, maintain and support the FlexPod components
- Cisco Intersight Assist Virtual Appliance to help connect NetApp ONTAP and VMware vCenter with Cisco Intersight
- NetApp Active IQ Unified Manager to monitor and manage the storage and for NetApp ONTAP integration with Cisco Intersight
- VMware vCenter to set up and manage the virtual infrastructure as well as Cisco Intersight integration

These key product highlights and features are outlined below.

Cisco Unified Compute System X-Series

The Cisco UCS X-Series Modular System is designed to take the current generation of the Cisco UCS platform to the next level with its future-ready design and cloud-based management. Decoupling and moving the platform management to the cloud allows Cisco UCS to respond to customer feature and scalability requirements in a much faster and efficient manner. Cisco UCS X-Series state of the art hardware simplifies the data-center design by providing flexible server options. A single server type, supporting a broader range of workloads, results in fewer different data-center products to manage and maintain. The Cisco Intersight cloud-management platform manages Cisco UCS X-Series as well as integrating with third-party devices, including VMware vCenter and NetApp storage, to provide visibility, optimization, and orchestration from a single platform, thereby driving agility and deployment consistency.

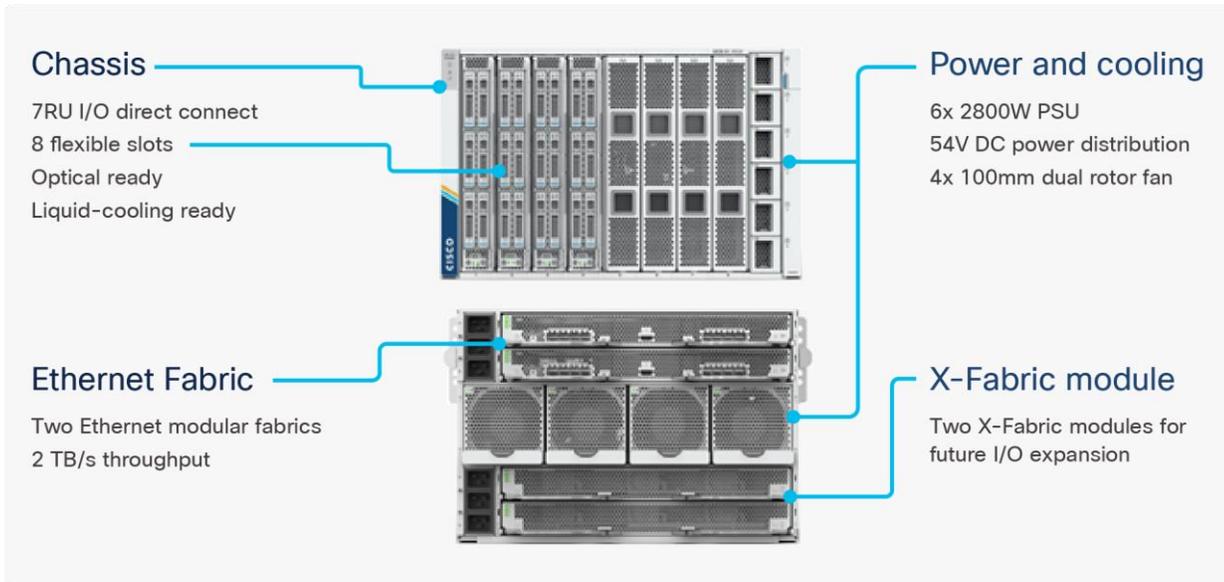


Figure 2.
Cisco UCS X9508 Chassis

The various components of the Cisco UCS X-Series are discussed below.

Cisco UCS X9508 Chassis

The Cisco UCS X-Series chassis is engineered to be adaptable and flexible. As seen in [Figure 3](#), the UCS X9508 chassis has only a power-distribution midplane. This midplane-free design provides fewer obstructions for better airflow. For I/O connectivity, vertically oriented compute nodes intersect with horizontally oriented fabric modules, allowing the chassis to support future fabric innovations. Cisco UCS X9508 Chassis' superior packaging enables larger compute nodes, thereby providing more space for actual compute components, such as memory, GPU, drives, and accelerators. Improved airflow through the chassis enables support for higher power components, and more space allows for future thermal solutions (such as liquid cooling) without limitations.



Figure 3.
Cisco UCS X9508 Chassis - midplane free design

The Cisco UCS X9508 7-Rack-Unit (7RU) chassis has eight flexible slots. These slots can house a combination of compute nodes and a pool of future I/O resources that may include GPU accelerators, disk storage, and nonvolatile memory. At the top rear of the chassis are two Intelligent Fabric Modules (IFMs) that connect the chassis to upstream Cisco UCS 6400 Series Fabric Interconnects. At the bottom rear of the chassis are slots

ready to house future X-Fabric modules that can flexibly connect the compute nodes with I/O devices. Six 2800W Power Supply Units (PSUs) provide 54V power to the chassis with N, N+1, and N+N redundancy. A higher voltage allows efficient power delivery with less copper and reduced power loss. Efficient, 100mm, dual counter-rotating fans deliver industry-leading airflow and power efficiency, and optimized thermal algorithms enable different cooling modes to best support the customer's environment.

Cisco UCSX 9108-25G Intelligent Fabric Modules

For the Cisco UCS X9508 Chassis, the network connectivity is provided by a pair of Cisco UCSX 9108-25G Intelligent Fabric Modules (IFMs). Like the fabric extenders used in the Cisco UCS 5108 Blade Server Chassis, these modules carry all network traffic to a pair of Cisco UCS 6400 Series Fabric Interconnects (FIs). IFMs also host the Chassis Management Controller (CMC) for chassis management. In contrast to systems with fixed networking components, Cisco UCS X9508's midplane-free design enables easy upgrades to new networking technologies as they emerge making it straightforward to accommodate new network speeds or technologies in the future.



Figure 4.
Cisco UCSX 9108-25G Intelligent Fabric Module

Each IFM supports eight 25Gb uplink ports for connecting the Cisco UCS X9508 Chassis to the FIs and 32 25Gb server ports for the eight compute nodes. IFM server ports can provide up to 200 Gbps of unified fabric connectivity per compute node across the two IFMs. The uplink ports connect the chassis to the UCS FIs, providing up to 400Gbps connectivity across the two IFMs. The unified fabric carries management, VM, and Fibre Channel over Ethernet (FCoE) traffic to the FIs, where management traffic is routed to the Cisco Intersight cloud operations platform, FCoE traffic is forwarded to the native Fibre Channel interfaces through unified ports on the FI (to Cisco MDS switches), and data Ethernet traffic is forwarded upstream to the data center network (via Cisco Nexus switches).

Cisco UCS X210c M6 Compute Node

The Cisco UCS X9508 Chassis is designed to host up to 8 Cisco UCS X210c M6 Compute Nodes. The hardware details of the Cisco UCS X210c M6 Compute Nodes are shown in [Figure 5](#):

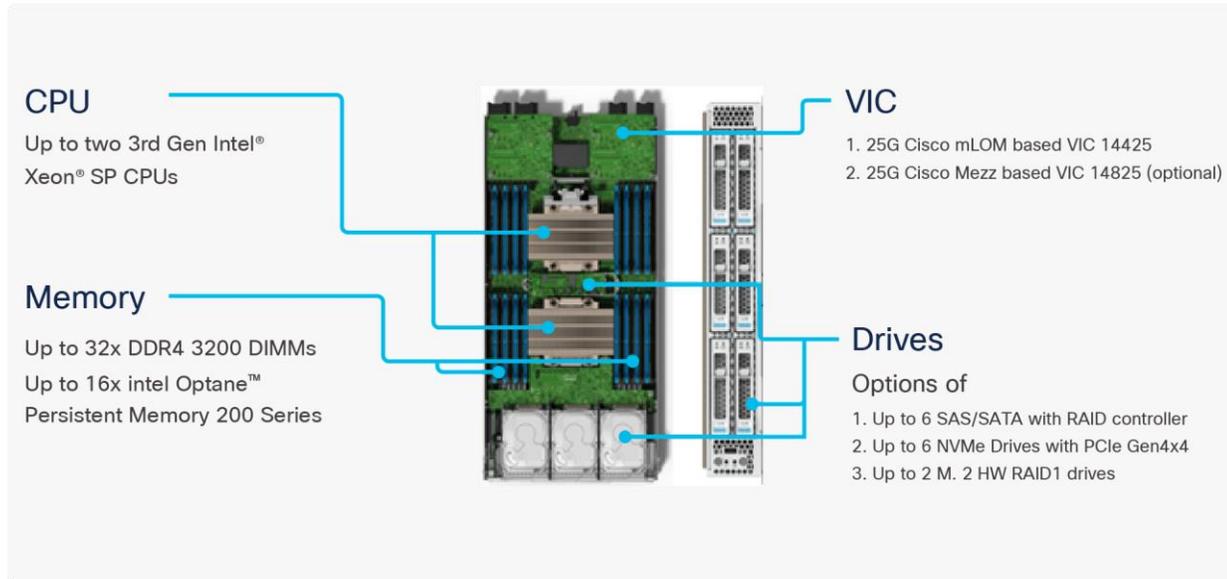


Figure 5.
Cisco UCS X210c M6 Compute Node

The Cisco UCS X210c M6 features:

- **CPU:** Up to 2x 3rd Gen Intel Xeon Scalable Processors with up to 40 cores per processor and 1.5 MB Level 3 cache per core
- **Memory:** Up to 32 x 256 GB DDR4-3200 DIMMs for a maximum of 8 TB of main memory. The Compute Node can also be configured for up to 16 x 512-GB Intel Optane persistent memory DIMMs for a maximum of 12 TB of memory
- **Disk storage:** Up to 6 SAS or SATA drives can be configured with an internal RAID controller, or customers can configure up to 6 NVMe drives. 2 M.2 memory cards can be added to the Compute Node with RAID 1 mirroring.
- **Virtual Interface Card (VIC):** Up to 2 VICs including an mLOM Cisco VIC 14425 and a mezzanine Cisco VIC card 14825 can be installed in a Compute Node.
- **Security:** The server supports an optional Trusted Platform Module (TPM). Additional security features include a secure boot FPGA and ACT2 anticounterfeit provisions.

Cisco UCS Virtual Interface Cards (VICs)

Cisco UCS X210c M6 Compute Nodes support the following two Cisco fourth-generation VIC cards:

Cisco VIC 14425

Cisco VIC 14425 fits the mLOM slot in the Cisco X210c Compute Node and enables up to 50 Gbps of unified fabric connectivity to each of the chassis IFMs for a total of 100 Gbps of connectivity per server. Cisco VIC 14425 connectivity to the IFM and up to the fabric interconnects is delivered through 4x 25-Gbps connections, which are configured automatically as 2x 50-Gbps port channels. Cisco VIC 14425 supports 256 virtual interfaces (both Fibre Channel and Ethernet) along with the latest networking innovations such as NVMeoF over RDMA (ROCEv2), VxLAN/NVGRE offload, etc.

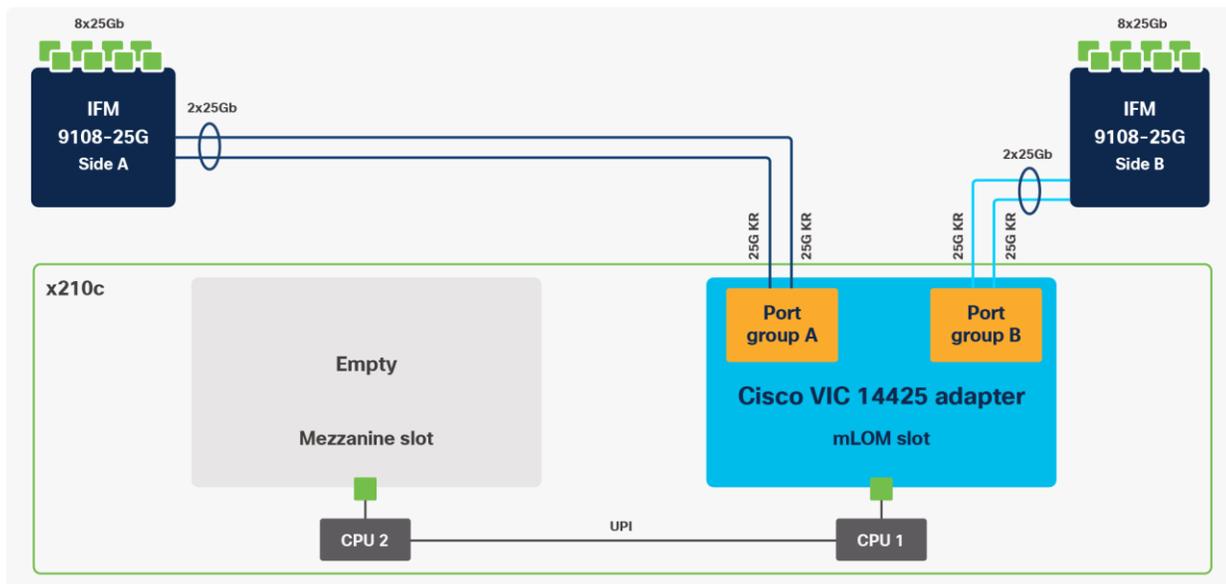


Figure 6.
Single Cisco VIC 14425 in Cisco UCS X210c M6

The connections between the 4th generation Cisco VIC (Cisco UCS VIC 1440) in the Cisco UCS B200 blades and the I/O modules in the Cisco UCS 5108 chassis comprise of multiple 10Gbps KR lanes. The same connections between Cisco VIC 14425 and IFMs in Cisco UCS X-Series comprise of multiple 25Gbps KR lanes resulting in 2.5x better connectivity in Cisco UCS X210c M6 Compute Nodes. The network interface speed comparison between VMware ESXi installed on Cisco UCS B200 M5 with VIC 1440 and Cisco UCS X210c M6 with VIC 14425 is shown in [Figure 7](#).

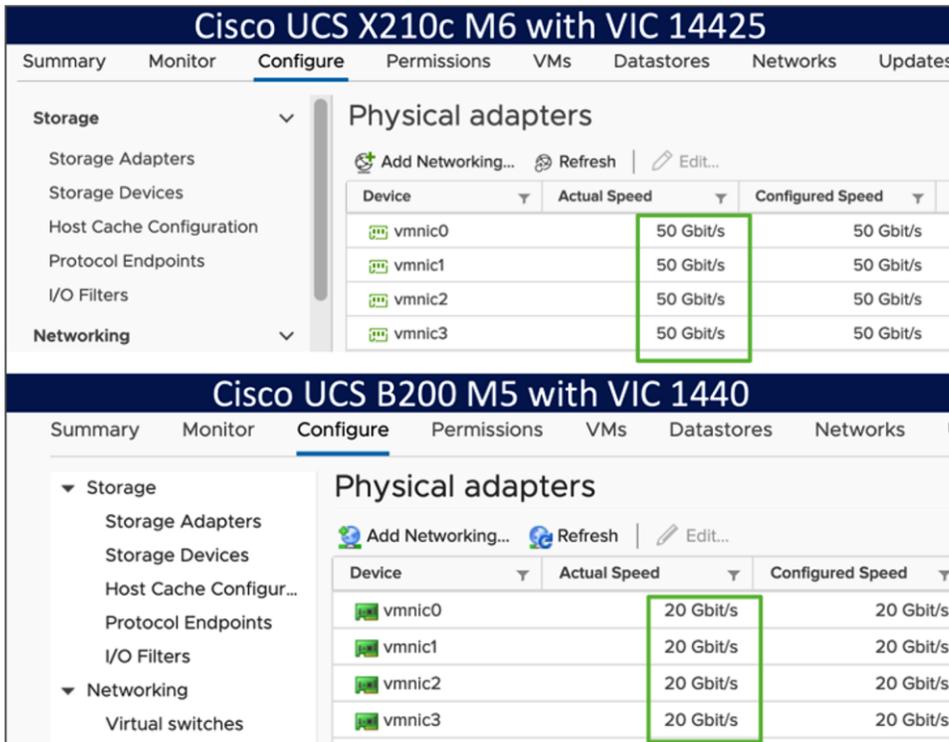


Figure 7.
Network Interface speed comparison

Cisco VIC 14825

The optional Cisco VIC 14825 fits the mezzanine slot on the server. A bridge card (UCSX-V4-BRIDGE) extends this VIC's 2x 50 Gbps of network connections up to the mLOM slot and out through the mLOM's IFM connectors, bringing the total bandwidth to 100 Gbps per fabric for a total bandwidth of 200 Gbps per server.

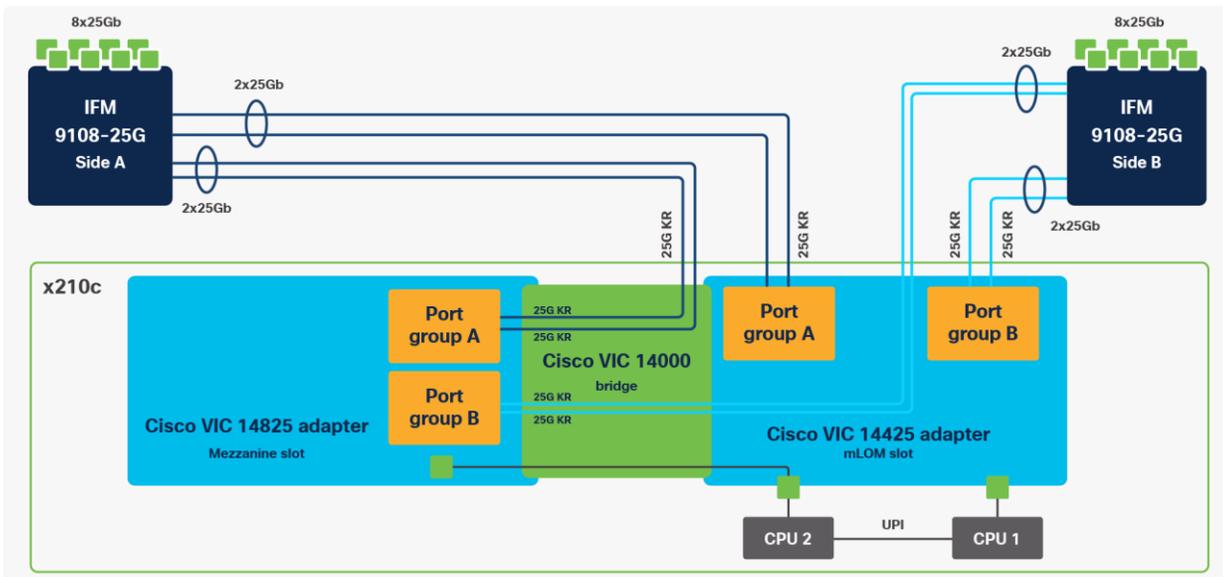


Figure 8.
Cisco VIC 14425 and 14825 in Cisco UCS X210c M6

Cisco UCS 6400 Series Fabric Interconnects

The Cisco UCS Fabric Interconnects (FIs) provide a single point for connectivity and management for the entire Cisco UCS system. Typically deployed as an active/active pair, the system's FIs integrate all components into a single, highly available management domain controlled by the Cisco UCS Manager or Cisco Intersight. Cisco UCS FIs provide a single unified fabric for the system, with low-latency, lossless, cut-through switching that supports LAN, SAN, and management traffic using a single set of cables.



Figure 9.
Cisco UCS 6454 Fabric Interconnect

Cisco UCS 6454 utilized in the current design is a 54-port Fabric Interconnect. This single RU device includes 28 10/25 Gbps Ethernet ports, 4 1/10/25-Gbps Ethernet ports, 6 40/100-Gbps Ethernet uplink ports, and 16 unified ports that can support 10/25 Gigabit Ethernet or 8/16/32-Gbps Fibre Channel, depending on the SFP.

Note: For supporting the Cisco UCS X-Series, the fabric interconnects must be configured in Intersight Managed Mode (IMM). This option replaces the local management with Cisco Intersight cloud- or appliance-based management.

Cisco Intersight

The Cisco Intersight platform is a Software-as-a-Service (SaaS) infrastructure lifecycle management platform that delivers simplified configuration, deployment, maintenance, and support. The Cisco Intersight platform is designed to be modular, so customers can adopt services based on their individual requirements. The platform significantly simplifies IT operations by bridging applications with infrastructure, providing visibility and management from bare-metal servers and hypervisors to serverless applications, thereby reducing costs and mitigating risk. This unified SaaS platform uses a unified Open API design that natively integrates with third-party platforms and tools.

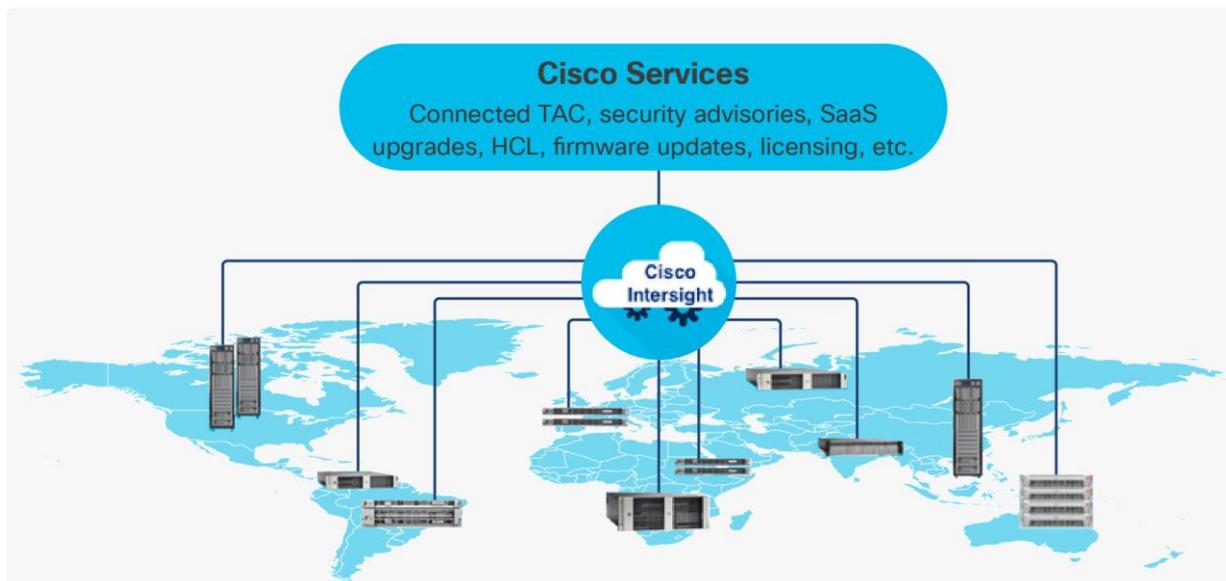


Figure 10.
Cisco Intersight overview

The main benefits of Cisco Intersight infrastructure services are as follows:

- Simplify daily operations by automating many daily manual tasks
- Combine the convenience of a SaaS platform with the capability to connect from anywhere and manage infrastructure through a browser or mobile app
- Stay ahead of problems and accelerate trouble resolution through advanced support capabilities
- Gain global visibility of infrastructure health and status along with advanced management and support capabilities
- Upgrade to add workload optimization and Kubernetes services when needed

Cisco Intersight Virtual Appliance and Private Virtual Appliance

In addition to the SaaS deployment model running on Intersight.com, on-premises options can be purchased separately. The Cisco Intersight Virtual Appliance and Cisco Intersight Private Virtual Appliance are available for organizations that have additional data locality or security requirements for managing systems. The Cisco Intersight Virtual Appliance delivers the management features of the Cisco Intersight platform in an easy-to-deploy VMware Open Virtualization Appliance (OVA) or Microsoft Hyper-V Server virtual machine that allows you to control the system details that leave your premises. The Cisco Intersight Private Virtual Appliance is provided in a form factor specifically designed for users who operate in disconnected (air gap) environments. The Private Virtual Appliance requires no connection to public networks or back to Cisco to operate.

Cisco Intersight Assist

Cisco Intersight Assist helps customers add endpoint devices to Cisco Intersight. A data center could have multiple devices that do not connect directly with Cisco Intersight. Any device that is supported by Cisco Intersight, but does not connect directly with it, will need a connection mechanism. Cisco Intersight Assist provides that connection mechanism. In FlexPod, VMware vCenter and NetApp Active IQ Unified Manager connect to Intersight with the help of Intersight Assist VM.

Cisco Intersight Assist is available within the Cisco Intersight Virtual Appliance, which is distributed as a deployable virtual machine contained within an Open Virtual Appliance (OVA) file format. More details about the Cisco Intersight Assist VM deployment configuration is covered in later sections.

Licensing requirements

The Cisco Intersight platform uses a subscription-based license with multiple tiers. Customers can purchase a subscription duration of one, three, or five years and choose the required Cisco UCS server volume tier for the selected subscription duration. Each Cisco endpoint automatically includes a Cisco Intersight Base license at no additional cost when customers access the Cisco Intersight portal and claim a device. Customers can purchase any of the following higher-tier Cisco Intersight licenses using the Cisco ordering tool:

Cisco Intersight Essentials: Essentials includes all the functions of the Base license plus additional features, including Cisco UCS Central Software and Cisco Integrated Management Controller (IMC) supervisor entitlement, policy-based configuration with server profiles, firmware management, and evaluation of compatibility with the Cisco Hardware Compatibility List (HCL).

Cisco Intersight Advantage: Advantage offers all the features and functions of the Base and Essentials tiers. It includes storage widgets and cross-domain inventory correlation across compute, storage, and virtual environments (VMWare ESXi). It also includes OS installation for supported Cisco UCS platforms.

Cisco Intersight Premier: In addition to all of the functions provided in the Advantage tier, Premier includes full subscription entitlement for Intersight Orchestrator, which provides orchestration across Cisco UCS and third-party systems.

Servers in the Cisco Intersight managed mode require at least the Essentials license. For more information about the features provided in the various licensing tiers, see https://intersight.com/help/getting_started#licensing_requirements.

Cisco Nexus Switching Fabric

The Cisco Nexus 9000 Series Switches offer both modular and fixed 1/10/25/40/100 Gigabit Ethernet switch configurations with scalability up to 60 Tbps of nonblocking performance with less than five-microsecond latency, wire speed VXLAN gateway, bridging, and routing support.



Figure 11.
Cisco Nexus 93180YC-FX3 Switch

The Nexus 9000 series switch featured in this design is the Nexus 93180YC-FX3 configured in NX-OS standalone mode. NX-OS is a purpose-built data-center operating system designed for performance, resiliency, scalability, manageability, and programmability at its foundation. It provides a robust and comprehensive feature set that meets the demanding requirements of virtualization and automation.

The Cisco Nexus 93180YC-FX3 Switch is a 1RU switch that supports 3.6 Tbps of bandwidth and 1.2 bpps. The 48 downlink ports on the 93180YC-FX3 can support 1-, 10-, or 25-Gbps Ethernet, offering deployment flexibility and investment protection. The six uplink ports can be configured as 40- or 100-Gbps Ethernet, offering flexible migration options.

Cisco MDS 9132T 32G Multilayer Fabric Switch

The Cisco MDS 9132T 32G Multilayer Fabric Switch is the next generation of the highly reliable, flexible, and low-cost Cisco MDS 9100 Series switches. It combines high performance with exceptional flexibility and cost effectiveness. This powerful, compact one Rack-Unit (1RU) switch scales from 8 to 32 line-rate 32 Gbps Fibre Channel ports.



Figure 12.
Cisco MDS 9132T 32G Multilayer Fabric Switch

The Cisco MDS 9132T delivers advanced storage networking features and functions with ease of management and compatibility with the entire Cisco MDS 9000 family portfolio for reliable end-to-end connectivity. This switch also offers state-of-the-art SAN analytics and telemetry capabilities that have been built into this next-generation hardware platform. This new state-of-the-art technology couples the next-generation port ASIC with a fully dedicated network processing unit designed to complete analytics calculations in real time. The telemetry data extracted from the inspection of the frame headers are calculated on board (within the switch) and, using an industry-leading open format, can be streamed to any analytics-visualization platform. This switch also includes a dedicated 10/100/1000BASE-T telemetry port to maximize data delivery to any telemetry receiver, including Cisco Data Center Network Manager.

Cisco DCNM-SAN

Cisco DCNM-SAN can be used to monitor, configure, and analyze Cisco 32Gbps Fibre Channel fabrics and show information about the Cisco Nexus switching fabric. Cisco DCNM-SAN is deployed as a virtual appliance from an OVA and is managed through a web browser. Once the Cisco MDS and Nexus switches are added with the appropriate credentials and licensing, monitoring of the SAN and Ethernet fabrics can begin. Additionally, VSANs, device aliases, zones, and zone sets can be added, modified, and deleted using the DCNM point-and-click interface. Device Manager can also be used to configure the Cisco MDS switches. SAN Analytics can be added to Cisco MDS switches to provide insights into the fabric by allowing customers to monitor, analyze, identify, and troubleshoot performance issues.

Cisco DCNM integration with Cisco Intersight

The Cisco Network Insights Base (Cisco NI Base) application provides a number of TAC assist functionalities which are useful when working with Cisco TAC. The Cisco NI Base app collects the CPU, device name, device product id, serial number, version, memory, device type, and disk usage information for the nodes in the fabric. Cisco NI Base application is connected to the Cisco Intersight cloud portal through a device connector which is embedded in the management controller of the Cisco DCNM platform. The device connector provides a secure way for connected Cisco DCNM to send and receive information from the Cisco Intersight portal, using a secure Internet connection.

NetApp AFF A-Series Storage

With the new NetApp AFF A-Series controller lineup, NetApp provides industry leading performance while continuing to provide a full suite of enterprise-grade data management and data protection features. AFF A-Series systems support end-to-end NVMe technologies, from NVMe-attached SSDs to frontend NVMe over Fibre Channel (NVMe/FC) host connectivity. These systems deliver enterprise class performance, making them a superior choice for driving the most demanding workloads and applications. With a simple software upgrade to the modern NVMe/FC SAN infrastructure, you can drive more workloads with faster response times, without disruption or data migration. Additionally, more and more organizations are adopting a “cloud first” strategy, driving the need for enterprise-grade data services for a shared environment across on-premises data centers and the cloud. As a result, modern all-flash arrays must provide robust data services, integrated data protection, seamless scalability, and new levels of performance – plus deep application and cloud integration. These new workloads demand performance that first-generation flash systems cannot deliver.

For more information about the NetApp AFF A-series controllers, see the AFF product page:

<https://www.netapp.com/us/products/storage-systems/all-flash-array/aff-a-series.aspx>.

You can view or download more technical specifications of the AFF A-series controllers here:

<https://www.netapp.com/us/media/ds-3582.pdf>

NetApp AFF A400

The NetApp AFF A400 offers full end-to-end NVMe support. The frontend NVMe/FC connectivity makes it possible to achieve optimal performance from an all-flash array for workloads that include artificial intelligence, machine learning, and real-time analytics as well as business-critical databases. On the back end, the A400 supports both serial-attached SCSI (SAS) and NVMe-attached SSDs, offering the versatility for current customers to move up from their legacy A-Series systems and satisfying the increasing interest that all customers have in NVMe-based storage.

The NetApp AFF A400 offers greater port availability, network connectivity, and expandability. The NetApp AFF A400 has 10 PCIe Gen3 slots per high availability pair. The NetApp AFF A400 offers 25GbE or 100GbE, as well as 32Gb/FC and NVMe/FC network connectivity. This model was created to keep up with changing business needs and performance and workload requirements by merging the latest technology for data acceleration and ultra-low latency in an end-to-end NVMe storage system.

Note: Cisco UCS X-Series is supported with all NetApp AFF systems running NetApp ONTAP 9 release.



Figure 13.
NetApp AFF A400 front view



Figure 14.
NetApp AFF A400 rear view

NetApp ONTAP 9

NetApp storage systems harness the power of ONTAP to simplify the data infrastructure from edge, core, and cloud with a common set of data services and 99.9999 percent availability. NetApp ONTAP 9 data management software from NetApp enables customers to modernize their infrastructure and transition to a cloud-ready data center. ONTAP 9 has a host of features to simplify deployment and data management, accelerate and protect critical data, and make infrastructure future-ready across hybrid-cloud architectures.

NetApp ONTAP 9 is the data management software that is used with the NetApp AFF A400 all-flash storage system in this solution design. ONTAP software offers secure unified storage for applications that read and write data over block- or file-access protocol storage configurations. These storage configurations range from high-speed flash to lower-priced spinning media or cloud-based object storage. ONTAP implementations can run on NetApp engineered FAS or AFF series arrays and in private, public, or hybrid clouds (NetApp Private Storage and NetApp Cloud Volumes ONTAP). Specialized implementations offer best-in-class converged infrastructure, featured here as part of the FlexPod Datacenter solution or with access to third-party storage arrays (NetApp FlexArray virtualization). Together these implementations form the basic framework of the NetApp Data Fabric, with a common software-defined approach to data management, and fast efficient replication across systems. FlexPod and ONTAP architectures can serve as the foundation for both hybrid cloud and private cloud designs.

Read more about all the capabilities of ONTAP data management software here:

<https://www.netapp.com/us/products/data-management-software/ontap.aspx>.

NetApp Active IQ Unified Manager

NetApp Active IQ Unified Manager is a comprehensive monitoring and proactive management tool for NetApp ONTAP systems to help manage the availability, capacity, protection, and performance risks of your storage systems and virtual infrastructure. The Unified Manager can be deployed on a Linux server, on a Windows server, or as a virtual appliance on a VMware host.

Active IQ Unified Manager enables monitoring your ONTAP storage clusters from a single redesigned, intuitive interface that delivers intelligence from community wisdom and AI analytics. It provides comprehensive operational, performance, and proactive insights into the storage environment and the virtual machines running on it. When an issue occurs on the storage infrastructure, Unified Manager can notify you about the details of the issue to help with identifying the root cause. The virtual machine dashboard gives you a view into the performance statistics for the VM so that you can investigate the entire I/O path from the vSphere host down through the network and finally to the storage. Some events also provide remedial actions that can be taken to rectify the issue. You can configure custom alerts for events so that when issues occur, you are notified through email and SNMP Traps. Active IQ Unified Manager enables planning for the storage requirements of your users by forecasting capacity and usage trends to proactively act before issues arise, preventing reactive short-term decisions that can lead to additional problems in the long term.

VMware vSphere 7.0

VMware vSphere is a virtualization platform for holistically managing large collections of infrastructures (resources including CPUs, storage, and networking) as a seamless, versatile, and dynamic operating environment. Unlike traditional operating systems that manage an individual machine, VMware vSphere aggregates the infrastructure of an entire data center to create a single powerhouse with resources that can be allocated quickly and dynamically to any application in need.

vSphere 7.0 brings several improvements and simplifications including, but not limited to:

- Fully featured vSphere Client (HTML5) client. (The flash-based vSphere Web Client has been deprecated and is no longer available.)
- Improved Distributed Resource Scheduler (DRS) – a very different approach that results in a much more granular optimization of resources
- Assignable hardware – a new framework that was developed to extend support for vSphere features when customers utilize hardware accelerators
- vSphere Lifecycle Manager – a replacement for VMware Update Manager, bringing a suite of capabilities to make lifecycle operations better
- Refactored vMotion – improved to support today’s workloads

For more information about VMware vSphere and its components, see:

<https://www.vmware.com/products/vsphere.html>.

VMware vSphere vCenter

VMware vCenter Server provides unified management of all hosts and VMs from a single console and aggregates performance monitoring of clusters, hosts, and VMs. VMware vCenter Server gives administrators a deep insight into the status and configuration of compute clusters, hosts, VMs, storage, the guest OS, and other critical components of a virtual infrastructure. VMware vCenter manages the rich set of features available in a VMware vSphere environment.

Cisco Intersight Assist device connector for VMware vCenter and NetApp ONTAP

Cisco Intersight integrates with VMware vCenter and NetApp storage as follows:

- Cisco Intersight uses the device connector running within Cisco Intersight Assist virtual appliance to communicate with the VMware vCenter.
- Cisco Intersight uses the device connector running within a Cisco Intersight Assist virtual appliance to integrate with NetApp Active IQ Unified Manager. The NetApp AFF A400 should be added to NetApp Active IQ Unified Manager.

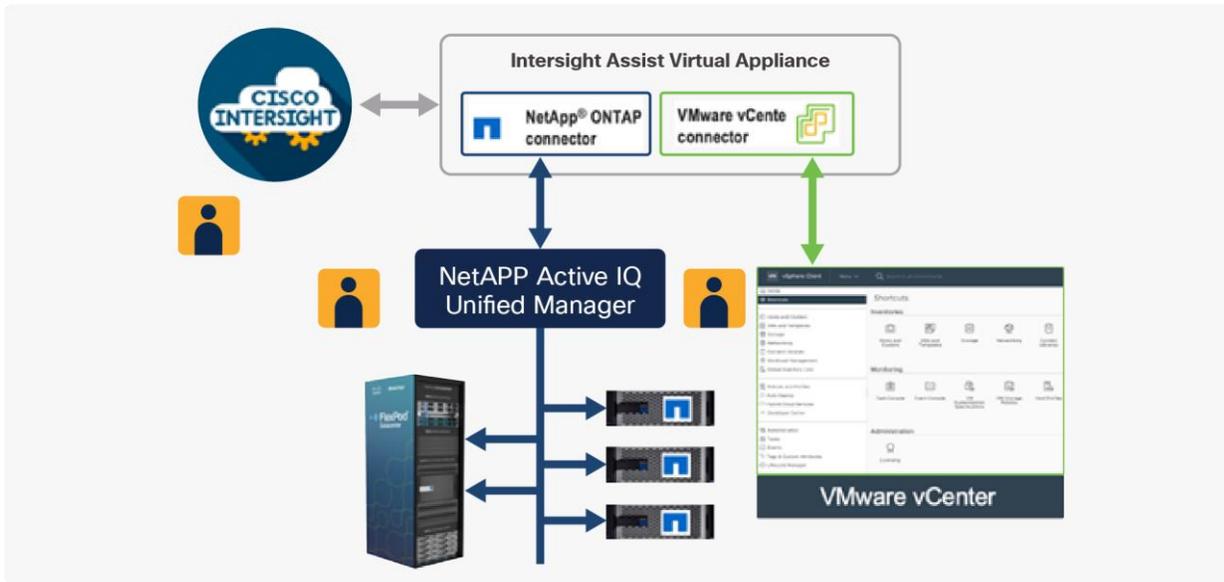


Figure 15.
Cisco Intersight and vCenter/NetApp Integration

The device connector provides a secure way for connected targets to send information and receive control instructions from the Cisco Intersight portal using a secure internet connection. The integration brings the full value and simplicity of Cisco Intersight infrastructure management service to VMware hypervisor and ONTAP data storage environments.

Enterprise SAN and NAS workloads can benefit equally from the integrated management solution. The integration architecture enables FlexPod customers to use new management capabilities with no compromise in their existing VMware or ONTAP operations. IT users will be able to manage heterogeneous infrastructure from a centralized Cisco Intersight portal. At the same time, the IT staff can continue to use VMware vCenter and NetApp Active IQ Unified Manager for comprehensive analysis, diagnostics, and reporting of virtual and storage environments. The functionality provided through this integration is covered in the upcoming solution design section.

Solution design

The FlexPod Datacenter with Cisco UCS X-Series and Intersight solution delivers a cloud-managed infrastructure solution on the latest Cisco UCS hardware. VMware vSphere 7.0 hypervisor is installed on the Cisco UCS X210c M6 Compute Nodes configured for stateless compute design using boot from SAN. NetApp AFF A400 provides the storage infrastructure required for setting up the VMware environment. The Cisco Intersight cloud-management platform is utilized to configure and manage the infrastructure. The solution requirements and design details are covered in this section.

Design requirements

The FlexPod Datacenter with Cisco UCS X-Series and Intersight design meets the following general design requirements:

- Resilient design across all layers of the infrastructure with no single point of failure
- Scalable design with the flexibility to add compute capacity, storage, or network bandwidth as needed
- Modular design that can be replicated to expand and grow as the needs of the business grow
- Flexible design that can support different models of various components with ease
- Simplified design with ability to automate and integrate with external automation tools
- Cloud-enabled design which can be configured, managed, and orchestrated from the cloud using GUI or APIs

Physical topology

FlexPod Datacenter with Cisco UCS X-Series supports both IP and Fibre Channel (FC)–based storage access design. For the IP-based solution, iSCSI configuration on Cisco UCS and NetApp AFF A400 is utilized to set up boot from SAN for the Compute Node. For the FC designs, NetApp AFF A400 and Cisco UCS X-Series are connected through Cisco MDS 9132T Fibre Channel Switches and boot from SAN uses the FC network. In both these designs, VMware ESXi hosts access the VM datastore volumes on NetApp using NFS. The physical connectivity details for both IP and FC designs are covered below.

IP-based storage access: iSCSI and NFS

The physical topology for the IP-based FlexPod Datacenter is shown in [Figure 16](#).

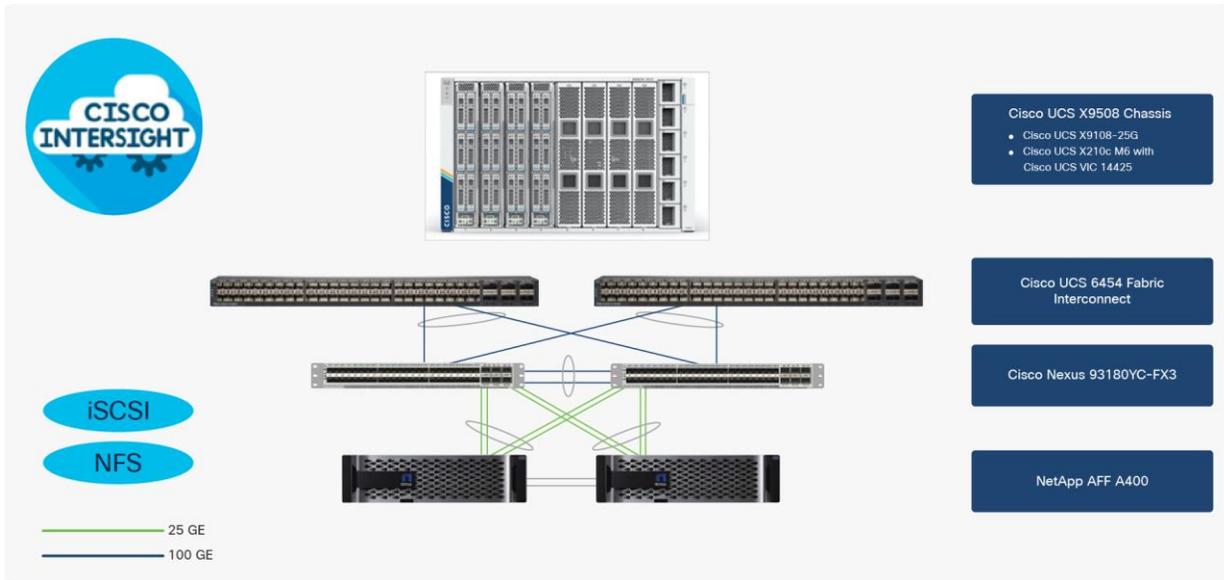


Figure 16.
FlexPod Datacenter physical topology for iSCSI and NFS

To validate the IP-based storage access in a FlexPod configuration, the components are set up as follows:

- Cisco UCS 6454 Fabric Interconnects provide the chassis and network connectivity.
- The Cisco UCS X9508 Chassis connects to fabric interconnects using Cisco UCSX 9108-25G intelligent fabric modules (IFMs), where four 25 Gigabit Ethernet ports are used on each IFM to connect to the appropriate FI. If additional bandwidth is required, all eight 25G ports can be utilized.
- Cisco UCSX-210c M6 Compute Nodes contain fourth-generation Cisco 14425 virtual interface cards.
- Cisco Nexus 93180YC-FX3 Switches in Cisco NX-OS mode provide the switching fabric.
- Cisco UCS 6454 Fabric Interconnect 100-Gigabit Ethernet uplink ports connect to Cisco Nexus 93180YC-FX3 Switches in a Virtual Port Channel (vPC) configuration.
- The NetApp AFF A400 controller connects to the Cisco Nexus 93180YC-FX3 Switches using four 25 GE ports from each controller configured as a vPC.
- VMware 7.0 ESXi software is installed on Cisco UCSX-210c M6 Compute Nodes to validate the infrastructure.

FC-based storage access: FC and NFS

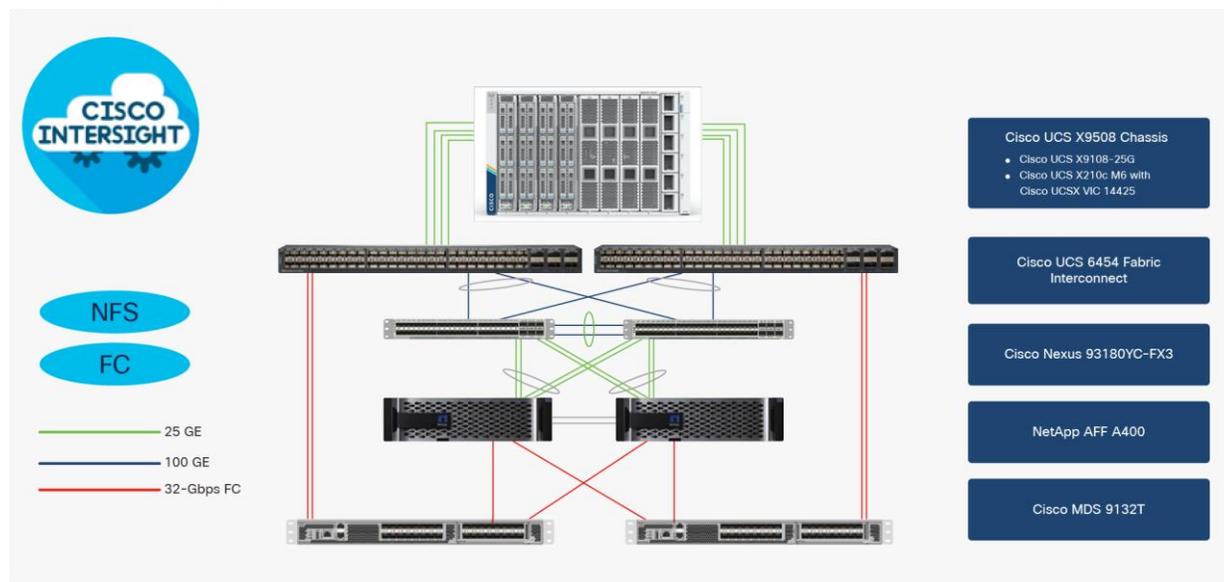


Figure 17.
FlexPod Datacenter physical topology for FC and NFS

To validate the FC-based storage access in a FlexPod configuration, the components are set up as follows:

- Cisco UCS 6454 Fabric Interconnects provide the chassis and network connectivity.
- The Cisco UCS X9508 Chassis connects to fabric interconnects using Cisco UCSX 9108-25G Intelligent Fabric Modules (IFMs), where four 25 Gigabit Ethernet ports are used on each IFM to connect to the appropriate FI.
- Cisco UCS X210c M6 Compute Nodes contain fourth-generation Cisco 14425 virtual interface cards.
- Cisco Nexus 93180YC-FX3 Switches in Cisco NX-OS mode provide the switching fabric.
- Cisco UCS 6454 Fabric Interconnect 100 Gigabit Ethernet uplink ports connect to Cisco Nexus 93180YC-FX3 Switches in a vPC configuration.
- The NetApp AFF A400 controller connects to the Cisco Nexus 93180YC-FX3 Switches using four 25 GE ports from each controller configured as a vPC for NFS traffic.
- Cisco UCS 6454 Fabric Interconnects are connected to the Cisco MDS 9132T switches using 32-Gbps Fibre Channel connections configured as a single port channel for SAN connectivity.
- The NetApp AFF controller connects to the Cisco MDS 9132T switches using 32-Gbps Fibre Channel connections for SAN connectivity.
- VMware 7.0 ESXi software is installed on Cisco UCS X210c M6 Compute Nodes to validate the infrastructure.

VLAN configuration

Table 1 lists VLANs configured for setting up the FlexPod environment along with their usage.

Table 1. VLAN usage

VLAN ID	Name	Usage
2	Native-VLAN	Use VLAN 2 as native VLAN instead of default VLAN (1).
3072	OOB-MGMT-VLAN	Out-of-band management VLAN to connect management ports for various devices
17	IB-MGMT-VLAN	In-band management VLAN utilized for all in-band management connectivity - for example, ESXi hosts, VM management, etc.
172	VM-Traffic	VM data traffic VLAN
3017	NFS-VLAN	NFS VLAN for mounting datastores in ESXi servers for VMs
3117*	iSCSI-A	iSCSI-A path for boot-from-san traffic
3217*	iSCSI-B	iSCSI-B path for boot-from-san traffic
3317	vMotion	VMware vMotion traffic

* iSCSI VLANs are not required if using FC storage access.

Some of the key highlights of VLAN usage are as follows:

- VLAN 3072 allows customers to manage and access out-of-band management interfaces of various devices.
- VLAN 17 is used for in-band management of VMs, ESXi hosts, and other infrastructure services
- VLAN 3017 provides ESXi hosts access to the NSF datastores hosted on the NetApp Controllers for deploying VMs.
- A pair of iSCSI VLANs (3117 and 3217) is configured to provide access to boot LUNs for ESXi hosts. These VLANs are not needed when configuring Fibre Channel connectivity.

Logical topology

In FlexPod Datacenter deployments, each Cisco UCS server equipped with a Cisco Virtual Interface Card (VIC) is configured for multiple virtual Network Interfaces (vNICs), which appear as standards-compliant PCIe endpoints to the OS. The end-to-end logical connectivity including VLAN/VSAN usage between the server profile for an ESXi host and the storage configuration on NetApp AFF A400 controllers is captured in the following subsections.

Logical topology for IP-based storage access

[Figure 18](#) captures end-to-end connectivity design for IP-based storage access.

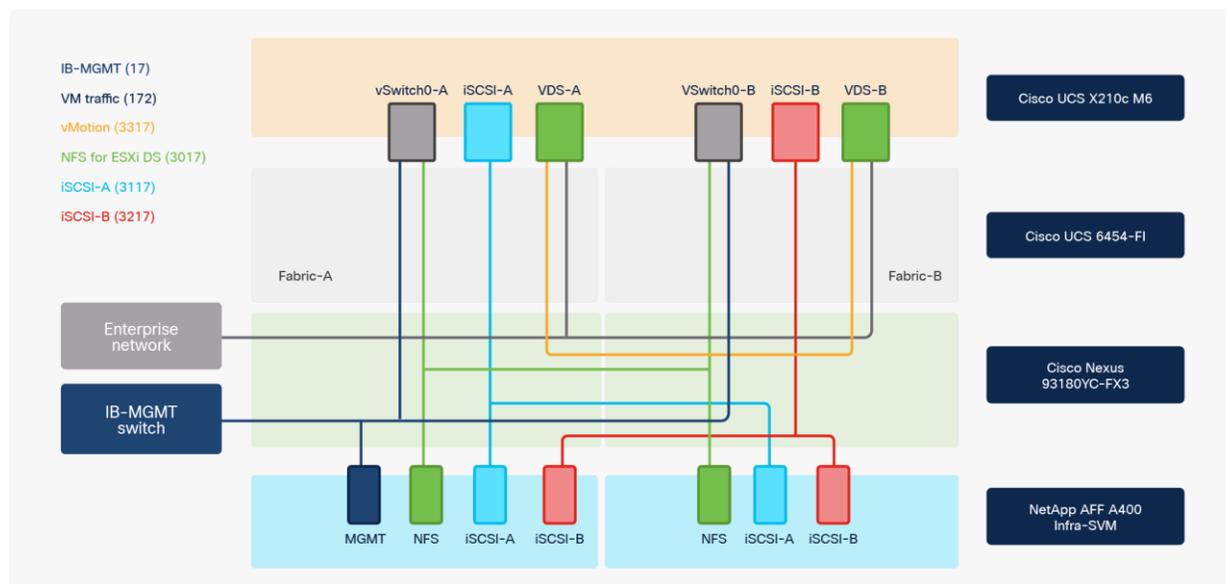


Figure 18.
Logical end-to-end connectivity for iSCSI design

Each ESXi service profile supports:

- Managing the ESXi hosts using a common management segment
- Diskless SAN boot using iSCSI with persistent operating system installation for true stateless computing
- Six vNICs where:
 - Two redundant vNICs (vSwitch0-A and vSwitch0-B) carry management and infrastructure NFS traffic. The MTU value for these vNICs is set as a Jumbo MTU (9000).
 - Two redundant vNICs (VDS-A and VDS-B) are used by the vSphere Distributed switch and carry VMware vMotion traffic and customer application data traffic. The MTU for the vNICs is set to Jumbo MTU (9000).
 - One iSCSI-A vNIC used by iSCSI-A vSwitch to provide access to iSCSI-A path. The MTU value for the vNIC is set to Jumbo MTU (9000).
 - One iSCSI-B vNIC used by iSCSI-B vSwitch to provide access to iSCSI-B path. The MTU value for this vNIC is set to Jumbo MTU (9000).

-
- Each ESXi host (compute node) mounts VM datastores from NetApp AFF A400 controllers using NFS for deploying virtual machines.

Logical topology for FC-based storage access

Figure 19 captures the end-to-end connectivity design for FC-based storage access.

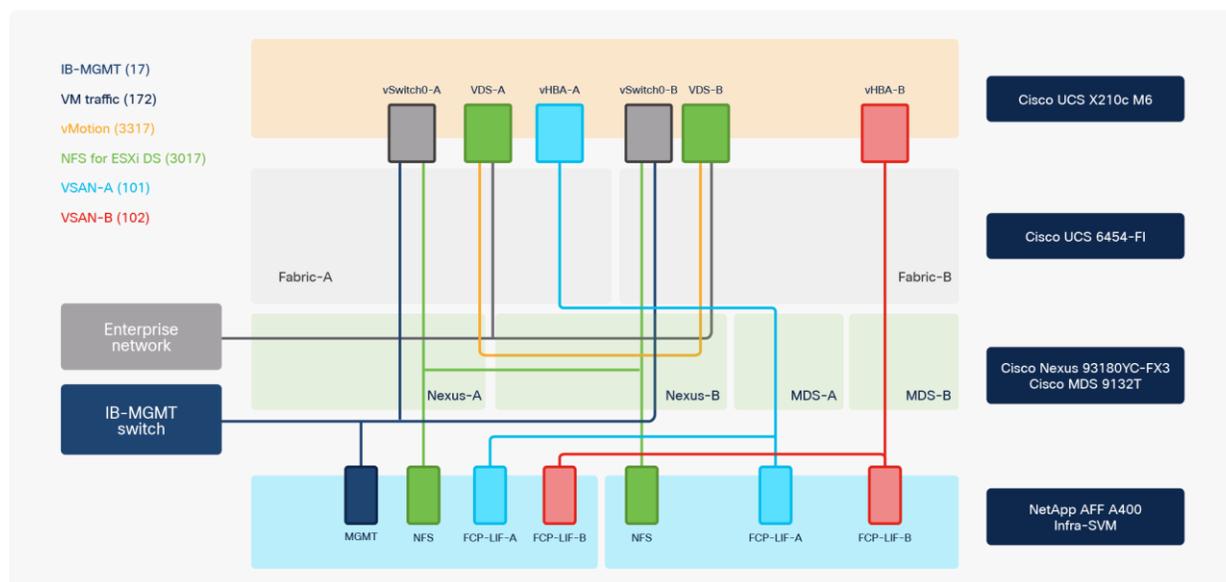


Figure 19.
Logical end-to-end connectivity for FC design

Each ESXi service profile supports:

- Managing the ESXi hosts using a common management segment
- Diskless SAN boot using FC with persistent operating system installation for true stateless computing
- Four vNICs where:
 - Two redundant vNICs (vSwitch0-A and vSwitch0-B) carry in-band management, and Infrastructure NFS VLANs. The MTU value for these vNICs is set as a Jumbo MTU (9000).
 - Two redundant vNICs (VDS-A and VDS-B) are used by the vSphere Distributed switch and carry VMware vMotion traffic and customer application data traffic. The MTU for the vNICs is set to Jumbo MTU (9000).
 - One vHBA defined on Fabric A to provide access to SAN-A path.
 - One vHBA defined on Fabric B to provide access to SAN-B path.
- Each ESXi host (blade) mounts VM datastores from NetApp AFF A400 controllers using NFS for deploying virtual machines.

Compute system connectivity

The Cisco UCS X9508 Chassis is equipped with the Cisco UCSX 9108-25G intelligent fabric modules (IFMs). The Cisco UCS X9508 Chassis connects to each Cisco UCS 6454 FI using four 25GE ports, as shown in [Figure 20](#). If the customers require more bandwidth, all eight ports on the IFMs can be connected to each FI.

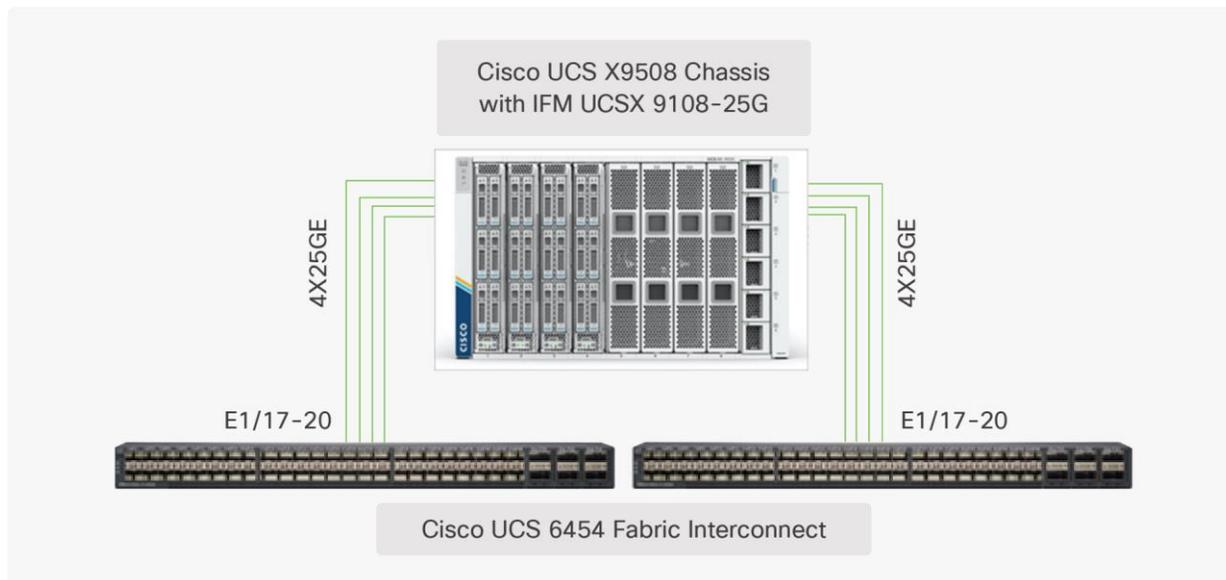


Figure 20.
Cisco UCS X9508 Chassis connectivity to Cisco UCS Fabric Interconnects

Cisco Nexus Ethernet connectivity

The Cisco Nexus 93180YC-FX3 device configuration covers the core networking requirements for Layer 2 and Layer 3 communication. Some of the key NX-OS features implemented within the design are:

- Feature interface-vans - Allows for VLAN IP interfaces to be configured within the switch as gateways.
- Feature HSRP - Allows for Hot Standby Routing Protocol configuration for high availability.
- Feature LACP - Allows for the utilization of Link Aggregation Control Protocol (802.3ad) by the port channels configured on the switch.
- Feature VPC - Virtual Port-Channel (vPC) presents the two Nexus switches as a single “logical” port channel to the connecting upstream or downstream device.
- Feature LLDP - Link Layer Discovery Protocol (LLDP), a vendor-neutral device discovery protocol, allows the discovery of both Cisco devices and devices from other sources.
- Feature NX-API - NX-API improves the accessibility of CLI by making it available outside of the switch by using HTTP/HTTPS. This feature helps with configuring the Cisco Nexus switch remotely using the automation framework.
- Feature UDLD: to enable unidirectional link detection for various interfaces

Cisco UCS Fabric Interconnect 6454 Ethernet connectivity

Cisco UCS 6454 FIs are connected to Cisco Nexus 93180YC-FX3 switches using 100GE connections configured as virtual port channels. Each FI is connected to both Cisco Nexus switches using a 100G connection; additional links can easily be added to the port channel to increase the bandwidth as needed.

[Figure 21](#) covers the physical connectivity details.

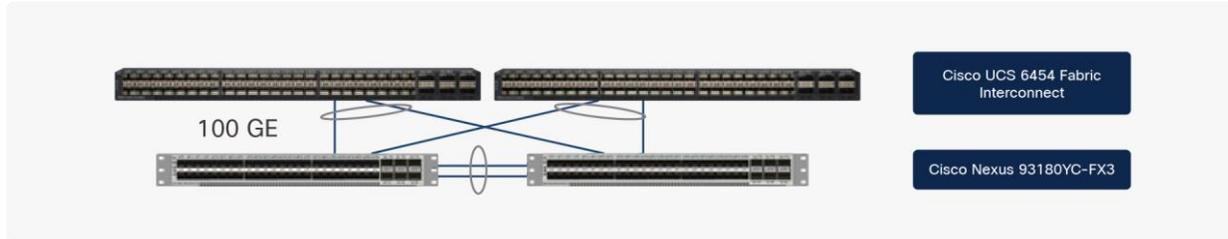


Figure 21.
Cisco UCS 6454 FI SAN connectivity

NetApp AFF A400 Ethernet connectivity

NetApp AFF A400 controllers are connected to Cisco Nexus 93180YC-FX3 switches using 25GE connections configured as virtual port channels. The storage controllers are deployed in a switchless cluster configuration and are connected to each other using the 100GE ports e3a and e3b. [Figure 22](#) illustrates the physical connectivity details.

Note: In [Figure 22](#), the two storage controllers in the high-availability pair are drawn separately for clarity. Physically, the two controllers exist within a single chassis.

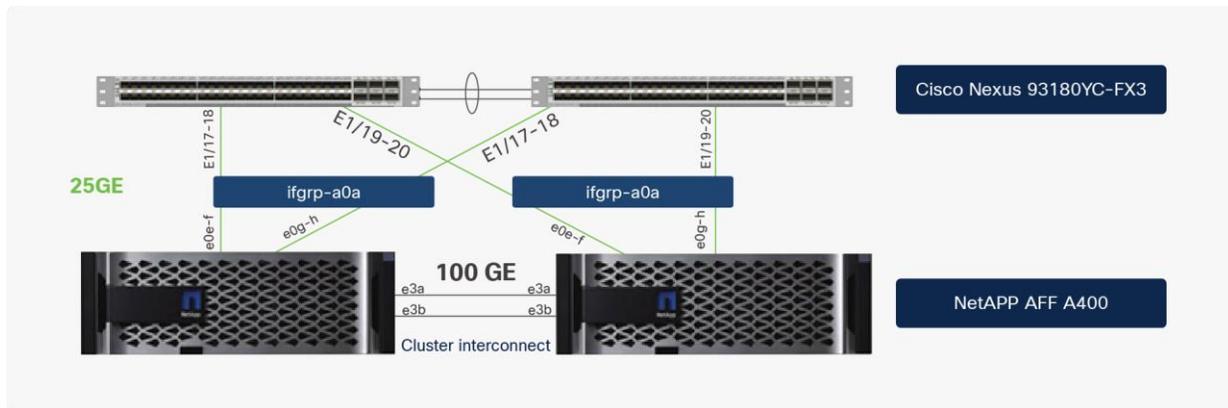


Figure 22.
NetApp AFF A400 IP

Cisco MDS SAN connectivity – Fibre Channel design only

The Cisco MDS 9132T is the key design component bringing together the 32Gbps Fibre Channel (FC) capabilities to the FlexPod design. A redundant 32 Gbps Fibre Channel SAN configuration is deployed utilizing two MDS 9132Ts switches. Some of the key MDS features implemented within the design are:

- Feature NPIV – N port identifier virtualization (NPIV) provides a means to assign multiple FC IDs to a single N port.
- Feature fport-channel-trunk – F-port-channel-trunks allow for the fabric logins from the NPV switch to be virtualized over the port channel. This provides nondisruptive redundancy should individual member links fail.
- Smart-Zoning – a feature that reduces the number of TCAM entries by identifying the initiators and targets in the environment

Cisco UCS Fabric Interconnect 6454 SAN connectivity

For SAN connectivity, each Cisco UCS 6454 Fabric Interconnect is connected to a Cisco MDS 9132T SAN switch using 2 x 32G Fibre Channel port-channel connection, as shown in [Figure 23](#):

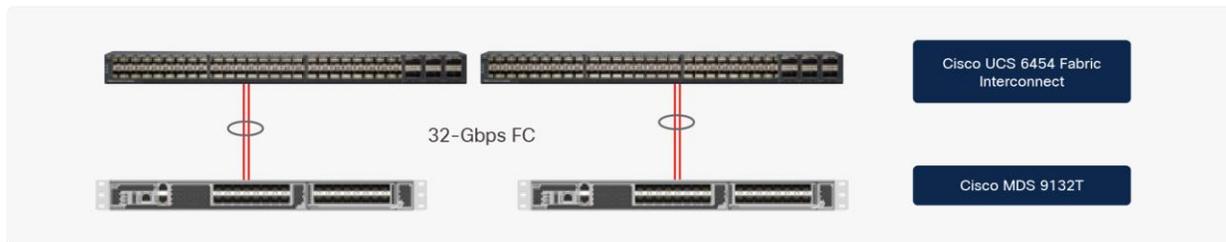


Figure 23.
Cisco UCS 6454 FI SAN connectivity

NetApp AFF A400 SAN connectivity

For SAN connectivity, each NetApp AFF A400 controller is connected to both of Cisco MDS 9132T SAN switches using 32G Fibre Channel connections, as shown in [Figure 24](#):

Note: In [Figure 24](#), the two storage controllers in the high-availability pair are drawn separately for clarity. Physically, the two controllers exist within a single chassis.

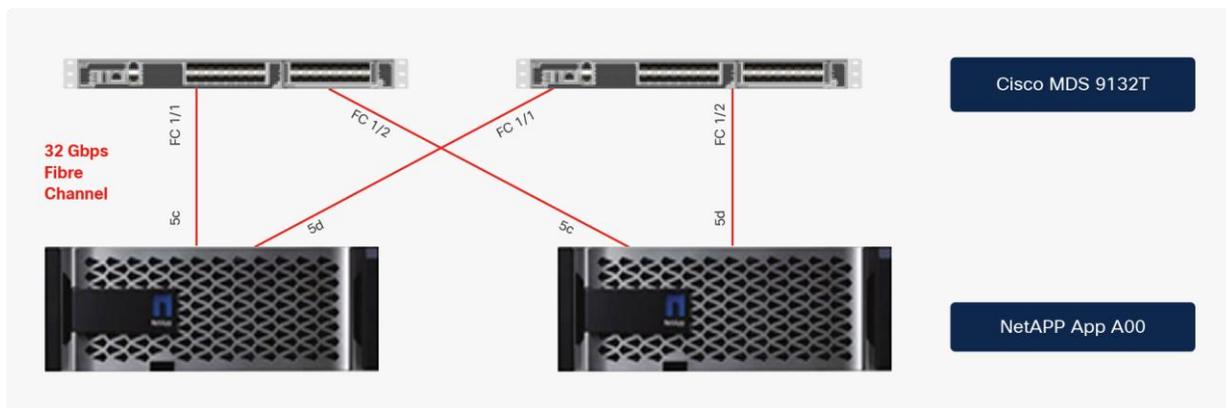


Figure 24.
NetApp AFF A400 SAN connectivity

Cisco UCS X-Series configuration - Cisco Intersight Managed Mode

Cisco Intersight Managed Mode standardizes policy and operation management for Cisco UCS X-Series. The compute nodes in Cisco UCS X-Series are configured using server profiles defined in Cisco Intersight. These server profiles derive all the server characteristics from various policies and templates. At a high level, configuring Cisco UCS using Intersight Managed Mode consists of the steps shown in [Figure 25](#).

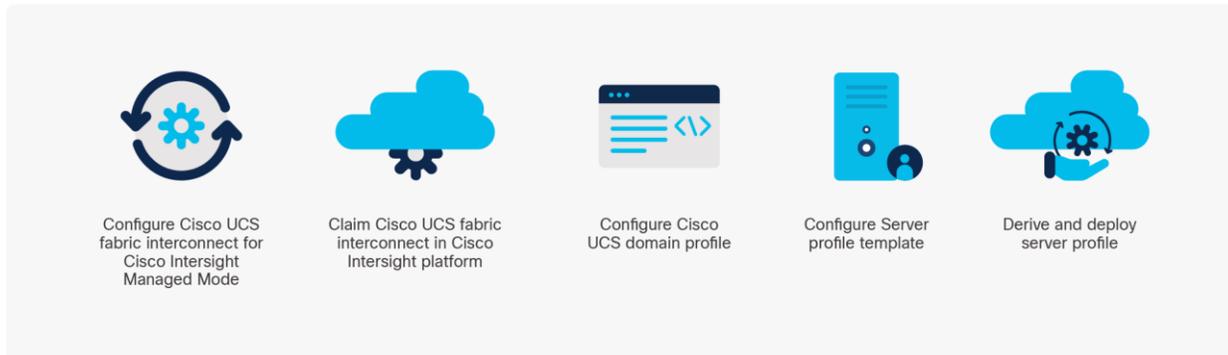


Figure 25.
Configuration steps for Cisco Intersight Managed Mode

Setting up Cisco UCS Fabric Interconnect for Cisco Intersight Managed Mode

During the initial configuration, for the management mode the configuration wizard enables customers to choose whether to manage the fabric interconnect through Cisco UCS Manager or the Cisco Intersight platform. Customers can switch the management mode for the fabric interconnects between Cisco Intersight and Cisco UCS Manager at any time; however, Cisco UCS FIs must be set up in Intersight Managed Mode (IMM) for configuring the Cisco UCS X-Series system. [Figure 26](#) shows the dialog during initial configuration of Cisco UCS FIs for setting up IMM.

```
UCSM image signature verification successful

---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the Fabric interconnect and its clustering mode is performed through these steps.

Type Ctrl-C at any time to abort configuration and reboot system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.

Enter the configuration method. (console/gui) ? console

Enter the management mode. (ucsm/intersight)? intersight

You have chosen to setup a new Fabric interconnect in "intersight" managed mode. Continue? (y/n): y

Enforce strong password? (y/n) [y]:
```

Figure 26.
Fabric Interconnect setup for Cisco Intersight Managed Mode

Claiming a Cisco UCS fabric interconnect in the Cisco Intersight platform

After setting up the Cisco UCS fabric interconnect for Cisco Intersight Managed Mode, FIs can be claimed to a new or an existing Cisco Intersight account. When a Cisco UCS fabric interconnect is successfully added to the Cisco Intersight platform, all future configuration steps are completed in the Cisco Intersight portal.

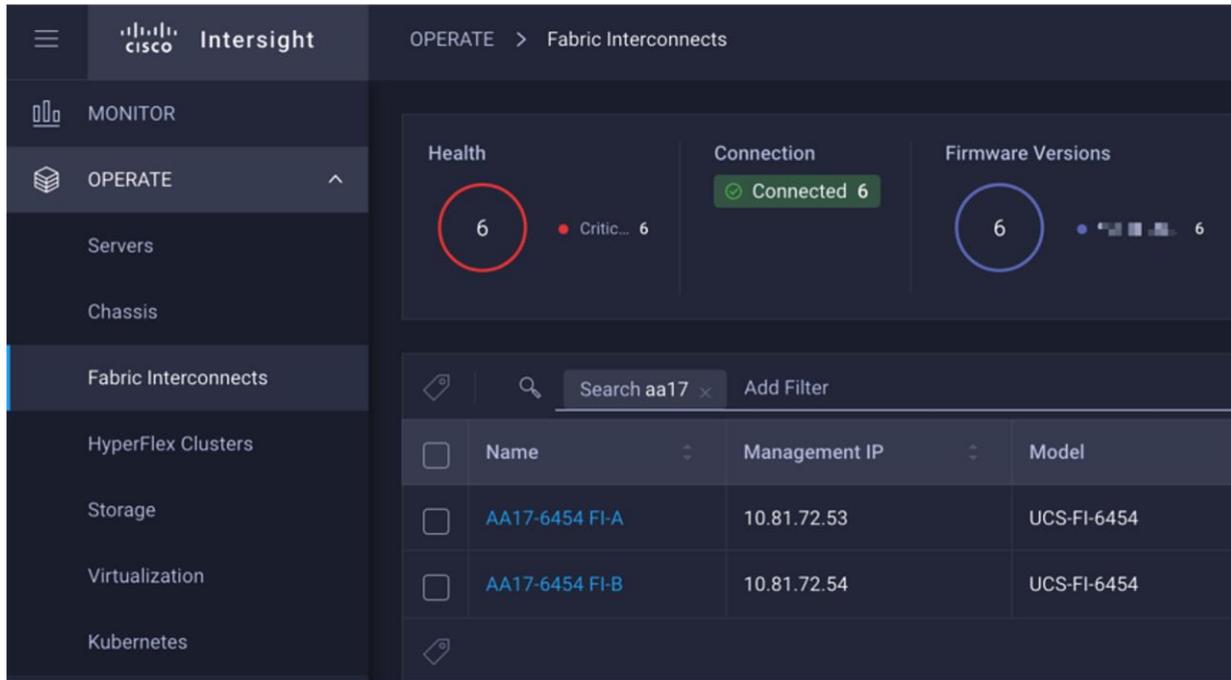


Figure 27.
Cisco Intersight: adding fabric interconnects as targets

Customers can verify whether a Cisco UCS fabric interconnect is in Cisco UCS Manager managed mode or Cisco Intersight Managed Mode by clicking on the fabric interconnect name and looking at the detailed information screen for the FI, as shown in [Figure 28](#).

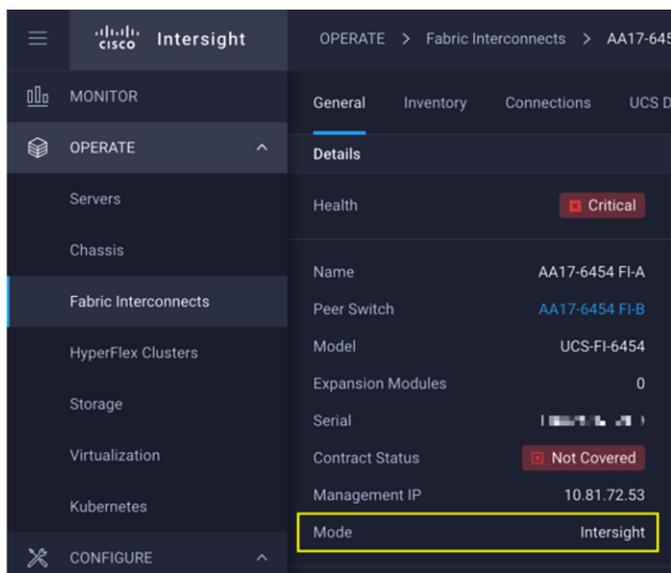


Figure 28.
Cisco UCS FI in Intersight Managed Mode

Cisco UCS domain profile

A Cisco UCS domain profile configures a fabric interconnect pair through reusable policies, allows configuration of the ports and port channels, and configures the VLANs and VSANs to be used in the network. It defines the characteristics of and configures the ports on the fabric interconnects. One Cisco UCS domain profile can be assigned to one fabric interconnect domain, and the Cisco Intersight platform supports the attachment of one port policy per Cisco UCS domain profile.

Some of the characteristics of the Cisco UCS domain profile in the FlexPod environment are:

- A single domain profile is created for the pair of Cisco UCS fabric interconnects.
- Unique port policies are defined for the two fabric interconnects.
- The VLAN configuration policy is common to the fabric interconnect pair because both fabric interconnects are configured for same set of VLANs.
- The VSAN configuration policies (FC connectivity option) are unique for the two fabric interconnects because the VSANs are unique.
- The Network Time Protocol (NTP), network connectivity, and system Quality-of-Service (QoS) policies are common to the fabric interconnect pair.

After the Cisco UCS domain profile has been successfully created and deployed, the policies including the port policies are pushed to Cisco UCS fabric interconnects. Cisco UCS domain profile can easily be cloned to install additional UCS systems. When cloning the UCS domain profile, the new UCS domains utilize the existing policies for consistent deployment of additional UCS systems at scale.

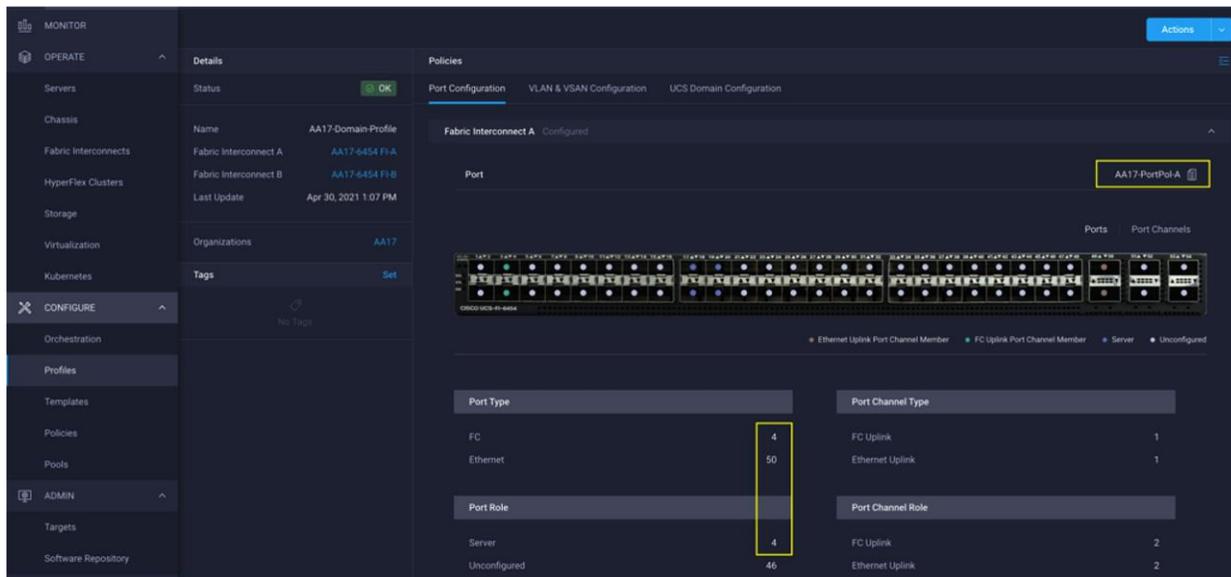


Figure 29.
Cisco UCS domain profile

The Cisco UCS X9508 Chassis and Cisco UCS X210c M6 Compute Nodes are automatically discovered when the ports are successfully configured using the domain profile as shown in [Figure 30](#), [Figure 31](#), and [Figure 32](#).

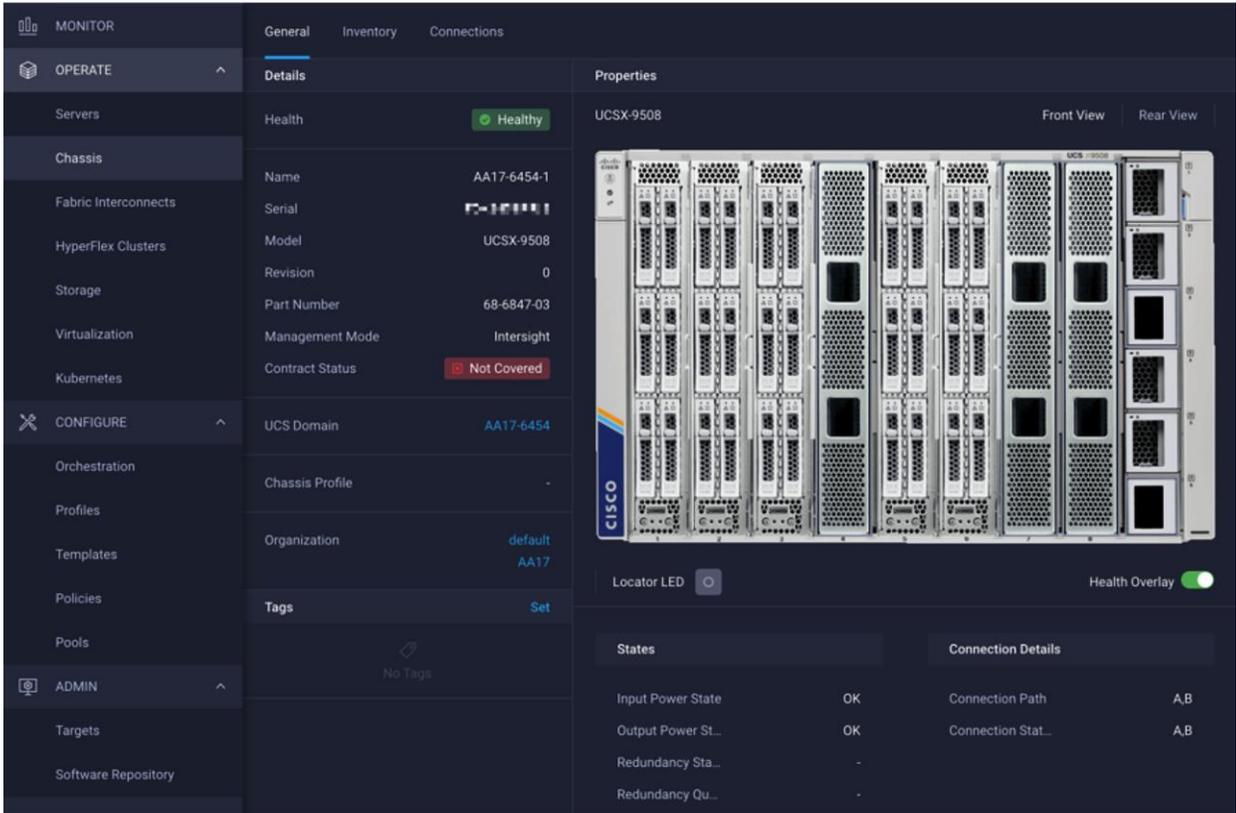


Figure 30.
Cisco UCS X9508 Chassis front view

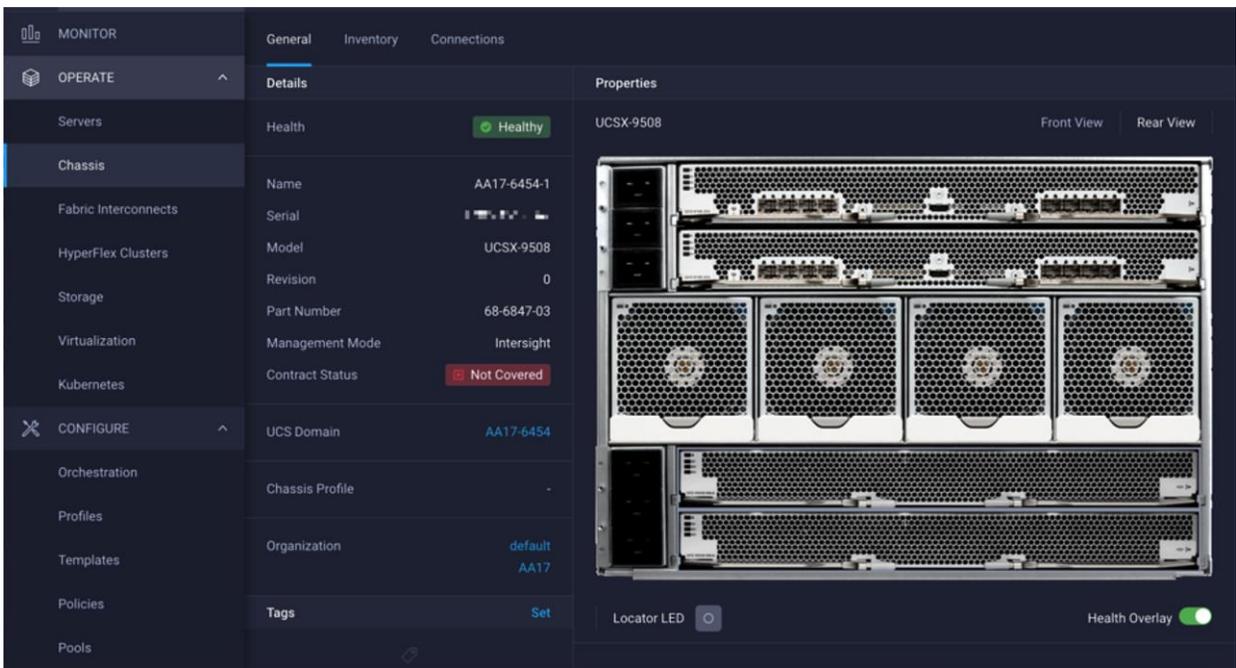


Figure 31.
Cisco UCS X9508 Chassis rear view

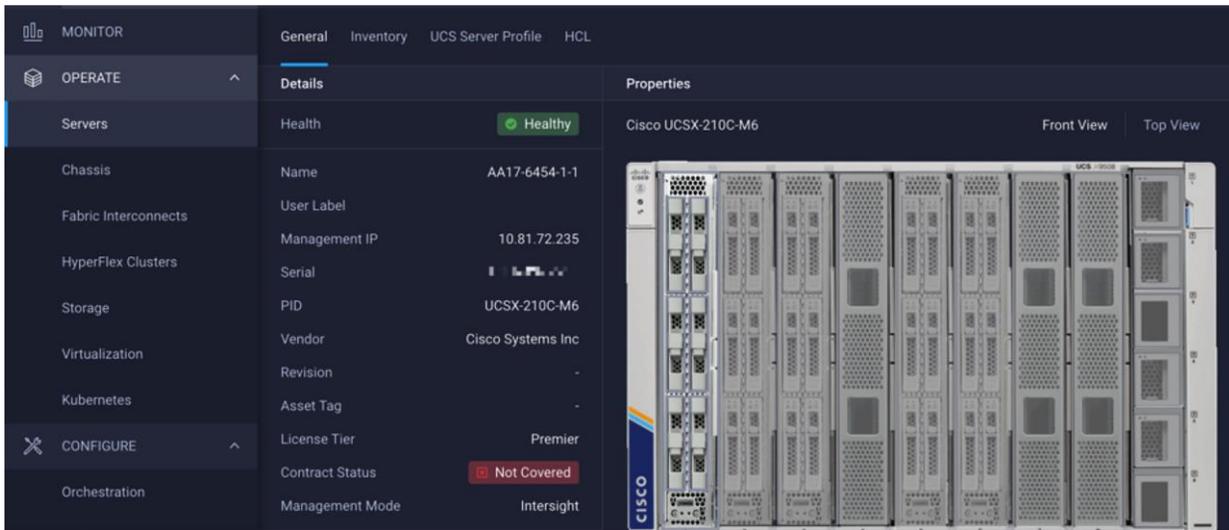


Figure 32.
Cisco UCS X210c M6 Compute Nodes

Server profile template

A server profile template enables resource management by simplifying policy alignment and server configuration. A server profile template is created using the server profile template wizard. The server profile template wizard groups the server policies into the following four categories to provide a quick summary view of the policies that are attached to a profile:

- Compute policies: BIOS, boot order, and virtual media policies
- Network policies: adapter configuration, LAN connectivity, and SAN connectivity policies
 - The LAN connectivity policy requires you to create Ethernet network policy, Ethernet adapter policy, and Ethernet QoS policy.
 - The SAN connectivity policy requires you to create Fibre Channel (FC) network policy, Fibre Channel adapter policy, and Fibre Channel QoS policy. SAN connectivity policy is only required for the FC connectivity option.
- Storage policies: not used in FlexPod
- Management policies: device connector, Intelligent Platform Management Interface (IPMI) over LAN, Lightweight Directory Access Protocol (LDAP), local user, network connectivity, Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP), Secure Shell (SSH), Serial over LAN (SOL), syslog, and virtual Keyboard, Video, and Mouse (KVM) policies

Some of the characteristics of the server profile template for FlexPod are as follows:

- BIOS policy is created to specify various server parameters in accordance with FlexPod best practices.
- Boot order policy defines virtual media (KVM mapper DVD), all SAN paths for NetApp iSCSI or Fibre Channel logical interfaces (LIFs), and UEFI Shell.
- IMC access policy defines the management IP address pool for KVM access.
- Local user policy is used to enable KVM-based user access.
- For the iSCSI boot from SAN configuration, LAN connectivity policy is used to create six virtual network interface cards (vNICs) – two for management virtual switch (vSwitch0), two for application Virtual Distributed Switch (VDS), and one each for iSCSI A/B vSwitches. Various policies and pools are also created for the vNIC configuration.
- For the FC boot from SAN configuration, LAN connectivity policy is used to create four virtual network interface cards (vNICs) – two for management virtual switches (vSwitch0) and two for application Virtual Distributed Switch (VDS) – along with various policies and pools.
- For the FC connectivity option, SAN connectivity policy is used to create two virtual host bus adapters (vHBAs) – one for SAN A and one for SAN B – along with various policies and pools. The SAN connectivity policy is not required for iSCSI setup.

Figure 33 shows various policies associated with the server profile template.

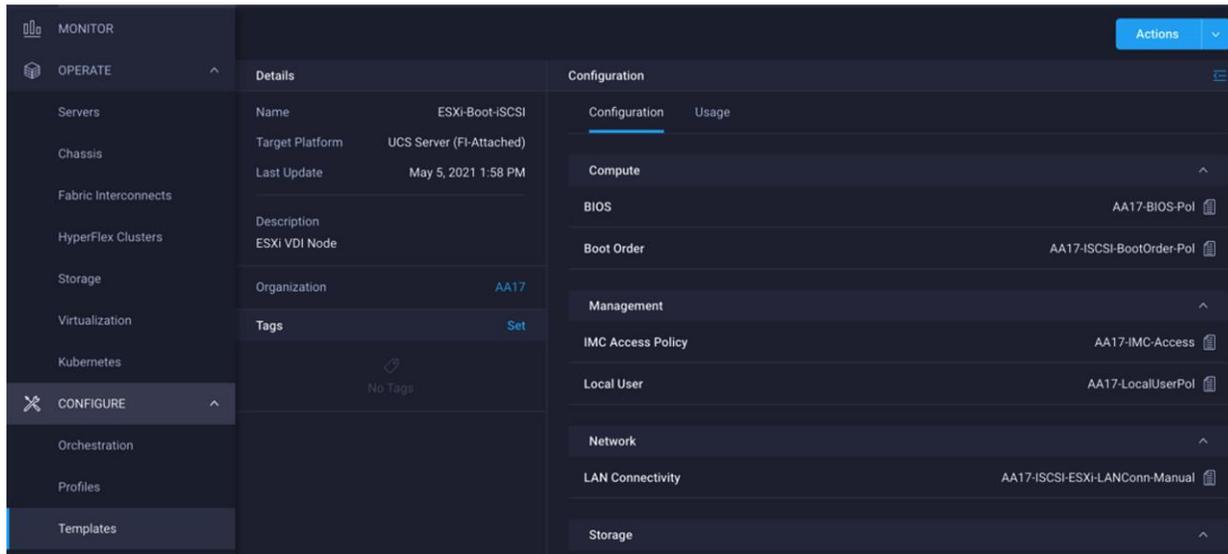


Figure 33. Server profile template for iSCSI boot from SAN

Derive and deploy server profiles from the Cisco Intersight server profile template

The Cisco Intersight server profile allows server configurations to be deployed directly on the compute nodes based on policies defined in the server profile template. After a server profile template has been successfully created, server profiles can be derived from the template and associated with the Cisco UCS X210c M6 Compute Nodes, as shown in [Figure 34](#).

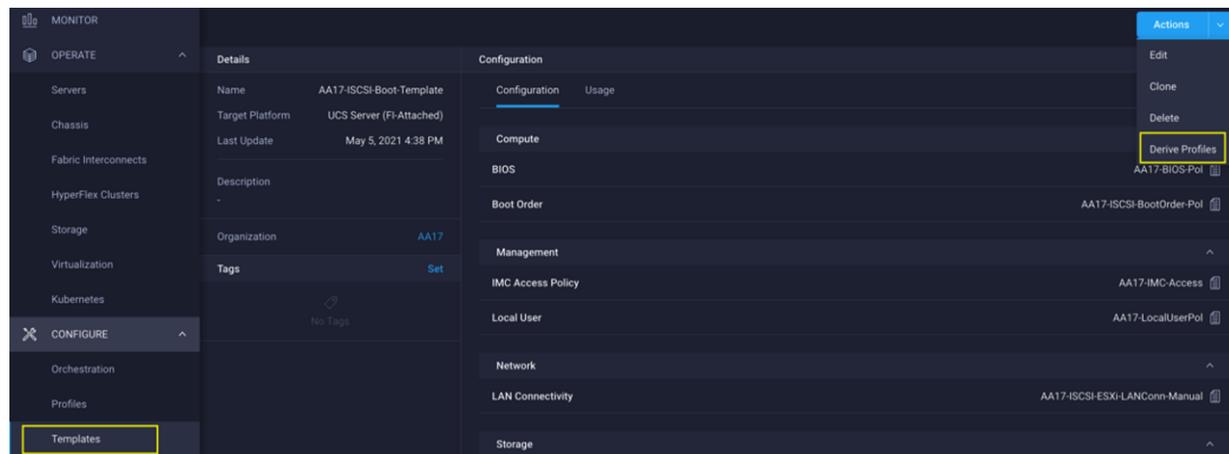


Figure 34.

Deriving a server profile from Templates

On successful deployment of the server profile, the Cisco UCS X210c M6 Compute Nodes are configured with parameters defined in the server profile and can boot from the storage LUN hosted on NetApp AFF A400.

NetApp AFF A400 – Server Virtual Machine (SVM) design

To provide the necessary data segregation and management, a dedicated SVM, Infra-SVM, is created for hosting the VMware environment. The SVM contains the following volumes and logical interfaces (LIFs):

- Volumes
 - ESXi boot LUNs used to enable ESXi host boot from SAN functionality using iSCSI or FC
 - Infrastructure datastore(s) used by the vSphere environment to store the VMs
- Logical interfaces (LIFs)
 - NFS LIFs to mount NFS datastores in the vSphere environment
 - iSCSI A/B LIFs for iSCSI traffic

or

- FC LIFs for supporting FC SAN traffic

Details on volumes, VLANs, and logical interfaces (LIFs) are shown in [Figure 35](#) and [Figure 36](#), below, for iSCSI and FC connectivity, respectively.

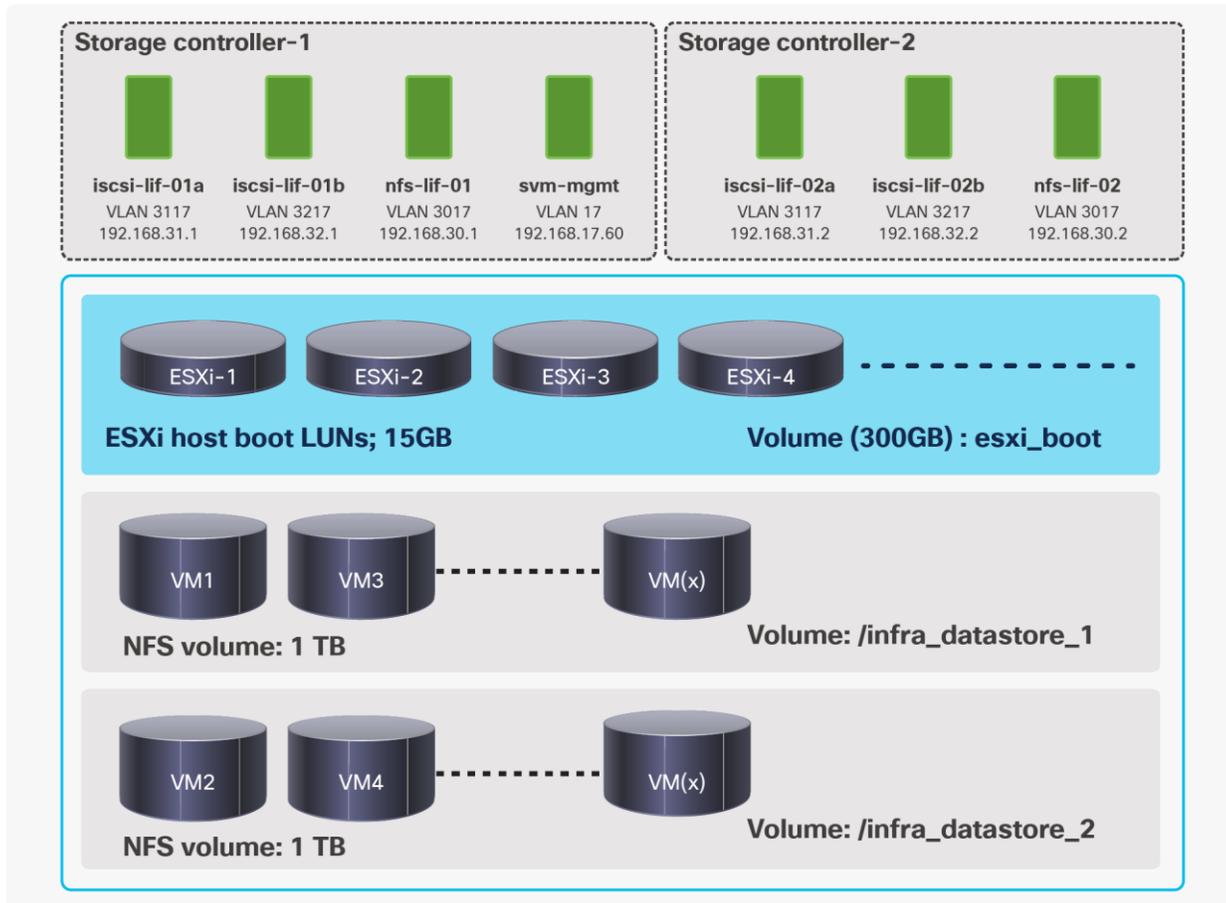


Figure 35.
NetApp AFF A400 – Infra-SVM for iSCSI boot

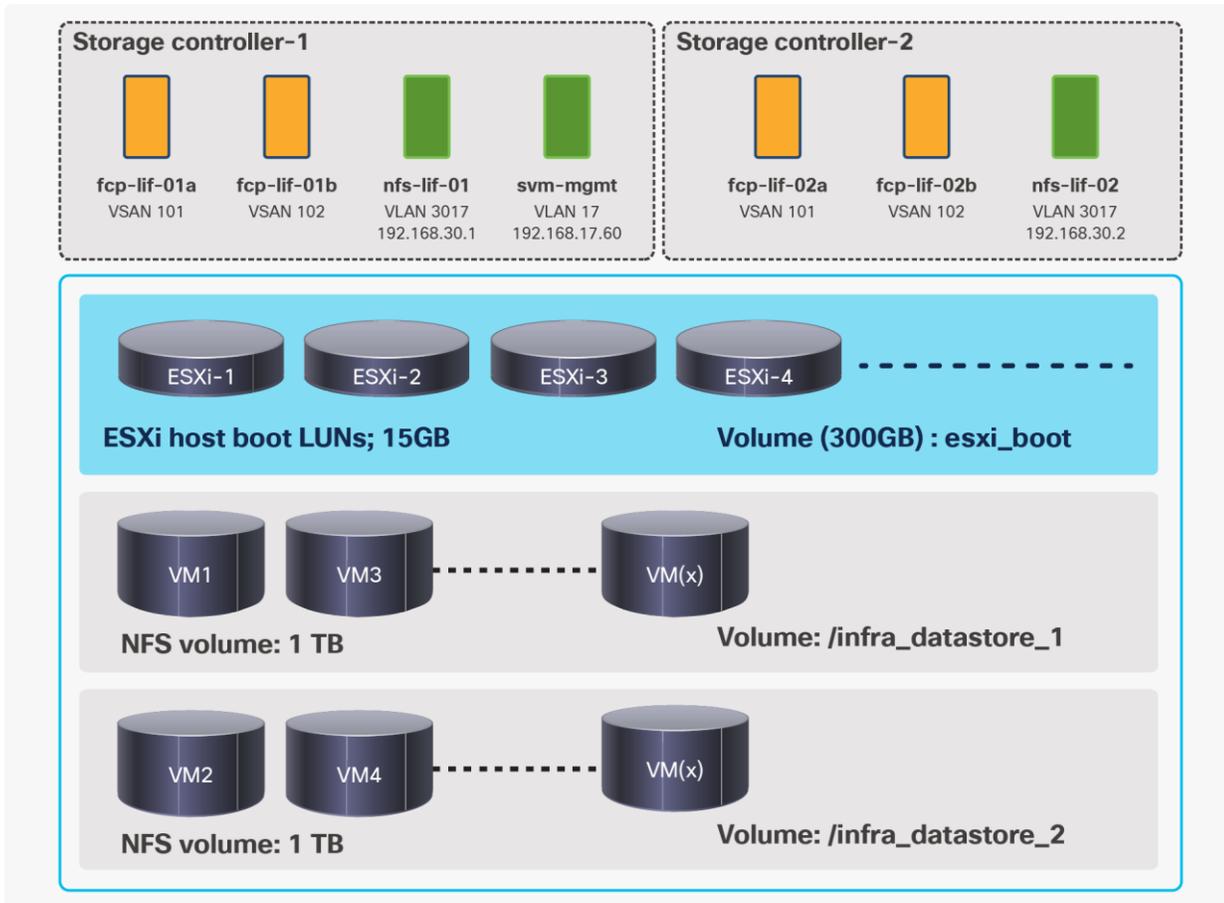


Figure 36.
NetApp AFF A400 – Infra-SVM for FC boot

VMware vSphere - ESXi design

Multiple vNICs (and vHBAs) are created for the ESXi hosts using the Cisco Intersight server profile and are then assigned to specific virtual and distributed switches. The vNIC and (optional) vHBA distribution for the ESXi hosts is as follows:

- Two vNICs (one on each fabric) for vSwitch0 to support core services such as management and NFS traffic.
- Two vNICs (one on each fabric) for vSphere Virtual Distributed Switch (VDS) to support customer data traffic and vMotion traffic.
- One vNIC each for Fabric-A and Fabric-B for iSCSI stateless boot. These vNICs are only required when iSCSI boot from SAN configuration is desired.
- One vHBA each for Fabric-A and Fabric-B for FC stateless boot. These vHBAs are only required when FC connectivity is desired.

Note: Typically, customers will either have iSCSI vNICs or the FC vHBAs configured for stateless boot from SAN of the ESXi servers.

Figure 37 and Figure 38 show the ESXi vNIC configurations in detail.

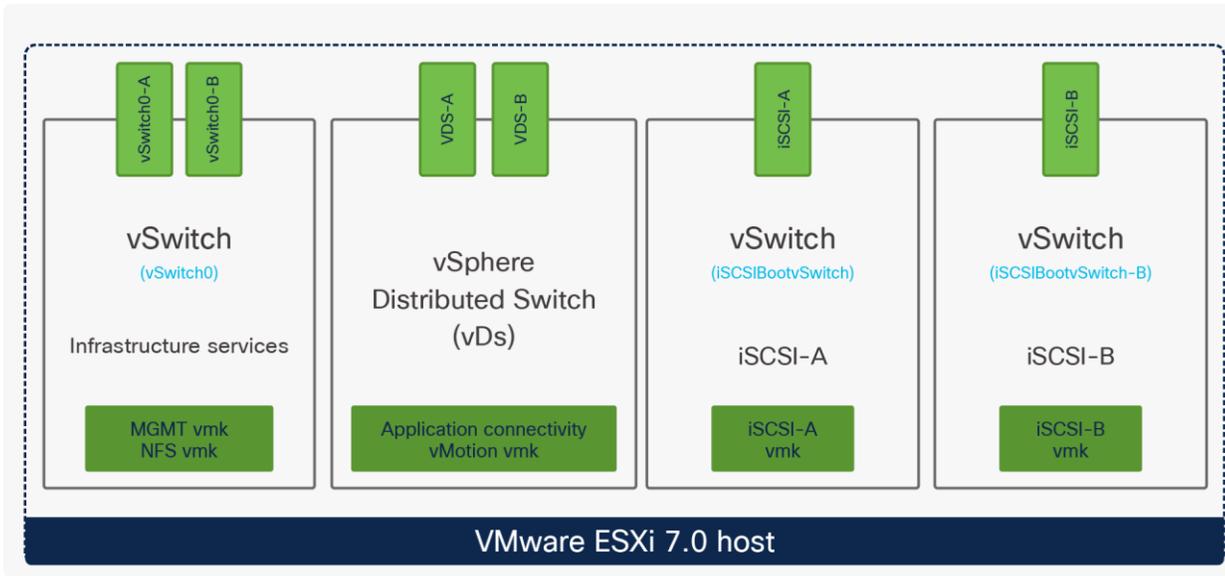


Figure 37.
VMware vSphere - ESXi host networking for iSCSI boot from SAN

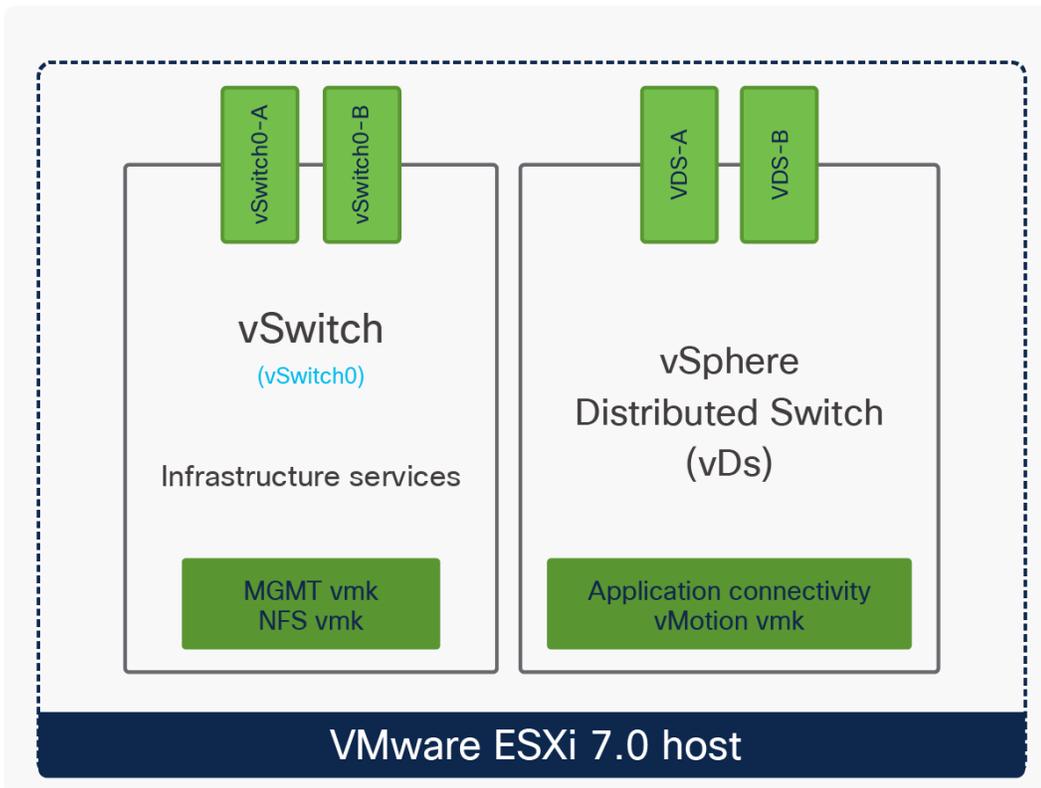


Figure 38.
VMware vSphere - ESXi host networking for FC boot from SAN

Cisco Intersight Integration with VMware vCenter and NetApp storage

Cisco Intersight works with NetApp's ONTAP storage and VMware vCenter using third-party device connectors. Since third-party infrastructure does not contain any built-in Intersight device connector, Cisco Intersight Assist virtual appliance enables Cisco Intersight to communicate with non-Cisco devices.

Note: A single Cisco Intersight Assist virtual appliance can support both NetApp ONTAP storage and VMware vCenter.

Cisco Intersight integration with VMware vCenter and NetApp ONTAP enables customers to perform following tasks right from the Intersight dashboard:

- Monitor the virtualization and storage environment.
- Add various dashboard widgets to obtain useful at-a-glance information.
- Perform common Virtual Machine tasks such as power on/off, remote console etc.
- Orchestrate virtual and storage environment to perform common configuration tasks.
- Orchestrate NetApp ONTAP storage tasks to setup a Storage Virtual Machine and provide NAS and SAN services.

The sections below cover the details of these operations. Since Cisco Intersight is a SaaS platform, the monitoring and orchestration capabilities are constantly being added and delivered seamlessly from the cloud.

Note: The monitoring capabilities and orchestration tasks and workflows listed below provide just an in-time snapshot for your reference. For the most up to date list of capabilities and features, customers should use the help and search capabilities in Cisco Intersight.

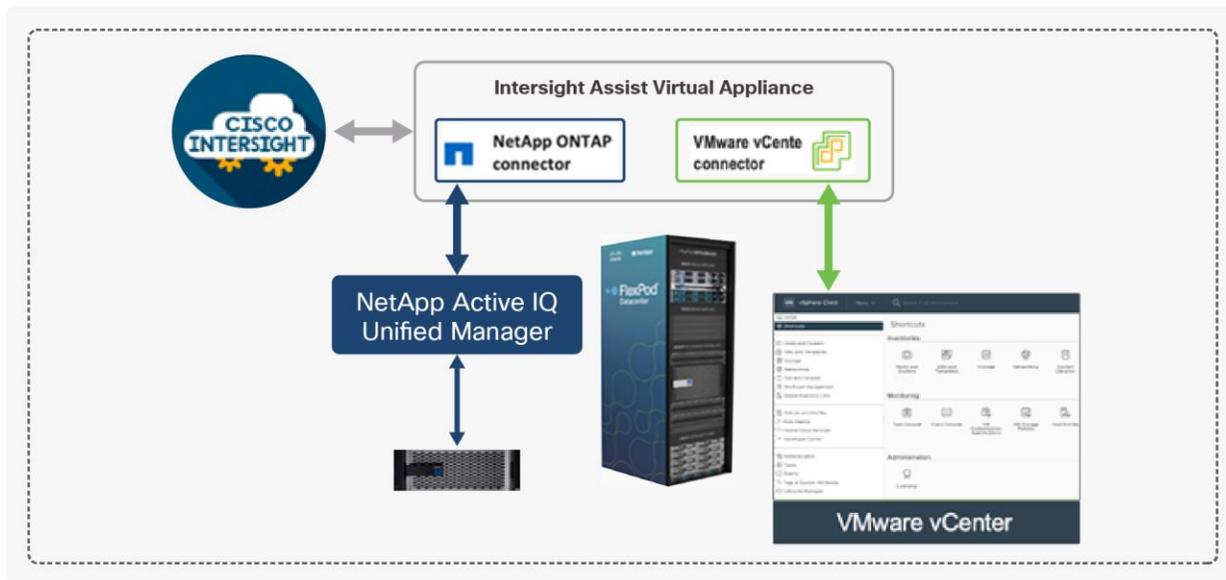


Figure 39.
Managing NetApp and VMware vCenter through Cisco Intersight using Intersight Assist

Licensing requirement

To integrate and view various NetApp storage and VMware vCenter parameters from Cisco Intersight, a Cisco Intersight Advantage license is required. To use Cisco Intersight orchestration and workflows to provision the storage and virtual environments, an Intersight Premier license is required.

Integrating Cisco Intersight with NetApp ONTAP storage

To integrate NetApp AFF A400 with Cisco Intersight, customers need to deploy:

- Cisco Intersight Assist virtual appliance
- NetApp Active IQ Unified Manager virtual appliance

Using the Cisco Intersight Assist, NetApp Active IQ Unified Manager is claimed as a target in Cisco Intersight, as shown in [Figure 40](#).

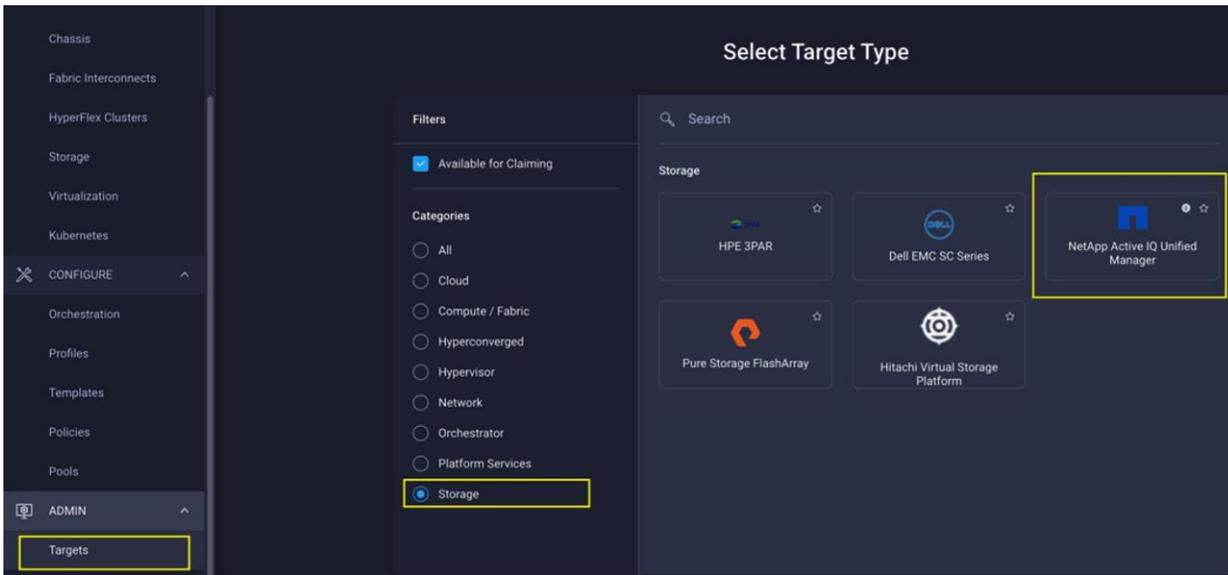


Figure 40.
Claiming NetApp Active IQ Unified Manager as a target in Cisco Intersight

Obtaining storage-level information

After successfully claiming the NetApp Active IQ Unified Manager as a target, customers can view storage-level information in Cisco Intersight if they have already added NetApp AFF A400 to the NetApp Active IQ Unified Manager.

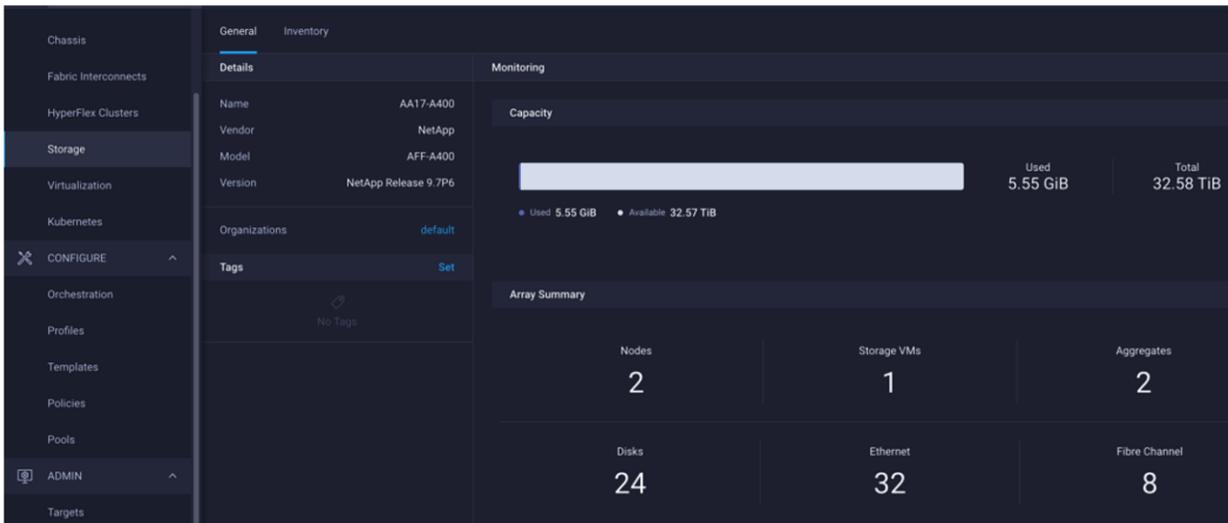


Figure 41.
NetApp AFF A400 information in Cisco Intersight

Table 2 lists some of the core NetApp AFF A400 information presented through Cisco Intersight.

Table 2. NetApp Storage information in Cisco Intersight

Category	Name	Details
General	Name	Name of the controller
	Vendor	NetApp
	Model	NetApp AFF model information (for example, AFF-A400)
	Version	Software version
Monitoring	Capacity	Total, used, and available system capacity
		Summary of Nodes, Storage VMs, Aggregates, disks etc. in the system
Inventory	Volumes	Volumes defined in the system and their status, size, usage, and configured export policies
	LUNs	LUNs defined in the system and their status, size, usage, and mapped iGroups
	Aggregates	Configured aggregates and their status, size, usage, and space savings
	Storage VMs	Storage VM (SVM) information, state, allowed protocols, and logical ethernet and fibre channel interface details.
	Export policies	Export policies defined in the system and the associated SVMs
	SAN initiator groups	SAN initiator groups, their type, protocol, initiator information, and associated SVMs
	Licenses	Licenses installed on the system
	Nodes	Controller information, such as model, OS, serial number, etc.
	Disks	Disk information, including type, model, size, node information, status of the disks, and aggregate details
	Ports	Ethernet and FC ports configured on the system

Storage widget in the dashboard

Customers can also add the storage dashboard widgets to Cisco Intersight for viewing NetApp AFF A400 information at a glance on the Cisco Intersight dashboard, as shown in [Figure 42](#).

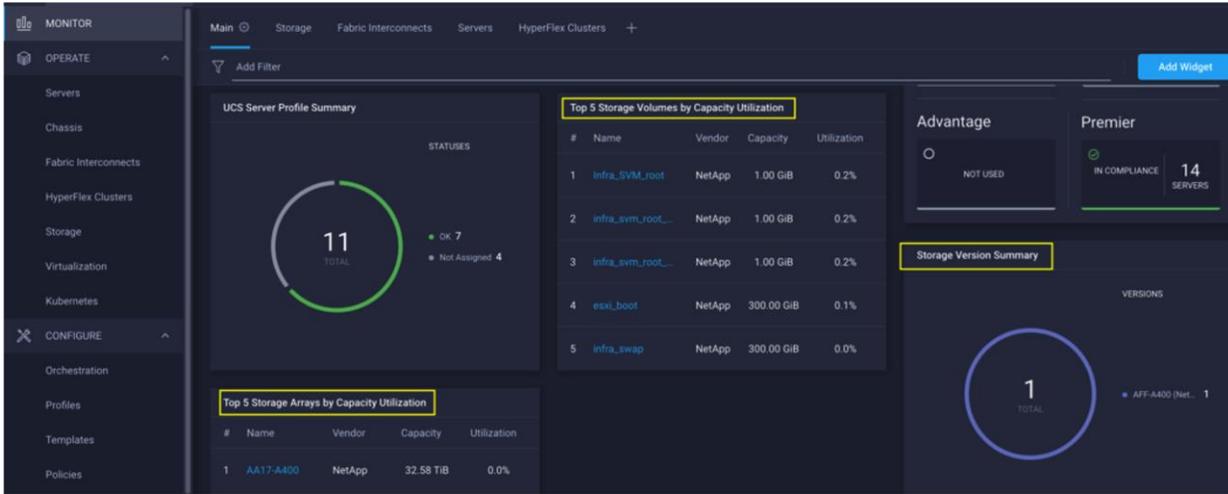


Figure 42.
Storage Widgets in Cisco Intersight Dashboard

These storage widgets provide useful information such as:

- Storage arrays and capacity utilization
- Top-five storage volumes by capacity utilization
- Storage versions summary, providing information about the software version and the number of storage systems running that version

Cisco Intersight Orchestrator - NetApp ONTAP storage

Cisco Intersight Orchestrator provides various workflows that can be used to automate storage provisioning. Some of the sample storage workflows available for NetApp ONTAP storage are listed in Table 3.

Table 3. NetApp ONTAP storage workflows in Cisco Intersight Orchestrator

Name	Details
New NAS datastore	Create a NFS storage volume and build NAS datastore on the volume
New storage export policy	Create a storage export policy and add the created policy to a NFS volume
New storage host	Create a new storage host or iGroup to enable SAN mapping
New storage interface	Create a storage IP or FC interface
New storage virtual machine	Create a storage virtual machine
New VMFS datastore	Create a storage volume and build a Virtual Machine File System (VMFS) datastore on the volume
Remove NAS datastore	Remove the NAS datastore and the underlying NFS storage volume

Name	Details
Remove storage export policy	Remove the NFS volume and the export policy attached to the volume
Remove storage host	Remove a storage host. If a host group name is provided as input, the workflow will also remove the host from the host group.
Remove VMFS datastore	Remove a VMFS data store and remove the backing volume from the storage device
Update NAS datastore	Update NAS datastore by expanding capacity of the underlying NFS volume
Update storage host	Update the storage host details. If the inputs for a task are provided, then the task is run; otherwise, it is skipped.
Update VMFS datastore	Expand a datastore on the hypervisor manager by extending the backing storage volume to specified capacity, and then expand the data store to use the additional capacity

In addition to the above workflows, Cisco Intersight Orchestrator also provides a large number of storage and virtualization tasks for customers to create custom workflow based on their specific needs. A sample subset of these tasks are highlighted in [Figure 43](#).

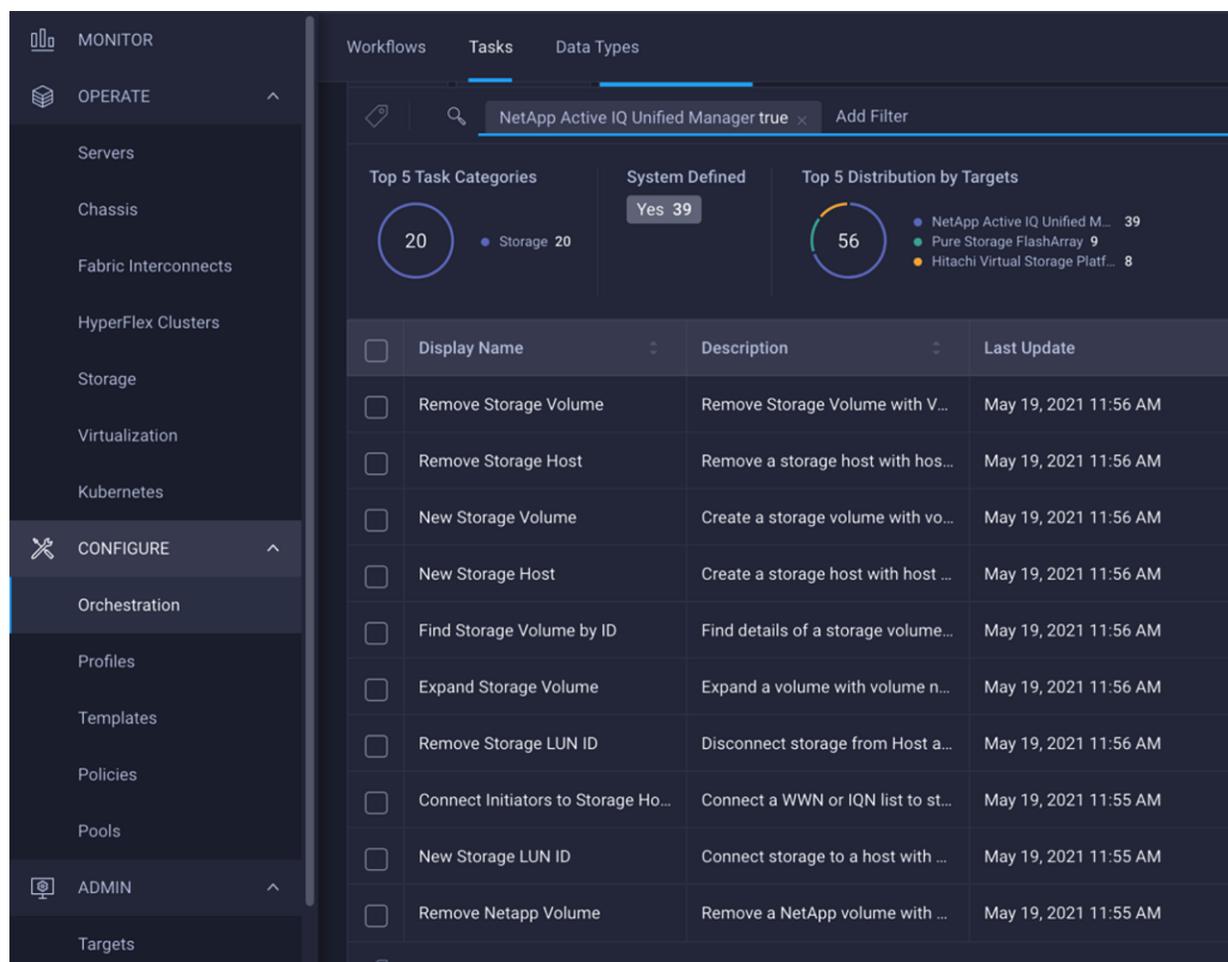


Figure 43.
Storage tasks for NetApp ONTAP

Integrating Cisco Intersight with VMware vCenter

To integrate VMware vCenter with Cisco Intersight, VMware vCenter can be claimed as a target using Cisco Intersight Assist Virtual Appliance, as shown in [Figure 44](#).

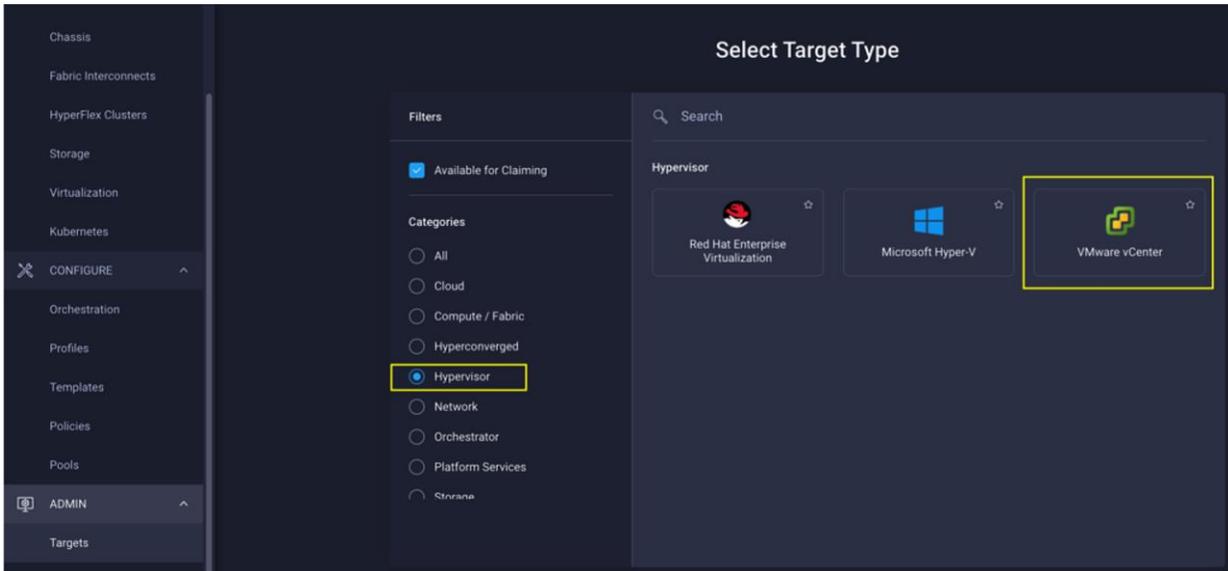


Figure 44.
Claiming VMware vCenter in Cisco Intersight as a target

Obtaining hypervisor-level information

After successfully claiming the VMware vCenter as a target, customers can view hypervisor-level information in Cisco Intersight including hosts, VMs, clusters, datastores, etc.

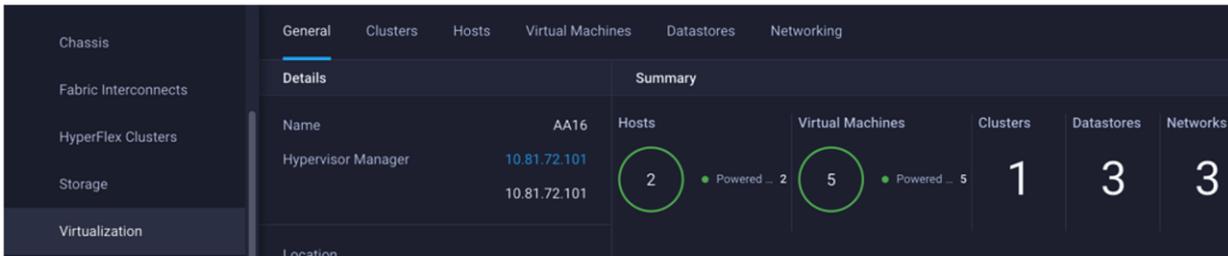


Figure 45.
VMware vCenter information in Cisco Intersight

Table 4 lists some of the main virtualization properties presented in Cisco Intersight.

Table 4. Virtualization (VMware vCenter) information in Cisco Intersight

Category	Name	Details
General	Name	Name of the data center
	Hypervisor manager	Host name or IP address of the vCenter
Clusters	Name	Name of the cluster
	Data center	Name of the data center
	Hypervisor type	ESXi
	Hypervisor manager	vCenter IP address or the host name
	CPU capacity	CPU capacity in the cluster (GHz)
	CPU consumes	CPU cycles consumed by workloads (percentage and GHz)
	Memory capacity	Total memory in the cluster (GB)
	Memory consumed	Memory consumed by workloads (percentage and GB)
	Total cores	All the CPU cores across the CPUs in the cluster
Hosts	Name	Host name or IP address
	Server	Server profile associated with the ESXi host
	Cluster	Cluster information if the host is part of a cluster
	Data center	VMware data center
	Hypervisor type	ESXi
	Hypervisor manager	vCenter IP address of host name
		Host information allows customers to access additional details about clusters, VMs, datastores, and networking related to the current ESXi host.
Virtual machines	Name	Name of the VM
	Guest OS	Operating system, for example, RHEL, CentOS, etc.
	Hypervisor type	ESXi
	Host	ESXi host information for the VM
	Cluster	VMware cluster name
	Data center	VMware data center name

Category	Name	Details
	IP address	IP address(s) assigned to the VM
	Hypervisor manager	IP address of host name of the vCenter
	VM information allows customers to access additional details about clusters, hosts, datastores, networking, and virtual disks related to the current VM.	
Datastores	Name	Name of the datastore in VMware vCenter
	Type	NFS or VMFS etc.
	Accessible	Yes, if datastore is accessible; No, if datastore is inaccessible
	Thin provisioning	Yes, if thin provisioning is allowed; No, if thin provisioning is not allowed
	Multiple host access	Yes, if multiple hosts can mount the datastore; No, if the datastore only allows a single host
	Storage capacity	Space in GB or TB
	Storage consumes	Percentage and GB
	Data center	Name of VMware vCenter data center
	Hypervisor manager	vCenter hostname or IP address
	Datastore information allows customers to access additional details about hosts and VMs associated with the datastore.	

Interacting with the virtual machines

VMware vCenter integration with Cisco Intersight allows customers to directly interact with the virtual machines (VMs) from the Cisco Intersight dashboard. In addition to obtaining in-depth information about a VM, including the operating system, CPU, memory, host name, and IP addresses assigned to the virtual machines, customers can use Intersight to perform following actions on the virtual machines ([Figure 46](#)):

- Launch VM console
- Power off
- Reset
- Shutdown guest OS
- Restart guest OS
- Suspend

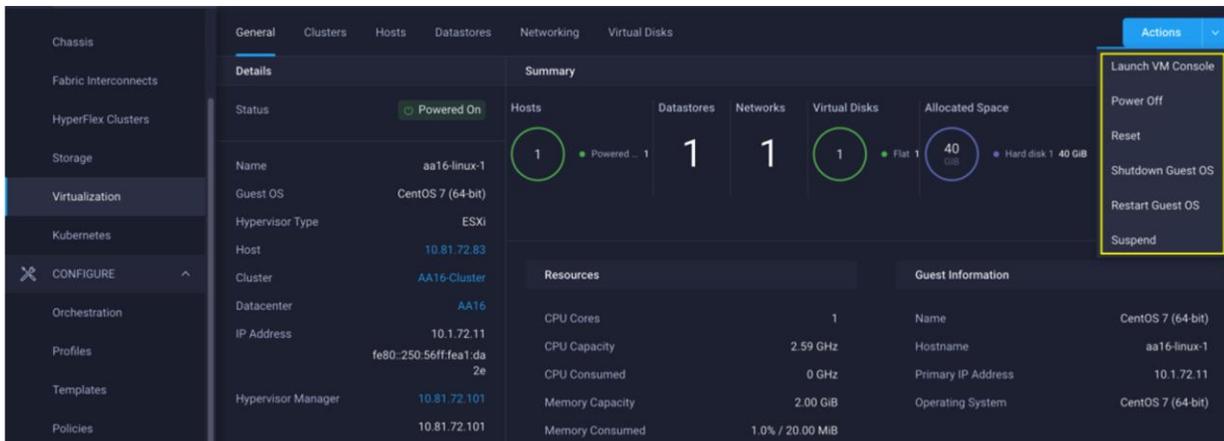


Figure 46.
Virtual machine actions in Cisco Intersight

Cisco Intersight Orchestrator - VMware vCenter

Cisco Intersight Orchestrator provides various workflows that can be used for the VM and hypervisor provisioning. Some of the sample workflows available for VMware vCenter are captured in [Table 5](#).

Table 5. VMware vCenter Workflows in Cisco Intersight Orchestrator

Name	Details
New NAS Datastore	Create a NFS storage volume and build NAS datastore on the volume.
New VMFS Datastore	Create a storage volume and build VMFS datastore on the volume.
New Virtual Machine	Create a new virtual machine on the hypervisor from an OVA or OVF file. Datastore, Host/Cluster, and Image URL fields are mandatory. All other inputs are optional.
Remove NAS Datastore	Remove the NAS datastore and the underlying NFS storage volume.
Remove VMFS Datastore	Remove VMFS datastore and remove the backing volume from the storage device.
Update NAS Datastore	Update NAS datastore by expanding capacity of the underlying NFS volume.
Update VMFS Datastore	Expand a datastore on hypervisor manager by extending the backing storage volume to specified capacity, and then grow the datastore to utilize the additional capacity.

In addition to the above workflows, Cisco Intersight Orchestrator provides a large number of tasks for customers to create custom workflows depending on their specific requirements. A sample subset of these tasks is highlighted in [Figure 47](#).

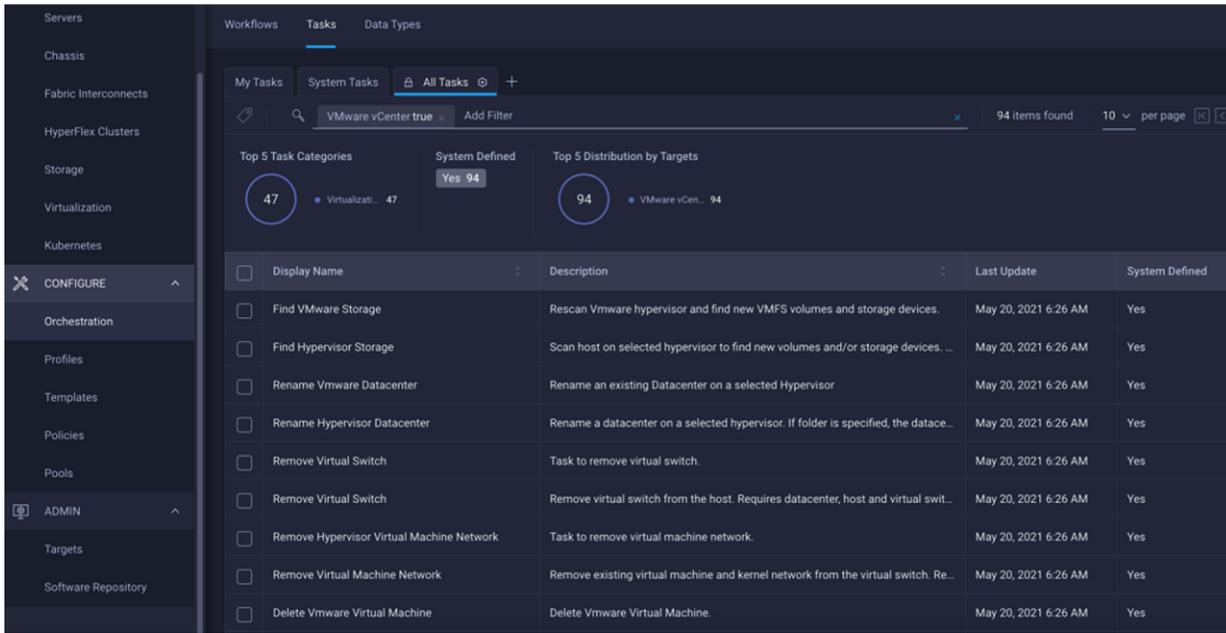


Figure 47. VMware vCenter tasks in Cisco Intersight Orchestrator

Deployment hardware and software

This section outlines the solution hardware and software components.

Hardware and software revisions

Table 6 covers the hardware and software releases for the FlexPod with Cisco UCS X-Series and Cisco Intersight solution.

Table 6. Hardware and software components

Component	
Network	Cisco Nexus 93180YC-FX3 configured in NxOS mode
	Cisco MDS 9132T
Compute	Cisco UCS Fabric Interconnect 6454 in Intersight Managed Mode
	Cisco UCSX-9508 Chassis and UCS X210c M6 Compute Nodes
	Cisco Intersight Assist virtual appliance
	VMware ESXi 7.0
	VMware vCenter Appliance 7.0
Storage	NetApp AFF A400; ONTAP 9
	NetApp Active IQ Unified Manager
	NetApp Virtual Storage Console

Summary

The FlexPod Datacenter solution is a validated approach for deploying Cisco and NetApp technologies and products for building shared private and public cloud infrastructure. With the introduction of Cisco X-Series modular platform to FlexPod Datacenter, customers now have the ability to manage and orchestrate the next-generation Cisco UCS platform from the cloud using Cisco Intersight. Some of the key advantages of integrating Cisco UCS X-Series and Cisco Intersight into the FlexPod infrastructure are:

- Simpler and programmable infrastructure
- Power and cooling innovations and better airflow
- Fabric innovations for heterogeneous compute and memory composability
- Innovative cloud operations providing continuous feature delivery
- Future-ready design built for investment protection

In addition to the Cisco UCS X-Series hardware and software innovations, integration of the Cisco Intersight cloud platform with VMware vCenter and NetApp Active IQ Unified Manager delivers monitoring, orchestration, and workload optimization capabilities for the different layers (including virtualization and storage) of the FlexPod infrastructure. The modular nature of the Cisco Intersight platform also provides an easy upgrade path to additional services, such as workload optimization and Kubernetes.

Appendix

This section includes links to various product pages.

Compute

Cisco Intersight: <https://www.intersight.com>

Cisco Intersight Managed Mode

https://www.cisco.com/c/en/us/td/docs/unified_computing/Intersight/b_Intersight_Managed_Mode_Configuration_Guide.html

Cisco Unified Computing System:

<http://www.cisco.com/en/US/products/ps10265/index.html>

Cisco UCS 6400 Series Fabric Interconnects:

<https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/datasheet-c78-741116.html>

Network

Cisco Nexus 9000 Series Switches:

<http://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/index.html>

Cisco MDS 9132T Switches:

<https://www.cisco.com/c/en/us/products/collateral/storage-networking/mds-9100-series-multilayer-fabric-switches/datasheet-c78-739613.html>

Storage

NetApp ONTAP: <https://docs.netapp.com/ontap-9/index.jsp>

NetApp Active IQ Unified Manager:

<https://docs.netapp.com/ocum-98/index.jsp?topic=%2Fcom.netapp.doc.onc-um-isg-lin%2FGUID-FA7D1835-F32A-4A84-BD5A-993F7EE6BBAE.html>

ONTAP Storage Connector for Cisco Intersight:

<https://www.netapp.com/pdf.html?item=/media/25001-tr-4883.pdf>

Virtualization

VMware vCenter Server:

<http://www.vmware.com/products/vcenter-server/overview.html>

VMware vSphere: <https://www.vmware.com/products/vsphere>

Americas Headquarters

Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters

Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters

Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)