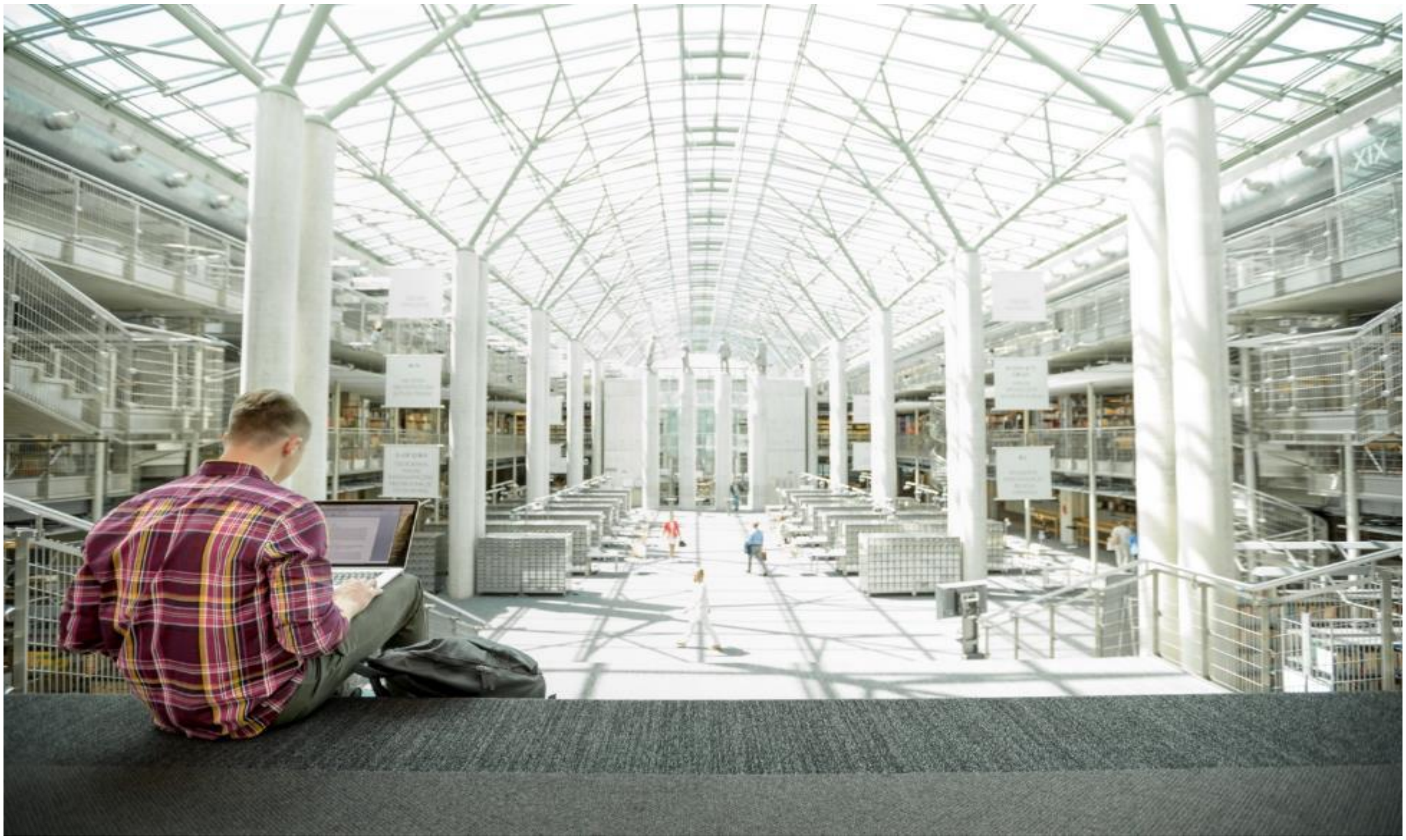


FlexPod Datacenter for SAP Solution using FibreChannel SAN with Cisco UCS Manager 4.0 and NetApp ONTAP 9.7 Design Guide

Published: October 2020

CISCO VALIDATED DESIGN

In partnership with:

NetApp

About the Cisco Validated Design Program

The Cisco Validated Design (CVD) program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information, go to:

http://www.cisco.com/go/designzone.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Contents

Executive Summary

Cisco Validated Designs (CVDs) consist of systems and solutions that are designed, tested, and documented to facilitate and improve customer deployments. These designs incorporate a wide range of technologies and products into a portfolio of solutions that have been developed to address the business needs of our customers and to guide them from design to deployment.

Cisco and NetApp have partnered to deliver a series of FlexPod solutions that enable strategic data center platforms. FlexPod solution delivers an integrated architecture that incorporates compute, storage, and network design best practices thereby minimizing IT risks by validating the integrated architecture to ensure compatibility between various components. The solution also addresses IT pain points by providing documented design guidance, deployment guidance and support that can be used in various stages (planning, designing and implementation) of a deployment.

While the previous validations with FlexPod have been primarily NFS centric, this exercise addresses the Fibre Channel (FC) based solution as a validated approach for deploying SAP HANA® Tailored Data Center Integration (TDI) environments. This design guide provides guidelines and a framework for implementing SAP HANA with best practices from Cisco and NetApp.

The recommended solution architecture is built on the Cisco Unified Computing System (Cisco UCS) using a unified software release to support Cisco UCS hardware platforms and NetApp All Flash storage. It includes the following components:

- Cisco UCS B-Series blade servers and Cisco UCS C-Series rack servers configurable with Intel Optane Data Center Persistent Memory Module (DCPMM) option
- Cisco UCS 6400 series Fabric Interconnects
- Cisco Nexus 9000 Series switches and Cisco Multilayer Director Switches(MDS) switches
- NetApp All Flash series storage arrays
- Additionally, this guide provides validations for both Red Hat Enterprise Linux and SUSE Linux Enterprise Server for SAP HANA.

Overview

Introduction

Industry trends indicate a vast data center transformation toward shared infrastructure and cloud computing. Business agility requires application agility, so IT teams need to provision applications quickly and resources need to be able to scale up (or down) in minutes.

FlexPod Datacenter is a best practice datacenter architecture, designed and validated by Cisco and NetApp to meet the needs of enterprise customers and service providers. FlexPod Datacenter is built on NetApp All Flash FAS, Cisco Unified Computing System (Cisco UCS), Cisco MDS, and the Cisco Nexus family of switches. These components combine to enable management synergies across all of a business's IT infrastructure. FlexPod Datacenter has been proven to be the optimal platform for both virtualized & bare metal workloads enabling enterprises to standardize all of their IT infrastructure for SAP and SAP HANA..

Audience

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

What's New in this Release?

This validated design introduces an FC centric approach to FlexPod Datacenter for SAP Solution and also newer hardware and software into the portfolio, enabling 25/40/100GbE with Cisco FX series Cisco Nexus Switches along with native 32Gb FC via the Cisco MDS switches.

- Validation of Cisco UCS 4.1(1d) unified software release, with Cisco UCS B480-M5 servers with 2nd Generation Intel Xeon Scalable Processors, and Cisco 1400 Series Virtual Interface Cards (VICs)
- Validation with the latest Cisco UCS 6454 Fabric Interconnects and Cisco UCS 2408 Fabric Extender
- Validation with NetApp AFF A400 Storage Controller running the latest release of NetApp ONTAP® 9.7
- Support for NetApp SnapCenter and NetApp SnapCenter Plug-in for SAP HANA Version 4.3
- Validation with primarily 32 Gbps FC design and supplementary 25/40/100GbE NFS for the shared filesystem requirement.
- Support for Cisco Data Center Network Manager (DCNM)-SAN Version 11.3(1)
- Addition of Cisco Intersight Software as a Service (SaaS) Management

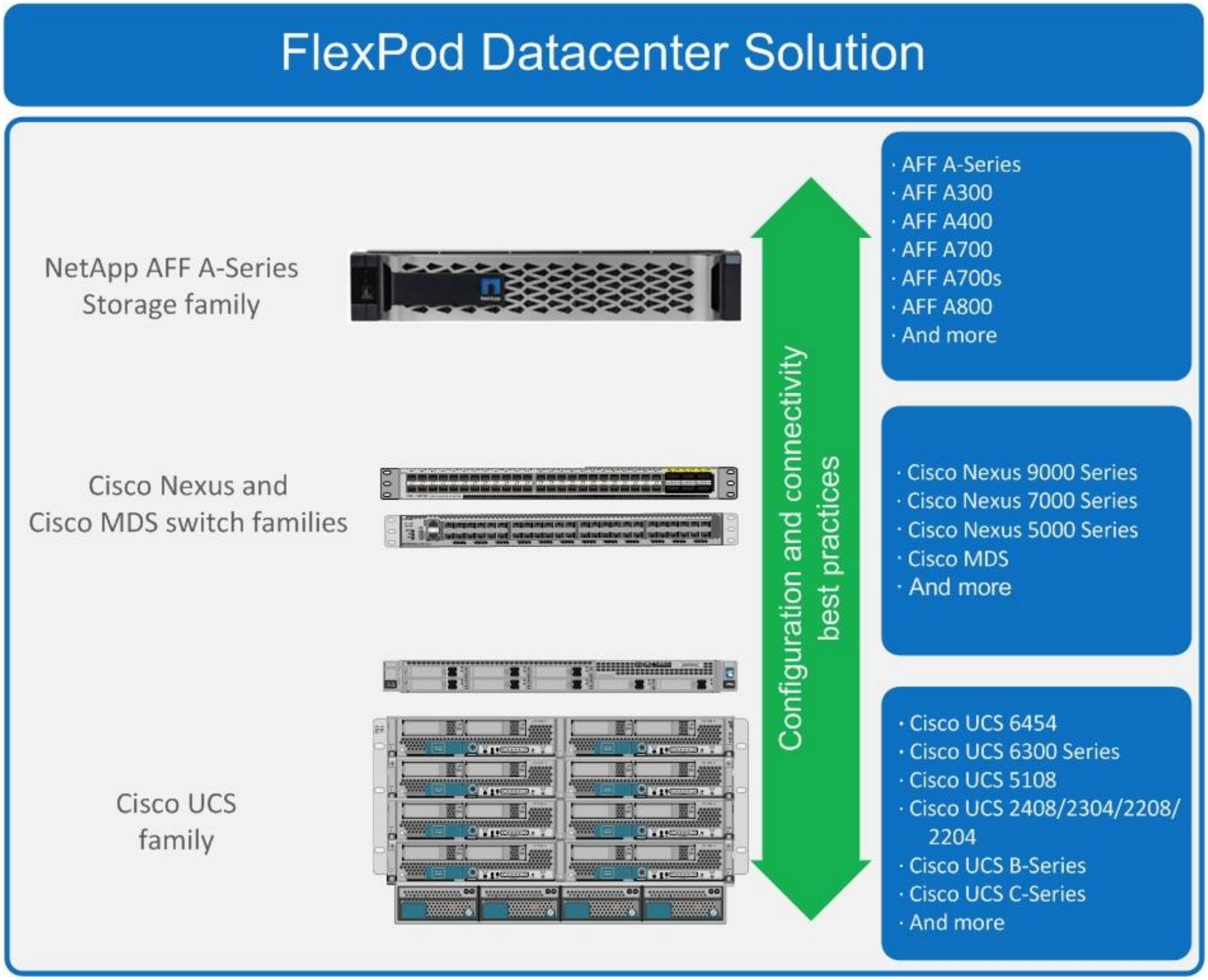
Technology Overview

FlexPod System Overview

FlexPod is a best practice datacenter architecture that includes the following components:

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

Figure 1. **FlexPod Component Families**


FlexPod Datacenter Solution
NetApp AFF A-Series Storage family
Cisco Nexus and Cisco MDS switch families
Cisco UCS family
Configuration and connectivity best practices
· AFF A-Series
· AFF A300
· AFF A400
· AFF A700
· AFF A700s
· AFF A800
· And more
· Cisco Nexus 9000 Series
· Cisco Nexus 7000 Series
· Cisco Nexus 5000 Series
· Cisco MDS
· And more
· Cisco UCS 6454
· Cisco UCS 6300 Series
· Cisco UCS 5108
· Cisco UCS 2408/2304/2208/2204
· Cisco UCS B-Series
· Cisco UCS C-Series
· And more

These components are connected and configured according to the best practices of both Cisco and NetApp to provide an ideal platform for running a variety of enterprise workloads with confidence. FlexPod can scale up for greater performance and capacity (adding compute, network, or storage resources individually as needed), or it can scale out for environments that require multiple consistent deployments (such as rolling out of additional FlexPod stacks). The reference architecture covered in this document leverages Cisco Nexus 9000 for the network switching element and pulls in the Cisco MDS 9000 for the SAN switching component.

One of the key benefits of FlexPod is its ability to maintain consistency during scale. Each of the component families shown (Cisco UCS, Cisco Nexus, and NetApp AFF) offers platform and resource options to scale the infrastructure up or down, while supporting the same features and functionality that are required under the configuration and connectivity best practices of FlexPod.

Cisco Nexus

Cisco Nexus series switches provide an Ethernet switching fabric for communications between the Cisco UCS, NetApp storage controllers, and the rest of a customer's network. There are many factors to consider when choosing the main data switch in this type of architecture to support both the scale and the protocols required for the resulting applications. All Nexus switch models including the Nexus 5000 and Nexus 7000 are supported in this design and may provide additional features such as FCoE or OTV. However, be aware that there may be slight differences in setup and configuration based on the switch used. The validation for this deployment leverages the Cisco Nexus 9000 series switches, which deliver high performance 25/40/100GbE ports density, low latency, and exceptional power efficiency in a broad range of compact form factors.

Many of the most recent single-site FlexPod designs also use this switch due to the advanced feature set and the ability to support Application Centric Infrastructure (ACI) mode. When leveraging ACI fabric mode, the Nexus 9000 series switches are deployed in a spine-leaf architecture. Although the reference architecture covered in this design does not leverage ACI, it lays the foundation for customer migration to ACI in the future, and fully supports ACI when required.

For more information, refer to http://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/index.html.

This FlexPod design deploys a single pair of Cisco Nexus 93180YC-FX top-of-rack switches within each placement, using the traditional standalone mode running NX-OS.

The traditional deployment model delivers numerous benefits for this design:

- High performance and scalability with L2 and L3 support per port
- Layer 2 multipathing with all paths forwarding through the Virtual port-channel (vPC) technology
- VXLAN support at line rate
- Advanced reboot capabilities include hot and cold patching
- Hot-swappable power-supply units (PSUs) and fans with N+1 redundancy

Cisco Nexus 9000 provides an Ethernet switching fabric for communications between the Cisco UCS domain, the NetApp storage system, and the enterprise network. In the FlexPod design, Cisco UCS Fabric Interconnects and NetApp storage systems are connected to the Cisco Nexus 9000 switches using virtual Port Channels (vPC)

Virtual Port Channel (vPC)

A virtual Port Channel (vPC) allows links that are physically connected to two different Cisco Nexus 9000 Series devices to appear as a single Port Channel. In a switching environment, the vPC provides the following benefits:

- Allows a single device to use a Port Channel across two upstream devices
- Eliminates Spanning Tree Protocol blocked ports and uses all available uplink bandwidth
- Provides a loop-free topology
- Provides fast convergence if either one of the physical links or a device fails
- Helps ensure high availability of the overall FlexPod system

Figure 2. **Cisco Nexus 9000 Connections**

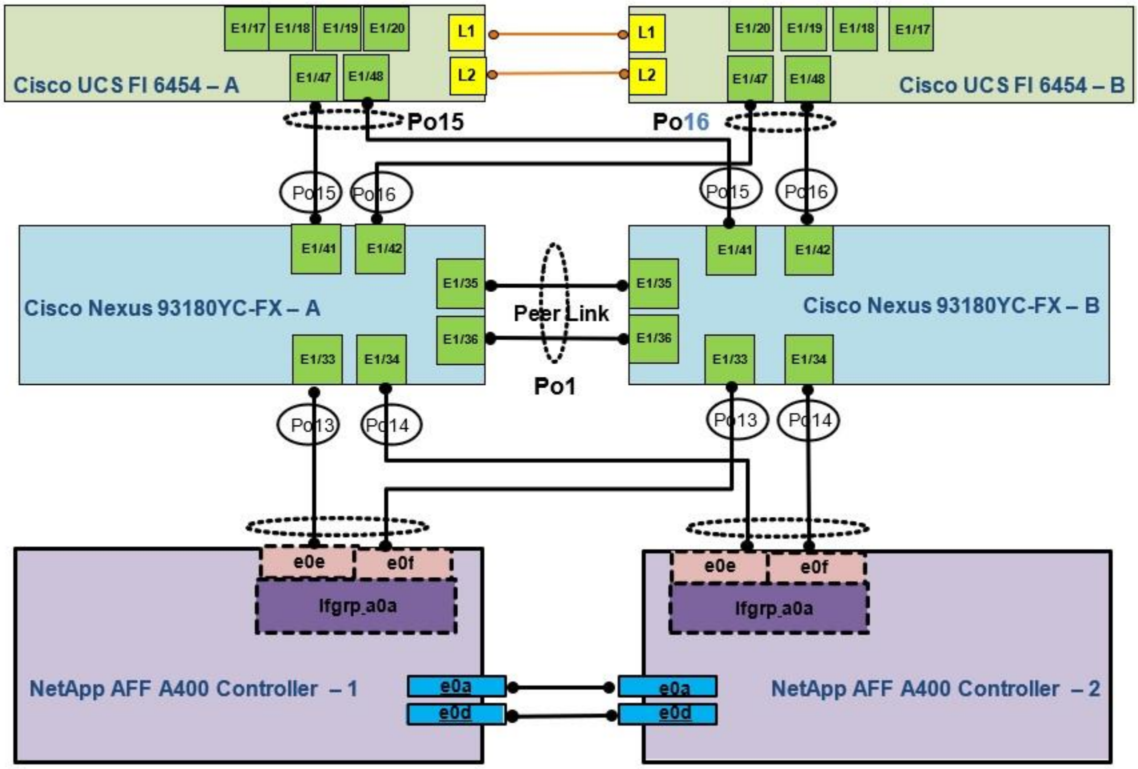


Figure 2 shows the connections between the Cisco Nexus 9000s, Cisco UCS Fabric Interconnects, and NetApp AFF A400s. A vPC requires a “peer link” which is documented as port channel 1 in this diagram. In addition to the vPC peer-link, the vPC peer keepalive link is a required component of a vPC configuration. The peer keepalive link allows each vPC enabled switch to monitor the health of its peer. This link accelerates convergence and reduces the occurrence of split-brain scenarios. In this validated solution, the vPC peer keepalive link uses the out-of-band management network. This link is not shown in Figure 2.

Cisco Nexus 9000 Best Practices

Cisco Nexus 9000 related best practices used in the validation of the FlexPod architecture are summarized below:

Cisco Nexus 9000 Features Enabled

- Link Aggregation Control Protocol (LACP part of 802.3ad)
- Cisco Virtual Port Channeling (vPC) for link and device resiliency
- Cisco Discovery Protocol (CDP) for infrastructure visibility and troubleshooting
- Link Layer Discovery Protocol (LLDP) for additional infrastructure visibility and troubleshooting
- Port channel type Port Profiles for consistent provisioning across port channel instances

vPC Considerations

- Define a unique domain ID
- Set the priority of the intended vPC primary switch lower than the secondary (default priority is 32768)
- Establish peer keepalive connectivity. It is recommended to use the out-of-band management network (mgmt0) or a dedicated switched virtual interface (SVI)
- Enable vPC auto-recovery feature
- Enable peer-gateway. Peer-gateway allows a vPC switch to act as the active gateway for packets that are addressed to the router MAC address of the vPC peer allowing vPC peers to forward traffic
- Enable IP ARP synchronization to optimize convergence across the vPC peer link.
- A minimum of two 10 Gigabit Ethernet connections are required for vPC
- All port channels should be configured in LACP active mode

Spanning Tree Considerations

- The spanning tree priority was not modified. Peer-switch (part of vPC configuration) is enabled which allows both switches to act as root for the VLANs
- Loopguard is disabled by default
- BPDU guard and filtering are enabled by default
- Bridge assurance is only enabled on the vPC Peer Link
- Ports facing the NetApp storage controller and Cisco UCS are defined as “edge” trunk ports

For configuration details, refer to the Cisco Nexus 9000 Series Switches Configuration guides: http://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-installation-and-configuration-guides-list.html.

Cisco MDS

The next-generation Cisco® MDS 9148T 32-Gbps 48-Port Fibre Channel Switch provides high-speed Fibre Channel connectivity for All-Flash arrays. This switch offers state-of-the-art analytics and telemetry capability built into its next-generation Application-Specific Integrated Circuit (ASIC) platform. This switch allows seamless transition to Fibre Channel Non-Volatile Memory Express (FC-NVMe) workloads whenever available without any hardware upgrade in the SAN. It empowers small, midsize, and large enterprises that are rapidly deploying cloud-scale applications using extremely dense virtualized servers, providing the benefits of greater bandwidth, scale, and consolidation. Some of the main benefits for a small-scale Storage Area Network (SAN) are automatic zoning, nonblocking forwarding, and smaller port groups of 16 ports. Benefits for a mid- to large-size SAN include higher scale for Fibre Channel control-plane functions, virtual SANs, fabric login (FLOGI), device alias and name server scale, 48 ports of 32-Gbps non-oversubscribed line-rate ports, bidirectional airflow, and a fixed-form FC-NVMe-ready SAN switch with enhanced Buffer-to-Buffer (B2B) credits connecting both storage and host ports and Fibre Channel link encryption. Large-scale SAN architectures built with SAN core directors can expand 32-Gbps connectivity to the server rack using these switches in either switch mode or Network Port Virtualization (NPV) mode. For more information about the MDS 9148T, review the product data sheet: https://www.cisco.com/c/en/us/products/collateral/storage-networking/mds-9148t-32-gbps-48-port-fibre-channel-switch/data-sheet-c78-740623.html

MDS Insertion into FlexPod

The MDS 9148T is inserted into the FlexPod design to provide 32 Gbps Fibre Channel switching between the NetApp AFF A400 storage controllers, and Cisco UCS Managed B-Series connected to the Cisco UCS 6454 Fabric Interconnects. Adding the MDS to the FlexPod infrastructure allows for:

- Increased scaling of both the NetApp storage and the Cisco UCS compute resources
- Large range of existing models supported from the 9100, 9200, 9300, and 9700 product lines
- A dedicated network for fibre channel storage traffic
- Increased tenant separation
- Deployments utilizing existing qualified SAN switches that might be within the customer environment

Smart Zoning with MDS

Configuration of the Cisco MDS within this FlexPod design takes advantage of Smart Zoning to increase zoning and administration efficiency within the MDS. Smart Zoning allows for reduced TCAM (ternary content addressable memory) entries, which are fabric ACL entries of the MDS allowing traffic between targets and initiators. When calculating TCAMs used, two TCAM entries will be created for each connection of devices within the zone. Without Smart Zoning enabled for a zone, all targets will have a pair of TCAMs established between each other, and all initiators will additionally have a pair of TCAMs established to other initiators in the zone. In other words, all targets are zoned to all targets and all initiators are zoned to all initiators in addition to the desired all initiators being zoned to all targets.

Using Smart Zoning, Targets and Initiators are identified, reducing TCAMs needed to only target to initiator within the zone.

Within the traditional zoning model for a multiple initiator, multiple target zone, the TCAM entries will grow rapidly, representing a relationship of TCAMs = (T+I)*(T+I)-1) where T = targets and I = initiators. For Smart Zoning configuration, this same multiple initiator, multiple target zone will instead have TCAMs = 2*T*I where T = targets and I = initiators.

With Smart Zoning, zones can now be defined as one-to-many, many-to-one, or many-to-many without incurring a penalty in switch resource consumption. Thus, administrators can now define zones to correspond to entities that actually are meaningful in their data center operations. For example, they can define a zone for an application, or for an application cluster, or for a hypervisor cluster without compromising internal resource utilization. It is recommended in FlexPod to configure zones corresponding to NetApp Storage Virtual Machines (SVMs). In this configuration, the one zone for each SVM contains the Fibre Channel Logical Interface (LIF) targets for that fabric defined in the SVM, and the initiator worldwide node names (WWNNs) for that fabric for all Cisco UCS servers that need to access the SVM storage. Later, if any servers are added, the initiator WWNNs can then simply be added to the appropriate zones. This saves significant administrative effort over defining a separate zone for each UCS server and adding the redundant targets used by other UCS servers.

For more information about Smart Zoning, see: https://www.cisco.com/c/dam/en/us/products/collateral/storage-networking/mds-9100-series-multilayer-fabric-switches/at_a_glance_c45-708533.pdf.

Cisco Data Center Network Manager (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 and Cisco UCS Ethernet 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 and UCS fabric interconnects are added with the appropriate credentials and licensing, monitoring of the SAN and Ethernet fabrics can begin. Additionally, VSANs, Device Aliases, Zones, and Zonesets 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 provide insights into your fabric by allowing you to monitor, analyze, identify, and troubleshoot performance issues.

Cisco Unified Computing System

Cisco Unified Computing System (Cisco UCS) is a next-generation data center platform that integrates computing, networking, storage access, and virtualization resources into a cohesive system designed to reduce total cost of ownership and increase business agility. The system integrates a low-latency, lossless 10-100 Gigabit Ethernet unified network fabric with enterprise-class, x86-architecture servers. The system is an integrated, scalable, multi-chassis platform with a unified management domain for managing all resources.

Cisco Unified Computing System consists of the following subsystems:

- Compute - The compute piece of the system incorporates servers based on the 2nd Generation Intel® Xeon® Scalable processors. Servers are available in blade and rack form factor, managed by Cisco UCS Manager.
- Network - The integrated network fabric in the system provides a low-latency, lossless, 10/25/40/100 Gbps Ethernet fabric. Networks for LAN, SAN and management access are consolidated within the fabric. The unified fabric uses the innovative Single Connect technology to lowers costs by reducing the number of network adapters, switches, and cables. This in turn lowers the power and cooling needs of the system.
- Virtualization - The system unleashes the full potential of virtualization by enhancing the scalability, performance, and operational control of virtual environments. Cisco security, policy enforcement, and diagnostic features are now extended into virtual environments to support evolving business needs.
- Storage access – Cisco UCS provides consolidated access to both SAN storage and Network Attached Storage over the unified fabric. This provides customers with storage choices and investment protection. Also, the server administrators can pre-assign storage-access policies to storage resources, for simplified storage connectivity and management leading to increased productivity.
- Management - The system uniquely integrates compute, network, and storage access subsystems, enabling it to be managed as a single entity through Cisco UCS Manager software. Cisco UCS Manager increases IT staff productivity by enabling storage, network, and server administrators to collaborate on Service Profiles that define the desired physical configurations and infrastructure policies for applications.

Service Profiles increase business agility by enabling IT to automate and provision resources in minutes instead of days.

Cisco UCS Differentiators

Cisco Unified Computing System is revolutionizing the way servers are managed in the datacenter. The following are the unique differentiators of Cisco Unified Computing System and Cisco UCS Manager:

- Embedded Management — In Cisco UCS, the servers are managed by the embedded firmware in the Fabric Interconnects, eliminating need for any external physical or virtual devices to manage the servers.
- Unified Fabric — In Cisco UCS, from blade server chassis or rack servers to FI, there is a single Ethernet cable used for LAN, SAN, and management traffic. This converged I/O results in reduced cables, SFPs and adapters – reducing capital and operational expenses of the overall solution.
- Auto Discovery — By simply inserting the blade server in the chassis or connecting the rack server to the fabric interconnect, discovery and inventory of compute resources occurs automatically without any management intervention. The combination of unified fabric and auto-discovery enables the wire-once architecture of Cisco UCS, where compute capability of Cisco UCS can be extended easily while keeping the existing external connectivity to LAN, SAN, and management networks.
- Policy Based Resource Classification — Once a compute resource is discovered by Cisco UCS Manager, it can be automatically classified to a given resource pool based on policies defined. This capability is useful in multi-tenant cloud computing. This CVD showcases the policy-based resource classification of Cisco UCS Manager.
- Combined Rack and Blade Server Management — Cisco UCS Manager can manage Cisco UCS B-series blade servers and Cisco UCS C-series rack servers under the same Cisco UCS domain. This feature, along with stateless computing makes compute resources truly hardware form factor agnostic.
- Model based Management Architecture — The Cisco UCS Manager architecture and management database is model based, and data driven. An open XML API is provided to operate on the management model. This enables easy and scalable integration of Cisco UCS Manager with other management systems.
- Policies, Pools, Templates — The management approach in Cisco UCS Manager is based on defining policies, pools, and templates, instead of cluttered configuration, which enables a simple, loosely coupled, data driven approach in managing compute, network, and storage resources.
- Loose Referential Integrity — In Cisco UCS Manager, a service profile, port profile or policies can refer to other policies or logical resources with loose referential integrity. A referred policy cannot exist at the time of authoring the referring policy or a referred policy can be deleted even though other policies are referring to it. This provides different subject matter experts to work independently from each other. This provides great flexibility where different experts from different domains, such as network, storage, security, server, and virtualization work together to accomplish a complex task.
- Policy Resolution — In Cisco UCS Manager, a tree structure of organizational unit hierarchy can be created that mimics the real-life tenants and/or organization relationships. Various policies, pools and templates can be defined at different levels of organization hierarchy. A policy referring to another policy by name is resolved in the organizational hierarchy with closest policy match. If no policy with specific name is found in the hierarchy of the root organization, then the special policy named “default” is searched. This policy

resolution practice enables automation friendly management APIs and provides great flexibility to owners of different organizations.

- Service Profiles and Stateless Computing – A service profile is a logical representation of a server, carrying its various identities and policies. This logical server can be assigned to any physical compute resource as far as it meets the resource requirements. Stateless computing enables procurement of a server within minutes, which used to take days in legacy server management systems.
- Built-in Multi-Tenancy Support – The combination of policies, pools and templates, loose referential integrity, policy resolution in the organizational hierarchy and a service profiles-based approach to compute resources makes Cisco UCS Manager inherently friendly to multi-tenant environments typically observed in private and public clouds.
- Extended Memory – The enterprise-class Cisco UCS Blade Server extends the capabilities of the Cisco Unified Computing System portfolio in a half-width blade form factor. It harnesses the power of the latest Intel® Xeon® Scalable Series processor family CPUs and Intel® Optane DC Persistent Memory (DCPMM) with up to 18TB of RAM (using 256GB DDR4 DIMMs and 512GB DCPMM).
- Simplified QoS – Even though Fibre Channel and Ethernet are converged in the Cisco UCS fabric, built-in support for QoS and lossless Ethernet makes it seamless. Network Quality of Service (QoS) is simplified in Cisco UCS Manager by representing all system classes in one GUI panel.

Cisco UCS Manager

Cisco UCS Manager (UCSM) provides unified, integrated management for all software and hardware components in Cisco UCS. Using Cisco Single Connect technology, it manages, controls, and administers multiple chassis for thousands of virtual machines. Administrators use the software to manage the entire Cisco Unified Computing System as a single logical entity through an intuitive graphical user interface (GUI), a command line interface (CLI), or a through a robust application programming interface (API).

Cisco UCS Manager is embedded into the Cisco UCS Fabric Interconnects and provides a unified management interface that integrates server, network, and storage. Cisco UCS Manager performs auto-discovery to detect inventory, manage, and provision system components that are added or changed. It offers comprehensive set of XML API for third party integration, exposes thousands of integration points, and facilitates custom development for automation, orchestration, and to achieve new levels of system visibility and control.

Cisco UCS™ Manager, Release 4.0 provides unified, embedded management of all software and hardware components of the Cisco Unified Computing System™ (Cisco UCS) across multiple chassis and Cisco UCS servers. Cisco UCS Manager, Release 4.0 is a unified software release for all supported Cisco UCS hardware platforms. Release 4.0 enables support for Cisco UCS 6454 Fabric Interconnects, Cisco UCS VIC 1400 series adapter cards on Cisco UCS M5 servers and 2nd Intel® Xeon® Scalable processor refresh and Intel® Optane™ Data Center persistent memory modules on Cisco UCS Intel-based M5 servers.

For more information on Cisco UCSM Release 4.0 refer to the Release Notes for Cisco UCS Manager, release 4.0.

Cisco Intersight

Cisco Intersight is Cisco's new systems management platform that delivers intuitive computing through cloud-powered intelligence. This platform offers a more intelligent management level and enables IT organizations to analyze, simplify and automate their IT environments in ways that were not possible with prior generations of tools. This capability empowers organizations to achieve significant savings in Total Cost of Ownership (TCO) and to deliver applications faster to support new business initiatives.

The Cisco UCS platform uses model-based management to provision servers and fabric automatically, regardless of form factor. Cisco Intersight works in conjunction with Cisco UCS Manager and the Cisco Integrated Management Controller (IMC). By simply associating a model-based configuration with a resource through service profiles, your IT staff can consistently align policy, server personality, and workloads. These policies can be created once and used by IT staff with minimal effort to deploy servers. The result is improved productivity and compliance and lower risk of failures due to inconsistent configuration.

Cisco Intersight will be integrated with data center, hybrid cloud platforms and services to securely deploy and manage infrastructure resources across data center and edge environments. In addition, Cisco will provide future integrations to third-party operations tools to allow customers to use their existing solutions more effectively.

Cisco Intersight monitors all Cisco UCS servers and switches in the solution and offers cloud-based, centralized management of Cisco UCS servers across all Enterprise locations and delivers unique capabilities such as:

- Integration with Cisco TAC for support and case management
- Proactive, actionable intelligence for issues and support based on telemetry data
- Compliance check through integration with Cisco Hardware Compatibility List (HCL)
- Centralized service profiles for policy-based configuration

For more information about Cisco Intersight and the different editions, go to: Cisco Intersight - SaaS Systems Management Platform.

Cisco UCS 6454 Fabric Interconnects

The Cisco UCS Fabric Interconnects provide a single point for connectivity and management for the entire system. Deployed as an active-active pair, the system’s fabric interconnects integrate all components into a single, highly available management domain controlled by Cisco UCS Manager. The fabric interconnects manage all I/O efficiently and securely at a single point, resulting in deterministic I/O latency regardless of a server or virtual machine’s topological location in the system.

The Cisco UCS Fabric Interconnect provides both network connectivity and management capabilities for Cisco UCS. IO modules in the blade chassis support power supply, along with fan and blade management. They also support port channeling and, thus, better use of bandwidth. The IOMs support virtualization-aware networking in conjunction with the Fabric Interconnects and Cisco Virtual Interface Cards (VIC).

The Cisco UCS 6454 Fabric Interconnect is a core part of the Cisco Unified Computing System, providing both network connectivity and management capabilities for the system. The Cisco UCS 6454 offers line-rate, low-latency, lossless 10/25/40/100 Gigabit Ethernet, Fibre Channel over Ethernet (FCoE), and 32 Gigabit Fibre Channel functions.

The Cisco UCS 6454 54-Port Fabric Interconnect is a One-Rack-Unit (1RU) 10/25/40/100 Gigabit Ethernet, FCoE and Fibre Channel switch offering up to 3.82 Tbps throughput and up to 54 ports. The switch has 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-Gbps Ethernet ports or 8/16/32-Gbps Fibre Channel ports. All Ethernet ports are capable of supporting FCoE.

Figure 3. **Cisco UCS 6454 Fabric Interconnect**

Cisco UCS 2408 Fabric Extender

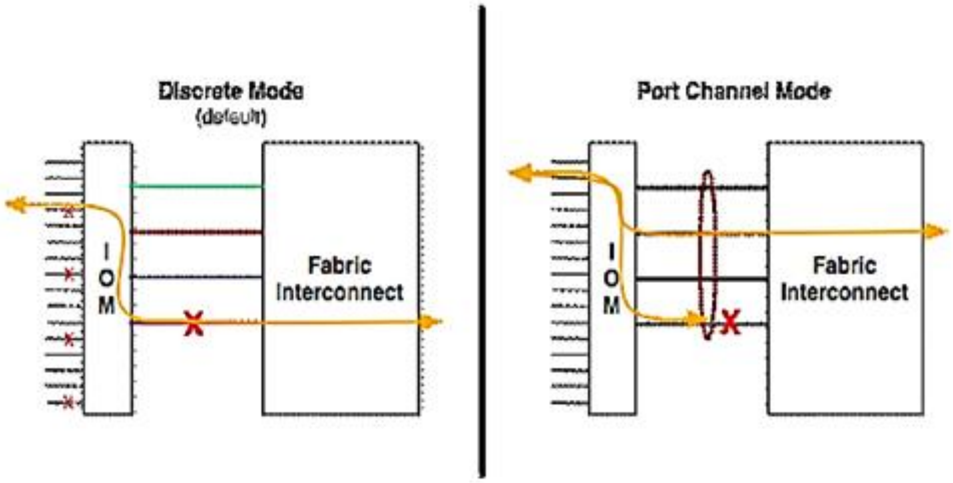
The Cisco UCS 2408 connects the I/O fabric between the Cisco UCS 6454 Fabric Interconnect and the Cisco UCS 5100 Series Blade Server Chassis, enabling a lossless and deterministic converged fabric to connect all blades and chassis together. Because the fabric extender is similar to a distributed line card, it does not perform any switching and is managed as an extension of the fabric interconnects. This approach removes switching from the chassis, reducing overall infrastructure complexity, and enabling Cisco UCS to scale to many chassis without multiplying the number of switches needed, reducing TCO, and allowing all chassis to be managed as a single, highly available management domain.

The Cisco UCS 2408 Fabric Extender [FEX] has eight 25-Gigabit Ethernet, FCoE-capable, Small Form-Factor Pluggable (SFP28) ports that connect the blade chassis to the fabric interconnect. Each Cisco UCS 2408 provides 10-Gigabit Ethernet ports connected through the midplane to each half-width slot in the chassis, giving it a total 32 10G interfaces to Cisco UCS blades. Typically configured in pairs for redundancy, two fabric extenders provide up to 400 Gbps of I/O from FI 6454's to 5108 chassis.

Figure 4. **Cisco UCS FEX 2408**

Each fabric extender connects to one Fabric Interconnect using multiple Ethernet 25Gbps links – the number of links determines the uplink I/O bandwidth through that FEX. The number of links can be 1, 2, 4 or 8. These links can be deployed as independent links (discrete Mode) or grouped together using link aggregation (port channel mode).

Figure 5. Fabric Extender to Fabric Interconnect Connectivity Options



In discrete mode, each server is pinned to a FEX link going to a port on the fabric interconnect and if the link goes down, the server's connection also goes down through the FEX link. In port channel mode, the flows from the server will be redistributed across the remaining port channel members. This is less disruptive overall and therefore port channel mode is recommended for this FlexPod design.

Cisco UCS 1400 Series Virtual Interface Cards (VICs)

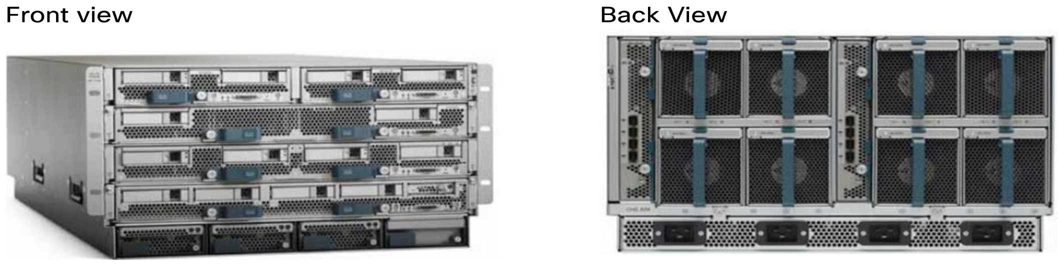
Cisco VICs support Cisco SingleConnect technology, which provides an easy, intelligent, and efficient way to connect and manage computing in your data center. Cisco SingleConnect unifies LAN, SAN, and systems management into one simplified link for rack servers and blade servers. This technology reduces the number of network adapters, cables, and switches needed and radically simplifies the network, reducing complexity. Cisco VICs can support 256 Express (PCIe) virtual devices, either virtual Network Interface Cards (vNICs) or virtual Host Bus Adapters (vHBAs), with a high rate of I/O Operations Per Second (IOPS), support for lossless Ethernet, and 10/25/40/100-Gbps connection to servers. The PCIe Generation 3 x16 interface helps ensure optimal bandwidth to the host for network-intensive applications, with a redundant path to the fabric interconnect. Cisco VICs support NIC teaming with fabric failover for increased reliability and availability. In addition, it provides a policy-based, stateless, agile server infrastructure for your data center.

The Cisco VIC 1400 series is designed exclusively for the M5 generation of Cisco UCS B-Series Blade Servers and Cisco UCS C-Series Rack Servers. The adapters are capable of supporting 10/25/40/100-Gigabit Ethernet and Fibre Channel over Ethernet (FCoE). It incorporates Cisco's next-generation Converged Network Adapter (CNA) technology and offers a comprehensive feature set, providing investment protection for future feature software releases.

Cisco UCS 5108 Blade Server Chassis

The Cisco UCS 5108 Blade Server Chassis is a fundamental building block of the Cisco Unified Computing System, delivering a scalable and flexible blade server architecture. The Cisco UCS blade server chassis uses an innovative unified fabric with fabric-extender technology to lower TCO by reducing the number of network interface cards (NICs), host bus adapters (HBAs), switches, and cables that need to be managed, cooled, and powered. It is a 6-RU chassis that can house up to 8 x half-width or 4 x full-width Cisco UCS B-series blade servers. A passive mid-plane provides up to 80Gbps of I/O bandwidth per server slot and up to 160Gbps for two slots (full-width). The rear of the chassis contains two I/O bays to house a pair of Cisco UCS 2000 Series Fabric Extenders to enable uplink connectivity to FIs for both redundancy and bandwidth aggregation.

Figure 6. **Cisco UCS 5108 Blade Server Chassis**



Front view

Back View

Cisco UCS B200 M5 Blade Servers

The Cisco UCS B200 M5 Blade Server shown in Figure 7, is a half-width blade successor from the Cisco UCS B200 M4.

Figure 7. **Cisco UCS B200 M5 Blade Server**

It features:

- 2nd Generation Intel® Xeon® Scalable processors with up to 28 cores per socket
- Up to 3 terabytes (TB) of DDR4 memory for improved performance
- Up to 7.5 terabytes (TB) using 12x128G DDR4 DIMMs and 12x512G Intel® Optane DCPMM nonvolatile memory technology
- Up to two NIVIDA GPUs
- Two Small-Form-Factor (SFF) drive slots
- Up to two Secure Digital (SD) cards or M.2 SATA drives

For more information about the Cisco UCS B200 M5 Blade Servers, see the Cisco UCS B200 M5 Blade Server datasheet.

Cisco UCS B480 M5 Servers

The enterprise-class Cisco UCS B480 M5 Blade Server delivers market-leading performance, versatility, and density without compromise for memory-intensive mission-critical enterprise applications and virtualized workloads, among others. The Cisco UCS B480 M5 is a full-width blade server supported by the Cisco UCS 5108 Blade Server Chassis.

The Cisco UCS B480 M5 Blade Server offers Four Intel Xeon Scalable CPUs (up to 28 cores per socket), up to 12 TB of DDR4 memory and 18 TB using 24x256G DDR4 DIMMs and 24x512G Intel® Optane DC Persistent

Memory. Five mezzanine adapters and support for up to four GPUs and Cisco UCS Virtual Interface Card (VIC) 1440 modular LAN on Motherboard (mLOM) and Cisco UCS Virtual Interface Card (VIC) 1480 is a dual-port 40-Gbps Ethernet.

Figure 8. **Cisco UCS B480 M5 Blade Server**

For more information about the Cisco UCS B480 M5 Blade Servers, see the Cisco UCS B480 M5 Blade Server datasheet.

Cisco UCS VICs for Cisco UCS B-Series Blade Servers

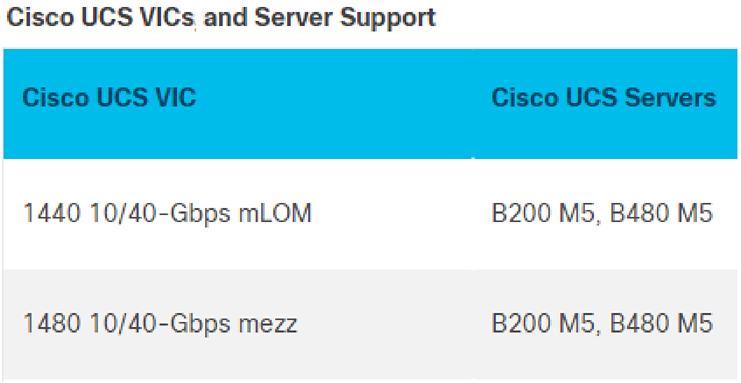
The Cisco UCS VIC 1440 (Figure 9) is a single-port 40-Gbps or 4x10-Gbps Ethernet/FCoE capable modular LAN On Motherboard (mLOM) designed exclusively for the M5 generation of Cisco UCS B-Series Blade Servers. When used in combination with an optional port expander, the Cisco UCS VIC 1440 capabilities are enabled for two ports of 40-Gbps Ethernet. The Cisco UCS VIC 1440 enables a policy-based, stateless, agile server infrastructure that can present to the host PCIe standards-compliant interfaces that can be dynamically configured as either NICs or HBAs.

The Cisco UCS VIC 1480 (Figure 10) is a single-port 40-Gbps or 4x10-Gbps Ethernet/FCoE capable mezzanine card (mezz) designed exclusively for the M5 generation of Cisco UCS B-Series Blade Servers. The card enables a policy-based, stateless, agile server infrastructure that can present PCIe standards-compliant interfaces to the host that can be dynamically configured as either NICs or HBAs.

Figure 9. **Cisco UCS VIC 1440**

Figure 10. **Cisco VIC UCS 1480**

Table 1. Supported Servers



Cisco UCS VICs and Server Support

Cisco UCS VIC	Cisco UCS Servers
1440 10/40-Gbps mLOM	B200 M5, B480 M5
1480 10/40-Gbps mezz	B200 M5, B480 M5

Cisco UCS C480 M5 Rack Server

The Cisco UCS C480 M5 Rack Server (Figure 11) can be deployed as a standalone server or in a Cisco UCS managed environment. When used in combination with Cisco UCS Manager, the Cisco UCS C480 M5 brings the power and automation of unified computing to enterprise applications, including Cisco SingleConnect technology, drastically reducing switching and cabling requirements. Cisco UCS Manager uses service profiles, templates, and policy-based management to enable rapid deployment and help ensure deployment consistency. It also enables end-to-end server visibility, management, and control in both virtualized and bare-metal environments.

The Cisco UCS C480 M5 is a storage- and I/O-optimized enterprise-class rack server that delivers industry-leading performance for IMDBs, Big Data analytics, Virtualization workloads and bare-metal applications.

It delivers outstanding levels of expandability and performance for standalone or Cisco UCS managed environments in a 4-rack-unit (4RU) form factor, and because of its modular design, you pay for only what you need.

The Cisco UCS C480 M5 offers these capabilities:

- Latest Intel Xeon Scalable processors with up to 28 cores per socket and support for two- or four-processor configurations
- 2933-MHz DDR4 memory and 48 DIMM slots for up to 6 TB of total memory
- 12 PCI Express (PCIe) 3.0 slots

- Six x8 full-height, full-length slots
- Six x16 full-height, full-length slots
- Flexible storage options with support up to 32 small-form-factor (SFF) 2.5-inch, SAS, SATA, and PCIe Non-Volatile Memory Express (NVMe) disk drives
- Cisco 12-Gbps SAS modular RAID controller in a dedicated slot
- Internal Secure Digital (SD) and M.2 boot options
- Dual embedded 10 Gigabit Ethernet LAN-on-motherboard (LOM) ports

Figure 11. **Cisco UCS C480 M5 Rack Server**

Cisco UCS C240 M5 Rack Server

The Cisco UCS C240 M5 Rack Server (Figure 12) is a 2-socket, 2RU rack server offering industry-leading performance and expandability. Cisco UCS C-Series Rack Servers can be deployed as standalone servers or as part of a Cisco UCS managed environment to take advantage of Cisco's standards-based unified computing innovations that help reduce customers' TCO and increase their business agility.

In response to ever increasing computing and data-intensive real-time workloads, the enterprise-class Cisco UCS C240 M5 server extends the capabilities of the Cisco UCS portfolio in a 2RU form factor. It incorporates the Intel Xeon Scalable processors, supporting up to 20 percent more cores per socket, twice the memory capacity, and five times more NVMe PCIe SSDs than the previous generation of servers. These improvements deliver significant performance and efficiency gains that will improve your application performance. The Cisco UCS C240 M5 delivers outstanding storage expandability with exceptional performance, with:

- Latest Intel Xeon Scalable CPUs with up to 28 cores per socket
- Up to 24 DDR4 DIMMs for improved performance
- Intel 3D XPoint-ready support, with built-in support for next-generation nonvolatile memory technology
- Up to 26 hot-swappable SFF 2.5-inch drives, including 2 rear hot-swappable SFF drives (up to 10 support NVMe PCIe SSDs on the NVMe-optimized chassis version), or 12 large form factor (LFF) 3.5-inch drives plus 2 rear hot-swappable SFF drives
- Support for a 12-Gbps SAS modular RAID controller in a dedicated slot, leaving the remaining PCIe Generation 3.0 slots available for other expansion cards

- Modular LOM (mLOM) slot that can be used to install a Cisco UCS VIC without consuming a PCIe slot, supporting dual 10- or 40-Gbps network connectivity
- Dual embedded Intel x550 10GBASE-T LOM ports
- Modular M.2 or SD cards that can be used for bootup
- High performance for data-intensive applications

The Cisco UCS C240 M5 Rack Server is well-suited for a wide range of enterprise workloads, including; big data and analytics, collaboration, small and medium-sized business (SMB) databases, virtualization and consolidation, storage servers and high-performance appliances.

Cisco UCS C240 M5 servers can be deployed as standalone servers or in a Cisco UCS managed environment. When used in combination with Cisco UCS Manager, the Cisco UCS C240 M5 brings the power and automation of unified computing to enterprise applications, including Cisco SingleConnect technology, drastically reducing switching and cabling requirements.

Cisco UCS Manager uses service profiles, templates, and policy-based management to enable rapid deployment and help ensure deployment consistency. If also enables end-to-end server visibility, management, and control in both virtualized and bare-metal environments.

Figure 12. Cisco UCS C240 M5 Rack Server

Cisco UCS C220 M5 Rack Server

The Cisco UCS C220 M5 Rack Server (Figure 13) is among the most versatile general-purpose enterprise infrastructure and application servers in the industry. It is a high-density 2-socket rack server that delivers industry-leading performance and efficiency for a wide range of workloads, including virtualization, collaboration, and bare-metal applications. The Cisco UCS C-Series Rack Servers can be deployed as standalone servers or as part of Cisco UCS to take advantage of Cisco's standards-based unified computing innovations that help reduce customers' TCO and increase their business agility.

The Cisco UCS C220 M5 server extends the capabilities of the Cisco UCS portfolio in a 1RU form factor. It incorporates the Intel Xeon Scalable processors, supporting up to 20 percent more cores per socket, twice the memory capacity, 20 percent greater storage density, and five times more PCIe NVMe SSDs than the previous generation of servers. These improvements deliver significant performance and efficiency gains that will improve your application performance. The Cisco UCS C220 M5 server delivers outstanding levels of expandability and performance in a compact package, with:

- Latest Intel Xeon Scalable CPUs with up to 28 cores per socket
- Up to 24 DDR4 DIMMs for improved performance
- Intel 3D XPoint-ready support, with built-in support for next-generation nonvolatile memory technology

- Up to 10 SFF 2.5-inch drives or 4 LFF 3.5-inch drives (77 TB of storage capacity with all NVMe PCIe SSDs)
- Support for a 12-Gbps SAS modular RAID controller in a dedicated slot, leaving the remaining PCIe Generation 3.0 slots available for other expansion cards
- mLOM slot that can be used to install a Cisco UCS VIC without consuming a PCIe slot, supporting dual 10- or 40-Gbps network connectivity
- Dual embedded Intel x550 10GBASE-T LOM ports
- High performance for data-intensive applications

The Cisco UCS C220 M5 Rack Server is well-suited for a wide range of enterprise workloads, including: Big Data and analytics, Collaboration. SMB databases, Virtualization, and consolidation. Storage servers, high-performance appliances.

Cisco UCS C220 M5 servers can be deployed as standalone servers or in a Cisco UCS managed environment. When used in combination with Cisco UCS Manager, the Cisco UCS C220 M5 brings the power and automation of unified computing to enterprise applications, including Cisco SingleConnect technology, drastically reducing switching and cabling requirements.

Cisco UCS Manager uses service profiles, templates, and policy-based management to enable rapid deployment and help ensure deployment consistency. If also enables end-to-end server visibility, management, and control in both virtualized and bare-metal environments.

Figure 13. **Cisco UCS C220 M5 Rack Server**

Cisco UCS VICs For Cisco UCS C-Series Rack Servers

The Cisco UCS VIC 1455 (Figure 14) is a quad-port Small Form-Factor Pluggable (SFP28) half-height PCIe card designed for the M5 generation of Cisco UCS C-Series Rack Servers. The card supports 10/25-Gbps Ethernet or FCoE.

The Cisco UCS VIC 1457 (Figure 15) is a quad-port Small Form-Factor Pluggable (SFP28) mLOM card designed for the M5 generation of Cisco UCS C-Series Rack Servers. The card supports 10/25-Gbps Ethernet or FCoE.

Figure 14. Cisco UCS VIC 1455

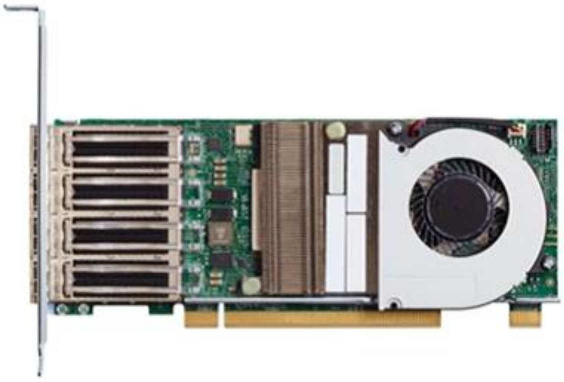


Figure 15. Cisco UCS VIC 1457

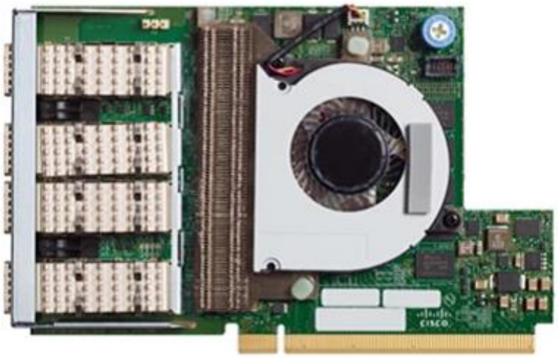
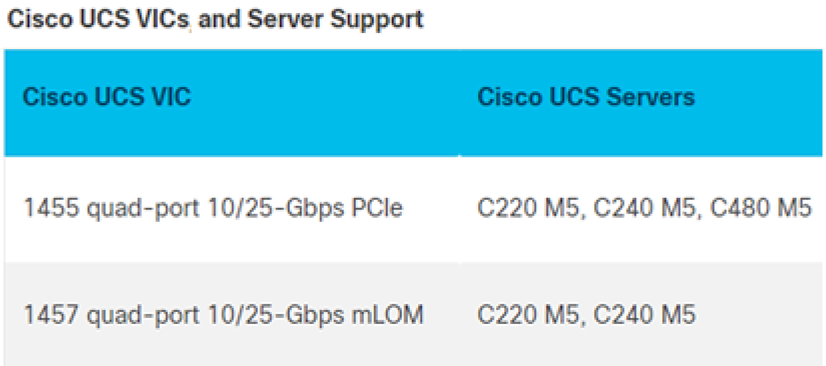


Table 2. Supported Servers



Cisco UCS VICs and Server Support

Cisco UCS VIC	Cisco UCS Servers
1455 quad-port 10/25-Gbps PCIe	C220 M5, C240 M5, C480 M5
1457 quad-port 10/25-Gbps mLOM	C220 M5, C240 M5

NetApp AFF 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 front-end NVMe over Fibre Channel (NVMe/FC) host connectivity. These systems deliver the industry’s lowest latency for an enterprise all-flash array, making them a superior choice for driving the most demanding workloads and artificial intelligence (AI) and deep learning (DL) 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.

This architecture uses the NetApp AFF A400 all-flash array as the foundation of the infrastructure storage. The AFF A400 controllers provide the high-performance benefits of 100GbE and NVMe all-flash solid-state drives (SSDs). Configured with 48 x 15.3TB SSDs, the AFF A400 provides high performance, over 316PB of effective capacity, and decreases power consumption up to 15x. The AFF A400 is available with a full range of high bandwidth connectivity, such as 100/40/25GbE and 32/16Gb FC.

The NetApp AFF A400 is connected to the NetApp NS224 storage shelf. The NetApp NS224 storage shelf is a 2U shelf that has 24 NVMe SSD bays (that support 1.9TB, 3.8TB, 7.6TB and 15.3TB NVMe SSDs) and is connected via the high-speed NVMe/RoCE protocol. Connectivity to traditional SAS storage shelves such as the DS224C, is also supported to extend the life of your existing storage investment.

The AFF A400 system enables customers to:

- Accelerate traditional and emerging enterprise applications such as artificial intelligence and deep learning, analytics, and databases with extremely low latency.
- Reduce data center costs by consolidating applications with a powerful and efficient system.
- Future-proof their environment with NVMe technology, 100GbE Ethernet, 32GB FC, and robust cloud integration with ONTAP 9.

NetApp also expanded its services to improve efficiency and performance while protecting against disruption and data loss.

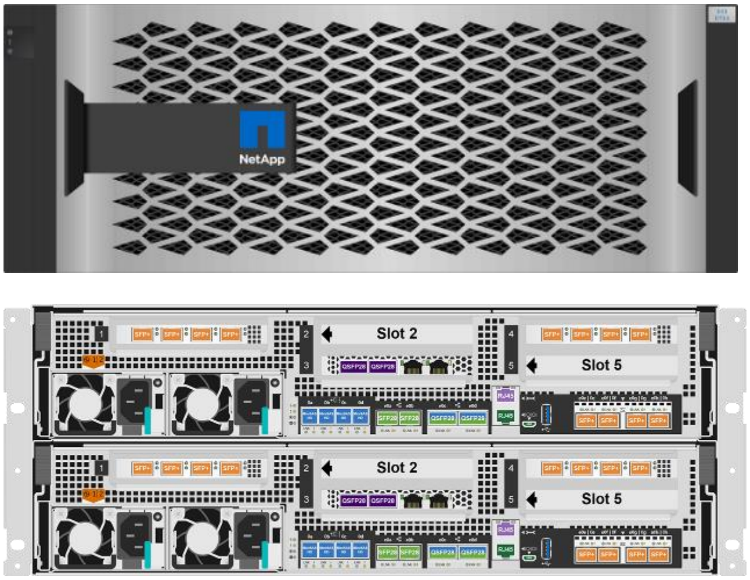
NetApp’s expanded services portfolio now includes:

- SupportEdge Prestige offers a high-touch, concierge level of technical support that resolves issues faster through priority call routing. Customers are assigned a designated team of NetApp experts and receive specialized reporting, tools, and storage environment health assessments.
- Tiered Deployment Service accelerates time to value for new NetApp technology and reduces the risk of improper installation or misconfiguration. Three new high-quality options include Basic, Standard and Advanced Deployment, each aligned to customer business objectives.
- Managed Upgrade Service is a remotely delivered service that reduces security risks by ensuring NetApp software is always up to date with all security patches and firmware upgrades.

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

Figure 16. NetApp AFF A400



NetApp ONTAP 9.7

NetApp ONTAP® 9.7 is the data management software that is used with the NetApp AFF A400 all-flash storage system in the 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. They can run on commodity hardware (NetApp ONTAP Select), 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.

The following sections provide an overview of how ONTAP 9.7 is an industry-leading data management software architected on the principles of software defined storage.

Read more about all the capabilities of ONTAP data management software here:
https://www.netapp.com/us/products/data-management-software/ontap.aspx

NetApp Storage Virtual Machine

A NetApp ONTAP cluster serves data through at least one, and possibly multiple, storage virtual machines (SVMs). An SVM is a logical abstraction that represents the set of physical resources of the cluster. Data volumes and network LIFs are created and assigned to an SVM and can reside on any node in the cluster to which that SVM has access. An SVM can own resources on multiple nodes concurrently, and those resources can be moved non-disruptively from one node in the storage cluster to another. For example, a NetApp FlexVol® flexible volume can be non-disruptively moved to a new node and aggregate, or a data LIF can be transparently reassigned to a different physical network port. The SVM abstracts the cluster hardware, and therefore it is not tied to any specific physical hardware.

An SVM can support multiple data protocols concurrently. Volumes within the SVM can be joined to form a single NAS namespace. The namespace makes all of the SVM's data available through a single share or mount point to NFS and CIFS clients. SVMs also support block-based protocols, and LUNs can be created and exported by using iSCSI, FC, and FCoE. Any or all of these data protocols can be used within a given SVM. Storage administrators and management roles can be associated with an SVM, offering higher security and access control. This security is important in environments that have more than one SVM and when the storage is configured to provide services to different groups or sets of workloads. In addition, you can configure external key management for a named SVM in the cluster. This is a best practice for multitenant environments in which each tenant uses a different SVM (or set of SVMs) to serve data.

Storage Efficiencies

Storage efficiency is a primary architectural design point of ONTAP data management software. A wide array of features enables you to store more data that uses less space. In addition to deduplication and compression, you can store your data more efficiently by using features such as unified storage, multitenancy, thin provisioning, and by using NetApp Snapshot™ technology.

Starting with ONTAP 9, NetApp guarantees that the use of NetApp storage efficiency technologies on AFF systems reduces the total logical capacity used to store customer data up to a data reduction ratio of 7:1, based on the workload. This space reduction is enabled by a combination of several different technologies, including deduplication, compression, and compaction.

Compaction, which was introduced in ONTAP 9, is the latest patented storage efficiency technology released by NetApp. In the NetApp WAFL® file system, all I/O takes up 4KB of space, even if it does not actually require 4KB of data. Compaction combines multiple blocks that are not using their full 4KB of space together into one block. This single block can be more efficiently stored on the disk to save space. These storage efficiencies improve the ability of ONTAP to store more data in less space, reducing storage costs and maximizing the effective capacity of your storage system.

Encryption

Data security remains an important consideration for customers purchasing storage systems. Before ONTAP 9, NetApp supported full disk encryption in storage clusters. However, in ONTAP 9, the encryption capabilities of ONTAP are extended by adding an Onboard Key Manager (OKM). The OKM generates and stores keys for each of the drives in ONTAP, enabling ONTAP to provide all functionality required for encryption out of the box. Through this functionality, known as NetApp Storage Encryption (NSE), sensitive data stored on disk is secure and can only be accessed by ONTAP.

NetApp has extended the encryption capabilities further with NetApp Volume Encryption (NVE), a software-based mechanism for encrypting data. It allows a user to encrypt data at the volume level instead of requiring encryption of all data in the cluster, providing more flexibility and granularity to ONTAP administrators. This encryption extends to Snapshot copies and NetApp FlexClone volumes that are created in the cluster. One benefit of NVE is that it runs after the implementation of the storage efficiency features, and, therefore, it does not interfere with the ability of ONTAP to create space savings. Continuing in ONTAP 9.7 is the ability to preserve NVE in NetApp Cloud Volumes. NVE unifies the data encryption capabilities available on-premises and extends them into the cloud. NVE in ONTAP 9.7 is also FIPS 140-2 compliant. This compliance helps businesses adhere to federal regulatory guidelines for data at rest in the cloud.

ONTAP 9.7 introduces data-at-rest encryption as the default. Data-at-rest encryption is now enabled when an external or onboard key manager (OKM) is configured on the cluster or SVM. This means that all new aggregates created will have NetApp Aggregate Encryption (NAE) enabled and any volumes created in non-encrypted aggregates will have NetApp Volume Encryption (NVE) enabled by default. Aggregate level deduplication is not sacrificed, as keys are assigned to the containing aggregate during volume creation, thereby extending the native storage efficiency features of ONTAP without sacrificing security.

For more information about encryption in ONTAP, see the NetApp Power Encryption Guide in the NetApp ONTAP 9 Documentation Center.

FlexClone

NetApp FlexClone technology enables instantaneous point-in-time copies of a FlexVol volume without consuming any additional storage until the cloned data changes from the original. FlexClone volumes add extra agility and efficiency to storage operations. They take only a few seconds to create and do not interrupt access to the parent FlexVol volume. FlexClone volumes use space efficiently, applying the ONTAP architecture to store only data that changes between the parent and clone. FlexClone volumes are suitable for testing or development environments, or any environment where progress is made by locking-in incremental improvements. FlexClone volumes also benefit any business process where you must distribute data in a changeable form without endangering the integrity of the original.

SnapMirror (Data Replication)

NetApp SnapMirror® is an asynchronous replication technology for data replication across different sites, within the same data center, on-premises datacenter to cloud, or cloud to on-premises datacenter. SnapMirror Synchronous (SM-S) offers volume granular, zero data loss protection. It extends traditional SnapMirror volume replication to synchronous mode meeting zero recovery point objective (RPO) disaster recovery and compliance objectives. ONTAP 9.7 extends support for SnapMirror Synchronous to application policy-based replication providing a simple and familiar configuration interface that is managed with the same tools as traditional SnapMirror. This includes ONTAP CLI, NetApp ONTAP System Manager, NetApp Active IQ Unified Manager, and NetApp Manageability SDK.

NetApp SnapCenter

NetApp SnapCenter® is a NetApp next-generation data protection software for tier 1 enterprise applications. SnapCenter Software is a simple, centralized, scalable platform that provides application-consistent data protection for applications, databases, host file systems, and virtual machines (VMs) running on ONTAP systems anywhere in the Hybrid Cloud.

SnapCenter leverages NetApp Snapshot, SnapRestore, FlexClone, SnapMirror, and SnapVault technologies to provide the following:

- Fast, space-efficient, application-consistent, disk-based backups
- Rapid, granular restore and application-consistent recovery
- Quick, space-efficient cloning

SnapCenter enables seamless integration with Oracle, Microsoft, SAP, MongoDB and VMware across FC, iSCSI, and NAS protocols. This integration enables IT organizations to scale their storage infrastructure, meet increasingly stringent SLA commitments, and improve the productivity of administrators across the enterprise.

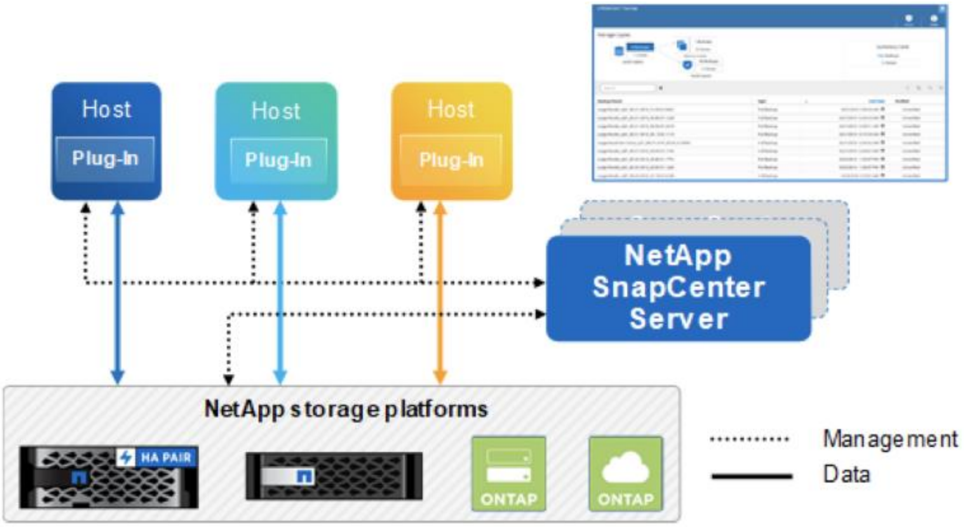
Starting with SnapCenter 4.3, SnapCenter Server has been decoupled from the SnapCenter plugin for VMware vSphere and is no longer required to backup the VM's and datastores. VM and datastore backup functions have been moved exclusively to the SnapCenter plugin for VMware vSphere which was deployed as part of this design. SnapCenter server is still required for application-level VM backups such as for Microsoft SQL Server, Oracle, and SAP HANA.

SnapCenter Architecture

The SnapCenter platform is based on a multitiered architecture that includes a centralized management server (SnapCenter Server) and a SnapCenter plug-in host.

Figure 17 illustrates the high-level architecture of the NetApp SnapCenter Server.

Figure 17. **SnapCenter Architecture**



The SnapCenter Server includes a web server, a centralized HTML5-based user interface, PowerShell cmdlets, REST APIs, and the SnapCenter repository.

SnapCenter enables load balancing, high availability, and horizontal scaling across multiple SnapCenter Servers within a single user interface. You can accomplish high availability by using Network Load Balancing (NLB) and Application Request Routing (ARR) with SnapCenter. For larger environments with thousands of hosts, adding multiple SnapCenter Servers can help balance the load.

The SnapCenter Server can push out plug-ins to remote hosts. These plug-ins are used to interact with an application, a database, or a file system. The SnapCenter Server and plug-ins communicate with the host agent using HTTPS. Usually, the plug-ins must be present on the remote host so that application-level or database-level commands can be issued from the same host where the application or database is running.

To manage the plug-ins and the interaction between the SnapCenter Server and the plug-in host, SnapCenter uses SM Service. SM service is a NetApp SnapManager® web service running on top of Windows Server internet information services (IIS) on the SnapCenter Server. SM Service takes all client requests such as backup, restore, and clone.

The SnapCenter Server communicates those requests to SMCore, which is a service that runs co-located within the SnapCenter Server and remote servers. SMCore plays a significant role in coordinating with the SnapCenter plug-ins package for Windows.

SnapCenter features

SnapCenter enables you to create application-consistent Snapshot copies and to complete data protection operations, including Snapshot copy-based backup, clone, restore, and backup-verification operations. SnapCenter provides a centralized management environment, and it uses role-based access control (RBAC) to delegate data protection and management functions to individual application users across the SnapCenter Server and Windows hosts.

SnapCenter includes the following key features:

- A unified and scalable platform across applications and database environments with virtual and nonvirtual storage powered by the SnapCenter Server
- Consistency of features and procedures across plug-ins and environments supported by the SnapCenter GUI
- RBAC for security and centralized role delegation
- Application-consistent Snapshot copy management, restore, clone, and backup verification support from both primary and secondary destinations (NetApp SnapMirror and NetApp SnapVault® technology)
- Remote package installation from the SnapCenter GUI
- Nondisruptive, remote upgrades
- A dedicated SnapCenter repository for faster data retrieval
- Load balancing that is implemented by using Microsoft Windows network load balancing (NLB) and application request routing (ARR) with support for horizontal scaling
- Centralized scheduling and policy management to support backup and clone operations
- Centralized reporting, monitoring, and dashboard views
- SnapCenter 4.3 support for data protection for VMware VMs, SQL Server databases, Oracle databases, MySQL, SAP HANA, MongoDB, and Microsoft Exchange

SAP HANA Data Protection with SnapCenter

The FlexPod solution can be extended with additional software and hardware components to cover data protection, backup and recovery, and disaster recovery operations. The following chapter provides a high-level overview of how to enhance SAP HANA backup and disaster recovery using the NetApp SnapCenter plug-In for SAP HANA.

More details on the setup and configuration of SnapCenter for backup and recovery or disaster recovery operations can be found in the following technical reports:

[SAP HANA Backup and Recovery with SnapCenter]

[SAP HANA Disaster Recovery with Asynchronous Storage Replication]

SAP HANA Backup

Storage-based Snapshot backups are a fully supported and integrated backup method available for SAP HANA.

Storage-based Snapshot backups are implemented with the NetApp SnapCenter plug-in for SAP HANA, which creates consistent Snapshot backups by using the interfaces provided by the SAP HANA database. SnapCenter registers the Snapshot backups in the SAP HANA backup catalog so that they are visible within the SAP HANA studio or cockpit and can be selected for restore and recovery operations.

Snapshot copies created within primary storage can be replicated to the secondary backup storage by using NetApp SnapMirror technology controlled by SnapCenter. Different backup retention policies can be defined for backups held on the primary storage and to those backups held on the secondary storage. The SnapCenter Plug-In for SAP HANA manages the retention of Snapshot copy-based data backups and log backups, including housekeeping of the backup catalog. The SnapCenter plug-in for SAP HANA also allows the execution of a block integrity check of the SAP HANA database by executing a file-based backup.

Storage-based Snapshot backups provide significant advantages when compared to file-based backups. Advantages include the following:

- Rapid backup (less than a minute)
- Faster restore on the storage layer (less than a minute)
- No performance effect on the SAP HANA database host, network, or storage during backup
- Space-efficient and bandwidth-efficient replication to secondary storage based on block changes

SAP HANA Disaster Recovery with Asynchronous Storage Replication

SAP HANA disaster recovery can be performed either on the database layer by using SAP system replication or on the storage layer by using storage replication technologies. This section provides an overview of disaster recovery solutions based on asynchronous storage replication.

The same SnapCenter plug-in that is described in section SAP HANA Backup is also used for the asynchronous mirroring solution. A consistent Snapshot image of the database at the primary site is asynchronously replicated to the disaster recovery site with SnapMirror.

High-level Architecture Description

Figure 18 shows a high-level overview of the data protection architecture.

For an offsite backup and disaster recovery solution, the following additional hardware and software components are required:

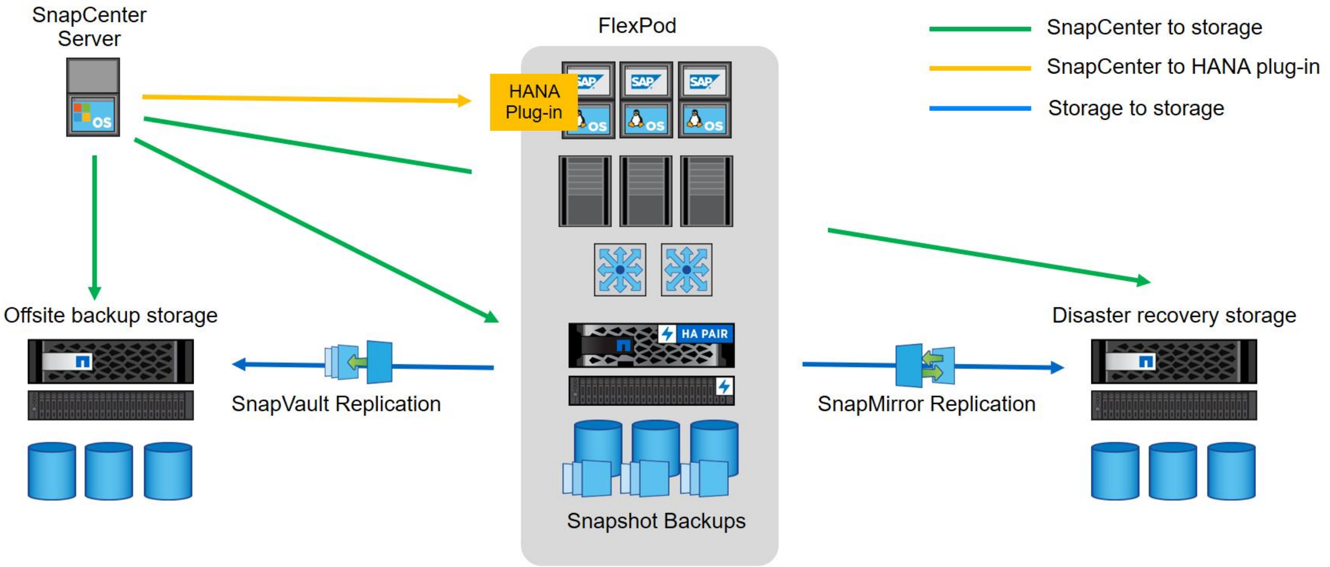
- A Windows host to run SnapCenter server software
- Offsite backup storage to replicate backups from primary storage to a secondary storage system
- Disaster recovery storage to replicate backups from primary storage to a disaster recovery site

The SnapCenter Server must be able to communicate with the SVMs that are used at the primary (within the FlexPod instance), the offsite backup location, and the disaster recovery storage.

The primary storage must have a network connection to the offsite storage and the disaster recovery storage. A storage cluster peering must be established between the primary storage, the offsite storage, and the disaster recovery storage.

The SnapCenter Server must have a network connection to the SAP HANA database hosts to deploy the HANA plug-in and to communicate with the plug-in after deployment. As an alternative, the HANA plug-in can also be deployed at the FlexPod management server. See SAP HANA Backup and Recovery with SnapCenter for more details on the deployment options for the HANA plug-in.

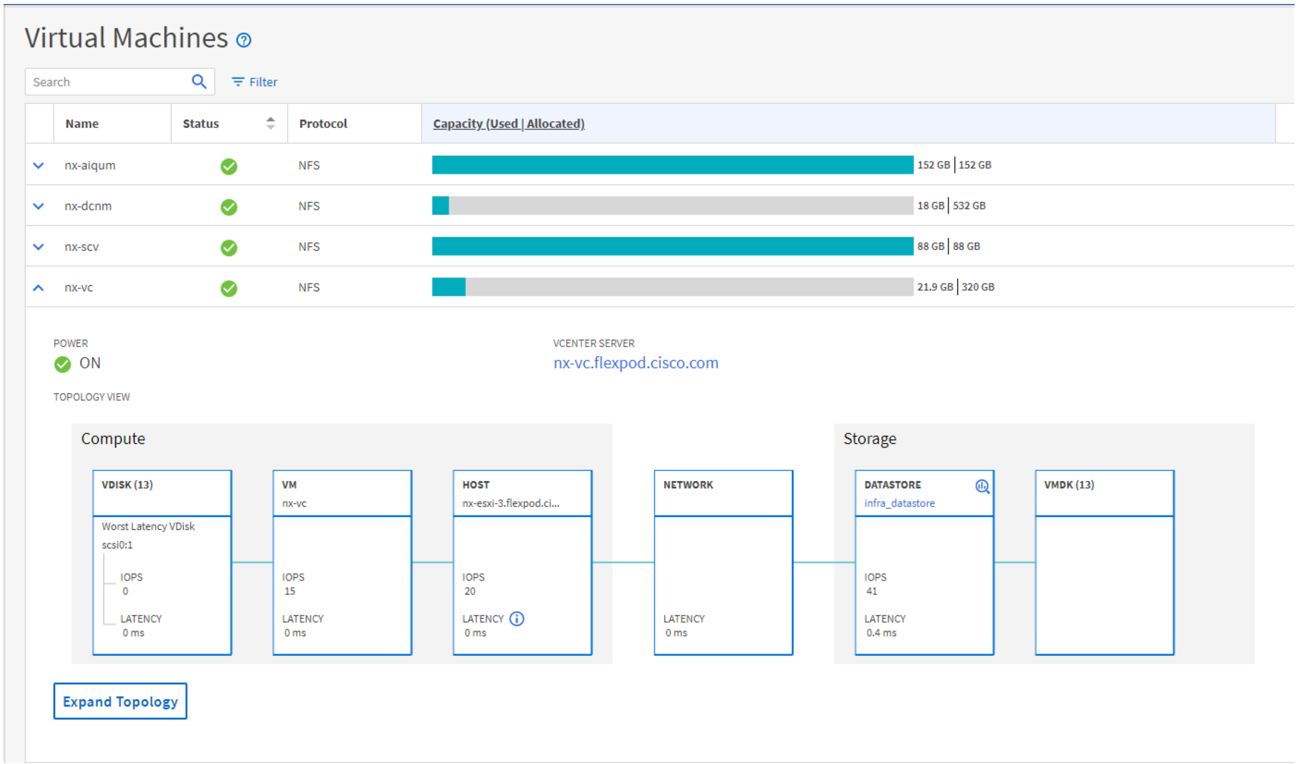
Figure 18. **Data Protection with SnapCenter**



Active IQ Unified Manager 9.7

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. You can deploy Unified Manager on a Linux server, on a Windows server, or as a virtual appliance on a VMware host.

Unified Manager enables monitoring your ONTAP storage clusters, VMware vCenter server and VMs 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 VMs running on it. When an issue occurs on the storage or virtual infrastructure, Unified Manager can notify you about the details of the issue to help with identifying root cause. The VM 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 which 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.



Virtual Machines

	Name	Status	Protocol	Capacity (Used | Allocated)
⌄	nx-aiqum	✓	NFS	152 GB | 152 GB
⌄	nx-dcnm	✓	NFS	18 GB | 532 GB
⌄	nx-scv	✓	NFS	88 GB | 88 GB
⌃	nx-vc	✓	NFS	21.9 GB | 320 GB

POWER
✓ ON

VCENTER SERVER
nx-vc.flexpod.cisco.com

TOPOLOGY VIEW

Compute

VDISK (13)
Worst Latency VDisk
scsi0:1
IOPS
0
LATENCY
0 ms

VM
nx-vc
IOPS
15
LATENCY
0 ms

HOST
nx-esxi-3.flexpod.ci...
IOPS
20
LATENCY
0 ms

NETWORK
LATENCY
0 ms

Storage

DATASTORE
infra_datastore
IOPS
41
LATENCY
0.4 ms

VMDK (13)

Active IQ Unified Manager enables management of storage objects in your environment by associating them with annotations. You can create custom annotations and dynamically associate clusters, storage virtual machines (SVMs), and volumes with the annotations through rules.

Unified Manager also enables reporting different views of your network, providing actionable intelligence on capacity, health, performance, and data protection. You can customize your views by showing and hiding columns, rearranging columns, filtering data, sorting data, and searching the results. You can save custom views for re-use, download them as reports, and schedule them as recurring reports to distribute through email. AIQ 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 which often lead additional problems in the long-term.

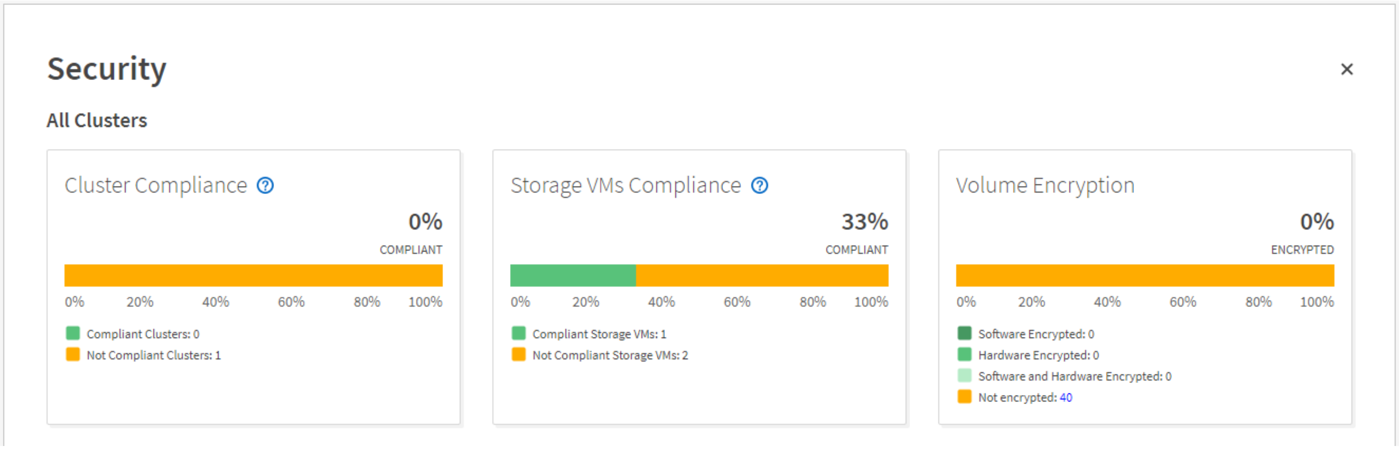
Active IQ Unified Manager 9.7 introduces a new security risk panel that provide an overview of the security posture of the storage system and provides corrective actions to harden ONTAP. AIQ Unified Manager uses rules based on the recommendations made in the Security Hardening Guide for NetApp ONTAP 9 (TR-4569) to evaluate the cluster and SVM configuration. Each recommendation is assigned a value and used to provide an overall compliance score for the ONTAP environment.

The status icons in the security cards have the following meanings in relation to their compliance:

- ✓ - The parameter is configured as recommended.
- ⚠ - The parameter is not configured as recommended.
- ℹ - Either the functionality is not enabled on the cluster, or the parameter is not configured as recommended, but this parameter does not contribute to the compliance of the object.

Note that volume encryption status does not contribute to whether the cluster or SVM are considered compliant.

The compliance score is calculated by auditing certain recommendations made in the Security Hardening Guide and whether the remediation for those risks have been completed. The recommendations included are general in nature and can be applied to most ONTAP environments regardless of workload. Certain criteria are not counted against the compliance score because those configurations cannot be generally applied to all storage environments. Volume encryption would be one an example of this.



Security

All Clusters

Cluster Compliance ?

0%
COMPLIANT

🟩 Compliant Clusters: 0
🟧 Not Compliant Clusters: 1

Storage VMs Compliance ?

33%
COMPLIANT

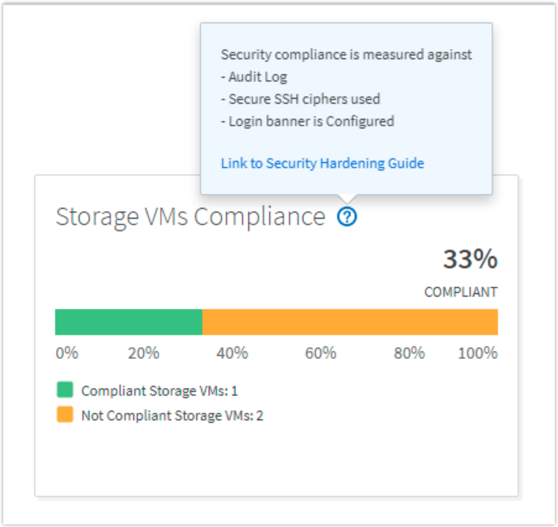
🟩 Compliant Storage VMs: 1
🟧 Not Compliant Storage VMs: 2

Volume Encryption

0%
ENCRYPTED

🟩 Software Encrypted: 0
🟩 Hardware Encrypted: 0
🟩 Software and Hardware Encrypted: 0
🟧 Not encrypted: 40

A list of recommendations being evaluated for compliance can be seen by selecting the blue question mark in each security card which also contains a link to the [Security Hardening Guide for NetApp ONTAP 9](#).



Security compliance is measured against
- Audit Log
- Secure SSH ciphers used
- Login banner is Configured

Link to Security Hardening Guide

Storage VMs Compliance ?

33%
COMPLIANT

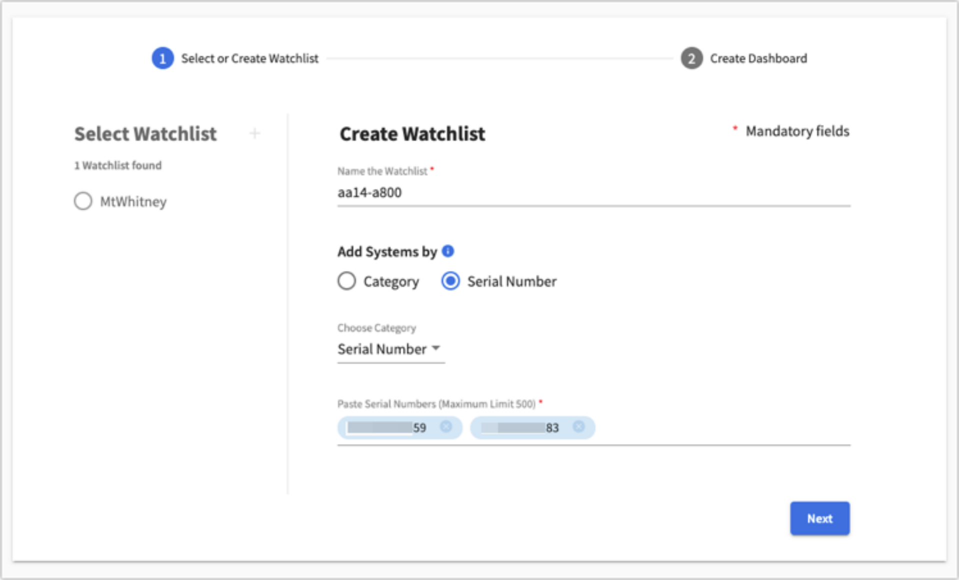
🟩 Compliant Storage VMs: 1
🟧 Not Compliant Storage VMs: 2

For more information on Active IQ Unified Manager refer to the Active IQ Unified Manager Documentation Resources page complete with a video overview and other product documentation.

Active IQ

NetApp Active IQ is a cloud service that provides proactive care and optimization of your NetApp environment, leading to reduced risk and higher availability. Active IQ leverages community wisdom and AIOps artificial intelligence to provide proactive recommendations and risk identification. The latest release of Active IQ offers an enhanced user interface and a personalized experience with Active IQ Digital Advisor dashboards. It allows smooth and seamless navigation, with its intuitiveness throughout different dashboards, widgets, and screens. It provides insights that help you detect and validate important relationships and meaningful differences based on the data that is presented by different dashboards.

Watchlists are a way to organize a group of systems inside Active IQ Digital Advisor and create custom dashboards based on the system grouping. Watchlists provide quick access to only the group of storage systems you are concerned without having to sort or filter those you don't.



Select Watchlist +

1 Watchlist found

○ MtWhitney

Create Watchlist

* Mandatory fields

Name the Watchlist *

aa14-a800

Add Systems by

○ Category ● Serial Number

Choose Category

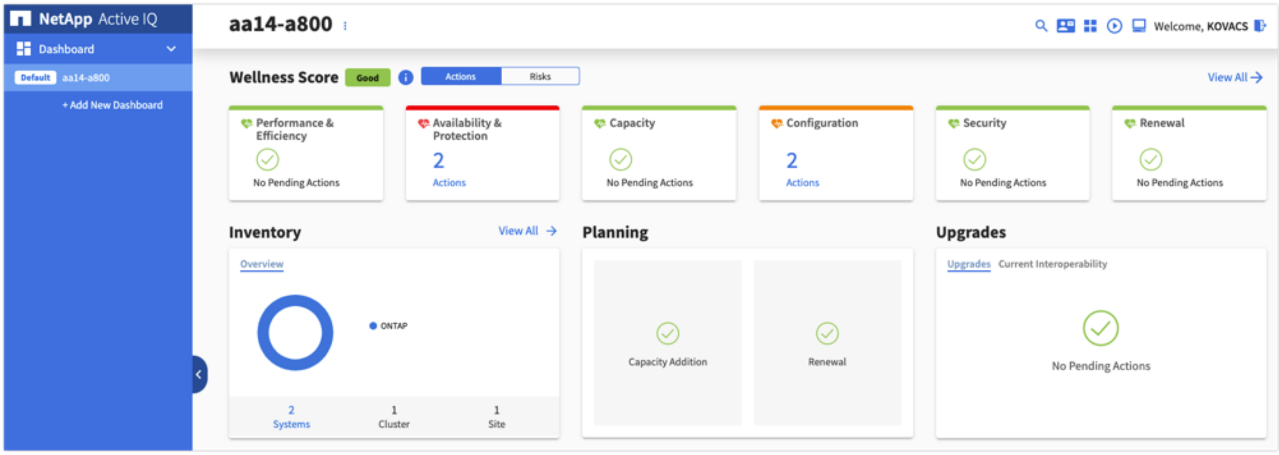
Serial Number

Paste Serial Numbers (Maximum Limit 500) *

[redacted]59 [redacted]83

The Wellness score on the dashboard provides a quick at-a-glance summary on the health of the installed systems based on the number of high risks and expired support contracts. Detailed information about the status of your storage system are sorted into the following six widgets:

- Performance and Efficiency
- Availability and Protection
- Capacity
- Configuration
- Security
- Renewals



The intuitive interface allows you to switch between the Actions and Risks tab to view how the findings are broken down by category, or each unique risk. Color-coding the identified risks into four levels; Critical, High, Medium and No risks, further helps to quickly identify issues that need immediate attention.

Color	Severity
⬛	Critical
🟥	High
🟧	Medium
🟩	No risks

Links to NetApp Bugs Online or NetApp MySupport Knowledge Base articles are incorporated in the corrective actions so that you can obtain further information about the issue and how to correct it before it becomes a problem in the environment.

Active IQ also integrates with the on-premises installation of Active IQ Unified Manager to correct certain issues identified in the Active IQ portal. These risks are identified with the green wrench symbol in the Risks tab inside Active IQ. Clicking the *Fix It* button will launch the installation of AIQ Unified Manager 9.7 to proceed with correcting the issue. If no installation of AIQ Unified Manager 9.7 exists, the option to install or upgrade an existing version of Unified Manager will be presented for future risk mitigation.

SAP Application Monitoring with AppDynamics

AppDynamics is an Application Performance Monitoring (APM) Platform that helps you to understand and optimize the performance of your business, from its software to infrastructure to business journeys.

The AppDynamics APM Platform enables you to monitor and manage your entire application-delivery ecosystem, from the mobile app or browser client request through your network, backend databases and application servers and more. AppDynamics APM gives you a single view across your application landscape, letting you quickly navigate from the global perspective of your distributed application right down to the call graphs or exception reports generated on individual hosts.

AppDynamics has an agent-based architecture. Once our agents are installed it gives you a dynamic flow map or topography of your application. It uses the concept of traffic lights to indicate the health of your application (green is good, yellow is slow and red indicates potential issues) with dynamics baselining. AppDynamics measures application performance based on business transactions which essentially are the key functionality of the application. When the application deviates from the baseline AppDynamics captures and provides deeper diagnostic information to help be more proactive in troubleshooting and reduce the MTTR (Mean Time To Repair).

For more information, go to: https://docs.appdynamics.com/display/SAP/SAP+Monitoring+Using+AppDynamics

Solution Design

The SAP HANA TDI option enables multiple SAP HANA production systems to run on the same infrastructure. In this configuration, the existing blade servers used by different SAP HANA systems share the same network infrastructure and storage systems. In addition, the SAP application server can share the same infrastructure as the SAP HANA database.

SAP HANA in FlexPod environment qualify as SAP HANA TDI implementations.

The section explains the SAP HANA system requirements defined by SAP and Architecture of FlexPod Datacenter Solution providing the platform for SAP and SAP HANA.

SAP HANA System Implementation Options

Because multiple implementation options are available specific to this shared TDI usage, you need to define your requirements before you can select the solution components. This section defines the basic requirements for each option.

Single SAP HANA System on a Single Server: Scale-Up (Bare Metal or Virtualized)

A scale-up TDI solution is the simplest of the installation types. In general, this solution provides the best SAP HANA performance. All data and processes are located on the same server and can be accessed locally, and no network communication with other SAP HANA nodes is required. SAP HANA scale-up TDI solutions are based on a standalone rack-mount server or blade server and use the intended external storage.

The network requirements for this option depend on the client and application access and storage connections. If you don’t need system replication or a backup network, a 1 Gigabit Ethernet (access) network and bandwidth factored for the data, log and shared filesystem access storage networks are required to run SAP HANA in a scale-up configuration.

The storage IO as well as latency Key Performance Indicators (KPI) requirements by SAP need to be fulfilled.

For a virtualized SAP HANA installation, remember that hardware components, such as network interfaces and host bus adapters (HBAs), are shared. If possible, use dedicated network adapters and HBAs for each virtualized SAP HANA system. The storage requirements are similar to a bare metal use case with respect to storage IO and latency KPIs.

Single SAP HANA System on Multiple Servers: Scale-Out

You should use a scale-out TDI solution if the SAP HANA system does not fit into the main memory of a single server based on the rules defined by SAP. In this method, multiple independent servers are combined to form one system and the load is distributed among multiple servers. In a distributed system, each index server is usually assigned to its own host to achieve maximum performance. It is possible to assign different tables to different hosts (partitioning the database), or a single table can be split across hosts (partitioning of tables). SAP HANA Scale-Out supports failover scenarios and high availability. Individual hosts in a distributed system have different roles master, worker, slave, standby depending on the task.

The network requirements for this option are higher than for scale-up systems. In addition to the client and application access and storage access networks, you also must have a node-to-node network. If you don’t need system replication or a backup network, a 10 Gigabit Ethernet (access) network and a mandatory minimum of 10 Gigabit Ethernet (node-to-node) and bandwidth factored for the data, log and shared filesystem access storage networks are required to run SAP HANA in a scale-out configuration.

The storage configuration should take care that the IO as well as latency KPI requirements by SAP are fulfilled.

For a virtualized SAP HANA installation, remember that hardware components, such as network interfaces and host bus adapters (HBAs), are shared. If possible, use dedicated network adapters and HBAs for each virtualized SAP HANA system. The network and storage requirements are similar to a bare metal use case with respect to storage IO/latency and inter-node network bandwidth.

Multiple SAP HANA Systems: Scale-Up (Bare Metal or Virtualized)

Using the SAP HANA TDI option for shared storage and a shared network, you can build a solution to run multiple SAP HANA scale-up systems on shared infrastructure. One approach is to use a SAP HANA scale-out solution and install one SAP HANA system per server. A 4 + 1 scale-out solution (four active nodes and one standby node) includes all the components needed to run five SAP HANA systems based on the TDI key performance indicators (KPIs).

The network requirements are the same as for a single SAP system.

The storage IO as well as latency KPI requirements by SAP need to be fulfilled for each individual system at all times.

For a virtualized SAP HANA installation, remember that some hardware components are shared: for example, network interfaces and HBAs. If possible, you should use dedicated network adapters and HBAs for each virtualized SAP HANA system. The storage requirements are similar to a bare metal use case with respect to storage IO and latency KPIs.

Multiple SAP HANA Systems: Scale-Out (Bare Metal or Virtualized)

Using the SAP HANA TDI option for shared storage and a shared network, you can build a solution to run multiple SAP HANA scale-out systems on shared infrastructure. One approach is to use an SAP HANA scale-out solution infrastructure and install two or more SAP HANA systems on it. As an example, you can use an 11 + 1 scale-out solution (11 active nodes and 1 standby node) includes all the components to install two 5 + 1 systems or three 3 + 1 systems or any other supported scale-out configuration.

The network requirements are the same as for a single SAP HANA system.

The storage IO as well as latency KPI requirements by SAP need to be fulfilled for each individual scale-out system at all times.

For a virtualized SAP HANA installation, remember that some hardware components are shared: for example, network interfaces and HBAs. If possible, you should use dedicated network adapters and HBAs for each virtualized SAP HANA system. The network and storage requirements are similar to a bare metal use case with respect to storage IO/latency and inter-node network bandwidth.

Co-existing SAP HANA and SAP Application Workloads

With SAP HANA TDI it is possible to run SAP HANA on shared infrastructure that also hosts non-HANA workloads as standard SAP applications. Scenarios where SAP HANA database bare metal installation along with virtualized SAP application workloads are common in the datacenter. It is important make sure there is appropriate storage IO and network bandwidth segregation so that HANA systems get their due to comfortably satisfy the storage and network KPIs for production support.

Scale-Up and Scale-Out SAP HANA Systems

Hosting multiple scale-up and scale out systems call for proper sizing of the infrastructure with a clear compute node to storage system ratio. The number of compute nodes along with storage arrays has to be determined based on the number total number of SAP HANA nodes that would make up the system landscape and would involve corresponding scaling of associated compute gear and networking components based on port availability and usage.

Hardware Requirements for the SAP HANA Database

There are hardware and software requirements defined by SAP to run SAP HANA systems. This Cisco Validated Design uses guidelines provided by SAP.

For additional information, go to: SAP HANA Hardware Directory

CPU

With the release of the Second-Generation Intel® Xeon® Scalable processors (Cascade Lake), SAP supports Intel Xeon Platinum CPUs with 28 cores per CPU in SAP HANA environments. The Cisco UCS B-Series Blade Servers are capable to be configured with full or half size amount of Intel Xeon scalable family CPUs.

Memory

The Cisco Integrated Management Controller (IMC) and Cisco UCS Manager Release 4.0(4) introduce support for Intel® Optane™ Data Center persistent memory modules (DCPMM) on Cisco UCS M5 servers based on the Second-Generation Intel ® Xeon® Scalable processors (Cascade Lake).

Detailed information on the configuration and management is available in the whitepaper Cisco UCS: Configuring and Managing Intel Optane Data Center Persistent Memory Modules.

Intel Optane DCPMMs must be installed with DRAM dual in-line memory modules (DIMM) in the same system and will not function without any DRAM DIMMs installed. In two- or four-socket configurations, each socket contains two IMCs. Each memory controller connects to three double data rate (DDR) memory channels which connects to two physical DIMM/persistent memory slots.

SAP HANA 2.0 SPS03 revision 35+ currently support various memory capacity ratios between Intel Optane DCPMM and DRAM DIMMs in the same system and will not function without any DRAM DIMMs installed.

In DDR4 DIMM memory only population the following configuration rules apply:

- Homogenous symmetric assembly of dual in-line memory modules (DIMMs) for example, DIMM size or speed should not be mixed
- Maximum use of all available memory channels
- Supported Memory Configuration for SAP NetWeaver Business Warehouse (BW) and DataMart
  - 1.5 TB on Cisco UCS B200 M5 Servers with 2 CPUs
  - 3 TB on Cisco UCS B480 M5 Servers with 4 CPUs
- Supported Memory Configuration for SAP Business Suite on SAP HANA (SoH)
  - 3 TB on Cisco UCS B200 M5 Servers with 2 CPUs
  - 6 TB on Cisco UCS B480 M5 Servers with 4 CPUs

In Intel Optane DCPPM/DDR4 DIMM mixed memory population the following rules apply:

- Maximum use of all available memory channels
- Supported Memory Configuration for SAP Business Suite on SAP HANA (SoH)
  - 7.5 TB on Cisco B200 M5 Servers with 2 CPUs
  - 18 TB on Cisco B480 M5 Servers with 4 CPUs

Network

An SAP HANA data center deployment can range from a database running on a single host to a complex distributed system. Distributed systems can get complex with multiple hosts located at a primary site having one or more secondary sites; supporting a distributed multi-terabyte database with full fault and disaster recovery.

SAP HANA has different types of network communication channels to support the different SAP HANA scenarios and setups:

- Client zone. Different clients, such as SQL clients on SAP application servers, browser applications using HTTP/S to the SAP HANA XS server and other data sources (such as BI) need a network communication channel to the SAP HANA database.
- Internal zone. The internal zone covers the communication between hosts in a distributed SAP HANA system as well as the communication used by SAP HANA system replication between two SAP HANA sites.
- Storage zone. Although SAP HANA holds the bulk of its data in memory, the data is also saved in persistent storage locations. In most cases, the preferred storage solution involves separate, externally attached storage subsystem devices that can provide dynamic mount-points for the different hosts, according to the overall landscape. A storage area network (SAN) can also be used for storage connectivity.

Storage

SAP HANA is an in-memory database which uses storage devices to save a persistent copy of the data for the purpose of startup and fault recovery without data loss. The choice of the specific storage technology is driven by various requirements like size, performance, and high availability. To use a storage system in the SAP HANA TDI option, the storage must be certified as SAP HANA certified Enterprise Storage.

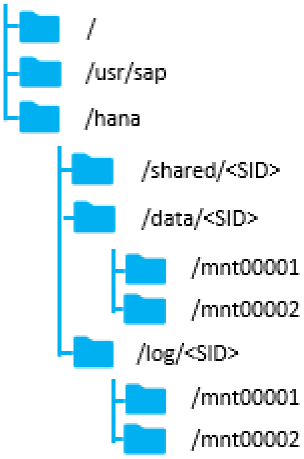
The Solution References section provides links to the SAP HANA certified hardware directory and a white paper which discuss all relevant information about the storage requirements.

The solution needs to pass the SAP HANA Hardware and Cloud Measurement Tool (HCMT) check successfully prior of reporting IO performance related SAP HANA incidents.

File System Layout

Figure 19 illustrates the SAP HANA file system layout and the recommended storage sizes to install and operate SAP HANA. The recommendation is to reserve for the Linux operating system root volume 10GB of disk space and to store the SAP software 50GB of disk space. In this solution the root volume /root and SAP software /usr/sap are in the same disk volume, although they can be setup in two different volumes as well.

Figure 19. **File System Layout for 2 Node Scale-Out System**



The sizing for SAP HANA file system volumes is based on the amount of memory equipped on the SAP HANA host.

Scale-Up Solutions

The recommended, minimum disk space requirements for SAP HANA TDI installations are:

/ (root)	100 GB inclusive of space required for /usr/sap
/hana/shared	1 × RAM or 1TB whichever is less
/hana/data	1 × RAM
/hana/log	512 GB

Scale-Out Solutions

The recommended, minimum disk space requirements for SAP HANA TDI installations are:

/ (root)	100 GB inclusive of space required for /usr/sap
/hana/shared	1 × RAM for every 4 active HANA nodes
/hana/data	1 × RAM for each active HANA node
/hana/log	512 GB for each active HANA node

Operating System

The supported operating systems for SAP HANA with Intel® Optane™ DCPMM are, as follows:

- SUSE Linux Enterprise Server for SAP Applications 15 GA
- Red Hat Enterprise Linux for SAP HANA 7.6

High Availability

The infrastructure for an SAP HANA solution must not have single point of failure. To support high-availability, the hardware and software requirements are:

- External storage: Redundant data paths, dual controllers, and a RAID-based configuration are required
- Ethernet switches: Two or more independent switches should be used

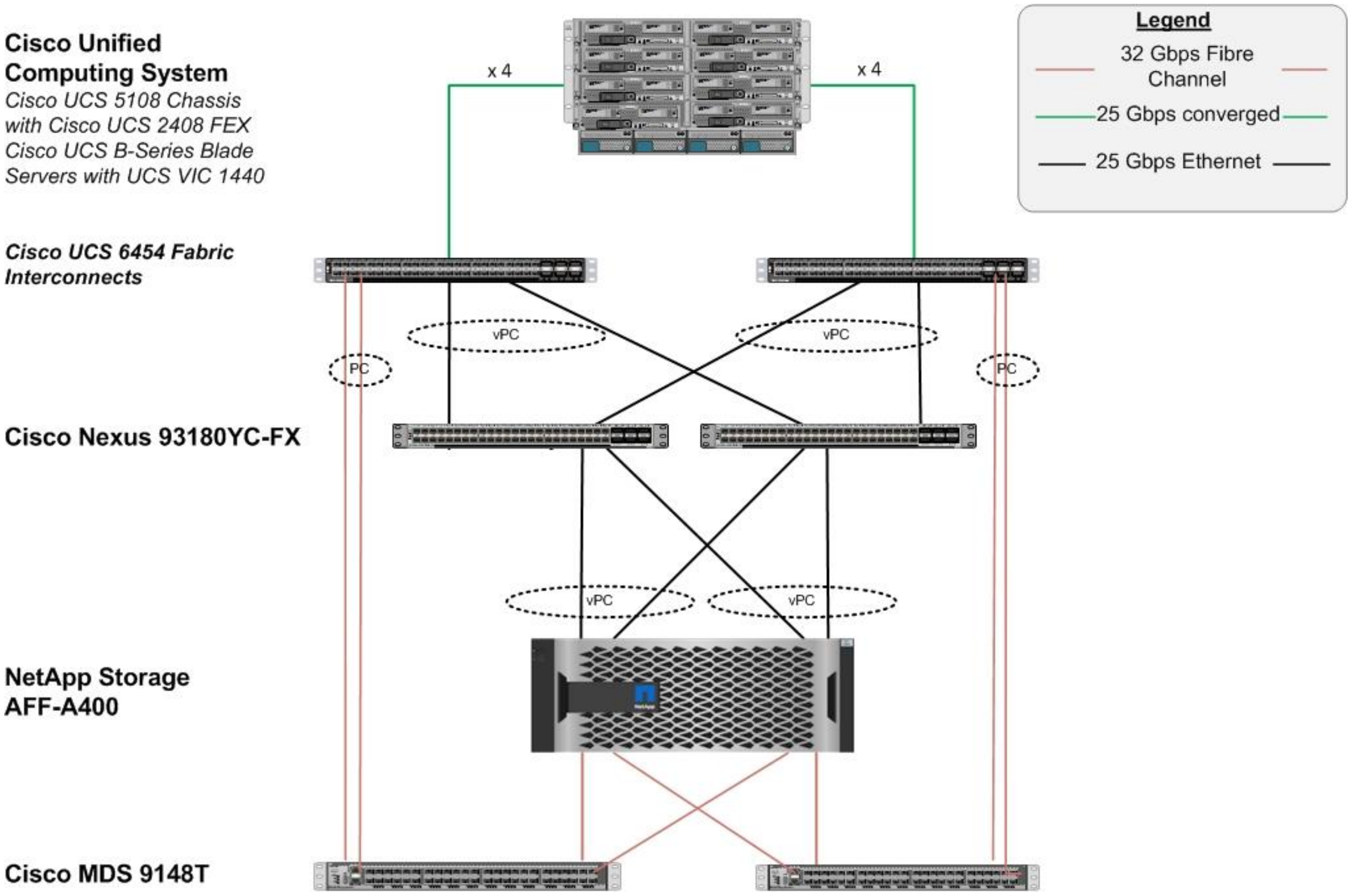
SAP HANA Scale-Out comes with integrated high-availability functionality. If an SAP HANA system is configured with a stand-by node, a failed part of SAP HANA will start on the stand-by node automatically. For automatic host failover, storage connector API must be properly configured for the implementation and operation of the SAP HANA.

Although not tested and validated in this design, additional high-availability solutions like SAP HANA System Replication with Linux Cluster are available as well. For detailed information from SAP refer to SAP HANA Administration Guide - High Availability for SAP HANA or SAP HANA Administration Guide – Configuring SAP HANA System Replication.

Physical Topology

Figure 20 shows the SAP HANA TDI solution built on FlexPod components and the network connections for a configuration with the Cisco UCS 6454 Fabric Interconnects. This design has port-channeled 25 Gb Ethernet connections between the Cisco UCS 5108 Blade Chassis and the Cisco UCS Fabric Interconnects and 40/100 Gb Ethernet connections between the Cisco UCS Fabric Interconnect and Cisco Nexus 9000s, and between Cisco Nexus 9000s and NetApp AFF A400 storage array.

Figure 20. FlexPod Topology


Cisco Unified Computing System
Cisco UCS 5108 Chassis with Cisco UCS 2408 FEX Cisco UCS B-Series Blade Servers with UCS VIC 1440
Cisco UCS 6454 Fabric Interconnects
Cisco Nexus 93180YC-FX
NetApp Storage AFF-A400
Cisco MDS 9148T
x 4
x 4
vPC
vPC
PC
PC
vPC
vPC
Legend
32 Gbps Fibre Channel
25 Gbps converged
25 Gbps Ethernet

This infrastructure option expanded with Cisco MDS switches sitting between the Cisco UCS Fabric Interconnect and the NetApp AFF A400 to provide FC-booted hosts with 32 Gb FC block-level access to storage. The reference architecture reinforces the "wire-once" strategy, because as additional storage is added to the architecture, no re-cabling is required from the hosts to the Cisco UCS fabric interconnect.

The reference 32FC based hardware configuration includes:

- Two Cisco Nexus 93180YC-FX switches
- Two Cisco UCS 6454 fabric interconnects with Cisco UCS 2408 fabric extenders
- Two Cisco MDS 9148T multilayer fabric switches
- One NetApp AFF A400 (HA pair) running ONTAP 9.7 with external NVMe SSD drives

Design Specifications

Compute Layer

The Cisco UCS platform provides the compute resources in the FlexPod Datacenter. The design supports both Cisco UCS B-Series blade servers and Cisco UCS C-Series rack-mount servers, connected and managed through a pair of Cisco UCS Fabric Interconnects running Cisco UCS Manager.

Each Cisco UCS server is equipped with a Virtual Interface Cards (VIC) that aggregate all LAN and SAN traffic to and from the server across a single interface.

The blade servers are housed in a Cisco UCS 5108 Blade Server Chassis that can support up to 8 Cisco UCS B200 M5s or 4 Cisco UCS B480 M5 blades. A blade server chassis can have up to two fabric extenders (FEX) or I/O Modules (IOM) that connect the chassis to the Fabric Interconnects.

In FlexPod designs, the supported Cisco UCS C-Series servers can be either directly connected to the FIs using 25GbE links or through supported top-of-rack Cisco Nexus Fabric Extenders that connects to the FIs. FlexPod designs do require that these servers be managed by Cisco UCS Manager in order to ensure consistent policy-based provisioning, stateless computing, and uniform management of the server resources, independent of the form-factor.

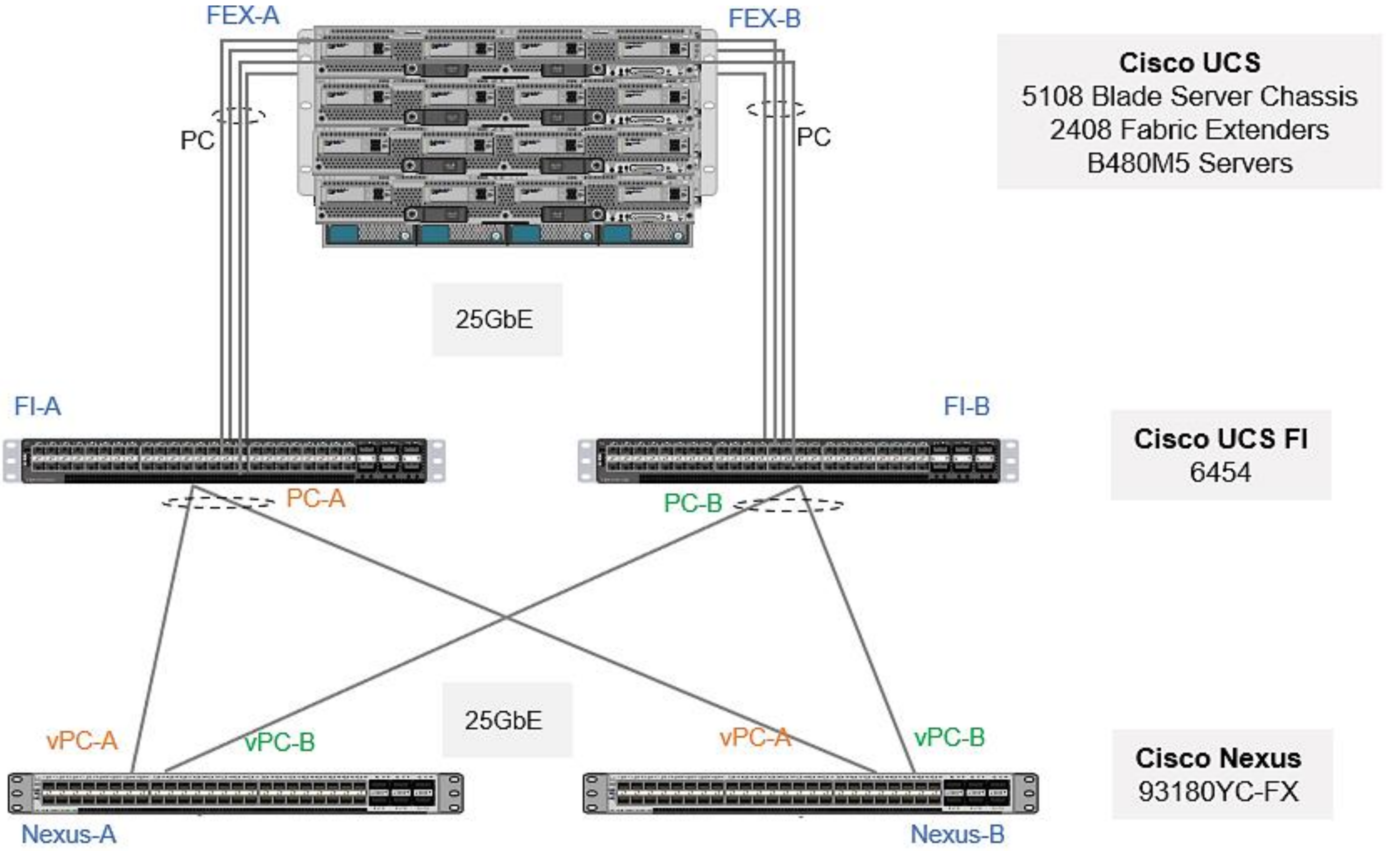
Cisco UCS Fabric Interconnect Connectivity to Datacenter Network

In this design, each Fabric Interconnect connects into a pair of upstream Cisco Nexus 9000 access switches. The links on each FI are bundled into a port-channel while links on access switches that connect to this FI are bundled into a vPC. This design provides link and node-level redundancy, higher aggregate bandwidth, and the flexibility to increase the bandwidth as the uplink bandwidth needs grow.

Validation - Compute Layer Connectivity

To validate the compute layer design, a Cisco UCS 5108 server chassis with Cisco UCS B480 M5 blade servers are connected through a pair of Cisco UCS 6454 Fabric Interconnects as shown in Figure 21.

Figure 21. Validated - Compute Layer Connectivity



The blade server chassis is deployed using 2 x Cisco UCS 2408 FEX (IOMs), with each FEX connecting to one fabric interconnect, forming two distinct paths (Fabric-A, Fabric-B) through the unified fabric as follows:

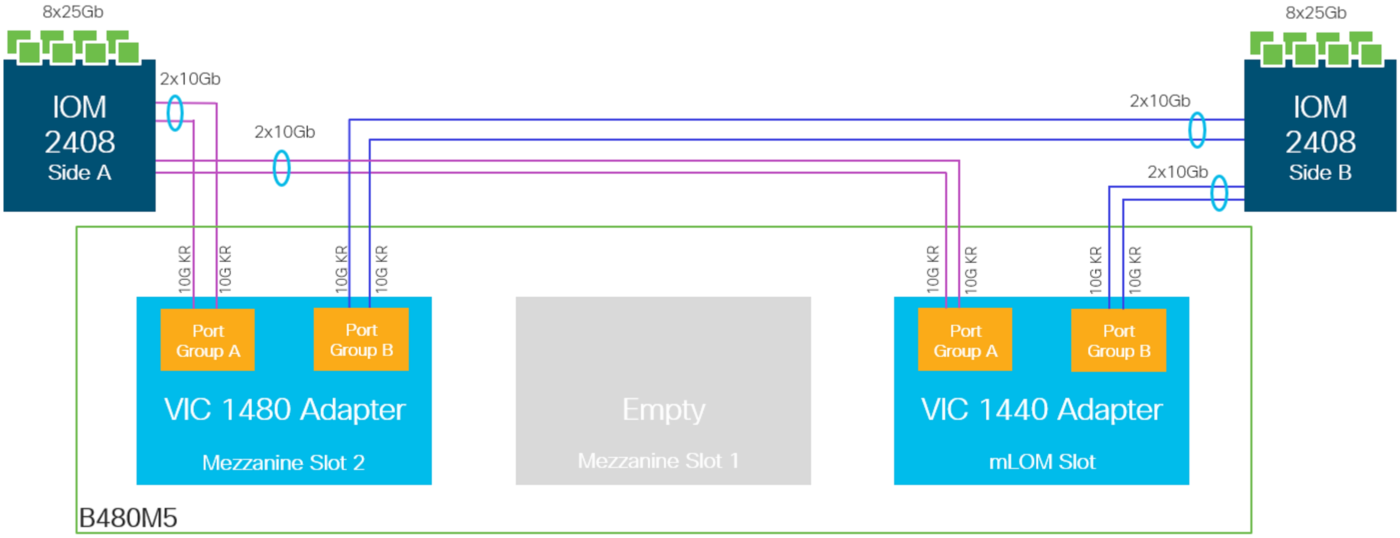
- Fabric-A: 4 x 25GbE links from FEX-A to FI-A, links bundled into a port-channel
- Fabric-B: 4 x 25GbE links from FEX-B to FI-B, links bundled into a port-channel

This provides the blade server chassis with an aggregate uplink bandwidth of 200Gbps. Additional ports on each FEX can be used to further increase the bandwidth. For the Cisco UCS 2408 FEX model, all 8 ports can be used for a total of 400Gbps of uplink bandwidth to a single blade server chassis.

The blade servers in the blade server chassis are each deployed with a mLOM slot VIC 1440 and mezzanine VIC 1480 adapters, as illustrated in Figure 22. The Cisco UCS VIC 1440 adapter provides 40Gbps of uplink connectivity, 20Gbps through each Fabric (Fabric-A, Fabric-B) path. The uplink bandwidth is increased to 40Gbps per Fabric path with the additional mezzanine slot VIC 1480 adapter. That gives 80Gbps to a Cisco UCS B480 M5. It is highly recommended to use Cisco UCS VIC 1440 + VIC 1480 for optimum bandwidth availability.

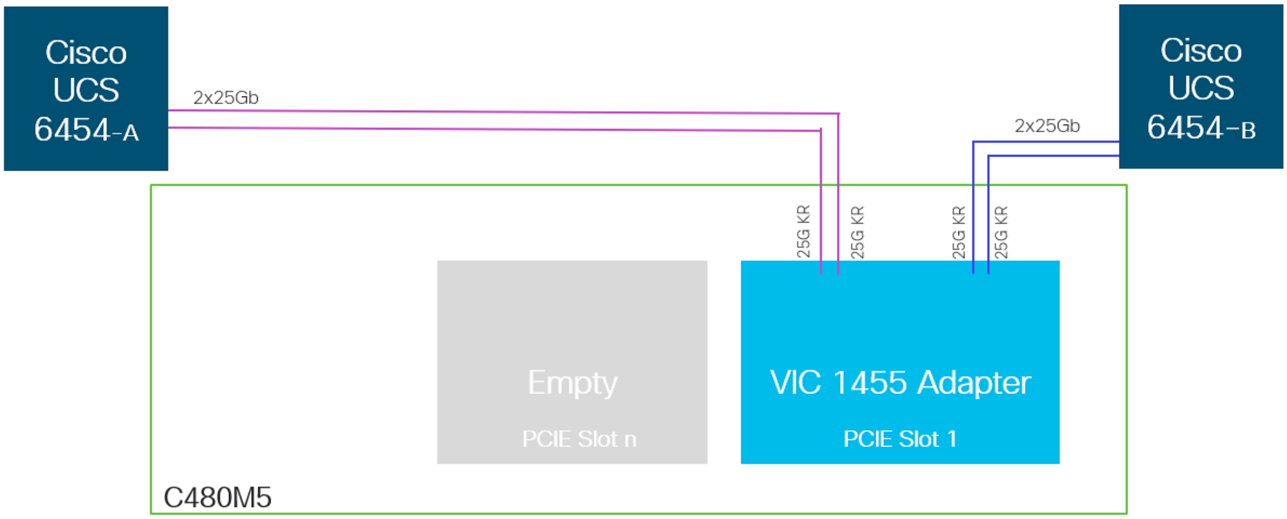
The port expander slot with Cisco UCS VIC 1440 is unsupported with IOM 2408.

Figure 22. **Cisco UCS B480 M5 Blade Server VIC 1440/1480 Uplink Connectivity**



The Cisco UCS C480 M5 rack-mount servers are deployed with quad-port VIC 1455 adapter and directly connected to Fabric Interconnects, as shown in Figure 23, with two VIC (25GbE) port/s going to each FI, providing the rack servers with an aggregate uplink bandwidth of 100Gbps with high availability.

Figure 23. **Cisco UCS C480 M5 Rack-Mount Server - VIC 1455 Uplink Connectivity**



To connect to the upstream data center network, each FI is connected to a pair of Nexus 9300 series access layer switches in the validation setup as follows:

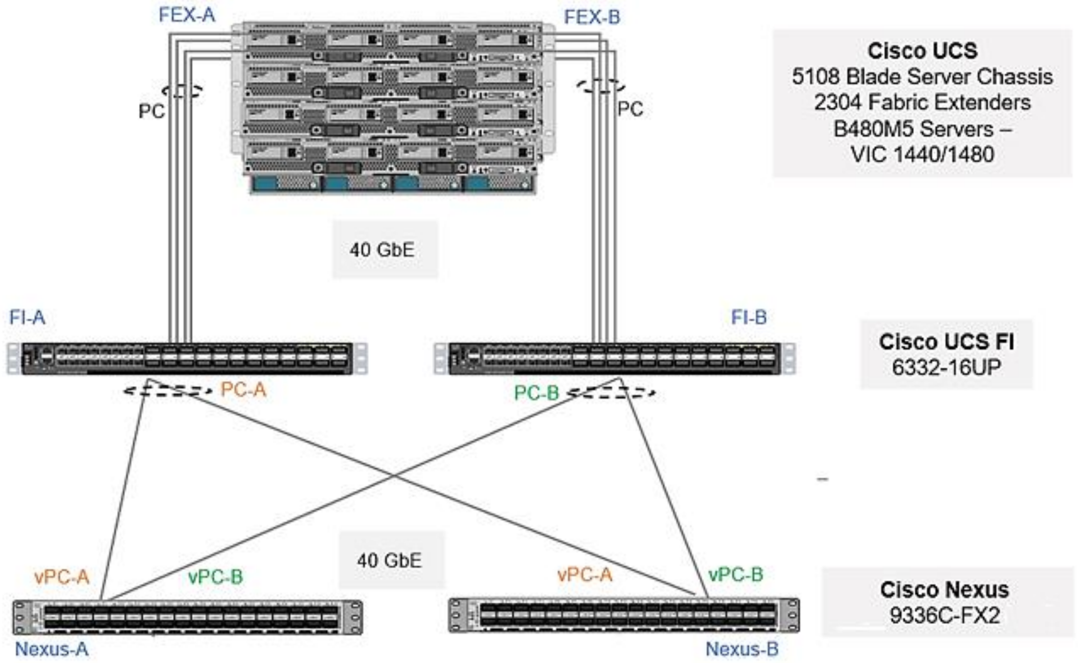
- 2 x 25GbE links from FI-A to access layer Nx93180YC-FX A
- 2 x 25GbE links from FI-B to access layer Nx93180YC-FX B

The FI uplink ports are configured in port channels with 2 ports each, with corresponding vPC configurations on the Nexus switches. This provides the UCS domain with redundant paths and 100 Gbps of aggregate uplink bandwidth to/from access layer catering to SAP HANA networks primarily the internode and shared NFS access to SAP HANA nodes. The uplink bandwidth can be further increased as needed by adding additional connections to the port-channel.

Configuration with Cisco UCS 6300 Series Fabric Interconnects

With Cisco UCS 6300 series fabric interconnects managing the Cisco UCS B480 M5 servers populated with VICs 1440, port expander and/or VIC 1480 via Cisco UCS 2304 FEXs, it will be an end-to-end 40 GbE, with Nx9336C-FX2 40/100GbE switches, as illustrated in Figure 24.

Figure 24. Design Option with 3rd Gen FIs



Design Options

The Cisco UCS B-series servers used in the validated design setup are configured in the design with:

- SAN Boot – Persistent operating system installation, independent of the physical blade for true stateless computing
- Cisco UCS VIC 1440 + Cisco UCS VIC 1480
- Intel® Optane™ Data Center Persistent Memory Module (DCPMM)

Memory for databases is currently small, expensive, and volatile. Intel Optane DC persistent memory is denser, more affordable, and persistent, and it performs at speeds close to that of memory. These features of Intel Optane DC persistent memory can help lower TCO through reduced downtime and simplified data-tiering operations. These same features can also make SAP HANA in-memory databases economically viable for a wider range of use cases. Intel Optane DC persistent memory provides near-DRAM in-memory computing speed in a form factor similar to that of dual inline memory modules (DIMMs) at a lower price per gigabyte than DRAM. With its persistence, performance, and lower cost per gigabyte than conventional memory, Intel Optane DC persistent memory can help reduce total cost of ownership (TCO), reshape the way that businesses tier their data for database systems, and open new use cases for the speed and power of the SAP HANA platform.

Table 3 and Table 4 lists the server specifications with possible memory configurations for the SAP HANA use case.

Table 3. Cisco UCS B480 M5 Blade Server and Cisco UCS C480 M5 Rack Server Configuration

CPU specifications	Intel Xeon Platinum 8276L/8280L processor: Quantity 4
Possible memory configurations	32-GB DDR4: Quantity 24 (768 GB) 64-GB DDR4: Quantity 24 (1.5 TB) 128-GB DDR4: Quantity 24 (3 TB)
Possible DCPMM memory configurations	128-GB DCPMM: Quantity 24 (3 TB) 256-GB DCPMM: Quantity 24 (6 TB) 512-GB DCPMM: Quantity 24 (12 TB)

Table 4. Cisco UCS C240 and Cisco UCS C220 M5 Rack Server and Cisco UCS B200 M5 Blade Server Configuration

CPU specifications	Intel Xeon Platinum 8276L/8280L processor: Quantity 2
Possible memory configurations	16-GB DDR4: Quantity 12 (192 GB) 32-GB DDR4: Quantity 12 (384 GB) 64-GB DDR4: Quantity 12 (768 TB) 128-GB DDR4: Quantity 12 (1.5 TB)
Possible DCPMM memory configurations	128-GB DCPMM: Quantity 12(1.5 TB) 256-GB DCPMM: Quantity 12 (3 TB) 512-GB DCPMM: Quantity 12 (6 TB)

Intel Optane DCPMMs must be installed with DRAM DIMMs in the same system. The persistent memory modules will not function without any DRAM DIMMs installed. In two-, four-, and eight-socket configurations, each socket contains two IMCs. Each memory controller is connected to three double data rate (DDR) memory channels that are then connected to two physical DIMM persistent memory slots.

SAP HANA 2.0 SPS 03 currently supports various capacity ratios between Intel Optane DCPMMs and DIMMs.

For information regarding the Cisco UCS compute with Intel Optane DC Persistent Memory Module (DCPMM) and possible capacity ratios between DCPMMs and DIMMs, go to: https://www.cisco.com/c/dam/en/us/products/servers-unified-computing/ucs-b-series-blade-servers/whitepaper-c11-742627.pdf

Storage layer

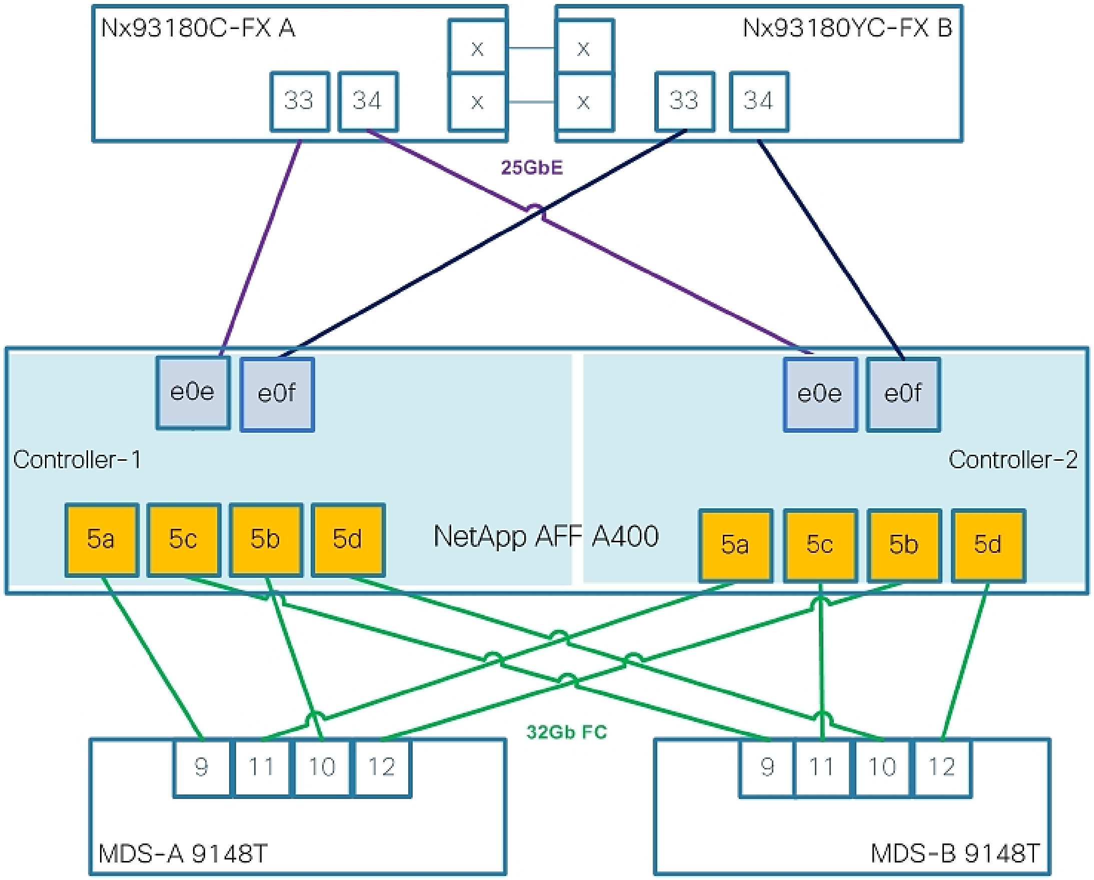
This design uses NetApp AFF A400 to provide the storage resources. This FlexPod Datacenter solution for SAP HANA leverages SAN booting, FC based access to persistence partitions and NFS protocol for the shared filesystem /hana/shared access to HANA nodes. NetApp Storage connects into the Cisco MDS switches using all four onboard 32Gb FC ports configured as targets and access layer Cisco Nexus switches using dual 25GbE uplinks, configured for port-channeling to provide higher aggregate bandwidth and availability. Cisco Nexus switches that connect to the NetApp storage is configured for vPC to provide node-availability, in addition to link-availability and higher aggregate bandwidth.

Validation - Storage Layer Connectivity

The storage controllers are connected to a Cisco MDS 9148T SAN switching infrastructure for FC boot and is connected to Cisco Nexus 93180YC-FX for all Ethernet traffic. Although smaller configurations can use the direct-attached, FC/FCoE storage method of the Cisco UCS fabric interconnect, the Cisco MDS provides increased scalability for larger configurations. The Cisco MDS has multiple Cisco UCS domains and the ability to connect to a data center SAN.

An ONTAP storage controller uses N_Port ID virtualization (NPIV) to allow each network interface to log in to the FC fabric using a separate worldwide port name (WWPN). This feature allows a host to communicate with a FC target network interface, regardless of where that network interface is placed. To ensure that NPIV is enabled, use the '*show npiv status*' command on the MDS switch. Each controller can be equipped with host bus adapters (HBA) that operate at 8Gb, 16Gb, and 32Gb FC. For the FC design, the FC HBA ports operate in FC target mode and the ports are connected to two SAN fabrics. This method provides increased redundancy to make sure that the paths from the host to its storage LUNs are always available. Figure 28 shows the port and interface assignment connection diagram for the AFF storage to the Cisco MDS 9148T SAN fabrics as well as access layer Cisco Nexus switches. This FlexPod design uses the following port and interface assignments. In this design, NFS uses 25GbE and FC uses the 32Gb bandwidth.

Figure 25. **Storage NFS / FC Connectivity**



NetApp AFF A400 supports 8/16/32 Gb FC connections. To connect to the SAN fabric, the AFF A400 is connected to a pair of Cisco MDS 9148T switches, as follows:

- 4 x 32GbE links from each array controller's ports to SAN Fabrics A and B, two links to each side for greater control over availability management in case of failover scenarios.

The connectivity described above, provides NetApp AFF A400 with redundant uplinks through separate Cisco MDS switches and 64 Gb (128Gb FC for the HA controller pairs) of FC bandwidth to the fabric.

NetApp AFF A400 supports on board 25/40/100GbE ports depending on the configuration. To connect to the upstream data center network, the AFF A400 is connected to a pair of Nexus 9300 series access layer switches as follows:

- 2 x 25GbE links from each array controller's onboard ports to access switches, one link to each Nexus-A, Nexus-B
- Port-channel configuration with 2 x 25GbE ports on each array controller
- vPC configuration on Nexus switches, one vPC to each NetApp controller. Each VPC has 2 links, one from each Nexus switch to a NetApp controller.

The connectivity described above, provides each NetApp AFF A400 with redundant uplinks through separate access layer switches and 50Gbps (100Gbps for the HA controller pair) of bandwidth to the fabric. With SAP

HANA persistence traffic being FC managed, 50Gbps Ethernet bandwidth per fabric, more than suffices the SAP HANA networks and /hana/shared filesystem traffic.

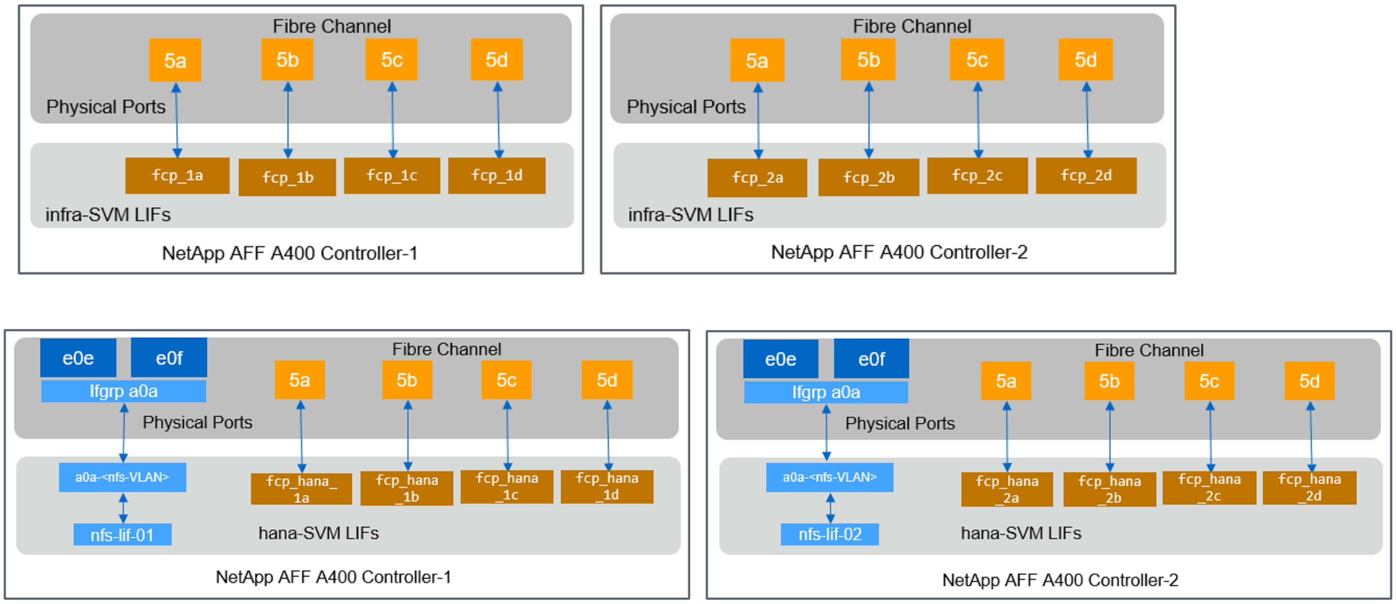
In this configuration, NetApp AFF A400 onboard ports e0g and e0h were still available for scaling the bandwidth with two more possible 25GbE links to Nexus switches.

SAN Boot

NetApp recommends implementing SAN boot for Cisco UCS Servers in the FlexPod Datacenter solution. Implementing SAN boot enables the operating system to be safely secured by the NetApp AFF storage system, providing better performance and flexibility. In this design, FC SAN boot is validated.

In the FC SAN boot architecture, each Cisco UCS Server boots by connecting the NetApp AFF storage to the Cisco MDS switch. The 32Gb FC storage ports, in this example 5a, 5b, 5c and 5d, are connected to the Cisco MDS switch. The FC LIFs are created on the physical ports for each SVM and each FC LIF is uniquely identified by its target WWPN. The storage system target WWPNs can be zoned with the server initiator WWPNs in the Cisco MDS switches. The FC boot LUN is exposed to the servers through the FC LIF by using the MDS switch. This feature enables only the authorized server to have access to the boot LUN. See Figure 26 for the port and LIF layout.

Figure 26. **FC - SVM specific ports and LIF layout**



Unlike NAS network interfaces, the SAN network interfaces are not configured to fail over during a failure. Instead if a network interface becomes unavailable, the host chooses a new optimized path to an available network interface by communicating with the storage controllers via Asymmetric Logical Unit Access (ALUA). The ALUA protocol is an industry standard protocol supported by NetApp that is used to provide information about SCSI targets. This information enables a host to identify the optimal path to the storage.

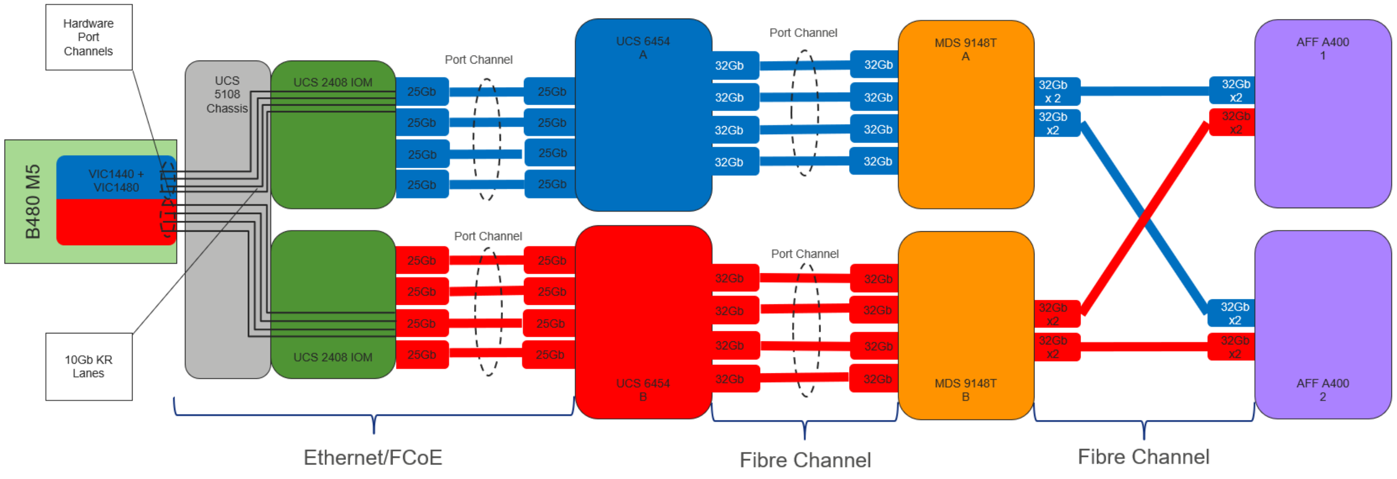
Network Layer – FC and NFS Traffic

End-to-End Fibre Channel Network Connectivity

The Cisco MDS 9148T is the key component bringing together the 32Gbps Fibre Channel capabilities of the other pieces of this design. Redundant 32 Gbps Fibre Channel links extend from the MDS 9148Ts to both the storage controllers and the Cisco UCS 6454 FIs. Passage of this traffic shown in Figure 30 from left to right is as follows:

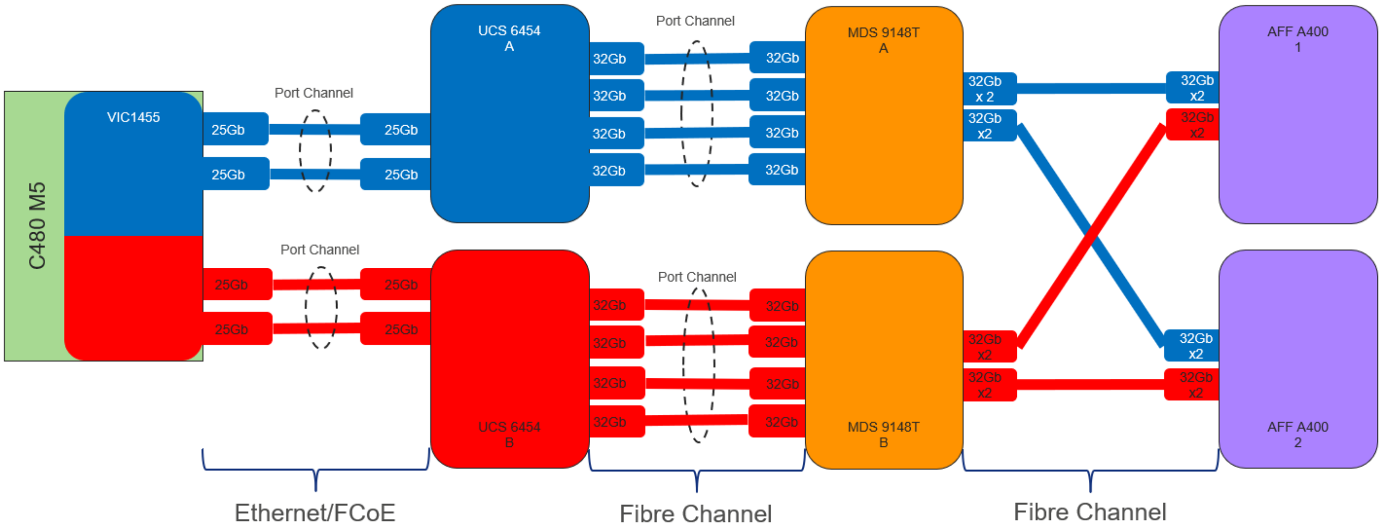
- Coming from the Cisco UCS B480 M5 server, equipped with a VIC 1440 adapter and mezzanine VIC 1480, allowing for 40Gb on each side of the fabric (A/B) into the server.
- Pathing through 10Gb KR lanes of the Cisco UCS 5108 Chassis backplane into the Cisco UCS 2408 IOM (Fabric Extender).
- Connecting from each IOM to the Fabric Interconnect with up to eight 25Gb links automatically configured as port channels during chassis association.
- Continuing from the Cisco UCS 6454 Fabric Interconnects into the Cisco MDS 9148T with a 128Gbps (4x32Gbps) SAN port channel.
- Ending at the AFF A400 Controllers with 32Gbps FC links.

Figure 27. FC End-to-End Design with Cisco UCS B480 M5



The equivalent view for a Cisco UCS C480 M5 server is shown in Figure 28. The main difference is that the two 25Gbps interfaces are connected directly between the VIC 1455 and the FI and are port-channeled into a 50Gbps interface. In this case, a FC flow is limited to 25 Gbps:

Figure 28. **FC End-to-End Design with Cisco UCS C480 M5**

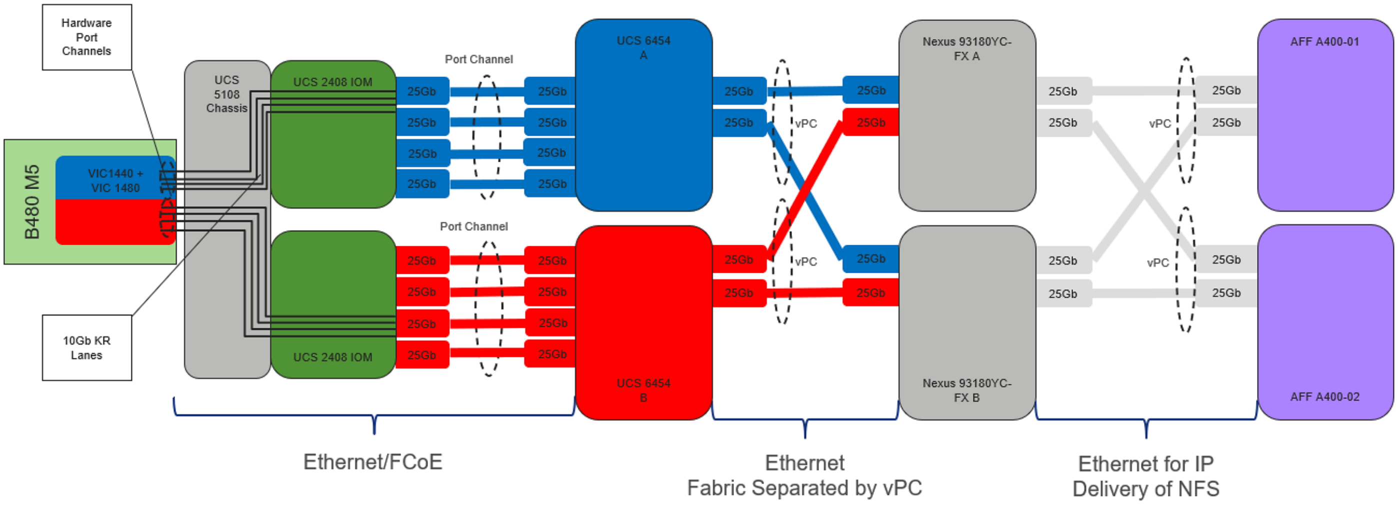


End-to-End IP Network Connectivity

The Cisco Nexus 9000 is the key component bringing together the 40/100Gbps capabilities of the other pieces of this design. vPCs extend to both the AFF A400 Controllers and the Cisco UCS 6454 Fabric Interconnects. Passage of this traffic shown in Figure 32 from left to right is as follows:

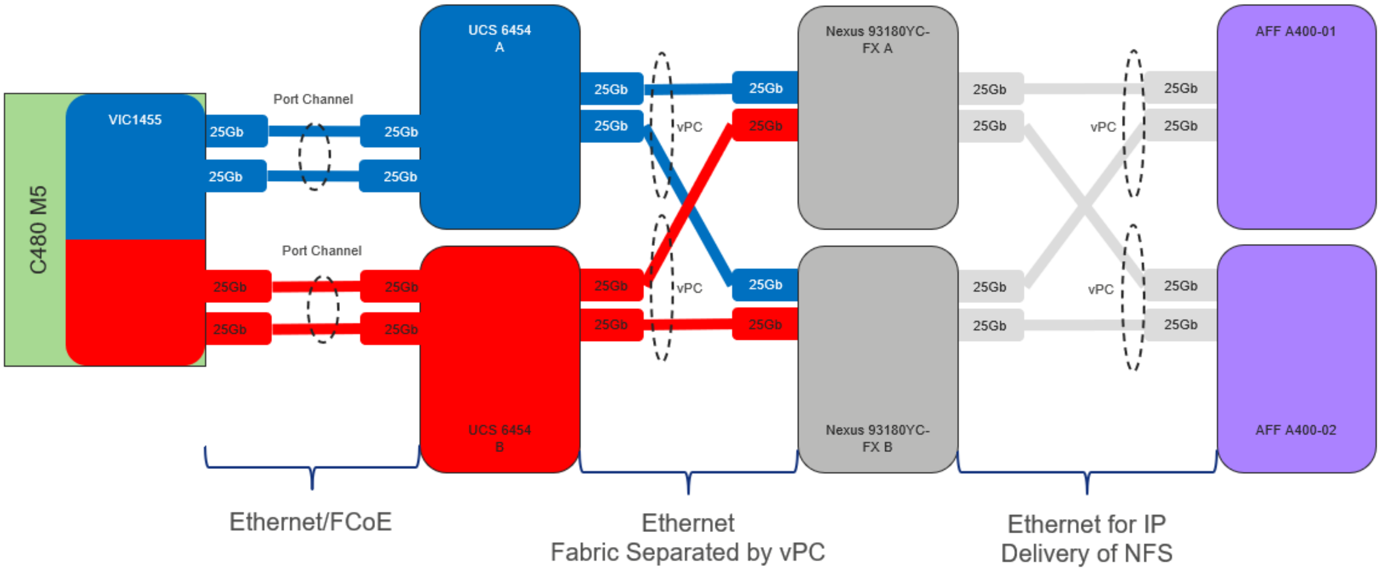
- Coming from the Cisco UCS B480 M5 server, equipped with a VIC 1440 adapter and mezzanine VIC1480, allowing for 20Gb on each side of the fabric (A/B) into the server.
- Pathing through 10Gb KR lanes of the Cisco UCS 5108 Chassis backplane into the Cisco UCS 2408 IOM (Fabric Extender).
- Connecting from each IOM to the Fabric Interconnect with up to eight 25Gb links automatically configured as port channels during chassis association.
- Continuing from the Cisco UCS 6454 Fabric Interconnects into the Cisco Nexus 93180YC-FX with a bundle of 25Gb ports presenting each side of the fabric from the Nexus pair as a common switch using a vPC.
- Ending at the AFF A400 Controllers with 25Gb bundled vPCs from the Nexus switches now carrying both sides of the fabric.

Figure 29. IP Traffic with Cisco UCS B-Series Server



The equivalent view for a Cisco UCS C-Series server is shown in Figure 30. The main difference is that the two 25Gbps interfaces are connected directly between the VIC 1455 and the FI and are port-channeled into a 50Gbps interface. In this case, a given flow is limited to 25 Gbps:

Figure 30. IP traffic with Cisco UCS C-Series Server



Solution Validation

This section provides a high-level summary of the FlexPod Datacenter Design validation. Installation procedures for both, SUSE, and Red Hat Linux, following best practices from Cisco, NetApp, and SAP. All SAP HANA TDI phase 5 requirements are tested and passed for performance and high availability, including:

- Cisco UCS setup and configuration
- NetApp setup and configuration
- FCP boot option
- Operating System Configuration for SAP HANA
- Installation of SAP HANA 2.0 SPS5
- Performance Tests using SAP's test tools

Validated Hardware and Software

Table 5 lists the hardware and software versions used during solution validation. It is important to note that Cisco and NetApp have interoperability matrixes that should be referenced to determine support for any specific implementation of FlexPod. Click the following links for more information:

- NetApp Interoperability Matrix Tool
- Cisco UCS Hardware and Software Interoperability Tool

Table 5. Validated Hardware and Software Revisions

Layer	Device	Image	Comments
Compute	Cisco UCS Fabric Interconnects 6454, Cisco UCS B480 M5	UCSM 4.1(1d)	Includes the Cisco UCS-IOM 2408, Cisco UCS Manager, Cisco UCS VIC 1440, and Cisco UCS VIC 1480. Also valid for rack form factor Cisco UCS C480 M5 and two socket Cisco UCS blade and rack servers.

Network	Cisco Nexus 93180YC-FX NX-OS
	Cisco MDS 9148T
		7.0(3)I7(9)
		8.4(1a)	

Storage	NetApp AFF A400	ONTAP 9.7 with FCP and NFSv3 only for /hana/shared NFS access	
Operating		SLES for SAP Applications	FC SAN boot

Layer	Device	Image	Comments
System		15 SP1 RHEL for SAP HANA 8.1	

Summary

FlexPod features the latest Cisco UCS servers, Nexus fabric switches and NetApp All Flash storage. Cisco UCS has its own policy-based management with service profiles and self-integrating components. And it works with the Cisco Nexus series switches for a Unified Fabric, simple scaling, and high-performance I/O. NetApp AFF Arrays, along with ONTAP data management software defines truly unified storage that delivers the built-in storage efficiencies, integrated data protection, and intelligent management.

FlexPod Datacenter with SAP HANA is the optimal shared infrastructure foundation to deploy a variety of IT workloads that is future proofed with 32 Gbps FC or 25/40/100Gbps Ethernet connectivity. It is the optimal infrastructure foundation to deploy SAP HANA be it bare metal or virtualized to implement a TDI environment. It is validated for both SUSE Linux Enterprise Server and Red Hat Enterprise Linux operating systems. It is designed and validated using compute, network and storage best practices for high performance, scalability, and resiliency throughout the architecture. The flexibility and scalability of FlexPod also enables customers to start out with a right-sized infrastructure that can ultimately grow with and adapt to their evolving business requirements.

References

Products and Solutions

Cisco Unified Computing System:

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

Cisco UCS 6454 Fabric Interconnect:

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

Cisco UCS 5100 Series Blade Server Chassis:

http://www.cisco.com/en/US/products/ps10279/index.html

Cisco UCS B-Series Blade Servers:

http://www.cisco.com/en/US/partner/products/ps10280/index.html

Cisco UCS C-Series Rack Mount Servers:

http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-c-series-rack-servers/index.html

Cisco UCS Adapters:

http://www.cisco.com/en/US/products/ps10277/prod_module_series_home.html

Cisco UCS Manager:

http://www.cisco.com/en/US/products/ps10281/index.html

Cisco Nexus 9000 Series Switches:

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

Cisco MDS 9000 Multilayer Fabric Switches:

http://www.cisco.com/c/en/us/products/storage-networking/mds-9000-series-multilayer-switches/index.html

VMware vCenter Server:

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

VMware vSphere:

https://www.vmware.com/products/vsphere

NetApp ONTAP 9:

http://www.netapp.com/us/products/platform-os/ontap/index.aspx

NetApp AFF A-Series:

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

NetApp OnCommand:

http://www.netapp.com/us/products/management-software/

NetApp SnapCenter:

https://www.netapp.com/us/products/backup-recovery/snapcenter-backup-management.aspx

NetApp FCP based configuration guide

TR-4436: SAP HANA on NetApp All Flash FAS Systems with FCP Configuration Guide

SAP HANA Backup and Recovery with SnapCenter

https://www.netapp.com/us/media/tr-4614.pdf

SAP HANA Disaster Recovery with Asynchronous Storage Replication

https://www.netapp.com/us/media/tr-4646.pdf

Integrating NetApp ONTAP systems with SAP Landscape Management

https://www.netapp.com/us/media/tr-4018.pdf

Interoperability Matrixes

Cisco UCS Hardware Compatibility Matrix:

https://ucshcltool.cloudapps.cisco.com/public/

VMware and Cisco Unified Computing System:

http://www.vmware.com/resources/compatibility

NetApp Interoperability Matrix Tool:

http://support.netapp.com/matrix/

About the Authors

Pramod Ramamurthy, Technical Marketing Engineer, Cisco Systems, Inc.

Pramod is a Technical Marketing Engineer with Cisco UCS Solutions and Performance Group. Pramod has more than 15 years of experience in the IT industry focusing on SAP technologies. Pramod is currently focusing on the Converged Infrastructure Solutions design, validation and associated collaterals build for SAP HANA.

Marco Schoen, Technical Marketing Engineer, NetApp, Inc.

Marco is a Technical Marketing Engineer with NetApp and has over 20 years of experience in the IT industry focusing on SAP technologies. His specialization areas include SAP NetWeaver Basis technology and SAP HANA. He is currently focusing on the SAP HANA infrastructure design, validation and certification on NetApp Storage solutions and products including various server technologies.

Acknowledgements

For their support and contribution to the design, validation, and creation of this Cisco Validated Design, the authors would like to thank:

- Shailendra Mruthunjaya, Cisco Systems, Inc.

Feedback

For comments and suggestions about this guide and related guides, join the discussion on Cisco Community at https://cs.co/en-cvds.

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**.