FlexPod Datacenter for SAP Solution with Cisco Nexus 9000 Switches
Design and Deployment of SAP HANA and SAP Application on Cisco UCS, Cisco Nexus 9000 Series Switches and NetApp FAS Storage

Last Updated: July 30, 2015
About Cisco Validated Design (CVD) Program

The CVD program consists of systems and solutions designed, tested, and documented to facilitate faster, more reliable, and more predictable customer deployments. For more information visit 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.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksyx, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networxers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0809R)

© 2015 Cisco Systems, Inc. All rights reserved.
About the Authors

Shailendra Mruthunjaya is a Technical Marketing Engineer with Cisco UCS Solutions and Performance Group and has over 4 years of experience on SAP HANA with Cisco UCS platform. Shailendra has designed several SAP landscapes in public and private cloud environments. He is currently focused on developing and validating infrastructure best practices for SAP applications on Cisco UCS Servers, Cisco Nexus products and storage technologies.

Ulrich Kleidon is a Principal Engineer with Cisco UCS Solutions and Performance group has over 10+ years of experience in compute, network, storage and server virtualization design. Ulrich has delivered solutions around Server and SAP applications with extensive experience with Cisco UCS, Nexus products and Storage technologies. Ulrich has worked on performance and benchmarking on Cisco UCS servers. Ulrich holds certification in SAP NetWeaver Administration and Cisco Unified Computing Systems Design Specialist.

Ralf Klahr is a Technical Marketing Engineer with Cisco UCS Solutions and Performance Group and has over 20 years of experience in the IT industry focusing on SAP technologies. His specialization areas include SAP Landscape virtualization and SAP NetWeaver Basis technology. He is currently focused on the SAP HANA infrastructure design and validation to ensure reliable customer deployments.

Acknowledgements

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

- Siva Sivakumar, Cisco Systems, Inc.
- Shanthi Adloori, Cisco Systems, Inc.
- Michael Dougherty, Cisco Systems, Inc.
- Chris O’Brien, Cisco Systems, Inc.
- Dan Laden, Cisco Systems, Inc.
- Bathumalai Krishnan, Cisco Systems, Inc
- Matthias Schlarb, Cisco Systems, Inc.
- Nils Bauer, NetApp
- Marco Schön, NetApp
FlexPod Datacenter for SAP Solution with Cisco Nexus 9000 Switches

About this Document

Cisco® Validated Designs include 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 customers. Cisco and NetApp have partnered to deliver FlexPod, which serves as the foundation for a variety of workloads and enables efficient architectural designs that are based on customer requirements. A FlexPod solution is a validated approach for deploying Cisco and NetApp technologies as a shared cloud infrastructure. This document describes the architecture and deployment procedures for SAP HANA Tailored DataCenter Integration option for FlexPod infrastructure composed of Cisco® compute and switching products, VMware® virtualization and NetApp® NFS and iSCSI-based SAN storage components. The intent of this document is to show the configuration principles with the detailed configuration steps.

Target Audience

The intended audience for this document includes, but is not limited to, sales engineers, field consultants, professional services, IT managers, partner engineering, and customers deploying the FlexPod Datacenter Solution for SAP HANA with NetApp clustered Data ONTAP®. External references are provided wherever applicable, but readers are expected to be familiar with the technology, infrastructure, and database security policies of the customer installation.

Purpose of this Document

This document describes the steps required to deploy and configure a FlexPod Datacenter Solution for SAP HANA. Cisco’s validation provides further confirmation with regard to component compatibility, connectivity and correct operation of the entire integrated stack. This document showcases one of the variants of cloud architecture for SAP HANA. While readers of this document are expected to have sufficient knowledge to install and configure the products used, configuration details that are important to the deployment of this solution are provided in this CVD.
Names, Terms and Definitions Used in this Document

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAP HANA</td>
<td>SAP HANA Database</td>
</tr>
<tr>
<td>TDI</td>
<td>Tailored Data Center Integration</td>
</tr>
<tr>
<td>KPI</td>
<td>Key Performance Indicators</td>
</tr>
<tr>
<td>SoH</td>
<td>SAP Business Suite on SAP HANA Database</td>
</tr>
<tr>
<td>BWoH</td>
<td>SAP Business Warehouse on SAP HANA Database</td>
</tr>
<tr>
<td>UCS</td>
<td>Cisco Unified Computing System</td>
</tr>
<tr>
<td>GbE</td>
<td>Gigabit Ethernet</td>
</tr>
<tr>
<td>SLES</td>
<td>SUSE Linux Enterprise Server</td>
</tr>
<tr>
<td>SLES4SAP</td>
<td>SUSE Linux Enterprise Server for SAP Applications</td>
</tr>
<tr>
<td>GB</td>
<td>Gigabyte</td>
</tr>
<tr>
<td>TB</td>
<td>Terabyte</td>
</tr>
<tr>
<td>IVB</td>
<td>Ivy Bridge</td>
</tr>
<tr>
<td>DB</td>
<td>Database</td>
</tr>
<tr>
<td>OS</td>
<td>Operating System</td>
</tr>
<tr>
<td>IOM</td>
<td>UCS IO-Module</td>
</tr>
<tr>
<td>FI</td>
<td>UCS Fabric Interconnect</td>
</tr>
<tr>
<td>vNIC</td>
<td>Virtual Network Interface Card</td>
</tr>
<tr>
<td>RAM</td>
<td>Server Main Memory</td>
</tr>
<tr>
<td>SID</td>
<td>System Identifier</td>
</tr>
</tbody>
</table>
Introduction

FlexPod is a defined set of hardware and software that serves as an integrated foundation for virtualized and non-virtualized data center solutions. It provides a prevalidated, ready-to-deploy infrastructure, which reduces the time and complexity involved in configuring and validating a traditional data center deployment. FlexPod datacenter Solution for SAP HANA includes NetApp storage, NetApp® Data ONTAP, Cisco Nexus® networking, the Cisco UCS™ (Cisco UCS®), and VMware® vSphere software in a single package.

The design is flexible enough that the networking, computing, and storage can fit in one data center rack and can be deployed according to a customer's data center design. A Key benefit of the FlexPod architecture is the ability to customize or "flex" the environment to suit a customer's requirements. A FlexPod can easily be scaled as requirements and demand change. The unit can be scaled both up (adding resources to a FlexPod unit) and out (adding more FlexPod units). The reference architecture detailed in this document highlights the resiliency, cost benefit, and ease of deployment of an IP-based storage solution. A storage system capable of serving multiple protocols across a single interface allows for customer choice and investment protection because it truly a wire-once architecture. The solution is designed to host scalable, mixed SAP HANA workloads.

SAP HANA is SAP SE’s implementation of in-memory database technology. The SAP HANA database takes advantage of the low cost main memory (RAM), data-processing capabilities of multicore processors, and faster data access to provide better performance for analytical and transactional applications. SAP HANA offers a multi-engine, query-processing environment that supports relational data (with both row- and column-oriented physical representations in a hybrid engine) as well as a graph and text processing for semi-structured and unstructured data management within the same system. As an appliance, SAP HANA combines software components from SAP optimized for certified hardware. However, this solution had a preconfigured hardware set-up and preinstalled software package that were dedicated for SAP HANA. In 2013, SAP introduced SAP HANA Tailored Datacenter Integration (TDI) option; TDI solution offers a more open and flexible way for integrating SAP HANA into the data center by reusing existing enterprise storage hardware, thereby reducing hardware costs. With the introduction of SAP HANA TDI for shared infrastructure, the Cisco and NetApp® FlexPod® solution gives you the advantage of having the compute, storage, and network stack integrated with the programmability of the Cisco Unified Computing System (Cisco UCS). SAP HANA TDI option enables organizations to run multiple SAP HANA production systems in one FlexPod solution. It also enables customers to run the SAP applications servers and SAP HANA database hosted on the same infrastructure.

For more information about SAP HANA, see the SAP help portal: http://help.sap.com/hana/.
Technology Overview

The FlexPod Datacenter Solution for SAP HANA is composed of Cisco UCS servers, Cisco Nexus switches, NetApp FAS storage and VMware vSphere. This section describes the main features of these elements.

Cisco Unified Computing System

The Cisco Unified Computing System is a state-of-the-art data center platform that unites computing, network, storage access, and virtualization into a single cohesive system. The main components of the Cisco Unified Computing System are:

- **Computing** - The system is based on an entirely new class of computing system that incorporates rack mount and blade servers based on Intel Xeon Processor E5 and E7. The Cisco UCS Servers offer the patented Cisco Extended Memory Technology to support applications with large datasets and allow more virtual machines per server.

- **Network** - The system is integrated onto a low-latency, lossless, 10-Gbps unified network fabric. This network foundation consolidates LANs, SANs, and high-performance computing networks which are separate networks today. The unified fabric lowers costs by reducing the number of network adapters, switches, and cables, and by decreasing the power and cooling requirements.

- **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 virtualized environments to better support changing business and IT requirements.

- **Storage access** - The system provides consolidated access to both SAN storage and Network Attached Storage (NAS) over the unified fabric. By unifying the storage access, the Cisco Unified Computing System can access storage over Ethernet (NFS or iSCSI) and Fibre Channel over Ethernet (FCoE). This provides customers with choice for storage access and investment protection. In addition, the server administrators can pre-assign storage-access policies for system connectivity to storage resources, simplifying storage connectivity, and management for increased productivity.

The Cisco Unified Computing System is designed to deliver:

- A reduced Total Cost of Ownership (TCO) and increased business agility.
- Increased IT staff productivity through just-in-time provisioning and mobility support.
- A cohesive, integrated system, which unifies the technology in the data center.
- Industry standards supported by a partner ecosystem of industry leaders.

Cisco Nexus 9396PX Switch

The Cisco Nexus 9000 family of switches supports two modes of operation: NXOS standalone mode and Application Centric Infrastructure (ACI) fabric mode. In standalone mode, the switch performs as a typical Cisco Nexus switch with increased port density, low latency and 40G connectivity. In fabric mode, the administrator can take advantage of Cisco ACI.

The Cisco Nexus 9396PX is a 2RU switch, which delivers comprehensive line-rate layer 2 and layer 3 features in a two-rack-unit form factor. It supports line rate 1/10/40 GE with 960 Gbps of switching capacity. It is ideal for top-of-rack and middle-of-row deployments in both traditional and Cisco Application Centric Infrastructure (ACI)–enabled enterprise, service provider, and cloud environments.
Specifications At-a-Glance
- Forty-eight 1/10 Gigabit Ethernet Small Form-Factor Pluggable (SFP+) nonblocking ports
- Twelve 40 Gigabit Ethernet Quad SFP+ (QSFP+) nonblocking ports
- Low latency (approximately 2 microseconds)
- 50 MB of shared buffer
- Line rate VXLAN bridging, routing, and gateway support
- Fibre Channel over Ethernet (FCoE) capability
- Front-to-back or back-to-front airflow

Figure 1.  Cisco Nexus 9396PX Switch

Cisco UCS Manager
Cisco Unified Computing System (UCS) Manager provides unified, embedded management of all software and hardware components of the Cisco UCS through an intuitive GUI, a command line interface (CLI), or an XML API. The Cisco UCS Manager provides unified management domain with centralized management capabilities and controls multiple chassis and thousands of virtual machines.

Fabric Interconnect
These devices provide a single point for connectivity and management for the entire system. Typically 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.

Cisco UCS 6248UP Fabric Interconnect
Cisco UCS 6200 Series Fabric Interconnects support the system’s 10-Gbps unified fabric with low-latency, lossless, cut-through switching that supports IP, storage, and management traffic using a single set of cables. The fabric interconnects feature virtual interfaces that terminate both physical and virtual connections equivalently, establishing a virtualization-aware environment in which blade, rack servers, and virtual machines are interconnected using the same mechanisms. The Cisco UCS 6248UP is a 1-RU Fabric Interconnect that features up to 48 universal ports that can support 10 Gigabit Ethernet, Fibre Channel over Ethernet, or native Fibre Channel connectivity. The Cisco UCS 6296UP packs 96 universal ports into only two rack units.

Figure 2.  Cisco UCS 6248UP Fabric Interconnect

Cisco UCS 2204XP Fabric Extender
The Cisco UCS 2204XP Fabric Extender (Figure 3.) has four 10 Gigabit Ethernet, FCoE-capable, and Enhanced Small Form-Factor Pluggable (SFP+) ports that connect the blade chassis to the fabric interconnect. Each Cisco UCS 2204XP has thirty-two 10 Gigabit Ethernet ports connected through the
midplane to each half-width slot in the chassis. Typically configured in pairs for redundancy, two fabric extenders provide up to 80 Gbps of I/O to the chassis.

**Figure 3.** Cisco UCS 2204 XP

---

**Cisco UCS 2208XP Fabric Extender**

The Cisco UCS 2208XP Fabric Extender (Figure 4.) has eight 10 Gigabit Ethernet, FCoE-capable, and Enhanced Small Form-Factor Pluggable (SFP+) ports that connect the blade chassis to the fabric interconnect. Each Cisco UCS 2208XP has thirty-two 10 Gigabit Ethernet ports connected through the midplane to each half-width slot in the chassis. Typically configured in pairs for redundancy, two fabric extenders provide up to 160 Gbps of I/O to the chassis.

**Figure 4.** Cisco UCS 2208 XP

---

**Cisco UCS Blade Chassis**

The Cisco UCS 5100 Series Blade Server Chassis is a crucial building block of the Cisco Unified Computing System, delivering a scalable and flexible blade server chassis.

The Cisco UCS 5108 Blade Server Chassis, is six rack units (6RU) high and can mount in an industry-standard 19-inch rack. A single chassis can house up to eight half-width Cisco UCS B-Series Blade Servers and can accommodate both half-width and full-width blade form factors. Four single-phase, hot-swappable power supplies are accessible from the front of the chassis. These power supplies are 92 percent efficient and can be configured to support non-redundant, N+ 1 redundant and grid-redundant configurations. The rear of the chassis contains eight hot-swappable fans, four power connectors (one per power supply), and two I/O bays for Cisco UCS 2200XP Fabric Extenders.

A passive mid-plane supports up to 2x 40 Gbit Ethernet links to each half-width blade slot or up to 4x 40 Gbit links to each full-width slot. It provides 8 blades with 1.2 terabits (Tb) of available Ethernet throughput for future I/O requirements. Note that the Cisco UCS 6324 FI supports only 512 Gbps. The chassis is capable of supporting future 80 Gigabit Ethernet standards. The Cisco UCS Blade Server Chassis is shown in Figure 5.

**Figure 5.** Cisco Blade Server Chassis (front and back view)
Cisco UCS B200 M4 Blade Server

Optimized for data center or cloud, the Cisco UCS B200 M4 can quickly deploy stateless physical and virtual workloads, with the programmability of the UCS Manager and simplified server access of SingleConnect technology. The UCS B200 M4 is built with the Intel® Xeon® E5-2600 v3 processor family, up to 768 GB of memory (with 32 GB DIMMs), up to two drives, and up to 80 Gbps total bandwidth. It offers exceptional levels of performance, flexibility, and I/O throughput to run the most demanding applications.

In addition, Cisco UCS has the architectural advantage of not having to power and cool switches in each blade chassis. Having a larger power budget available for blades allows Cisco to design uncompromised expandability and capabilities in its blade servers.

The Cisco UCS B200 M4 Blade Server delivers:

- Suitability for a wide range of applications and workload requirements
- Highest-performing CPU and memory options without constraints in configuration, power or cooling
- Half-width form factor offering industry-leading benefits
- Latest features of Cisco UCS Virtual Interface Cards (VICs)

Figure 6. Cisco UCS B200 M4 Blade Server

Cisco C220 M4 Rack Servers

The Cisco UCS C220 M4 Rack Server is the most versatile, high-density, general-purpose enterprise infrastructure and application server in the industry today. It delivers world-record performance for a wide range of enterprise workloads, including virtualization, collaboration, and bare-metal applications.

The enterprise-class UCS C220 M4 server extends the capabilities of the Cisco Unified Computing System (UCS) portfolio in a one rack-unit (1 RU) form-factor. It provides:

- Dual Intel® Xeon® E5-2600 v3 processors for improved performance suitable for nearly all 2-socket applications
- Next-generation double-data-rate 4 (DDR4) memory and 12 Gbps SAS throughput
- Innovative Cisco UCS virtual interface card (VIC) support in PCIe or modular LAN on motherboard (MLOM) form factor

The Cisco UCS C220 M4 server also offers maximum reliability, availability, and serviceability (RAS) features, including:

- Tool-free CPU insertion
- Easy-to-use latching lid
- Hot-swappable and hot-pluggable components
- Redundant Cisco Flexible Flash SD cards.

In Cisco UCS-managed operations, Cisco UCS C220 M4 takes advantage of our standards-based unified computing innovations to significantly reduce customers’ TCO and increase business agility.
Cisco UCS B260 M4 Blade Server
Optimized for data center or cloud, the Cisco UCS B260 M4 can quickly deploy stateless physical and virtual workloads, with the programmability of the Cisco UCS Manager and simplified server access of SingleConnect technology. The Cisco UCS B260 M4 is built with the Intel® Xeon® E7-4800 v2 processor family, up to 1.5 Terabyte of memory (with 32 GB DIMMs), up to two drives, and up to 160 Gbps total bandwidth. It offers exceptional levels of performance, flexibility, and I/O throughput to run the most demanding applications.

In addition, Cisco Unified Computing System has the architectural advantage of not having to power and cool switches in each blade chassis. Having a larger power budget available for blades allows Cisco to design uncompromised expandability and capabilities in its blade servers.

The Cisco UCS B260 M4 Blade Server delivers:
- Suitability for a wide range of applications and workload requirements
- Highest-performing CPU and memory options without constraints in configuration, power or cooling
- Full-width form factor offering industry-leading benefits
- Latest features of Cisco UCS Virtual Interface Cards (VICs)

Cisco UCS B460 M4 Blade Server
Optimized for data center or cloud, the Cisco UCS B460 M4 can quickly deploy stateless physical and virtual workloads, with the programmability of the Cisco UCS Manager and simplified server access of SingleConnect technology. The Cisco UCS B460 M4 is built with the Intel® Xeon® E7-4800 v2 processor family, up to 3 Terabyte of memory (with 32 GB DIMMs), up to two drives, and up to 320 Gbps total bandwidth. It offers exceptional levels of performance, flexibility, and I/O throughput to run the most demanding applications.

In addition, Cisco Unified Computing System has the architectural advantage of not having to power and cool switches in each blade chassis. Having a larger power budget available for blades allows Cisco to design uncompromised expandability and capabilities in its blade servers.

The Cisco UCS B460 M4 Blade Server delivers:
- Suitability for a wide range of applications and workload requirements
- Highest-performing CPU and memory options without constraints in configuration, power or cooling
- Full-width double high form factor offering industry-leading benefits
- Latest features of Cisco UCS Virtual Interface Cards (VICs)

Figure 9. Cisco UCS B460 M4 Blade Server

Cisco UCS C460 M4 Rack-Mount Server

The Cisco UCS C460 M4 Rack-Mount Server offers industry-leading performance and advanced reliability well suited for the most demanding enterprise and mission-critical workloads, large-scale virtualization, and database applications.

Either as standalone or in Cisco UCS-managed operations, customers gain the benefits of the Cisco UCS C460 M4 server’s high-capacity memory when very large memory footprints such as the following are required:
- SAP workloads
- Database applications and data warehousing
- Large virtualized environments
- Real-time financial applications
- Java-based workloads
- Server consolidation

The enterprise-class Cisco UCS C460 M4 server extends the capabilities of the Cisco Unified Computing System (UCS) portfolio in a four rack-unit (4RU) form-factor. It provides:
- Either Two or Four Intel® Xeon® processor E7-4800 v2 or E7-8800 v2 product family CPU
- Up to 6 terabytes (TB)* of Double-data-rate 3 (DDR3) memory in 96 dual in-line memory (DIMM) slots
- Up to 12 Small Form Factor (SFF) hot-pluggable SAS/SATA/SSD disk drives
- 10 PCI Express (PCIe) Gen 3 slots supporting the Cisco UCS Virtual Interface Cards and third-party adapters and GPUs
- Two Gigabit Ethernet LAN-on-motherboard (LOM) ports
- Two 10-Gigabit Ethernet ports
- A dedicated out-of-band (OOB) management port

Note: With 64GB DIMMs The UCS C460 M4 server also offers maximum reliability, availability, and serviceability (RAS) features, including:
- Tool-free CPU insertion
- Easy-to-use latching lid
- Hot-swappable and hot-pluggable components
- Redundant Cisco Flexible Flash SD cards
In Cisco UCS-managed operations, UCS C460 M4 takes advantage of our standards-based unified computing innovations to significantly reduce customers’ TCO and increase business agility.

**Figure 10.** Cisco UCS C460 M4 Rack Server

---

**Cisco I/O Adapters for Blade and Rack-Mount Servers**

**Cisco VIC 1240 Virtual Interface Card**

The Cisco UCS blade server has various Converged Network Adapters (CNA) options. The Cisco UCS VIC 1240 Virtual Interface Card (VIC) option is used in this Cisco Validated Design.

The Cisco UCS Virtual Interface Card (VIC) 1240 (0) is a 4 x 10-Gbps Ethernet, Fibre Channel over Ethernet (FCoE)-capable modular LAN on motherboard (mLOM) designed for the M3 and M4 generation of Cisco UCS B-Series Blade Servers. When used in combination with an optional port expander, the Cisco UCS VIC 1240 capabilities is enabled for eight ports of 10-Gbps Ethernet.

**Figure 11.** Cisco UCS VIC 1240 Card

The Cisco UCS VIC 1240 enables a policy-based, stateless, agile server infrastructure that can present over 256 PCIe standards-compliant interfaces to the host that can be dynamically configured as either network interface cards (NICs) or host bus adapters (HBAs). In addition, the Cisco UCS VIC 1240 supports Cisco® Data Center Virtual Machine Fabric Extender (VM-FEX) technology, which extends the Cisco UCS fabric interconnect ports to virtual machines, simplifying server virtualization deployment and management.
The Cisco UCS blade server has various Converged Network Adapters (CNA) options. The Cisco UCS VIC 1280 Virtual Interface Card (VIC) option is used in this Cisco Validated Design.

The Cisco UCS Virtual Interface Card (VIC) 1280 (Figure 13.) is a 8 x 10-Gbps Ethernet, Fibre Channel over Ethernet (FCoE)-capable modular LAN on motherboard (mLOM) designed for the M3 and M4 generation of Cisco UCS B-Series Blade Servers.

The Cisco UCS VIC 1280 enables a policy-based, stateless, agile server infrastructure that can present over 256 PCIe standards-compliant interfaces to the host that can be dynamically configured as either network interface cards (NICs) or host bus adapters (HBAs). In addition, the Cisco UCS VIC 1280 supports Cisco® Data Center Virtual Machine Fabric Extender (VM-FEX) technology, which extends the Cisco UCS fabric interconnect ports to virtual machines, simplifying server virtualization deployment and management.
Cisco VIC 1227/1225 Virtual Interface Card

The Cisco UCS rack-mount server has various Converged Network Adapters (CNA) options. The Cisco UCS 1227 Virtual Interface Card (VIC) is used in this Cisco Validated Design. The Cisco UCS Virtual Interface Card (VIC) 1227 is a dual-port Enhanced Small Form-Factor Pluggable (SFP+) 10-Gbps Ethernet and Fibre Channel over Ethernet (FCoE)-capable PCI Express (PCIe) modular LAN-on-motherboard (mLOM) adapter designed exclusively for Cisco UCS C-Series Rack Servers (Figure 15). New to Cisco rack servers, the mLOM slot can be used to install a Cisco VIC without consuming a PCIe slot, which provides greater I/O expandability. It incorporates next-generation converged network adapter (CNA) technology from Cisco, providing investment protection for future feature releases. The card enables a policy-based, stateless, agile server infrastructure that can present up to 256 PCIe standards-compliant interfaces to the host that can be dynamically configured as either network interface cards (NICs) or host bus adapters (HBAs). In addition, the Cisco UCS VIC 1227 supports Cisco® Data Center Virtual Machine Fabric Extender (VM-FEX) technology, which extends the Cisco UCS fabric interconnect ports to virtual machines, simplifying server virtualization deployment.

A Cisco® innovation, the Cisco UCS Virtual Interface Card (VIC) 1225 (Figure 16) is a dual-port Enhanced Small Form-Factor Pluggable (SFP+) 10 Gigabit Ethernet and Fibre Channel over Ethernet (FCoE)-capable PCI Express (PCIe) card designed exclusively for Cisco UCS C-Series Rack Servers.
Cisco UCS 1225 VIC provides the capability to create multiple VNICS (up to 128) on the CNA. This allows complete I/O configurations to be provisioned in virtualized or non-virtualized environments using just-in-time provisioning, providing tremendous system flexibility and allowing consolidation of multiple physical adapters.

System security and manageability is improved by providing visibility and portability of network policies and security all the way to the virtual machines. Additional 1225 features like VM-FEX technology and pass-through switching, minimize implementation overhead and complexity.

**Figure 16.** Cisco UCS 1225 VIC

---

**Cisco UCS Differentiators**

Cisco’s Unified Compute System is revolutionizing the way servers are managed in data-center. The following are the unique differentiators of Cisco Unified Computing System and Cisco UCS Manager.

- **Embedded management:** In Cisco Unified Computing System, 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. Also, a pair of FIs can manage up to 40 chassis, each containing 8 blade servers. This gives enormous scaling on management plane.

- **Unified fabric:** In Cisco Unified Computing System, from blade server chassis or rack server fabric-extender 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 overall solution.

- **Auto Discovery:** By simply inserting the blade server in the chassis or connecting rack server to the fabric extender, discovery and inventory of compute resource occurs automatically without any management intervention. Combination of unified fabric and auto-discovery enables wire-once architecture of Cisco Unified Computing System, where compute capability of Cisco Unified Computing System can extending easily while keeping the existing external connectivity to LAN, SAN and management networks.

- **Policy based resource classification:** When 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 show cases the policy based resource classification of Cisco UCS Manager.

- **Combined Rack and Blade server management:** Cisco UCS Manager can manage B-Series blade servers and C-Series rack server under the same Cisco UCS domain. This feature, along with stateless computing makes compute resources truly hardware form factor agnostic. In this CVD, we are show casing combination of B-Series and C-Series Servers to demonstrate stateless and form factor independent computing work load.

- **Model based management architecture:** Cisco UCS Manager architecture and management database is model based and data driven. Open, standard based XML API is provided to operate on the management model. This enables easy and scalable integration of UCSM with other management system, such as VMware vCloud director, Microsoft system center, and Citrix CloudPlatform.
- **Policies, Pools, Templates:** Management approach in UCSM is based on defining policies, pools and templates, instead of cluttered configuration, which enables 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 flexibilities 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 other policy by name is resolved in the org hierarchy with closest policy match. If no policy with specific name is found in the hierarchy till root org, then special policy named “default” is searched. This policy resolution practice enables automation friendly management APIs and provides great flexibilities to owners of different orgs.

- **Service profiles and stateless computing:** 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:** Combination of policies, pools and templates, loose referential integrity, policy resolution in org hierarchy and service profile based approach to compute resources makes Cisco UCS Manager inherently friendly to multi-tenant environment typically observed in private and public clouds.

- **Virtualization aware network:** VM-FEX technology makes access layer of network aware about host virtualization. This prevents domain pollution of compute and network domains with virtualization when virtual network is managed by port-profiles defined by the network administrators’ team. VM-FEX also offloads hypervisor CPU by performing switching in the hardware, thus allowing hypervisor CPU to do more virtualization related tasks. VM-FEX technology is well integrated with VMware vCenter, Linux KVM and Hyper-V SR-IOV to simplify cloud management.

- **Simplified QoS:** Even though fibre-channel and Ethernet are converged in 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.

### VMware vSphere 5.5

VMware vSphere 5.5 is a next-generation virtualization solution from VMware, which builds upon ESXi 5.1 and provides greater levels of scalability, security, and availability to virtualized environments. vSphere 5.5 offers improvements in performance and utilization of CPU, memory, and I/O. It also provides the option to assign up to 32 virtual CPU to a virtual machine—giving system administrators more flexibility in their virtual server farms as processor-intensive workloads continue to increase.

The VMware vSphere 5.5 provides VMware vCenter Server that allows system administrators to manage their ESXi hosts and virtual machines on a centralized management platform. With the Cisco UCS Fabric Interconnects integrated into the VMware vCenter Server, deploying and administering virtual machines is similar to deploying and administering physical servers. Network administrators can continue to own the responsibility for configuring and monitoring network resources for virtualized servers as they did with physical servers. System administrators can continue to “plug-in” their virtual machines into network ports that have Layer 2 configurations, port access and security policies, monitoring features, etc., that have been pre-defined by the network administrators; in the same way they would plug in their physical servers to a previously-configured access switch. In this virtualized environment, the system administrator has the added benefit of the network port configuration/policies moving with the virtual machine if it is ever migrated to different server hardware.
NetApp FAS and Data ONTAP

NetApp solutions are user-friendly, easy to manage, quick to deploy, and offer increased availability while consuming fewer IT resources. This means they dramatically lower the lifetime TCO. A NetApp solution extends hardware in the form of controllers, disk storage, and the NetApp Data ONTAP operating system, which is regarded as the number one storage OS.

NetApp offers the NetApp Unified Storage Architecture. The term "unified" refers to a family of storage systems that simultaneously support storage area network (SAN) and network-attached storage (NAS) across many operating environments such as VMware, Windows®, and UNIX®. This single architecture provides access to data by using industry-standard protocols, including NFS, CIFS, iSCSI, FCP, SCSI, FCoE, FTP, and HTTP. Connectivity options include standard Ethernet (10/100/1000, or 10GbE) and Fibre Channel (1, 2, 4, or 8Gb/sec). In addition, all systems can be configured with high-performance solid state drives (SSDs) or serial ATA (SAS) disks for primary storage applications and low-cost SATA disks for secondary applications (backup, archive, and so on) or a mix of the different disk types.

This version of FlexPod introduces the NetApp FAS8000 series unified scale-out storage systems. Powered by NetApp clustered Data ONTAP, the FAS8000 series unifies the SAN and NAS storage infrastructure. The FAS8000 features a multiprocessor Intel chipset and leverages high-performance memory modules, NVRAM to accelerate and optimize writes, and an I/O-tuned PCIe gen3 architecture that maximizes application throughput. The FAS8000 series comes with integrated unified target adapter (UTA2) ports that support 16Gb Fibre Channel (FC), 10GbE, or FCoE.

A storage system running NetApp Data ONTAP has a main unit, known as the controller, which is a hardware device that receives and sends data. This unit detects and gathers information about the hardware configuration, storage system components, operational status, hardware failures, and other error conditions. A storage system uses storage on disk shelves. The disk shelves are the containers or device carriers that hold disks and associated hardware, such as power supplies, connectivity interfaces, and cabling. If storage requirements change over time, NetApp storage offers the flexibility to change quickly, as needed, and without expensive and disruptive "forklift" upgrades. For example, a LUN can be changed from FC access to iSCSI access without moving or copying the data. Only a simple dismount of the FC LUN and a mount of the same LUN using iSCSI are required. In addition, a single copy of data can be shared between Windows and UNIX systems while allowing each environment to access the data through native protocols and applications. If a system was originally purchased with all SATA disks for backup applications, high-performance SAS disks can be added to support primary storage applications such as Oracle®, Microsoft® Exchange Server, or ClearCase.

NetApp storage solutions provide redundancy and fault tolerance through clustered storage controllers, hot-swappable redundant components (such as cooling fans, power supplies, disk drives, and shelves), and multiple network interfaces. This highly available and flexible architecture enables customers to manage all data under one common infrastructure while achieving mission requirements. The NetApp Unified Storage Architecture allows data storage with higher availability and performance, easier dynamic expansion, and unrivaled ease of management.

The storage efficiency built into Data ONTAP provides substantial space savings, allowing more data to be stored at a lower cost. Data protection provides replication services, making sure that valuable data is backed up and recoverable. The following features provide storage efficiency and data protection:

- **Thin provisioning.** Volumes are created through virtual sizing. They appear to be provisioned to their full capacity, but are actually created much smaller and use additional space only when it is needed. Extra-unused storage is shared across all volumes, and the volumes can grow and shrink on demand.

- **NetApp Snapshot® copies.** Automatically scheduled point-in-time copies that write only changed blocks, with no performance penalty. The Snapshot copies consume minimal storage space, since only changes to the active file system are written. Individual files and directories can be easily recovered from any Snapshot copy, and the entire volume can be restored back to any Snapshot state in seconds.
- **NetApp FlexClone® volumes.** Near-zero space and instant virtual copies of datasets. The clones are writable, but only changes to the original are stored. FlexClone technology rapidly creates additional, space-efficient data copies ideally suited for dev/test environments.
- **Deduplication.** Removes redundant data blocks in primary and secondary storage with flexible policies to determine when the deduplication process is run.
- **Compression.** Compresses data blocks. Compression can be run whether or not deduplication is enabled, and it can provide additional space savings when run alone or together with deduplication.
- **NetApp SnapMirror®.** Volumes can be asynchronously replicated either within the cluster or to another cluster.

For more information, refer to the [NetApp Data ONTAP 8.3 Operating System](#) website.

## Clustered Data ONTAP

With clustered Data ONTAP, NetApp provides enterprise-ready, unified scale-out storage. Developed from a solid foundation of proven Data ONTAP technology and innovation, clustered Data ONTAP is the basis for large, virtualized, shared-storage infrastructures that are architected for nondisruptive operations over the system for lifetime. Controller nodes are deployed in HA pairs, with these HA pairs participating in a single storage domain or cluster.

Data ONTAP scale-out is one way to respond to growth in a storage environment. All storage controllers have physical limits to their expandability, such as the number of CPUs, memory slots, and space for disk shelves that dictate the maximum capacity and controller performance. If more storage or performance capacity is required, it might be possible to add CPUs and memory or install additional disk shelves, but ultimately the controller becomes completely populated, with no further expansion possible. At this stage, the only option is to acquire another controller. One way to do this is to “scale up” or add additional controllers in such a way that each controller is a completely independent management entity that does not share storage resources. If the original controller must be completely replaced by a newer and larger controller, data migration is required to transfer the data from the old controller to the new one. Data migration is time consuming and potentially disruptive, and it most likely necessitates configuration changes on all of the attached host systems.

If the newer controller can coexist with the original controller, two storage controllers must now be managed individually, and there are no native tools to balance or reassign workloads across them. The situation becomes worse as the number of controllers increases. If the scale-up approach is used, the operational burden increases consistently as the environment grows, and the result is an unbalanced, difficult-to-manage environment. Technology refresh cycles require substantial advanced planning, lengthy outages, and configuration changes that can introduce risk to the system.

By contrast, scaling out means that as the storage environment grows, additional controllers are added seamlessly to the resource pool residing on a shared storage infrastructure. Host and client connections, as well as datastores, can move seamlessly and nondisruptively anywhere in the resource pool, so that existing workloads can be easily balanced over the available resources, and new workloads can be easily deployed. Technology refreshes, such as replacing disk shelves, adding or completely replacing storage controllers, are accomplished while the environment remains online serving data.

Although scale-out products have been available for some time, these were typically subject to one or more of the following shortcomings:

- Limited protocol support: NAS only
- Limited hardware support: only a particular type of storage controller or a very limited set
- Limited or no storage efficiency: thin provisioning, deduplication, and compression
- Limited or no data replication capability

Therefore, although these products work well for certain specialized workloads, they are less flexible, less capable, and not robust enough for broad deployment throughout the enterprise. Data ONTAP is the first product to offer a complete scale-out solution, and it offers an adaptable, always-available storage infrastructure for today's highly virtualized environment.
Architecture

The FlexPod Datacenter solution for SAP HANA with NetApp FAS storage provides an end-to-end architecture with Cisco, NetApp and VMware technologies that demonstrate support for multiple SAP HANA workloads with high availability and server redundancy. The architecture uses UCS 2.2(3c) with combined Cisco UCS B-Series and C-Series Servers with NetApp FAS 8000 series storage attached to the Nexus 9396PX switches for NFS access and iSCSI. The C-Series Rack Servers are connected directly to Cisco UCS Fabric Interconnect with single-wire management feature. This infrastructure is deployed to provide PXE and iSCSI boot options for hosts with file-level and block-level access to shared storage. VMware vSphere 5.5 is used as server virtualization architecture. The reference architecture reinforces the “wire-once” strategy, because when the additional storage is added to the architecture, no re-cabling is required from hosts to the Cisco UCS Fabric Interconnect.

Figure 17. shows the FlexPod Datacenter reference architecture for SAP HANA workload, described in this Cisco Validation Design. It highlights the FlexPod hardware components and the network connections for a configuration with IP-based storage.
Figure 17. FlexPod Datacenter Reference Architecture for SAP HANA

Cisco UCS
5108 B-Series Blade Chassis
2208XP Chassis FEX Modules
B460 M4 B-Series Blades

Cisco UCS
5108 B-Series Blade Chassis
2208XP Chassis FEX Modules
B260 M4 and B200 M4 Blades

Cisco UCS
C460 M4 C-Series Server(s)

Cisco UCS
C240 M4 C-Series Server(s)

Cisco UCS
C220 M4 C-Series Server(s)

Cisco UCS
6248UP Fabric Interconnects

Cisco Nexus
9396 Switches

NetApp FAS8040
Storage Controllers
w/ HA Backplane

Controller 1
Controller 2

Cisco Nexus 5596
Cluster Interconnects

NetApp
DS2246 Disk Shelves

Legend
SAS only
10Gbe Only
The reference hardware configuration includes:

**Cisco Unified Computing System**
- 2 x Cisco UCS 6248UP 48-Port or 6296UP 96-Port Fabric Interconnects
- 2 x Cisco UCS 5108 Blade Chassis with 2 x Cisco UCS 2204 Fabric Extenders with 4x 10 Gigabit Ethernet interfaces
- 2 x Cisco UCS B460 M4 High-Performance Blade Servers with 2x Cisco UCS Virtual Interface Card (VIC) 1280 and 2x Cisco UCS Virtual Interface Card (VIC) 1240
- 2 x Cisco UCS B260 M4 High-Performance Blade Servers with 1x Cisco UCS Virtual Interface Card (VIC) 1280 and 1x Cisco UCS Virtual Interface Card (VIC) 1240
- 1 x Cisco UCS C460 M4 High-Performance Rack-Mount Servers with 2x Cisco UCS Virtual Interface Card (VIC) 1225.
- 4 x Cisco UCS B200 M4 High-Performance Blade Servers with Cisco UCS Virtual Interface Card (VIC) 1340
- 1 x Cisco UCS C220 M4 High-Performance Blade Servers with Cisco UCS Virtual Interface Card (VIC) 1225
- 1 x Cisco UCS C240 M4 High-Performance Blade Servers with Cisco UCS Virtual Interface Card (VIC) 1225
- 2 x Cisco UCS C220 M3 for Management Servers with Cisco UCS Virtual Interface Card (VIC) 1225 and RAID controller with Internal Disks

**Cisco Nexus Switches**
- 2 x Cisco Nexus 9396 Switch for 10 Gigabit Ethernet connectivity between the two UCS Fabric Interconnects

**NetApp FAS8040 Storage**
- NetApp FAS8040HA Storage Clustered Data ONTAP
- 4 x NetApp Disk Shelf DS2246 with 24x 600GB 10k 2.5” SAS Disks
- 2 x Cisco Nexus 5596 Switch for FAS 8000 Cluster Interconnect
- Server virtualization is achieved by VMware vSphere 5.5.

Although this is the base design, each of the components can be scaled easily to support specific business requirements. Additional servers or even blade chassis can be deployed to increase compute capacity without additional Network components. Two Cisco UCS 6248UP 48-Port Fabric interconnect can support up to:
- 20 Cisco UCS B-Series B460 M4 or 40 B260 M4 Server with 10 Blade Server Chassis
- 20 Cisco UCS C460 M4 Server
- 40 Cisco UCS C220 M4/C240 M4 Server

For every eight Cisco UCS Server, One NetApp FAS8040 HA pair with Clustered Data ONTAP is required to meet the SAP HANA storage performance. While adding compute and storage for scaling, it is required to increase the network bandwidth between Cisco UCS Fabric Interconnect and Cisco Nexus 9000 switch. Addition of each NetApp Storage requires additional four 10 GbE connectivity from each Cisco UCS Fabric Interconnect to Cisco Nexus 9000 switches.

**Note:** The number of Cisco UCS C-Series or Cisco UCS B-Series Servers and the NetApp FAS storage type depends on the number of SAP HANA instances. SAP specifies the storage performance for SAP HANA, based on a per server rule independent of the server size. In other words, the maximum number of servers per storage will remain the same if you want to use Cisco UCS B200 M4 with 192GB physical memory or Cisco UCS B460 M4 with 2TB physical memory.

Figure 18. shows a block diagram of a complete SAP Landscape built using the FlexPod architecture. It composed of multiple SAP HANA systems and SAP applications with shared infrastructure as illustrated in the figure. The FlexPod Datacenter reference architecture for SAP solutions supports SAP HANA system
in both Scale-Up mode (bare metal/virtualization) and Scale-Out mode with multiple servers with the shared infrastructures.

Virtualized SAP application servers with VMware vSphere 5.5 allows application servers to run on the same infrastructure as the SAP HANA database. The FlexPod datacenter solution manages the communication between the application server and the SAP HANA database. This approach enhances system performance by improving bandwidth and latency. It also improves system reliability by including the application server in the disaster-tolerance solution with the SAP HANA database.

**Figure 18.** Shared Infrastructure Block Diagram

Storage isolation requirements when using mixed workloads:

The FlexPod architecture for SAP HANA TDI allows to run other workloads on the same infrastructure, as long as the rules for workload isolation are considered.

The following workloads could be potentially run on the FlexPod architecture.

1. Production SAP HANA databases
2. SAP application servers
3. Non-production SAP HANA databases
4. Production and non-production SAP systems on traditional databases
5. Non-SAP workloads

In order to ensure that the storage KPIs for SAP HANA production databases are fulfilled, the SAP HANA production databases must have dedicated storage controller of a NetApp FAS Storage HA pair. SAP application servers could share the same storage controller with the production SAP HANA databases.

This document describes in detail the procedure for the reference design and outlines the network, compute and storage configurations and deployment process for running SAP HANA on FlexPod platform. This document does not describe the procedure for deploying SAP applications.

Management Pod

Comprehensive management is an important element for a FlexPod environment running SAP HANA, especially in a system involving multiple FlexPod platforms. Management pod built to handle this efficiently. It is an optional to build a dedicated Management environment; customer can use their existing Management environment for the same functionality. Management Pod includes (but is not limited to) a pair of Cisco Nexus 9000 Series switches in standalone mode and a pair of Cisco UCS C220 M3 Rack Servers. The Cisco Nexus switch provides the out-of-band management network. It is recommended to use additional NetApp FAS Storage in the Management Pod for redundancy and failure scenarios. The Rack-Mount Cisco UCS C220 M3 Servers will run ESXi with PXE boot server, vCenter with additional management and monitoring virtual machines.

Management Pod switches can connect directly to FlexPod switches or customer’s existing network infrastructure. If customer’s existing network infrastructure is used, the uplink from FlexPod switches are connected same pair of switch as uplink from Management Pod switches as shown in Figure 19. The customer’s LAN switch must allow all the necessary VLANs for managing the FlexPod environment.

![Figure 19. Management Pod Using Customer Existing Network](image)

The dedicated Management Pod can connect directly each FlexPod environment as shown in Figure 20. In this topology, the switches are configured as port-channels for unified management. This CVD describes procedure for direct connection option.
SAP HANA Solution implementations

This section outlines the various implementation options and their requirements for a SAP HANA system.

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

A single-host system is the simplest of the installation types. It is possible to run an SAP HANA system entirely on one host and then scale the system up as needed. All data and processes are located on the same server and can be accessed locally. The network requirements for this option minimum one 1-Gb Ethernet (access) and one 10-Gb Ethernet storage networks are sufficient to run SAP HANA scale-up. Virtualized SAP HANA Scale-Up system requires dedicated 10 Gigabit Ethernet network adapters per virtualized SAP HANA system. With SAP HANA TDI option, multiple SAP HANA scale-up systems can be built on a shared infrastructure.

SAP HANA System on Multiple Servers—Scale-Out

SAP HANA Scale-Out option is used 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.
Some use cases are not supported on SAP HANA Scale-Out configuration and it is recommended to check with SAP whether a use case can be deployed as a Scale-Out solution.

The network requirements for this option are higher than for Scale-Up systems. In addition to the client and application access and storage access network, a node-to-node network is necessary. One 10 Gigabit Ethernet (access) and one 10 Gigabit Ethernet (node-to-node) and one 10 Gigabit Ethernet storage networks are required to run SAP HANA Scale-Out system. Additional network bandwidth is required to support system replication or backup capability.

Based on the SAP HANA TDI option for shared storage and shared network, multiple SAP HANA Scale-Out systems can be built on a shared infrastructure.

Virtualized SAP HANA Scale-Out is not supported by SAP as of December 2014.

Hardware Requirements for the SAP HANA Database

There are hardware and software requirements defined by SAP to run SAP HANA systems in Tailored Datacenter Integration (TDI) option. This Cisco Validated Design uses guidelines provided by SAP. Additional information is available at: [http://saphana.com](http://saphana.com).

This document does not cover the updated information published by SAP in year 2015.

CPU

SAP HANA supports servers equipped with Intel Xeon processor E7-2870, E7-4870, or E7-8870 CPUs, or Intel Xeon processor E7-2890v2, E7-4890v2, or E7-8890v2 CPUs. In addition, the Intel Xeon processor E5-26xx v3 is supported for scale-up systems with the SAP HANA TDI option.

Memory

SAP HANA is supported in the following memory configurations:

- 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
- Memory per socket of 64, 128, or 256 GB for SAP NetWeaver Business Warehouse (BW) and DataMart
- Memory per socket of 64, 128, 256, or 512 GB for SAP Business Suite on SAP HANA (SoH) on 2- or 4-socket server

CPU and Memory Combinations

SAP HANA allows a specific set of CPU and memory combinations. Table 1 describes the list of certified Cisco UCS servers for SAP HANA with supported Memory and CPU configuration for different use cases.
Table 1. List of Cisco UCS Servers Defined in FlexPod Datacenter Solution for SAP

<table>
<thead>
<tr>
<th>Cisco UCS Server</th>
<th>CPU</th>
<th>Supported Memory</th>
<th>Scale UP/ Suite on HANA</th>
<th>Scale Out</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS B200 M4</td>
<td>2 x Intel Xeon E5-26xx v2</td>
<td>128 GB to 1.5 TB</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Cisco UCS C220 M4</td>
<td>2 x Intel Xeon E5-26xx v2</td>
<td>128 GB to 1.5 TB</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Cisco UCS C240 M4</td>
<td>2 x Intel Xeon E5-26xx v2</td>
<td>128 GB to 1.5 TB</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Cisco UCS B260 M4</td>
<td>2 x Intel E7-48x0 v2</td>
<td>128 GB to 512 GB</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Cisco UCS B460 M4</td>
<td>4 x Intel E7-48x0 v2</td>
<td>128 GB to 1 TB</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Cisco UCS C460 M4</td>
<td>4 x Intel E7-48x0 v2</td>
<td>128 GB to 3 TB for SoH</td>
<td>Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>

Network

A 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**: Channels used for external access to SAP HANA functions by end-user clients, administration clients, and application servers, and for data provisioning through SQL or HTTP
- **Internal zone**: Channels used for SAP HANA internal communication within the database or, in a distributed scenario, for communication between hosts
- **Storage zone**: Channels used for storage access (data persistence) and for backup and restore procedures

Table 2 lists all the networks defined by SAP or Cisco or requested by customers.

Table 2. List of Known Networks

<table>
<thead>
<tr>
<th>Name</th>
<th>Use Case</th>
<th>Solutions</th>
<th>Bandwidth requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Client Zone Networks</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Server Network</td>
<td>SAP Application Server to DB communication</td>
<td>All</td>
<td>1 or 10 GbE</td>
</tr>
<tr>
<td>Client Network</td>
<td>User / Client Application to DB communication</td>
<td>All</td>
<td>1 or 10 GbE</td>
</tr>
<tr>
<td>Data Source Network</td>
<td>Data import and external data integration</td>
<td>Optional for all SAP HANA systems</td>
<td>1 or 10 GbE</td>
</tr>
<tr>
<td><strong>Internal Zone Networks</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inter-Node Network</td>
<td>Node to node communication within a scale-out configuration</td>
<td>Scale-Out</td>
<td>10 GbE</td>
</tr>
<tr>
<td>System Replication Network</td>
<td>For SAP HANA Disaster Tolerance</td>
<td>TBD with Customer</td>
<td></td>
</tr>
<tr>
<td><strong>Storage Zone Networks</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Use Case</td>
<td>Solutions</td>
<td>Bandwidth requirements</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------</td>
<td>----------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Backup Network</td>
<td>Data Backup</td>
<td>Optional for all SAP HANA systems</td>
<td>10 GbE</td>
</tr>
<tr>
<td>Storage Network</td>
<td>Node to Storage communication</td>
<td>All</td>
<td>10 GbE</td>
</tr>
</tbody>
</table>

**Infrastructure Related Networks**

<table>
<thead>
<tr>
<th>Name</th>
<th>Use Case</th>
<th>Solutions</th>
<th>Bandwidth requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administration Network</td>
<td>Infrastructure and SAP HANA administration</td>
<td>Optional for all SAP HANA systems</td>
<td>1 GbE</td>
</tr>
<tr>
<td>Boot Network</td>
<td>Boot the Operating Systems via PXE/NFS or FCoE</td>
<td>Optional for all SAP HANA systems</td>
<td>1 GbE</td>
</tr>
</tbody>
</table>

Details about the network requirements for SAP HANA are available in the white paper from SAP SE at: [http://www.saphana.com/docs/DOC-4805](http://www.saphana.com/docs/DOC-4805).

The network need to be properly segmented and must be connected to the same core/ backbone switch as shown in Figure 21. based on customer’s high-availability and redundancy requirements for different SAP HANA network segments.

![Figure 21. High-Level SAP HANA Network Overview](image)

**High-Level SAP HANA Network Overview**

Based on the listed network requirements every server must be equipped with 2x 10 Gigabit Ethernet for scale-up systems to establish the communication with the application or user (Client Zone) and a 10 GbE Interface for Storage access.

For Scale-Out solutions an additional redundant network for SAP HANA node to node communication with 10 GbE is required (Internal Zone).

**Note:** For more information on SAP HANA Network security please refer to [SAP HANA Security Guide](http://www.sap.com).

**Storage**

As an in-memory database, SAP HANA uses storage devices to save a 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 Storage system in the Tailored Datacenter Integration option, the storage must be certified for SAP HANA TDI option at http://scn.sap.com/docs/DOC-48516.

All relevant information about storage requirements is documented in the white paper “SAP HANA Storage Requirements” and is available at: http://www.saphana.com/docs/DOC-4071.

**Note**: SAP can only support performance related SAP HANA topics if the installed solution has passed the validation test successfully.

Refer to SAP HANA Administration Guide section 2.8 Hardware Checks for Tailored Datacenter Integration for Hardware check test tool and the related documentation.

**Filesystem Layout**

Figure 22. shows the file system layout and the required storage sizes to install and operate SAP HANA. For the Linux OS installation (/root) 10 GB of disk size is recommended. Additionally 50 GB must be provided for the /usr/sap since the volume used for SAP software that supports SAP HANA. While installing SAP HANA on a host, we specify the mount point for the installation binaries (/hana/shared/<<sid>>), data files (/hana/data/<<sid>>) and log files (/hana/log/<<sid>>), where sid is the instance identifier of the SAP HANA installation.

![File System Layout for 2 Node Scale-Out System](image)

The storage sizing for filesystem is based on the amount of memory equipped on the SAP HANA host. Below is a sample filesystem size for a single system with 512GB memory:

- **Root-FS**: 10 GB
- **/usr/sap**: 50 GB
- **/hana/shared**: 1x memory (512 GB)
- **/hana/data**: 1x memory (512 GB)
- **/hana/log**: 1x Memory (512 GB)

In case of distributed installation of SAP HANA Scale-Out, each server will have the following:

- **Root-FS**: 10 GB
/usr/sap: 50 GB

The installation binaries, trace and configuration files are stored on a shared filesystem, which should be accessible for all hosts in the distributed installation. The size of shared filesystem should be equal to the number of hosts, times memory in each host.

For example: In a distributed installation with three hosts with 512 GB of memory each, shared file system should be 3 x 512 GB = 1536 GB

For each HANA host there should be mount point for data and log volume. Size of the file system for data volume with TDI option is one times the host memory.

/hana/data/<sid>/mntXXXXX: 1x Memory (512 GB)

For solutions based on Intel E7-x890v2 CPU the size of the Log volume must be as follows:

- Half of the server memory for systems ≤ 256 GB memory
- Min 512 GB for systems with ≥ 512 GB memory

### Operating System

The supported operating systems for SAP HANA are as follows:

- SUSE Linux Enterprise Server 11
- SUSE Linux Enterprise Server for SAP Applications
- RedHat Enterprise Linux for SAP HANA

### High Availability

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

- Internal storage: A RAID-based configuration is preferred
- 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 an integrated high-availability function. If a 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.

Please check the latest information from SAP at: [http://saphana.com](http://saphana.com) or [http://service.sap.com/notes](http://service.sap.com/notes).
Software Revisions

Table 3 details the software revisions used for validating various components of the FlexPod Datacenter Reference Architecture for SAP HANA.

Table 3. Hardware and Software Components of the FlexPod Datacenter Reference Architecture for SAP Solutions

<table>
<thead>
<tr>
<th>Vendor</th>
<th>Product</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco</td>
<td>UCSM</td>
<td>2.2(3c)</td>
<td>UCS Manager</td>
</tr>
<tr>
<td>Cisco</td>
<td>UCS 6248UP FI</td>
<td>2.2(3c)</td>
<td>UCS Fabric Interconnects</td>
</tr>
<tr>
<td>Cisco</td>
<td>UCS 5108 Blade Chassis</td>
<td>NA</td>
<td>UCS Blade Server Chassis</td>
</tr>
<tr>
<td>Cisco</td>
<td>UCS 2200XP FEX</td>
<td>2.2(3c)</td>
<td>UCS Fabric Extenders for Blade Server chassis</td>
</tr>
<tr>
<td>Cisco</td>
<td>UCS B-Series M4 Servers</td>
<td>2.2(3c)</td>
<td>Cisco B-Series M4 Blade Servers</td>
</tr>
<tr>
<td>Cisco</td>
<td>UCS VIC 1240/1280</td>
<td>2.1.1.75</td>
<td>Cisco UCS VIC 1240/1280 Adapters</td>
</tr>
<tr>
<td>Cisco</td>
<td>UCS C220 M4 Servers</td>
<td>2.0.3e – CIMC C220M4.2.0.3c - BIOS</td>
<td>Cisco C220 M4 Rack Servers</td>
</tr>
<tr>
<td>Cisco</td>
<td>UCS VIC 1227</td>
<td>2.1.1.75</td>
<td>Cisco UCS VIC Adapter</td>
</tr>
<tr>
<td>Cisco</td>
<td>UCS C460 M4 Servers</td>
<td>2.0.3e – CIMC C460M4.2.0.3c - BIOS</td>
<td>Cisco C460 M4 Rack Servers</td>
</tr>
<tr>
<td>Cisco</td>
<td>UCS VIC 1225</td>
<td>2.1.1.75</td>
<td>Cisco UCS VIC Adapter</td>
</tr>
<tr>
<td>Cisco</td>
<td>UCS C220 M3 Servers</td>
<td>CIMC 1.5(7a) BIOS 1.5.7.0</td>
<td>Cisco C220 M3 Rack Servers for Management</td>
</tr>
<tr>
<td>Cisco</td>
<td>Nexus 9396PX Switches</td>
<td>6.1(2)I2(2a)</td>
<td>Cisco Nexus 9396x Switches</td>
</tr>
<tr>
<td>NetApp</td>
<td>NetApp FAS8040</td>
<td>Clustered Data ONTAP 8.2.2</td>
<td>Operating system version</td>
</tr>
<tr>
<td>Cisco</td>
<td>Cisco Nexus 5596UP Cluster Interconnect</td>
<td>5.2(1)N1(1)</td>
<td>Operating system version</td>
</tr>
<tr>
<td>VMware</td>
<td>ESXi 5.5</td>
<td>5.5</td>
<td>Hypervisor</td>
</tr>
<tr>
<td>VMware</td>
<td>vCenter Server</td>
<td>5.5</td>
<td>VMware Management</td>
</tr>
<tr>
<td>SUSE</td>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>11 SP3 (64 bit)</td>
<td>Operating System to host SAP HANA</td>
</tr>
<tr>
<td>RedHat</td>
<td>RedHat Enterprise Linux (RHEL) for SAP HANA</td>
<td>6.5 (64 bit)</td>
<td>Operating System to host SAP HANA</td>
</tr>
</tbody>
</table>

Configuration Guidelines

This document provides details for configuring a fully redundant, highly available configuration for a FlexPod unit with clustered Data ONTAP storage. Therefore, reference is made to which component is being configured with each step, either 01 or 02. For example, node01 and node02 are used to identify the
two NetApp storage controllers that are provisioned with this document and Cisco Nexus A and Cisco Nexus B identifies the pair of Cisco Nexus switches that are configured.

The Cisco UCS Fabric Interconnects are similarly configured. Additionally, this document details the steps for provisioning multiple Cisco UCS hosts, and these are identified sequentially: HANA-Server01, HANA-Server02, and so on. Finally, to indicate that you should include information pertinent to your environment in a given step, <text> appears as part of the command structure. See the following example for the network port vlan create command:

Usage:

```
network port vlan create ?
   [-node] <nodename>                  Node
   { [-vlan-name] {<netport>|<ifgrp>} } VLAN Name
   | -port {<netport>|<ifgrp>}          Associated Network Port
   [-vlan-id] <integer> }              Network Switch VLAN Identifier
```

Example:

```
network port vlan -node <node01> -vlan-name i0a-<vlan id>
```

This document is intended to enable you to fully configure the customer environment. In this process, various steps require you to insert customer-specific naming conventions, IP addresses, and VLAN schemes, as well as to record appropriate MAC addresses. Table 4 lists the configuration variables that are used throughout this document. This table can be completed based on the specific site variables and used in implementing the document configuration steps.

Table 4. Configuration Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;&lt;var_nexus_mgmt_A_hostname&gt;&gt;</td>
<td>Cisco Nexus Management A host name</td>
</tr>
<tr>
<td>&lt;&lt;var_nexus_mgmt_A_mgmt0_ip&gt;&gt;</td>
<td>Out-of-band Cisco Nexus Management A management IP address</td>
</tr>
<tr>
<td>&lt;&lt;var_nexus_mgmt_A_mgmt0_netmask&gt;&gt;</td>
<td>Out-of-band management network netmask</td>
</tr>
<tr>
<td>&lt;&lt;var_nexus_mgmt_A_mgmt0_gw&gt;&gt;</td>
<td>Out-of-band management network default gateway</td>
</tr>
<tr>
<td>&lt;&lt;var_nexus_mgmt_B_hostname&gt;&gt;</td>
<td>Cisco Nexus Management B host name</td>
</tr>
<tr>
<td>&lt;&lt;var_nexus_mgmt_B_mgmt0_ip&gt;&gt;</td>
<td>Out-of-band Cisco Nexus Management B management IP address</td>
</tr>
<tr>
<td>&lt;&lt;var_nexus_mgmt_B_mgmt0_netmask&gt;&gt;</td>
<td>Out-of-band management network netmask</td>
</tr>
<tr>
<td>&lt;&lt;var_nexus_mgmt_B_mgmt0_gw&gt;&gt;</td>
<td>Out-of-band management network default gateway</td>
</tr>
<tr>
<td>&lt;&lt;var_global_ntp_server_ip&gt;&gt;</td>
<td>NTP server IP address</td>
</tr>
<tr>
<td>&lt;&lt;var_oob_vlan_id&gt;&gt;</td>
<td>Out-of-band management network VLAN ID</td>
</tr>
<tr>
<td>&lt;&lt;var_admin_vlan_id&gt;&gt;</td>
<td>Admin network VLAN ID</td>
</tr>
<tr>
<td>&lt;&lt;var_boot_vlan_id&gt;&gt;</td>
<td>PXE boot network VLAN ID</td>
</tr>
<tr>
<td>&lt;&lt;var_esx_mgmt_vlan_id&gt;&gt;</td>
<td>ESXi Management Network for Management Server VLAN ID</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>&lt;&lt;var_esx_vmotion_vlan_id&gt;&gt;</td>
<td>ESXi vMotion Network VLAN ID</td>
</tr>
<tr>
<td>&lt;&lt;var_esx_nfs_vlan_id&gt;&gt;</td>
<td>ESXi NFS Storage Network VLAN ID</td>
</tr>
<tr>
<td>&lt;&lt;var_nexus_vpc_domain_mgmt_id&gt;&gt;</td>
<td>Unique Cisco Nexus switch VPC domain ID for Management Switch</td>
</tr>
<tr>
<td>&lt;&lt;var_nexus_vpc_domain_id&gt;&gt;</td>
<td>Unique Cisco Nexus switch VPC domain ID</td>
</tr>
<tr>
<td>&lt;&lt;var_vm_host_mgmt_01_ip&gt;&gt;</td>
<td>ESXi Server 01 for Management Server IP Address</td>
</tr>
<tr>
<td>&lt;&lt;var_vm_host_mgmt_02_ip&gt;&gt;</td>
<td>ESXi Server 02 for Management Server IP Address</td>
</tr>
<tr>
<td>&lt;&lt;var_nexus_A_hostname&gt;&gt;</td>
<td>Cisco Nexus A host name</td>
</tr>
<tr>
<td>&lt;&lt;var_nexus_A_mgmt0_ip&gt;&gt;</td>
<td>Out-of-band Cisco Nexus A management IP address</td>
</tr>
<tr>
<td>&lt;&lt;var_nexus_A_mgmt0_netmask&gt;&gt;</td>
<td>Out-of-band management network netmask</td>
</tr>
<tr>
<td>&lt;&lt;var_nexus_A_mgmt0_gw&gt;&gt;</td>
<td>Out-of-band management network default gateway</td>
</tr>
<tr>
<td>&lt;&lt;var_nexus_B_hostname&gt;&gt;</td>
<td>Cisco Nexus B host name</td>
</tr>
<tr>
<td>&lt;&lt;var_nexus_B_mgmt0_ip&gt;&gt;</td>
<td>Out-of-band Cisco Nexus B management IP address</td>
</tr>
<tr>
<td>&lt;&lt;var_nexus_B_mgmt0_netmask&gt;&gt;</td>
<td>Out-of-band management network netmask</td>
</tr>
<tr>
<td>&lt;&lt;var_nexus_B_mgmt0_gw&gt;&gt;</td>
<td>Out-of-band management network default gateway</td>
</tr>
<tr>
<td>&lt;&lt;var_storage_vlan_id&gt;&gt;</td>
<td>Storage network for HANA Data/log VLAN ID</td>
</tr>
<tr>
<td>&lt;&lt;var_internal_vlan_id&gt;&gt;</td>
<td>Node to Node Network for HANA Data/log VLAN ID</td>
</tr>
<tr>
<td>&lt;&lt;var_backup_vlan_id&gt;&gt;</td>
<td>Backup Network for HANA Data/log VLAN ID</td>
</tr>
<tr>
<td>&lt;&lt;var_client_vlan_id&gt;&gt;</td>
<td>Client Network for HANA Data/log VLAN ID</td>
</tr>
<tr>
<td>&lt;&lt;var_appserver_vlan_id&gt;&gt;</td>
<td>Application Server Network for HANA Data/log VLAN ID</td>
</tr>
<tr>
<td>&lt;&lt;var_datasource_vlan_id&gt;&gt;</td>
<td>Data source Network for HANA Data/log VLAN ID</td>
</tr>
<tr>
<td>&lt;&lt;var_replication_vlan_id&gt;&gt;</td>
<td>Replication Network for HANA Data/log VLAN ID</td>
</tr>
<tr>
<td>&lt;&lt;var_vhana_esx_mgmt_vlan_id&gt;&gt;</td>
<td>vHANA ESXi host Management network VLAN ID</td>
</tr>
<tr>
<td>&lt;&lt;var_vhana_esx_vmotion_vlan_id&gt;&gt;</td>
<td>vHANA ESXi host vMotion network VLAN ID</td>
</tr>
<tr>
<td>&lt;&lt;var_vhana_esx_nfs_vlan_id&gt;&gt;</td>
<td>vHANA ESXi host Storage network VLAN ID</td>
</tr>
<tr>
<td>&lt;&lt;var_vhana_storage_vlan_id&gt;&gt;</td>
<td>vHANA VMs Storage network VLAN ID</td>
</tr>
<tr>
<td>&lt;&lt;var_vhana_access_vlan_id&gt;&gt;</td>
<td>vHANA VMs Access network VLAN ID</td>
</tr>
<tr>
<td>&lt;&lt;iSCSI_vlan_id_A&gt;&gt;</td>
<td>iSCSI-A VLAN ID</td>
</tr>
<tr>
<td>&lt;&lt;iSCSI_vlan_id_B&gt;&gt;</td>
<td>iSCSI-B VLAN ID</td>
</tr>
<tr>
<td>&lt;&lt;var_ucs_clustername&gt;&gt;</td>
<td>Cisco UCS Manager cluster host name</td>
</tr>
<tr>
<td>&lt;&lt;var_ucsa_mgmt_ip&gt;&gt;</td>
<td>Cisco UCS fabric interconnect (FI) A out-of-band management IP address</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td><code>&lt;&lt;var_ucsa_mgmt_mask&gt;&gt;</code></td>
<td>Out-of-band management network netmask</td>
</tr>
<tr>
<td><code>&lt;&lt;var_ucsa_mgmt_gateway&gt;&gt;</code></td>
<td>Out-of-band management network default gateway</td>
</tr>
<tr>
<td><code>&lt;&lt;var_ucs_cluster_ip&gt;&gt;</code></td>
<td>Cisco UCS Manager cluster IP address</td>
</tr>
<tr>
<td><code>&lt;&lt;var_ucs_cluster_ip&gt;&gt;</code></td>
<td>Cisco UCS F1 B out-of-band management IP address</td>
</tr>
<tr>
<td><code>&lt;&lt;var_cimc_gateway&gt;&gt;</code></td>
<td>Out-of-band management network default gateway</td>
</tr>
<tr>
<td><code>&lt;&lt;var_ib-mgmt_vlan_id&gt;&gt;</code></td>
<td>In-band management network VLAN ID</td>
</tr>
<tr>
<td><code>&lt;&lt;var_node01_mgmnt_ip&gt;&gt;</code></td>
<td>Out-of-band management IP for cluster node 01</td>
</tr>
<tr>
<td><code>&lt;&lt;var_node01_mgmnt_mask&gt;&gt;</code></td>
<td>Out-of-band management network netmask</td>
</tr>
<tr>
<td><code>&lt;&lt;var_node01_mgmnt_gateway&gt;&gt;</code></td>
<td>Out-of-band management network default gateway</td>
</tr>
<tr>
<td><code>&lt;&lt;var_url_boot_software&gt;&gt;</code></td>
<td>Data ONTAP 8.2.2 URL; format: http://</td>
</tr>
<tr>
<td><code>&lt;&lt;var_number_of_disks&gt;&gt;</code></td>
<td>Number of disks to assign to each storage controller</td>
</tr>
<tr>
<td><code>&lt;&lt;var_node02_mgmnt_ip&gt;&gt;</code></td>
<td>Out-of-band management IP for cluster node 02</td>
</tr>
<tr>
<td><code>&lt;&lt;var_node02_mgmnt_mask&gt;&gt;</code></td>
<td>Out-of-band management network netmask</td>
</tr>
<tr>
<td><code>&lt;&lt;var_node02_mgmnt_gateway&gt;&gt;</code></td>
<td>Out-of-band management network default gateway</td>
</tr>
<tr>
<td><code>&lt;&lt;var_clustername&gt;&gt;</code></td>
<td>Storage cluster host name</td>
</tr>
<tr>
<td><code>&lt;&lt;var_cluster_base_license_key&gt;&gt;</code></td>
<td>Cluster base license key</td>
</tr>
<tr>
<td><code>&lt;&lt;var_nfs_license&gt;&gt;</code></td>
<td>NFS protocol license key</td>
</tr>
<tr>
<td><code>&lt;&lt;var_iscsi_license&gt;&gt;</code></td>
<td>iSCSI protocol license key</td>
</tr>
<tr>
<td><code>&lt;&lt;var_flexclone_license&gt;&gt;</code></td>
<td>FlexClone license key</td>
</tr>
<tr>
<td><code>&lt;&lt;var_password&gt;&gt;</code></td>
<td>Global default administrative password</td>
</tr>
<tr>
<td><code>&lt;&lt;var_cluster_mgmnt_ip&gt;&gt;</code></td>
<td>In-band management IP for the storage cluster</td>
</tr>
<tr>
<td><code>&lt;&lt;var_cluster_mgmnt_mask&gt;&gt;</code></td>
<td>Out-of-band management network netmask</td>
</tr>
<tr>
<td><code>&lt;&lt;var_cluster_mgmnt_gateway&gt;&gt;</code></td>
<td>Out-of-band management network default gateway</td>
</tr>
<tr>
<td><code>&lt;&lt;var_dns_domain_name&gt;&gt;</code></td>
<td>DNS domain name</td>
</tr>
<tr>
<td><code>&lt;&lt;var_nameserver_ip&gt;&gt;</code></td>
<td>DNS server IP(s)</td>
</tr>
<tr>
<td><code>&lt;&lt;var_node_location&gt;&gt;</code></td>
<td>Node location string for each node</td>
</tr>
<tr>
<td><code>&lt;&lt;var_node01&gt;&gt;</code></td>
<td>Cluster node 01 host name</td>
</tr>
<tr>
<td><code>&lt;&lt;var_node02&gt;&gt;</code></td>
<td>Cluster node 02 host name</td>
</tr>
<tr>
<td><code>&lt;&lt;var_node01_sp_ip&gt;&gt;</code></td>
<td>Out-of-band cluster node 01 service processor</td>
</tr>
<tr>
<td><code>&lt;&lt;var_node01_sp_mask&gt;&gt;</code></td>
<td>Out-of-band management network netmask</td>
</tr>
<tr>
<td><code>&lt;&lt;var_node01_sp_gateway&gt;&gt;</code></td>
<td>Out-of-band management network default gateway</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>&lt;&lt;var_node02_sp_ip&gt;&gt;</td>
<td>Out-of-band cluster node 02 device processor management IP</td>
</tr>
<tr>
<td>&lt;&lt;var_node02_sp_mask&gt;&gt;</td>
<td>Out-of-band management network netmask</td>
</tr>
<tr>
<td>&lt;&lt;var_node02_sp_gateway&gt;&gt;</td>
<td>Out-of-band management network default gateway</td>
</tr>
<tr>
<td>&lt;&lt;var_timezone&gt;&gt;</td>
<td>FlexPod time zone (for example, America/New_York)</td>
</tr>
<tr>
<td>&lt;&lt;var_snmp_contact&gt;&gt;</td>
<td>Administrator e-mail address</td>
</tr>
<tr>
<td>&lt;&lt;var_snmp_location&gt;&gt;</td>
<td>Cluster location string</td>
</tr>
<tr>
<td>&lt;&lt;var_oncommand_server_fqdn&gt;&gt;</td>
<td>VSC or OnCommand virtual machine fully qualified domain name (FQDN)</td>
</tr>
<tr>
<td>&lt;&lt;var_snmp_community&gt;&gt;</td>
<td>Storage cluster SNMP v1/v2 community name</td>
</tr>
<tr>
<td>&lt;&lt;var_mailhost&gt;&gt;</td>
<td>Mail server host name</td>
</tr>
<tr>
<td>&lt;&lt;var_storage_admin_email&gt;&gt;</td>
<td>Administrator e-mail address</td>
</tr>
<tr>
<td>&lt;&lt;var_security_cert_vserver_common_name&gt;&gt;</td>
<td>Infrastructure Vserver FQDN</td>
</tr>
<tr>
<td>&lt;&lt;var_country_code&gt;&gt;</td>
<td>Two-letter country code</td>
</tr>
<tr>
<td>&lt;&lt;var_state&gt;&gt;</td>
<td>State or province name</td>
</tr>
<tr>
<td>&lt;&lt;var_city&gt;&gt;</td>
<td>City name</td>
</tr>
<tr>
<td>&lt;&lt;var_org&gt;&gt;</td>
<td>Organization or company name</td>
</tr>
<tr>
<td>&lt;&lt;var_unit&gt;&gt;</td>
<td>Organizational unit name</td>
</tr>
<tr>
<td>&lt;&lt;var_security_cert_cluster_common_name&gt;&gt;</td>
<td>Storage cluster FQDN</td>
</tr>
<tr>
<td>&lt;&lt;var_security_cert_node01_common_name&gt;&gt;</td>
<td>Cluster node 01 FQDN</td>
</tr>
<tr>
<td>&lt;&lt;var_security_cert_node02_common_name&gt;&gt;</td>
<td>Cluster node 02 FQDN</td>
</tr>
<tr>
<td>&lt;&lt;var_clustermgmt_port&gt;&gt;</td>
<td>Port for cluster management</td>
</tr>
<tr>
<td>&lt;&lt;var_vsadmin_password&gt;&gt;</td>
<td>Password for VS admin account</td>
</tr>
<tr>
<td>&lt;&lt;var_vserver_mgmt_ip&gt;&gt;</td>
<td>Management IP address for Vserver</td>
</tr>
<tr>
<td>&lt;&lt;var_vserver_mgmt_mask&gt;&gt;</td>
<td>Subnet mask for Vserver</td>
</tr>
<tr>
<td>&lt;&lt;var_node01_boot_lif_ip&gt;&gt;</td>
<td>Cluster node 01 Boot VLAN IP address</td>
</tr>
<tr>
<td>&lt;&lt;var_node01_boot_lif_mask&gt;&gt;</td>
<td>Boot VLAN netmask</td>
</tr>
<tr>
<td>&lt;&lt;var_node02_boot_lif_ip&gt;&gt;</td>
<td>Cluster node 02 NFS Boot IP address</td>
</tr>
<tr>
<td>&lt;&lt;var_node02_boot_lif_mask&gt;&gt;</td>
<td>Boot VLAN netmask</td>
</tr>
<tr>
<td>&lt;&lt;var_node01_storage_data_lif_ip&gt;&gt;</td>
<td>Cluster node 01 Storage for HANA Data/Log VLAN IP address</td>
</tr>
<tr>
<td>&lt;&lt;var_node01_storage_data_lif_mask&gt;&gt;</td>
<td>Storage for HANA Data/Log VLAN netmask</td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>&lt;&lt;var_node02_storage_data_lif_ip&gt;&gt;</td>
<td>Cluster node 02 Storage for HANA Data/Log VLAN IP address</td>
</tr>
<tr>
<td>&lt;&lt;var_node02_storage_data_lif_mask&gt;&gt;</td>
<td>Storage for HANA Data/Log VLAN netmask</td>
</tr>
<tr>
<td>&lt;&lt;var_node01_esx_lif_ip&gt;&gt;</td>
<td>Cluster node 01 Storage for ESXi VLAN IP address</td>
</tr>
<tr>
<td>&lt;&lt;var_node01_esx_lif_mask&gt;&gt;</td>
<td>Storage for ESXi VLAN netmask</td>
</tr>
<tr>
<td>&lt;&lt;var_node02_esx_lif_ip&gt;&gt;</td>
<td>Cluster node 02 Storage for ESXi VLAN IP address</td>
</tr>
<tr>
<td>&lt;&lt;var_node02_esx_lif_mask&gt;&gt;</td>
<td>Storage for ESXi VLAN netmask</td>
</tr>
<tr>
<td>&lt;&lt;var_node01_vhana_lif_ip&gt;&gt;</td>
<td>Cluster node 01 vHANA Storage for VMs VLAN IP address</td>
</tr>
<tr>
<td>&lt;&lt;var_node01_vhana_lif_mask&gt;&gt;</td>
<td>vHANA Storage for VMs VLAN netmask</td>
</tr>
<tr>
<td>&lt;&lt;var_node02_vhana_lif_ip&gt;&gt;</td>
<td>Cluster node 02 vHANA Storage for VMs VLAN IP address</td>
</tr>
<tr>
<td>&lt;&lt;var_node02_vhana_lif_mask&gt;&gt;</td>
<td>vHANA Storage for VMs VLAN netmask</td>
</tr>
<tr>
<td>&lt;&lt;var_esxi_host1_nfs_ip&gt;&gt;</td>
<td>Storage Network VLAN IP address for each VMware ESXi host</td>
</tr>
<tr>
<td>&lt;&lt;var_vhana_storage_ip&gt;&gt;</td>
<td>Storage Network VLAN IP address for each vHANA VMs</td>
</tr>
<tr>
<td>&lt;&lt;var_node01_iscsi_A_IP&gt;&gt;</td>
<td>Cluster node 01 iSCSI A VLAN IP address</td>
</tr>
<tr>
<td>&lt;&lt;var_node01_iscsi_B_IP&gt;&gt;</td>
<td>Cluster node 01 iSCSI B VLAN IP address</td>
</tr>
<tr>
<td>&lt;&lt;var_node02_iscsi_A_IP&gt;&gt;</td>
<td>Cluster node 02 iSCSI A VLAN IP address</td>
</tr>
<tr>
<td>&lt;&lt;var_node02_iscsi_B_IP&gt;&gt;</td>
<td>Cluster node 02 iSCSI B VLAN IP address</td>
</tr>
<tr>
<td>&lt;&lt;var_backup_node01&gt;&gt;</td>
<td>NetApp Storage 01 for Backup</td>
</tr>
<tr>
<td>&lt;&lt;var_backup_node02&gt;&gt;</td>
<td>NetApp Storage 02 for Backup</td>
</tr>
<tr>
<td>&lt;&lt;var_host_boot_subnet&gt;&gt;</td>
<td>Boot VLAN IP range</td>
</tr>
<tr>
<td>&lt;&lt;var_host_data_subnet&gt;&gt;</td>
<td>ESXi Storage VLAN IP range</td>
</tr>
<tr>
<td>&lt;&lt;var_rule_index&gt;&gt;</td>
<td>Rule index number</td>
</tr>
<tr>
<td>&lt;&lt;var_ftp_server&gt;&gt;</td>
<td>IP address for FTP server</td>
</tr>
<tr>
<td>&lt;&lt;var_pxe_oob_IP&gt;&gt;</td>
<td>Out-of-band IP address for PXE boot Server</td>
</tr>
<tr>
<td>&lt;&lt;var_pxe_oob_subnet&gt;&gt;</td>
<td>Out-of-band netmask for PXE boot Server</td>
</tr>
<tr>
<td>&lt;&lt;var_pxe_boot_IP&gt;&gt;</td>
<td>Boot VLAN IP address for PXE boot Server</td>
</tr>
<tr>
<td>&lt;&lt;var_pxe_boot_subnet&gt;&gt;</td>
<td>Boot VLAN netmask for PXE boot Server</td>
</tr>
<tr>
<td>&lt;&lt;var_pxe_admin_IP&gt;&gt;</td>
<td>Admin Network IP address for PXE boot Server</td>
</tr>
<tr>
<td>&lt;&lt;var_pxe_admin_subnet&gt;&gt;</td>
<td>Admin VLAN netmask for PXE boot Server</td>
</tr>
<tr>
<td>&lt;&lt;var_vhana_host_mgnt_01_ip&gt;&gt;</td>
<td>vHANA host Management Network IP address</td>
</tr>
</tbody>
</table>
### Device Cabling

The information in this section is provided as a reference for cabling the network and storage components. The tables in this section contain details for the prescribed and supported configuration of the NetApp FAS8040 running NetApp Clustered Data ONTAP 8.2.2. For any modifications of this prescribed architecture, consult the NetApp Interoperability Matrix Tool (IMT). To simplify cabling requirements, the tables include both local and remote device and port locations. The tables show the out-of-band management ports connectivity into Management Pod Cisco Nexus 9000 Series Switches. To utilize a preexisting management infrastructure, the Management Ports cabling needs to be adjusted accordingly. These Management interfaces will be used in various configuration steps.

**Note:** In addition to the NetApp FAS 8000 configurations listed in the tables below, other configurations can be used so long as the configurations match the descriptions given in the tables and diagrams in this section.

Figure 23. shows a cabling diagram for a FlexPod configuration using the Cisco Nexus 9000 and NetApp FAS 8000 storage systems with NetApp Clustered Data ONTAP. The NetApp Storage Controller and disk shelves are connected according to best practices for the specific storage controller and disk shelves as shown. For disk shelf cabling, refer to the Universal SAS and ACP Cabling Guide.
Figure 23. Cable Connection Diagram
Table 5 through Table 12 provides the details of all the connections.

**Table 5.** Cisco Nexus 9000-A Cabling Information

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Nexus 9000 A</td>
<td>Eth1/1</td>
<td>10GbE Uplink to Customer Data Switch A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/2</td>
<td>10GbE Cisco UCS fabric interconnect A</td>
<td>Eth1/1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/3</td>
<td>10GbE Uplink to Customer Data Switch B</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/4</td>
<td>10GbE Cisco UCS fabric interconnect A</td>
<td>Eth1/3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/5*</td>
<td>10GbE Cisco Nexus 9000 Mgmt A</td>
<td>Eth1/3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/6</td>
<td>10GbE Cisco UCS fabric interconnect B</td>
<td>Eth1/1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/7*</td>
<td>10GbE Cisco Nexus 9000 Mgmt B</td>
<td>Eth1/3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/8</td>
<td>10GbE Cisco UCS fabric interconnect B</td>
<td>Eth1/3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/9*</td>
<td>10GbE Cisco Nexus 9000 B</td>
<td>Eth1/9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/10*</td>
<td>10GbE Cisco Nexus 9000 B</td>
<td>Eth1/10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/11*</td>
<td>10GbE Cisco Nexus 9000 B</td>
<td>Eth1/11</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/12*</td>
<td>10GbE Cisco Nexus 9000 B</td>
<td>Eth1/12</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/15</td>
<td>10GbE NetApp controller 1</td>
<td>e0b</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/16</td>
<td>10GbE NetApp controller 2</td>
<td>e0b</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/17</td>
<td>10GbE NetApp controller 1</td>
<td>e0e</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/18</td>
<td>10GbE NetApp controller 1</td>
<td>e0g</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/19</td>
<td>10GbE NetApp controller 2</td>
<td>e0e</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/20</td>
<td>10GbE NetApp controller 2</td>
<td>e0g</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/29</td>
<td>10GbE Cisco UCS fabric interconnect A</td>
<td>Eth1/9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/30</td>
<td>10GbE Cisco UCS fabric interconnect B</td>
<td>Eth1/9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/31</td>
<td>10GbE Cisco UCS fabric interconnect A</td>
<td>Eth1/13</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/32</td>
<td>10GbE Cisco UCS fabric interconnect B</td>
<td>Eth1/13</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MGMT0</td>
<td>GbE Cisco Nexus 9000 Mgmt A</td>
<td>Eth1/14</td>
<td></td>
</tr>
</tbody>
</table>

* The ports ETH1/9-12 can be replaced with E2/11 and E2/12 for 40G connectivity.
* The ports ETH1/5 and ETH1/7 can be replaced with E2/9 and E2/10 for 40G connectivity.

**Note:** For devices requiring GbE connectivity, use the GbE Copper SFP+s (GLC–T=).

**Table 6.** Cisco Nexus 9000-B Cabling Information

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/1</td>
<td>10GbE</td>
<td>Uplink to Customer Data Switch A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Device</td>
<td>Local Port</td>
<td>Connection</td>
<td>Remote Device</td>
<td>Remote Port</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------</td>
<td>------------</td>
<td>--------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Cisco Nexus 9000 B</td>
<td>Eth1/2</td>
<td>10GbE</td>
<td>Cisco UCS fabric interconnect A</td>
<td>Eth 1/5</td>
</tr>
<tr>
<td></td>
<td>Eth1/3</td>
<td>10GbE</td>
<td>Uplink to Customer Data Switch B</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/4</td>
<td>10GbE</td>
<td>Cisco UCS fabric interconnect A</td>
<td>Eth 1/7</td>
</tr>
<tr>
<td></td>
<td>Eth1/5*</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 Mgmt A</td>
<td>Eth 1/4</td>
</tr>
<tr>
<td></td>
<td>Eth1/6</td>
<td>10GbE</td>
<td>Cisco UCS fabric interconnect B</td>
<td>Eth 1/5</td>
</tr>
<tr>
<td></td>
<td>Eth1/7*</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 Mgmt B</td>
<td>Eth 1/4</td>
</tr>
<tr>
<td></td>
<td>Eth1/8</td>
<td>10GbE</td>
<td>Cisco UCS fabric interconnect B</td>
<td>Eth 1/7</td>
</tr>
<tr>
<td></td>
<td>Eth1/9*</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 A</td>
<td>Eth1/9</td>
</tr>
<tr>
<td></td>
<td>Eth1/10*</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 A</td>
<td>Eth1/10</td>
</tr>
<tr>
<td></td>
<td>Eth1/11*</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 A</td>
<td>Eth1/11</td>
</tr>
<tr>
<td></td>
<td>Eth1/12*</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 A</td>
<td>Eth1/12</td>
</tr>
<tr>
<td></td>
<td>Eth1/15</td>
<td>10GbE</td>
<td>NetApp controller 1</td>
<td>e0d</td>
</tr>
<tr>
<td></td>
<td>Eth1/16</td>
<td>10GbE</td>
<td>NetApp controller 2</td>
<td>e0d</td>
</tr>
<tr>
<td></td>
<td>Eth1/17</td>
<td>10GbE</td>
<td>NetApp controller 1</td>
<td>e0f</td>
</tr>
<tr>
<td></td>
<td>Eth1/18</td>
<td>10GbE</td>
<td>NetApp controller 1</td>
<td>e0h</td>
</tr>
<tr>
<td></td>
<td>Eth1/19</td>
<td>10GbE</td>
<td>NetApp controller 2</td>
<td>e0f</td>
</tr>
<tr>
<td></td>
<td>Eth1/20</td>
<td>10GbE</td>
<td>NetApp controller 2</td>
<td>e0h</td>
</tr>
<tr>
<td></td>
<td>Eth1/29</td>
<td>10GbE</td>
<td>Cisco UCS fabric interconnect A</td>
<td>Eth1/11</td>
</tr>
<tr>
<td></td>
<td>Eth1/30</td>
<td>10GbE</td>
<td>Cisco UCS fabric interconnect B</td>
<td>Eth1/11</td>
</tr>
<tr>
<td></td>
<td>Eth1/31</td>
<td>10GbE</td>
<td>Cisco UCS fabric interconnect A</td>
<td>Eth1/15</td>
</tr>
<tr>
<td></td>
<td>Eth1/32</td>
<td>10GbE</td>
<td>Cisco UCS fabric interconnect B</td>
<td>Eth1/15</td>
</tr>
<tr>
<td></td>
<td>MGMT0</td>
<td>GbE</td>
<td>Cisco Nexus 9000 Mgmt B</td>
<td>Eth1/14</td>
</tr>
</tbody>
</table>

* The ports ETH1/9-12 can be replaced with E2/11 and E2/12 for 40G connectivity.
* The ports ETH1/5 and ETH1/7 can be replaced with E2/9 and E2/10 for 40G connectivity.

**Note:** For devices requiring GbE connectivity, use the GbE Copper SFP+s (GLC-T=).

**Table 7.** NetApp Controller-1 Cabling Information

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetApp controller 1</td>
<td>e0M</td>
<td>GbE</td>
<td>Cisco Nexus 9000 Mgmt A</td>
<td>ETH1/18</td>
</tr>
<tr>
<td></td>
<td>e0i</td>
<td>GbE</td>
<td>Cisco Nexus 9000 Mgmt A</td>
<td>ETH1/19</td>
</tr>
<tr>
<td></td>
<td>e0P</td>
<td>GbE</td>
<td>SAS shelves</td>
<td>ACP port</td>
</tr>
<tr>
<td></td>
<td>e0a</td>
<td>10GbE</td>
<td>Cisco Nexus 5596 A</td>
<td>Eth1/1</td>
</tr>
<tr>
<td>Local Device</td>
<td>Local Port</td>
<td>Connection</td>
<td>Remote Device</td>
<td>Remote Port</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>------------</td>
<td>-----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>e0b</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 A</td>
<td>Eth1/15</td>
<td></td>
</tr>
<tr>
<td>e0c</td>
<td>10GbE</td>
<td>Cisco Nexus 5596 B</td>
<td>Eth1/1</td>
<td></td>
</tr>
<tr>
<td>e0d</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 B</td>
<td>Eth1/15</td>
<td></td>
</tr>
<tr>
<td>e0e</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 A</td>
<td>Eth 1/17</td>
<td></td>
</tr>
<tr>
<td>e0f</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 B</td>
<td>Eth 1/17</td>
<td></td>
</tr>
<tr>
<td>e0g</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 A</td>
<td>Eth 1/18</td>
<td></td>
</tr>
<tr>
<td>e0h</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 B</td>
<td>Eth 1/18</td>
<td></td>
</tr>
</tbody>
</table>

Note: When the term e0M is used, the physical Ethernet port to which the table is referring is the port indicated by a wrench icon on the rear of the chassis.

**Table 8.** NetApp Controller-2 Cabling Information

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetApp controller 2</td>
<td>e0M</td>
<td>GbE</td>
<td>Cisco Nexus 9000 Mgmt B</td>
<td>ETH1/18</td>
</tr>
<tr>
<td></td>
<td>e0i</td>
<td>GbE</td>
<td>Cisco Nexus 9000 Mgmt B</td>
<td>ETH1/19</td>
</tr>
<tr>
<td></td>
<td>e0P</td>
<td>GbE</td>
<td>SAS shelves</td>
<td>ACP port</td>
</tr>
<tr>
<td></td>
<td>e0a</td>
<td>10GbE</td>
<td>Cisco Nexus 5596 A</td>
<td>Eth1/2</td>
</tr>
<tr>
<td></td>
<td>e0b</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 A</td>
<td>Eth1/16</td>
</tr>
<tr>
<td></td>
<td>e0c</td>
<td>10GbE</td>
<td>Cisco Nexus 5596 B</td>
<td>Eth1/2</td>
</tr>
<tr>
<td></td>
<td>e0d</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 B</td>
<td>Eth1/16</td>
</tr>
<tr>
<td></td>
<td>e0e</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 A</td>
<td>Eth 1/19</td>
</tr>
<tr>
<td></td>
<td>e0f</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 B</td>
<td>Eth 1/19</td>
</tr>
<tr>
<td></td>
<td>e0g</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 A</td>
<td>Eth 1/20</td>
</tr>
<tr>
<td></td>
<td>e0h</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 B</td>
<td>Eth 1/20</td>
</tr>
</tbody>
</table>

Note: When the term e0M is used, the physical Ethernet port to which the table is referring is the port indicated by a wrench icon on the rear of the chassis.

**Table 9.** Cisco Nexus 5596-A Cabling Information

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Nexus 5596 A</td>
<td>Eth1/1</td>
<td>10GbE</td>
<td>NetApp controller 1</td>
<td>e0a</td>
</tr>
<tr>
<td></td>
<td>Eth1/2</td>
<td>10GbE</td>
<td>NetApp controller 2</td>
<td>e0a</td>
</tr>
<tr>
<td></td>
<td>Eth1/41</td>
<td>10GbE</td>
<td>Cisco Nexus 5596 B</td>
<td>Eth1/41</td>
</tr>
<tr>
<td></td>
<td>Eth1/42</td>
<td>10GbE</td>
<td>Cisco Nexus 5596 B</td>
<td>Eth1/42</td>
</tr>
</tbody>
</table>
### Table 10. Cisco Nexus 5596-B Cabling Information

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/43</td>
<td>10GbE</td>
<td>Cisco Nexus 5596 B</td>
<td>Eth1/43</td>
<td></td>
</tr>
<tr>
<td>Eth1/44</td>
<td>10GbE</td>
<td>Cisco Nexus 5596 B</td>
<td>Eth1/44</td>
<td></td>
</tr>
<tr>
<td>Eth1/45</td>
<td>10GbE</td>
<td>Cisco Nexus 5596 B</td>
<td>Eth1/45</td>
<td></td>
</tr>
<tr>
<td>Eth1/46</td>
<td>10GbE</td>
<td>Cisco Nexus 5596 B</td>
<td>Eth1/46</td>
<td></td>
</tr>
<tr>
<td>Eth1/47</td>
<td>10GbE</td>
<td>Cisco Nexus 5596 B</td>
<td>Eth1/47</td>
<td></td>
</tr>
<tr>
<td>Eth1/48</td>
<td>10GbE</td>
<td>Cisco Nexus 5596 B</td>
<td>Eth1/48</td>
<td></td>
</tr>
<tr>
<td>MGMT0</td>
<td>GbE</td>
<td>Cisco Nexus 9000 Mgmt A</td>
<td>ETH1/16</td>
<td></td>
</tr>
</tbody>
</table>

### Table 11. Cisco UCS Fabric Interconnect A - Cabling Information

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/1</td>
<td>10GbE</td>
<td>NetApp controller 1</td>
<td>e0c</td>
<td></td>
</tr>
<tr>
<td>Eth1/2</td>
<td>10GbE</td>
<td>NetApp controller 2</td>
<td>e0c</td>
<td></td>
</tr>
<tr>
<td>Eth1/41</td>
<td>10GbE</td>
<td>Cisco Nexus 5596 A</td>
<td>Eth1/41</td>
<td></td>
</tr>
<tr>
<td>Eth1/42</td>
<td>10GbE</td>
<td>Cisco Nexus 5596 A</td>
<td>Eth1/42</td>
<td></td>
</tr>
<tr>
<td>Eth1/43</td>
<td>10GbE</td>
<td>Cisco Nexus 5596 A</td>
<td>Eth1/43</td>
<td></td>
</tr>
<tr>
<td>Eth1/44</td>
<td>10GbE</td>
<td>Cisco Nexus 5596 A</td>
<td>Eth1/44</td>
<td></td>
</tr>
<tr>
<td>Eth1/45</td>
<td>10GbE</td>
<td>Cisco Nexus 5596 A</td>
<td>Eth1/45</td>
<td></td>
</tr>
<tr>
<td>Eth1/46</td>
<td>10GbE</td>
<td>Cisco Nexus 5596 A</td>
<td>Eth1/46</td>
<td></td>
</tr>
<tr>
<td>Eth1/47</td>
<td>10GbE</td>
<td>Cisco Nexus 5596 A</td>
<td>Eth1/47</td>
<td></td>
</tr>
<tr>
<td>Eth1/48</td>
<td>10GbE</td>
<td>Cisco Nexus 5596 A</td>
<td>Eth1/48</td>
<td></td>
</tr>
<tr>
<td>MGMT0</td>
<td>GbE</td>
<td>Cisco Nexus 9000 Mgmt B</td>
<td>ETH1/16</td>
<td></td>
</tr>
</tbody>
</table>

### Table 11. Cisco UCS Fabric Interconnect A - Cabling Information

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/1</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 A</td>
<td>Eth 1/2</td>
<td></td>
</tr>
<tr>
<td>Eth1/2</td>
<td>10GbE</td>
<td>Cisco UCS Chassis 1 Fabric Extender (FEX) A</td>
<td>IOM 1/1</td>
<td></td>
</tr>
<tr>
<td>Eth1/3</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 A</td>
<td>Eth 1/4</td>
<td></td>
</tr>
<tr>
<td>Eth1/4</td>
<td>10GbE</td>
<td>Cisco UCS Chassis 1 Fabric Extender (FEX) A</td>
<td>IOM 1/2</td>
<td></td>
</tr>
<tr>
<td>Eth1/5</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 B</td>
<td>Eth 1/2</td>
<td></td>
</tr>
</tbody>
</table>
### Table 12. Cisco UCS Fabric Interconnect B - Cabling Information

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth1/6</td>
<td>10GbE</td>
<td>Cisco UCS Chassis 1 Fabric Extender (FEX) A</td>
<td>IOM 1/3</td>
<td></td>
</tr>
<tr>
<td>Eth1/7</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 B</td>
<td>Eth 1/4</td>
<td></td>
</tr>
<tr>
<td>Eth1/8</td>
<td>10GbE</td>
<td>Cisco UCS Chassis 1 Fabric Extender (FEX) A</td>
<td>IOM 1/4</td>
<td></td>
</tr>
<tr>
<td>Eth1/9</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 A</td>
<td>Eth 1/29</td>
<td></td>
</tr>
<tr>
<td>Eth1/10</td>
<td>10GbE</td>
<td>Cisco UCS Chassis 2 Fabric Extender (FEX) A</td>
<td>IOM 1/1</td>
<td></td>
</tr>
<tr>
<td>Eth1/11</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 B</td>
<td>Eth 1/29</td>
<td></td>
</tr>
<tr>
<td>Eth1/12</td>
<td>10GbE</td>
<td>Cisco UCS Chassis 2 Fabric Extender (FEX) A</td>
<td>IOM 1/2</td>
<td></td>
</tr>
<tr>
<td>Eth1/13</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 A</td>
<td>Eth 1/31</td>
<td></td>
</tr>
<tr>
<td>Eth1/14</td>
<td>10GbE</td>
<td>Cisco UCS Chassis 2 Fabric Extender (FEX) A</td>
<td>IOM 1/3</td>
<td></td>
</tr>
<tr>
<td>Eth1/15</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 B</td>
<td>Eth 1/31</td>
<td></td>
</tr>
<tr>
<td>Eth1/16</td>
<td>10GbE</td>
<td>Cisco UCS Chassis 2 Fabric Extender (FEX) A</td>
<td>IOM 1/4</td>
<td></td>
</tr>
<tr>
<td>Eth1/17</td>
<td>10GbE</td>
<td>Cisco UCS C460-M4-1</td>
<td>PCI Slot 4 Port 0</td>
<td></td>
</tr>
<tr>
<td>Eth1/18</td>
<td>10GbE</td>
<td>Cisco UCS C460-M4-1</td>
<td>PCI Slot 9 Port 0</td>
<td></td>
</tr>
<tr>
<td>Eth1/19</td>
<td>10GbE</td>
<td>Cisco UCS C220-M4-1</td>
<td>VIC 1225 Port 0</td>
<td></td>
</tr>
<tr>
<td>Eth1/20</td>
<td>10GbE</td>
<td>Cisco UCS C240-M4-1</td>
<td>VIC 1225 Port 0</td>
<td></td>
</tr>
<tr>
<td>MGMT0</td>
<td>GbE</td>
<td>Cisco Nexus 9000 Mgmt A</td>
<td>ETH1/15</td>
<td></td>
</tr>
<tr>
<td>L1</td>
<td>GbE</td>
<td>Cisco UCS fabric interconnect B</td>
<td>L1</td>
<td></td>
</tr>
<tr>
<td>L2</td>
<td>GbE</td>
<td>Cisco UCS fabric interconnect B</td>
<td>L2</td>
<td></td>
</tr>
</tbody>
</table>

**Table 12.** Cisco UCS Fabric Interconnect B - Cabling Information
<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS fabric interconnect B</td>
<td>Eth1/2</td>
<td>10GbE</td>
<td>Cisco UCS Chassis 1 Fabric Extender (FEX) B</td>
<td>IOM 1/1</td>
</tr>
<tr>
<td></td>
<td>Eth1/3</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 A</td>
<td>Eth 1/8</td>
</tr>
<tr>
<td></td>
<td>Eth1/4</td>
<td>10GbE</td>
<td>Cisco UCS Chassis 1 Fabric Extender (FEX) B</td>
<td>IOM 1/2</td>
</tr>
<tr>
<td></td>
<td>Eth1/5</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 B</td>
<td>Eth 1/6</td>
</tr>
<tr>
<td></td>
<td>Eth1/6</td>
<td>10GbE</td>
<td>Cisco UCS Chassis 1 Fabric Extender (FEX) B</td>
<td>IOM 1/3</td>
</tr>
<tr>
<td></td>
<td>Eth1/7</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 B</td>
<td>Eth 1/8</td>
</tr>
<tr>
<td></td>
<td>Eth1/8</td>
<td>10GbE</td>
<td>Cisco UCS Chassis 1 Fabric Extender (FEX) B</td>
<td>IOM 1/4</td>
</tr>
<tr>
<td></td>
<td>Eth1/9</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 A</td>
<td>Eth 1/40</td>
</tr>
<tr>
<td></td>
<td>Eth1/10</td>
<td>10GbE</td>
<td>Cisco UCS Chassis 2 Fabric Extender (FEX) B</td>
<td>IOM 1/1</td>
</tr>
<tr>
<td></td>
<td>Eth1/11</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 B</td>
<td>Eth 1/30</td>
</tr>
<tr>
<td></td>
<td>Eth1/12</td>
<td>10GbE</td>
<td>Cisco UCS Chassis 2 Fabric Extender (FEX) B</td>
<td>IOM 1/2</td>
</tr>
<tr>
<td></td>
<td>Eth1/13</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 A</td>
<td>Eth 1/31</td>
</tr>
<tr>
<td></td>
<td>Eth1/14</td>
<td>10GbE</td>
<td>Cisco UCS Chassis 2 Fabric Extender (FEX) B</td>
<td>IOM 1/3</td>
</tr>
<tr>
<td></td>
<td>Eth1/15</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 B</td>
<td>Eth 1/31</td>
</tr>
<tr>
<td></td>
<td>Eth1/16</td>
<td>10GbE</td>
<td>Cisco UCS Chassis 2 Fabric Extender (FEX) B</td>
<td>IOM 1/4</td>
</tr>
<tr>
<td></td>
<td>Eth1/17</td>
<td>10GbE</td>
<td>Cisco UCS C460-M4-1</td>
<td>PCI Slot 4 Port 1</td>
</tr>
<tr>
<td></td>
<td>Eth1/18</td>
<td>10GbE</td>
<td>Cisco UCS C460-M4-1</td>
<td>PCI Slot 9 Port 1</td>
</tr>
<tr>
<td></td>
<td>Eth1/19</td>
<td>10GbE</td>
<td>Cisco UCS C220-M4-1</td>
<td>VIC 1225 Port 1</td>
</tr>
<tr>
<td></td>
<td>Eth1/20</td>
<td>10GbE</td>
<td>Cisco UCS C240-M4-1</td>
<td>VIC 1225 Port 1</td>
</tr>
<tr>
<td></td>
<td>MGMT0</td>
<td>GbE</td>
<td>Cisco Nexus 9000 Mgmt B</td>
<td>ETH1/15</td>
</tr>
<tr>
<td></td>
<td>L1</td>
<td>GbE</td>
<td>Cisco UCS fabric interconnect A</td>
<td>L1</td>
</tr>
<tr>
<td></td>
<td>L2</td>
<td>GbE</td>
<td>Cisco UCS fabric interconnect A</td>
<td>L2</td>
</tr>
</tbody>
</table>
Management Pod Cabling

Table 13 through Table 16 provides the details of the connections used for Management Pod. As described earlier, in this reference design the Management Pod is directly connected to FlexPod as shown in Figure 20.

Table 13. Cisco Nexus 9000-A Management Pod Cabling Information

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Nexus 9000</td>
<td>Eth1/1</td>
<td>10GbE Uplink to Customer Data Switch A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mgmt A</td>
<td>Eth1/2</td>
<td>10GbE Uplink to Customer Data Switch B</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/3*</td>
<td>10GbE Uplink to FlexPod Cisco Nexus 9000 A</td>
<td>Eth1/5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/4*</td>
<td>10GbE Uplink to FlexPod Cisco Nexus 9000 B</td>
<td>Eth1/5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/5</td>
<td>10GbE Cisco UCS C-220-A</td>
<td>Port 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/7</td>
<td>10GbE Cisco UCS C-220-B</td>
<td>Port 0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/9*</td>
<td>10GbE Cisco Nexus 9000 Mgmt B</td>
<td>Eth1/9</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/10*</td>
<td>10GbE Cisco Nexus 9000 Mgmt B</td>
<td>Eth1/10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/11*</td>
<td>10GbE Cisco Nexus 9000 Mgmt B</td>
<td>Eth1/11</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/12*</td>
<td>10GbE Cisco Nexus 9000 Mgmt B</td>
<td>Eth1/12</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/14</td>
<td>1 GbE Cisco Nexus 9000 A</td>
<td>Mgmt0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/15</td>
<td>1 GbE Cisco UCS fabric interconnect A</td>
<td>Mgmt0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/16</td>
<td>1 GbE Cisco Nexus 5596 A</td>
<td>Mgmt0</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/17</td>
<td>1 GbE Cisco UCS C-220-A</td>
<td>CIMC M</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/18</td>
<td>1 GbE NetApp controller 1</td>
<td>e0M</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Eth1/19</td>
<td>1 GbE NetApp controller 1</td>
<td>e0i</td>
<td></td>
</tr>
<tr>
<td></td>
<td>MGMT0</td>
<td>GbE Customer GbE management switch</td>
<td>Any</td>
<td></td>
</tr>
</tbody>
</table>

* The ports ETH1/9-12 can be replaced with E2/11 and E2/12 for 40G connectivity.
* The ports ETH1/3-4 can be replaced with E2/9 and E2/10 for 40G connectivity.

Table 14. Cisco Nexus 9000-B Management Pod Cabling Information

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Nexus 9000</td>
<td>Eth1/1</td>
<td>10GbE Uplink to Customer Data Switch A</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mgmt B</td>
<td>Eth1/2</td>
<td>10GbE Uplink to Customer Data Switch B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local Device</td>
<td>Local Port</td>
<td>Connection</td>
<td>Remote Device</td>
<td>Remote Port</td>
</tr>
<tr>
<td>--------------</td>
<td>------------</td>
<td>------------</td>
<td>---------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>Eth1/3*</td>
<td>10GbE</td>
<td>Uplink to FlexPod Cisco Nexus 9000 A</td>
<td>Eth1/7</td>
</tr>
<tr>
<td></td>
<td>Eth1/4*</td>
<td>10GbE</td>
<td>Uplink to FlexPod Cisco Nexus 9000 B</td>
<td>Eth1/7</td>
</tr>
<tr>
<td></td>
<td>Eth1/5</td>
<td>10GbE</td>
<td>Cisco UCS C-220-A</td>
<td>Port 1</td>
</tr>
<tr>
<td></td>
<td>Eth1/7</td>
<td>10GbE</td>
<td>Cisco UCS C-220-B</td>
<td>Port 1</td>
</tr>
<tr>
<td></td>
<td>Eth1/9*</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 Mgmt A</td>
<td>Eth1/9</td>
</tr>
<tr>
<td></td>
<td>Eth1/10*</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 Mgmt A</td>
<td>Eth1/10</td>
</tr>
<tr>
<td></td>
<td>Eth1/11*</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 Mgmt A</td>
<td>Eth1/11</td>
</tr>
<tr>
<td></td>
<td>Eth1/12*</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 Mgmt A</td>
<td>Eth1/12</td>
</tr>
<tr>
<td></td>
<td>Eth1/14</td>
<td>1 GbE</td>
<td>Cisco Nexus 9000 B</td>
<td>Mgmt0</td>
</tr>
<tr>
<td></td>
<td>Eth1/15</td>
<td>1 GbE</td>
<td>Cisco UCS fabric interconnect B</td>
<td>Mgmt0</td>
</tr>
<tr>
<td></td>
<td>Eth1/16</td>
<td>1 GbE</td>
<td>Cisco Nexus 5596 B</td>
<td>Mgmt0</td>
</tr>
<tr>
<td></td>
<td>Eth1/17</td>
<td>1 GbE</td>
<td>Cisco UCS C-220-B</td>
<td>CIMC M</td>
</tr>
<tr>
<td></td>
<td>Eth1/18</td>
<td>1 GbE</td>
<td>NetApp controller 2</td>
<td>e0M</td>
</tr>
<tr>
<td></td>
<td>Eth1/19</td>
<td>1 GbE</td>
<td>NetApp controller 2</td>
<td>e0i</td>
</tr>
<tr>
<td></td>
<td>MGMT0</td>
<td>GbE</td>
<td>Customer GbE management switch</td>
<td>Any</td>
</tr>
</tbody>
</table>

* The ports ETH1/9-12 can be replaced with E2/11 and E2/12 for 40G connectivity.
* The ports ETH1/3-4 can be replaced with E2/9 and E2/10 for 40G connectivity.

Table 15. Cisco UCS C-Series Server-A

<table>
<thead>
<tr>
<th>Local Device</th>
<th>Local Port</th>
<th>Connection</th>
<th>Remote Device</th>
<th>Remote Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco UCS C-220-A</td>
<td>CIMC Port M</td>
<td>1GbE</td>
<td>Cisco Nexus 9000 Management A</td>
<td>Eth 1/17</td>
</tr>
<tr>
<td></td>
<td>Port 0</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 Management A</td>
<td>Eth 1/5</td>
</tr>
<tr>
<td></td>
<td>Port 1</td>
<td>10GbE</td>
<td>Cisco Nexus 9000 Management B</td>
<td>Eth 1/5</td>
</tr>
</tbody>
</table>

Table 16. Cisco UCS C-Series Server-B
Management Pod Installation

This section describes the configuration of the Management Pod to manage the multiple FlexPod environments for SAP HANA. In this reference architecture, the Management Pod includes a pair of Cisco Nexus 9000 Switches in standalone mode for out of band management network and a pair of Cisco UCS C220 M3 Rack-Mount Servers. The rack-mount servers for management are built on VMware ESXi. ESXi hosts will run PXE boot server, VMware vCenter and Windows Jump Host for Management. The next sections outline the configurations of each component in the Management Pod.

Network Configuration for Management Pod

The following section provides a detailed procedure for configuring the Cisco Nexus 9000 Series Switches for the Management Pod. It is based on cabling plan described in the Device Cabling section. If the systems connected on different ports, configure the switches accordingly following the guidelines described in this section.

Note: The configuration steps detailed in this section provides guidance for configuring the Cisco Nexus 9000 running release 6.1(2) within a multi-VDC environment.

Cisco Nexus 9000 Series Switches—Network Initial Configuration Setup

These steps provide details for the initial Cisco Nexus 9000 Series Switch setup.

Cisco Nexus 9000 A

To set up the initial configuration for the first Cisco Nexus switch complete the following steps:

Note: On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start and attempt to enter Power on Auto Provisioning.

```
----- Basic System Configuration Dialog VDC: 1 -----

This setup utility will guide you through the basic configuration of the system. Setup configures only enough connectivity for management of the system.

*Note: setup is mainly used for configuring the system initially, when no configuration is present. So setup always assumes system defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes

Do you want to enforce secure password standard (yes/no) [y]:

Create another login account (yes/no) [n]:

Configure read-only SNMP community string (yes/no) [n]:

Configure read-write SNMP community string (yes/no) [n]:

Enter the switch name : <<var_nexus_mgmt_A_hostname>>
```
Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:

  Mgmt0 IPv4 address : <<var_nexus_mgmt_A_mgmt0_ip>>
  Mgmt0 IPv4 netmask : <<var_nexus_mgmt_A_mgmt0_netmask>>

Configure the default gateway? (yes/no) [y]:

  IPv4 address of the default gateway : <<var_nexus_mgmt_A_mgmt0_gw>>

Configure advanced IP options? (yes/no) [n]:

  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]:
    Type of ssh key you would like to generate (dsa/rsa) [rsa]:
    Number of rsa key bits <1024-2048> [2048]:
  Configure the ntp server? (yes/no) [n]: y
    NTP server IPv4 address : <<var_global_ntp_server_ip>>

Configure CoPP system profile (strict/moderate/lenient/dense/skip) [strict]:

The following configuration will be applied:
password strength-check
switchname <<var_nexus_mgmt_A_hostname>>
vrf context management
ip route 0.0.0.0/0 <<var_nexus_mgmt_A_mgmt0_gw>>
exit
no feature telnet
ssh key rsa 2048 force
feature ssh
ntp server <<var_global_ntp_server_ip>>
copp profile strict
interface mgmt0
ip address <<var_nexus_mgmt_A_mgmt0_ip>> <<var_nexus_mgmt_A_mgmt0_netmask>>
no shutdown

Would you like to edit the configuration? (yes/no) [n]: Enter

Use this configuration and save it? (yes/no) [y]: Enter

[########################################] 100%
Copy complete.

Cisco Nexus 9000 B
To set up the initial configuration for the second Cisco Nexus switch complete the following steps:

Note: On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start and attempt to enter Power on Auto Provisioning.
Enable Appropriate Cisco Nexus 9000 Series Switches - Features and Settings

Cisco Nexus 9000 A and Cisco Nexus 9000 B

The following commands enable IP switching feature and set default spanning tree behaviors:
1. On each Nexus 9000, enter configuration mode:

   ```
   config terminal
   ```

2. Use the following commands to enable the necessary features:

   ```
   feature udld
   feature lacp
   feature vpc
   feature interface-vlan
   feature lldp
   ```

3. Configure spanning tree defaults:

   ```
   spanning-tree port type network default
   spanning-tree port type edge bpduguard default
   spanning-tree port type edge bpdufilter default
   ```

4. Save the running configuration to start-up:

   ```
   copy run start
   ```

**Create VLANs for Management Traffic**

**Cisco Nexus 9000 A and Cisco Nexus 9000 B**
To create the necessary virtual local area networks (VLANs), complete the following step on both switches:

From the configuration mode, run the following commands:

```
vlan <<var_oob_vlan_id>>
name OOB-Mgmt

vlan <<var_admin_vlan_id>>
name HANA-Admin

vlan <<var_boot_vlan_id>>
name HANA-Boot
```}

**Create VLANs for ESXi Traffic**

**Cisco Nexus 9000 A and Cisco Nexus 9000 B**
To create the necessary virtual local area networks (VLANs), complete the following step on both switches:

From the configuration mode, run the following commands:

```
vlan <<var_esx_mgmt_vlan_id>>
name ESX-MGMT

vlan <<var_esx_vmotion_vlan_id>>
name ESX-vMotion

vlan <<var_esx_nfs_vlan_id>>
name ESX-NFS
```}

**Configure Virtual Port Channel Domain**

**Cisco Nexus 9000 A**
To configure virtual port channels (vPCs) for switch A, complete the following step:

1. From the global configuration mode, create a new vPC domain:

   ```
   vpc domain <<var_nexus_vpc_domain_mgmt_id>>
   ```

2. Make Nexus 9000A the primary vPC peer by defining a low priority value:

   ```
   role priority 10
   ```
3. Use the management interfaces on the supervisors of the Nexus 9000s to establish a keepalive link:

```
peer-keepalive destination <<var_nexus_mgmnt_B_mgmt0_ip>> source <<var_nexus_mgmnt_A_mgmt0_ip>>
```

4. Enable following features for this vPC domain:

```
peer-switch
delay restore 150
peer-gateway
auto-recovery
```

**Cisco Nexus 9000 B**

To configure vPCs for switch B, complete the following steps:

1. From the global configuration mode, create a new vPC domain:

```
vpc domain <<var_nexus_vpc_domain_mgmt_id>>
```

2. Make Cisco Nexus 9000 B the secondary vPC peer by defining a higher priority value than that of the Nexus 9000 A:

```
role priority 20
```

3. Use the management interfaces on the supervisors of the Cisco Nexus 9000s to establish a keepalive link:

```
peer-keepalive destination <<var_nexus_mgmnt_A_mgmt0_ip>> source <<var_nexus_mgmnt_B_mgmt0_ip>>
```

4. Enable following features for this vPC domain:

```
peer-switch
delay restore 150
peer-gateway
auto-recovery
```

**Configure Network Interfaces for the VPC Peer Links**

**Cisco Nexus 9000 A**

1. Define a port description for the interfaces connecting to VPC Peer `<<var_nexus_mgmnt_B_hostname>>`

```
interface Eth1/9
description VPC Peer `<<var_nexus_mgmnt_B_hostname>>`:1/9

interface Eth1/10
description VPC Peer `<<var_nexus_mgmnt_B_hostname>>`:1/10

interface Eth1/11
description VPC Peer `<<var_nexus_mgmnt_B_hostname>>`:1/11

interface Eth1/12
description VPC Peer `<<var_nexus_mgmnt_B_hostname>>`:1/12
```

2. Apply a port channel to both VPC Peer links and bring up the interfaces.

```
interface Eth1/9-12
channel-group 1 mode active
no shutdown
```

3. Define a description for the port-channel connecting to `<<var_nexus_mgmnt_B_hostname>>`.

```
interface Po1
description vPC peer-link
```

4. Make the port-channel a switchport, and configure a trunk to allow Management VLANs.
5. Make this port-channel the VPC peer link and bring it up.

```plaintext
switchport
switchport mode trunk
switchport trunk allowed vlan
<<var_admin_vlan_id>>,<<var_boot_vlan_id>>,<<var_oob_vlan_id>>,<<var_esx_mgmt_vlan_id>>,<<var_esx_vmotion_vlan_id>>,<<var_esx_nfs_vlan_id>>
```

53 FlexPod Datacenter Reference Architecture for SAP Solution

---

**Cisco Nexus 9000 B**

1. Define a port description for the interfaces connecting to VPC peer <<var_nexus_A_hostname>>.

```plaintext
interface Eth1/9
description VPC Peer <<var_nexus_mgmt_A_hostname>>:1/9
interface Eth1/10
description VPC Peer <<var_nexus_mgmt_A_hostname>>:1/10
interface Eth1/11
description VPC Peer <<var_nexus_mgmt_A_hostname>>:1/11
interface Eth1/12
description VPC Peer <<var_nexus_mgmt_A_hostname>>:1/12
```

2. Apply a port channel to both VPC peer links and bring up the interfaces.

```plaintext
interface Eth1/9-12
channel-group 1 mode active
no shutdown
```

3. Define a description for the port-channel connecting to <<var_nexus_A_hostname>>.

```plaintext
interface Po1
description vPC peer-link
```

4. Make the port-channel a switchport, and configure a trunk to allow Management VLANs

```plaintext
switchport
switchport mode trunk
switchport trunk allowed vlan
<<var_admin_vlan_id>>,<<var_boot_vlan_id>>,<<var_oob_vlan_id>>,<<var_esx_mgmt_vlan_id>>,<<var_esx_vmotion_vlan_id>>,<<var_esx_nfs_vlan_id>>
```

5. Make this port-channel the VPC peer link and bring it up.

```plaintext
spanning-tree port type network
vpc peer-link
no shutdown
```

6. Save the running configuration to start-up in both Nexus 9000s.

```plaintext
copy run start
```

---

**Configure Network Interfaces to Cisco UCS C220 Management Server**

**Cisco Nexus 9000 A**

1. Define a port description for the interface connecting to <<var_c220>>-A and <<var_c220>>-B

```plaintext
interface Eth1/5
description << var_C220>>-A:P1
interface Eth1/7
description << var_C220>>-B:P1
```

2. Make the a switchport, and configure a trunk to allow NFS, PXE, Management, VM traffic VLANs

```plaintext
interface Eth1/5
switchport
switchport mode trunk
```
Cisco Nexus 9000 B

1. Define a port description for the interface connecting to <<var_c220>>-A and <<var_c220>>-B

```
interface Eth1/5
description << var_C220>>-A:P2

interface Eth1/7
description << var_C220>>-B:P2
```

2. Make the a switchport, and configure a trunk to allow NFS, PXE, Management, VM traffic VLANs

```
interface Eth1/5
switchport
switchport mode trunk
switchport trunk allowed vlan
<<var_admin_vlan_id>>,<<var_boot_vlan_id>>,<<var_oob_vlan_id>>,<<var_esx_mgmt>>

interface Eth1/7
switchport
switchport mode trunk
switchport trunk allowed vlan
<<var_admin_vlan_id>>,<<var_boot_vlan_id>>,<<var_oob_vlan_id>>,<<var_esx_mgmt>>
```

Configure Network Interfaces for Out of Band Management Plane Access

The following is an example of configuration for the Management Ports. Cable and configure based on the datacenter requirement. Since most the Management Ports are 1-GbE, please use 1-GbE SFPs to connect Twisted Pair Ethernet Cable.

**Cisco Nexus 9000 A**

To enable management access across the IP switching environment:

1. Define a port description for the interface connecting to the management switch:

```
interface 1/14
description OOB-Mgmt-FlexPod-NX9396-A

interface 1/15
description OOB-Mgmt-UCS-FI-A

interface 1/16
description OOB-Mgmt-NX5596-A

interface 1/17
description OOB-Mgmt-C220-CIMC-A

interface 1/18
description OOB-Mgmt-NetApp-8000-A-e0M

interface 1/19
description OOB-Mgmt-NetApp-8000-A-e0i
```

2. Configure the port as an access VLAN carrying the Out of Band management VLAN traffic.

```
interface 1/14-19
```
Cisco Nexus 9000 B

1. Define a port description for the interface connecting to the management switch:

   interface 1/14
   description OOB-Mgmt-FlexPod-NX9396-B

   interface 1/15
   description OOB-Mgmt-UCS-FI-B

   interface 1/16
   description OOB-Mgmt-NX5596-B

   interface 1/17
   description OOB-Mgmt-C220-CIMC-B

   interface 1/18
   description OOB-Mgmt-NetApp-8000-B-e0M

   interface 1/19
   description OOB-Mgmt-NetApp-8000-B-e0i

2. Configure the port as an access VLAN carrying the Out of Band management VLAN traffic.

   interface 1/14-19
   switchport
   switchport mode access
   switchport access vlan <<var_oob_vlan_id>>
   speed 1000
   no shutdown

3. Save the running configuration to start-up.

   copy run start

Direct Connection of Management Pod to Flexpod Infrastructure

This section describes the configuration steps for Cisco Nexus 9000 switches in the Management Pod connected to each FlexPod instance.

Cisco Nexus 9000 A

1. Define a port description for the interface connecting to <<var_nexus_A_hostname>>.

   interface Eth1/3
   description <<var_nexus_A_hostname>>:1/5

2. Apply it to a port channel and bring up the interface.

   interface eth1/3
   channel-group 6 mode active
   no shutdown

3. Define a port description for the interface connecting to <<var_nexus_B_hostname>>.

   interface Eth1/4
   description <<var_nexus_B_hostname>>:1/5

4. Apply it to a port channel and bring up the interface.

   interface Eth1/4
channel-group 6 mode active
no shutdown

5. Define a description for the port-channel connecting to FlexPod Switch

interface Po6
description <<var_nexus_A_hostname>>

6. Make the port-channel a switchport, and configure a trunk to allow all Management VLANs

switchport
switchport mode trunk
switchport trunk allowed vlan
<<var_admin_vlan_id>>,<<var_boot_vlan_id>>,<<var_oob_vlan_id>>,<<var_esx_mgmtn>>
na_esx_mgmt_vlan_id>>

7. Make the port channel and associated interfaces spanning tree network ports.

spanning-tree port type network

8. Set the MTU to be 9216 to support jumbo frames.

mtu 9216

9. Make this a VPC port-channel and bring it up.

vpc 6
no shutdown

10. Save the running configuration to start-up.

copy run start

Cisco Nexus 9000 B

1. Define a port description for the interface connecting to <<var_nexus_A_hostname>>.

interface Eth1/3
description <<var_nexus_A_hostname>>:1/7

2. Apply it to a port channel and bring up the interface.

interface eth1/3
channel-group 6 mode active
no shutdown

3. Define a port description for the interface connecting to <<var_nexus_B_hostname>>.

interface Eth1/4
description <<var_nexus_B_hostname>>:1/7

4. Apply it to a port channel and bring up the interface.

interface Eth1/4
channel-group 6 mode active
no shutdown

5. Define a description for the port-channel connecting to FlexPod Switch

interface Po6
description <<var_nexus_A_hostname>>

6. Make the port-channel a switchport, and configure a trunk to allow all Management VLANs

switchport
switchport mode trunk
switchport trunk allowed vlan
<<var_admin_vlan_id>>,<<var_boot_vlan_id>>,<<var_oob_vlan_id>>,<<var_esx_mgmtn>>
na_esx_mgmt_vlan_id>>

7. Make the port channel and associated interfaces spanning tree network ports.

spanning-tree port type network

8. Set the MTU to be 9216 to support jumbo frames.

mtu 9216

9. Make this a VPC port-channel and bring it up.

vpc 6
Uplink into Existing Network Infrastructure
Depending on the available network infrastructure, several methods and features can be used to uplink from the Management environment to connect to Flexpod SAP HANA environment. If an existing Cisco Nexus environment is present, Cisco recommends using vPCs to uplink the Cisco Nexus 9000 switches in the Management environment to the Flexpod SAP HANA environment. The previously described procedures can be used to create an uplink vPC to the existing environment. Make sure to run `copy run start` to save the configuration on each switch after configuration is completed.

Management Server Installation
The Cisco UCS C220 Server will act as a management server for the Solution. It requires VMware ESXi 5.5 both the Cisco UCS C220 Servers and for PXE boot tasks, it needs SLES11SP3 64Bit configuration. Windows system can also be considered (optional) on this management servers.

Server Configuration
The Cisco UCS C220 M3 Rack-Mount Servers are used to manage the Flexpod environment. Cisco Integrated Management Controller (CIMC) of Cisco UCS C220 M3 Servers and both the Cisco UCS VIC 1225 card ports must be connected to Cisco Nexus 9000 Series Switches in the management network, as defined in the Cabling Section. Three IP addresses are necessary for each Cisco UCS C220 M3 Server - one each for the CIMC, ESXi console and PXE boot VM.

CIMC Configuration
Use the following procedures to configure the IP-Address on the CIMC.
To configure the IP-Address on the CIMC complete the following steps:
1. With a direct attached monitor and keyboard press F8 when the following screen appears:

   ![CIMC Boot Up Screen](image)

   Press <F2> Setup, <F6> Boot Menu, <F7> Diagnostics, <F8> CIMC Config, <F12> Network Boot

   BIOS Version : C220M3.1.5.7.0.042820140436
   Platform ID : C220M3

   CIMC IP Address : 172.36.215.104
   \ Loading LSI EFI SAS Driver

   Processor(s) Genuine Intel(R) CPU @ 2.70GHz
   Total Memory = 192 GB  Effective Memory = 192 GB
   Memory Operating Speed 1600 KHz

   Entering CIMC Configuration Utility...
2. Configure the CIMC as required to be accessible from the Management LAN.

![CIMC Configuration Utility](image)

### NIC Properties
- **Mode**: Dedicated
- **IP address for CIMC**: 192.168.76.104
- **Subnet mask**: 255.255.255.0
- **Default Gateway**: 192.168.76.1
- **Default password**: Reenter password

### Storage Configuration
It is required to create a redundant virtual drive (RAID 1) on the internal disks to host ESXi and VMs. It is created from BIOS using the steps provided below:

**Note**: Virtual Drive on RAID can be created from BIOS.

6. On your browser go to IP address Set for CIMC.
7. In the Navigation Pane Server → Summary.
8. Click on Launch KVM Console.
9. Open with Java JRE installed.
10. Press Ctrl H to Launch WebBIOS.
11. Click Start to Configure the RAID

12. Click the Configuration Wizard.
13. Click New Configuration.

**Figure 29. Create New Configuration**
14. Click Yes to Clear the configuration.

**Figure 30.** RAID Configuration

15. Choose the Disks and click Add To Array.

**Figure 31.** Create Drive Group
16. Click on Accept DG.
17. Click Next.
18. Choose Drive Group and Click on Add to SPAN.

**Figure 32.** RAID Span

19. Click Next on the Span Definition screen.
20. Make sure that RAID Level RAID 1 is selected.
21. Click Accept.
22. Click Yes to Accept Write through Mode
23. Click Next to Create Virtual Drive
24. Click Accept to Save the Configuration
25. Click Yes to Initialize the Virtual Drive
26. Click Home and Exit the RAID Configuration.
27. Reboot the server from CIMC web browser Server --> Summary --> Hard Reset Server

Note: Alternately, RAID1 for two internal disks in the Management server can be set up from the CIMC web browser by completing the following steps:

23. Open a web browser and navigate to the Cisco C220-M3 CIMC IP address.
24. Enter admin as the user name and enter the administrative password, which was set previously
25. Click Login to log in to CIMC
26. On the Control Pane click the Storage tab.

27. Click Create Virtual Drive from Unused Physical Drives.
28. Choose RAID Level 1 and Select the Disks and Click on >> to add them in the Drive Groups.
29. Click Create Virtual Drive to create the virtual drive.
30. Click the Virtual Drive Info.
31. Click Initialize.

32. Click Initialize VD.
Cisco UCS VIC1225 vNIC Configuration

To configure Cisco UCS VIC 1225 vNIC through the CIMC browser, complete the following steps:

1. Click Inventory under the Server tab.
2. Click the Cisco VIC Adapters.

3. Click vNICs.
4. Under eth0 click Properties to change the MTU to 9000.
5. Under eth1 click Properties to change the MTU to 9000.

6. Reboot the server From Server --> Summary → Hard Reset Server.
VMware ESXi Installation
Install VMware ESXi 5.5 on the Cisco UCS M3 C-Series server and configure both Cisco UCS VIC 1225 interfaces as the ESX Management Network by completing the following steps.

Download Cisco Custom Image for ESXi 5.5.0 U1
1. Click the following link [vmware login page](#)
2. Type your email or customer number and the password and then click Log in
3. Click the following link [CiscoCustomImage5.5.0U1](#)
4. Click Download
5. Save it to your destination folder.

VMware ESXi Hosts ESXi-Mgmt-01 and ESXi-Mgmt-02
To prepare the server for the OS installation, complete the following steps on each ESXi host:

1. On your Browser go to IP address Set for CIMC
2. In the Navigation Pane Server ➔ Summary
3. Click Launch KVM Console
4. Open with Java JRE installed.
5. Click the VM Tab
6. Click Add Image.
7. Browse to the ESXi installer ISO image file and click Open.
8. Download ESXi-5.5.0-1746018-Custom-Cisco-5.5.1.3.iso
9. Select the Mapped checkbox to map the newly added image.
10. Click the KVM tab to monitor the server boot.
11. Boot the server by selecting Boot Server and click OK. Then click OK again.

Install ESXi
Management Server ESXi-Mgmt-01 and ESXi-Mgmt-02
To install VMware ESXi on the local disk, complete the following steps on each host:

1. On reboot, the machine detects the presence of the ESXi installation media. Select the ESXi installer from the menu that is displayed.
2. After the installer is finished loading, press Enter to continue with the installation.
3. Read and accept the end-user license agreement (EULA). Press F11 to accept and continue.
4. Select the local disk which was previously created for ESXi and press Enter to continue with the installation.
5. Select the appropriate keyboard layout and press Enter.
6. Enter and confirm the root password and press Enter.
7. The installer issues a warning that existing partitions will be removed from the volume. Press F11 to continue with the installation.
8. After the installation is complete, clear the Mapped checkbox (located in the Virtual Media tab of the KVM console) to unmap the ESXi installation image.
9. The ESXi installation image must be unmapped to make sure that the server reboots into ESXi and not into the installer.
10. The Virtual Media window might issue a warning stating that it is preferable to eject the media from the guest. Click Yes to unmap the image.
11. From the KVM tab, press Enter to reboot the server.

Set Up Management Networking for ESXi Hosts
Adding a management network for each VMware host is necessary for managing the host. To add a management network for the VMware hosts, complete the following steps on each ESXi host:
VMware ESXi Host ESXi-Mgmt-01
To configure the ESXi-Mgmt-01 ESXi host with access to the management network, complete the following steps:

1. After the server has finished rebooting, press F2 to customize the system.
2. Log in as root and enter the corresponding password.
3. Select the Configure the Management Network option and press Enter.
4. Select the VLAN (Optional) option and press Enter.
5. Enter the <<var_oob_vlan_id>> and press Enter.
6. From the Configure Management Network menu, select IP Configuration and press Enter.
7. Select the Set Static IP Address and Network Configuration option by using the space bar.
8. Enter the IP address for managing the first ESXi host: <<var_vm_host_mgmt_01_ip>>.
9. Enter the subnet mask for the first ESXi host.
10. Enter the default gateway for the first ESXi host.
11. Press Enter to accept the changes to the IP configuration.
12. Select the IPv6 Configuration option and press Enter.
13. Using the spacebar, unselect Enable IPv6 (restart required) and press Enter.
14. Select the DNS Configuration option and press Enter.
15. Because the IP address is assigned manually, the DNS information must also be entered manually.
16. Enter the IP address of the primary DNS server.
17. Optional: Enter the IP address of the secondary DNS server.
18. Enter the fully qualified domain name (FQDN) for the first ESXi host.
19. Press Enter to accept the changes to the DNS configuration.
20. Press Esc to exit the Configure Management Network submenu.
21. Press Y to confirm the changes and return to the main menu.
22. The ESXi host reboots. After reboot, press F2 and log back in as root.
23. Select Test Management Network to verify that the management network is set up correctly and press Enter.
24. Press Enter to run the test.
25. Press Enter to exit the window.
26. Press Esc to log out of the VMware console.

VMware ESXi Host ESXi-Mgmt-02
To configure the ESXi-Mgmt-02 ESXi host with access to the management network, complete the following steps:

1. After the server has finished rebooting, press F2 to customize the system.
2. Log in as root and enter the corresponding password.
3. Select the Configure the Management Network option and press Enter.
4. Select the VLAN (Optional) option and press Enter.
5. Enter the <<var_oob_vlan_id>> and press Enter.
6. From the Configure Management Network menu, select IP Configuration and press Enter.
7. Select the Set Static IP Address and Network Configuration option by using the space bar.
8. Enter the IP address for managing the second ESXi host: <<var_vm_host_mgmt_02_ip>>.
9. Enter the subnet mask for the second ESXi host.
10. Enter the default gateway for the second ESXi host.
11. Press Enter to accept the changes to the IP configuration.
12. Select the IPv6 Configuration option and press Enter.
13. Using the spacebar, unselect Enable IPv6 (restart required) and press Enter.
14. Select the DNS Configuration option and press Enter.

Note: Since the IP address is assigned manually, the DNS information must also be entered manually.

15. Enter the IP address of the primary DNS server.
16. Optional: Enter the IP address of the secondary DNS server.
17. Enter the FQDN for the second ESXi host.
18. Press Enter to accept the changes to the DNS configuration.
19. Press Esc to exit the Configure Management Network submenu.
20. Press Y to confirm the changes and return to the main menu.
22. Select Test Management Network to verify that the management network is set up correctly and press Enter.
23. Press Enter to run the test.
24. Press Enter to exit the window.
25. Press Esc to log out of the VMware console.

Download VMware vSphere Client and vSphere Remote CLI
To download the VMware vSphere Client and install Remote CLI, complete the following steps:
1. Open a web browser on the management workstation and navigate to the ESXi-Mgmt-01 management IP address.
2. Download and install both the vSphere Client and the Windows version of vSphere Remote Command Line.
3. These applications are downloaded from the VMware website and Internet access is required on the management workstation.

Log in to VMware ESXi Hosts Using VMware vSphere Client
VMware ESXi Host vHANA-Host-01
To log in to the ESXi-Mgmt-01 ESXi host by using the VMware vSphere Client, complete the following steps:
1. Open the recently downloaded VMware vSphere Client and enter the IP address of ESXi-Mgmt-01 as the host you are trying to connect to: <<var_vm_host_mgmt_02_ip>>.
2. Enter root for the user name.
3. Enter the root password.
4. Click Login to connect.

VMware ESXi Host VM-Host-Infra-02
To log in to the ESXi-Mgmt-02 ESXi host by using the VMware vSphere Client, complete the following steps:
1. Open the recently downloaded VMware vSphere Client and enter the IP address of VM-Host-Infra-02 as the host you are trying to connect to: <<var_vm_host_mgmt_02_ip>>.
2. Enter root for the user name.
3. Enter the root password.
4. Click Login to connect.

Set Up VMkernel Ports and Virtual Switch
VMware ESXi Host ESXi-Mgmt-01 (Repeat the steps in this section for all the ESXi Hosts)
To set up the VMkernel ports and the virtual switches on the ESXi-Mgmt-01 ESXi host, complete the following steps:
1. From each vSphere Client, select the host in the inventory.
2. Click the Configuration tab.
3. Click Networking in the Hardware pane.
4. Click Properties on the right side of vSwitch0.
5. Select the vSwitch configuration and click Edit.
6. From the General tab, change the MTU size based on the configuration of the Management switch
7. Click OK to close the properties for vSwitch0.
8. Select the Management Network configuration and click Edit.
9. Change the network label to VMkernel-MGMT and select the Management Traffic checkbox.
10. Click OK to finalize the edits for Management Network.
11. Select the VM Network configuration and click Edit.
12. Change the network label to Management Network and enter <<var_oob_vlan_id>> in the VLAN ID (Optional) field.
13. Click OK to finalize the edits for VM Network.
14. On the right, click Add Networking.
15. Select Virtual Machine and click Next.
16. Leave Create a vSphere standard switch selected select vmnic2 and vmnic3. Click Next.
17. For Network Label enter HANA-Boot
18. Enter VLAN ID for PXE Boot
19. Click Finish. vSwitch 1 is created.
20. In the Standard Switch: vSwitch1 Click on Properties
21. On the bottom left Click on Add
22. Leave Virtual Machine Connection type selected, then click Next
23. For Network Label enter HANA-Management
24. Enter VLAN ID for HANA Management Network
25. Click Next
26. Click Finish

Mount Required Datastores
For VMware ESXi Hosts ESXi-Mgmt-01 and ESXi-Mgmt-02, it is recommended to use Additional NetApp Storage for Management Pod for redundancy and failure scenarios. If you have NetApp storage for Management, then create a volume for datastores, create a VM Kernel port for storage, assign IP address and complete the following steps on each of the ESXi hosts:

1. From each vSphere Client, select the host in the inventory.
2. Click the Configuration tab to enable configurations.
3. Click Storage in the Hardware pane.
4. From the Datastore area, click Add Storage to open the Add Storage wizard.
5. Select Network File System and click Next.
6. The wizard prompts for the location of the NFS export. Enter the IP address for NFS Storage Device
7. Enter Volume path for the NFS export.
8. Make sure that the Mount NFS read only checkbox is NOT selected.
9. Enter mgmt_datastore_1 as the datastore name.
10. Click Next to continue with the NFS datastore creation.
11. Click Finish to finalize the creation of the NFS datastore.

Configure NTP on ESXi Hosts

VMware ESXi Hosts ESXi-Mgmt-01 and ESXi-Mgmt-02
To configure Network Time Protocol (NTP) on the ESXi hosts, complete the following steps on each host:

1. From each vSphere Client, select the host in the inventory.
2. Click the Configuration tab to enable configurations.
3. Click Time Configuration in the Software pane.
4. Click Properties at the upper right side of the window.
5. At the bottom of the Time Configuration dialog box, click Options.
6. In the NTP Daemon Options dialog box, complete the following steps:
   a. Click General in the left pane, select Start and stop with host.
   b. Click NTP Settings in the left pane and click Add.
7. In the Add NTP Server dialog box, enter <<var_global_ntp_server_ip>> as the IP address of the NTP server and click OK.
8. In the NTP Daemon Options dialog box, select the Restart NTP Service to Apply Changes checkbox and click OK.
9. In the Time Configuration dialog box, complete the following steps:
a. Select the NTP Client Enabled checkbox and click OK.
b. Verify that the clock is now set to approximately the correct time.

The NTP server time may vary slightly from the host time.

FlexPod Network Configuration for SAP HANA

The following section provides a detailed procedure for configuring the Cisco Nexus 9000 Switches for SAP HANA environment. The switch configuration in this section based on cabling plan described in the Device Cabling section. If the systems connected on different ports, configure the switches accordingly following the guidelines described in this section.

Note: The configuration steps detailed in this section provides guidance for configuring the Cisco Nexus 9000 running release 6.1(2) within a multi-VDC environment.

Cisco Nexus 9000 Series Switch—Network Initial Configuration Setup

These steps provide details for the initial Cisco Nexus 9000 Series Switch setup.

Cisco Nexus A

To set up the initial configuration for the first Cisco Nexus switch complete the following steps:

Note: On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start and attempt to enter Power on Auto Provisioning.

| ---- Basic System Configuration Dialog VDC: 1 ---- |
| This setup utility will guide you through the basic configuration of the system. Setup configures only enough connectivity for management of the system. |
| *Note: setup is mainly used for configuring the system initially, when no configuration is present. So setup always assumes system defaults and not the current system configuration values. |
| Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip the remaining dialogs. |
| Would you like to enter the basic configuration dialog (yes/no): yes |

Do you want to enforce secure password standard (yes/no) [y]:

Create another login account (yes/no) [n]:

Configure read-only SNMP community string (yes/no) [n]:

Configure read-write SNMP community string (yes/no) [n]:

Enter the switch name : <<var_nexus_A_hostname>>

Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:

Mgmt0 IPv4 address : <<var_nexus_A_mgmt0_ip>>

Mgmt0 IPv4 netmask : <<var_nexus_A_mgmt0_netmask>>
Configure the default gateway? (yes/no) [y]:
IPV4 address of the default gateway : <<var_nexus_A_mgmt0_gw>>

Configure advanced IP options? (yes/no) [n]:

Enable the telnet service? (yes/no) [n]:

Enable the ssh service? (yes/no) [y]:
Type of ssh key you would like to generate (dsa/rsa) [rsa]:
Number of rsa key bits <1024-2048> [2048]:

Configure the ntp server? (yes/no) [n]: y
NTP server IPV4 address : <<var_global_ntp_server_ip>>

Configure CoPP system profile (strict/moderate/lenient/dense/skip) [strict]:

The following configuration will be applied:
password strength-check
  switchname <<var_nexus_A_hostname>>
  vrf context management
  ip route 0.0.0.0/0 <<var_nexus_A_mgmt0_gw>>
exit
  no feature telnet
  ssh key rsa 2048 force
  feature ssh
  ntp server <<var_global_ntp_server_ip>>
  copp profile strict
  interface mgmt0
  ip address <<var_nexus_A_mgmt0_ip>> <<var_nexus_A_mgmt0_netmask>>
  no shutdown

Would you like to edit the configuration? (yes/no) [n]: Enter
Use this configuration and save it? (yes/no) [y]: Enter
[########################################] 100%
Copy complete.

Cisco Nexus B
To set up the initial configuration for the second Cisco Nexus switch complete the following steps:

Note: On initial boot and connection to the serial or console port of the switch, the NX-OS setup should automatically start and attempt to enter Power on Auto Provisioning.

---- Basic System Configuration Dialog VDC: 1 ----
This setup utility will guide you through the basic configuration of the system. Setup configures only enough connectivity for management of the system.

*Note: setup is mainly used for configuring the system initially, when no configuration is present. So setup always assumes system defaults and not the current system configuration values.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes
Create another login account (yes/no) [n]:
Configure read-only SNMP community string (yes/no) [n]:
Configure read-write SNMP community string (yes/no) [n]:
Enter the switch name: <<var_nexus_B_hostname>>

Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]:

Mgmt0 IPv4 address: <<var_nexus_B_mgmt0_ip>>
Mgmt0 IPv4 netmask: <<var_nexus_B_mgmt0_netmask>>

Configure the default gateway? (yes/no) [y]:

IPv4 address of the default gateway: <<var_nexus_B_mgmt0_gw>>

Configure advanced IP options? (yes/no) [n]:

Enable the telnet service? (yes/no) [n]:

Enable the ssh service? (yes/no) [y]:

Type of ssh key you would like to generate (dsa/rsa) [rsa]:

Number of rsa key bits <1024-2048> [2048]:

Configure the ntp server? (yes/no) [n]: y

NTP server IPv4 address: <<var_global_ntp_server_ip>>

Configure default interface layer (L3/L2) [L3]: L2

Configure default switchport interface state (shut/noshut) [shut]: Enter

Configure CoPP system profile (strict/moderate/lenient/dense/skip) [strict]:

The following configuration will be applied:
password strength-check
switchname <<var_nexus_B_hostname>>
vrf context management
ip route 0.0.0.0/0 <<var_nexus_B_mgmt0_gw>>
exit
no feature telnet
ssh key rsa 2048 force
feature ssh
ntp server <<var_global_ntp_server_ip>>
copp profile strict
interface mgmt0
ip address <<var_nexus_B_mgmt0_ip>> <<var_nexus_B_mgmt0_netmask>>
no shutdown

Would you like to edit the configuration? (yes/no) [n]: Enter

Use this configuration and save it? (yes/no) [y]: Enter

[########################################] 100%
Copy complete.

Enable Appropriate Cisco Nexus 9000 Series Switches—Features and Settings

Cisco Nexus 9000 A and Cisco Nexus 9000 B
The following commands enable IP switching feature and set default spanning tree behaviors:

1. On each Nexus 9000, enter configuration mode:

   config terminal

2. Use the following commands to enable the necessary features:
feature udld
feature lacp
feature vpc
feature interface-vlan
feature lldp

3. Configure spanning tree defaults:

spanning-tree port type network default
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default

4. Save the running configuration to start-up:

copy run start

Create VLANs for SAP HANA Traffic

Cisco Nexus 9000 A and Cisco Nexus 9000 B

To create the necessary VLANs, complete the following step on both switches:

From the configuration mode, run the following commands:

```bash
vlan <<var_storage_vlan_id>>
name HANA-Storage

vlan <<var_admin_vlan_id>>
name HANA-Admin

vlan <<var_boot_vlan_id>>
name HANA-Boot

vlan <<var_internal_vlan_id>>
name HANA-Internal

vlan <<var_backup_vlan_id>>
name HANA-Backup

vlan <<var_client_vlan_id>>
name HANA-Client

vlan <<var_appserver_vlan_id>>
name HANA-AppServer

vlan <<var_datasource_vlan_id>>
name HANA-DataSource

vlan <<var_replication_vlan_id>>
name HANA-Replication
```

Create VLANs for Virtualized SAP HANA (vHANA) Traffic

Cisco Nexus 9000 A and Cisco Nexus 9000 B

To create the necessary VLANs for vHANA traffic, complete the following step on both switches:

From the configuration mode, run the following commands:

```bash
vlan <<var_vhana_esx_mgmt_vlan_id>>
name ESX-MGMT

vlan <<var_vhana_esx_vmotion_vlan_id>>
name ESX-vMotion

vlan <<var_vhana_esx_nfs_vlan_id>>
```
name ESX-NFS
vlan <<var_vhana_storage_vlan_id>>
vHANA-Storage
vlan <<var_vhana_access_vlan_id>>
name vHANA-Access
vlan <<iSCSI_vlan_id_A>>
name iSCSI-VLAN-A
vlan <<iSCSI_vlan_id_B>>
name iSCSI-VLAN-B

Configure Virtual Port-Channel Domain

Cisco Nexus 9000 A
To configure vPCs for switch A, complete the following steps:
1. From the global configuration mode, create a new vPC domain:
   vpc domain <<var_nexus_vpc_domain_id>>
2. Make Nexus 9000A the primary vPC peer by defining a low priority value:
   role priority 10
3. Use the management interfaces on the supervisors of the Nexus 9000s to establish a keepalive link:
   peer-keepalive destination <<var_nexus_B_mgmt0_ip>> source <<var_nexus_A_mgmt0_ip>>
4. Enable following features for this vPC domain:
   peer-switch
delay restore 150
peer-gateway
auto-recovery

Cisco Nexus 9000 B
To configure vPCs for switch B, complete the following steps:
1. From the global configuration mode, create a new vPC domain:
   vpc domain <<var_nexus_vpc_domain_id>>
2. Make Cisco Nexus 9000 B the secondary vPC peer by defining a higher priority value than that of the Nexus 9000 A:
   role priority 20
3. Use the management interfaces on the supervisors of the Cisco Nexus 9000s to establish a keepalive link:
   peer-keepalive destination <<var_nexus_A_mgmt0_ip>> source <<var_nexus_B_mgmt0_ip>>
4. Enable following features for this vPC domain:
   peer-switch
delay restore 150
peer-gateway
auto-recovery
### Configure Network Interfaces for the VPC Peer Links

**Cisco Nexus 9000 A**

1. Define a port description for the interfaces connecting to VPC Peer `<var_nexus_B_hostname>`.

   ```
   interface Eth1/9
   description VPC Peer `<var_nexus_B_hostname>`:1/9
   
   interface Eth1/10
   description VPC Peer `<var_nexus_B_hostname>`:1/10
   
   interface Eth1/11
   description VPC Peer `<var_nexus_B_hostname>`:1/11
   
   interface Eth1/12
   description VPC Peer `<var_nexus_B_hostname>`:1/12
   ```

2. Apply a port channel to both VPC Peer links and bring up the interfaces.

   ```
   interface Eth1/9-12
   channel-group 1 mode active
   no shutdown
   ```

3. Define a description for the port-channel connecting to `<var_nexus_B_hostname>`.

   ```
   interface Po1
   description vPC peer-link
   ```

4. Make the port-channel a switchport, and configure a trunk to allow HANA VLANs

   ```
   switchport
   switchport mode trunk
   switchport trunk allowed vlan
   `<var_storage_vlan_id>`,`<var_admin_vlan_id>`,`<var_boot_vlan_id>`,`<var_internal_vlan_id>`,
   `<var_backup_vlan_id>`,`<var_client_vlan_id>`,`<var_appserver_vlan_id>`,
   `<var_datasource_vlan_id>`,
   `<var_replication_vlan_id>`
   ```

5. For Additional vHANA VLANs

   ```
   switchport trunk allowed vlan add
   `<var_vhana_esx_mgmt_vlan_id>`,`<var_vhana_esx_vmotion_vlan_id>`,`<var_vhana_esx_nfs_vlan_id>`,
   `<var_vhana_storage_vlan_id>`,`<var_vhana_access_vlan_id>`,<iSCSI_vlan_id_A>`,<iSCSI_vlan_id_B>
   ```

6. Make this port-channel the VPC peer link and bring it up.

   ```
   spanning-tree port type network
   vpc peer-link
   no shutdown
   ```

**Cisco Nexus 9000 B**

1. Define a port description for the interfaces connecting to VPC peer `<var_nexus_A_hostname>`.

   ```
   interface Eth1/9
   description VPC Peer `<var_nexus_A_hostname>`:1/9
   
   interface Eth1/10
   description VPC Peer `<var_nexus_A_hostname>`:1/10
   
   interface Eth1/11
   description VPC Peer `<var_nexus_A_hostname>`:1/11
   
   interface Eth1/12
   description VPC Peer `<var_nexus_A_hostname>`:1/12
   ```

2. Apply a port channel to both VPC peer links and bring up the interfaces.

   ```
   interface Eth1/9-12
   channel-group 1 mode active
   no shutdown
   ```

3. Define a description for the port-channel connecting to `<var_nexus_A_hostname>`.

   ```
   interface Po1
   description vPC peer-link
   ```
4. Make the port-channel a switchport, and configure a trunk to allow HANA VLANs

```
switchport
switchport mode trunk
switchport trunk allowed vlan
<<var_storage_vlan_id>>,<<var_admin_vlan_id>>,<<var_boot_vlan_id>>,<<var_internal_vlan_id >>,
<<var_backup_vlan_id>>, <<var_client_vlan_id>>, <<var_appserver_vlan_id>>,
<<var_datasource_vlan_id>>,<<var_replication_vlan_id>>
```

5. For Additional vHANA VLANs with iSCSI boot

```
switchport trunk allowed vlan add
<<var_vhana_esx_mgmt_vlan_id>>,<<var_vhana_esx_vmotion_vlan_id>>,<<var_vhana_esx_nfs_vlan_id>> ,
<<var_vhana_storage_vlan_id>>,<<var_vhana_access_vlan_id>>,<<iSCSI_vlan_id_A>>,<<iSCSI_vlan_id_B>>
```

6. Make this port-channel the VPC peer link and bring it up.

```
spanning-tree port type network
vpc peer-link
no shutdown
```

**Configure Network Interfaces to NetApp Storage for Data Traffic**

**Cisco Nexus 9000 A**

1. Define a port description for the interface connecting to <<var_node01>>.

```
interface Eth1/15
description <<var_node01>>_OS:e0b
```

2. Apply it to a port channel and bring up the interface.

```
channel-group 41 mode active
no shutdown
```

3. Define a description for the port-channel connecting to <<var_node01>>.

```
interface Po41
description <<var_node01>>_OS
```

4. Make the port-channel a switchport, and configure a trunk to allow NFS VLAN for OS.

```
switchport
switchport mode trunk
switchport trunk allowed vlan <<var_boot_vlan_id>>
```

5. For vHANA iSCSI Boot

```
switchport trunk allowed vlan add <<iSCSI_vlan_id_A>>,<<iSCSI_vlan_id_B>>
```

6. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

7. Make this a VPC port-channel and bring it up.

```
vpc 41
no shutdown
```

8. Define a port description for the interface connecting to <<var_node02>>.

```
interface Eth1/16
description <<var_node02>>_OS:e0b
```

9. Apply it to a port channel and bring up the interface

```
channel-group 42 mode active
no shutdown
```

10. Define a description for the port-channel connecting to <<var_node02>>.

```
interface Po42
```
11. Make the port-channel a switchport, and configure a trunk to allow NFS VLAN for Boot

```
switchport
switchport mode trunk
switchport trunk allowed vlan <<var_boot_vlan_id>>
```

12. For vHANA iSCSI Boot

```
switchport trunk allowed vlan add <<iSCSI_vlan_id_A>>,<<iSCSI_vlan_id_B>>
```

13. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

14. Make this a VPC port-channel and bring it up.

```
vpc 42
no shutdown
```

15. Define a port description for the interface connecting to `<<var_node01>>`.

```
interface Eth1/17
description `<<var_node01>>_DATA:e0e`
interface Eth1/18
description `<<var_node01>>_DATA:e0g`
```

16. Apply it to a port channel and bring up the interface.

```
interface eth1/17-18
cchannel-group 51 mode active
no shutdown
```

17. Define a description for the port-channel connecting to `<<var_node01>>`.

```
interface Po51
description `<<var_node01>>_DATA`
```

18. Make the port-channel a switchport, and configure a trunk to allow NFS VLAN for DATA.

```
switchport
switchport mode trunk
switchport trunk allowed vlan <<var_storage_vlan_id>>
```

19. For vHANA Storage

```
switchport trunk allowed vlan add
<<var_vhana_esx_nfs_vlan_id>>,<<var_vhana_storage_vlan_id>>
```

20. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

21. Set the MTU to be 9216 to support jumbo frames.

```
mtu 9216
```

22. Make this a VPC port-channel and bring it up.

```
vpc 51
no shutdown
```

23. Define a port description for the interface connecting to `<<var_node02>>`.

```
interface Eth1/17
description `<<var_node02>>_DATA:e0e`
interface Eth1/18
description `<<var_node02>>_DATA:e0g`
```

24. Apply it to a port channel and bring up the interface.

```
channel-group 52 mode active
no shutdown
```

25. Define a description for the port-channel connecting to `<<var_node02>>`.

```
interface Po52
description `<<var_node02>>_DATA`
```

26. Make the port-channel a switchport, and configure a trunk to allow NFS VLAN for DATA.

```
switchport
switchport mode trunk
switchport trunk allowed vlan <<var_storage_vlan_id>>
```
27. For vHANA Storage

```
switchport trunk allowed vlan add
<<var_vhana_esx_nfs_vlan_id>>,<<var_vhana_storage_vlan_id>>
```

28. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

29. Set the MTU to be 9216 to support jumbo frames.

```
mtu 9216
```

30. Make this a VPC port-channel and bring it up.

```
vpc 52
no shutdown
```

---

**Cisco Nexus 9000 B**

1. Define a port description for the interface connecting to `<<var_node01>>`.

```
interface Eth1/15
description <<var_node01>>_OS:e0d
```

2. Apply it to a port channel and bring up the interface.

```
channel-group 41 mode active
no shutdown
```

3. Define a description for the port-channel connecting to `<<var_node01>>`.

```
interface Po41
description <<var_node01>>_OS
```

4. Make the port-channel a switchport, and configure a trunk to allow NFS VLAN for OS.

```
switchport
switchport mode trunk
switchport trunk allowed vlan <<var_boot_vlan_id>>
```

5. For vHANA iSCSI Boot

```
switchport trunk allowed vlan add <<iSCSI_vlan_id_A>>,<<iSCSI_vlan_id_B>>
```

6. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

7. Make this a VPC port-channel and bring it up.

```
vpc 41
no shutdown
```

8. Define a port description for the interface connecting to `<<var_node02>>`.

```
interface Eth1/16
description <<var_node02>>_OS:e0d
```

9. Apply it to a port channel and bring up the interface.

```
channel-group 42 mode active
no shutdown
```

10. Define a description for the port-channel connecting to `<<var_node02>>`.

```
interface Po42
description <<var_node02>>_OS
```

11. Make the port-channel a switchport, and configure a trunk to allow NFS VLAN for Boot

```
switchport
switchport mode trunk
switchport trunk allowed vlan <<var_boot_vlan_id>>
```

12. For vHANA iSCSI Boot

```
switchport trunk allowed vlan add <<iSCSI_vlan_id_A>>,<<iSCSI_vlan_id_B>>
```

13. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

14. Make this a VPC port-channel and bring it up.
15. Define a port description for the interface connecting to <var_node01>.

```plaintext
interface Eth1/17
description <var_node01>_DATA:e0f
interface Eth1/18
description <var_node01>_DATA:e0h
```

16. Apply it to a port channel and bring up the interface.

```plaintext
interface eth1/17-18
channel-group 51 mode active
no shutdown
```

17. Define a description for the port-channel connecting to <var_node01>.

```plaintext
interface Po51
description <var_node01>_DATA
```

18. Make the port-channel a switchport, and configure a trunk to allow NFS VLAN for DATA.

```plaintext
switchport
switchport mode trunk
switchport trunk allowed vlan <var_storage_vlan_id>
```

19. For vHANA Storage

```plaintext
switchport trunk allowed vlan add
<var_vhana_esx_nfs_vlan_id>,<var_vhana_storage_vlan_id>
```

20. Make the port channel and associated interfaces spanning tree edge ports.

```plaintext
spanning-tree port type edge trunk
```

21. Set the MTU to be 9216 to support jumbo frames.

```plaintext
mtu 9216
```

22. Make this a VPC port-channel and bring it up.

```plaintext
vpc 51
no shutdown
```

23. Define a port description for the interface connecting to <var_node02>.

```plaintext
interface Eth1/17
description <var_node02>_DATA:e0f
interface Eth1/18
description <var_node02>_DATA:e0h
```

24. Apply it to a port channel and bring up the interface.

```plaintext
channel-group 52 mode active
no shutdown
```

25. Define a description for the port-channel connecting to <var_node02>.

```plaintext
interface Po52
description <var_node02>_DATA
```

26. Make the port-channel a switchport, and configure a trunk to allow NFS VLAN for DATA.

```plaintext
switchport
switchport mode trunk
switchport trunk allowed vlan <var_storage_vlan_id>
```

27. For vHANA Storage

```plaintext
switchport trunk allowed vlan add
<var_vhana_esx_nfs_vlan_id>,<var_vhana_storage_vlan_id>
```

28. Make the port channel and associated interfaces spanning tree edge ports.

```plaintext
spanning-tree port type edge trunk
```

29. Set the MTU to be 9216 to support jumbo frames.

```plaintext
mtu 9216
```

30. Make this a VPC port-channel and bring it up.

```plaintext
vpc 52
no shutdown
```
31. Save the running configuration to start-up in both Nexus 9000s.

```
copy run start
```

## Configure Network Interfaces with Cisco UCS Fabric Interconnect

### Cisco Nexus 9000 A
1. Define a port description for the interface connecting to `<var_ucs_clustername>-A`.

```
interface Eth1/2
description `<var_ucs_clustername>-A:1/1`
interface Eth1/4
description `<var_ucs_clustername>-A:1/3`
```

2. Apply it to a port channel and bring up the interface.

```
interface eth1/2
channel-group 11 mode active
no shutdown
interface eth1/4
channel-group 11 mode active
no shutdown
```

3. Define a description for the port-channel connecting to `<var_ucs_clustername>-A`.

```
interface Po11
description `<var_ucs_clustername>-A`
```

4. Make the port-channel a switchport, and configure a trunk to allow all HANA VLANs

```
switchport
switchport mode trunk
switchport trunk allowed vlan
`<<var_storage_vlan_id>>,<<var_admin_vlan_id>>,<<var_boot_vlan_id>>,<<var_internal_vlan_id >>,,<<var_backup_vlan_id>>, <<var_client_vlan_id>>, <<var_appserver_vlan_id>>, 
<<var_datasource_vlan_id>>, 
<<var_replication_vlan_id>>`
```

5. Make the port channel and associated interfaces spanning tree edge ports.

```
spanning-tree port type edge trunk
```

6. Set the MTU to be 9216 to support jumbo frames.

```
mtu 9216
```

7. Make this a VPC port-channel and bring it up.

```
vpc 11
no shutdown
```

8. Define a port description for the interface connecting to `<var_ucs_clustername>-B`.

```
interface Eth1/6
description `<var_ucs_clustername>-B:1/1`
interface Eth1/8
description `<var_ucs_clustername>-B:1/3`
```

9. Apply it to a port channel and bring up the interface.

```
interface Eth1/6
channel-group 12 mode active
no shutdown
interface Eth1/8
channel-group 12 mode active
no shutdown
```

10. Define a description for the port-channel connecting to `<var_ucs_clustername>-B`.

```
interface Po12
description `<var_ucs_clustername>-B`
```
11. Make the port-channel a switchport, and configure a trunk to allow InBand management, NFS, and VM traffic VLANs and the native VLAN.

```plaintext
switchport
switchport mode trunk
switchport trunk allowed vlan
<<var_storage_vlan_id>>,<<var_admin_vlan_id>>,<<var_boot_vlan_id>>,<<var_internal_vlan_id>>,<<var_backup_vlan_id>>, <<var_client_vlan_id>>, <<var_appserver_vlan_id>>, <<var_datasource_vlan_id>>, <<var_replication_vlan_id>>
```

12. Make the port channel and associated interfaces spanning tree edge ports.

```plaintext
spanning-tree port type edge trunk
```

13. Set the MTU to be 9216 to support jumbo frames.

```plaintext
mtu 9216
```

14. Make this a VPC port-channel and bring it up.

```plaintext
vpc 12
no shutdown
```

### Cisco Nexus 9000 B

1. Define a port description for the interface connecting to <<var_ucs_clustername>>-A.

```plaintext
interface Eth1/2
description <<var_ucs_clustername>>-A:1/5

interface Eth1/4
description <<var_ucs_clustername>>-A:1/7
```

2. Apply it to a port channel and bring up the interface.

```plaintext
interface eth1/2
cchannel-group 11 mode active
no shutdown

interface eth1/4
cchannel-group 11 mode active
no shutdown
```

3. Define a description for the port-channel connecting to <<var_ucs_clustername>>-A.

```plaintext
interface Po11
description <<var_ucs_clustername>>-A
```

4. Make the port-channel a switchport, and configure a trunk to allow all HANA VLANs

```plaintext
switchport
switchport mode trunk
switchport trunk allowed vlan
<<var_storage_vlan_id>>,<<var_admin_vlan_id>>,<<var_boot_vlan_id>>,<<var_internal_vlan_id>>,<<var_backup_vlan_id>>, <<var_client_vlan_id>>, <<var_appserver_vlan_id>>, <<var_datasource_vlan_id>>, <<var_replication_vlan_id>>
```

5. Make the port channel and associated interfaces spanning tree edge ports.

```plaintext
spanning-tree port type edge trunk
```

6. Set the MTU to be 9216 to support jumbo frames.

```plaintext
mtu 9216
```

7. Make this a VPC port-channel and bring it up.

```plaintext
vpc 11
no shutdown
```

8. Define a port description for the interface connecting to <<var_ucs_clustername>>-B.

```plaintext
interface Eth1/6
description <<var_ucs_clustername>>-B:1/5

interface Eth1/8
description <<var_ucs_clustername>>-B:1/7
```

9. Apply it to a port channel and bring up the interface.
10. Define a description for the port-channel connecting to `<<var_ucs_clustername>>`-B.

```bash
interface Po12
description <<var_ucs_clustername>>-B
```

11. Make the port-channel a switchport, and configure a trunk to allow InBand management, NFS, and VM traffic VLANs and the native VLAN.

```bash
switchport
switchport mode trunk
switchport trunk allowed vlan
<<var_storage_vlan_id>>,<<var_admin_vlan_id>>,<<var_boot_vlan_id>>,<<var_internal_vlan_id>>,<<var_backup_vlan_id>>,<<var_client_vlan_id>>,<<var_appserver_vlan_id>>,<<var_datasource_vlan_id>>,<<var_replication_vlan_id>>
```

12. Make the port channel and associated interfaces spanning tree edge ports.

```bash
spanning-tree port type edge trunk
```

13. Set the MTU to be 9216 to support jumbo frames.

```bash
mtu 9216
```

14. Make this a VPC port-channel and bring it up.

```bash
vpc 12
no shutdown
```

## Configure Additional Uplink to Cisco UCS Fabric Interconnect

When SAP HANA and SAP Application servers, run on a single Cisco UCS domain, their data traffic can be separated using the port-channel option to dedicated bandwidth for SAP HANA servers and SAP application servers. This is done by configuring an additional Uplink in the reference design as described below.

### Cisco Nexus 9000 A

1. Define a port description for the interface connecting to `<<var_ucs_clustername>>`-A.

```bash
interface Eth1/31
description <<var_ucs_clustername>>-A:1/13
```

2. Apply it to a port channel and bring up the interface.

```bash
interface eth1/31
channel-group 31 mode active
no shutdown
```

3. Define a description for the port-channel connecting to `<<var_ucs_clustername>>`-A.

```bash
interface Po31
description <<var_ucs_clustername>>-A
```

4. Make the port-channel a switchport, and configure a trunk to allow all `vHANA` VLANs

```bash
switchport
switchport mode trunk
switchport trunk allowed vlan add
<<var_vhana_esx_mgmt_vlan_id>>,<<var_vhana_esx_vmotion_vlan_id>>,<<var_vhana_esx_nfs_vlan_id>>,<<var_vhana_storage_vlan_id>>,<<var_vhana_access_vlan_id>>,<<iSCSI_vlan_id_A>>,<<iSCSI_vlan_id_B>>
```

5. Make the port channel and associated interfaces spanning tree edge ports.

```bash
spanning-tree port type edge trunk
```
6. Set the MTU to be 9216 to support jumbo frames.

```text
mtu 9216
```

7. Make this a VPC port-channel and bring it up.

```text
vpc 31
no shutdown
```

8. Define a port description for the interface connecting to `<<var_ucs_clustername>>-B`.

```text
interface Eth1/32
description `<<var_ucs_clustername>>-B:1/13`
```

9. Apply it to a port channel and bring up the interface.

```text
interface Eth1/32
cchannel-group 32 mode active
no shutdown
```

10. Define a description for the port-channel connecting to `<<var_ucs_clustername>>-B`.

```text
interface Po32
description `<<var_ucs_clustername>>-B`
```

11. Make the port-channel a switchport, and configure a trunk to allow InBand management, NFS, and VM traffic VLANs and the native VLAN.

```text
switchport
switchport mode trunk
switchport trunk allowed vlan add
`<<var_vhana_esx_mgmmt_vlan_id>>,<<var_vhana_esx_vmotion_vlan_id>>,<<var_vhana_esx_nfs_vlan_id>>,<<var_vhana_storage_vlan_id>>,<<var_vhana_access_vlan_id>>,<<iSCSI_vlan_id_A>>,<<iSCSI_vlan_id_B>>`
```

12. Make the port channel and associated interfaces spanning tree edge ports.

```text
spanning-tree port type edge trunk
```

13. Set the MTU to be 9216 to support jumbo frames.

```text
mtu 9216
```

14. Make this a VPC port-channel and bring it up.

```text
vpc 32
no shutdown
```

**Cisco Nexus 9000 B**

1. Define a port description for the interface connecting to `<<var_ucs_clustername>>-A`.

```text
interface Eth1/31
description `<<var_ucs_clustername>>-A:1/15`
```

2. Apply it to a port channel and bring up the interface.

```text
interface eth1/31
channel-group 31 mode active
no shutdown
```

3. Define a description for the port-channel connecting to `<<var_ucs_clustername>>-A`.

```text
interface Po31
description `<<var_ucs_clustername>>-A`
```

4. Make the port-channel a switchport, and configure a trunk to allow all HANA VLANs

```text
switchport
switchport mode trunk
switchport trunk allowed vlan add
`<<var_vhana_esx_mgmmt_vlan_id>>,<<var_vhana_esx_vmotion_vlan_id>>,<<var_vhana_esx_nfs_vlan_id>>,<<var_vhana_storage_vlan_id>>,<<var_vhana_access_vlan_id>>,<<iSCSI_vlan_id_A>>,<<iSCSI_vlan_id_B>>`
```

5. Make the port channel and associated interfaces spanning tree edge ports.

```text
spanning-tree port type edge trunk
```

6. Set the MTU to be 9216 to support jumbo frames.

```text
mtu 9216
```

7. Make this a VPC port-channel and bring it up.
Define a port description for the interface connecting to <<var_ucs_clustername>>-B.

```plaintext
interface Eth1/32
description <<var_ucs_clustername>>-B:1/15
```

Apply it to a port channel and bring up the interface.

```plaintext
interface Eth1/32
cchannel-group 32 mode active
no shutdown
```

Define a description for the port-channel connecting to <<var_ucs_clustername>>-B.

```plaintext
interface Po32
description <<var_ucs_clustername>>-B
```

Make the port-channel a switchport, and configure a trunk to allow InBand management, NFS, and VM traffic VLANs and the native VLAN.

```plaintext
switchport
switchport mode trunk
switchport trunk allowed vlan add
<<var_vhanna_esx_mgmt_vlan_id>>,<<var_vhanna_esx_vmotion_vlan_id>>,<<var_vhanna_esx_nfs_vlan_id>>,<<var_vhanna_storage_vlan_id>>,<<var_vhanna_access_vlan_id>>,<<iSCSI_vlan_id_A>>,<<iSCSI_vlan_id_B>>
```

Make the port channel and associated interfaces spanning tree edge ports.

```plaintext
spanning-tree port type edge trunk
```

Set the MTU to be 9216 to support jumbo frames.

```plaintext
mtu 9216
```

Make this a VPC port-channel and bring it up.

```plaintext
vpc 12
no shutdown
```

(Optional) Configure Network Interfaces for SAP HANA Backup/Data Source/Replication

You can define the port-channel for each type Network to have dedicated bandwidth. Below is an example to create such port-channel for Backup Network, these cable are connected to Storage for Backup. Here we assume two ports (Ethernet 1/29 and 1/30) are connected to dedicated NetApp Storage to backup HANA.

**Cisco Nexus 9000 A and Cisco Nexus 9000 B**

1. Define a port description for the interface connecting to <<var_node01>>.

```plaintext
interface Eth1/29
description <<var_backup_node01>>:<<Port_Number>>
```

2. Apply it to a port channel and bring up the interface.

```plaintext
interface Eth1/29
cchannel-group 21 mode active
no shutdown
```

3. Define a description for the port-channel connecting to <<var_backup_node01>>.

```plaintext
interface Po21
description <<var_backup_vlan_id>>
```

4. Make the port-channel a switchport, and configure a trunk to allow NFS VLAN for DATA.

```plaintext
switchport
switchport mode trunk
switchport trunk allowed vlan <<var_backup_vlan_id>>
```

5. Make the port channel and associated interfaces spanning tree edge ports.

```plaintext
spanning-tree port type edge trunk
```

6. Set the MTU to be 9216 to support jumbo frames.
mtu 9216
7. Make this a VPC port-channel and bring it up.

vpc 21
no shutdown
8. Define a port description for the interface connecting to <<var_node02>>.

interface Eth1/30
description <<var_backup_node01>>:<<Port_Number>>
9. Apply it to a port channel and bring up the interface

channel-group 22 mode active
no shutdown
10. Define a description for the port-channel connecting to <<var_node02>>.

interface Po22
description <<var_backup_node02>>
11. Make the port-channel a switchport, and configure a trunk to allow NFS VLAN for DATA

switchport
switchport mode trunk
switchport trunk allowed vlan <<var_backup_vlan_id>>
12. Make the port channel and associated interfaces spanning tree edge ports.

spanning-tree port type edge trunk
13. Set the MTU to be 9216 to support jumbo frames.

mtu 9216
14. Make this a VPC port-channel and bring it up.

vpc 22
no shutdown

(Optional) Management Plane Access for Cisco UCS Servers and VMs
This is an optional step, which can be used to implement a management plane access for the Cisco UCS servers and VMs.

Cisco Nexus 9000 A and Cisco Nexus 9000 B
To enable management access across the IP switching environment:

Note: You may want to create a dedicated Switch Virtual Interface (SVI) on the Nexus data plane to test and troubleshoot the management plane. If an L3 interface is deployed be sure it is deployed on both Cisco Nexus 9000s to ensure Type-2 VPC consistency.

1. Define a port description for the interface connecting to the management plane.

interface Eth1/<<interface_for_in_band_mgmnt>>
description IB-Mgmt:<<mgmt_uplink_port>>
2. Apply it to a port channel and bring up the interface.

channel-group 6 mode active
no shutdown
3. Define a description for the port-channel connecting to management switch.

interface Po6
description IB-Mgmt
4. Configure the port as an access VLAN carrying the InBand management VLAN traffic.

switchport
switchport mode access
switchport access vlan <<var_ib-mgmt_vlan_id>>
5. Make the port channel and associated interfaces normal spanning tree ports.
spanning-tree port type normal

6. Make this a VPC port-channel and bring it up.

vpc 6
no shutdown

7. Save the running configuration to start-up in both Nexus 9000s.

copy run start

Direct Connection of Flexpod Infrastructure to Management Pod

This section describes how to configure the Cisco Nexus 9000 switches from each Flexpod infrastructure to Management Pod. Cisco recommends using vPCs to uplink the Cisco Nexus 9000 switches from Flexpod SAP HANA environment to Management Pod. If an existing Cisco Nexus environment is present, the procedure described in this section can be used to create an uplink vPC to the existing environment.

Cisco Nexus 9000 A

1. Define a port description for the interface connecting to <<var_nexus_mgmt_A_hostname>>

   interface Eth1/5
   description <<var_nexus_mgmt_A_hostname>>:1/3

2. Apply it to a port channel and bring up the interface.

   interface Eth1/5
   channel-group 5 mode active
   no shutdown

3. Define a port description for the interface connecting to <<var_nexus_mgmt_B_hostname>>

   interface Eth1/7
   description <<var_nexus_mgmt_B_hostname>>:1/3

4. Apply it to a port channel and bring up the interface.

   interface Eth1/7
   channel-group 5 mode active
   no shutdown

5. Define a description for the port-channel connecting to <<var_nexus_mgmt >>

   interface Po5
   description <<var_nexus_mgmt_A_hostname>>

6. Make the port-channel a switchport, and configure a trunk to allow all Management VLANs

   switchport
   switchport mode trunk
   switchport trunk allowed vlan
   <<var_admin_vlan_id>>,<<var_boot_vlan_id>>,<<var_oob_vlan_id>>,<<var_esx_mgmt>>,<<var_vha
   na_esx_mgmt_vlan_id>>

7. Make the port channel and associated interfaces spanning tree network ports.

   spanning-tree port type network

8. Set the MTU to be 9216 to support jumbo frames.

   mtu 9216

9. Make this a VPC port-channel and bring it up.

   vpc 5
   no shutdown

10. Save the running configuration to start-up.

    copy run start
### Cisco Nexus 9000 B

1. Define a port description for the interface connecting to `<<var_nexus_mgmt_A_hostname>>`

   ```
   interface Eth1/5
   description <<var_nexus_mgmt_A_hostname>>:1/4
   ```

2. Apply it to a port channel and bring up the interface.

   ```
   interface eth1/5
   channel-group 5 mode active
   no shutdown
   ```

3. Define a port description for the interface connecting to `<<var_nexus_mgmt_B_hostname>>`

   ```
   interface Eth1/7
   description <<var_nexus_mgmt_B_hostname>>:1/4
   ```

4. Apply it to a port channel and bring up the interface.

   ```
   interface Eth1/7
   channel-group 5 mode active
   no shutdown
   ```

5. Define a description for the port-channel connecting to `<<var_nexus_mgmt>>`

   ```
   interface Po5
   description <<var_nexus_mgmt_A_hostname>>
   ```

6. Make the port-channel a switchport, and configure a trunk to allow all Management VLANs

   ```
   switchport
   switchport mode trunk
   switchport trunk allowed vlan <<var_admin_vlan_id>>,<<var_boot_vlan_id>>,<<var_oob_vlan_id>>,<<var_esx_mgmt>>,<<var_vhana_esx_mgmt_vlan_id>>
   ```

7. Make the port channel and associated interfaces spanning tree network ports.

   ```
   spanning-tree port type network
   ```

8. Set the MTU to be 9216 to support jumbo frames.

   ```
   mtu 9216
   ```

9. Make this a VPC port-channel and bring it up.

   ```
   vpc 5
   no shutdown
   ```

10. Save the running configuration to start-up.

    ```
    copy run start
    ```

### Uplink into Existing Network Infrastructure

Depending on the available network infrastructure, several methods and features can be used to uplink the SAP HANA environment. If an existing Cisco Nexus environment is present, Cisco recommends using vPCs to uplink the Cisco Nexus 9000 switches in the SAP HANA environment to the existing infrastructure. The previously described procedures can be used to create an uplink vPC to the existing environment. Make sure to run `copy run start` to save the configuration on each switch after configuration is completed.
Cisco UCS Solution for SAP HANA TDI

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. As mentioned earlier, this configuration provides better performance and superior disaster-tolerance solution for the whole system.

Cisco UCS servers enable separation of traffic, between a SAP HANA system and a non-SAP HANA system. This is achieved by creating a separate network uplink port-channel on Cisco UCS 6200 Fabric Interconnect, for each system type using the VLAN group option. This approach will guarantee the network bandwidth for each tenant in a secured environment. Figure 41 shows an example configuration to achieve this. In this example, two port-channels on each of the Cisco UCS Fabric Interconnects are created:

- Port-channel 11 and 13 are created on Cisco UCS Fabric Interconnect A
- Port-channel 12 and 14 are created on Cisco UCS Fabric Interconnect B

A VLAN group for SAP HANA is created and all the VLANs carrying traffic for SAP HANA is added to this VLAN group. This VLAN group can be forced to use port-channel 11 on Cisco UCS Fabric Interconnect A and port-channel 12 on Cisco UCS Fabric Interconnect B as shown. Similarly, a VLAN group for application servers can be created and all the VLANs carrying traffic for application servers can be added to this VLAN group. The VLAN group can be forced to use port-channel 13 on fabric interconnect A and port-channel 14 on fabric interconnect B.

This approach, archives bandwidth-separation between SAP HANA servers and applications servers and bandwidth for SAP HANA servers can be increased or decreased by altering the number of ports in the port-channel 11 and port-channel 12.
Figure 41. Network Separation Of Multiple Systems Using Port-Channel and VLAN Groups

Cisco Nexus 9396 Switches

Po 13 VPC

Po 11 VPC

Po 12 VPC

Po 14 VPC

Cisco UCS 6248UP F1

Cisco UCS B460 M4 Blades for SAP HANA

Cisco UCS B260 M4 / B200 M4 Blades for SAP Application
Cisco UCS Server Configuration

This section describes the specific configurations on Cisco UCS servers to address SAP HANA requirements.

Initial Setup of Cisco UCS 6248 Fabric Interconnect

This section provides detailed procedures for configuring the Cisco Unified Computing System (Cisco UCS) for use in FlexPod Datacenter Solution for SAP HANA environment. The steps are necessary to provision the Cisco UCS C-Series and B-Series servers to meet SAP HANA requirement.

Cisco UCS 6248 Fabric Interconnect A

To configure the Cisco UCS Fabric Interconnect A, complete the following steps:

1. Connect to the console port on the first Cisco UCS 6200 Fabric Interconnect.

   Enter the configuration method: console
   Enter the setup mode: set up newly or restore from backup (setup/restore)? setup
   You have chosen to setup a new fabric interconnect? Continue? (y/n): y
   Enforce strong passwords? (y/n) [y]: y
   Enter the password for "admin" <<var_password>>
   Enter the same password for "admin" <<var_password>>
   Is this fabric interconnect part of a cluster (select 'no' for standalone)? (yes/no) [n]: y
   Which switch fabric (A|B): A
   Enter the system name: <<var_ucs_clustername>>
   Physical switch Mgmt0 IPv4 address: <<var_ucsa_mgmt_ip>>
   Physical switch Mgmt0 IPv4 netmask: <<var_ucsa_mgmt_mask>>
   IPv4 address of the default gateway: <<var_ucsa_mgmt_gateway>>
   Cluster IPv4 address: <<var_ucs_cluster_ip>>
   Configure DNS Server IPv4 address? (yes/no) [no]: y
   DNS IPv4 address: <<var_nameserver_ip>>
   Configure the default domain name? y
   Default domain name: <<var_dns_domain_name>>
   Join centralized management environment (UCS Central)? (yes/no) [n]: Enter

2. Review the settings printed to the console. If they are correct, answer yes to apply and save the configuration.

3. Wait for the login prompt to make sure that the configuration has been saved.

Cisco UCS 6248 Fabric Interconnect B

To configure the Cisco UCS Fabric Interconnect B, complete the following steps:

1. Connect to the console port on the second Cisco UCS 6200 Fabric Interconnect.

   Enter the configuration method: console
   Installer has detected the presence of a peer Fabric interconnect. This Fabric interconnect will be added to the cluster. Do you want to continue [y/n]?: y
   Enter the admin password for the peer fabric interconnect: <<var_password>>
   Physical switch Mgmt0 IPv4 address: <<var_ucsb_mgmt_ip>>
   Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): y

2. Wait for the login prompt to make sure that the configuration has been saved.

Cisco UCS for SAP HANA

Log in to Cisco UCS Manager

To log in to the Cisco Unified Computing System (UCS) environment, complete the following steps:

1. Open a web browser and navigate to the Cisco UCS 6248 Fabric Interconnect cluster address.
2. Click the Launch UCS Manager link to download the Cisco UCS Manager software.
3. If prompted to accept security certificates, accept as necessary.
4. When prompted, enter admin as the user name and enter the administrative password.
5. Click Login to log in to Cisco UCS Manager.

**Figure 42. UCS Manager Log in**

---

**Upgrade Cisco UCS Manager Software to Version 2.2(3c)**

This document assumes the use of Cisco UCS Manager Software version 2.2(3c). To upgrade the Cisco UCS Manager software and the UCS 6248 Fabric Interconnect software to version 2.2(3c), refer to Cisco UCS Manager Install and Upgrade Guides.

**Add Block of IP Addresses for KVM Access**

To create a block of IP addresses for server Keyboard, Video, Mouse (KVM) access in the Cisco UCS environment, complete the following steps:

1. This block of IP addresses should be in the same subnet as the management IP addresses for the Cisco UCS Manager.
2. In Cisco UCS Manager, click the LAN tab in the navigation pane.
4. In the Actions pane, select Create Block of IP Addresses.
5. Enter the starting IP address of the block and the number of IP addresses required, and the subnet and gateway information.
6. Click OK to create the IP block.
7. Click OK in the confirmation message.

**Synchronize Cisco UCS to NTP**

To synchronize the Cisco UCS environment to the NTP server, complete the following steps:

1. In Cisco UCS Manager, click the Admin tab in the navigation pane.
2. Select All > Timezone Management.
3. In the Properties pane, select the appropriate time zone in the Timezone menu.
4. Click Save Changes, and then click OK.
5. Click Add NTP Server.
6. Enter \texttt{<<var\_global\_ntp\_server\_ip>>} and click OK.
7. Click OK.

**Cisco UCS Blade Chassis Connection Options**

For the Cisco UCS 2200 Series Fabric Extenders, two configuration options are available: pinning and port-channel.

SAP HANA node communicates with every other SAP HANA node using multiple I/O streams and this makes the port-channel option a highly suitable configuration. However, there are also SAP HANA use-cases in which only a few large I/O streams are used and for these cases, the pinning option provides a more stable performance. Because communication behavior varies between use-cases, SAP has defined a single-stream network performance test as part of the hardware validation tool (hwcct or hwval). To pass the hwval test, the pinning mode was used in this Cisco Validation Design.

**Cisco UCS Blade Chassis Connection in Pinning Mode**

In the pinning mode, every VIC in Cisco UCS B-Series server is pinned to an uplink port from the fabric extender (or I/O module [IOM]) to the fabric interconnect based on the availability of uplink ports. In most cases, the chassis is connected with four 10 Gigabit Ethernet cables per IOM to the fabric interconnect. The chassis backplane provides eight internal connections; a half-width blade can use one connection, and a full-width blade can use two connections. Every connector is mapped to a VIC on the blade, and every VIC is represented by a virtual network interface connection (vCON) in Cisco UCS Manager.

To run SAP HANA on an infrastructure with four uplinks per IOM, use Tables 17, 18 and 19 to understand the pinning of IOM uplink ports (Port1 to Port4) and vCON. This pinning information is used when the virtual network interface card (vNIC) and virtual host bus adapter (vHBA) placement policy is defined.

<table>
<thead>
<tr>
<th>Table 17. Cisco UCS 5108 Chassis with Eight Half-Width Blades (i.e.B200)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOM Port1 - vCON1 (Blade 1)</td>
</tr>
<tr>
<td>IOM Port3 - vCON1 (Blade 3)</td>
</tr>
<tr>
<td>IOM Port1 - vCON1 (Blade 5)</td>
</tr>
<tr>
<td>IOM Port3 - vCON1 (Blade 7)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 18. Cisco UCS 5108 Chassis with Four Full-Width Blades (i.e. B260)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOM Port1 - vCON1 (Blade 1)</td>
</tr>
<tr>
<td>IOM Port3 - vCON1 (Blade 2)</td>
</tr>
<tr>
<td>IOM Port1 - vCON1 (Blade 3)</td>
</tr>
<tr>
<td>IOM Port3 - vCON1 (Blade 4)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 19. Cisco UCS 5108 Chassis with Two Full-Width Double-High Blades (i.e. B460)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IOM Port1 - vCON3 (Blade 1)</td>
</tr>
<tr>
<td>IOM Port3 – vCON1 (Blade 1)</td>
</tr>
<tr>
<td>IOM Port1 – vCON3 (Blade 2)</td>
</tr>
<tr>
<td>IOM Port3 – vCON1 (Blade 2)</td>
</tr>
</tbody>
</table>
## Edit Chassis Discovery Policy
Setting the discovery policy simplifies the addition of Cisco UCS B-Series chassis and of additional fabric extenders for further C-Series connectivity.

To modify the chassis discovery policy, complete the following steps:

1. In Cisco UCS Manager, click the Equipment tab in the navigation pane and select Equipment in the list on the left.
2. In the right pane, click the Policies tab.
3. Under Global Policies, set the Chassis/FEX Discovery Policy to match the number of uplink ports that are cabled between the chassis or fabric extenders (FEXes) and the fabric interconnects.
4. Set the Link Grouping Preference to “none” for pinning mode.
5. Click Save Changes.
6. Click OK.

![Chassis Discovery Policy](image)

## Enable Server and Uplink Ports
To enable server and uplink ports, complete the following steps:

1. In Cisco UCS Manager, click the Equipment tab in the navigation pane.
3. Expand Ethernet Ports.
4. Select the ports that are connected to the chassis and / or to the Cisco C-Series Server (two per FI), right-click them, and select Configure as Server Port.
5. Click Yes to confirm server ports and click OK.
6. Verify that the ports connected to the chassis and / or to the Cisco C-Series Server are now configured as server ports.
7. Select ports that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port.
8. Click Yes to confirm uplink ports and click OK.
10. Expand Ethernet Ports.
11. Select the ports that are connected to the chassis or to the Cisco C-Series Server (two per FI), right-click them, and select Configure as Server Port.
12. Click Yes to confirm server ports and click OK.
13. Select ports that are connected to the Cisco Nexus switches, right-click them, and select Configure as Uplink Port.
14. Click Yes to confirm the uplink ports and click OK.

**Acknowledge Cisco UCS Chassis and Rack-Mount Servers**

To acknowledge all Cisco UCS chassis and Rack Mount Servers, complete the following steps:

1. In Cisco UCS Manager, click the Equipment tab in the navigation pane.
2. Expand Chassis and select each chassis that is listed.
3. Right-click each chassis and select Acknowledge Chassis.
4. Click Yes and then click OK to complete acknowledging the chassis.
5. If C-Series servers are part of the configuration, expand Rack Mounts and FEX.
6. Right-click each Server that is listed and select Acknowledge Server.
7. Click Yes and then click OK to complete acknowledging the Rack Mount Servers

Create Uplink Port Channels to Cisco Nexus Switches

A separate uplink port-channels for each of the network zones are defined as per SAP. For example, we create port-channel 11 on fabric interconnect A and port-channel 12 on fabric interconnect B for internal zone network. Create additional port-channel 21 on fabric interconnect A and port-channel 22 on fabric interconnect B for backup network, these uplinks are dedicated for backup traffic only. Configure the additional backup storage to communicate with backup VLAN created on Cisco UCS.

To configure the necessary port channels out of the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. In this procedure, two port channels are created: one from fabric A to both Cisco Nexus switches and one from fabric B to both Cisco Nexus switches.
4. Right-click Port Channels.
5. Select Create Port Channel.
6. Enter 11 as the unique ID of the port channel.
7. Enter vPC-11-Nexus as the name of the port channel.
8. Click Next.
9. Select the following ports to be added to the port channel:
   - Slot ID 1 and port 1
   - Slot ID 1 and port 3
   - Slot ID 1 and port 5
   - Slot ID 1 and port 7
10. Click >> to add the ports to the port channel.
11. Click Finish to create the port channel.
12. Click OK.
13. In the navigation pane, under LAN > LAN Cloud, expand the fabric B tree.
14. Right-click Port Channels.
15. Select Create Port Channel.
16. Enter 12 as the unique ID of the port channel.
17. Enter vPC-12-NEXUS as the name of the port channel.
18. Click Next.
19. Select the following ports to be added to the port channel:
   - Slot ID 1 and port 1
   - Slot ID 1 and port 3
   - Slot ID 1 and port 5
   - Slot ID 1 and port 7
20. Click >> to add the ports to the port channel.
21. Click Finish to create the port channel.
22. Click OK.

**Note:** For each additional NetApp Storage four Uplink ports from each Cisco UCS Fabric Interconnect is required. When more than one NetApp storage is configured additional Uplink ports should be included in the Port-Channel 11 on FI A and Port-Channel 12 on FI B.

Repeat the steps 1-22 to create Additional port-channel for each network zone.
Complete the following steps to create port-channel for backup network.

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Under LAN > LAN Cloud, expand the Fabric A tree.
3. Right-click Port Channels.
4. Select Create Port Channel (Figure 47).
5. Enter 21 as the unique ID of the port channel.
6. Enter vPC-21-Backup as the name of the port channel.
7. Click Next.

**Figure 47.** Cisco UCS - Port Channel wizard for Backup

8. Select the following ports to be added to the port channel:
   - Slot ID 1 and port 9
   - Slot ID 1 and port 11
9. Click >> to add the ports to the port channel.
10. Click Finish to create the port channel.
11. Click OK.
12. In the navigation pane, under LAN > LAN Cloud, expand the fabric B tree.
13. Right-click Port Channels.
14. Select Create Port Channel.
15. Enter 22 as the unique ID of the port channel.
16. Enter vPC-21-Backup as the name of the port channel.
17. Click Next.
18. Select the following ports to be added to the port channel:
   - Slot ID 1 and port 9
   - Slot ID 1 and port 11
19. Click >> to add the ports to the port channel.
20. Click Finish to create the port channel.
21. Click OK.

**Create New Organization**

For secure multi-tenancy within the Cisco UCS domain, a logical entity created known as organizations. To create organization unit, complete the following steps:

1. In Cisco UCS Manager, on the Tool bar click on New
2. From the drop down menu select Create Organization
3. Enter the Name as HANA
4. Optional Enter the Description as Org for HANA
Create MAC Address Pools

To configure the necessary MAC address pools for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Pools > root > Sub-Organization > HANA
3. In this procedure, two MAC address pools are created, one for each switching fabric.
4. Right-click MAC Pools under the root organization.
5. Select Create MAC Pool to create the MAC address pool.
6. Enter MAC_Pool_A as the name of the MAC pool.
7. Optional: Enter a description for the MAC pool.
8. Choose Assignment Order Sequential
9. Click Next.
10. Click Add.
11. Specify a starting MAC address.
12. The recommendation is to place 0A in the next-to-last octet of the starting MAC address to identify all of the MAC addresses as Fabric Interconnect A addresses.
13. Specify a size for the MAC address pool that is sufficient to support the available blade or server resources.

![Figure 48. Cisco UCS - Create MAC Pool for Fabric A](image)

14. Click OK.
15. Click Finish.
16. In the confirmation message, click OK.
17. Right-click MAC Pools under the HANA organization.
18. Select Create MAC Pool to create the MAC address pool.
19. Enter MAC_Pool_B as the name of the MAC pool.
20. Optional: Enter a description for the MAC pool.
21. Click Next.
22. Click Add.
23. Specify a starting MAC address.

**Note:** The recommendation is to place 0B in the next to last octet of the starting MAC address to identify all the MAC addresses in this pool as fabric B addresses.

24. Specify a size for the MAC address pool that is sufficient to support the available blade or server resources.
25. Click OK.
26. Click Finish.
27. In the confirmation message, click OK.

**Note:** You can also define separate MAC address Pool for each Network Zone. Follow the above steps 1-16 to create MAC address pool for each Network Zone. The recommendation is to create at least a separate Pool for Boot Network, as MAC address of the vNIC is required to configure DHCP for PXE Boot.

To configure the MAC address pools for the Boot vNIC, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Pools > root > Sub-Organization > HANA
3. Right-click MAC Pools under the root organization.
4. Select Create MAC Pool to create the MAC address pool
5. Enter HANA-Boot as the name of the MAC pool.
6. Optional: Enter a description for the MAC pool.
7. Choose Assignment Order Sequential
8. Click Next.
9. Click Add.
10. Specify a starting MAC address.
11. Specify a size for the MAC address pool that is sufficient to support the available blade or server resources.

**Figure 50.** Cisco UCS - Create MAC Pool for PXE Boot

12. Click OK.
13. Click Finish.

Figure 51 shows the overall MAC Address Pool created.
Create UUID Suffix Pool

To configure the necessary universally unique identifier (UUID) suffix pool for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Pools > root.
3. Right-click UUID Suffix Pools.
4. Select Create UUID Suffix Pool.
5. Enter UUID.Pool1 as the name of the UUID suffix pool.
6. Optional: Enter a description for the UUID suffix pool.
7. Keep the Prefix as the Derived option.
8. Select Sequential for Assignment Order
9. Click Next.
10. Click Add to add a block of UUIDs.
11. Keep the From field at the default setting.
12. Specify a size for the UUID block that is sufficient to support the available blade or server resources.
13. Click OK.
14. Click Finish.
15. Click OK.
Server Pool for SAP HANA

Server configuration to run SAP HANA is defined by SAP. Within Cisco UCS, it is possible to specify a policy to pull in all servers for SAP HANA in a pool.

Create Server Pool Policy Qualifications

To configure the qualification for server pool, complete the following steps:

**Note:** Consider creating unique server pools for each type of HANA servers. The following steps show qualifications for Cisco UCS B460 M4 Server with 1TB RAM and Intel E7-4890 Processors for HANA.

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
5. Enter HANA-1TB as the name of the server pool.
6. Optional: Enter a description for the server pool policy qualification.
7. In the Actions panel click on Create Memory Qualifications.
8. On Min Cap (MB) choose select button and enter 1048576 (for B260-M4 with 512 GB memory use 524288).
9. Click OK.
10. In the Actions panel click on Create CPU/Cores Qualifications.
11. On Min Number of Cores choose select button and enter 60 (for B260-M4 with 2 Socket choose 30).
12. On Min Number of Threads choose select button and enter 120 (for B260-M4 with 2 Socket choose 60).
13. On CPU Speed (MHz) choose select button and enter 2800.
14. Click OK.
15. Click OK.
16. Click OK.

![Create CPU/Cores Qualifications](image)

**Create Server Pool**

To configure the necessary server pool for the Cisco UCS environment, complete the following steps:

1. Consider creating unique server pools to achieve the granularity that is required in your environment.
2. In Cisco UCS Manager, click the Servers tab in the navigation pane.
4. Right-click Server Pools.
5. Select Create Server Pool.
6. Enter HANA-1TB-4890 as the name of the server pool.
7. Optional: Enter a description for the server pool.
8. Click Next.
9. Click Finish.
10. Click OK.

Cisco Server Pool Policy
The server pool for the SAP HANA nodes and its qualification policy are defined. With the server pool policy, the two definitions are mapped together.
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
3. Right-click Server Pool Policy.
4. Select Create Server Pool Policy.
5. Enter HANA-1TB as the name of the server pool.
6. For Target Pool choose HANA-1TB-4890 Server Pool created from the drop-down menu.
7. For Qualification choose HANA-1TB Server Pool Policy Qualifications created from the drop-down menu.
8. Click OK.

Figure 54. Server Pool Policy

As a result, all the servers with the specified qualification are now available in the server pool as shown in Figure 55.
To run Cisco UCS with two independent power distribution units, the redundancy must be configured as Grid. Complete the following steps:

1. In Cisco UCS Manager, click the Equipment tab in the navigation pane and select Equipment in the list on the left.
2. In the right pane, click the Policies tab.
3. Under Global Policies, set the Power Policy to “Grid.”
4. Click Save Changes.
5. Click OK.

Power Control Policy

Power Capping feature in Cisco UCS is designed to save power with a legacy data center use cases. This feature does not contribute much to the high performance behavior of SAP HANA. By choosing the option “No Cap” for power control policy, the SAP HANA server nodes will not have a restricted power supply. It is recommended to have this power control policy to ensure sufficient power supply for high performance and critical applications like SAP HANA.

To create a power control policy for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
4. Select Create Power Control Policy.
5. Enter HANA as the power control policy name.
6. Change the power capping setting to No Cap.
7. Click OK to create the power control policy.
8. Click OK.
Create Host Firmware Package

Firmware management policies allow the administrator to select the corresponding packages for a given server configuration. These policies often include packages for adapter, BIOS, board controller, FC adapters, host bus adapter (HBA) option ROM, and storage controller properties.

To create a firmware management policy for a given server configuration in the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Host Firmware Packages.
4. Select Create Host Firmware Package.
5. Enter `HANA-FW` as the name of the host firmware package.
7. Select the version 2.2(3c) for both the Blade and Rack Packages.
8. Click OK to create the host firmware package.
9. Click OK.

Figure 58. Host Firmware Package

Cisco UCS Manager only enforces power capping when the servers in a power group require more power than is currently available. With sufficient power, all servers run at full capacity regardless of their priority.
Create Local Disk Configuration Policy (Optional)

A local disk configuration for the Cisco UCS environment is necessary if the servers in the environment do not have a local disk.

**Note:** This policy should not be used on servers that contain local disks.

To create a local disk configuration policy, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
3. Right-click Local Disk Config Policies.
4. Select Create Local Disk Configuration Policy.
5. Enter **No-Local** as the local disk configuration policy name.
6. Change the mode to No Local Storage.
7. Click OK to create the local disk configuration policy.

**Figure 59.** Cisco UCS - Create Local Disk Policy

8. Click OK.

Create Server BIOS Policy

To get best performance for HANA it is required to configure the Server BIOS accurately. To create a server BIOS policy for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root > Sub-Organization > HANA.
4. Select Create BIOS Policy.
5. Enter **HANA-BIOS** as the BIOS policy name.
6. Change the Quiet Boot setting to Disabled.
7. Click Next.
8. Recommendation from SAP for SAP HANA is to disable all Processor C States. This will force the CPU to stay on maximum frequency and allow SAP HANA to run with best performance.

9. Click Next.
10. No changes required at the Intel Direct IO
11. Click Next.
12. In the RAS Memory please select maximum-performance and enable NUMA.

13. Click Next.
14. In the Serial Port Tab the Serial Port A: must be enabled.
15. Click Next.
16. No changes required at the USB settings

Figure 65. BIOS Policy – Advanced USB

17. Click Next.
18. No changes required at the PCI Configuration.
19. Click Next.
20. No changes required at the QPI.

**Figure 67.** BIOS Policy – QPI Configuration

21. Click Next.
22. No changes required at the LOM and PCIe Slots.
23. Click Next.
24. No changes required at the Boot Options.

25. Click Next.
26. Configure the Console Redirection to serial-port-a with the BAUD Rate 115200 and enable the feature Legacy OS redirect. This is used for Serial Console Access over LAN to all SAP HANA servers.
27. Click Finish to Create BIOS Policy.
28. Click OK.

Create Serial Over LAN Policy

The Serial over LAN policy is required to get console access to all the SAP HANA servers through SSH from the management network. This is used in case of the server hang or a Linux kernel crash, where the dump is required. Configure the speed in the Server Management Tab of the BIOS Policy.

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root > Sub-Organization > HANA.
3. Right-click Serial over LAN Policies.
4. Select Create Serial over LAN Policy.
5. Enter SoL-Console as the Policy name.
6. Select Serial over LAN State to enable.
7. Change the Speed to 115200.
8. Click OK.
Update Default Maintenance Policy

It is recommended to update the default Maintenance Policy with the Reboot Policy “User Ack” for the SAP HANA server. This policy will wait for the administrator to acknowledge the server reboot for the configuration changes to take effect.

To update the default Maintenance Policy, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root.
5. Click Save Changes.
6. Click OK to accept the change.

![Maintenance Policy](image)

### IPMI Access Profiles

The Serial over LAN access requires an IPMI access control to the board controller. This is also used for the STONITH function of the SAP HANA mount API to kill a hanging server. The default user is “sapadm” with the password “cisco”.

To create an IPMI Access Profile, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root > Sub-Organization > HANA.
4. Select Create IPMI Access Profile.
5. Enter HANA-IPMI as the Profile name.
6. Click on + (add) button.
7. Enter Username in the Name field and password.
8. Select Admin as Role.

9. Click OK to create user.
10. Click OK to Create IPMI Access Profile.
11. Click OK.
Adapter Policy Configuration
This section describes the Ethernet Adapter Policy with optimized RSS, Receive Queues and Interrupts values. This policy must be used for the SAP HANA internal network to provide best network performance.

To create an Ethernet Adapter Policy, complete the following steps:
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root > Sub-Organization > HANA.
4. Select Create Ethernet Adapter Policy.
5. Enter Linux-B460 as the Ethernet Adapter policy name.
6. Expand Resources ➔ Change the Receive Queues to 8.
7. Change the Interrupts to 11.
8. Expand Options ➔ Change Receive Side Scaling (RSS) to Enabled
9. Change Accelerated Receive Flow Steering to Enabled
10. Click OK to create the Ethernet Adapter policy.
11. Click OK.
Network Configuration

The core network requirements for SAP HANA are covered by Cisco UCS defaults. Cisco UCS is based on 10-GbE and provides redundancy via the Dual Fabric concept. The Service Profile is configured to distribute the traffic across Fabric Interconnect A and B. During normal operation, the traffic in the Internal Zone is on FI A and all the other traffic (Client Zone and Storage Zone) is on FI B. The inter-node traffic flows from a Blade Server to the Fabric Interconnect A and back to other Blade Server. All the other traffic must go over the Cisco Nexus 9000 switches to storage or to the data center network. With the integrated algorithms for bandwidth allocation and quality of service the Cisco UCS and Cisco Nexus distributes the traffic in an efficient way.

Set Jumbo Frames in Cisco UCS Fabric

To configure jumbo frames and enable quality of service in the Cisco UCS fabric, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select LAN > LAN Cloud > QoS System Class.
3. In the right pane, click the General tab.
4. On the MTU Column, enter 9216 in the box.
5. Check Enabled Under Priority for Platinum.
6. Click Save Changes in the bottom of the window.
7. Click OK
LAN Tab Configurations
Within Cisco UCS, all the network types for an SAP HANA system are reflected by defined VLANs. Network design from SAP has seven SAP HANA related networks and two infrastructure related networks. The VLAN IDs can be changed if required to match the VLAN IDs in the data center network – for example, ID 221 for backup should match the configured VLAN ID at the data center network switches. Even though nine VLANs are defined, VLANs for all the networks are not necessary if the solution will not use the network. For example if the Replication Network is not used in the solution, then VLAN ID 225 need not be created.

Create VLANs
To configure the necessary VLANs for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
   Note: In this procedure, Nine VLANs are created.
2. Select LAN > LAN Cloud.
3. Right-click VLANs.
4. Select Create VLANs.
5. Enter HANA-Boot as the name of the VLAN to be used for PXE boot network
6. Keep the Common/Global option selected for the scope of the VLAN.
7. Enter <<var_boot_vlan_id>> as the ID of the PXE boot network.
8. Keep the Sharing Type as None.
9. Click OK, and then click OK again.

Figure 78. Create VLAN for Boot
10. Repeat the Steps 1-9 for each VLAN.
11. Create VLAN for HANA-Admin.

**Figure 79.** Create VLAN for Admin


**Figure 80.** Create VLAN for AppServer

13. Create VLAN for HANA-Backup.

**Figure 81.** Create VLAN for Backup

**Figure 82.** Create VLAN for Client Network

15. Create VLAN for HANA-DataSource.

**Figure 83.** Create VLAN for Data Source

16. Create VLAN for HANA-Internal.

**Figure 84.** Create VLAN for Internal network

17. Create VLAN for HANA-Replication.
**Figure 85.** Create VLAN for Replication

18. Create VLAN for HANA-Storage

**Figure 86.** Create VLAN for Storage Access

Figure 87 shows the overview of VLANs created

**Figure 87.** VLAN definition in Cisco UCS

<table>
<thead>
<tr>
<th>Name</th>
<th>ID</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN HANA-Admin (112)</td>
<td>112</td>
<td>Lan</td>
</tr>
<tr>
<td>VLAN HANA-AppServer (223)</td>
<td>223</td>
<td>Lan</td>
</tr>
<tr>
<td>VLAN HANA-Backup (221)</td>
<td>221</td>
<td>Lan</td>
</tr>
<tr>
<td>VLAN HANA-Boot (127)</td>
<td>127</td>
<td>Lan</td>
</tr>
<tr>
<td>VLAN HANA-Client (222)</td>
<td>222</td>
<td>Lan</td>
</tr>
<tr>
<td>VLAN HANA-DataSource (224)</td>
<td>224</td>
<td>Lan</td>
</tr>
<tr>
<td>VLAN HANA-Internal (220)</td>
<td>220</td>
<td>Lan</td>
</tr>
<tr>
<td>VLAN HANA-Replication (225)</td>
<td>225</td>
<td>Lan</td>
</tr>
<tr>
<td>VLAN HANA-Storage (110)</td>
<td>110</td>
<td>Lan</td>
</tr>
<tr>
<td>VLAN default (1)</td>
<td>1</td>
<td>Lan</td>
</tr>
</tbody>
</table>
Create VLAN Groups

For easier management and bandwidth allocation to a dedicated uplink on the Fabric Interconnect, VLAN Groups are created within the Cisco UCS. The FlexPod Datacenter Solution for SAP HANA uses the following VLAN groups:

- Admin Zone
- Client Zone
- Internal Zone
- Backup Network
- Replication Network

To configure the necessary VLAN Groups for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.

   **Note:** In this procedure, five VLAN Groups are created. Based on the solution requirement create VLAN groups, it not required to create all five VLAN groups.

2. Select LAN > LAN Cloud.
3. Right-click VLAN Groups
4. Select Create VLAN Groups.
5. Enter Admin-Zone as the name of the VLAN Group used for Infrastructure network.
6. Select HANA-Admin

   **Figure 88.** Create VLAN Group for Admin Zone

7. Click Next
8. Click Next on Add Uplink Ports, since you will use Port-Channel
9. Choose Port-Channels Create for Admin Network
10. Click Finish
11. Follow the steps 1-10 for each VLAN Group
12. Create VLAN Groups for Internal Zone

13. Create VLAN Groups for Client Zone
14. Create VLAN Groups for Backup Network

**Figure 92.** Create VLAN Group for Backup Network

15. Click Next

16. Click Next on Add Uplink Ports, since we will use Port-Channel

17. Choose Port-Channels created for Backup Network
18. Click Finish
19. Create VLAN Groups for Replication Network

**Figure 94.** Create VLAN Group for Replication Network
Figure 95. VLAN Groups in UCS

<table>
<thead>
<tr>
<th>Name</th>
<th>Native VLAN</th>
<th>Native VLAN DM</th>
<th>Size</th>
<th>VLAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Group Admin-Zone</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN Group Backup-Zone</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN Group Client-Zone</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLAN Group Storage-Zone</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: For each VLAN Group a dedicated or shared Ethernet Uplink Port or Port Channel can be selected.

Figure 96. VLAN Groups – Uplink Port Channels for Admin-Zone

Create QoS Policies

QoS policies assign a system class to the network traffic for a vNIC. To create QoS Policy for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Policies > root > Sub-Organization > HANA.
3. Right-click QoS Policies
4. Select Create QoS Policy.
5. Enter Platinum as the QoS Policy name.
6. For Priority Select Platinum from the dropdown list.
7. Click OK to create Platinum QoS Policy.
Create vNIC Template

Each VLAN is mapped to a vNIC template to specify the characteristic of a specific network. The vNIC template configuration settings include MTU size, Failover capabilities and MAC-Address pools.

To create vNIC templates for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Policies > root > Sub-Organization > HANA.
3. Right-click vNIC Templates.
4. Select Create vNIC Template (Figure 97).
5. Enter HANA-Boot as the vNIC template name.
7. Select the Enable Failover checkbox.
8. Under Target, make sure that the VM checkbox is not selected.
9. Select Updating Template as the Template Type.
10. Under VLANs, select the checkboxes for HANA-Boot.
11. Set HANA-Boot as the native VLAN.
12. For MTU, enter 1500.
13. In the MAC Pool list, select HANA-Boot.

Figure 97. Create vNIC Template for Boot
14. Click OK to create the vNIC template.
15. Click OK.

Note: For most SAP HANA use cases the network traffic is well distributed across the two Fabrics (Fabric A and Fabric B) using the default setup. In special cases, it can be required to rebalance this distribution for better overall performance. This can be done in the vNIC template with the Fabric ID setting. Note that the MTU settings must match the configuration in customer data center. MTU setting of 9000 is recommended for best performance.

16. Follow the steps above 1-15 to create vNIC template for each Network zone.
17. Create vNIC template for Internal Network

**Note:** Internal Network requires >9.0 Gbps for SAP HANA inter-node communication, choose Platinum QoS Policy created for HANA-Internal vNIC Template.

**Figure 98.** Create vNIC Template for Internal Network
18. Create vNIC template for Storage Network

Figure 99. Create vNIC Template for Storage Access
19. Create vNIC template for Admin Network

**Figure 100.** Create vNIC Template for Admin Network
20. Create vNIC template for AppServer Network

**Figure 101.** Create vNIC template for AppServer Network
21. Create vNIC template for Backup Network

Figure 102. Create vNIC template for Backup Network
22. Create vNIC template for Client Network

Figure 103. Create vNIC template for Client Network
23. Create vNIC template for DataSource Network

**Figure 104.** Create vNIC template for DataSource Network
24. Create vNIC template for Replication Network

Figure 105. Create vNIC template for Replication Network
Create vNIC/vHBA Placement Policy

To create a vNIC/vHBA placement policy for the SAP HANA hosts, complete the following steps:

For Cisco UCS B260 and C460:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root > Sub-Organization > HANA.
3. Right-click vNIC/vHBA Placement Policies.
4. Select Create Placement Policy.
5. Enter HANA-B260 as the name of the placement policy.
6. Click 1 and select Assigned Only.
7. Click 2 and select Assigned Only.
8. Click OK, and then click OK again.
For Cisco UCS B460 with four VIC cards (2 x VIC 1240 and 2 x VIC 1280)

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root > Sub-Organization > HANA.
3. Right-click vNIC/vHBA Placement Policies.
4. Select Create Placement Policy.
5. Enter **HANA-B460** as the name of the placement policy.
6. Click 1 and select Assigned Only.
7. Click 2 and select Assigned Only.
8. Click 3 and select Assigned Only.
9. Click 4 and select Assigned Only.
10. Click OK, and then click OK again.
Create PXE Boot Policies
To create PXE boot policies, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root > Sub-Organization > HANA.
4. Select Create Boot Policy
5. Enter PXE-Boot as the name of the boot policy.
6. Optional: Enter a description for the boot policy.
7. Check the Reboot on Boot Order Change option.
8. Expand the Local Devices drop-down menu and select Add CD/DVD.
9. Expand the vNICs section and select Add LAN Boot
10. In the Add LAN Boot dialog box, enter HANA-Boot
11. Click OK.
12. Click OK.
13. Click OK to save the boot policy. Click OK to close the Boot Policy window.

Create Service Profile Templates Bare Metal SAP HANA Scale-Out
The LAN configurations and relevant SAP HANA policies must be defined prior to creating, a Service Profile Template. For Scale-Out solution, two Service Profile templates are created - the only difference between the two is the vCon placement to achieve maximum network throughput per blade.
The guidelines to use service profile for scale-out system to achieve maximum network throughput between servers with a SAP HANA system are outlined below.

SAP HANA-A is used for:
- Server 1 and Server 3 of a blade chassis for Cisco UCS B260 M4 Server.
- Server 3 for Cisco UCS B2460 M4 Server and Cisco UCS C460 M4 Server

SAP HANA-B is used for:
- Server 5 and Server 7 of a blade chassis for Cisco UCS B260 M4 Server.
- Server 7 for Cisco UCS B460 M4 Server

To create the service profile template, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root > Sub-Organization > HANA.
3. Right-click on HANA.
4. Select Create Service Profile Template (Expert) to open the Create Service Profile Template wizard.
5. Identify the service profile template:
   - Enter HANA-A as the name of the service profile template.
   - Select the Updating Template option.
   - Under UUID, select HANA-UUID as the UUID pool.
   - Click Next.

6. Configure the networking options:
   - Keep the default setting for Dynamic vNIC Connection Policy.
   - Select the Expert option to configure the LAN connectivity.
   - Click the upper Add button to add a vNIC to the template.
   - In the Create vNIC dialog box, enter HANA-Boot as the name of the vNIC.
   - Select the Use vNIC Template checkbox.
   - In the vNIC Template list, select HANA-Boot.
   - In the Adapter Policy list, select Linux-B460.
   - Click OK to add this vNIC to the template.
i. Repeat the above steps c-h for each vNIC

7. Add vNIC for HANA-Internal

Figure 112. Service Profile Template vNIC Internal

8. Add vNIC for HANA-Storage

Figure 113. Service Profile Template vNIC Storage
9. Add vNIC for HANA-Client

Figure 114. Service Profile Template vNIC Client

10. Add vNIC for HANA-AppServer

Figure 115. Service Profile Template vNIC AppServer

11. Add vNIC for HANA-DataSource
12. Add vNIC for HANA-Replication

13. Add vNIC for HANA-Backup
14. Add vNIC for HANA-Admin

15. Review the table in the Networking page to make sure that all vNICs were created.

16. Click Next.

17. Configure the storage options:
   a. No change required for local disk configuration policy
   b. Select the No vHBAs option for the “How would you like to configure SAN connectivity?” field.
c. Click Next.
18. Set no Zoning options and click Next
19. Set the vNIC/vHBA placement options.

20. For Cisco UCS B260 M4 and C460 M4 servers

a. In the "Select Placement" list, select the HANA-B260 placement policy.
b. Select vCon1 and assign the vNICs to the virtual network interfaces policy in the following order:
   1) HANA-Boot
   2) HANA-Internal
   3) HANA-Client
   4) HANA-DataSource
   5) HANA-Replication
c. Select vCon2 and assign the vNICs to the virtual network interfaces policy in the following order:
   1) HANA-Storage
   2) HANA-Backup
   3) HANA-AppServer
   4) HANA-Admin
d. Review the table to verify that all vNICs are assigned to the policy in the appropriate order.
e. Click Next.

21. For Cisco UCS B460 M4 Servers

   a. In the “Select Placement” list, select the HANA-B460 placement policy.
   
   b. Select vCon1 and assign the vNICs to the virtual network interfaces policy in the following order:
      1) HANA-Boot
      2) HANA-Internal
      3) HANA-Client

   c. Select vCon2 and assign the vNICs to the virtual network interfaces policy in the following order:
      1) HANA-Storage
      2) HANA-AppServer

   d. Select vCon3 and assign the vNICs to the virtual network interfaces policy in the following order:
      1) HANA-DataSource
      2) HANA-Replication
e. Select vCon4 and assign the vNICs to the virtual network interfaces policy in the following order:

1) HANA-Backup
2) HANA-Admin

<table>
<thead>
<tr>
<th>vNIC</th>
<th>Assigned Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>HANA-Backup</td>
<td>1</td>
</tr>
<tr>
<td>HANA-Admin</td>
<td>2</td>
</tr>
</tbody>
</table>

22. Review the table to verify that all vNICs are assigned to the policy in the appropriate order and click Next.
23. No Change required on the vMedia Policy, Click Next
24. Set the server boot order:
   a. Select PXE-Boot for Boot Policy.

Figure 122. Service Profile Template PXE Configuration

b. Click Next
25. Add a maintenance policy:
   a. Select the default Maintenance Policy.
   b. Click Next.
26. Specify the server assignment:
   a. In the Pool Assignment list, select HANA-1TB.
   b. Optional: Select a Server Pool Qualification policy HANA-1TB

**Note:** Choose the Pool Assignment as per the Server Pool policy created for each type of servers. In this example, choose Servers with 1TB of RAM.
   c. Select Down as the power state to be applied when the profile is associated with the server.
   d. Expand Firmware Management at the bottom of the page and select HANA-FW from the Host Firmware list.
   e. Click Next.
27. Add operational policies
   
   a. In the BIOS Policy list, select HANA-BIOS.
   
   b. Expand the External IPMI Management Configuration and select HANA-IPMI in the IPMI Access Profile. Select SoL-Console in the SoL Configuration Profile
   
   c. Expand Management IP Address, in the Outband IPv4 tap choose ext-mgmt in the Management IP Address Policy
   
28. Click Finish to create the service profile template
29. Click OK in the confirmation message
30. To meet the Network bandwidth requirement defined by SAP, create the second service profile template and modify the vNIC placement policy.

To create a clone service profile template created, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root > Sub-Organization > HANA.
3. Right-click on Service Template HANA-A
4. Select Create a Clone
5. Enter HANA-B for Clone name and Choose root as Org

6. Click OK to Create the clone of HANA-A
7. Click OK to confirm
8. On the cloned Service Profile Template Select HANA-B in the Navigation pane and click Network tab
9. Under Actions Click on Modify vNIC/vHBA Placement
For Cisco UCS B260 M4 Servers
1. In the “Select Placement” list, select the HANA-B260 placement policy.
2. Select vCon1 and assign the vNICs to the virtual network interfaces policy in the following order:
   1) HANA-Boot
   2) HANA-Storage
   3) HANA-Backup
   4) HANA-AppServer
   5) HANA-Admin

3. Select vCon2 and assign the vNICs to the virtual network interfaces policy in the following order
   1) HANA-Internal
   2) HANA-Client
   3) HANA-DataSource
   4) HANA-Replication

4. Click OK to complete the vNIC/vHBA Placement policy.
5. Click OK to confirm

For Cisco UCS B460 M4 Server
1. In the “Select Placement” list, select the HANA-B460 placement policy.
2. Select vCon1 and assign the vNICs to the virtual network interfaces policy in the following order:
   1) HANA-Boot
   2) HANA-Backup
   3) HANA-Admin
3. Select vCon2 and assign the vNICs to the virtual network interfaces policy in the following order:
   1) HANA-DataSource
2) HANA-Replication

4. Select vCon3 and assign the vNICs to the virtual network interfaces policy in the following order:
   1) HANA-Storage
   2) HANA-AppServer

3. Select vCon4 and assign the vNICs to the virtual network interfaces policy in the following order:
   1) HANA-Internal
   2) HANA-Client

4. Click OK to complete the vNIC/vHBA Placement policy.

5. Click OK to confirm

(Optional) Create IP Pool for Service Profiles

For SAP HANA High Availability configuration we would be using IPMI tool, for ease of management create a block of IP addresses for SAP HANA servers. In the Cisco UCS environment, complete the following steps:

Note: This block of IP addresses should be in the same subnet as the management IP addresses for the Cisco UCS Manager.

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Pools > root >> Sub-Organization > HANA > IP Pools Right Click Create a IP Pool
3. For the Name enter HANA-Server
4. For Assignment order select Sequential and Click Next
5. Click Add
6. Enter the starting IP address of the block and the number of IP addresses required, and the subnet and gateway information.
7. Click OK to create the IP block.
8. Click OK in the confirmation message.

Edit the Management IP for the Service Profile template created:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root > Sub-Organization > HANA Service Template HANA-A.
3. In the right pane Click on Change Management IP Address
4. In the Outband IPv4 tab under Management IP Address Policy Select HANA-Server
5. Click OK to change the Management IP
6. Repeat the above steps for Service Template HANA-B

Create Service Profile from the Template

To create service profiles from the service profile template, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root > Sub-Organization > HANA > Service Template HANA-A.
3. Right-click Service Template HANA-A and select Create Service Profiles from Template
4. Enter HANA-Server0 as the service profile prefix.
5. Enter 1 as “Name Suffix Starting Number”
6. Enter 1 as the “Number of Instances”.
7. Click OK to create the service profile.
To create service profiles from the service profile template HANA-B, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root > Sub-Organization > HANA > Service Template HANA-B.
3. Right-click Service Template HANA-B and select Create Service Profiles from Template.
4. Enter HANA-Server0 as the service profile prefix.
5. Enter 2 as “Name Suffix Starting Number”
6. Enter 1 as the “Number of Instances”.
7. Click OK to create the service profile.

**Note:** As soon as the specified number of Service Profiles are created, profiles will associate with a blade if physically available.

![Create Service Profiles From Template](image)

As mentioned previously, the Service Profiles are created in order to distribute network bandwidth across Fabric A and Fabric B. The vNIC is placed so that more than 9.5 Gbps is achieved between node-to-node server communication.

- For Cisco UCS B460 M4 Servers use the service profile template HANA-A for servers in slot 3 and service profile template HANA-B for servers in slot 7.
- For Cisco UCS B260 M4 Servers use service profile template HANA-A for servers in slot 1 and 3 and service profile template HANA-B for servers in slot 5 and 7.
For Cisco UCS C460 M4 Server either of the service profile templates HANA-A or service profile template HANA-B with vCon placement can be used.

To associate service profile created for a specific slot, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile > root > Sub-Organization > HANA > HANA-Server01.
3. Right-click HANA-Server01 and select Change Service Profile Association.
4. For Server Assignment Choose Select existing Server for the drop down.
5. Click on the button All Servers.
6. Select the Server as recommended.

Create Service Profile Templates Bare Metal SAP HANA Scale-Up

To create the service profile template for SAP HANA Scale-Up, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root > Sub-Organization > HANA.
3. Right-click HANA.
4. Select Create Service Profile Template to open the Create Service Profile Template wizard.
5. Identify the service profile template
   a. Enter HANA-Scale-UP as the name of the service profile template.
   b. Select the Updating Template option.
   c. Under UUID, select HANA-UUID as the UUID pool.
   d. Click Next.
6. Configure the networking options:
   a. Keep the default setting for Dynamic vNIC Connection Policy.
   b. Select the Expert option to configure the LAN connectivity.
   c. Click the upper Add button to add a vNIC to the template.
   d. In the Create vNIC dialog box, enter HANA-Boot as the name of the vNIC.
   e. Select the Use vNIC Template checkbox.
   f. In the vNIC Template list, select HANA-Boot.
   g. In the Adapter Policy list, select Linux-B460.
   h. Click OK to add this vNIC to the template.
   i. Repeat steps c-h for each vNIC.
j. Add vNIC for HANA-Storage
k. Add vNIC for HANA-Client
l. Add vNIC for HANA-AppServer
m. Add vNIC for HANA-DataSource
n. Add vNIC for HANA-Replication
o. Add vNIC for HANA-Backup
p. Add vNIC for HANA-Admin
q. Review the table in the Networking page to make sure that all vNICs were created.
r. Click Next.

Note: Even though we define eight Networks, there are optional and if they are not needed in the
customer deployment, addition of vNIC template for such optional network is not required.

7. Configure the storage options:
   a. No change required for local disk configuration policy
   b. Select the No vHBAs option for the “How would you like to configure SAN connectivity?” field
c. Click Next.

8. Set no Zoning options and click Next

9. Set the vNIC/vHBA placement options

10. For Cisco UCS B200 M4 Server / Cisco UCS C240 M4 Server / Cisco UCS B240 M4 Server with one
    VIC cards:
    a. In the "Select Placement" list, select the Specify Manually
    b. Select vCon1 and assign the vNICs to the virtual network interfaces policy in the following order:
       1) HANA-Boot
       2) HANA-Client
       3) HANA-Storage
       4) HANA-Backup
       5) HANA-AppServer
       6) HANA-DataSource
       7) HANA-Replication
       8) HANA-Admin
c. Review the table to verify that all vNICs were assigned to the policy in the appropriate order.
d. Click Next.

11. For Cisco UCS B260 M4 / Cisco UCS B460 M4 Servers with two VIC cards
    a. In the "Select Placement" list, select the HANA-B260 placement policy.
b. Select vCon1 and assign the vNICs to the virtual network interfaces policy in the following order:
   1) HANA-Boot
   2) HANA-Client
   3) HANA-DataSource
   4) HANA-Replication
c. Select vCon2 and assign the vNICs to the virtual network interfaces policy in the following order
   1) HANA-Storage
   2) HANA-Backup
   3) HANA-AppServer
   4) HANA-Admin
e. Review the table to verify that all vNICs were assigned to the policy in the appropriate order.
f. Click Next.

12. For Cisco UCS B460 M4 Servers with four VIC cards
   a. In the “Select Placement” list, select the HANA-B460 placement policy.
   b. Select vCon1 and assign the vNICs to the virtual network interfaces policy in the following order:
      1) HANA-Boot
         2) HANA-Client
   c. Select vCon2 and assign the vNICs to the virtual network interfaces policy in the following order
      1) HANA-Storage
         2) HANA-AppServer
   d. Select vCon3 and assign the vNICs to the virtual network interfaces policy in the following order
      1) HANA-DataSource
         2) HANA-Replication
   e. Select vCon4 and assign the vNICs to the virtual network interfaces policy in the following order
      1) HANA-Backup
         2) HANA-Admin
   f. Review the table to verify that all vNICs were assigned to the policy in the appropriate order and click Next.

13. No Change required on the vMedia Policy, Click Next

14. Set the server boot order: Select PXE-Boot for Boot Policy.

**Figure 128.** Service Profile Template PXE Configuration

15. Click Next

16. Add a maintenance policy:
   a. Select the default Maintenance Policy.
   b. Click Next.

17. Specify the server assignment:
   a. In the Pool Assignment list, select the appropriated pool created for scale-up servers
b. Optional: Select a Server Pool Qualification policy

c. Select Down as the power state to be applied when the profile is associated with the server.

d. Expand Firmware Management at the bottom of the page and select HANA-FW from the Host Firmware list.

e. Click Next.

18. Add operational policies

a. In the BIOS Policy list, select HANA-BIOS.

b. Leave External IPMI Management Configuration as <not set> in the IPMI Access Profile. Select SoL-Console in the SoL Configuration Profile

c. Expand Management IP Address, in the Outband IPv4 tap choose ext-mgmt in the Management IP Address Policy


19. Click Finish to create the service profile template

20. Click OK in the confirmation message

Create Service Profiles
To create service profiles from the service profile template, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root > Sub-Organization > HANA > Service Template HANA-Scale-UP
3. Right-click HANA-Scale-UP and select Create Service Profiles from Template
4. Enter appropriate name for the service profile prefix.
5. Enter 1 as “Name Suffix Starting Number”
6. Enter appropriate number of service profile to be created in the “Number of Instances”.
7. Click OK to create the service profile.

Service Profile for Virtualized SAP HANA (vHANA)
Hosts
The Service Profile is created for virtualized SAP HANA which can be used for Cisco UCS B200 M4 Server, Cisco UCS B260 M4 Server, Cisco UCS C220 M4 Server, Cisco UCS C240 M4 Server, Cisco UCS C460 M4 Server and Cisco UCS B460 M4 Server with iSCSI boot for ESXi.

These Service Profiles created for vHANA can used for virtualized environment for SAP Application Servers.

Create New Organization
To create organization unit, complete the following steps:

1. In Cisco UCS Manager, on the Tool bar click on New
2. From the drop down menu select Create Organization
3. Enter the Name as vHANA
4. Optional Enter the Description as Org for Virtual HANA
5. Click OK to create the Organization

Create Additional Port-Channel for SAP vHANA
Create a separate Network Uplink for SAP vHANA, to have a dedicated bandwidth for virtualization environment. The virtualization environment can also be used for application servers connecting to SAP HANA are in the same Cisco UCS domain.
Complete the following steps to create port-channel for vHANA:
1. In Cisco UCS Manager, click the LAN tab in the navigation pane
2. Under LAN > LAN Cloud, expand the Fabric A tree.
3. Right-click Port Channels.
4. Select Create Port Channel
5. Enter 31 as the unique ID of the port channel.
6. Enter vPC-31-vHANA as the name of the port channel.
7. Click Next.
8. Select the following ports to be added to the port channel:
   - Slot ID 1 and port 13
   - Slot ID 1 and port 15
9. Click >> to add the ports to the port channel.
10. Click Finish to create the port channel.
11. Click OK.
12. In the navigation pane, under LAN > LAN Cloud, expand the Fabric B tree.
13. Right-click Port Channels.
14. Select Create Port Channel.
15. Enter 32 as the unique ID of the port channel.
16. Enter vPC-32-vHANA as the name of the port channel.
17. Click Next.
18. Select the following ports to be added to the port channel:
   - Slot ID 1 and port 13
   - Slot ID 1 and port 15
19. Click >> to add the ports to the port channel.
20. Click Finish to create the port channel.
21. Click OK.

Create IQN Pools for iSCSI Boot
To configure the necessary IQN pools for the Cisco UCS environment, complete the following steps.

1. In the Cisco UCS Manager, Select the SAN tab on the left.
2. Select Pools > root > Sub-Organization > vHANA
3. Right-click IQN Pools under the vHANA sub-organization.
4. Select Create IQN Suffix Pool to create the IQN pool.
5. Enter IQN_Pool for the name of the IQN pool.
6. Optional: Enter a description for the IQN pool.
7. Enter `iqn.1992-08.com.cisco` as the prefix
8. Select Sequential for Assignment Order.
9. Click Next.
10. Click Add.
11. Enter `ucs-host` as the suffix.
12. Enter 1 in the From field.
13. Specify a size of the IQN block sufficient to support the available server resources.
14. Click OK.
15. Click Finish.
16. In the message box that displays, click OK.

**Create IP Pools for iSCSI Boot**
These steps provide details for configuring the necessary IP pools iSCSI boot for the Cisco UCS environment.

1. In the Cisco UCS Manager, Select the LAN tab on the left.
2. Select Pools > root > Sub-Organization > vHANA

**Note:** Two IP pools are created, one for each switching fabric.

3. Right-click IP Pools under the vHANA sub-organization.
4. Select Create IP Pool to create the IP pool.
5. Enter iSCSI_IP_Pool_A for the name of the IP pool.
6. Optional: Enter a description of the IQN pool.
7. Select Sequential for Assignment Order.
8. Click Next.
9. Click Add.
10. In the From field, enter the beginning of the range to assign as iSCSI IP addresses.
11. Set the size to enough addresses to accommodate the servers.
12. Click OK.
13. Click Finish.
14. Right-click IP Pools under the root organization.
15. Select Create IP Pool to create the IP pool.
16. Enter iSCSI_IP_Pool_B for the name of the IP pool.
17. Optional: Enter a description of the IQN pool.
18. Select Sequential for Assignment Order.
19. Click Next.
20. Click Add.
21. In the From field, enter the beginning of the range to assign as iSCSI IP addresses.
22. Set the size to enough addresses to accommodate the servers.
23. Click OK.
24. Click Finish.
Create VLANs
To configure the necessary VLANs for the virtualized environment, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.

   **Note:** In this procedure, Eight VLANs are created.

2. Select LAN > LAN Cloud.
3. Right-click VLANs.
4. Select Create VLANs (Figure 131).
5. Enter ESX-MGMT as the name of the VLAN to be used for management traffic.
6. Keep the Common/Global option selected for the scope of the VLAN.
7. Enter <<var_vhana_esx_mgmt_vlan_id>> as the ID of the management VLAN.
8. Keep the Sharing Type as None.
9. Click OK, and then click OK again.

   **Figure 131.** Cisco UCS Manager - Create Management VLAN.

10. Right-click VLANs.
11. Select Create VLANs.
12. Enter ESX-NFS as the name of the VLAN to be used for NFS.
13. Keep the Common/Global option selected for the scope of the VLAN.
14. Enter the `<<var_vhana_esx_nfs_vlan_id>>` for the NFS VLAN.
15. Keep the Sharing Type as None.
16. Click OK, and then click OK again.

**Figure 132.** Cisco UCS Manager - Create NFS VLAN

17. Right-click VLANs.
18. Select Create VLANs.
19. Enter ESX-vMotion as the name of the VLAN to be used for vMotion.
20. Keep the Common/Global option selected for the scope of the VLAN.
21. Enter the `<<var_vhana_esx_vmotion_vlan_id>>` as the ID of the vMotion VLAN.
22. Keep the Sharing Type as None.
23. Click OK, and then click OK again.

**Figure 133.** Cisco UCS Manager - Create vMotion VLAN

24. Right-click VLANs.
25. Select Create VLANS.
26. Enter vHANA-Access as the name of the VLAN to be used to Access vHANA
27. Keep the Common/Global option selected for the scope of the VLAN.
28. Enter the <<var_vhana_access_vlan_id>> as the ID of the vHANA-Access VLAN.
29. Keep the Sharing Type as None.
30. Click OK, and then click OK again

**Figure 134.** Cisco UCS Manager- Create vHANA-Access VLAN

31. Right-click VLANS.
32. Select Create VLANS.
33. Enter vHANA-Storage as the name of the VLAN to be used for Data and Log Access for HANA.
34. Keep the Common/Global option selected for the scope of the VLAN.
35. Enter the <<var_vhana_storage_vlan_id>> as the ID of the vHANA-Storage VLAN.
36. Keep the Sharing Type as None.
37. Click OK, and then click OK again

**Figure 135.** Cisco UCS Manager - Create vHANA-Storage VLAN

38. Right-click VLANS.
39. Select Create VLANs.
40. Enter iSCSI-A as the name of the VLAN to be used for the first iSCSI VLAN.
41. Keep the Common/Global option selected for the scope of the VLAN.
42. Enter the VLAN ID for the first iSCSI VLAN.
43. Click OK, then OK.

**Figure 136.** Cisco UCS Manager - Create iSCSI-A VLAN

44. Right-click VLANs.
45. Select Create VLANs.
46. Enter iSCSI-B-VLAN as the name of the VLAN to be used for the second iSCSI VLAN.
47. Keep the Common/Global option selected for the scope of the VLAN.
48. Enter the VLAN ID for the second iSCSI VLAN.
49. Click OK, then OK.
Create VLAN Group for vHANA
1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select LAN > LAN Cloud.
3. Right-click VLAN Groups
4. Select Create VLAN Groups
5. Enter vHANA-Zone as the name of the VLAN Group
6. Select ESX-MGMT, ESX-vMotion, ESX-NFS, vHANA-Access, vHANA-Storage, iSCSI-A and iSCSI-B
7. Click Next
8. Click Next on Add Uplink Ports
9. Choose Port-Channels Create for vHANA vPC-31-vHANA and vPC-32-vHANA
10. Click Finish

Create vNIC Templates
To create multiple virtual network interface card (vNIC) templates for the Cisco UCS environment, complete the following steps:
1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Policies > root > Sub-Organization > vHANA
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter vNIC_Template_A as the vNIC template name.
7. Do not select the Enable Failover checkbox.
8. Under Target, make sure that the VM checkbox is not selected.
9. Select Updating Template as the Template Type.
10. Under VLANS, select the checkboxes for ESX-MGMT, ESX-NFS, ESX-vMotion
11. For MTU, enter 9000.
12. In the MAC Pool list, select MAC_Pool_A.
13. Click OK to create the vNIC template.
14. Click OK.

15. In the navigation pane, select the LAN tab.
17. Right-click vNIC Templates.
18. Select Create vNIC Template.
19. Enter `vNIC_Template_B` as the vNIC template name.
20. Select Fabric B.
21. Do not select the Enable Failover checkbox.
22. Under Target, make sure the VM checkbox is not selected.
23. Select Updating Template as the template type.
24. Under VLANs, select the checkboxes for ESX-MGMT, ESX-NFS, ESX-vMotion.
25. For MTU, enter 9000.
26. In the MAC Pool list, select `MAC_Pool_B`.
27. Click OK to create the vNIC template.
28. Click OK.
29. Select the LAN tab on the left.
30. Select Policies > root.
31. Right-click vNIC Templates.
32. Select Create vNIC Template.
33. Enter iSCSI_Template_A as the vNIC template name.
34. Leave Fabric A selected.
35. Do not select the Enable Failover checkbox.
36. Under Target, make sure that the VM checkbox is not selected.
37. Select Updating Template for Template Type.
38. Under VLANs, select iSCSI-A-VLAN. Set iSCSI-A-VLAN as the native VLAN.
39. Under MTU, enter 1500.
40. From the MAC Pool list, select MAC_Pool_A.
41. Click OK to complete creating the vNIC template.
42. Click OK.
43. Select the LAN tab on the left.
44. Select Policies > root.
45. Right-click vNIC Templates.
46. Select Create vNIC Template.
47. Enter iSCSI_Template_B as the vNIC template name.
48. Select Fabric B.
49. Do not select the Enable Failover checkbox.
50. Under Target, make sure that the VM checkbox is not selected.
51. Select Updating Template for Template Type.
52. Under VLANs, select iSCSI-B-VLAN. Set iSCSI-B-VLAN as the native VLAN.
53. Under MTU, enter 1500.
54. From the MAC Pool list, select MAC_Pool_B.
55. Click OK to complete creating the vNIC template.
Additional vNIC templates are created for each vHANA system to separate the traffic between ESX management and vHANA VMs. These vNICs are used for vHANA system storage access, client access and access for application server.

To create additional vNIC templates, complete the following steps:

1. In Cisco UCS Manager, click the LAN tab in the navigation pane.
2. Select Policies > root > Sub-Organization > vHANA
3. Right-click vNIC Templates.
4. Select Create vNIC Template.
5. Enter vNIC_vhana2_A as the vNIC template name.
7. Do not select the Enable Failover checkbox.
8. Under Target, make sure that the VM checkbox is not selected.
9. Select Updating Template as the Template Type.
10. Under VLANs, select the checkboxes for vHANA-Storage and vHANA-Access.
11. For MTU, enter 9000.
12. In the MAC Pool list, select MAC_Pool_A.
13. Click OK to create the vNIC template.
14. Click OK.
15. In the navigation pane, select the LAN tab.
17. Right-click vNIC Templates.
18. Select Create vNIC Template
19. Enter vNIC_vHANA2_B as the vNIC template name.
20. Select Fabric B.
21. Do not select the Enable Failover checkbox.
22. Under Target, make sure the VM checkbox is not selected.
23. Select Updating Template as the template type.
24. Under VLANs, select the checkboxes for vHANA-Storage and vHANA-Access
25. For MTU, enter 9000.
26. In the MAC Pool list, select MAC_Pool_B.
27. Click OK to create the vNIC template.
28. Click OK.

Create Boot Policies

This procedure applies to a Cisco UCS environment in which two iSCSI logical interfaces (LIFs) are on cluster node 1 (iscsi lif01a and iscsi lif01b) and two iSCSI LIFs are on cluster node 2 (iscsi lif02a and iscsi lif02b).

One boot policy is configured in this procedure. This policy configures the primary target to be iscsi_lif01a.

To create boot policies for the Cisco UCS environment, complete the following steps:
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root > Sub-Organization > vHANA
4. Select Create Boot Policy.
5. Enter Boot-Fabric-A as the name of the boot policy.
6. Optional: Enter a description for the boot policy.
7. Keep the Reboot on Boot Order Change option cleared.
8. Expand the Local Devices drop-down menu and select Add CD-ROM.
9. Expand the iSCSI vNICs section and select Add iSCSI Boot.
10. In the Add iSCSI Boot dialog box, enter iSCSI_A-vNIC.
11. Click OK.
12. Select Add iSCSI Boot.
13. In the Add iSCSI Boot dialog box, enter iSCSI_B-vNIC.
14. Click OK.
15. Click OK to save the boot policy. Click OK to close the Boot Policy window.
Create BIOS Policies
To create a server BIOS policy for the Cisco UCS environment, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Policies > root > Sub-Organization > vHANA
4. Select Create BIOS Policy
5. Enter vHANA-Host as the BIOS policy name.
6. Change the Quiet Boot setting to Disabled.
7. Click Next
8. Select Hyper Threading enabled
9. Select Virtualization Technology (VT) enabled
10. Click Finish to create the BIOS policy.

Create Service Profile Templates
To create the service profile template, complete the following steps:
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root > Sub-Organization > vHANA
3. Right-click vHANA
4. Select Create Service Profile Template to open the Create Service Profile Template wizard.
5. Identify the service profile template:
a. Enter vHANA-Host as the name of the service profile template.
b. Select the Updating Template option.
c. Under UUID, select HANA_UUID as the UUID pool.
d. Click Next.

Figure 143. Cisco UCS Manager - Service Profile Template - UUID Assignment

6. Configure the networking options:
   1) Keep the default setting for Dynamic vNIC Connection Policy.
   2) Select the Expert option to configure the LAN connectivity.
   3) Click the upper Add button to add a vNIC to the template.
   4) In the Create vNIC dialog box, enter vNIC-A as the name of the vNIC.
   5) Select the Use vNIC Template checkbox.
   6) In the vNIC Template list, select vNIC_Template_A.
   7) In the Adapter Policy list, select VMWare.
   8) Click OK to add this vNIC to the template.
9) On the Networking page of the wizard, click the upper Add button to add another vNIC to the template.

10) In the Create vNIC box, enter vNIC-B as the name of the vNIC.

11) Select the Use vNIC Template checkbox.

12) In the vNIC Template list, select vNIC_Template_B.

13) In the Adapter Policy list, select VMWare.

14) Click OK to add the vNIC to the template.
Figure 145. Cisco UCS Manager – Service Profile Template - Fabric A and B vNICs

Note: If additional vNIC templates are created to separate the traffic between SAP vHANA VMs, repeat the above steps 3-14 to add 2 more vNICs

Figure 146. Cisco UCS Manager - Service Profile Template - vHANA Host Networking
15) Click the upper Add button to add a vNIC to the template.
16) In the Create vNIC dialog box, enter iSCSI-A-vNIC as the name of the vNIC.
17) Select the Use vNIC Template checkbox.
18) In the vNIC Template list, select iSCSI_Template_A.
19) In the Adapter Policy list, select VMware.
20) Click OK to add this vNIC to the template.

**Figure 147.** Cisco UCS Manager - Service Profile Template – iSCSI-A vNIC

21) Click the upper Add button to add a vNIC to the template.
22) In the Create vNIC dialog box, enter iSCSI-B-vNIC as the name of the vNIC.
23) Select the Use vNIC Template checkbox.
24) In the vNIC Template list, select iSCSI_Template_B.
25) In the Adapter Policy list, select VMware.
26) Click the lower Add button in the iSCSI vNIC section to define a vNIC.
27) Enter iSCSI-A-vNIC as the name of the vNIC.
28) Select iSCSI-A-vNIC for Overlay vNIC.
29) Set the iSCSI Adapter Policy to default.
30) Set the VLAN to iSCSI-A-VLAN.
31) Leave the MAC Address set to None.
32) Click OK.
33) Expand the “iSCSI vNICs” section
34) Select “iqn-pool” under “Initiator Name Assignment”
35) Click the lower Add button in the iSCSI vNIC section to define a vNIC.
36) Enter iSCSI-B-vNIC as the name of the vNIC.
37) Set the Overlay vNIC to iSCSI-B-vNIC
38) Set the iSCSI Adapter Policy to default.
39) Set the VLAN to iSCSI-B-VLAN
40) Leave the MAC Address set to None.
41) Click OK.
42) Click OK.
43) Review the table in the Networking page to make sure that all vNICs were created.
44) Click Next.
7. Configure the storage options:
   a. Select a local disk configuration policy:
      i. If the server in question has local disks, select default in the Local Storage list.
      ii. If the server in question does not have local disks, select No-Local.
   b. Select the No vHBAs option for the “How would you like to configure SAN connectivity?” field.
   c. Click Next.
8. Set no Zoning options and click Next.
9. Set the vNIC/vHBA placement options.
10. For Cisco UCS B260 M4 Server, Cisco UCS B460 M4 Server and Cisco UCS C460 M4 Server with two or more VIC adapters:
   a. In the “Select Placement” list, select the Specify Manually placement policy.
   b. Select vCon1 and assign the vHBAs/vNICs to the virtual network interfaces policy in the following order:
      1) iSCSI-vNIC-A
      2) iSCSI-vNIC-B
      3) vNIC-A
      4) vNIC-B
c. Select vCon2 and assign the vHBAs/vNICs to the virtual network interfaces policy in the following order:
      1) vNIC-vHANA2-A
      2) vNIC-vHANA2-B
d. Review the table to verify that all vNICs and vHBAs were assigned to the policy in the appropriate order.
e. Click Next.
11. For SAP vHANA Hosts Cisco UCS B200 M4 Server, Cisco UCS C220 M4 Server and Cisco UCS C240 M4 Server with single VIC Card:
   a. In the “Select Placement” list, select the Specify Manually placement policy.
   b. Select vCon1 and assign the vHBAs/vNICs to the virtual network interfaces policy in the following order:
      1) iSCSI-vNIC-A
      2) iSCSI-vNIC-B
      3) vNIC-A
      4) vNIC-B
      5) vNIC-vHANA2-A
      6) vNIC-vHANA2-B
   c. Review the table to verify that all vNICs and vHBAs were assigned to the policy in the appropriate order.
   d. Click Next.
12. Click Next on vMedia Policy
13. Set the server boot order:

   1) Select Boot-Fabric-A for Boot Policy.
   2) In the Boot Order pane, select iSCSI-A-vNIC.
   3) Click the “Set iSCSI Boot Parameters” button.
   4) Leave the “Set iSCSI Boot Parameters” dialog box <not set> to use the single Service Profile Initiator Name defined in the previous steps.
   5) Set iSCSI_IP_Pool_A as the “Initiator IP address Policy”.
   6) Keep the “iSCSI Static Target Interface” button selected and click the + button.
   7) Log in to the storage cluster management interface and run the following command:

```
iscsi nodename
```

8) Note or copy the iSCSI target name for infra_vs1.
9) In the Create iSCSI Static Target dialog box, paste the iSCSI target node name from infra_vs1 into the iSCSI Target Name field.
10) Enter the IP address of iSCSI_lif02a for the IPv4 Address field.
11) Click OK to add the iSCSI static target.
12) Keep the iSCSI Static Target Interface option selected and click the button.
13) In the Create iSCSI Static Target window paste the iSCSI target node name from infra_vs1 into the iSCSI Target Name field.
14) Enter the IP address of iscsi_lif01a in the IPv4 Address field.
15) Click OK.
16) Click OK.

17) In the Boot Order pane, select iSCSI-vNIC-B.

18) Click the Set iSCSI Boot Parameters button.

19) In the Set iSCSI Boot Parameters dialog box, set the Initiator Name Assignment to <not set>.

20) In the Set iSCSI Boot Parameters dialog box, set the initiator IP address policy to iSCSI_IP_Pool_B.

21) Keep the iSCSI Static Target Interface option selected and click the + button.

22) In the Create iSCSI Static Target window, paste the iSCSI target node name from infra_vs1 into the iSCSI Target Name field (same target name as above).

23) Enter the IP address of iscsi_lif02b in the IPv4 address field.
24) Click OK to add the iSCSI static target.

25) Keep the iSCSI Static Target Interface option selected and click the button.

26) In the Create iSCSI Static Target dialog box, paste the iSCSI target node name from infra_vs1 into the iSCSI Target Name field.

27) Enter the IP address of iscsi_lif01b in the IPv4 Address field.

28) Click OK.
29) Click OK.

30) Review the table to make sure that all boot devices were created and identified. Verify that the boot devices are in the correct boot sequence.

31) Click Next to continue to the next section.

14. Add a maintenance policy:
   a. Select the default Maintenance Policy.
   b. Click Next.

15. Specify the server assignment:
   a. In the Pool Assignment list, select an appropriate server pool.
   b. Optional: Select a Server Pool Qualification policy.
   c. Select Down as the power state to be applied when the profile is associated with the server.
d. Expand Firmware Management at the bottom of the page and select HANA-FW from the Host Firmware list.
e. Click Next.

16. Add operational policies:
   a. In the BIOS Policy list, select vHANA-Host.

**Figure 159. Cisco UCS Manager - Service Profile – Operational Policies**

17. Click Finish to create the service profile template.
18. Click OK in the confirmation message.

**Create Service Profiles**

To create service profiles from the service profile template, complete the following steps:

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root > Sub-Organization > vHANA > Service Template vHANA-Host.
3. Right-click vHANA-Host and select Create Service Profiles from the template.
4. Enter vHANA-Host-0 as the service profile prefix.
5. Enter 1 as “Name Suffix Starting Number”
6. Enter 1 as the “Number of Instances”.
7. Click OK to create the service profile.
Storage Configuration

This section describes the configuration for NetApp FAS 8040 HA pair used in the FlexPod Datacenter Solution for SAP HANA.

Note: For configurations with a different number of SAP HANA nodes or different NetApp FAS storage systems follow the guidelines described in TR-4290 SAP HANA on NetApp FAS Systems with NFS Configuration Guide

Controller NetApp FAS80xx Series

The site requirement prerequisites are listed in the table below

Table 20. NetApp FAS80XX Controller Series Prerequisites

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Reference</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical site where storage system needs to be installed must be ready</td>
<td>Site Requirements Guide</td>
<td>Refer to the “Site Preparation” section.</td>
</tr>
<tr>
<td>Storage system connectivity requirements</td>
<td>Site Requirements Guide</td>
<td>Refer to the “System Connectivity Requirements” section.</td>
</tr>
<tr>
<td>Storage system general power requirements</td>
<td>Site Requirements Guide</td>
<td>Refer to the “Circuit Breaker, Power Outlet Balancing, System Cabinet Power Cord Plugs, and Console Pinout Requirements” section.</td>
</tr>
<tr>
<td>Storage system model-specific requirements</td>
<td>Site Requirements Guide</td>
<td>Refer to the “FAS80xx Series Systems” section.</td>
</tr>
</tbody>
</table>

Hardware and software component versions and compatibility information for NetApp FAS controllers and NetApp DATA ONTAP operating system are provided in NetApp System Configuration Guides at the NetApp Support site.

Physical installation procedures for the NetApp FAS80xx controllers can be found at: FAS80xx documentation at the NetApp Support site.

Disk Shelves DS2246 Series

Each SAS stack configured with dual port HA cabling supports two disk shelves. This solution uses two SAS stacks i.e., 4 NetApp DS2246 disk shelves. The disks within each stack must be distributed equally to both controllers of the HA pair.

Cisco NX5596 Cluster Network Switch Configuration

Table 21. Cisco Nexus 5596 Cluster Network Switch Configuration Prerequisites

Description

- Rack and connect power to the new Cisco Nexus 5596 switches
- Provide a terminal session that connects to the switch's serial console port (9600, 8, n, 1)
- Connect the mgmt0 port to the management network and be prepared to provide IP address information
- Obtain password for admin
Initial Setup of Cisco Nexus 5596 Cluster Interconnect

The first time a Cisco Nexus 5596 cluster interconnect is accessed, it runs a setup program that prompts the user to enter an IP address and other configuration information needed for the switch to communicate over the management Ethernet interface. This information is required to configure and manage the switch. If the configuration must be changed later, the setup wizard can be accessed again by running the `setup` command in EXEC mode.

To set up the Cisco Nexus 5596 cluster interconnect, complete the following steps. These steps will need to be completed on both cluster interconnects.

1. Provide applicable responses to the setup prompts displayed on the Cisco Nexus 5596 cluster interconnect.

   Do you want to enforce secure password standard (yes/no): yes
   Enter the password for the "admin": <password>
   Confirm the password for "admin": <password>
   Would you like to enter the basic configuration dialog (yes/no): yes
   Create another login account (yes/no) [n]: Enter
   Configure read-only SNMP community string (yes/no) [n]: Enter
   Configure read-write SNMP community string (yes/no) [n]: Enter
   Enter the switch name: <switchname>
   Continue with out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter
   Mgmt0 IPv4 address: <ic_mgmt0_ip>
   Mgmt0 IPv4 netmask: <ic_mgmt0_netmask>
   Configure the default gateway? (yes/no) [y]: Enter
   IPv4 address of the default gateway: <ic_mgmt0_gw>
   Enable the telnet service? (yes/no) [n]: Enter
   Enable the ssh service? (yes/no) [y]: Enter
   Type of ssh key you would like to generate (dsa/rsa): rsa
   Number of key bits <768–2048>: 1024
   Configure the ntp server? (yes/no) [n]: y
   NTP server IPv4 address: <ntp_server_ip>
   Enter basic FC configurations (yes/no) [n]: Enter

2. At the end of the setup, the configuration choices are displayed. Verify the information and save the configuration at this time.

   Would you like to edit the configuration? (yes/no) [n]: <n>
   Use this configuration and save it? (yes/no) [y]: <y>

Download and Install NetApp Cluster Switch Software

When the Cisco Nexus 5596 is used as a cluster network switch with NetApp Data ONTAP 8.2.2, it should be running NX-OS version 5.2(1)N1(1).

Note: The `show version` command from the switch command line interface will show the switch version currently running on the switch. If it is different from NX-OS version 5.2(1)N1(1), go to the NetApp Support site and download and install NX-OS 5.2(1)N1(1) for the Cisco Nexus 5596 switch.
Download and Merge of NetApp Cluster Switch Reference Configuration File

Cluster network and management network switches are shipped without the configuration files installed. These files must be downloaded to the switches during deployment. Configuration files must be downloaded when the cluster network and management network switches are first installed or after the Cisco switch software is updated or reinstalled.

After the initial setup is complete, the NetApp cluster network switch reference configuration must be transferred to the switch and merged with the existing configuration. Instructions for this task and the reference configuration files for the appropriate switches are available on the NetApp Support site.

To download configuration files to a host and install them on a Cisco Nexus 5596 switch, complete the following steps on both cluster interconnects:

1. Obtain a console connection to the switch. Verify the existing configuration on the switch by running the `show run` command.
2. Log in to the switch. Make sure that the host recognizes the switch on the network (for example, use the `ping` utility).
3. Enter the following command:
   ```text
   copy <transfer protocol>: bootflash: vrf management
   ```
4. Verify that the configuration file is downloaded.
5. Merge the configuration file into the existing `running-config`. Run the following command, where `<config file name>` is the file name for the switch type. A series of warnings regarding PortFast is displayed as each port is configured.
   ```text
   copy <config file name> running-config
   ```
6. Verify the success of the configuration merge by running the `show run` command and comparing its output to the contents of the configuration file (a `.txt` file) that was downloaded.
   a. The output for both installed-base switches and new switches should be identical to the contents of the configuration file for the following items:
      - `banner` (should match the expected version)
      - Switch port descriptions such as `description Cluster Node x`
      - The new ISL algorithm `port-channel load-balance Ethernet source-dest-port`
   b. The output for new switches should be identical to the contents of the configuration file for the following items:
      - Port channel
      - Policy map
      - System QoS
      - Interface
      - Boot
   c. The output for installed-base switches should have the flow control receive and send values on for the following items:
      - Interface port-channel 1 and 2
      - Ethernet interface 1/41 through Ethernet interface 1/48.
7. Copy the `running-config` to the `startup-config`.
   ```text
   copy running-config startup-config
   ```
Cisco Smart Call Home Setup
To configure Smart Call Home on a Cisco Nexus 5596 switch, complete the following steps:

1. Enter the mandatory system contact using the `snmp-server contact` command in global configuration mode. Then run the `callhome` command to enter callhome configuration mode.

   NX-5596# config t
   NX-5596(config)# snmp-server contact <sys-contact>
   NX-5596(config)# callhome

2. Configure the mandatory contact information (phone number, e-mail address, and street address).

   NX-5596(config-callhome)# email-contact <email-address>
   NX-5596(config-callhome)# phone-contact <+1-000-000-0000>
   NX-5596(config-callhome)# street-address <a-street-address>

3. Configure the mandatory e-mail server information. The server address is an IPv4 address, IPv6 address, or the domain-name of a SMTP server to which Call Home will send e-mail messages. Optional port number (default=25) and VRF may be configured.

   NX-5596(config-callhome)# transport email smtp-server <ip-address> port 25 use-vrf <vrf-name>

4. Set the destination profile CiscoTAC-1 e-mail address to `callhome@cisco.com`

   NX-5596(config-callhome)# destination-profile CiscoTAC-1 email-addr callhome@cisco.com vrf management

5. Enable periodic inventory and set the interval.

   NX-5596(config-callhome)# periodic-inventory notification
   NX-5596(config-callhome)# periodic-inventory notification interval 30

6. Enable callhome, exit, and save the configuration.

   NX-5596(config-callhome)# enable
   NX-5596(config-callhome)# end
   NX-5596# copy running-config startup-config

7. Send a callhome inventory message to start the registration process.

   NX-5596# callhome test inventory
   trying to send test callhome inventory message
   successfully sent test callhome inventory message

8. Watch for an e-mail from Cisco regarding the registration of the switch. Follow the instructions in the e-mail to complete the registration for Smart Call Home.

SNMP Monitoring Setup
Configure SNMP by using the following example as a guideline. This example configures a host receiver for SNMPv1 traps and enables all link up/down traps.

NX-5596(config)# snmp-server host <ip-address> traps { version 1 } <community> [udp_port <number>]
NX-5596(config)# snmp-server enable traps link

NetApp Clustered Data ONTAP 8.2.2
Complete the Configuration Worksheet
Before running the setup script, complete the Configuration worksheet from the product manual.

<table>
<thead>
<tr>
<th>How to Access the Configuration Worksheet Configuration Guide</th>
<th>Comments</th>
</tr>
</thead>
</table>
### Cluster Create in NetApp Clustered Data ONTAP

#### Table 22. Cluster create in NetApp Clustered Data ONTAP Prerequisites

<table>
<thead>
<tr>
<th>Cluster Detail</th>
<th>Cluster Detail Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster name</td>
<td>&lt;&lt;var_clustername&gt;&gt;</td>
</tr>
<tr>
<td>Clustered Data ONTAP base license</td>
<td>&lt;&lt;var_cluster_base_license_key&gt;&gt;</td>
</tr>
<tr>
<td>Cluster management IP address</td>
<td>&lt;&lt;var_clustermgmt_ip&gt;&gt;</td>
</tr>
<tr>
<td>Cluster management netmask</td>
<td>&lt;&lt;var_clustermgmt_mask&gt;&gt;</td>
</tr>
<tr>
<td>Cluster management port</td>
<td>&lt;&lt;var_clustermgmt_port&gt;&gt;</td>
</tr>
<tr>
<td>Cluster management gateway</td>
<td>&lt;&lt;var_clustermgmt_gateway&gt;&gt;</td>
</tr>
<tr>
<td>Cluster Node01 IP address</td>
<td>&lt;&lt;var_node01_mgmt_ip&gt;&gt;</td>
</tr>
<tr>
<td>Cluster Node01 netmask</td>
<td>&lt;&lt;var_node01_mgmt_mask&gt;&gt;</td>
</tr>
<tr>
<td>Cluster Node01 gateway</td>
<td>&lt;&lt;var_node01_mgmt_gateway&gt;&gt;</td>
</tr>
</tbody>
</table>

The first node in the cluster performs the **cluster create** operation. All other nodes perform a **cluster join** operation. The first node in the cluster is considered Node01.

1. Type “admin” in the “login” prompt

2. During the first node boot, the Cluster Setup wizard starts running on the console.

   Welcome to the cluster setup wizard.
   You can enter the following commands at any time:
   "help" or "?" - if you want to have a question clarified,
   "back" - if you want to change previously answered questions, and
   "exit" or "quit" - if you want to quit the cluster setup wizard.
   Any changes you made before quitting will be saved.
   You can return to cluster setup at any time by typing “cluster setup”.
   To accept a default or omit a question, do not enter a value.

   **Note:** Do you want to create a new cluster or join an existing cluster? {create, join}: If a login prompt appears instead of the Cluster Setup wizard, start the wizard by logging in using the factory default settings and then enter the **cluster setup** command.

3. Enter the following command to create a new cluster:

   create

4. Type no for single node cluster option

   Do you intend for this node to be used as a single node cluster? {yes, no} [no]: no

5. Type yes for cluster network using network switches.

   Will the cluster network be configured to use network switches? [yes]: yes

6. To activate HA and set storage failover, complete the following step.

   Non-HA mode, Reboot node to activate HA

   Do you want to reboot now to set storage failover (SFO) to HA mode? {yes, no} [yes]: Enter

7. After the reboot, type “admin” in the “login” prompt.

   admin

8. Proceed with creating the cluster. Enter create on the cluster setup wizard.

   create

9. Repeat steps 4 and 5, if the cluster setup wizard prompts again.

10. The system defaults are displayed. Type “no” for using the system defaults. Follow the below prompts to configure the cluster ports.
Existing cluster interface configuration found:

<table>
<thead>
<tr>
<th>Port</th>
<th>MTU</th>
<th>IP</th>
<th>Netmask</th>
</tr>
</thead>
<tbody>
<tr>
<td>e0a</td>
<td>9000</td>
<td>169.254.166.221</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>e0c</td>
<td>9000</td>
<td>169.254.20.239</td>
<td>255.255.0.0</td>
</tr>
</tbody>
</table>

Do you want to use this configuration? {yes, no} [yes]: no

System Defaults:
- Private cluster network ports [e0a,e0c].
- Cluster port MTU values will be set to 9000.
- Cluster interface IP addresses will be automatically generated.

Do you want to use these defaults? {yes, no} [yes]: yes

11. The steps to create a cluster are displayed.

Enter the cluster name: <<var_clustername>>
Enter the cluster base license key: <<var_cluster_base_license_key>>
Creating cluster <<var_clustername>>
Enter an additional license key []:<<var_nfs_license>>
Enter an additional license key []:<<var_fcp_license>>
Enter an additional license key []:<<var_iscsi_license>>
Enter an additional license key []:<<var_flexclone_license>>

Note: The cluster is created. This can take a minute or two.

Note: For this validated architecture NetApp recommends installing license keys for SnapRestore®, FlexClone®, and SnapManager® Suite. After you finish entering the license keys, press Enter.

Enter the cluster administrators (username "admin") password: <<var_password>>
Retype the password: <<var_password>>
Enter the node management interface port [e0M]: e0i
Enter the node management interface IP address: <<var_node01_mgmt_ip>>
Enter the node management interface netmask: <<var_node01_mgmt_mask>>
Enter the node management interface default gateway: <<var_node01_mgmt_gateway>>

12. Enter the DNS Domain Name

Enter the DNS domain names:<<var_dns_domain_name>>
Enter the name server IP addresses:<<var_nameserver_ip>>

Note: If you have more than one name server IP address, separate them with a comma.

13. Set Up the Node

Where is the controller located []:<<var_node_location>>
Enter the node management interface port [e0M]: e0M
Enter the node management interface IP address: <<var_node01_mgmt_ip>>
Enter the node management interface netmask:<<var_node01_mgmt_mask>>
Enter the node management interface default gateway:<<var_node01_mgmt_gateway>>

14. The node management interface should be in a different subnet than the cluster management interface.
The node management interfaces can reside on the out-of-band management network, and the cluster management interface can be on the in-band management network.

16. Type no for IPV4 DHCP on the service processor

Enable IPV4 DHCP on the service processor interface [yes]: no

17. Set up the Service Processor (SP)

Enter the service processor interface IP address: <<var_node01_sp_ip>>
Enter the service processor interface netmask:<<var_node01_sp_netmask>>
Enter the service processor interface default gateway:<<var_node01_sp_gateway>>

18. Press Enter to accept the AutoSupport™ message.
19. Log in to the Cluster Interface with the admin user id and <<var_password>>.
20. Reboot the Service Processor.

system node service-processor reboot-sp -node <<var_node01>>
Note: If your console connection is through the SP, it will be disconnected.
Cluster Join in NetApp Clustered Data ONTAP

Table 23. Cluster Join in NetApp Clustered Data ONTAP Prerequisites.

<table>
<thead>
<tr>
<th>Cluster Detail</th>
<th>Cluster Detail Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster name</td>
<td>&lt;&lt;var_clustername&gt;&gt;</td>
</tr>
<tr>
<td>Cluster management IP address</td>
<td>&lt;&lt;var_clustermgmt_ip&gt;&gt;</td>
</tr>
<tr>
<td>Cluster node 02 IP address</td>
<td>&lt;&lt;var_node02_mgmt_ip&gt;&gt;</td>
</tr>
<tr>
<td>Cluster node 02 netmask</td>
<td>&lt;&lt;var_node02_mgmt_mask&gt;&gt;</td>
</tr>
<tr>
<td>Cluster node 02 gateway</td>
<td>&lt;&lt;var_node02_mgmt_gateway&gt;&gt;</td>
</tr>
</tbody>
</table>

The first node in the cluster performs the `cluster create` operation. All other nodes perform a `cluster join` operation. The first node in the cluster is considered node01, and the node joining the cluster in this example is node02.

1. Type “admin” in the “login” prompt
   
   admin
2. The Cluster Setup wizard starts running on the console.

   Welcome to the cluster setup wizard.
   You can enter the following commands at any time:
   "help" or "?" - if you want to have a question clarified,
   "back" - if you want to change previously answered questions, and
   "exit" or "quit" - if you want to quit the cluster setup wizard.
   Any changes you made before quitting will be saved.
   You can return to cluster setup at any time by typing "cluster setup".
   To accept a default or omit a question, do not enter a value.
   Do you want to create a new cluster or join an existing cluster? 
   {create, join}:

   Note: If a login prompt is displayed instead of the Cluster Setup wizard, start the wizard by logging in using the factory default settings, and then enter the `cluster setup` command.
3. Enter the following command to join a cluster:
   
   join
4. To activate HA and set storage failover, complete the following steps.

   Non-HA mode, Reboot node to activate HA
   Do you want to reboot now to set storage failover (SFO) to HA mode? {yes, no} [yes]: Enter

5. After the reboot, continue the Cluster Join Process
6. NetApp Data ONTAP detects existing cluster and agrees to join the same cluster. Follow the below prompts to join the cluster.

   Existing cluster interface configuration found:

<table>
<thead>
<tr>
<th>Port</th>
<th>MTU</th>
<th>IP</th>
<th>Netmask</th>
</tr>
</thead>
<tbody>
<tr>
<td>e0a</td>
<td>9000</td>
<td>169.254.226.177</td>
<td>255.255.0.0</td>
</tr>
<tr>
<td>e0c</td>
<td>9000</td>
<td>169.254.36.57</td>
<td>255.255.0.0</td>
</tr>
</tbody>
</table>

   Do you want to use this configuration? {yes, no} [yes]: no

   System Defaults:
   Private cluster network ports [e0a,e0c].
   Cluster port MTU values will be set to 9000.
   Cluster interface IP addresses will be automatically generated.
Do you want to use these defaults? [yes, no] [yes]: yes

7. The steps to create a cluster are displayed.

Enter the name of the cluster you would like to join [<<var_clustername>>]: Enter

**Note:** The node should find the cluster name.

8. Set up the node.

Enter the node management interface port [e0M]: e0M
Enter the node management interface IP address: <<var_node02_mgmt_ip>> Enter
Enter the node management interface netmask: <<var_node02_netmask>> Enter
Enter the node management interface default gateway: <<var_node02_gw>> Enter

**Note:** The node management interface should be in a subnet different from the cluster management interface. The node management interfaces can reside on the out-of-band management network, and the cluster management interface can be on the in-band management network.

9. Type no for IPV4 DHCP on the service processor.

Enable IPV4 DHCP on the service processor interface [yes]: no

10. Set up the Service Processor (SP)

Enter the service processor interface IP address: <<var_node01_sp_ip>>
Enter the service processor interface netmask: <<var_node01_sp_netmask>> Enter
Enter the service processor interface default gateway: <<var_node01_sp_gateway>> Enter

11. Press Enter to accept the AutoSupport message.

12. Log in to the Cluster Interface with the admin user id and <<var_password>>.

13. Reboot Service Processor.

```bash
system node service-processor reboot-sp -node <<var_node02>>
```

Note: If your console connection is through the SP, it will be disconnected. Do you want to reboot the SP? {y|n}: y

14. Reboot the Node

```bash
system node reboot <<var_node02>>
y
```

15. When you see Press Ctrl-C for Boot Menu, enter:

```
Ctrl-C
```

16. Select 5 to boot into maintenance mode.

```
5
```

17. At the question, Continue with boot? enter:

```
y
```

18. To verify the HA status of your environment, enter:

**Note:** If either component is not in HA mode, use the `ha-config modify` command to put the components in HA mode.

```
ha-config show
```

19. To see how many disks are unowned, enter:

```
disk show -a
```

20. Assign disks.
Note: This reference architecture allocates half the disks to each controller. Workload design determines the percentage allocations. In this case, assign all remaining disks to node 02.

disk assign -n <<var_number_of_disks>>

21. Reboot the controller:

halt

22. At the LOADER-A prompt, enter:

autoboot

23. Press Ctrl-C for boot menu when prompted.

Ctrl-C

Log in to the Cluster
Open either an SSH connection to cluster IP or host name and log in to the admin user with the password you provided earlier.

Zero All Spare Disks
Zero all spare disks in the cluster.

disk zerospares

Set Auto-Revert on Cluster Management
To set the auto-revert parameter on the cluster management interface, enter:

network interface modify -vserver <<var_clustername>> -lif cluster_mgmt -auto-revert true

Failover Groups Management in NetApp Clustered Data ONTAP
Create a management port failover group.

network interface failover-groups create -failover-group fg-cluster-mgmt -node <<var_node01>> -port e0i
network interface failover-groups create -failover-group fg-cluster-mgmt -node <<var_node02>> -port e0i
Assign Management Failover Group to Cluster Management LIF

Assign the management port failover group to the cluster management LIF.

```bash
network interface modify -vserver <<var_clustername>> -lif cluster_mgmt -failover-group fg-cluster-mgmt
```

Failover Groups Node Management in NetApp Clustered Data ONTAP

Create a management port failover group.

```bash
network interface failover-groups create -failover-group fg-node-mgmt-01 -node <<var_node01>> -port e0i
network interface failover-groups create -failover-group fg-node-mgmt-01 -node <<var_node01>> -port e0M
network interface failover-groups create -failover-group fg-node-mgmt-02 -node <<var_node02>> -port e0i
network interface failover-groups create -failover-group fg-node-mgmt-02 -node <<var_node02>> -port e0M
```

Assign Node Management Failover Groups to Node Management LIFs

Assign the management port failover group to the cluster management LIF.

```bash
network interface modify -vserver <<var_node01>> -lif mgmt1 -auto-revert true -use-failover-group enabled -failover-group fg-node-mgmt-01
network interface modify -vserver <<var_node02>> -lif mgmt1 -auto-revert true -use-failover-group enabled -failover-group fg-node-mgmt-02
```

64-Bit Aggregates in NetApp Clustered Data ONTAP

A 64-bit aggregate containing the root volume is created during the NetApp Data ONTAP setup process. To create additional 64-bit aggregates, determine the aggregate name, the node on which to create it, and the number of disks it will contain.

1. Execute the following command to create new aggregates:

   ```bash
   aggr create -aggregate aggr_hana01 -nodes <<var_node01>> -diskcount 44 -maxraidsize 22
   aggr create -aggregate aggr_hana02 -nodes <<var_node02>> -diskcount 44 -maxraidsize 22
   ```

   **Note:** In this configuration, an aggregate with 44 disks is created for the 8-node HANA sizing per NetApp FAS8040 HA pair. This provides enough space for SAP HANA workload to pass 8 node TDI KPI.

   **Note:** Retain at least one disk (select the largest disk) in the configuration as a spare. A best practice is to have at least one spare for each disk type and size.

   **Note:** The default RAID group size for the aggregate can be specified by adding the “-s <raidsize>” parameter. Calculate the RAID group size to form balanced RAID groups of (12-24 SAS disks) within the aggregate. For example, if 44 disks were being assigned to the aggregate, select a RAID group size of 22. A RAID group size of 22 would yield two 22-disk RAID groups. Keep in mind that the default RAID group size is 16 disks, and that the larger the RAID group size, the longer the disk rebuild time in case of a failure.

   **Note:** The aggregate cannot be created until disk zeroing completes. Use the `aggr show` command to display aggregate creation status. Do not proceed until both aggr_hana01 and aggr_hana02 are online.

2. Disable Snapshot copies for the two data aggregates just created.
node run <<var_node01>> aggr options aggr_hana01 nosnap on
node run <<var_node02>> aggr options aggr_hana02 nosnap on

3. Delete any existing Snapshot copies for the two data aggregates.
node run <<var_node01>> snap delete -A -a -f aggr_hana01
node run <<var_node02>> snap delete -A -a -f aggr_hana02

4. Aggregate performance configuration

set diag
storage aggregate modify -aggregate aggr_hana* -max-write-alloc-blocks 256
set admin

Service Processor
Gather information about the network and the AutoSupport settings before configuring the Service Processor (SP).

SP can be configured using DHCP or static addressing. If it uses a static IP address, verify that the following SP prerequisites are satisfied:

- An available static IP address
- The network netmask
- The network gateway IP
- AutoSupport information

A best practice is to configure the AutoSupport recipients and mail host before configuring the NetApp SP. Data ONTAP automatically sends AutoSupport configuration to the SP, allowing the SP to send alerts and notifications through an AutoSupport message to the system administrative recipients specified in AutoSupport. When configuring the SP, enter the name or the IP address of the AutoSupport mail host, when prompted.

A service processor needs to be set up on each node.

Storage Failover in NetApp Clustered Data ONTAP
Run the following commands in a failover pair to enable storage failover.

1. Verify the status of storage failover

storage failover show

Note: Both the nodes <<var_node01>> and <<var_node02>> must be capable of performing a takeover. Proceed to step 3 if the nodes are capable of performing a takeover.

2. Enable failover on one of the two nodes.

storage failover modify -node <<var_node01>> -enabled true

Note: Enabling failover on one node enables it for both nodes.

3. Verify HA status for two-node clusters

Note: This step is not applicable for clusters with more than two nodes.

cluster ha show

4. Enable HA mode for two-node clusters only.

Note: Do not run this command for clusters with more than two nodes because it will cause problems with failover.

cluster ha modify -configured true
Do you want to continue? [y|n]: y
5. Verify that hardware assist is correctly configured and if needed modify the partner IP address.

```
storage failover hwassist show
storage failover modify -hwassist-partner-ip <<var_node02_mgmt_ip>> -node <<var_node01>>
storage failover modify -hwassist-partner-ip <<var_node01_mgmt_ip>> -node <<var_node02>>
```

## Disable Flow Control on 10GbE and UTA2 Ports

NetApp recommends disabling flow control on all the 10GbE and UTA2 ports that are connected to external devices.

To disable flow control and verify, run the following commands:

```
network port modify -node fas8040-cluster-01 -port e0a,e0b,e0c,e0d,e0f,e0e,e0f,e0g -flowcontrol-admin none
network port modify -node fas8040-cluster-02 -port e0a,e0b,e0c,e0d,e0f,e0e,e0f,e0g -flowcontrol-admin none
net port show -fields flowcontrol-admin
```

## IFGRP LACP in NetApp Clustered Data ONTAP

This type of interface group requires two or more Ethernet interfaces and a switch that is configured to support LACP

1. Run the following commands on the command line to create interface groups (ifgrps) for PXE boot

```
ifgrp create -node <<var_node01>> -ifgrp a0b -distr-func port -mode multimode_lacp
network port ifgrp add-port -node <<var_node01>> -ifgrp a0b -port e0b
nenetwork port ifgrp add-port -node <<var_node01>> -ifgrp a0b -port e0d
ifgrp create -node <<var_node02>> -ifgrp a0b -distr-func port -mode multimode_lacp
network port ifgrp add-port -node <<var_node02>> -ifgrp a0b -port e0b
network port ifgrp add-port -node <<var_node02>> -ifgrp a0b -port e0d
```

2. Run the following commands on the command line to create interface groups (ifgrps) for SAP HANA Storage

```
ifgrp create -node <<var_node01>> -ifgrp a0d -distr-func port -mode multimode_lacp
network port ifgrp add-port -node <<var_node01>> -ifgrp a0d -port e0e
network port ifgrp add-port -node <<var_node01>> -ifgrp a0d -port e0f
network port ifgrp add-port -node <<var_node01>> -ifgrp a0d -port e0g
network port ifgrp add-port -node <<var_node01>> -ifgrp a0d -port e0h
ifgrp create -node <<var_node02>> -ifgrp a0d -distr-func port -mode multimode_lacp
network port ifgrp add-port -node <<var_node02>> -ifgrp a0d -port e0e
network port ifgrp add-port -node <<var_node02>> -ifgrp a0d -port e0f
network port ifgrp add-port -node <<var_node02>> -ifgrp a0d -port e0g
network port ifgrp add-port -node <<var_node02>> -ifgrp a0d -port e0h
```

**Note:** All interfaces must be in the down status before being added to an interface group. The interface group name must follow the standard naming convention of a0x.

## Create VLAN

NFS VLANs are created by running the commands shown below.

```
network port vlan create -node <<var_node01>> -vlan-name a0b<<var_boot_vlan_id>>
network port vlan create -node <<var_node02>> -vlan-name a0b<<var_boot_vlan_id>>
network port vlan create -node <<var_node01>> -vlan-name a0d<<var_storage_vlan_id>>
network port vlan create -node <<var_node02>> -vlan-name a0d<<var_storage_vlan_id>>
```
Enable Jumbo Frames

Jumbo Frames improve SAP HANA Storage Access performance. To configure a NetApp Clustered Data ONTAP network port to use jumbo frames (which usually have an MTU of 9,000 bytes), run the following command from the cluster shell:

```bash
network port modify -node <<var_node01>> -port a0d -mtu 9000
WARNING: Changing the network port settings will cause a several second interruption in carrier.
Do you want to continue? {y|n}: y

network port modify -node <<var_node02>> -port a0d -mtu 9000
WARNING: Changing the network port settings will cause a several second interruption in carrier.
Do you want to continue? {y|n}: y

network port modify -node <<var_node01>> -port a0d-<<var_storage_vlan_id>> -mtu 9000
WARNING: Changing the network port settings will cause a several second interruption in carrier.
Do you want to continue? {y|n}: y

network port modify -node <<var_node02>> -port a0d-<<var_storage_vlan_id>> -mtu 9000
WARNING: Changing the network port settings will cause a several second interruption in carrier.
Do you want to continue? {y|n}: y
```

For iSCSI boot and PXE boot environment, MTU size of 1500 bytes is configured. To verify NetApp Clustered Data ONTAP network ports are using mtu size of 1500, run the following command from the cluster shell:

```bash
network port modify -node <<var_node01>> -port a0b -mtu 1500
WARNING: Changing the network port settings will cause a several second interruption in carrier.
Do you want to continue? {y|n}: y

network port modify -node <<var_node02>> -port a0b -mtu 1500
WARNING: Changing the network port settings will cause a several second interruption in carrier.
Do you want to continue? {y|n}: y

network port modify -node <<var_node01>> -port a0b-<<var_boot_vlan_id>> -mtu 1500
WARNING: Changing the network port settings will cause a several second interruption in carrier.
Do you want to continue? {y|n}: y

network port modify -node <<var_node02>> -port a0b-<<var_boot_vlan_id>> -mtu 1500
WARNING: Changing the network port settings will cause a several second interruption in carrier.
Do you want to continue? {y|n}: y
```
Configure NTP
To configure time synchronization on the cluster, complete the following steps:

1. Set the time zone for the cluster.
   
   timezone <var_timezone>

   For example, in the Eastern United States, the time zone is America/New_York.

2. Set the date for the cluster.
   
   date <ccyymmddhhmm>

   The format for the date is <[Century][Year][Month][Day][Hour][Minute]>; for example, 201208081240.

3. Configure the Network Time Protocol (NTP) for each node in the cluster.
   
   system services ntp server create -node <<var_node01>> -server <<var_global_ntp_server_ip>>
   system services ntp server create -node <<var_node02>> -server <<var_global_ntp_server_ip>>

4. Enable the NTP for the cluster.
   
   system services ntp config modify -enabled true

Configure SNMP
Configure SNMP basic information, such as the location and contact. When polled, this information is visible as the sysLocation and sysContact variables in SNMP.

   snmp contact <<var_snmp_contact>>
   snmp location "<<var_snmp_location>>"
   snmp init 1
   options snmp.enable on

   Configure SNMP traps to send to remote hosts, such as a DataFabric® Manager server or another fault management system.
   
   snmp traphost add <<var_oncommand_server_fqdn>>

SNMPv1
Set the shared secret plain-text password, which is called a community.

   snmp community delete all
   snmp community add ro <<var_snmp_community>>

   Note: Use the delete all command with caution. If community strings are used for other monitoring products, the delete all command will remove them.

SNMPv3
SNMPv3 requires that a user is defined and configured for authentication.

1. Create a user called snmpv3user.
   
   security login create -username snmpv3user -authmethod usm -application snmp

2. Select all of the default authoritative entities and select md5 as the authentication protocol.
3. Enter an eight-character minimum-length password for the authentication protocol, when prompted.
4. Select des as the privacy protocol.
5. Enter an eight-character minimum-length password for the privacy protocol, when prompted.
AutoSupport HTTPS
AutoSupport sends support summary information to NetApp through HTTPS.

Execute the following commands to configure AutoSupport:

```
system node autosupport modify -node * -state enable -mail-hosts <<var_mailhost>> -transport https -support enable -noteto <<var_storage_admin_email>>
```

Enable Cisco Discovery Protocol
Enable Cisco Discovery Protocol (CDP) on the NetApp storage controllers by using the following procedure.

**Note:** To be effective, CDP must also be enabled on directly connected networking equipment such as switches and routers.

To enable CDP on the NetApp storage controllers, complete the following step:

Enable CDP on NetApp Data ONTAP.

```
node run -node <<var_node01>> options cdpd.enable on
node run -node <<var_node02>> options cdpd.enable on
```

Storage Virtual Machine (SVM)
It is recommended to create a separate Storage Virtual Machine for Infrastructure which contains the iSCSI Boot volumes of the ESXi hosts, Infrastructure datastores for ESXi cluster which contains Virtual Machines, SAP Application Servers Virtual Machines. The SVM provides additional security and QoS at various levels of granularity. It also provides secured multi-tenancy between SAP HANA and Application Servers.

Storage Virtual Machine for SAP HANA
To create an SAP HANA SVM complete the following steps:

1. Run the Vserver setup wizard.
   
   vserver setup
   
   Welcome to the Vserver Setup Wizard, which will lead you through the steps to create a virtual storage server that serves data to clients.
   
   You can enter the following commands at any time: "help" or "?" if you want to have a question clarified, "back" if you want to change your answers to previous questions, and "exit" if you want to quit the Vserver Setup Wizard. Any changes you made before typing "exit" will be applied.
   
   You can restart the Vserver Setup Wizard by typing "vserver setup". To accept a default or omit a question, do not enter a value.
   
   Step 1. Create a Vserver.
   
   You can type "back", "exit", or "help" at any question.
   
   Enter the Vserver name:
   
   Enter the Vserver name:hana_vs1
   
   3. Select the Vserver data protocols to configure.
   
   Choose the Vserver data protocols to be configured {nfs, cifs, fcp, iscsi}: nfs
   
   4. Select the Vserver client services to configure.
   
   Choose the Vserver client services to configure {ldap, nis, dns}: Enter
   
   5. Enter the Vserver’s root volume aggregate:
   
   Enter the Vserver’s root volume aggregate {aggr_hana01, aggr_hana02} [aggr_hana01]: Enter
   
   6. Enter the Vserver language setting. English is the default [C].
Enter the Vserver language setting, or "help" to see all languages [C]: Enter

7. Enter the Vserver’s security style:

Enter the Vservers root volume’s security style {unix, ntfs, mixed} [unix]: Enter

8. Answer no to Do you want to create a data volume?

Do you want to create a data volume? {yes, no} [Yes]: no

9. Answer no to Do you want to create a logical interface?

Do you want to create a logical interface? {yes, no} [Yes]: no

10. Add the two data aggregates to the hana_vs1 aggregate list for NetApp Virtual Console.

vserver modify -vserver hana_vs1 -aggr-list aggr_hana01, aggr_hana02

Storage Virtual Machine for Infrastructure

To create an infrastructure Vserver, complete the following steps:

1. Run the Vserver setup wizard.

vserver setup

Welcome to the Vserver Setup Wizard, which will lead you through the steps to create a virtual storage server that serves data to clients.

You can enter the following commands at any time: "help" or "?" if you want to have a question clarified, "back" if you want to change your answers to previous questions, and "exit" if you want to quit the Vserver Setup Wizard. Any changes you make before typing "exit" will be applied.

You can restart the Vserver Setup Wizard by typing "vserver setup". To accept a default or omit a question, do not enter a value.

Step 1. Create a Vserver.
You can type "back", "exit", or "help" at any question.

2. Enter the Vserver name.

Enter the Vserver name: infra_vs1

3. Select the Vserver data protocols to configure.

Choose the Vserver data protocols to be configured {nfs, cifs, fcp, iscsi}: nfs, iscsi

4. Select the Vserver client services to configure.

Choose the Vserver client services to configure {ldap, nis, dns}: Enter

5. Enter the Vserver’s root volume aggregate:

Enter the Vserver’s root volume aggregate {aggr_hana01, aggr_hana02} [aggr_hana01]: Enter

6. Enter the Vserver language setting. English is the default [C].

Enter the Vserver language setting, or "help" to see all languages [C]: Enter

7. Enter the Vserver’s security style:

Enter the Vserver’s root volume’s security style {unix, ntfs, mixed} [unix]: Enter

8. Answer no to Do you want to create a data volume?

Do you want to create a data volume? {yes, no} [Yes]: no

9. Answer no to Do you want to create a logical interface?

Do you want to create a logical interface? {yes, no} [Yes]: no

10. Add the two data aggregates to the hana_vs1 aggregate list for NetApp Virtual Console.

vserver modify -vserver infra_vs1 -aggr-list aggr_hana01, aggr_hana02
Create Load Sharing Mirror of Vserver Root Volume in NetApp Clustered Data ONTAP

**SAP HANA Vserver**
1. Create a volume to be the load sharing mirror of the HANA Vserver root volume on each node.
   
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
   | `volume create -vserver hana_vs1 -volume root_vol_m01 -aggregate aggr_hana01 -size 1GB -type DP` | Create volume root_vol_m01
   | `volume create -vserver hana_vs1 -volume root_vol_m02 -aggregate aggr_hana02 -size 1GB -type DP` | Create volume root_vol_m02

2. Create the mirroring relationships.
   
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
   | `snapmirror create -source-path hana_vs1:rootvol -destination-path hana_vs1:root_vol_m01 -type LS` | Create mirroring relationship
   | `snapmirror create -source-path hana_vs1:rootvol -destination-path hana_vs1:root_vol_m02 -type LS` | Create mirroring relationship

3. Initialize the mirroring relationship.
   
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
   | `snapmirror initialize-ls-set -source-path hana_vs1:rootvol` | Initialize mirroring relationship

4. Set an update schedule for every 15 minutes on each mirroring relationship.
   
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
   | `job schedule interval create -name 15min -minutes 15` | Create job schedule
   | `snapmirror modify -source-path hana_vs1:rootvol -destination-path * -schedule 15min` | Modify mirroring relationship schedule

**Infra Vserver**
1. Create a volume to be the load sharing mirror of the Infra Vserver root volume on each node.
   
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
   | `volume create -vserver infra_vs1 -volume root_vol_m01 -aggregate aggr_hana01 -size 1GB -type DP` | Create volume root_vol_m01
   | `volume create -vserver infra_vs1 -volume root_vol_m02 -aggregate aggr_hana02 -size 1GB -type DP` | Create volume root_vol_m02

2. Create the mirroring relationships.
   
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
   | `snapmirror create -source-path infra_vs1:rootvol -destination-path infra_vs1:root_vol_m01 -type LS` | Create mirroring relationship
   | `snapmirror create -source-path infra_vs1:rootvol -destination-path infra_vs1:root_vol_m02 -type LS` | Create mirroring relationship

3. Initialize the mirroring relationship.
   
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
   | `snapmirror initialize-ls-set -source-path infra_vs1:rootvol` | Initialize mirroring relationship

4. Set an update schedule for every 15 minutes on each mirroring relationship.
   
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
   | `job schedule interval create -name 15min -minutes 15` | Create job schedule
   | `snapmirror modify -source-path infra_vs1:rootvol -destination-path * -schedule 15min` | Modify mirroring relationship schedule

**Configure HTTPS Access**
Secure access to the storage controller must be configured.

1. Increase the privilege level to access the certificate commands.
   
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
   | `set -privilege advanced` | Increase privilege level
   | `Do you want to continue? [y|n]: y` | Continue with command

2. Generally, a self-signed certificate is already in place. Check it with the following command:
   
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
   | `security certificate show` | Check certificate
3. Run the following commands as one-time commands to generate and install self-signed certificates:

**Note:** The `security certificate delete` command to delete expired certificates

```bash
security certificate create -vserver Infra_Vserver -common-name <<var_security_cert_vserver_common_name>> -size 2048 -country <<var_country_code>> -state <<var_state>> -locality <<var_city>> -organization <<var_org>> -unit <<var_unit>> -email <<var_storage_admin_email>>
security certificate create -vserver <<var_clustername>> -common-name <<var_security_cert_cluster_common_name>> -size 2048 -country <<var_country_code>> -state <<var_state>> -locality <<var_city>> -organization <<var_org>> -unit <<var_unit>> -email <<var_storage_admin_email>>
security certificate create -vserver <<var_node01>> -common-name <<var_security_cert_node01_common_name>> -size 2048 -country <<var_country_code>> -state <<var_state>> -locality <<var_city>> -organization <<var_org>> -unit <<var_unit>> -email <<var_storage_admin_email>>
security certificate create -vserver <<var_node02>> -common-name <<var_security_cert_node02_common_name>> -size 2048 -country <<var_country_code>> -state <<var_state>> -locality <<var_city>> -organization <<var_org>> -unit <<var_unit>> -email <<var_storage_admin_email>>
```

4. Configure and enable SSL and HTTPS access and disable Telnet access.

```bash
system services web modify -external true -sslv3-enabled true
Do you want to continue {y|n}: y
system services firewall policy create -policy mgmt -service http -action deny -ip-list 0.0.0.0/0
system services firewall policy create -policy mgmt -service telnet -action deny -ip-list 0.0.0.0/0
security ssl modify -vserver Infra_Vserver -certificate <<var_security_cert_vserver_common_name>> -enabled true
security ssl modify -vserver <<var_clustername>> -certificate <<var_security_cert_cluster_common_name>> -enabled true
security ssl modify -vserver <<var_node01>> -certificate <<var_security_cert_node01_common_name>> -enabled true
security ssl modify -vserver <<var_node02>> -certificate <<var_security_cert_node02_common_name>> -enabled true
```

5. Use the `security certificate show` command to obtain the values for the parameters that would be needed in the step below.

6. The required parameters are:
   - common-name: << example FAS8040-Cluster.cert>>
   - Certificate Authority: << example FAS8040-Cluster.cert>>
   - Serial Number: << example 12345678>>

7. Use these values in the command below.

```bash
security ssl modify -vserver infra_vs1 -common-name <<var_security_certificate_vserver_common_name>> -server-enabled true -client-enabled false -ca <<var_security_certificate_vserver_authority>> -serial <<var_security_certificate_vserver_serial_no>>
security ssl modify -vserver <<var_clustername>> -common-name <<var_security_certificate_cluster_common_name>> -server-enabled true -client-enabled false -ca <<var_security_certificate_cluster_authority>> -serial <<var_security_certificate_cluster_serial_no>>
security ssl modify -vserver <<var_node01>> -common-name <<var_security_certificate_node01_common_name>> -server-enabled true -client-enabled false -ca <<var_security_certificate_node01_authority>> -serial <<var_security_certificate_node01_serial_no>>
security ssl modify -vserver <<var_node02>> -common-name <<var_security_certificate_node02_common_name>> -server-enabled true -client-enabled false -ca <<var_security_certificate_node02_authority>> -serial <<var_security_certificate_node02_serial_no>>
```
Note: It is normal for some of these commands to return an error message stating that the entry does not exist.

## Configure NFSv3

### Performance Optimization Options for NFSv3 for SAP HANA

1. Set NFS TCP window size
   ```
   fas8040-cluster::> set diag
   Warning: These diagnostic commands are for use by NetApp personnel only.
   Do you want to continue? {y|n}: y
   fas8040-cluster::*> nfs modify -vserver hana_vs1 -tcp-max-xfer-size 65536
   fas8040-cluster::*> set admin
   ```

2. Set NFS read size
   ```
   fas8040-cluster::> set diag
   Warning: These diagnostic commands are for use by NetApp personnel only.
   Do you want to continue? {y|n}: y
   fas8040-cluster::*> nfs modify -vserver hana_vs1 -v3-tcp-max-read-size 65536
   fas8040-cluster::*> set admin
   ```

3. Run all commands to configure NFS on the Vserver.

4. Secure the default rule for the default export policy and create data export policy.
   ```
   vserver export-policy rule modify –vserver hana_vs1 –policyname default –ruleindex 1 -rorule never -rwrule never -superuser never
   vserver export-policy rule modify –vserver infra_vs1 –policyname default –ruleindex 1 -rorule never -rwrule never -superuser never
   vserver export-policy create –vserver infra_vs1 boot
   vserver export-policy create –vserver hana_vs1 data
   ```

5. Create a new rule for the boot export policy.
   ```
   vserver export-policy rule create –vserver infra_vs1 -policyname boot –ruleindex 1 –protocol nfs -clientmatch <<var_host_boot_subnet>> -rorule sys –rwrule sys -superuser sys –allow-suid false
   ```

6. Create a new rule for the data export policy.
   ```
   vserver export-policy rule create –vserver hana_vs1 -policyname data -ruleindex 1 –protocol nfs -clientmatch <<var_host_data_subnet>> -rorule sys –rwrule sys -superuser sys –allow-suid false
   ```

## Create FlexVol

The information required to create a FlexVol® volume includes volume’s name and size, and the aggregate on which it will exist. Create volumes for master OS boot, which will be used to clone boot volume for each server, tftpboot used for PXE boot for servers

```
volume create -vserver infra_vs1 -volume os_master -aggregate aggr_hana02 -size 50g -state online -policy boot -junction-path /os_master -space-guarantee none -percent-snapshot-space 0
volume modify -volume os_master -snapdir-access false
volume create -vserver infra_vs1 -volume software -aggregate aggr_hana02 -size 100g -
```
Configure Failover Groups NAS

Create an NFS port failover group.

```bash
network interface failover-groups create -failover-group fg-nfs-<var_boot_vlan_id> -node <var_node01> -port a0b-<var_boot_vlan_id>
network interface failover-groups create -failover-group fg-nfs-<var_boot_vlan_id> -node <var_node02> -port a0b-<var_boot_vlan_id>
```

Configure NFS LIF

Create an NFS logical interface (LIF).

```bash
network interface create -vserver infra_vs1 -lif pxe_lif01 -role data -data-protocol nfs -home-node <var_node01> -home-port a0b-<var_boot_vlan_id> -address <var_node01_boot_lif_ip> -netmask <var_node01_boot_lif_mask> -status-admin up -failover-policy nextavail -firewall-policy data -auto-revert true -use-failover-group enabled -failover-group fg-nfs-<var_boot_vlan_id>
```

SAP Virtualized HANA (vHANA) Storage Configuration

1. Create export policy for ESX Hosts

   ```bash
   vserver export-policy create -vserver infra_vs1 vhana-hosts
   ```

2. Create a new rule for the export policy.

   **Note:** For each ESXi host being created, create a rule. Each host will have its own rule index. i.e., first ESXi host will have rule index 1, second ESXi host will have rule index 2, and so on.
### vserver export-policy rule create
- vserver infra_vs1
- policyname vhana-hosts
- ruleindex 1
- protocol nfs
- clientmatch <<var_esxi_host1_nfs_ip>>
- rorule sys
- rwrule sys
- superuser sys
- allow-suid false

3. Create export policy for vHANA VMs

vserver export-policy create -vserver infra_vs1 vhana-vm

4. Create a new rule for the vHANA VMs export policy.

vserver export-policy rule create -vserver infra_vs1 -policyname vhana-vm -ruleindex 1 -protocol nfs -clientmatch <<var_vhana_storage_ip>> -rorule sys -rwrule sys -superuser sys -allow-suid false

5. Create a volumes required vHANA

6. The following information is required to create a FlexVol® volume: the volume’s name and size, and the aggregate on which it will exist. Create two VMware datastore volumes, a esxi boot volume

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>volume create</code></td>
<td>-vserver infra_vs1 -volume vhana_datastore_1 -aggregate aggr_hana01 -size 450g -state online -policy vhana-hosts -junction-path /vhana_datastore_1 -space-guarantee file -percent-snapshot-space 0</td>
</tr>
<tr>
<td><code>volume create</code></td>
<td>-vserver infra_vs1 -volume vhana_swap -aggregate aggr_hana01 -size 100g -state online -policy vhana-hosts -junction-path /vhana_swap -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none</td>
</tr>
<tr>
<td><code>volume create</code></td>
<td>-vserver infra_vs1 -volume esxi_boot -aggregate aggr_hana01 -size 100g -state online -policy default -space-guarantee file -percent-snapshot-space 0</td>
</tr>
</tbody>
</table>

7. LUN in NetApp Clustered Data ONTAP

8. Create two boot LUNS: vhana-host-01 and vhana-host-01.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>lun create</code></td>
<td>-vserver infra_vs1 -volume esxi_boot -lun vhana-host-01 -size 10g -ostype vmware -space-reserve disabled</td>
</tr>
<tr>
<td><code>lun create</code></td>
<td>-vserver infra_vs1 -volume esxi_boot -lun vhana-host-02 -size 10g -ostype vmware -space-reserve disabled</td>
</tr>
</tbody>
</table>

9. Enable deduplication on appropriate volumes.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>volume efficiency on</code></td>
<td>-vserver infra_vs1 -volume vhana_datastore_1</td>
</tr>
<tr>
<td><code>volume efficiency on</code></td>
<td>-vserver infra_vs1 -volume esxi_boot</td>
</tr>
</tbody>
</table>

10. Create NFS VLANs.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>network port vlan create</code></td>
<td>-node &lt;&lt;var_node01&gt;&gt; -vlan-name a0d-&lt;&lt;var_vhana_esx_vlan_id&gt;&gt;</td>
</tr>
<tr>
<td><code>network port vlan create</code></td>
<td>-node &lt;&lt;var_node02&gt;&gt; -vlan-name a0d-&lt;&lt;var_vhana_esx_vlan_id&gt;&gt;</td>
</tr>
<tr>
<td><code>network port vlan create</code></td>
<td>-node &lt;&lt;var_node01&gt;&gt; -vlan-name a0d-&lt;&lt;var_vhana_storage_vlan_id&gt;&gt;</td>
</tr>
<tr>
<td><code>network port vlan create</code></td>
<td>-node &lt;&lt;var_node02&gt;&gt; -vlan-name a0d-&lt;&lt;var_vhana_storage_vlan_id&gt;&gt;</td>
</tr>
</tbody>
</table>

11. Create an NFS port failover group.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>network interface failover-groups create</code></td>
<td>-failover-group fg-nfs-&lt;&lt;var_vhana_esx_nfs_vlan_id&gt;&gt;  -node &lt;&lt;var_node01&gt;&gt; -port a0d-&lt;&lt;var_vhana_esx_nfs_vlan_id&gt;&gt;</td>
</tr>
<tr>
<td><code>network interface failover-groups create</code></td>
<td>-failover-group fg-nfs-&lt;&lt;var_vhana_esx_nfs_vlan_id&gt;&gt;  -node &lt;&lt;var_node02&gt;&gt; -port a0d-&lt;&lt;var_vhana_esx_nfs_vlan_id&gt;&gt;</td>
</tr>
<tr>
<td><code>network interface failover-groups create</code></td>
<td>-failover-group fg-nfs-&lt;&lt;var_vhana_storage_vlan_id&gt;&gt;  -node &lt;&lt;var_node01&gt;&gt; -port a0d-&lt;&lt;var_vhana_storage_vlan_id&gt;&gt;</td>
</tr>
<tr>
<td><code>network interface failover-groups create</code></td>
<td>-failover-group fg-nfs-&lt;&lt;var_vhana_storage_vlan_id&gt;&gt;  -node &lt;&lt;var_node02&gt;&gt; -port a0d-&lt;&lt;var_vhana_storage_vlan_id&gt;&gt;</td>
</tr>
</tbody>
</table>

12. Create an NFS logical interface (LIF).

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>network interface create</code></td>
<td>-vserver infra_vs1 -lif esx_lif01 -role data -data-protocol nfs -home-node &lt;&lt;var_node01&gt;&gt; -home-port a0d-&lt;&lt;var_vhana_esx_nfs_vlan_id&gt;&gt; -address &lt;&lt;var_node01_esx_lif_ip&gt;&gt; -netmask &lt;&lt;var_node01_esx_nfs_vlan_id&gt;&gt;</td>
</tr>
</tbody>
</table>
network interface create -vserver infra_vs1 -lif esx_lif02 -role data -data-protocol nfs -home-node <<var_node02>> -home-port a0d-<<var_vhana_esx_nfs_vlan_id>> -address <<var_node02_esx_lif_ip>> -netmask <<var_node01_esx_lif_mask>> -status-admin up -failover-policy nextavail -firewall-policy data -auto-revert true -failover-group fg-nfs-<<var_vhana_esx_nfs_vlan_id>>

network interface create -vserver infra_vs1 -lif vhana_lif01 -role data -data-protocol nfs -home-node <<var_node01>> -home-port a0d-<<var_vhana_storage_vlan_id>> -address <<var_node01_vhana_lif_ip>> -netmask <<var_node01_vhana_lif_mask>> -status-admin up -failover-policy nextavail -firewall-policy data -auto-revert true -failover-group fg-nfs-<<var_vhana_storage_vlan_id>>

network interface create -vserver infra_vs1 -lif vhana_lif02 -role data -data-protocol nfs -home-node <<var_node02>> -home-port a0d-<<var_vhana_storage_vlan_id>> -address <<var_node02_vhana_lif_ip>> -netmask <<var_node02_vhana_lif_mask>> -status-admin up -failover-policy nextavail -firewall-policy data -auto-revert true -failover-group fg-nfs-<<var_vhana_storage_vlan_id>>

iSCSI Boot for ESXi

For ESXi hosts, iSCSI boot is recommended below are the steps to configure iSCSI boot on the NetApp FAS 8000.

Create iSCSI VLANs

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>network port vlan create -node &lt;&lt;var_node01&gt;&gt; -vlan-name a0b-&lt;&lt;iSCSI_vlan_id_A&gt;&gt;</td>
<td>Create iSCSI VLAN A on node 01</td>
</tr>
<tr>
<td>network port vlan create -node &lt;&lt;var_node01&gt;&gt; -vlan-name a0b-&lt;&lt;iSCSI_vlan_id_B&gt;&gt;</td>
<td>Create iSCSI VLAN B on node 01</td>
</tr>
<tr>
<td>network port vlan create -node &lt;&lt;var_node02&gt;&gt; -vlan-name a0b-&lt;&lt;iSCSI_vlan_id_A&gt;&gt;</td>
<td>Create iSCSI VLAN A on node 02</td>
</tr>
<tr>
<td>network port vlan create -node &lt;&lt;var_node02&gt;&gt; -vlan-name a0b-&lt;&lt;iSCSI_vlan_id_B&gt;&gt;</td>
<td>Create iSCSI VLAN B on node 02</td>
</tr>
</tbody>
</table>

Start iSCSI Service

Create the iSCSI service on each Vserver. This command also starts the iSCSI service and sets the IQN target of the Vserver.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>iscsi create -vserver infra_vs1</td>
<td>Create and start the iSCSI service on the Vserver</td>
</tr>
</tbody>
</table>

Create iSCSI LIF

Create four iSCSI LIFs, two on each node.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>network interface create -vserver infra_vs1 -lif iscsi_lif01a -role data -data-protocol iscsi -home-node &lt;&lt;var_node01&gt;&gt; -home-port a0b-&lt;&lt;iscsi_A_vlan_id&gt;&gt; -address &lt;&lt;var_node01_iscsi_A_IP&gt;&gt; -netmask &lt;&lt;var_iscsi_A_mask&gt;&gt;</td>
<td>Create iSCSI LIF on node 01 for VM host 01</td>
</tr>
<tr>
<td>network interface create -vserver infra_vs1 -lif iscsi_lif01b -role data -data-protocol iscsi -home-node &lt;&lt;var_node01&gt;&gt; -home-port a0b-&lt;&lt;iscsi_B_vlan_id&gt;&gt; -address &lt;&lt;var_node01_iscsi_B_IP&gt;&gt; -netmask &lt;&lt;var_iscsi_B_mask&gt;&gt;</td>
<td>Create iSCSI LIF on node 01 for VM host 02</td>
</tr>
<tr>
<td>network interface create -vserver infra_vs1 -lif iscsi_lif02a -role data -data-protocol iscsi -home-node &lt;&lt;var_node02&gt;&gt; -home-port a0b-&lt;&lt;iscsi_A_vlan_id&gt;&gt; -address &lt;&lt;var_node02_iscsi_A_IP&gt;&gt; -netmask &lt;&lt;var_iscsi_A_mask&gt;&gt;</td>
<td>Create iSCSI LIF on node 02 for VM host 01</td>
</tr>
<tr>
<td>network interface create -vserver infra_vs1 -lif iscsi_lif02b -role data -data-protocol iscsi -home-node &lt;&lt;var_node02&gt;&gt; -home-port a0b-&lt;&lt;iscsi_B_vlan_id&gt;&gt; -address &lt;&lt;var_node02_iscsi_B_IP&gt;&gt; -netmask &lt;&lt;var_iscsi_B_mask&gt;&gt;</td>
<td>Create iSCSI LIF on node 02 for VM host 02</td>
</tr>
</tbody>
</table>

Create igroups

From the cluster management node SSH connection, enter the following:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igroup create -vserver infra_vs1 -igroup vhana-host-01 -protocol iscsi -ostype vmware -initiator &lt;&lt;var_vhana_host_01_iqn&gt;&gt;</td>
<td>Create iGroup for the Vserver</td>
</tr>
</tbody>
</table>
igroup create -vserver infra_vs1 -igroup vhana-host-02 -protocol iscsi -ostype vmware -initiator <<var_vhana_host_02_iqn>>
igroup create -vserver infra_vs1 -igroup vhana-hosts -protocol iscsi -ostype vmware -initiator <<var_vhana_host_01_iqn>>,<<var_vhana_host_02_iqn>>

Note: To gather the vNIC IQN information, launch the Cisco UCS Manager GUI. In the navigation pane, click the Servers tab. Expand Servers > Service Profiles > root > Sub-Organization > vHANA Click each service profile and then click the “iSCSI vNICs” tab on the right. Note “Initiator Name” displayed at the top of the page under “Service Profile Initiator Name”

Map Boot LUNs to igroups

From the cluster management SSH connection, enter the following:

lun map -vserver infra_vs1 -volume esxi_boot -lun vhana-host-01 -igroup vhana-host-01 -lun-id 0
lun map -vserver infra_vs1 -volume esxi_boot -lun vhana-host-02 -igroup vhana-host-02 -lun-id 0

Preparation of PXE Boot Environment

Two PXE boot servers are used for a PXE boot to provide redundancy - one on Management Server 01 (ESXi-Mgmt-01) another on Management Server 02 (ESXi-Mgmt-02) for redundancy.

Installing PXE Boot VM on the Management Servers

To build a PXE Boot virtual machine (VM) on the ESXi-Mgmt-01 complete the following steps:

1. Log in to the host by using the VMware vSphere Client.
2. In the VMware vSphere Client, select the host in the inventory pane.
3. Right-click the host and select New Virtual Machine.
4. Select Custom and click Next.
5. Enter a name for the VM, example HANA-Mgmt01, click Next.
6. Select the datastore where the PXE server resides. Click Next.
8. Select the Linux option and the SUSE Linux Enterprise 11 (64-bit) version are selected. Click Next.
9. Select two virtual sockets and one core per virtual socket. Click Next.
10. Select 4GB of memory. Click Next.
11. Select three network interface card (NIC).
12. For NIC 1, select the OOB-MGMT Network option and the VMXNET 3 adapter
13. For NIC 2, select the HANA-Boot Network option and the VMXNET 3 adapter
14. For NIC 1, select the HANA-Admin Network option and the VMXNET 3 adapter
15. Click Next.
16. Keep the LSI Logic SAS option for the SCSI controller selected. Click Next.
17. Keep the Create a New Virtual Disk option selected. Click Next.
18. Make the disk size at least 60GB. Click Next.
19. Click Next.
20. Select the checkbox for Edit the Virtual Machine Settings Before Completion. Click Continue.
21. Click the Options tab.
22. Select Boot Options.
23. Select the Force BIOS Setup checkbox.
24. Click Finish.
25. From the left pane, expand the host field by clicking the plus sign (+).
26. Right-click the newly created HANA-Mgmt01 and click Open Console.
27. Click the third button (green right arrow) to power on the VM.
28. Click the ninth button (CD with a wrench) to map the SLES-11-SP3-x86_64, and then select Connect to ISO Image on Local Disk.
29. Navigate to the SLES-11 SP3 64 bit ISO, select it, and click Open.
30. Click in the BIOS Setup Utility window and use the right arrow key to navigate to the Boot menu. Use the down arrow key to select CD-ROM Drive. Press the plus (+) key twice to move CD-ROM Drive to the top of the list. Press F10 and Enter to save the selection and exit the BIOS Setup Utility.
31. The SUSE Installer boots. Select the Installation by pressing down arrow key and press Enter
32. Agree to the License Terms, Select Next and press Enter
33. Skip Media test and Click on Next
34. Leave New Installation selected and Click Next
35. Under Choose Scenario Keep Physical Machine (also for Fully Virtualized Guests) selected and Click Next
36. In the Overview section click Software and Choose DHCP and DNS Server Under Primary Functions.
37. Press OK and Accept.
38. Click and Install to perform the installation.
39. After Installation Virtual Machine will reboot
40. After reboot, system will continue the installation to customize the installed Operating System
41. Enter the Password for root User and Confirm Password, then click Next
42. Enter Hostname and Domain Name, uncheck Change Hostname via DHCP, then click Next
43. Under Network Configuration, keep Use Following Configuration selected:
   a. Under General Network Settings Support for IPv6 protocol is enabled click Disable IPv6, on the Warning To apply this change, a reboot is needed Press OK
   b. Under Firewall → Firewall is enabled Click disable
   c. Click on Network Interfaces, Under the Overview Select the first device and Click on Edit and enter IP Address <<var_pxe_oob_IP>> and Subnet Mask <<var_pxe_oob_subnet>>. Enter the Hostname, Click on the General Tab and Set MTU 1500 or 9000 depending on the Customer switch config, Click Next
   d. Under the Overview Select the second device and Click on Edit and enter IP Address <<var_pxe_boot_IP>> and Subnet Mask <<var_pxe_boot_subnet>>. Enter the Hostname, Click on the General Tab and Set MTU 1500, click Next
   e. Under the Overview Select the third device and Click on Edit and enter IP Address <<var_pxe_admin_IP>> and Subnet Mask <<var_pxe_admin_subnet>>. Enter the Hostname, Click the General Tab and Set MTU 1500, click Next
   f. Click Hostname/DNS tab Under Name Server 1 enter the IP address of the DNS Server, optionally enter the IP address for Name Server 2 and Name Server 2, under Domain Search enter the Domain name for DNS
   g. Click the Routing tab and Enter the IP address for Default Gateway for Out Band Management IP address, and Press OK
45. Click the VNC Remote Administration and select Allow Remote Administration. Click Finish
46. Optional if there is proxy server required for Internet access click on Proxy Configuration, check Enable Proxy. Enter the HTTP Proxy URL, HTTPS Proxy URL or based on proxy server configuration check Use the Same Proxy for All Protocols. If proxy server requires Authentication enter Proxy User Name and Proxy Password and Click Finish
47. Click Next to finish Network Configuration
48. Under Test Internet Connection Choose No, Skip This Test
49. For Network Service Configuration, choose default and Click Next
50. For User Authentication Method select default Local (/etc/passwd), if there are other option like LDAP, NIS, Windows Domain configure accordingly.
51. Create New Local User, enter password and Confirm Password.
52. Release Notes, click Next
53. Use Default Hardware Configuration, click Next
54. Uncheck Clone This System for AutoYaST and click Finish

To build a PXE Boot virtual machine (VM) on the Management Server 02 complete the above steps
ESXi – Mgmt – 02
Customize PXE Boot Server
1. Check the IP address are assigned correctly and network are reachable

```
HANA-mgmtsrv01:~ # ifconfig
eth0    Link encap:Ethernet  HWaddr 00:0C:29:3D:3F:58
        inet addr:172.25.186.27  Bcast:172.25.186.255  Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:109046 errors:0 dropped:0 overruns:0 frame:0
        TX packets:2928 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:26977355 (25.7 Mb)  TX bytes:653460 (638.1 Kb)

eth1    Link encap:Ethernet  HWaddr 00:0C:29:3D:3F:62
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:15 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:5124 (5.0 Kb)  TX bytes:0 (0.0 b)

eth2    Link encap:Ethernet  HWaddr 00:0C:29:3D:3F:6C
        inet addr:172.29.112.27  Bcast:172.29.112.255  Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:2 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:120 (120.0 b)  TX bytes:0 (0.0 b)
```

Configure the NTP Server
```
vi /etc/ntp.conf
server  <<var_global_ntp_server_ip>>
```

Configure the /etc/hosts File of the Management Stations
```
cat /etc/hosts
# # This file describes a number of hostname-to-address # mappings for the TCP/IP subsystem. It is mostly # used at boot time, when no name servers are running. # On small systems, this file can be used instead of a # "named" name server.
# Syntax:
# # IP-Address  Full-Qualified-Hostname  Short-Hostname #

127.0.0.1  localhost
172.25.186.27  mgmtsrv01.ciscolab.local  mgmtsrv01
## PXE VLAN
192.168.127.11  nfspxe
192.168.127.6   mgmtsrv01b
192.168.127.201 server01b
192.168.127.202 server02b
192.168.127.203 server03b
192.168.127.204 server04b
192.168.127.205 server05b
```
Mount Volume for PXE Boot Configuration

1. To mount the tftpboot, software and osmaster volumes, add the entry to /etc/fstab with the values listed below:

```
vim /etc/fstab
```

```
nfspxe:/tftpboot          /tftpboot       nfs     defaults        0 0
nfspxe:/software          /NFS/software   nfs     defaults        0 0
nfspxe:/suse_os_master    /NFS/osmaster   nfs     defaults        0 0
```

2. Create the directories for mount points

```
mkdir /tftpboot
mkdir /NFS
mkdir /NFS/osmaster
mkdir /NFS/software
```

3. Mount the nfs file system

```
mount /NFS/osmaster
mount /tftpboot
mount /NFS/software
```

Download the SUSE ISO

1. Download the SUSE Linux Enterprise for SAP Applications 11 SP3 ISO from https://www.suse.com/
2. Upload ISO downloaded to /NFS/software directory using scp tool

Update PXE Boot VM

To update the SUSE virtual machine to latest patch level, complete the following steps:

**Note:** The document assumes that SUSE License key is obtained and registered username and password is available. VM has internet access.

1. `ssh` to the PXE boot VM
2. Login as root and password
3. Execute the below command to Register the SUSE

```
suse_register -i -r -n -a email=<<email_address>> -a regcode-sles=<<registration_code>>
```

4. After the registration, all the repository will be updated

```
All services have been refreshed.
All repositories have been refreshed.
Refreshing service 'nu_novell_com'.
Adding repository 'SLES11-SP3-Updates' [done]
Adding repository 'SLES11-Extras' [done]
Adding repository 'SLES11-SP1-Pool' [done]
Adding repository 'SLES11-SP2-Updates' [done]
Adding repository 'SLES11-SP3-Pool' [done]
Adding repository 'SLES11-SP2-Extension-Store' [done]
Adding repository 'SLES11-SP3-Debuginfo-Pool' [done]
Adding repository 'SLES11-SP3-Debuginfo-Updates' [done]
Adding repository 'SLES11-SP1-Debuginfo-Updates' [done]
Adding repository 'SLES11-SP1-Extension-Store' [done]
Adding repository 'SLES11-SP1-Debuginfo-Pool' [done]
Adding repository 'SLES11-SP1-Debuginfo-Updates' [done]
Adding repository 'SLES11-SP2-Debuginfo-Pool' [done]
Adding repository 'SLES11-SP2-Debuginfo-Updates' [done]
Adding repository 'SLES11-SP2-Debuginfo-Updates' [done]
Adding repository 'SLES11-SP2-Debuginfo-Core' [done]
Adding repository 'SLES11-SP2-Debuginfo-Updates' [done]
Adding repository 'SLES11-SP2-Debuginfo-Updates' [done]
Adding repository 'SLES11-SP3-Debuginfo-Updates' [done]
Adding repository 'SLES11-SP3-Debuginfo-Updates' [done]
Adding repository 'SLES11-SP3-Debuginfo-Updates' [done]
All services have been refreshed.
Retrieving repository 'SLES11-SP3-Pool' metadata [done]
Building repository 'SLES11-SP3-Pool' cache [done]
```
5. Execute the below command to update the server

zypper update

6. Follow the on screen instruction to complete the update process.

7. Reboot the server

### Initial PXE Configuration

To configure a PXE (Preboot Execution Environment) boot server, two packages, the DHCP (Dynamic Host Configuration Protocol) server and tftp server are required. DHCP server is already installed in the previous step.

Follow the below steps to install and configure tftp server.

1. **Configuration of tftp server**
2. Log in to the VM created PXE boot Server using SSH
3. Search the package tftp server using command shown below

```bash
HANA-mgmtsrv01:~ # zypper se tftp
```

Reading installed packages...

<table>
<thead>
<tr>
<th>S</th>
<th>Name</th>
<th>Summary</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>atftp</td>
<td>Advanced TFTP Server and Client</td>
<td>package</td>
</tr>
<tr>
<td></td>
<td>atftp</td>
<td>Advanced TFTP Server and Client</td>
<td>srcpackage</td>
</tr>
<tr>
<td></td>
<td>tftp</td>
<td>Trivial File Transfer Protocol (TFTP)</td>
<td>package</td>
</tr>
<tr>
<td></td>
<td>tftp</td>
<td>Trivial File Transfer Protocol (TFTP)</td>
<td>srcpackage</td>
</tr>
<tr>
<td>i</td>
<td>yast2-tftp-server</td>
<td>Configuration of TFTP server</td>
<td>package</td>
</tr>
<tr>
<td>i</td>
<td>yast2-tftp-server</td>
<td>Configuration of TFTP server</td>
<td>srcpackage</td>
</tr>
</tbody>
</table>

4. **Install the tftp server**

```bash
HANA-mgmtsrv01:~ # zypper in tftp
```

Reading installed packages...

The following NEW package is going to be installed:

```
tftp
```

1 new package to install.

Overall download size: 42.0 KiB. After the operation, additional 81.0 KiB will be used.

Continue? [y/n/?] (y): y

Retrieving package tftp-0.48-101.31.27.x86_64 (1/1), 42.0 KiB (81.0 KiB unpacked)

Installing: tftp-0.48-101.31.27 [done]

5. **Configuration of the xinetd to respond to tftp requests**

```bash
# default: off
# description: tftp service is provided primarily for booting or when a \ 
# router need an upgrade. Most sites run this only on machines acting as 
# "boot servers".

service tftp {
    socket_type  = dgram
    protocol    = udp
    wait        = yes
    flags       = IPv6 IPv4
    user        = root
    server      = /usr/sbin/in.tftpd
    server_args = -s /tftpboot
}
```

6. To configure your TFTP server create a directory, which will be the base directory for Linux boot images and the PXE boot server configuration files.
mkdir /tftpboot
chmod 755 tftpboot

7. To make sure the TFTP servers can startup on subsequent reboots, execute the below command

chkconfig xinetd on
chkconfig tftp on
rcxinetd restart

Shutting down xinetd: (waiting for all children to terminate) done
Starting INST services. (xinetd) done

8. Make sure syslinux is installed,

rpm -qa syslinux
syslinux-3.82-8.10.23

9. Copy the pxelinux image on to the root directory of the tftp server

cp /usr/share/syslinux/pxelinux.0 /tftpboot/

10. PXELinux relies on the pxelinux.cfg directory to be in the root of the tftp directory for configuration.

mkdir /tftpboot/pxelinux.cfg

Configuration of the DHCP Server for PXE Boot

1. Activate the DHCP server to listen on eth1, which is configured for PXE boot VLAN 127

vi /etc/sysconfig/dhcpd
#
DHCPD_INTERFACE="eth1"

2. Get the MAC Address List for HANA-Boot vNIC for service Profiles created. Separate MAC address pool was created for HANA-Boot and assigned in the sequential order; follow the steps below to get MAC address for HANA-Boot.
   a. Log in to Cisco UCS Manager; click the LAN tab in the navigation pane.
   b. Select Pools > root > MAC pools > MAC Pool HANA-Boot
   c. Expand MAC Pool HANA-Boot
   d. Click on MAC Addresses tab on the right pane

   Figure 160. MAC Address for Service Profile

<table>
<thead>
<tr>
<th>ID</th>
<th>Assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC 00:25:05:1A:10:00</td>
<td>servHANA-01/VLAN127</td>
</tr>
<tr>
<td>MAC 00:25:05:1A:10:01</td>
<td>servHANA-02/VLAN127</td>
</tr>
<tr>
<td>MAC 00:25:05:1A:10:02</td>
<td>servHANA-03/VLAN127</td>
</tr>
<tr>
<td>MAC 00:25:05:1A:10:03</td>
<td>servHANA-04/VLAN127</td>
</tr>
<tr>
<td>MAC 00:25:05:1A:10:04</td>
<td>servHANA-05/VLAN127</td>
</tr>
<tr>
<td>MAC 00:25:05:1A:10:05</td>
<td>servHANA-06/VLAN127</td>
</tr>
</tbody>
</table>

   Note: The MAC address assigned to Service Profile in the sequential order

3. DHCP server requires ‘next-server’ directive to DHCP configuration file, this directive should have the IP address of the TFTP server i.e. (next-server 192.168.127.27;).

4. The second directive that needs to be added to DHCP configuration file is ‘filename’ and it should have the value of ‘pxelinux.0’ i.e. (filename “pxelinux.0”;) this will enable PXE booting.

5. To assign hostname to the server via DHCP use option host-name "<<hostname>>"

6. MAC Address configured for HANA-Boot in the Cisco UCS Service Profile would be reserved with an IP address for each server for PXE boot in the dhcp configuration.
Note: Below is an example of /etc/dhcpd.conf, VLAN ID 127 is used for PXE boot network. The PXE boot server IP address is 192.168.127.27, subnet 255.255.255.0. Assigned IP address for servers are 192.168.127.201-206.

```plaintext
# dhcpd.conf
# default-lease-time 14400;
 ddns-update-style none;
 ddns-updates off;
 filename "pxelinux.0";
 subnet 192.168.127.0 netmask 255.255.255.0 {
   group {
     next-server 192.168.127.27;
     filename "pxelinux.0";
     host server01b {
       hardware ethernet 00:25:B5:1A:10:00;
       fixed-address 192.168.127.201;
       option host-name cishana01;
     }
     host server02b {
       hardware ethernet 00:25:B5:1A:10:01;
       fixed-address 192.168.127.202;
       option host-name cishana02;
     }
     host server03b {
       hardware ethernet 00:25:B5:1A:10:02;
       fixed-address 192.168.127.203;
       option host-name cishana03;
     }
     host server04b {
       hardware ethernet 00:25:B5:1A:10:03;
       fixed-address 192.168.127.204;
       option host-name cishana04;
     }
     host server05b {
       hardware ethernet 00:25:B5:1A:10:04;
       fixed-address 192.168.127.205;
       option host-name cishana05;
     }
     host server06b {
       hardware ethernet 00:25:B5:1A:10:05;
       fixed-address 192.168.127.206;
       option host-name cishana06;
     }
   }
}
```

7. To make sure the DHCP servers can startup on subsequent reboots, execute the below command

```
chkconfig dhcpd on
```

8. Restart the dhcp service for new configuration to take effect

```
service dhcpcd restart
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shutting down ISC DHCPv4 4.x Server</td>
<td>done</td>
</tr>
<tr>
<td>Starting ISC DHCPv4 4.x Server [chroot]</td>
<td>done</td>
</tr>
</tbody>
</table>

**PXE Boot Preparation for SUSE OS Installation**

In order to use PXE boot server for OS installation follow the below steps:

1. Mount the SLES 11 SP3 ISO to temp directory

```
mount -o loop /NFS/software/SLES/SLE-11-SP3-SAP-DVD-x86_64-GM-DVD.iso /mnt
```

2. Create ISO image repository
3. Create a directory for SUSE installer

4. Copy two files “initrd” and “linux” from SLES 11 SP3 ISO

5. Create a text file that will hold the message which will be displayed to the user when PXE boot server is connected

6. Create a file called: “default” in the directory /tftpboot/pxelinux.cfg with similar syntax to the one shown below

```
# UCS PXE Boot Definition
DISPLAY ..../boot.msg
DEFAULT Install-SLES4SAP
PROMPT 1
TIMEOUT 50

LABEL Install-SLES4SAP
   KERNEL suse/linux-iso
   APPEND initrd=suse/initrd-iso
   install=nfs://192.168.127.11:/software/SLES/CD/?device=eth0
```

- PROMPT: This line allows user to choose a different booting method. The value of one allows the client to choose a different boot method.
- DEFAULT: This sets the default boot label.
- TIMEOUT: Indicates how long to wait at the “boot:” prompt until booting automatically, in units of 1/10 s.
- LABEL: This section defines a label called: “Install-SLES4SAP” so at the boot prompt when ‘Install-SLES4SAP’ is entered, it execute the commands related to the local label. Here Kernel image and initrd images are specified along with ISO location and the Ethernet device to use.

**PXE Boot Preparation for RHEL OS Installation**

In order to use PXE boot server for OS installation, complete the following steps:

1. Mount the RHEL 6.5 ISO to temp directory

2. Create ISO image repository

3. Create a directory for rhel installer

4. Copy two files “initrd” and “linux” RHEL 6.5 ISO

5. Create a text file that will hold the message, which will be displayed, to the user when PXE boot server is connected

6. Create a file called: “default” in the directory /tftpboot/pxelinux.cfg with similar syntax to the one shown below
# UCS PXE Boot Definition
DISPLAY ../boot.msg
DEFAULT Install-RHEL
PROMPT 1
TIMEOUT 50
#
LABEL Install-RHEL
   KERNEL rhel/vmlinuz-iso
   APPEND initrd= rhel/initrd-iso
install=nfs://192.168.127.11:/software/SLES/CD/?device=eth0

7. Mount the osmaster volume. Append the following line on /etc/fstab.

    nfspxe:/rhel_os_master /NFS/osmaster nfs defaults 0 0

8. Mount the osmaster volume on the pxe boot server

    mount /NFS/osmaster

Define the PXE Linux Configuration

PXE configuration file is required for each server. When the server boots up, it will get an IP from dhcp server based on dhcp configuration. When the IP address is assigned, the PXE boot environment will look for configuration file based on its boot IP. If the configuration file is missing “default” file will be used. To calculate the filename run “gethostip”, the output is a hex representation of the IP address will be configuration filename.

For example, to get hex for 192.1168.127.201

    gethostip 192.168.127.201
    192.168.127.201 192.168.127.201 C0A87FC9

The file name “C0A87FC9” contains the PXE boot configuration for server with IP 192.1168.127.201

Operating System Installation

After the PXE configuration is completed, proceed with the Operating System Installation.

Note: For the latest information on SAP HANA installation and OS customization requirement, see SAP HANA installation guide at http://www.saphana.com/

SUSE Linux Enterprise Server

The following procedure shows OS installation based on the PXE Boot Option.
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profiles > root > HANA-Server01
3. Click KVM Console
4. When the KVM Console is launched click Boot Server
5. If you using CD Click on Virtual Media > Activate Virtual Devices
   a. Select Accept this Session for Unencrypted Virtual Media Session then click Apply
   b. Click Virtual Media and Choose Map CD/DVD
   c. Click Browse to navigate ISO media location
   d. Click Map Device
6. For PXE Boot Installation, the “default” file is configured for OS installation. The IP address obtained from DHCP configured on the PXE Boot Server
7. Load the linux and initrd image from PXE server

8. Installation Process will start from the software directory specified in the “default” file from pxelinux.cfg
9. Agree to the License Terms, click Next
10. On the Disk Activation screen click Next
11. On the System Probing screen, it shows up error for No hard disks found, click OK since NFS volume is used for OS installation
12. Leave New Installation selected and click Next.
13. Select Appropriate Region and Time Zone. Click Next.

**Note:** SAP recommends setting the server time zone on all SAP HANA nodes to UTC.

14. Under Choose Scenario Keep Physical Machine (also for Fully Virtualized Guests) selected and click Next.
15. Click the Expert tab.
16. Click Partitioning.
17. In the Expert Partitioner screen, in the System View > Linux > Select NFS.

**Figure 166.** NFS Root Partition

18. Click Add.
19. Enter the IP address of the Filer <<var_node01_boot_lif_ip>>.
20. Enter the Remote Directory /suse_os_master.
21. Mount Point (local) enter /
22. Click OK
23. Click Accept
24. On the Installation Settings screen, click Software
25. Optionally uncheck GNOME Desktop Environment, if you don’t wish to use Graphical Desktop. This optional will reduce the size used for root Partition by 300 MB. Recommend to de-select the “GNOME Desktop Environment” package.
26. Check C/C++ Compiler and Tools Under Development
27. Check SAP HANA Server Base Under Primary Functions

Figure 168. SUSE Software Selection
28. Press OK and Accept.
29. On the Installation Settings screen Change Time Zone as per the requirement
30. On the Installation Settings screen click Default Runlevel
31. On the Set Default Runlevel screen select 3: Full multiuser with network and click OK
32. On the Installation Settings screen click Kdump
33. On the kdump Start-Up under Enable/Disable Kdump select Disable Kdump and click OK
34. Click and Install to perform the installation.
35. Wait for Installation to complete.
36. On the Finishing Basic Installation screen, for the initial reboot message click Stop

Figure 169. SUSE Installation Complete

37. Since Network boot is used, the bootloader will not be installed.
38. To create initrd image for PXE Boot environment follow the steps below
   a. Log into PXE Boot server using ssh
   b. Copy the initrd and vmlinux image from the system installed

   Note: Please check suse_os_master volume is mounted on the /NFS/osmaster

   ```
   cp /NFS/osmaster/boot/initrd-3.0.76-0.11-default /tftpboot/suse/
   cp /NFS/osmaster/boot/vmlinuz-3.0.76-0.11-default /tftpboot/suse/
   ```

39. Create new PXE Configuration file as described in the section Define the PXE Linux Configuration

   ```
   cd /tftpboot/pxelinux.cfg
   vi C0A87FC9
   
   # UCS PXE Boot Definition
   DISPLAY .../boot.msg
   DEFAULT SLES4SAP
   PROMPT 1
   TIMEOUT 50
   #
   LABEL SLES4SAP
   ```
40. Go back to KVM Console and Press OK to reboot the server
41. After reboot, system will continue the installation to customize the installed Operating System
42. Enter the Password for root User and Confirm Password, then click Next
43. Enter Hostname and Domain Name, uncheck Change Hostname via DHCP, then click Next
44. Under Network Configuration, keep Use Following Configuration selected
   a. Under General Network Settings Support for IPv6 protocol is enabled click Disable IPv6, on the
      Warning To apply this change, a reboot is needed Press OK
   b. Under Firewall → Firewall is enabled Click disable
   c. Keep the Network Interfaces configuration as default, as OS master image being created. IP
      address will be assigned after OS is deployed for the servers.
   d. Click on the VNC Remote Administration and select Allow Remote Administration. Click Finish
   e. Optional if there is proxy server required for Internet access Click on Proxy Configuration, check
      Enable Proxy. Enter the HTTP Proxy URL, HTTPS Proxy URL or based on proxy server
      configuration check Use the Same Proxy for All Protocols. If proxy server requires Authentication
      enter Proxy User Name and Proxy Password and Click Finish
45. Click Next to finish Network Configuration
46. Under Test Internet Connection Choose No, Skip This Test
47. For Network Service Configuration, choose default and Click Next
48. For User Authentication Method select default Local (/etc/passwd), additional methods can be done
   later if required.
49. Create New Local User, enter password and Confirm Password.
50. Release Notes, Click Next
51. Use Default Hardware Configuration, Click Next
52. Uncheck Clone This System for AutoYaST and Click Finish

Figure 170. OS Boot after SUSE Installation

53. Create Swap Partition in a file
   a. ssh to the os master on the PXE boot IP from PXE Boot Server
   b. Login as root and password
c. Create file for swap partition

```
-osmaster:~ # dd if=/dev/zero of=/swap-0001 bs=1M count=2048
2048+0 records in
2048+0 records out
2147483648 bytes (2.1 GB) copied, 3.64515 s, 589 MB/s
```

d. Set up a swap area in a file

```
osmaster:~ # mkswap /swap-0001
Setting up swapspace version 1, size = 2097148 KiB
no label, UUID=0f0f9606-dbe9-4301-9f65-293c3bab1346
```

e. To use swap file execute the below command

```
osmaster:~ # swapon /swap-0001
```

f. Verify if the swap partition is being used.

```
osmaster:~ # swapon -s
Filename Type Size Used Priority
swap-0001 file 2097148 0 -1
```

g. Add the below line to /etc/fstab for swap partition to be persistent after reboot

```
vi /etc/fstab

-swapon-0001 swap swap defaults 0 0
```

**Update OS Master**

To update the SUSE OS to the latest patch level, complete the following steps:

**Note:** This document assumes that the SUSE License key are available and registered username and password is available.

1. ssh to the os master on the PXE boot IP from PXE Boot Server
2. Login as root and password
3. Assign IP address to interface which can access Internet or Proxy Server
   In this example we use HANA-Admin vNIC to access internet
4. To configure the network interface on the OS, it is required to identify the mapping of the ethernet device on the OS to vNIC interface on the Cisco UCS.
5. From the OS execute the below command to get list of Ethernet device with MAC Address

```
-osmaster:~ # ifconfig -a|grep HWaddr
eth0 Link encap:Ethernet HWaddr 00:25:B5:1A:10:00
eth1 Link encap:Ethernet HWaddr 00:25:B5:00:0A:02
eth2 Link encap:Ethernet HWaddr 00:25:B5:00:0B:02
eth3 Link encap:Ethernet HWaddr 00:25:B5:00:0A:00
eth4 Link encap:Ethernet HWaddr 00:25:B5:00:0B:00
eth5 Link encap:Ethernet HWaddr 00:25:B5:00:0B:01
eth6 Link encap:Ethernet HWaddr 00:25:B5:00:0B:03
eth7 Link encap:Ethernet HWaddr 00:25:B5:00:0A:01
eth8 Link encap:Ethernet HWaddr 00:25:B5:00:0A:03
```

6. In Cisco UCS Manager, click the Servers tab in the navigation pane
7. Select Service Profiles > root > HANA-Server01 Expand by clicking on +
8. Click vNICs
9. On the Right pane list of the vNICs with MAC Address are listed.
10. Note the MAC Address of the HANA-Admin vNIC “00:25:B5:00:0A:03”
11. By comparing MAC Address on the OS and UCS, eth8 on OS will carry the VLAN for HANA-Admin
12. Go to network configuration directory and create a configuration for eth8

```
/etc/sysconfig/network
vi ifcfg-eth8
```

```
BOOTPROTO='static'
IPADDR='<<IP Address for HANA-Admin>>/24'
NAME='VIC Ethernet NIC'
STARTMODE='auto'
```

13. Add default gateway

```
cd /etc/sysconfig/network
d vi routes
default <<IP Address of default gateway>> - -
```

14. Add DNS IP if it’s required to access internet

```
v /etc/resolv.conf
vi
```

```
nameserver <<IP Address of DNS Server1>>
nameserver <<IP Address of DNS Server2>>
```

15. Restart network service for change to take effect

```
rcnetwork restart
```

16. Execute the below command to Register the SUSE

```
suse_register -i -r -n -a email=<<email_address>> -a regcode-sles=<<registration_code>>
```

17. After the registration, the entire repository will be updated

```
All services have been refreshed. 
Repository 'SLES-for-SAP-Applications 11.3.3-1.17' is up to date. 
All repositories have been refreshed. 
 Refreshing service 'nu_novell_com'.
Adding repository 'SLES11-SP3-Updates' [done]
Adding repository 'SLES11-SPxtras' [done]
Adding repository 'SLES11-SP1-Pool' [done]
Adding repository 'SLES11-SP2-Updates' [done]
Adding repository 'SLE11-HAE-SP3-Pool' [done]
Adding repository 'SLE11-HAE-SP3-Updates' [done]
Adding repository 'SLE11-SP3-SAP-Updates' [done]
Adding repository 'SLE11-SP3-Pool' [done]
Adding repository 'SLE11-SP2-Extension-Store' [done]
Adding repository 'SLE11-SP3-SAP-Pool' [done]
Adding repository 'SLE11-SP3-Debuginfo-Pool' [done]
```
Adding repository 'SLE11-SP2-WebYaST-1.3-Pool' [done]
Adding repository 'SLE11-SP1-Debuginfo-Updates' [done]
Adding repository 'SLES11-SP2-Core' [done]
Adding repository 'SLES11-SP1-Updates' [done]
Adding repository 'SLES11-SP3-Extension-Store' [done]
Adding repository 'SLE11-SP2-WebYaST-1.3-Updates' [done]
Adding repository 'SLE11-SP1-Debuginfo-Pool' [done]
Adding repository 'SLE11-SP3-Debuginfo-Updates' [done]
Adding repository 'SLE11-SP2-Debuginfo-Core' [done]
Adding repository 'SLE11-SP2-Debuginfo-Updates' [done]
All services have been refreshed.
Repository 'SLES-for-SAP-Applications 11.3.3-1.17' is up to date.
Retrieving repository 'SLE11-HAE-SP3-Pool' metadata [done]
Building repository 'SLE11-HAE-SP3-Pool' cache [done]
Retrieving repository 'SLE11-HAE-SP3-Updates' metadata [done]
Building repository 'SLE11-HAE-SP3-Updates' cache [done]
Retrieving repository 'SLE11-SP2-WebYaST-1.3-Pool' metadata [done]
Building repository 'SLE11-SP2-WebYaST-1.3-Pool' cache [done]
Retrieving repository 'SLE11-SP2-WebYaST-1.3-Updates' metadata [done]
Building repository 'SLE11-SP2-WebYaST-1.3-Updates' cache [done]
Retrieving repository 'SLE11-SP3-SAP-Pool' metadata [done]
Building repository 'SLE11-SP3-SAP-Pool' cache [done]
Retrieving repository 'SLE11-SP3-SAP-Updates' metadata [done]
Building repository 'SLE11-SP3-SAP-Updates' cache [done]
Retrieving repository 'SLES11-SP3-Pool' metadata [done]
Building repository 'SLES11-SP3-Pool' cache [done]
Retrieving repository 'SLES11-SP3-Updates' metadata [done]
Building repository 'SLES11-SP3-Updates' cache [done]
All repositories have been refreshed.
Registration finished successfully
18. Execute the below command to update the server

zypper update

19. Follow the on screen instruction to complete the update process.
20. Do not reboot the server, until initrd and vmlinuz images are updated.
21. To update initrd image for PXE Boot environment follow the steps below
   a. Log into PXE Boot server using ssh
   b. Copy the initrd and vmlinuz image from the system installed

   **Note:** Please check suse_os_master volume is mounted on the /NFS/osmaster

   cp /NFS/osmaster/boot/initrd-3.0.101-0.40-default /tftpboot/suse/initrd-sles4sap
   cp /NFS/osmaster/boot/vmlinuz-3.0.101-0.40-default /tftpboot/suse/vmlinuz-sles4sap

22. Update the PXE Configuration file

   vi /tftpboot/pxelinux.cfg/C0A87FC9

   # UCS PXE Boot Definition
   DISPLAY ../boot.msg
   DEFAULT SLES4SAP
   PROMPT 1
   TIMEOUT 50
   #
   LABEL SLES4SAP
   KERNEL suse/vmlinuz-sles4sap
   APPEND initrd=suse/initrd-sles4sap rw rootdev=192.168.127.11:/suse_os_master
   ip=dhcp

23. ssh to the os master server with PXE boot IP (192.168.127.201) from PXE Boot Server
24. Enter “reboot”

**Install Cisco enic Driver**

This procedure describes how to download the Cisco UCS Drivers ISO bundle, which contains most Cisco UCS Virtual Interface Card drivers.
1. In a web browser, navigate to http://www.cisco.com
2. Under Support, click All Downloads.
3. In the product selector, click Products, then click Server - Unified Computing
4. If prompted, enter your Cisco.com username and password to log in.

**Note:** You must be signed in to download Cisco Unified Computing System (UCS) drivers.

6. Click Cisco UCS B-Series Blade Server Software
7. Click on Cisco Unified Computing System (UCS) Drivers

**Note:** The latest release version is selected by default. This document is built on Version 2.2(3)

8. Click on 2.2(3) Version
9. Download ISO image of Cisco UCS-related drivers
10. Choose your download method and follow the prompts to complete your driver download.
11. After the download complete browse the ISO to Cisco ucs-bxxx-drivers.2.2.3/Linux/Network/Cisco/M81KR/SLES/SLES11.3 and copy cisco-enic-kmp-default-2.1.1.75_3.0.76_0.11-0.x86_64.rpm to PXE Boot Server /NFS/software/SLES
12. ssh to PXE Boot Server as root
13. Copy the rpm package to OS Master

```
scp /NFS/software/SLES/cisco-enic-kmp-default-2.1.1.75_3.0.76_0.11-0.x86_64.rpm
192.168.127.201:/tmp/cisco-enic-kmp-default-2.1.1.75_3.0.76_0.11-0.x86_64.rpm
```

14. ssh to the os master on the PXE boot IP from PXE Boot Server as root
15. Update the enic driver

```
rpm -Uvh /tmp/cisco-enic-kmp-default-2.1.1.75_3.0.76_0.11-0.x86_64.rpm
Preparing... #.......................................................... [100%]
1: cisco-enic-kmp-default #........................................... [100%]
```

Kernel image: /boot/vmlinuz-3.0.101-0.40-default
Initrd image: /boot/initrd-3.0.101-0.40-default
KMS drivers: mgag200
Kernel Modules: hwmon thermal_sys thermal_processor fanei scsi_mod scsi_dh scsi_dh_alua
csci dh_emc scsi dh_hp_sw scsi dh rdac sunrpc nfs acl auth rpcgss fscache lockd nfs
syscopyarea i2c-core sysfillrect sysimgblt i2c-algo-bit drm drm_kms_helper ttm mgag200
usb-common uasbcore ohci-hcd uhci-hcd ehci-hcd xhci-hcd hid usbhid af_packet enic
crc-t10dif sd_mod
Features: acpi kms usb network nfs resume.userspace resume.kernel
45343 blocks

16. Update initrd image for PXE Boot environment follow the steps below:
   a. Log into PXE Boot server using ssh
   b. Copy the initrd and vmlinuz image from the system installed

**Note:** Please check suse_os_master volume is mounted on the /NFS/osmaster.

```
cp /NFS/osmaster/boot/initrd-3.0.101-0.40-default /tftpboot/suse/initrd-sles4sap
```

17. ssh to the os master server with PXE boot IP (192.168.127.201) from PXE Boot Server
18. Enter “reboot”

**Operating System Configuration for SAP HANA**

SAP HANA running on a SLES 11 SP3 system requires configuration changes on the OS level, to achieve best performance and a stable system.

**Disabled Transparent Hugepages**

With SLES11 SP3 the usage of transparent hugepages (THP) is generally activated for the Linux kernel. The THP allows the handling of multiple pages as hugepages reducing the “translation look aside buffer” footprint (TLB), in situations where it might be useful. Due to the special manner of SAP HANA’s memory management, the usage of THP may lead to hanging situations and performance degradations.
To disable the usage of transparent hugepages set the kernel settings at runtime:

```
echo never > /sys/kernel/mm/transparent_hugepage/enabled
```

There is no need to shut down the database to apply this configuration. This setting is then valid until the next system start. To make this option persistent, integrate this command line within your system boot scripts (e.g. `/etc/init.d/after.local`)

**Configured C-States for Lower Latency in Linux**

The Linux Kernel 3.0 includes a new cpuidle driver for recent Intel CPUs: intel_idle. This driver leads to a different behavior in C-states switching. The normal operating state is C0, when the processor is put to a higher C state, it will save power. But for low latency applications, the additional time needed to start the execution of the code again will cause performance degradations.

Therefore it is necessary to edit the boot loader configuration. The location of the boot loader configuration file is usually `/etc/sysconfig/bootloader`.

1. Edit this file and append the following value to the "DEFAULT_APPEND" parameter value:

   ```
   intel_idle.max_cstate=0
   ```

2. With this a persistent change has been done for potential kernel upgrades and bootloader upgrades. For immediate configuration change, it is also necessary to append this parameter in the kernel command line of your current active bootloader file which is located on the PXE server under `/tftpboot/pxelinux.cfg`

3. Append the intel_idle value mentioned above only to the operational kernel's parameter line. The C states are disabled in BIOS but to be sure the C states are not used set the following parameter in addition to the previous one:

   ```
   processor.max_cstate=0
   ```

4. The CPU speed must be set to performance for SAP HANA so that all Cores run all time with highest frequency.

   ```
   /usr/bin/cpupower frequency-set -g performance 2>&1
   ```

5. To make this option persistent, integrate this command line within your system boot scripts (e.g. `/etc/init.d/after.local`)

**Configured Swappiness**

Set swappiness to 30 to avoid swapping

```
Echo 30 > /proc/sys/vm/swappiness
```

**RSS/RPS Settings on the OS**

To get use of the RSS setting in the Adapter policy it is required to configure the Receive Side Packet Steering (RPS) on the OS level.

RPS distributes the load of received packet processing across multiple CPUs. Problem statement: Protocol processing done in the NAPI context for received packets is serialized per device queue and becomes a bottleneck under high packet load. This substantially limits pps that can be achieved on a single queue NIC and provides no scaling with multiple cores.

The best performance resulted with the following setting for Ivy-Bridge Processor:

```
echo 7fff > /sys/class/net/${ethernet_device}/queues/rx-0/rps_cpus
```

Where `*${Ethernet_device}*` is to replace with all eth devices you need high throughput.

To make this option persistent, integrate this command line within your system boot scripts (e.g. `/etc/init.d/after.local`) Optimization setting on the OS Master

To configure the OS optimization settings mentioned above on the OS Master follow the steps below.

1. ssh to the os master on the PXE boot IP from PXE Boot Server
2. Login as root and password
3. Create a file `/etc/init.d/after.local`
vi /etc/init.d/after.local

#!/bin/bash
# (c) Cisco Systems Inc. 2014

# Performance Settings
#
# echo "Setting the CPU Speed to PERFORMANCE for SAP HANA" SAP Note 1824819
/usr/bin/cpupower frequency-set -g performance

echo never > /sys/kernel/mm/transparent_hugepage/enabled   # from kernel >= 3.0.80.7 THP
can be enabled again
. /etc/rc.status

# echo "Enable the Network Power Settings for SAP HANA"

# echo 7fff > /sys/class/net/eth0/queues/rx-0/rps_CPUs
# echo 7fff > /sys/class/net/eth1/queues/rx-0/rps_CPUs
# echo 7fff > /sys/class/net/eth2/queues/rx-0/rps_CPUs
# echo 7fff > /sys/class/net/eth3/queues/rx-0/rps_CPUs
# echo 7fff > /sys/class/net/eth4/queues/rx-0/rps_CPUs
# echo 7fff > /sys/class/net/eth5/queues/rx-0/rps_CPUs
# echo 7fff > /sys/class/net/eth6/queues/rx-0/rps_CPUs
# echo 7fff > /sys/class/net/eth7/queues/rx-0/rps_CPUs

# set sappiness to 30 to aviod swapping
# echo "Set swappiness to 30 to avoid swapping"
# echo 30 > /proc/sys/vm/swappiness
. /etc/rc.status

4. Add the following lines to /etc/sysctl.conf

```bash
# SAP Note 1275776
vm.max_map_count = 2000000
fs.file-max = 20000000
fs.aio-max-nr = 196608
vm.memory_failure_early_kill = 1
net.ipv4.tcp_slow_start_after_idle = 0
#
# NetApp TR-4290
#
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.core.rmem_default = 262144
net.core.wmem_default = 262144
net.core.optmem_max = 16777216
net.core.netdev_max_backlog = 300000
net.ipv4.tcp_rmem = 65536 262144 16777216
net.ipv4.tcp_wmem = 65536 262144 16777216
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp Moderate rcvbuf = 1
net.ipv4.tcp_windowscaling = 1
net.ipv4.tcp_timestamps = 1
sunrpc.tcp_slot_table_entries = 128
#
```

# Memory Page Cache Linit Feature SAP Note 1557506
vm.pagecache_limit_mb = 4096
vm.pagecache_limit Ignore_dirty = 1

5. Update the PXE Configuration file on the PXE Boot server

vi /tftpboot/pxelinux.cfg/C0A87FC9

# UCS PXE Boot Definition
DISPLAY .../boot.msg
DEFAULT SLES4SAP
PROMPT 1
TIMEOUT 50
#
LABEL SLES4SAP
```bash
        KERNEL suse/vmlinuz-sles4sap
        APPEND initrd=suse/initrd-sles4sap rw rootdev=192.168.127.11:/suse_os_master
    intel_idle.max_cstate=0 processor.max_cstate=0 ip=dhcp
```
Cloning OS Volumes
After OS Master image is created, prepare the os image for cloning.

Clean UP Master OS Image
1. ssh to osmaster
2. Remove the SUSE Registration information
   **Note:** This step is required for creating master image without the registration information. After OS deployment register each server with SUSE for OS support.

3. List the zypper service with zypper ls

<table>
<thead>
<tr>
<th>#</th>
<th>Alias</th>
<th>Name</th>
<th>Enabled</th>
<th>Refresh</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>nu_novell_com</td>
<td>nu_novell_com</td>
<td>Yes</td>
<td>No</td>
<td>ris</td>
</tr>
<tr>
<td>2</td>
<td>SLES-for-SAP-Applications 11.3.3-1.17</td>
<td>SLES-for-SAP-Applications 11.3.3-1.17</td>
<td>Yes</td>
<td>yast2</td>
<td></td>
</tr>
</tbody>
</table>

4. Remove the Update Service

   ```
   zypper removeservice nu_novell_com
   ```

   Removing service 'nu_novell_com':
   Removing repository 'SLE11-HAE-SP3-Pool' [done]
   Removing repository 'SLE11-HAE-SP3-Updates' [done]
   Removing repository 'SLE11-SP1-Debuginfo-Pool' [done]
   Removing repository 'SLE11-SP1-Debuginfo-Updates' [done]
   Removing repository 'SLE11-SP2-Debuginfo-Core' [done]
   Removing repository 'SLE11-SP2-Debuginfo-Updates' [done]
   Removing repository 'SLE11-SP2-WebYaST-1.3-Pool' [done]
   Removing repository 'SLE11-SP2-WebYaST-1.3-Updates' [done]
   Removing repository 'SLE11-SP3-Debuginfo-Pool' [done]
   Removing repository 'SLE11-SP3-Debuginfo-Updates' [done]
   Removing repository 'SLE11-SP3-SAP-Pool' [done]
   Removing repository 'SLE11-SP3-SAP-Updates' [done]
   Removing repository 'SLES11-Extras' [done]
   Removing repository 'SLES11-SP1-Pool' [done]
   Removing repository 'SLES11-SP1-Updates' [done]
   Removing repository 'SLES11-SP2-Core' [done]
   Removing repository 'SLES11-SP2-Extension-Store' [done]
   Removing repository 'SLES11-SP2-Updates' [done]
   Removing repository 'SLES11-SP3-Extension-Store' [done]
   Removing repository 'SLES11-SP3-Pool' [done]
   Removing repository 'SLES11-SP3-Updates' [done]
   Service 'nu_novell_com' has been removed.

5. Remove registration credentials

   ```
   cishana01:~ # rm /etc/zypp/credentials.d/NCCredentials
   cishana01:~ # rm /var/cache/SuseRegister/lastzmdconfig.cache
   ```

6. Shutdown the OS Master Server by issuing "halt" command

7. Log into PXE Boot server using ssh

   **Note:** Please check suse_os_master volume is mounted on the /NFS/osmaster

8. Clear the fstab entry

   ```
   vi /NFS/osmaster/etc/fstab
   ```

   delete the entry

   ```
   192.168.127.11:/suse_os_master /          nfs defaults 0 0
   ```

9. Clear the System logs

   ```
   rm /NFS/osmaster/var/log/* -r
   ```
10. Clear the Ethernet Persistent network information
   cat /dev/null > /NFS/osmaster/etc/udev/rules.d/70-persistent-net.rules

11. Remove any Ethernet configuration file except eth0
   rm /NFS/osmaster/etc/sysconfig/network/ifcfg-eth<<1-7>>

12. Remove default gateway
   rm /NFS/osmaster/etc/sysconfig/network/routes

13. Shut the OS master by executing “halt”

**Storage Clone of OS Volume**
To clone the os master image to new host complete the following steps:
1. Log in to Storage shell
2. Create a Clone of OS master volume

   ```
   volume clone create -flexclone server01 -parent-volume suse_os_master -vserver infra_vs1
   -junction-path /server01 -space-guarantee none
   ```

3. Split the volume from OS master volume

   ```
   fas8040-cluster:/> volume clone split start -flexclone server01
   Warning: Are you sure you want to split clone volume server01 in Vserver infra_vs1 ? {y|n}: y
   [Job 1372] Job is queued: Split server01.
   ```

4. Check for status of Clone split

   ```
   fas8040-cluster:/> volume clone split status -flexclone server01
   Inodes              Blocks
   --------------------- ---------------------
   Vserver   FlexClone      Processed      Total    Scanned    Updated % Complete
   --------- ------------- ---------- ---------- ---------- ---------- ----------
   infra_vs1  server01          149558     253365     541092     538390         59
   ```

5. When the clone split is completed

   ```
   fas8040-cluster:/> volume clone split status -flexclone server01
   There are no entries matching your query.
   ```

6. Repeat the steps 2-3 for each server to deploy OS image.

**PXE Configuration for Additional Server**
The PXE boot environment will look for configuration file based on its boot IP assigned through DHCP.
1. To calculate the filename run “gethostip”, the output is a hex representation of the IP address will be
   configuration filename

   ```
   gethostip 192.168.127.201
   192.168.127.201 192.168.127.201 C0A87FC9
   ```

2. The file name “C0A87FC9” contains the PXE boot configuration for server with IP 192.168.127.201
   a. ssh to PXE boot server
   b. Go to PXE boot configuration directory

   ```
   cd /tftpboot/pxelinux.cfg/
   ```

   c. Create a configuration file for each server

   ```
   vi C0A87FC9
   ```

   # UCS PXE Boot Definition
   DISPLAY ../boot.msg
   DEFAULT SLES4SAP
   PROMPT 1
   TIMEOUT 50
   #
   LABEL SLES4SAP
   KERNEL suse/vmlinux-sles4sap
   APPEND initrd=suse/initrd-sles4sap rw rootdev=192.168.127.11:/server01
   intel_idle.max_cstate=0 processor.max_cstate=0 ip=dhcp
   ```

   d. Repeat the previous step for each server

Example: PXE Boot configuration file for server with dhcp ip 192.168.201.202
Boot the Server
1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root > Service Profiles.
3. Expand the tree and Right-click Service Template HANA-Server02 and select Boot Server

Post Installation OS Customization
After the OS is deployed from the Master image, customization is required for each server.

Hostnames
The operating system must be configured such a way that the short name of the server is displayed for the command 'hostname' and Full Qualified Host Name is displayed with the command 'hostname –d'

ssh to the Server to PXE boot IP from PXE Boot Server
1. Login as root and password
2. Edit the Hostname
   vi /etc/HOSTNAME
   <<hostname>>.<<Domain Name>>

IP Address
Assign the IP address to each interface
1. ssh to the Server on the PXE boot IP from PXE Boot Server
2. Login as root and password
3. To configure the network interface on the OS, it is required to identify the mapping of the ethernet device on the OS to vNIC interface on the Cisco UCS. From the OS execute the below command to get list of Ethernet device with MAC Address
   ifconfig -a | grep HWaddr

   eth0  Link encap:Ethernet  HWaddr 00:25:B5:1A:10:00
   eth1  Link encap:Ethernet  HWaddr 00:25:B5:00:0A:02
   eth2  Link encap:Ethernet  HWaddr 00:25:B5:00:0B:02
   eth3  Link encap:Ethernet  HWaddr 00:25:B5:00:0A:00
   eth4  Link encap:Ethernet  HWaddr 00:25:B5:00:0B:00
   eth5  Link encap:Ethernet  HWaddr 00:25:B5:00:0B:01
   eth6  Link encap:Ethernet  HWaddr 00:25:B5:00:0B:03
   eth7  Link encap:Ethernet  HWaddr 00:25:B5:00:0A:01
   eth8  Link encap:Ethernet  HWaddr 00:25:B5:00:0A:03

4. In Cisco UCS Manager, click the Servers tab in the navigation pane
5. Select Service Profiles > root > HANA-Server01 Expand by clicking on +
6. Click vNICs
7. On the right pane list of the vNICs with MAC Address are listed.
8. Note the MAC Address of the HANA-Admin vNIC “00:25:B5:00:0A:03”

9. By comparing MAC Address on the OS and Cisco UCS, eth8 on OS will carry the VLAN for HANA-Admin

10. Go to network configuration directory and create a configuration for eth8

```
/etc/sysconfig/network
vi ifcfg-eth8
##
# HANA-Admin Network
##
BOOTPROTO='static'
IPADDR='<<IP Address for HANA-Admin>>/24'
MTU='<<9000 or 1500>>'
NAME='VIC Ethernet NIC'
STARTMODE='auto'
```

11. Repeat the steps 8 to 10 for each vNIC interface

12. Add default gateway

```
cd /etc/sysconfig/network
vi routes
default <<IP Address of default gateway>> - -
```

**Network Time**

It is important that the time on all components used for SAP HANA must be in sync. The configuration of NTP is important and configured on all systems.

```
vi /etc/ntp.conf
server <NTP-SERVER IP>
fudge <NTP-SERVER IP> stratum 10
keys /etc/ntp.keys
trustedkey 1
```

**DNS**

Domain Name Service configuration must be done based on the local requirements.

**Configuration Example**

```
vi /etc/resolv.conf
nameserver <<IP Address of DNS Server1>>
nameserver <<IP Address of DNS Server2>>
```
**HOSTS**

For SAP HANA Scale-Out system all nodes should be able to resolve Internal network IP address, below is an example of 8 node host file with all the network defined in the /etc/hosts file

```plaintext
# cishana01:- # cat /etc/hosts
#
# This file describes a number of hostname-to-address mappings for the TCP/IP subsystem. It is mostly used at boot time, when no name servers are running. On small systems, this file can be used instead of a "named" name server.
#
# Syntax:
# IP-Address  Full-Qualified-Hostname  Short-Hostname
#
127.0.0.1   localhost

# special IPv6 addresses
::1   localhost ipv6-localhost ipv6-loopback
fe00::0   ipv6-localnet
ff00::0   ipv6-mcastprefix
ff02::1   ipv6-allnodes
ff02::2   ipv6-allrouters
ff02::3   ipv6-allhosts

## NFS Storage
172.29.110.12   lifdata01
172.29.110.13   lifdata02
192.168.127.13   nfssap

## Internal Network
172.29.220.201   cishana01.ciscolab.local  cishana01
172.29.220.202   cishana02.ciscolab.local  cishana02
172.29.220.203   cishana03.ciscolab.local  cishana03
172.29.220.204   cishana04.ciscolab.local  cishana04
172.29.220.205   cishana05.ciscolab.local  cishana05
172.29.220.206   cishana06.ciscolab.local  cishana06
172.29.220.207   cishana07.ciscolab.local  cishana07
172.29.220.208   cishana08.ciscolab.local  cishana08

## Storage Network
172.29.110.201   cishana01s.ciscolab.local  cishana01s
172.29.110.202   cishana02s.ciscolab.local  cishana02s
172.29.110.203   cishana03s.ciscolab.local  cishana03s
172.29.110.204   cishana04s.ciscolab.local  cishana04s
172.29.110.205   cishana05s.ciscolab.local  cishana05s
172.29.110.206   cishana06s.ciscolab.local  cishana06s
172.29.110.207   cishana07s.ciscolab.local  cishana07s
172.29.110.208   cishana08s.ciscolab.local  cishana08s

## Client Network
172.29.222.201   cishana01c.ciscolab.local  cishana01c
172.29.222.202   cishana02c.ciscolab.local  cishana02c
172.29.222.203   cishana03c.ciscolab.local  cishana03c
172.29.222.204   cishana04c.ciscolab.local  cishana04c
172.29.222.205   cishana05c.ciscolab.local  cishana05c
172.29.222.206   cishana06c.ciscolab.local  cishana06c
172.29.222.207   cishana07c.ciscolab.local  cishana07c
172.29.222.208   cishana08c.ciscolab.local  cishana08c

## AppServer Network
172.29.223.201   cishana01a.ciscolab.local  cishana01a
172.29.223.202   cishana02a.ciscolab.local  cishana02a
```

SSH Keys

The SSH Keys must be exchanged between all nodes in a SAP HANA Scale-Out system for user ‘root’ and user <SID>adm.

1. Generate the rsa public key by executing the command `ssh-keygen -b 2048`

   ```bash
   cishana01:~ # ssh-keygen -b 2048
   ```
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
The key's randomart image is:
++-[ RSA 2048]----+
| . o               |
| . + o...          |
| S . +=.           |
| E . ...=          |
| . . + . oo+       |
| . o . o oo        |
| . . . .           |
+=-[MD5]----------+

2. The SSH Keys must be exchanged between all nodes in a SAP HANA Scale-Out system for user 'root' and user

3. Exchange the rsa public key by executing the below command from First server to rest of the servers in the scale-out system.
   “ssh-copy-id -i /root/.ssh/id_rsa.pub cishana02”

   cishana01/ # ssh-copy-id -i /root/.ssh/id_rsa.pub cishana02
   The authenticity of host 'cishana02 (172.29.220.202)' can't be established.
   Are you sure you want to continue connecting (yes/no)? yes
   Password:
   Number of key(s) added: 1
   Now try logging into the machine, with: "ssh 'cishana02'"
   and check to make sure that only the key(s) you wanted were added.

4. Repeat the steps 1-3 for all the servers in the single SID HANA system

(Optional) Syslog
For a centralized monitoring of all SAP HANA nodes, it is recommended that syslog-ng is configured to forward all messages to a central syslog server
Change the syslog-ng.conf file as shown below

vi /etc/syslog-ng/syslog-ng.conf
...
...
# Enable this and adopt IP to send log messages to a log server.
# destination logserver1 { udp("SYSLOG-Server IP"> port(SYSLOG-Server PORT)); };
log { source(src); destination(logserver1); };
destination logserver2 { udp("SYSLOG-Server IP"> port(SYSLOG-Server PORT)); };
log { source(src); destination(logserver2); };

Restart the syslog daemon
/etc/init.d/syslog restart
Red Hat Enterprise Linux

The following procedure show the OS installation based on the PXE Boot Option.

**Note:** Use the SAP HANA installation Guides for OS customization requirement

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profiles > root > HANA-Server01
3. Click KVM Console
4. When the KVM Console is launched click Boot Server

5. If you using CD click Virtual Media > Activate Virtual Devices
   a. Select Accept this Session for Unencrypted Virtual Media Session then click Apply
   b. Click Virtual Media and Choose Map CD/DVD
   c. Click Browse to navigate ISO media location
   d. Click Map Device

6. For PXE Boot Installation the default file configured for install will be get the IP address from DHCP configured on the PXE Boot Server

7. Load the linux and initrd image from PXE server
8. Choose Language and click OK
9. Choose Keyboard layout and click OK
10. Choose NFS directory for PXE boot, click OK

Figure 175. RHEL NFS Installation Media
11. Choose eth0 for Networking Device. Click OK

**Figure 176.** RHEL NFS Installation Media Ethernet Selection

12. Configure DHCP for IPv4. Click OK

**Figure 177.** RHEL NFS Installation Media Ethernet Configuration

13. Enter the IP of NFS server and Directory for CD repository. Click OK
14. Click Next to Begin the Installation

**Figure 179.** RHEL Installation screen
15. Select the ‘Basic Storage Devices’ from the menu and click ‘Next’
16. Install on the Local Storage Device
17. Enter the Hostname as osmaster.<domain_name>, Click Next
18. Select the appropriate Time Zone and click ‘Next’
19. Enter the root password and confirm. Click Next
20. Select ‘Use All Space’ and click ‘Next’
21. Use the Default Disk Layout and click Next

Figure 180. RHEL Disk Layout

<table>
<thead>
<tr>
<th>Device</th>
<th>Size (MB)</th>
<th>Mount Point/RAID/Volume</th>
<th>Type</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>LVM Volume Groups</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vg_osmaster</td>
<td>285600</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lv_root</td>
<td>51200</td>
<td>/</td>
<td>ext4</td>
<td></td>
</tr>
<tr>
<td>lv_home</td>
<td>230304</td>
<td>/home</td>
<td>ext4</td>
<td></td>
</tr>
<tr>
<td>lv_swap</td>
<td>4096</td>
<td></td>
<td>swap</td>
<td></td>
</tr>
<tr>
<td>Hard Drives</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sda /dev/sda</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sda1</td>
<td>500</td>
<td>/boot</td>
<td>ext4</td>
<td></td>
</tr>
<tr>
<td>sda2</td>
<td>285601</td>
<td>vg_osmaster</td>
<td>physical volume (LVM)</td>
<td></td>
</tr>
<tr>
<td>sdb /dev/sdb</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Free</td>
<td>286095</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

22. Click ‘Next’ to proceed with the next step of the installation
23. Select the installation mode as ‘Minimal and click ‘Next’
24. The installer starts the installation process and wait until it is completed.
25. When the installation is completed the server requires a reboot. Click Reboot
### 26. Log in to the newly installed system as root

27. Edit the file `/etc/ntp.conf` to reflect the appropriate ntp servers for the region and start the ntp service

```bash
service ntpd stop
ntpdate ntp.example.com
service ntpd start
chkconfig ntpd on
chkconfig ntpdate on
```

### 28. Updating the RedHat system

In order to patch the system, the repository must be updated. Note that the installed system doesn’t include any update information. In order to patch the Redhat System, it must be registered and attached to a valid.

Subscription. The following line will register the installation and update the repository information.

```
[root@osmaster ~]# subscription-manager register --username <<username>> --password <<password>> --force --auto-attach
```

### 29. Update only the OS kernel and firmware packages to the latest release that appeared in RHEL 6.5.

According to SAP Note 2013638 - SAP HANA DB: Recommended OS settings for RHEL 6.5 the system must not be updated to RHEL 6.6. SAP HANA is currently certified for RHEL 6.5 only. To lock the kernel version to the last available kernel of the 2.6.32-431 series you need the yum-versionlock plugin

```
[root@osmaster ~]#yum -y install yum-versionlock
```

### 30. Configure the plugin with adding an entry in the appropriate configuration file:

```
[root@osmaster ~]# echo kernel-2.6.32-431.* > /etc/yum/pluginconf.d/versionlock.list
[root@osmaster ~]# echo kernel-firmware-2.6.32-431.* >> /etc/yum/pluginconf.d/versionlock.list
```

### 31. Only security updates may be applied. Install the yum-security plugin:

```
[root@osmaster ~]# yum -y install yum-security
```
32. Depending on the repository configuration nss-softokn-freebl can be updated during the security update process. Check for this with:

```
[root@osmaster -]# yum versionlock nss-softokn-freebl nss-softokn
```

33. Apply the security updates. Typically, the kernel is updated as well:

```
[root@osmaster -]# yum --security update
```

34. The firmware package should be in sync with the kernel revision. Install it with:

```
[root@osmaster -]# yum -y update kernel kernel-firmware
```

35. Reboot the machine and use the new kernel:

```
[root@osmaster -]# yum -y groupinstall base
```

36. Install the base package group

```
[root@osmaster -]# yum -y groupinstall base
```

37. Install the base package group

```
[root@osmaster -]# yum install gtk2 libicu xulrunner ntp sudo tcsh libssh2 \expect cairo graphviz iptraf krb5-workstation krb5-libs.i686 nfs-utils lm_sensors rsyslog compat-sap-c++ openssl1098e openssl1 PackageKit-gtk-module libcanberra-gtk2 libtool-ltdl xauth compat-libstdc++-33 numacl
```

38. Install dependencies in accordance with the SAP HANA Server Installation and Update Guide and the numacl package if the benchmark HWCCT is to be used

```
[root@osmaster -]# yum install gnome-utils smbclient which parted
```

39. Install SELinux

```
[root@osmaster -]# vi /etc/sysconfig/selinux
```

```
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:    
#     enforcing - SELinux security policy is enforced.    
#     permissive - SELinux prints warnings instead of enforcing.    
#     disabled - No SELinux policy is loaded.    
SELINUX=disabled

# SELINUXTYPE= can take one of these two values:    
#     targeted - Targeted processes are protected,    
#     mls - Multi Level Security protection.    
SELINUXTYPE=targeted
```

39. Compatsap-c++: Install the most important package compat-sap-c++ from the RHEL for SAP HANA

```
[root@osmaster -]#rpm -ivh compat-sap-c++-4.7.2-10.el6_5.x86_64.rpm
```

40. Tuned SAP HANA Profile

```
[root@osmaster -]# rpm -ivh tuned-0.2.19-13.el6_6.1.noarch.rpm
```

```
[root@osmaster -]# rpm -ivh tuned-profiles-sap-hana-0.2.19-13.el6_6.1.noarch.rpm
```

```
[root@osmaster -]# tuned-adm profile sap-hana
```

41. Sysctl.conf: The following parameters must be set in /etc/sysctl.conf.

```
# Parameters for HANA
net.ipv4.tcp_slow_start_after_idle=0
net.ipv4.conf.all.rp_filter=0
net.ipv4.ip_local_port_range=40000 61000
net.ipv4.neigh.default.gc_thresh1=256
net.ipv4.neigh.default.gc_thresh2=1024
net.ipv4.neigh.default.gc_thresh3=4096
net.ipv6.neigh.default.gc_thresh1=256
net.ipv6.neigh.default.gc_thresh2=1024
net.ipv6.neigh.default.gc_thresh3=4096
kernel.shmmax=137438953472
kernel.shmall=33554432
# Next line modified for SAP HANA Database on 2014.11.05_18.49.07
kernel.shmmin=524288
kernel.msgmni=32768
```

```
[root@osmaster -]# tuned-adm profile sap-hana
```
43. Add the following line into /etc/modprobe.d/sunrpc-local.conf, Create the file, if it does not exist.

```
sunrpc.tcp_max_slot_table_entries = 128
```

44. For compatibility reasons, four symbolic links are required:

```
ln -s /usr/lib64/libssl.so.0.9.8e /usr/lib64/libssl.so.0.9.8
ln -s /usr/lib64/libssl.so.1.0.1e /usr/lib64/libssl.so.1.0.1
ln -s /usr/lib64/libcrypto.so.0.9.8e /usr/lib64/libcrypto.so.0.9.8
ln -s /usr/lib64/libcrypto.so.1.0.1e /usr/lib64/libcrypto.so.1.0.1
```

45. Transparent Hugepages

46. In the file /boot/grub/grub.conf add the kernel command line argument

```
transparent_hugepage=never
```

47. Use a tuned profile to minimize latencies:

```
# yum -y install tuned
# tuned-adm profile latency-performance
# chkconfig tuned on
# service tuned start
```

48. Disable Crash Dump

```
# chkconfig abrtd off
# chkconfig abrt-ccpp off
# service abrtd stop
# service abrt-ccpp stop
```

49. Disable core file creation. To disable core dumps for all users, open /etc/security/limits.conf, and add the line

```
* soft core 0
* hard core 0
```

50. Adaptation of the Basic SAP Notes settings

51. Edit the /boot/grub/menu.lst and append the below parameter to the kernel line per SAP Note
Install Cisco enic driver

This procedure describes how to download the Cisco UCS Drivers ISO bundle, which contains most Cisco UCS Virtual Interface Card drivers.

1. In a web browser, navigate to http://www.cisco.com
2. Under Support, click All Downloads.
3. In the product selector, click Products, then click Server - Unified Computing
4. If prompted, enter your Cisco.com username and password to log in.

**Note:** You must be signed in to download Cisco Unified Computing System (UCS) drivers.

6. Click UCS B-Series Blade Server Software
7. Click Cisco Unified Computing System (UCS) Drivers

**Note:** The latest release version is selected by default. This document is built on Version 2.2(3)

8. Click 2.2(3) Version
9. Download ISO image of Cisco UCS-related drivers
10. Choose your download method and follow the prompts to complete your driver download.

11. After the download complete browse the ucs-bxxx-drivers.2.2.3/Linux/Network/Cisco/12x0/RHEL/RHEL6.5 and copy kmod-enic-2.1.1.75-rhel6u5.el6.x86_64.rpm to PXE Boot Server /NFS/software/RHEL

12. Copy the rpm package to OS Master from PXE boot Server

```shell
scp /NFS/software/RHEL/kmod-enic-2.1.1.75-rhel6u5.el6.x86_64.rpm 192.168.127.201:/tmp/
kmod-enic-2.1.1.75-rhel6u5.el6.x86_64.rpm 100% 618KB 617.5KB/s 00:00
```

14. ssh to the os master on the PXE boot IP from PXE Boot Server as root
15. Update the enic driver

```shell
[root@osmaster ~]# rpm -Uvh /tmp/kmod-enic-2.1.1.75-rhel6u5.el6.x86_64.rpm
Preparing...                ########################################### [100%]
1:kmod-enic              ########################################### [100%]
```

**Prepare NFS Root Volume**

1. For PXE NFS boot, install network dracut modules to create a network aware initramfs image.

```shell
[root@osmaster ~]# rpm -Uvh /tmp/kmod-enic-2.1.1.75-rhel6u5.el6.x86_64.rpm
```

2. Create initramfs image.

```shell
[root@osmaster ~]# dracut -m "nfs network base" initramfs-nfs.img
```

3. From the PXE boot server copy the initramfs image

```shell
scp 192.168.127.211:/initramfs-nfs.img /tftpboot/rhel/initrd-rhel4sap
root@192.168.127.211's password: initramfs-nfs.img 100% 12MB 11.9MB/s
00:00
```

4. From the PXE boot server copy the vmlinuz

```shell
scp 192.168.127.211:/boot/vmlinuz-2.6.32-431.el6.x86_64 /tftpboot/rhel/vmlinuz-rhel4sap
```
5. Create the OS Image using rsync from the osmaster to mount on the PXE boot server

rsync -a -e ssh --exclude='/proc/*' --exclude='/sys/*' . 192.168.127.27:/NFS/osmaster

6. Edit the /etc/fstab entry to remove local disk entry

vi /NFS/osmaster/etc/fstab

tmpfs /dev/shm tmpfs defaults 0 0
devpts /dev/pts devpts gid=5,mode=620 0 0
sysfs /sys sysfs defaults 0 0
proc /proc proc defaults 0 0

7. Update the PXE Configuration for OS master on the PXE boot server

vi /tftpboot/pxelinux.cfg/C0A87FD3

# UCS PXE Boot Definition
DISPLAY ../boot.msg
DEFAULT RHEL4SAP
PROMPT 1
TIMEOUT 50
LABEL RHEL4SAP
    KERNEL rhel/vmlinuz-rhel4sap
    APPEND initrd=rhel/initrd-rhel4sap rw root=192.168.127.11:/rhel_os_master
    transparent_hugepage=never selinux=0 intel_idle.max_cstate=0 processor.max_cstate=0
    ip=dhcp

8. Reboot the server

Cloning OS Volumes
After OS Master Image is created, prepare the os image for cloning.

Clean UP Master OS image
1. ssh to osmaster
2. Remove the Red Hat Registration information

   Note: This step is required for creating master image without the registration information. After OS deployment register each server with RHEL for OS support.

   [root@osmaster ~]# subscription-manager unregister

3. Shutdown the OS Master Server by issuing “halt” command
4. Log into PXE Boot server using ssh

   Note: Please check rhel_os_master volume is mounted on the /NFS/osmaster

5. Clear the System logs

   rm /NFS/osmaster/var/log/* -r

6. Clear the Ethernet Persistent network information

   cat /dev/null > /NFS/osmaster/etc/udev/rules.d/70-persistent-net.rules

7. Remove any Ethernet configuration file except eth0

   rm /NFS/osmaster/etc/sysconfig/network-scripts/ifcfg-eth<<1-8>>

8. Use the configuration file for eth0

   vi /NFS/osmaster/etc/sysconfig/network-scripts/ifcfg-eth0

   #
   # PXE Boot LAN
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
USERCTL=no
IPV6INIT=no
TYPE=Ethernet
NM_CONTROLLED=no

**Storage Clone of OS Volume**

1. To clone the os master image to new host follow the steps below
2. Log in to Storage shell
3. Create a Clone of OS master volume

```bash
volume clone create -flexclone cishanar01 -parent-volume rhel_os_master -vserver infra_vs1 -junction-path /cishanar01 -space-guarantee none
```
4. Split the volume from OS master volume

```bash
fas8040-cluster::> volume clone split start -flexclone cishanar01
```
Warning: Are you sure you want to split clone volume cishanar01 in Vserver infra_vs1 ? {y|n}: y

```bash
[Job 1962] Job is queued: Split cishanar01.
```
5. Repeat the steps 3-4 for each server to deploy OS image

**PXE Configuration for Additional Server**

1. The PXE boot environment will look for configuration file based on its boot IP assigned via DHCP. To calculate the filename run “gethostip”, the output is a hex representation of the IP address will be configuration filename

```bash
gethostip 192.168.127.201
192.168.127.201 192.168.127.201 C0A87FC9
```
2. The file name “C0A87FC9” contains the PXE boot configuration for server with IP 192.168.127.201
3. ssh to PXE boot server
4. Go to PXE boot configuration directory

```bash
cd /tftpboot/pxelinux.cfg/
```
5. Create a configuration file for each server

```bash
vi C0A87FC9
```
# UCS PXE Boot Definition
DISPLAY ../../boot.msg
DEFAULT RHEL4SAP
PROMPT 1
TIMEOUT 50
#
LABEL RHEL4SAP
   KERNEL rhel/vmlinuz-rhel4sap
   APPEND initrd=rhel/initrd-rhel4sap rw root=192.168.127.11:/cishanar01
   transparent_hugepage=never selinux=0 intel_idle.max_cstate=0 processor.max_cstate=0
   ip=dhcp
```
6. Repeat the previous step for each server

**Boot the Server**

1. In Cisco UCS Manager, click the Servers tab in the navigation pane.
2. Select Service Profile Templates > root > Service Profiles.
3. Expand the tree and right-click Service Template HANA-Server01 and select Boot Server
Post Installation OS Customization

After the OS is deployed from the Master image, customization is required for each server.

Hostnames

1. The operating system must be configured such a way that the short name of the server is displayed for the command ‘hostname’ and Full Qualified Host Name is displayed with the command ‘hostname –d’
2. ssh to the Server to PXE boot IP from PXE Boot Server
3. Login as root and password
4. Edit the Hostname

```
vi /etc/sysconfig/network
HOSTNAME=<<hostname>>.<<Domain Name>>
```

IP Address

1. Assign the IP address to each interface
2. ssh to the Server01 on the PXE boot IP from PXE Boot Server
3. Login as root and password
4. To configure the network interface on the OS, it is required to identify the mapping of the ethernet device on the OS to vNIC interface on the Cisco UCS.
5. From the OS execute the below command to get list of Ethernet device with MAC Address

```
ifconfig -a |grep HWaddr
```

```
et0     Link encap:Ethernet  HWaddr 00:25:B5:1A:10:00  
et1     Link encap:Ethernet  HWaddr 00:25:B5:00:0A:02  
et2     Link encap:Ethernet  HWaddr 00:25:B5:00:0B:02  
et3     Link encap:Ethernet  HWaddr 00:25:B5:00:0A:00  
et4     Link encap:Ethernet  HWaddr 00:25:B5:00:0B:00  
et5     Link encap:Ethernet  HWaddr 00:25:B5:00:0B:01  
et6     Link encap:Ethernet  HWaddr 00:25:B5:00:0B:03  
et7     Link encap:Ethernet  HWaddr 00:25:B5:00:0A:01  
et8     Link encap:Ethernet  HWaddr 00:25:B5:00:0A:03
```

6. In Cisco UCS Manager, click the Servers tab in the navigation pane
7. Select Service Profiles > root > HANA-Server01 Expand by clicking on +
8. Click vNICs
9. On the Right pane list of the vNICs with MAC Address are listed.

**Figure 183.** Cisco UCS vNIC MAC Address

<table>
<thead>
<tr>
<th>vNICs</th>
<th>MAC Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>HANA-Admin</td>
<td>00:25:B5:00:0A:03</td>
</tr>
<tr>
<td>HANA-AppServer</td>
<td>00:25:B5:00:0A:01</td>
</tr>
<tr>
<td>HANA-Backup</td>
<td>00:25:B5:00:0B:03</td>
</tr>
<tr>
<td>HANA-Boot</td>
<td>00:25:B5:1A:10:00</td>
</tr>
<tr>
<td>HANA-Client</td>
<td>00:25:B5:00:00:02</td>
</tr>
<tr>
<td>HANA-DataSource</td>
<td>00:25:B5:00:0A:00</td>
</tr>
<tr>
<td>HANA-Internal</td>
<td>00:25:B5:00:0A:02</td>
</tr>
<tr>
<td>HANA-Replication</td>
<td>00:25:B5:00:08:00</td>
</tr>
<tr>
<td>HANA-Storage</td>
<td>00:25:B5:00:00:01</td>
</tr>
</tbody>
</table>

10. Note the MAC Address of the HANA-Admin vNIC “00:25:B5:00:0A:03”
11. By comparing MAC Address on the OS and Cisco UCS, eth8 on OS will carry the VLAN for HANA-Admin
12. Go to network configuration directory and create a configuration for eth8
/etc/sysconfig/network

vi ifcfg-eth8

##
# HANA-Admin Network
##
DEVICE=eth8
ONBOOT=yes
BOOTPROTO=static
IPV6INIT=no
USERCTL=no
TYPE=Ethernet
NM_CONTROLLED=no
NETWORK=<IP subnet for HANA-Admin example:192.168.201.0>
NETMASK=<subnet mask for HANA-Admin 255.255.255.0>
IPADDR=<IP address for HANA-Admin 192.168.201.102>

13. Repeat the steps 10 to 12 for each vNIC interface
14. Add default gateway

vi /etc/sysconfig/network

NETWORKING=yes
HOSTNAME=<HOSTNAME>
GATEWAY=<IP Address of default gateway>

Network Time
It is important that the time on all components used for SAP HANA is in sync. The configuration of NTP is important and to be done on all systems.

vi /etc/ntp.conf

server <NTP-SERVER1 IP>
server <NTP-SERVER2 IP>

service ntpd stop
ntpdate ntp.example.com
service ntpd start
chkconfig ntpd on
chkconfig ntpdate on

DNS
Domain Name Service configuration must be done based on the local requirements.
Configuration Example
Add DNS IP if it is required to access internet

vi /etc/resolv.conf

DNS1=<IP of DNS Server1>
DNS2=<IP of DNS Server2>
DOMAIN= <Domain_name>

HOSTS
For scale-out system all nodes should be able to resolve Internal network IP address, below is an example of 8 node host file with all the network defined in the /etc/hosts file

cat /etc/hosts

127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4 ::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
##
# NFS Storage
172.29.110.12 lifdata01
172.29.110.13 lifdata02
## Internal Network

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.29.220.201</td>
<td>cishana01.ciscolab.local cishana01</td>
</tr>
<tr>
<td>172.29.220.202</td>
<td>cishana02.ciscolab.local cishana02</td>
</tr>
<tr>
<td>172.29.220.203</td>
<td>cishana03.ciscolab.local cishana03</td>
</tr>
<tr>
<td>172.29.220.204</td>
<td>cishana04.ciscolab.local cishana04</td>
</tr>
<tr>
<td>172.29.220.205</td>
<td>cishana05.ciscolab.local cishana05</td>
</tr>
<tr>
<td>172.29.220.206</td>
<td>cishana06.ciscolab.local cishana06</td>
</tr>
<tr>
<td>172.29.220.207</td>
<td>cishana07.ciscolab.local cishana07</td>
</tr>
<tr>
<td>172.29.220.208</td>
<td>cishana08.ciscolab.local cishana08</td>
</tr>
</tbody>
</table>

## Storage Network

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.29.110.201</td>
<td>cishana01s.ciscolab.local cishana01s</td>
</tr>
<tr>
<td>172.29.110.202</td>
<td>cishana02s.ciscolab.local cishana02s</td>
</tr>
<tr>
<td>172.29.110.203</td>
<td>cishana03s.ciscolab.local cishana03s</td>
</tr>
<tr>
<td>172.29.110.204</td>
<td>cishana04s.ciscolab.local cishana04s</td>
</tr>
<tr>
<td>172.29.110.205</td>
<td>cishana05s.ciscolab.local cishana05s</td>
</tr>
<tr>
<td>172.29.110.206</td>
<td>cishana06s.ciscolab.local cishana06s</td>
</tr>
<tr>
<td>172.29.110.207</td>
<td>cishana07s.ciscolab.local cishana07s</td>
</tr>
<tr>
<td>172.29.110.208</td>
<td>cishana08s.ciscolab.local cishana08s</td>
</tr>
</tbody>
</table>

## Client Network

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.29.222.201</td>
<td>cishana01c.ciscolab.local cishana01c</td>
</tr>
<tr>
<td>172.29.222.202</td>
<td>cishana02c.ciscolab.local cishana02c</td>
</tr>
<tr>
<td>172.29.222.203</td>
<td>cishana03c.ciscolab.local cishana03c</td>
</tr>
<tr>
<td>172.29.222.204</td>
<td>cishana04c.ciscolab.local cishana04c</td>
</tr>
<tr>
<td>172.29.222.205</td>
<td>cishana05c.ciscolab.local cishana05c</td>
</tr>
<tr>
<td>172.29.222.206</td>
<td>cishana06c.ciscolab.local cishana06c</td>
</tr>
<tr>
<td>172.29.222.207</td>
<td>cishana07c.ciscolab.local cishana07c</td>
</tr>
<tr>
<td>172.29.222.208</td>
<td>cishana08c.ciscolab.local cishana08c</td>
</tr>
</tbody>
</table>

## AppServer Network

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.29.223.201</td>
<td>cishana01a.ciscolab.local cishana01a</td>
</tr>
<tr>
<td>172.29.223.202</td>
<td>cishana02a.ciscolab.local cishana02a</td>
</tr>
<tr>
<td>172.29.223.203</td>
<td>cishana03a.ciscolab.local cishana03a</td>
</tr>
<tr>
<td>172.29.223.204</td>
<td>cishana04a.ciscolab.local cishana04a</td>
</tr>
<tr>
<td>172.29.223.205</td>
<td>cishana05a.ciscolab.local cishana05a</td>
</tr>
<tr>
<td>172.29.223.206</td>
<td>cishana06a.ciscolab.local cishana06a</td>
</tr>
<tr>
<td>172.29.223.207</td>
<td>cishana07a.ciscolab.local cishana07a</td>
</tr>
<tr>
<td>172.29.223.208</td>
<td>cishana08a.ciscolab.local cishana08a</td>
</tr>
</tbody>
</table>

## Admin Network

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.29.112.201</td>
<td>cishana01m.ciscolab.local cishana01m</td>
</tr>
<tr>
<td>172.29.112.202</td>
<td>cishana02m.ciscolab.local cishana02m</td>
</tr>
<tr>
<td>172.29.112.203</td>
<td>cishana03m.ciscolab.local cishana03m</td>
</tr>
<tr>
<td>172.29.112.204</td>
<td>cishana04m.ciscolab.local cishana04m</td>
</tr>
<tr>
<td>172.29.112.205</td>
<td>cishana05m.ciscolab.local cishana05m</td>
</tr>
<tr>
<td>172.29.112.206</td>
<td>cishana06m.ciscolab.local cishana06m</td>
</tr>
<tr>
<td>172.29.112.207</td>
<td>cishana07m.ciscolab.local cishana07m</td>
</tr>
<tr>
<td>172.29.112.208</td>
<td>cishana08m.ciscolab.local cishana08m</td>
</tr>
</tbody>
</table>

## Backup Network

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.29.221.201</td>
<td>cishana01b.ciscolab.local cishana01b</td>
</tr>
<tr>
<td>172.29.221.202</td>
<td>cishana02b.ciscolab.local cishana02b</td>
</tr>
<tr>
<td>172.29.221.203</td>
<td>cishana03b.ciscolab.local cishana03b</td>
</tr>
<tr>
<td>172.29.221.204</td>
<td>cishana04b.ciscolab.local cishana04b</td>
</tr>
<tr>
<td>172.29.221.205</td>
<td>cishana05b.ciscolab.local cishana05b</td>
</tr>
<tr>
<td>172.29.221.206</td>
<td>cishana06b.ciscolab.local cishana06b</td>
</tr>
<tr>
<td>172.29.221.207</td>
<td>cishana07b.ciscolab.local cishana07b</td>
</tr>
<tr>
<td>172.29.221.208</td>
<td>cishana08b.ciscolab.local cishana08b</td>
</tr>
</tbody>
</table>

## DataSource Network

...
SSH Keys

The SSH Keys must be exchanged between all nodes in a SAP HANA Scale-Out system for user ‘root’ and user <SID>adm.

1. Generate the rsa public key by executing the command `ssh-keygen -b 2048`

```
[root@cishanar01 ~]# ssh-keygen -b 2048
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
14:5a:e6:d6:00:f3:81:86:38:47:e7:fb:de:78:f5:26 root@cishanar01.ciscolab.local
The key's randomart image is:
++-[ RSA 2048]-----
 o..+o*
 o oooB =
 o .O = .
 +
 . S
 . .
 . .
 . .
 o. E o
 o . o
-------------------
```

2. The SSH Keys must be exchanged between all nodes in a SAP HANA Scale-Out system for user ‘root’ and user

3. Exchange the rsa public key by executing the below command from First server to rest of the servers in the scale-out system.

```
"ssh-copy-id -i /root/.ssh/id_rsa.pub cishanar02"
```

```
[root@cishanar01 ~]# ssh-copy-id -i /root/.ssh/id_rsa.pub cishanar02
The authenticity of host 'cishanar02 (172.29.220.202)' can't be established.
```
Warning: Permanently added 'cishanar02,172.29.220.202' (RSA) to the list of known hosts.
root@cishanar02's password:
Now try logging into the machine, with "ssh 'cishanar02'", and check in:

.ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.

4 Repeat the 1-4 for all the servers in the single SID SAP HANA system
Storage for SAP HANA

This section describes configuration steps for SAP HANA related storages volumes at the OS level. The underlying infrastructure configuration is already defined in the earlier sections in this document.

File Storage for SAP HANA data and log

As per the SAP HANA requirement for Data and log volume size are defined. DATA volume should be equal to one times the size of the memory and LOG volume is equal to half the size of the memory for systems less than 256 GB and 512 GB for Systems greater than 512 GB of RAM.

Create Volumes for SAP HANA

In order to load balance across the NetApp Controllers, data and log volumes are distributed. For example for an 8-node SAP HANA system, the aggregate on NetApp Controller A contains the data volumes data001, data003 data005 and data007 and Log volumes log002, log004, log006 and log008. Similarly, aggregate on NetApp Controller B contains data volumes data002, data004, data006 and data008 and log volumes log001, log003, log005 and log007.

The following information is required to create a FlexVol® volume: the volume’s name and size, and the aggregate on which it will exist.
Open either an SSH connection to NetApp cluster IP or host name and log in as admin user with the password.

Execute the below commands to create data volume name hanadata01 in the aggregate aggr_hana01 with size 1 TB with export policy data

```
volume create -vserver hana_vs1 -volume hanadata01 -aggregate aggr_hana01 -size 1TB -state online -policy data -junction-path /hanadata01 -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none
```

For 8 node scale-out system execute the below commands to create eight data volumes.

```
volume create -vserver hana_vs1 -volume data001 -aggregate aggr_hana01 -size 1TB -state online -policy data -junction-path /data001 -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver hana_vs1 -volume data002 -aggregate aggr_hana02 -size 1TB -state online -policy data -junction-path /data002 -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver hana_vs1 -volume data003 -aggregate aggr_hana01 -size 1TB -state online -policy data -junction-path /data003 -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver hana_vs1 -volume data004 -aggregate aggr_hana02 -size 1TB -state online -policy data -junction-path /data004 -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver hana_vs1 -volume data005 -aggregate aggr_hana01 -size 1TB -state online -policy data -junction-path /data005 -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver hana_vs1 -volume data006 -aggregate aggr_hana02 -size 1TB -state online -policy data -junction-path /data006 -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver hana_vs1 -volume data007 -aggregate aggr_hana01 -size 1TB -state online -policy data -junction-path /data007 -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none
```
Execute the commands below to create log volume name hanalog01 in the aggregate aggr_hana02 with size 512 GB

volume create -vserver hana_vs1 -volume hanalog01 -aggregate aggr_hana02 -size 512g -state online -policy data -junction-path /hanalog01 -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none

For 8 node scale-out system execute the commands below to create eight log volumes.

volume create -vserver hana_vs1 -volume log001 -aggregate aggr_hana02 -size 512g -state online -policy data -junction-path /log001 -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver hana_vs1 -volume log002 -aggregate aggr_hana01 -size 512g -state online -policy data -junction-path /log002 -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver hana_vs1 -volume log003 -aggregate aggr_hana02 -size 512g -state online -policy data -junction-path /log003 -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver hana_vs1 -volume log004 -aggregate aggr_hana01 -size 512g -state online -policy data -junction-path /log004 -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver hana_vs1 -volume log005 -aggregate aggr_hana02 -size 512g -state online -policy data -junction-path /log005 -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver hana_vs1 -volume log006 -aggregate aggr_hana01 -size 512g -state online -policy data -junction-path /log006 -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver hana_vs1 -volume log007 -aggregate aggr_hana02 -size 512g -state online -policy data -junction-path /log007 -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none
volume create -vserver hana_vs1 -volume log008 -aggregate aggr_hana01 -size 512g -state online -policy data -junction-path /log008 -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none

Depending on number of nodes in the scale-out environment, create the appropriate number of data and log volume with SAP’s size guideline.

Set the following options for all SAP HANA data and log volumes

vol modify -vserver hana_vs1 -volume *log* -snapdir-access false
vol modify -vserver hana_vs1 -volume *data* -snapdir-access false
vol modify -vserver hana_vs1 -volume *log* -atime-update false
vol modify -vserver hana_vs1 -volume *data* -atime-update false

File Storage for /hana/shared

The size of the /hana/shared file system must be at least 1x main memory of all SAP HANA nodes and the file system type must be capable to expand the size in case a new node is added to the <SID>. One benefit of NFS in most cases is the capability to shrink the file system on demand without any downtime.

Execute the below commands to create shared volume name sapexe in the aggregate aggr_hana01 with size 8 TB with export policy data.

```bash
volume create -vserver hana_vs1 -volume data008 -aggregate aggr_hana02 -size 1TB -state online -policy data -junction-path /data008 -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none
```
volume create -vserver hana_vs1 -volume sapexe -aggregate aggr_hana01 -size 8TB -state online -policy data -junction-path /sapexe -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none

Create Qtree for shared directory

qtree create -vserver hana_vs1 -volume sapexe -qtree shared -security-style unix -export-policy os

Set the following options for SAP HANA shared volume

vol modify -vserver hana_vs1 -volume sapexe -snapdir-access false
vol modify -vserver hana_vs1 -volume sapexe -atime-update false

File Storage for /usr/sap

The recommended size of the /usr/sap file system is 50 GB for each SAP HANA nodes. With NetApp Clustered Data ONTAP, we create qtree for /usr/sap mount point under sapexe volume.

Execute the below commands to create qtree name usr_sap_01 for SAP HANA Node 1, under the volume sapexe in the aggregate aggr_hana01

qtree create -vserver hana_vs1 -volume sapexe -qtree usr_sap_01 -security-style unix -export-policy os

Repeat the above command to create qtree for each HANA node

qtree create -vserver hana_vs1 -volume sapexe -qtree usr_sap_02 -security-style unix -export-policy os
qtree create -vserver hana_vs1 -volume sapexe -qtree usr_sap_03 -security-style unix -export-policy os
qtree create -vserver hana_vs1 -volume sapexe -qtree usr_sap_04 -security-style unix -export-policy os
qtree create -vserver hana_vs1 -volume sapexe -qtree usr_sap_05 -security-style unix -export-policy os
qtree create -vserver hana_vs1 -volume sapexe -qtree usr_sap_06 -security-style unix -export-policy os
qtree create -vserver hana_vs1 -volume sapexe -qtree usr_sap_07 -security-style unix -export-policy os
qtree create -vserver hana_vs1 -volume sapexe -qtree usr_sap_08 -security-style unix -export-policy os
# Mount Options

Mount options vary from the default Linux setting for using NFS for SAP HANA data and log volumes. Here an example of `/etc/fstab` entry for an 8 node SAP HANA Scale-Out system with SID ANA.

```
# HANA Shared
nfssap:/sapexe/shared /hana/shared nfs
dir,VERS=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock 0 0
# User SAP
nfssap:/sapexe/usr_sap_01 /usr/sap nfs
dir,VERS=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock 0 0
# HANA DATA
#
lifdata01:/data001 /hana/data/ANA/mnt00001 nfs
dir,VERS=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock 0 0
lifdata02:/data002 /hana/data/ANA/mnt00002 nfs
dir,VERS=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock 0 0
lifdata01:/data003 /hana/data/ANA/mnt00003 nfs
dir,VERS=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock 0 0
lifdata02:/data004 /hana/data/ANA/mnt00004 nfs
dir,VERS=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock 0 0
lifdata01:/data005 /hana/data/ANA/mnt00005 nfs
dir,VERS=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock 0 0
lifdata02:/data006 /hana/data/ANA/mnt00006 nfs
dir,VERS=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock 0 0
lifdata01:/data007 /hana/data/ANA/mnt00007 nfs
dir,VERS=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock 0 0
lifdata02:/data008 /hana/data/ANA/mnt00008 nfs
dir,VERS=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock 0 0
# HANA LOG
#
lifdata02:/log001 /hana/log/ANA/mnt00001 nfs
dir,VERS=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock 0 0
lifdata01:/log002 /hana/log/ANA/mnt00002 nfs
dir,VERS=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock 0 0
lifdata02:/log003 /hana/log/ANA/mnt00003 nfs
dir,VERS=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock 0 0
lifdata01:/log004 /hana/log/ANA/mnt00004 nfs
dir,VERS=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock 0 0
lifdata02:/log005 /hana/log/ANA/mnt00005 nfs
dir,VERS=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock 0 0
lifdata01:/log006 /hana/log/ANA/mnt00006 nfs
dir,VERS=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock 0 0
lifdata02:/log007 /hana/log/ANA/mnt00007 nfs
```
Example of /etc/fstab entry for SAP HANA Scale-Up system with SID ANA

```
# HANA Shared
lifdata01:/hana01_sapexe/shared           /hana/shared    nfs
rw,bg,vers=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock  0 0

# User SAP
lifdata01:/hana01_sapexe/usr_sap_01      /usr/sap        nfs
rw,bg,vers=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock  0 0

# HANA DATA
lifdata01:/hana01_data                   /hana/data      nfs
rw,bg,vers=3,hard,timeo=500,rsize=65536,wsize=65536,intr,actimeo=500,noatime,nolock  0 0

# HANA LOG
lifdata02:/hana01_log                     /hana/log       nfs
rw,bg,vers=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=500,noatime,nolock  0 0
```

Create the required directory to mount /hana/shared, /hana/data and /hana/log volumes.
Mount all the volumes from /etc/fstab using “mount –a”
Check the status of all mounted volumes using “df –h” command

```
cishana01:/ # df -h
Filesystem   Size  Used  Avail Use% Mounted on
udev         253G   236K  253G   1% /dev
tmpfs        253G    0   253G    0% /dev/shm
192.168.127.11:/server01  50G  4.8G   46G  10% /
nfssap:/sapexe/shared     8.0T  361M  8.0T   1% /hana/shared
nfssap:/sapexe/usr_sap_01 50G   0   50G    0% /usr/sap
lifdata01:/data001        1.0T  1.0T   0% /hana/data/ANA/mnt00001
lifdata01:/data002        1.0T  1.0T   0% /hana/data/ANA/mnt00002
lifdata01:/data003        1.0T  1.0T   0% /hana/data/ANA/mnt00003
lifdata01:/data004        1.0T  1.0T   0% /hana/data/ANA/mnt00004
lifdata01:/data005        1.0T  1.0T   0% /hana/data/ANA/mnt00005
lifdata01:/data006        1.0T  1.0T   0% /hana/data/ANA/mnt00006
lifdata01:/data007        1.0T  1.0T   0% /hana/data/ANA/mnt00007
lifdata01:/data008        1.0T  1.0T   0% /hana/data/ANA/mnt00008
lifdata01:/log001         512G  47M  512G   1% /hana/log/ANA/mnt00001
lifdata01:/log002         512G  47M  512G   1% /hana/log/ANA/mnt00002
lifdata01:/log003         512G  47M  512G   1% /hana/log/ANA/mnt00003
lifdata01:/log004         512G  47M  512G   1% /hana/log/ANA/mnt00004
lifdata01:/log005         512G  47M  512G   1% /hana/log/ANA/mnt00005
lifdata01:/log006         512G  47M  512G   1% /hana/log/ANA/mnt00006
lifdata01:/log007         512G  47M  512G   1% /hana/log/ANA/mnt00007
lifdata01:/log008         512G  47M  512G   1% /hana/log/ANA/mnt00008
```

Make sure that the <SID>adm user owns the data and log volumes – use the chown command after the file systems are mounted on each HANA node

```
chown anaadm:sapsys /hana/data/ANA
chown anaadm:sapsys /hana/log/ANA
```
Virtualized SAP HANA (vHANA)

ESXi host Installation

Log in to Cisco UCS Manager
The IP KVM enables the administrator to begin the installation of the operating system (OS) through remote media. It is necessary to log in to the Cisco UCS environment to run the IP KVM.

To log in to the Cisco UCS environment, complete the following steps:

1. Open a web browser and enter the IP address for the Cisco UCS cluster address. This step launches the Cisco UCS Manager application.
2. Log in to Cisco UCS Manager by using the admin user name and password.
3. From the main menu, click the Servers tab.
5. Right-click vHANA-Host-01 and select KVM Console.

Set Up VMware ESXi Installation

Download Cisco Custom Image for ESXi 5.5.0 U1

1. Click the following link [vmware login page](#)
2. Type your email or customer number and the password and then click Log in
3. Click on the following link [CiscoCustomImage5.5.0U1](#)
4. Click Download
5. Save it to your destination folder

To prepare the server for the OS installation, complete the following steps on each ESXi host:

1. In the KVM window, click the Virtual Media tab.
2. Click Add Image.
3. Browse to the ESXi installer ISO image file and click Open.
   a. Download ESXi-5.5.0-1746018-Custom-Cisco-5.5.1.3.iso
4. Select the Mapped checkbox to map the newly added image.
5. Click the KVM tab to monitor the server boot.
6. Boot the server by selecting Boot Server and clicking OK. Then click OK again.

Install ESXi

ESXi Hosts vHANA Host for iSCSI boot
To install VMware ESXi to the SAN-bootable LUN of the hosts, complete the following steps on each host:

1. On reboot, the machine detects the presence of the ESXi installation media. Select the ESXi installer from the menu that is displayed.
2. After the installer is finished loading, press Enter to continue with the installation.
3. Read and accept the end-user license agreement (EULA). Press F11 to accept and continue.
4. Select the NetApp LUN that was previously set up as the installation disk for ESXi and press Enter to continue with the installation.
5. Select the appropriate keyboard layout and press Enter.
6. Enter and confirm the root password and press Enter.
7. The installer issues a warning that existing partitions will be removed from the volume. Press F11 to continue with the installation.
8. After the installation is complete, clear the Mapped checkbox (located in the Virtual Media tab of the KVM console) to unmap the ESXi installation image.
**Note:** The ESXi installation image must be unmapped to make sure that the server reboots into ESXi and not into the installer.

9. The Virtual Media window might issue a warning stating that it is preferable to eject the media from the guest. Because the media cannot be ejected and it is read-only, simply click Yes to unmap the image.
10. From the KVM tab, press Enter to reboot the server.

### Set Up Management Networking for ESXi Hosts

Adding a management network for each VMware host is necessary for managing the host. To add a management network for the VMware hosts, complete the following steps on each ESXi host:

To configure the `vHANA-Host-01` ESXi host with access to the management network, complete the following steps:

1. After the server has finished rebooting, press F2 to customize the system.
2. Log in as `root` and enter the corresponding password.
3. Select the Configure the Management Network option and press Enter.
4. Select the Network Adapters and press Enter.
5. Select the Devices under Device Name, which are used for Management Network, by matching the MAC address from the Cisco UCS Service Profile. Press Enter.
6. To get the MAC address from Cisco UCS Service Profile, follow the steps below:
   a. In Cisco UCS Manager, click the Servers tab in the navigation pane.
   b. Select Servers > Service Profiles > root > Sub-Organization > vHANA > `vHANA-Host-01`.
   c. Expand by clicking on +
   d. Click on vNICs.
   e. On the Right pane list of the vNICs with MAC Address are listed.
   f. Note the MAC Address of the vNIC-A and vNIC-B.
7. Select the VLAN (Optional) option and press Enter.
8. Enter the `<var_vhana_esx_mgmt_vlan_id>` and press Enter.
10. Select the Set Static IP Address and Network Configuration option by using the space bar.
11. Enter the IP address for managing the first ESXi host: `<var_vhana_host_mgmt_01_ip>`.
12. Enter the subnet mask for the first ESXi host.
13. Enter the default gateway for the first ESXi host.
14. Press Enter to accept the changes to the IP configuration.
15. Select the IPv6 Configuration option and press Enter.
16. Using the spacebar, unselect Enable IPv6 (restart required) and press Enter.
17. Select the DNS Configuration option and press Enter.

**Note:** Since the IP address is assigned manually, the DNS information must also be entered manually.

18. Enter the IP address of the primary DNS server.
19. Optional: Enter the IP address of the secondary DNS server.
20. Enter the fully qualified domain name (FQDN) for the first ESXi host.
21. Press Enter to accept the changes to the DNS configuration.
22. Press Esc to exit the Configure Management Network submenu.
23. Press Y to confirm the changes and return to the main menu.
24. The ESXi host reboots. After reboot, press F2 and log back in as root.
25. Select Test Management Network to verify that the management network is set up correctly and press Enter.
26. Press Enter to run the test.
27. Press Enter to exit the window.
28. Press Esc to log out of the VMware console.
Download VMware vSphere Client and VMware vSphere Remote CLI

To download the VMware vSphere Client and install Remote CLI, complete the following steps:

1. Open a web browser on the management workstation and navigate to the vHANA-Host-01 management IP address.
2. Download and install both the VMware vSphere Client and the Windows version of VMware vSphere Remote Command Line.

Note: These applications are downloaded from the VMware website and Internet access is required on the management workstation.

Log in to VMware ESXi Hosts Using VMware vSphere Client

ESXi Host vHANA-Host-01

To log in to the vHANA-Host-01 ESXi host by using the VMware vSphere Client, complete the following steps:

1. Open the recently downloaded VMware vSphere Client and enter the IP address of vHANA-Host-01 as the host you are trying to connect to: <<var_vhana_host_mgmt_01_ip>>.
2. Enter root for the user name.
3. Enter the root password.
4. Click Login to connect.

Post Install Configuration

To configure the ESXi as per SAP HANA requirement, complete the following steps:

1. From VMware vSphere Client, select the host in the inventory.
2. Click the Configuration tab
3. Click Power Management in the Hardware pane
4. Click Properties on the right side Power Management Setting
5. Under Power Management Policy choose High performance
6. Click OK

7. Adapt settings according to SAP Note 1606643:
Configure the host to activate the host accessor functions

1. From VMware vSphere client, select the host in the inventory.
2. Click the Configuration tab
3. Click "Advanced Settings" in the Software pane
4. In the list of software options, choose "Advanced Settings".
5. In "Advanced Settings", choose "Misc".
6. Scroll down to "Misc.GuestLibAllowHostInfo".
7. Set the value to "1".

Set Up VMkernel Ports and Virtual Switch

**ESXi vHANA Host Network Configuration for Management**

To set up the VMkernel ports and the virtual switches on the vHANA-Host-01 ESXi host, complete the following steps:

1. From VMware vSphere client, select the host in the inventory.
2. Click the Configuration tab.
3. Click Networking in the Hardware pane.
4. Click Properties on the right side of vSwitch0.
5. Click the Network Adapters tab
6. Click Add
7. Select vmnic1 and click Next
8. Click Next and click Finish

**Figure 185. vSwitch Network Adapter Configuration**

9. Select the vSwitch configuration and click Edit.
10. From the General tab, change the MTU to 9000.
11. Click OK to close the properties for vSwitch0.
12. Select the Management Network configuration and click Edit.
13. Change the network label to VMkernel-MGMT and select the Management Traffic checkbox.
14. Click OK to finalize the edits for Management Network.
15. Click Add to add a network element.
16. Select VMkernel and click Next.
17. Change the network label to VMkernel-NFS and enter $\langle var_vhana_esx_nfs_vlan_id \rangle$ in the VLAN ID (Optional) field.
18. Click Next to continue with the NFS VMkernel creation.
19. Enter the IP address $\langle var_vhana_host_nfs_01_ip \rangle$ and the subnet mask $\langle var_vhana_host_nfs_01_subnet \rangle$ for the NFS VLAN interface for vHANA-Host-01.
20. Click Next to continue with the NFS VMkernel creation.
21. Click Finish to finalize the creation of the NFS VMkernel interface.
22. Select the VMkernel-NFS configuration and click Edit.
23. Change the MTU to 9000.
24. Click OK to finalize the edits for the VMkernel-NFS network.
25. Click Add to add a network element.
26. Select VMkernel and click Next.
27. Change the network label to VMkernel-vMotion and enter $\langle var_vhana_esx_vmotion_vlan_id \rangle$ in the VLAN ID (Optional) field.
28. Select the Use This Port Group for vMotion checkbox.
29. Click Next to continue with the vMotion VMkernel creation.
30. Enter the IP address $\langle var_vhana_host_vmotion_01_ip \rangle$ and the subnet mask $\langle var_vhana_host_vmotion_01_subnet \rangle$ for the vMotion VLAN interface for vHANA-Host-01.
31. Click Next to continue with the vMotion VMkernel creation.
32. Click Finish to finalize the creation of the vMotion VMkernel interface.
33. Select the VMkernel-vMotion configuration and click Edit.
34. Change the MTU to 9000.
35. Click OK to finalize the edits for the VMkernel-vMotion network.
36. Close the dialog box to finalize the ESXi host networking setup.

**ESXi vHANA Host iSCSI Configuration**

The following configuration is required for Virtualized SAP HANA (vHANA) hosts with iSCSI boot, it’s not required for Local Boot ESXi hosts.

To set up iSCSI configuration on the vHANA-Host-01 ESXi host, complete the following steps:
1. From VMware vSphere client, select the host in the inventory.
2. Click the Configuration tab.
3. Click Networking in the Hardware pane.
4. Click Properties on the right side of iSCSIBootvSwitch.
5. Select the iSCSIBootPG configuration and click Edit.
6. Change the Network Label to VMkernel-iSCSI-A. Do not set a VLAN ID.
7. Click OK to save changes to the VMkernel port.
8. Click Close to close the vSwitch Properties window.
9. On the right, click Add Networking.
10. Select VMKernel and click Next.
11. Leave Create a vSphere standard switch selected. Clear select vmnic2. Click Next.
12. Change the Network Label to VMKernel-iSCSI-B. Leave the VLAN ID set to None. Click Next.
13. Set the VMKernel-iSCSI-B IP address and subnet mask. To get this information, select the vHANA-Host-01 Service Profile in Cisco UCS Manager. Select the Boot Order tab and select iSCSI-B-vNIC. Click “Set iSCSI Boot Parameters”. Obtain the IPv4 address and subnet mask from this window. Click Next.
14. Click Finish. vSwitch 1 is created.
15. The networking for the ESXi host should be similar to the following example:
16. Click Storage Adapters in the Hardware pane.
17. Select the iSCSI Software Adapter and click Properties in the Details pane.
18. Select the Network Configuration tab.
19. Click Add.
20. Select VMkernel-iSCSI-A and click OK.
21. Click Add.
22. Select VMkernel-iSCSI-B and click OK.
23. Select the Static Discovery tab.
24. Click Settings.
25. Select the entire iSCSI Target Name field, right-click, and select Copy to copy this target name to the clipboard.
26. Click Close to close the Static Target Server Settings window.
27. Click Add.
28. Right-click the iSCSI Target Name field and select Paste.
29. Type the IP address of one of the iSCSI LIFs that does not already appear in the list.
30. Click OK.
31. Repeat these steps until the IP addresses of all four iSCSI LIFs are in the list.
32. Click Close to close the iSCSI Initiator Properties windows.
33. Click Yes to rescan the host bus adapter.
34. Right-click the host in the left pane and select Reboot.
35. Click Yes.
36. Enter a reason for the reboot and click OK.
37. After the host has rebooted, log back into the host by using VMware vSphere client.
**ESXi vHANA Host Network Configuration for vHANA Virtual Machines**

To set up the Virtual Machine ports and the virtual switches for each vHANA Virtual Machine on the vHANA-Host-01 ESXi host, complete the following steps:

1. From VMware vSphere client, select the host in the inventory.
2. Click the Configuration tab.
3. Click Networking in the Hardware pane.
4. Click Add Networking on the right side.
5. Add Network Wizard will start
6. Leave the Virtual Machine Connection Types Selected, Click Next
7. Select Create a vSphere standard switch and check vmnic 4 and vmnic 5. Click Next
8. Change the network label to vhana-access and enter <<var_vhana_access_vlan_id>> in the VLAN ID (Optional) field. Click Next
9. Click Finish to create vSwtich2
10. Click Properties on the right side of vSwitch2
11. Under Ports, click Add
12. Click Add to add a network element.
14. Change the network label to vhana-storage and enter <<var_vhana_storage_vlan_id>> in the VLAN ID
15. Click Next and Click Finish to add for VM Network.

**Note:** Repeat the steps 10-15 for each VLAN IDs added to the vNIC Template in the UCS Service Profile for each vHANA Host

16. Select the vSwitch configuration and click Edit.
17. From the General tab, change the MTU to 9000.
18. Click OK to close the properties for vSwitch2
19. Close the dialog box to finalize the ESXi host networking setup.

**Mount Datastores**

Mount the NFS datastores for Virtual Machines.

**ESXi Hosts Virtualized SAP HANA (vHANA)-Host-01**

To mount the required datastores, complete the following steps on each ESXi host:

1. From VMware vSphere client, select the host in the inventory.
2. Click the Configuration tab to enable configurations.
3. Click Storage in the Hardware pane.
4. From the Datastore area, click Add Storage to open the Add Storage wizard.
5. Select Network File System and click Next.
6. The wizard prompts for the location of the NFS export. Enter <<var_node01_esx_lif_ip>> as the IP address for NFS server
7. Make sure that the Mount NFS read only checkbox is NOT selected.
8. Enter vhana_datastore_1 as the datastore name.
9. Click Next to continue with the NFS datastore creation.
10. Click Finish to finalize the creation of the NFS datastore.

**Configure NTP on ESXi Hosts**

**ESXi Hosts vHANA-Host-01**

To configure Network Time Protocol (NTP) on the ESXi hosts, complete the following steps on each host:

1. From each VMware vSphere client, select the host in the inventory.
2. Click the Configuration tab to enable configurations.
3. Click Time Configuration in the Software pane.
4. Click Properties at the upper right side of the window.
5. At the bottom of the Time Configuration dialog box, click Options.
6. In the NTP Daemon Options dialog box, complete the following steps:
   a. Click General in the left pane and select Start and stop with host.
   b. Click NTP Settings in the left pane and click Add.
7. In the Add NTP Server dialog box, enter <<var_global_ntp_server_ip>> as the IP address of
   the NTP server and click OK.
8. In the NTP Daemon Options dialog box, select the Restart NTP Service to Apply Changes checkbox
   and click OK.
9. In the Time Configuration dialog box, complete the following steps:
10. Select the NTP Client Enabled checkbox and click OK.
11. Verify that the clock is now set to approximately the correct time.
    Note: The NTP server time may vary slightly from the host time.

**VMware vCenter 5.5**
This CVD uses VMware vCenter Server 5.5 Appliance, deployed on the Cisco UCS C220 Management
Server.
For the detailed installation procedure for VMware vCenter 5.5, see: FlexPod Datacenter with VMware
vSphere 5.5 Update 1 and Cisco Nexus 9000 Standalone.

**Set Up vCenter Server**

**vCenter Server VM**
To set up vCenter Server on the vCenter Server VM, complete the following steps:

1. Using the VMware vSphere client, log in to the newly created vCenter Server as admin user.
2. Click Create a data center.
3. Enter vHANA_DC_1 as the data center name.
4. Right-click the newly created vHANA_DC_1 data center and select New Cluster.
5. Name the cluster vHANA_Cluster and select the checkboxes for Turn On VMware vSphere HA and
   Turn on VMware vSphere DRS. Click Next.
6. Accept the defaults for vSphere DRS. Click Next.
7. Accept the defaults for Power Management. Click Next.
8. Accept the defaults for vSphere HA. Click Next.
10. Accept the defaults for VM Monitoring. Click Next.
11. Accept the defaults for VMware EVC. Click Next.

**Note:** If mixing Cisco UCS B or C-Series servers within a vCenter cluster, it is necessary to enable VMware Enhanced vMotion Compatibility (EVC) mode. For more information about setting up EVC mode, refer to [Enhanced vMotion Compatibility (EVC) Processor Support](#).

12. Select “Store the swapfile in the datastore specified by the host”. Click Next.
13. Click Finish.
14. Right-click the newly created vHANA_Cluster cluster and select Add Host.
15. In the Host field, enter either the IP address or the host name of the vHANA-Host-01 host. Enter root as the user name and the root password for this host. Click Next.
16. Click Yes.
17. Click Next.
18. Select Assign a New License Key to the Host. Click Enter Key and enter a vSphere license key. Click OK, and then click Next.
19. Click Next.
20. Click Next.
21. Click Finish. vHANA-Host-01 is added to the cluster.
22. Repeat the steps 14-21 to add vHANA-Host-02 to the cluster.
Virtual Machine for vHANA

SAP supports virtualization of SAP HANA on validated single-node SAP HANA appliances or through SAP HANA TDI verified hardware configurations. The existing SAP HANA storage requirements regarding partitioning, configuration and sizing of data, log and binary volumes remain valid. It is important to note that a vCPU is not exactly equivalent to a full physical core because it is mapped to a logical execution thread. When hyper-threading is enabled, a physical core has two execution threads. This means, two vCPUs are needed in order to use both of them. However, the additional thread created by enabling hyper-threading does not double the performance of the core. It has been determined that enabling hyper-threading usually increases overall SAP HANA system performance by approximately 20 percent.

Please refer to “SAP HANA Guidelines for running virtualized” for more information
http://scn.sap.com/docs/DOC-60312

Create a Virtual Machine for Virtualized SAP HANA (vHANA)

To build a virtual machine (VM) for vHANA, complete the following steps:
1. Log in to the vCenter web console using web browser https://<<IP_vCenter>>:9443
2. In the VMware vSphere web client, Click on vCenter, navigate to the Inventory Trees and Click on Hosts and Clusters

   ![VMware vSphere Web Client](image)

3. Expand the Data Center Created and right-click the vHANA_Cluster and select New Virtual Machine.
4. Select Create a new virtual machine and click Next
5. Enter a name for the virtual machine; select the Data center in vCenter. Click Next.
6. Under Select a computer resource choose the cluster vHANA_Cluster. Click Next.
7. Select vHANA_datastore_1 as Storage. Click Next.
8. Select compatibility; choose ESXi5.5 and later, which is Virtual Machine Version: 10. Click Next.
9. Linux as an option for Guest OS Family. For Guest OS Version Select
   a. SUSE Linux Enterprise 11 (64-bit) version is selected for SLES
   b. Red Hat Enterprise Linux 6 (64-bit) version is selected for RHEL
10. Click Next.
11. Under Customize hardware
    a. CPU: The configuration of the vCPU depends on underlying hardware in the configuration. In this example, select 2 virtual sockets and 15 cores per virtual socket. Total number of vCPU is 30.

**Note:** If the VM runs on Intel E7 v2 CPUs with 15 physical cores, then 15 cores should be configured in the vCPU settings. Remind that vCPUs reflect logical cores, so one physical CPU with 15 physical cores and with Hyperthreading enabled corresponds to 30 vCPUs. Please follow “SAP HANA Guidelines for running virtualized.”
b. The configuration of the Memory depends on underlying hardware and the memory size required for vHANA. In this example, 256GB of memory is selected. Check Reserve all guest memory (All locked)

c. Under New Hard disk edit 60 GB for OS
d. Network connection

e. Under New Network, select the vHANA-Access and the VMXNET 3 as Adapter Type

f. For the Second network interface cards (NIC), at the bottom of the screen New device: Choose Network from the drop down and click Add. For NIC 2, select the vHANA-Storage Network option and the VMXNET 3 as Adapter Type.

g. Click the VM Options, expand Boot Options and Select the Force BIOS Setup checkbox.

**Figure 193. VMware vSphere Web Client VM BIOS configuration**

12. Click Next

13. Click Finish to Create the Virtual Machine

14. Configuring the virtual machine to activate the accessor functions

   a. In the VMware vSphere Web Client, select the virtual machine just created and right-click it.

   b. In the dropdown menu, choose "Edit Settings".

   c. Choose the tab " VM Options".

   d. Expand "Advanced" and click "Edit Configuration".

   e. In the "Configuration Parameters" window, insert the following value by clicking Add Row tools.guestlib.enableHostInfo = "TRUE"
OS Installation for vHANA

1. Log in to the vCenter using the VMware vSphere Client.
2. In the VMware vSphere client, select the host in the inventory pane.
3. Right-click the VM created and click Open Console.
4. Click the third button (green right arrow) to power on the VM.
5. Click the ninth button (CD with a wrench) to map the Operating System ISO, and then select Connect to ISO Image on Local Disk.
6. Navigate to the ISO location, select it, and click Open.
   a. For SLES: SLES-11-SP3-SAP-DVD-x86_64-GM-DVD.iso
   b. For RHEL: rhel-server-6.5-x86_64-dvd.iso
7. Click in the BIOS Setup Utility window and use the right arrow key to navigate to the Boot menu. Use the down arrow key to select CD-ROM Drive. Press the plus (+) key twice to move CD-ROM Drive to the top of the list. Press F10 and Enter to save the selection and exit the BIOS Setup Utility.

SUSE Linux Enterprise Server

1. The following procedure shows the OS installation on local disk.

Note: Please use the SAP HANA installation Guides for OS customization requirement.
2. OS installer will start choose SLES for SAP Applications – Installation and Press Enter
3. Agree to the License Terms, Click Next
4. Leave New Installation selected and Click Next
5. Select Appropriate Region and Time Zone. Click Next.

**Note:** The recommendation from SAP is to set the server time zone on all SAP HANA nodes to UTC. Every user configured on the system can have an “own” time zone setting to work with the local time.

6. Under Choose Scenario Keep Physical Machine (also for Fully Virtualized Guests) selected and click Next
7. Click the Expert tab
8. Click Partitioning
9. In the Expert Partitioner screen,
10. Select Custom Partition (for experts) and Click Next
11. In the System View Expand Hard disks and select sda with 60 GB space
12. Click Add and leave Primary Partition as selected. Click Next
13. Choose Custom Size 100 MB. Click Next
14. File System leave Ext3 and change the Mount Point to /boot. Click Finish
15. Click Add and leave Primary Partition as selected. Click Next
16. Choose Custom Size 2.00 GB. Click Next
17. Change File System swap and change the Mount Point to swap. Click Finish
18. Click Add and leave Primary Partition as selected. Click Next
19. Leave the Size as remaining free space. Click Next
20. File System leave Ext3 and Leave the Mount Point a / Click Finish
21. Click Accept
22. On the Installation Settings screen click Software
23. Optionally uncheck GNOME Desktop Environment, if you do not wish to use Graphical Desktop. This optional will reduce the size used for root Partition by 300 MB. Recommend to de-select the “GNOME Desktop Environment” package.
24. Check C/C++ Compiler and Tools Under Development
25. Check SAP HANA Server Base Under Primary Functions
27. On the Installation Settings screen Change Time Zone as per the requirement
28. On the Installation Settings screen click on Default Runlevel
29. On the Set Default Runlevel screen select 3: Full multiuser with network and click OK
30. On the Installation Settings screen Click on Kdump
31. On the kdump Start-Up under Enable/Disable Kdump select Disable Kdump and click OK
32. Click and Install to perform the installation.
33. Wait for Installation to complete.
34. After reboot, system will continue the installation to customize the installed Operating System
35. Enter the Password for root User and Confirm Password, then click Next
36. Enter Hostname and Domain Name, uncheck Change Hostname via DHCP, then click Next
37. Under Network Configuration, keep Use Following Configuration selected
   a. Under General Network Settings Support for IPv6 protocol is enabled click Disable IPv6, on the Warning To apply this change, a reboot is needed Press OK
   b. Under Firewall ➔ Firewall is enabled Click disable
   c. Click on Network Interfaces configuration
   d. Under the Overview tab, Select the first device and click edit
   e. Choose Statically assigned IP Address and Enter the IP Address and Subnet Mask for vHANA-Access network
   f. Click the General tab and change MTU to 9000. Click Next
   g. For vHANA with external Storage Select the second NIC card and click edit
   h. Choose Statically assigned IP Address and Enter the IP Address and Subnet Mask for vHANA-Storage network
   i. Click the General tab and change MTU to 9000. Click Next
   j. Click Hostname/DNS tab, Enter the IP address of DNS servers under Name Server 1 and Name Server 2
j. Click Routing tab and enter the IP address of Default Gateway. Click OK
k. Click the VNC Remote Administration and select Allow Remote Administration. Click Finish
l. Optional if there is proxy server required for Internet access Click on Proxy Configuration, check Enable Proxy. Enter the HTTP Proxy URL, HTTPS Proxy URL or based on proxy server configuration check Use the Same Proxy for All Protocols. If proxy server requires Authentication enter Proxy User Name and Proxy Password and Click Finish
38. Click Next to finish Network Configuration
39. Under Test Internet Connection Choose No, Skip This Test
40. For Network Service Configuration choose default and Click Next
41. For User Authentication Method select default Local (/etc/passwd), additional methods can be done later if required.
42. Create New Local User, enter password and Confirm Password.
43. Release Notes, Click Next
44. Use Default Hardware Configuration, Click Next
45. Uncheck Clone This System for AutoYaST and Click Finish
46. Login as root to the system
47. Update the OS to latest patch level
48. Execute the below command to Register the SUSE

```
suse_register -l -r -n -a email=<<email_address>> -a regcode-sles=<<registration_code>>
```
49. After the registration, the entire repository will be updated
50. Execute the below command to update the server

```
zypper update
```
51. Follow the on screen instruction to complete the update process.
52. Reboot the server

Network Time

```
v1 /etc/ntp.conf
server <NTP-SERVER IP>
fudge <NTP-SERVER IP> stratum 10
keys /etc/ntp.keys
tustedkey 1
```
53. To configure the OS optimization setting for HANA follow the steps below.
54. Create a file /etc/init.d/after.local

```
v1 /etc/init.d/after.local
#!/bin/bash
# (c) Cisco Systems Inc. 2014

echo never > /sys/kernel/mm/transparent_hugepage/enabled
. /etc/rc.status

# set swappiness to 30 to avoid swapping
echo "Set swappiness to 30 to avoid swapping"
echo 30 > /proc/sys/vm/swappiness
. /etc/rc.status
```
55. Add the following lines to /etc/sysctl.conf

```
#SAP Note 1275776
vm.max_map_count = 2000000
fs.file-max = 2000000
fs.aio-max-nr = 196608
vm.memory_failure_early_kill = 1
net.ipv4.tcp_slow_start_after_idle = 0
#
# NetApp TR-4290
#
net.core.rmem_max = 16777216
net.core.wmem_max = 16777216
net.core.rmem_default = 262144
net.core.wmem_default = 262144
net.core.optmem_max = 16777216
net.core.netdev_max_backlog = 300000
```
net.ipv4.tcp_rmem = 65536 262144 16777216
net.ipv4.tcp_wmem = 65536 262144 16777216
net.ipv4.tcp_no_metrics_save = 1
net.ipv4.tcp Moderate_rcvbuf = 1
net.ipv4.tcp_window_scaling = 1
net.ipv4.tcp_timestamps = 1
net.ipv4.tcp_sack = 1
sunrpc.tcp_slot_table_entries = 128
# Memory Page Cache Limit Feature SAP Note 1557506
vm.pagecache_limit_mb = 4096
vm.pagecache_limit_ignore_dirty = 1

56. Edit boot loader configuration file /etc/sysconfig/bootloader. Edit this file and append the following value to the "DEFAULT_APPEND" parameter value:

```
intel_idle.max_cstate=0
```

57. Append the "intel_idle.max_cstate=0 processor.max_cstate=0" value to the kernel's parameter line in /boot/grub/menu.lst

```
title SLES for SAP Applications - 3.0.101-0.46
  root (hd0,0)
kernal /vmlinuz-3.0.101-0.46-default root=/dev/sda3 resume=/dev/sda2 splash=silent
showopts intel_idle.max_cstate=0 processor.max_cstate=0
initrd /initrd-3.0.101-0.46-default
```

58. Reboot the server

Install VMware Tools
1. Click VM in the virtual machine menu, then click Guest > Install/Upgrade VMware Tools and click OK.
2. Create a mount point to mount ISO

```
mkdir /mnt/cdrom
```
3. Mount cdrom

```
mount /dev/cdrom /mnt/cdrom
```
4. Copy the Compiler gzip tar file to a temporary local directory, run:

```
cp /mnt/cdrom/VMwareTools-<<version>>.tar.gz /tmp/
```
5. Untar the copied file

```
cd /tmp
  tar -zxvf VMwareTools-version.tar.gz
```
6. Change directory to extracted vmware-tools-distrib and run the vmware-install.pl PERL script.

```
cd /tmp/vmware-tools-distrib
  ./vmware-install.pl
```
7. Follow the onscreen instruction to complete the VMware tools installation.
8. Reboot the VM
9. For VM template creation, clean up the master OS image
   a. Log in to the vHANA system
   b. Clear the System logs
   c. Clear the Ethernet Persistent network information
      ```
cat /dev/null > /etc/udev/rules.d/70-persistent-net.rules
```
   d. Remove any Ethernet configuration file
      ```
rm /etc/sysconfig/network/ifcfg-eth*
```
   e. Remove default gateway
      ```
rm /etc/sysconfig/network/routes
```
   f. Shut the OS master by executing “halt”
RHEL Installation
1. The following procedure shows the OS installation on local disk.

Note: Please use the SAP HANA installation Guides for OS customization requirement

2. OS installer will start choose ‘Install or upgrade an existing system’ from the Menu and Press Enter.

Figure 200. vHANA RHEL OS Install screen

3. Skip the media test to start the installation
4. On the Installation screen, click Next
5. Choose Language and Keyboard layout. Click Next
6. Select the ‘Basic Storage Devices’ from the menu and click ‘Next’

7. Enter the Hostname

   **Figure 203. vHANA RHEL Hostname**

8. Click Configure Network

9. Select eth0 and click edit

10. Set MTU to 9000 and Click on IPv4 Settings
11. Choose Manual Method, Click on Add, Enter IP address, Netmask and Gateway for vHANA-Access Network
12. Enter DNS Servers and Search domains. Click Apply
13. For vHANA with external Storage, Select the eth1 and Click edit
14. Set MTU to 9000 and Click on IPv4 Settings,
15. Choose Manual Method, Click on Add, Enter IP address, Netmask and Gateway for vHANA-Storage Network. Click Apply and Click Close, then Click Next
16. Select the appropriate Time Zone and Click ‘Next’
17. Enter the root password and confirm. Click ‘Next’
18. Select ‘Create Custom layout’ for customized disk partitioning and Click ‘Next’
19. With the disk sdd create two partitions for /boot and root volume group
   
a. Click Create, Choose Standard Partition and Click Create

   b. Choose /boot as mount point, File System Type ext3 and Size 200 MB and Click OK
Figure 207. vHANA RHEL Disk Layout for Boot

Click Create, Choose LVM Physical Volume and click Create
Figure 208. vHANA RHEL LVM for Disk

- Create Partition
  - Standard Partition
    - General purpose partition creation

- Create Software RAID
  - RAID Partition
    - Create a RAID formatted partition
  - RAID Device
    - Requires at least 2 free RAID formatted partitions

- Create LVM
  - LVM Volume Group
    - Requires at least 1 free LVM formatted partition
  - LVM Logical Volume
    - Create a logical volume on selected volume group
  - **LVM Physical Volume**
    - Create an LVM formatted partition

- Select Fill to maximum allowable size and click OK
Click Create, Choose LVM Volume Group and click Create
f. Enter rootvg as Volume Group Name.

Figure 211. vHANA RHEL LVM Root Volume Group

Click Add Under Logical Volumes
h. Choose File System Type swap, Enter Logical Volume Name swapvol and Size (MB) 2048. Click OK

Figure 212. vHANA RHEL Swap Volume

i. Click on Add Under Logical Volumes

j. Choose Mount Point /, File System Type ext3, Enter Logical Volume Name rootvol and Leave Max Size. Click OK

Figure 213. vHANA RHEL Root Partition

k. Click OK

l. The final disk layout screen should look similar below screen.
20. Click ‘Next’ to proceed with the next step of the installation
21. Select the installation mode as ‘Minimal and click ‘Next’
22. The installer starts the installation process and wait until it is completed
23. When the installation is completed, the server requires a reboot. Click Reboot
24. Log in to the newly installed system as root
25. Edit the file /etc/ntp.conf to reflect the appropriate ntp servers for the region and start the ntp service

```
```

26. Updating the RedHat system

**Note:** In order to patch the system, the repository must be updated. Note that the installed system does not include any update information. In order to patch the RedHat System, it must be registered and attached to a valid subscription.

The following line will register the installation and update the repository information.

```
[root@vhana-02 ~]# subscription-manager register --username <<username>> --password <<password>> --force --auto-attach
```

27. Update only the OS kernel and firmware packages to the latest release that appeared in RHEL 6.5.

According to SAP Note 2013638 - SAP HANA DB: Recommended OS settings for RHEL, SAP HANA is currently certified for RHEL 6.5 only. To lock the kernel version to the last available kernel of the 2.6.32-431 series you need the yum-versionlock plugin

```
[root@vhana02 ~]# yum -y install yum-versionlock
```

28. Configure the plugin with adding an entry in the appropriate configuration file:

```
[root@vhana02 ~]# echo kernel-2.6.32-431.* > /etc/yum/pluginconf.d/versionlock.list
[root@vhana02 ~]# echo kernel-firmware-2.6.32-431.* >> /etc/yum/pluginconf.d/versionlock.list
```

29. Only security updates may be applied. Install the yum-security plugin:

```
[root@vhana02 ~]# yum -y install yum-security
```

30. Depending on the repository configuration, nss-softokn-freebl can be updated during the security update process. Check for this with:
31. Apply the security updates. Typically, the kernel is updated as well:

```bash
[root@vhana02 ~]# yum versionlock nss-softokn-freebl nss-softokn
```

32. The firmware package should be in sync with the kernel revision. Install it with:

```bash
[root@vhana02 ~]# yum --security update
```

33. Reboot the machine and use the new kernel:

34. Install the base package group

```bash
[root@vhana02 ~]# yum -y groupinstall base
```

35. Install dependencies in accordance with the SAP HANA Server Installation and Update Guide and the numactl package if the benchmark HW/CCT is to be used

```bash
[root@vhana02 ~]# yum install gtk2 libicu xulrunner ntp sudo tcsh libssh2 \expect cairo graphviz iptraf krb5-workstation krb5-libs.i686 nfs-utils lm_sensors rsyslog compat-sap-c++ openssli098e openssl PackageKit-gtk-module libcanberra-gtk2 libtool-ltdl xauth compat-libstdc++-33 openssl PackageKit-gtk-module libcanberra-gtk2 libtool-ltdl xauth compat-libstdc++-33 numactl
```

36. Disable SELinux

```bash
[root@vhana-02 ~]# vi /etc/sysconfig/selinux
```

```bash
# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=disabled
# SELINUXTYPE= can take one of these two values:
#     targeted - Targeted processes are protected,
#     mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

37. Disable kdump service

```bash
[root@vhana-02 ~]# service kdump stop
[root@vhana-02 ~]# chkconfig kdump off
```

38. Compat-sap-c++ : Install the most important package `compat-sap-c++` from the RHEL for SAP HANA

```bash
[root@vhana-02 ~]# rpm –ivh compat-sap-c++-4.7.2-10.el6_5.x86_64.rpm
```

39. Tuned SAP HANA Profile: Install and configure the package `tuned-profiles-sap-hana` from the RHEL for SAP HANA

```bash
[root@osmaster ~]# rpm -ivh tuned-0.2.19-13.el6_6.1.noarch.rpm
[root@vhana-02 ~]# rpm -ivh tuned-profiles-sap-hana-0.2.19-13.el6_6.1.noarch.rpm
[root@vhana-02 ~]# tuned-adm profile sap-hana-vmware
```

40. Sysctl.conf: The following parameters must be set in `/etc/sysctl.conf.

**Note:** The SAP HANA Installer adds some of the configuration parameters; therefore, `/etc/sysctl.conf` should be configured after SAP HANA is installed.

```bash
# Parameters for HANA
net.ipv4.tcp_slow_start_after_idle=0
net.ipv4.conf.all.rp_filter=0
net.ipv4.ip_local_port_range=40000 61000
net.ipv4.neigh.default.gc_thresh1=256
net.ipv4.neigh.default.gc_thresh2=1024
net.ipv4.neigh.default.gc_thresh3=4096
net.ipv6.neigh.default.gc_thresh1=256
net.ipv6.neigh.default.gc_thresh2=1024
```
41. Add the following line into etc/modprobe.d/sunrpc-local.conf, Create the file, if it does not exist.

```
sunrpc.tcp_max_slot_table_entries = 128
```

42. For compatibility reasons, four symbolic links are required:

```
# ln -s /usr/lib64/libssl.so.0.9.8e /usr/lib64/libssl.so.0.9.8
# ln -s /usr/lib64/libssl.so.1.0.1e /usr/lib64/libssl.so.1.0.1
# ln -s /usr/lib64/libcrypto.so.0.9.8e /usr/lib64/libcrypto.so.0.9.8
# ln -s /usr/lib64/libcrypto.so.1.0.1e /usr/lib64/libcrypto.so.1.0.1
```

43. Transparent Hugepages In the file /boot/grub/grub.conf add the kernel command line argument

```
transparent_hugepage=never
```

44. Use a tuned profile to minimize latencies:

```
# yum -y install tuned
# tuned-adm profile latency-performance
# chkconfig tuned on
# service tuned start
```

44. Disable Crash Dump

```
# chkconfig abrtd off
# chkconfig abrt-ccpp off
# service abrtd stop
# service abrt-ccpp stop
```

45. Disable core file creation. To disable core dumps for all users, open /etc/security/limits.conf, and add the line

```
* soft core 0
* hard core 0
```

46. Adaptation of the Basic SAP Notes Settings
47. Edit the `/boot/grub/menu.lst` and append the below parameter to the kernel line per SAP Note

```
intel_idle.max_cstate=0
```

48. Reboot the OS.

**Install VMware Tools**

1. Click VM in the virtual machine menu, then click Guest > Install/Upgrade VMware Tools and click OK.
2. Create a mount point to mount ISO

```
mkdir /mnt/cdrom
```

3. Mount cdrom

```
mount /dev/cdrom /mnt/cdrom
```

4. Copy the Compiler gzip tar file to a temporary local directory, run:

```
cp /mnt/cdrom/VMwareTools-<<version>>.tar.gz /tmp/
```

5. Untar the copied file

```
cd /tmp
```
```
tar -zxvf VMwareTools-version.tar.gz
```

6. Change directory to extracted vmware-tools-distrib and run the vmware-install.pl PERL script.

```
```
cd /tmp/vmware-tools-distrib
```
```
./vmware-install.pl
```

7. Follow the onscreen instruction to complete the VMware tools installation.
8. Reboot the VM.
9. For VM template creation, clean up the master OS image
   a. Log into vHANA server
   b. Remove the Red Hat Registration information

```
subscription-manager unregister
```

   c. Clear the System logs

```
rm /var/log/* -r
```

   d. Clear the Ethernet Persistent network information

```
cat /dev/null > /etc/udev/rules.d/70-persistent-net.rules
```

10. Remove any Ethernet configuration file

```
rm /sysconfig/network-scripts/ifcfg-eth*
```

**vHANA Template**

The Virtual Machine created for vHANA can be converted to VM template and this template can be used to deploy multiple vHANA system with customized hardware and storage size.

**Note:** It is mandatory to connect the ESXi host to vCenter Server to enable VM deployment from templates and edit VM hardware.

To create a virtual machine (VM) template for vHANA, complete the following steps:
1. Log in to the vCenter using the VMware vSphere Client.
2. In the VMware vSphere client, select the Inventory ➔ VMs and Templates
3. Right-click the vHANA Virtual Machine
4. Select Template ➔ Convert to Template

**Deploy vHANA from the Template**

To deploy vHANA from the template, complete the following steps:
1. Log in to the vCenter using the VMware vSphere Client.
2. In the VMware vSphere Client, select the Inventory ➔ VMs and Templates
3. Right-click the vHANA Template. Select Deploy Virtual Machine from this Template.
4. Enter the Name of the vHANA Virtual Machine; Choose the Data Center and VM Directory. Click Next
5. Choose the Cluster. Click Next
6. Choose the Datastore. Click Next
7. Customize using the Customization Wizard
   a. Enter the Computer Name and Domain Name. Click Next
   b. Choose the Time Zone. Click Next
   c. Under Network Choose Custom Settings
   d. Click NIC1 and Enter IP Address, Subnet Mask and Default Gateway for vHANA-Access network
   e. For external Storage click on NIC2 and Enter IP Address, Subnet Mask for vHANA-Storage network. Click Next
   f. Enter the DNS server and Domain Name. Click Next
   g. (Optional) Save the Customization.
   h. Click Finish
8. Click Edit virtual hardware. Click Continue
   a. Edit Memory to increase or decrease the Memory Size.
   b. Edit the vCPU setting to add or remove number of cores.

Note: Please follow SAP guideline for CPU memory ratio.
9. Click OK

Storage for vHANA
The storage configuration and sizing for vHANA is identical to bare metal servers, which has been described in the section ‘Storage for SAP HANA’
The example below illustrates how to create volumes for 256 GB vHANA solution
1. Open SSH connection to NetApp cluster IP and log in as admin user with the password.
2. vHANA DATA
   Execute the below commands to create data volume name vhana01_data in the aggregate aggr_hana01 with size 256 GB with export policy vhana-vm
   ```bash
   volume create -vserver hana_vs1 -volume vhana01_data -aggregate aggr_hana01 -size 256GB -state online -policy vhana-vm -junction-path /vhana01_data -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none
   ```
3. vHANA LOG
   Execute the below commands to create log volume name vhana01_log in the aggregate aggr_hana02 with size 128 GB with export policy vhana-vm
   ```bash
   volume create -vserver hana_vs1 -volume vhana01_log -aggregate aggr_hana02 -size 128GB -state online -policy vhana-vm -junction-path /vhana01_log -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none
   ```
4. vHANA Shared
   Execute the below commands to create shared volume name vhana01_sapexe in the aggregate aggr_hana02 with size 256 GB with export policy vhana-vm
   ```bash
   volume create -vserver hana_vs1 -volume vhana01_sapexe -aggregate aggr_hana02 -size 256GB -state online -policy vhana-vm -junction-path /vhana01_sapexe -space-guarantee file -percent-snapshot-space 0 -snapshot-policy none
   ```
5. To use NFS for SAP HANA data and log volumes add the following lines to /etc/fstab entry for vHANA
   ```bash
   #HANA Shared
   vhana-lif01:/vhana01_sapexe /hana/shared nfs rw,bg,vers=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock 0 0
   vhana-lif01:/vhana01_log /hana/log nfs rw,bg,vers=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock 0 0
   vhana-lif01:/vhana01_data /hana/data nfs rw,bg,vers=3,hard,timeo=600,rsize=65536,wsize=65536,intr,actimeo=0,noatime,nolock 0 0
   ```
6. Update the /etc/hosts entry to reflect vhana-lif01 and vhana-lif02 IPs

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Host Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.51.12</td>
<td>vhana-lif01</td>
</tr>
<tr>
<td>192.168.51.13</td>
<td>vhana-lif02</td>
</tr>
</tbody>
</table>

7. Create the required directory to mount /hana/shared /hana/data and /hana/log volumes.

8. Mount all the volumes from /etc/fstab using “mount –a”

```
vhana-01:~ # df -h

Filesystem                   Size  Used Avail Use% Mounted on
/dev/sda3                     57G  3.6G   51G   7% /
udev                         127G  144K  127G   1% /dev
tmpfs                        127G  648K  127G   1% /dev/shm
/dev/sda1                     98M   25M   68M  27% /boot
vhana-lif01:/vhana01_sapexe  256G  128K  256G   1% /hana/shared
vhana-lif01:/vhana01_data    256G  128K  256G   1% /hana/data
vhana-lif02:/vhana01_log     128G  128G  128G   1% /hana/log
```

9. Make sure that the <SID>adm user owns the data and log volumes – use the chown command after the file systems are mounted.
SAP HANA Installation

Please use the official SAP documentation, which describes the installation process with and without the SAP unified installer.

SAP HANA installation documentation:

SAP HANA Server Installation Guide

All other SAP installation and administration documentation is available under:

http://service.sap.com/instguides

Important SAP Notes

Read the following SAP Notes before you start the installation. These SAP Notes contain the latest information about the installation, as well as corrections to the installation documentation.

The latest SAP Notes can be found at: https://service.sap.com/notes.

SAP HANA IMDB Related Notes
- SAP Note 1514967 - SAP HANA: Central Note
- SAP Note 2004651 - SAP HANA Platform SPS 08 Release Note
- SAP Note 2075266 - SAP HANA Platform SPS 09 Release Note
- SAP Note 1523337 - SAP HANA Database: Central Note
- SAP Note 2000003 - FAQ: SAP HANA
- SAP Note 1730999 - Configuration changes in SAP HANA appliance
- SAP Note 1514966 - SAP HANA 1.0: Sizing SAP In-Memory Database
- SAP Note 1780950 - Connection problems due to host name resolution
- SAP Note 1780950 - SAP HANA SPS06: Network setup for external communication
- SAP Note 1743225 - SAP HANA: Potential failure of connections with scale out nodes
- SAP Note 1755396 - Released DT solutions for SAP HANA with disk replication
- SAP Note 1890444 - HANA system slow due to CPU power save mode
- SAP Note 1681092 - Support for multiple SAP HANA databases on a single SAP HANA appliance
- SAP Note 1514966 - SAP HANA: Sizing SAP HANA Database
- SAP Note 1637145 - SAP BW on HANA: Sizing SAP HANA Database
- SAP Note 1793345 - Sizing for Suite on HANA

Linux Related Notes
- SAP Note 1944799 - SAP HANA Guidelines for SLES Operating System
- SAP Note 2009879 - SAP HANA Guidelines for RedHat Enterprise Linux (RHEL)
- SAP Note 1824819 - SAP HANA DB: Recommended OS settings for SLES11/SLES4SAP SP2
- SAP Note 1731000 - Non-recommended configuration changes
- SAP Note 1557506 - Linux paging improvements
- SAP Note 1310037 - SUSE Linux Enterprise Server 11 - installation notes
- SAP Note 1726839 - SAP HANA DB: potential crash when using xfs filesystem
- SAP Note 1740136 - SAP HANA: wrong mount option may lead to corrupt persistency
- SAP Note 1829651 - Time zone settings in SAP HANA scale out landscapes

SAP Application Related Notes
- SAP Note 1658845 - SAP HANA DB hardware check
- SAP Note 1637145 - SAP BW on SAP HANA: Sizing SAP In-Memory Database
- SAP Note 1661202 - Support for multiple applications on SAP HANA
High-Availability (HA) Configuration for Scale-Out
Since HANA revision 35, the ha_provider python class supports the STONITH functionality. STONITH = Shoot The Other Node In The Head. With this python class, we are able to reboot the failing node to prevent a split brain and thus an inconsistency of the database. Since we use NFSv3, we must implement the STONITH functionality to prevent the database for a corruption because of multiple access to mounted file systems. If a HANA node is failed over to another node, the failed node will be rebooted from the master name server. This eliminates the risk of multiple access to the same file systems.

High-Availability Configuration
The used version of the ucs_ha_class.py must be at least 1.1

```python
vi ucs_ha_class.py

```
Prepare the script to match the Cisco UCS Manager configured ipmi username and password. Default is ipmi-user sapadm and ipmi-user-password cisco.

```bash
#!/bin/bash
#set -x
# Cisco Systems Inc.
# SAP HANA High Availability
# Version 1.1 07/2014
# changelog: 09/16: -I lanplus

if [ -z $1 ]
then
    echo "please add the hostname to reset to the command line"
    exit 1
fi

# Trim the domain name off of the hostname
host=`echo "$1" | awk -F'.' '{print $1}'`
PASSWD=cisco
USER=sapadm

echo $host-ipmi

# Shut down the server via ipmitool power off
#/bin/logger `whoami"" Resetting the HANA Node $host because of an Nameserver reset command"
rc1="/usr/bin/ipmitool -I lanplus -H $host-ipmi -U $USER -P $PASSWD power status"
if [ "$rc1" = 'Chassis Power is on' ]
then
    power="on"
    rc2="/usr/bin/ipmitool -I lanplus -H $host-ipmi -U $USER -P $PASSWD power off"
    sleep 5
    rc3="/usr/bin/ipmitool -I lanplus -H $host-ipmi -U $USER -P $PASSWD power status"
    echo RC3: $rc3
    if [ "$rc3" = 'Chassis Power is on' ]
    then
        rc2="/usr/bin/ipmitool -I lanplus -H $host-ipmi -U $USER -P $PASSWD power off"
        sleep 10
```
Copy the HA scripts to the shared HA directory under /hana/shared/<SID>/HA
(HANA nameserver is responsible to reset the failed node)

```
ssh cishana01
mkdir /hana/shared/T01/HA
chown t01adm:sapsys /hana/shared/T01/HA
scp ucs_ipmi_reset.sh /hana/shared/T01/HA/
scp ucs_ha_class.py /hana/shared/T01/HA/
chown t01adm:sapsys /hana/shared/T01/HA/*
```

**Enable the SAP HANA Storage Connector API**

The SAP Storage Connector API provides a way to call a user procedure whenever the SAP HANA Nameserver triggers a node failover. The API requires the files mentioned above. The procedure is executed on the master nameserver.
To activate the procedure in case of a node failover, the global.ini file in `<HANA installdirectory>/<SID>/global/hdb/custom/config/` must be edited and the following entry must be added:

```ini
[Storage]
ha_provider = ucs_ha_class
ha_provider_path = /hana/shared/<SID>/HA
```

```bash
cd /hana/shared/<SID>/global/hdb/custom/config
vi global.ini
```

```ini
[persistence]
basepath_datavolumes=/hana/data/ANA
basepath_logvolumes=/hana/log/ANA

[storage]
ha_provider = ucs_ha_class
ha_provider_path = /hana/shared/T01/HA
```

Modify the `/etc/sudoers` file and append the below line on all the nodes. By adding the line `<sid>adm` account can execute commands mentioned without password.

```bash
cishana01:/ # vi /etc/sudoers

<sid>adm ALL=NOPASSWD: /bin/mount, /bin/umount, /bin/logger, /sbin/multipath, /sbin/multipathd, /usr/bin/sg_persist, /etc/init.d/multipathd, /bin/kill, /usr/bin/lsof, /sbin/vgchange, /sbin/vgscan
```

To activate the change, please restart the SAP HANA DB.

**Test the IPMI connectivity**

Test the ipmi connectivity on ALL nodes

```bash
cishana01:- # ipmitool -I lanplus -H cishana01-ipmi -U sapadm -P cisco power status
Chassis Power is on
```

Make sure that all nodes are responding to the ipmitool command and the IP address for the ipmi network match in the `/etc/hosts` file of all the servers.
Appendix A

Linux Kernel Crash Dump

In the event of server hangs, system panics or a Linux kernel crash, Kdump is used to capture kernel's memory for analysis. This section describes how to configure the Server in order to capture kernel crash dump.

Configure the System for Capturing Kernel Core Dumps

1. Make sure you have the following packages installed: kdump, kexec-tools, and makedumpfile.
2. Reserve memory for the capture kernel by passing “crashkernel=768M” parameter to the primary kernel in the PXE boot configuration file.

```
mgmtsrv01:/tftpboot/pxelinux.cfg # vi cishana01
# SAP UCS PXE Boot Definition
display ../boot.msg
default SLES11_SP3
prompt 1
timeout 10
LABEL SLES11_SP3
  KERNEL vmlinuz
    APPEND initrd=initrd rw rootdev=192.168.127.10:/vol/cishana01
  intel_idle.max_cstates=0 processor.max_cstate=0 crashkernel=768M ip=dhcp
```

3. Activate the kdump system service

   Run

   ```
   # chkconfig boot.kdump on
   ```

4. Root file system does not have enough space to store a complete memory dump – This will be up to the size of physical memory for a single SAP HANA node. Instead of a local dump destination, an NFS share can be used. Add the network device to be used for the variable: KDUMP_NETCONFIG in /etc/sysconfig/kdump. In order to automatically set up a network device, pass the option "auto". This option will use eth0 and obtain the IP from DHCP server.

   ```
   ## Type:        string
   ## Default:     auto
   ## ServiceRestart:      kdump
   #
   # Network configuration. Use "auto" for auto-detection in initrd, or a string
   # that contains the network device and the mode (dhcp,static), separated by
   # a colon. Example: "eth0:static" or "eth1:dhcp".
   #
   # For static configuration, you have to add the configuration to
   # KDUMP_COMMANDLINE_APPEND.
   #
   # See also: kdump(5)
   #
   KDUMP_NETCONFIG="auto"
   ```

5. Pass the dumping method and the destination directory to the parameter: KDUMP_SAVEDIR in /etc/sysconfig/kdump

   Supported methods are:

   ```
   ## Type:        string
   ```
## Default:
"file:///var/log/dump"
## ServiceRestart:  kdump
#
# Which directory should the dumps be saved in by the default dumper?
# This can be:
#
# - a local file, for example "file:///var/log/dump" (or, deprecated, just "/var/log/dump")
# - a FTP server, for example "ftp://user:password@host/var/log/dump"
# - a SSH server, for example "ssh://user:password@host/var/log/dump"
# - a NFS share, for example "nfs://server/export/var/log/dump"
# - a CIFS (SMB) share, for example "cifs://user:password@host/share/var/log/dump"
#
# See also: kdump(5) which contains an exact specification for the URL format.
# Consider using the "yast2 kdump" module if you are unsure.
# KDUMP_SAVEDIR="nfs://192.168.127.14/vol/os_crashdump"

Note: KDUMP_SAVEDIR should have sufficient space to prevent hanging systems waiting for completing the Kdump procedure.

Set Up Magic SysRq (recommended)
For kernel problems other than a kernel oops or panic, a kernel core dump is not triggered automatically. If the system still responds to keyboard input to some degree, a kernel core dump can be triggered manually through a "magic SysRq" keyboard combination (typically: hold down three keys simultaneously: the left Alt key, the Print Screen / SysRq key and a letter key indicating the command - 's' for sync, 'c' for core dump), if this feature has been enabled.

1. Magic SysRq can be configured in Cisco UCS Manger from KVM console → Macros → User Defined Macros → Manage → New

![Configure User Defined Macros](image)

2. To enable the magic SysRq feature permanently, edit /etc/sysconfig/sysctl, change the ENABLE_SYSRQ line to ENABLE_SYSRQ="yes". This change becomes active after a reboot.

```bash
# vi /etc/sysconfig/sysctl
## Path: System/Kernel
## Description: string
# Magic SysRq Keys enable some control over the system even if it crashes (e.g. during kernel debugging).
# Possible values:
# - no: disable sysrq completely
# - yes: enable all functions of sysrq
# bitmask of allowed sysrq functions:
```
3. To enable the feature for the running kernel, run

```
# echo 1>/proc/sys/kernel/sysrq
```

4. Reboot the system for the settings to take effect.

**Troubleshooting**

1. After reboot to make sure kdump is working correctly, check if boot.kdump service is started.

```
server01:~ # service boot.kdump status
kdump kernel loaded    running
server01:~ # service boot.kdump restart
Loading kdump
    done
```

2. If the kernel parameter “crashkernel=768M” is not passed correctly, you will see the error as below.

```
server01:~ # service boot.kdump start
Loading kdump
Regenerating kdump initrd ...
Then try loading kdump kernel
Memory for crashkernel is not reserved
Please reserve memory by passing "crashkernel=X@Y" parameter to the kernel
    failed
```

3. After the boot.kdump service is started, execute “depmod” which handle dependency descriptions for loadable kernel modules. If you are missing any driver it will show the warning, please make sure you have vNIC drivers otherwise, crash kernel will not function properly.

```
server01:~ # depmod
WARNING: Can't read module /lib/modules/3.0.80-0.7-default/weak-updates/updates/fnic.ko: No such file or directory
```

4. Execute the command mkinitrd, which creates initial ramdisk images for preloading modules, make sure network and nfs modules are included in the crash kernel. If you are missing nfs module, please check root “/” mount point in /etc/fstab entry.

```
server01:~ # mkinitrd
Kernel image: /boot/vmlinuz-3.0.80-0.7-default
```
Initrd image:  /boot/initrd-3.0.80-0.7-default
Kernel Modules:  hwnum thermal_sys thermal processor fan scsi_mod megaraid_sas
scsi_tgt scsi_transport_fc libfc libfcoe fnic af_packet enic sunrpc nfs_acl
auth_rpcgss fscache lockd nfs scsi_dh scsi_dh_alua scsi_dh_emc scsi_dh_hp_sw
scsi_dh_rdac usb-common usbcore ohci-hcd uhci-hcd ehci-hcd hid usbhid crc-
t10dif sd_mod
Features:    acpi usb network nfs resume.userspace resume.kernel
42493 blocks
<<< Calling mkinitrd -B -k /boot/vmlinuz-3.0.80-0.7-default -i
/tmp/mkdumprd.vqjQzDCHv2 -f 'kdump network' -s ''
Regenerating kdump initrd ...

Kernel image:   /boot/vmlinuz-3.0.80-0.7-default
Initrd image:   /tmp/mkdumprd.vqjQzDCHv2
Kernel Modules:  hwnum thermal_sys thermal processor fan scsi_mod megaraid_sas
scsi_tgt scsi_transport_fc libfc libfcoe fnic af_packet enic sunrpc nfs_acl
auth_rpcgss fscache lockd nfs scsi_dh scsi_dh_alua scsi_dh_emc scsi_dh_hp_sw
scsi_dh_rdac usb-common usbcore ohci-hcd uhci-hcd ehci-hcd hid usbhid nls_utf8
crc-t10dif sd_mod
Features:    acpi usb network nfs resume.userspace resume.kernel kdump
55144 blocks
Don't refresh the bootloader. You may have to do that manually!

5. Reboot your system for kdump to configure.

Test Local Kernel Core Dump Capture

To test the local kernel core dump capture, follow these steps.
If magic SysRq has been configured:
1. Magic-SysRq-S to sync (flush out pending writes)
2. Magic-SysRq-C to trigger the kernel core dump
3. Alternatively, without magic SysRq:
4. Open a shell or terminal
5. Run sync
6. Run echo c >/proc/sysrq-trigger

The system will boot the crash kernel and start the kernel dump. This can be observed on KVM console of the Cisco UCS manager. Once the system completes the crash dump, verify that a capture file created on
192.168.127.14/vol/os_crashdump/date example 192.168.127.10/vol/os_crashdump/2013-07-13-16:18. As per the parameter set on /etc/sysconfig/kdump
(KDUMP_SAVEDIR="nfs://192.168.127.14/vol/os_crashdump")

As per the http://www.novell.com/support/kb/doc.php?id=3374462, a kernel core dump can be triggered manually through a "magic SysRq" keyboard combination. This can be helpful if the system is hanging instead of going into a kernel panic.

OS Settings for Console Redirection

Add or uncomment the following in /etc/inittab:
se:2345:respawn:/sbin/agetty 115200 ttyS0

Added the following to /etc/security:
ttyS0

Configuration of the file /tftpboot/pxelinux.cfg/<IP in HEX>
Appended the following text to the APPEND line
console=tty1 console=ttyS0,115200
```bash
mgmtsrv01:/tftpboot/pxelinux.cfg # cat C0A87F5B
# SAP UCS PXE Boot Definition
display ../boot.msg
default SLES11_SP2
prompt 1
timeout 10
LABEL SLES11_SP2
  KERNEL vmlinuz-default
  APPEND initrd=initrd_cisco.gz rw
  rootdev=192.168.127.11:/FS_OS_01/SLES11SP2 rootfsopts=default
  intel_idle.max_cstate=0 ip=dhcp console=tty1 console=ttyS0,115200
  crashkernel=256M-:4G

With this, the Console redirection for SUSE Linux is configured.

Logon to Serial Console

Welcome to SLES for SAP Applications 11.2 (x86_64) - Kernel 3.0.80-0.7-default [ttyS0].
cishanar04 login: 

Serial Console POST screen

Cisco Systems, Inc.
Configuring and testing memory, please wait... Complete.
Configuring and testing platform hardware...
Serial Console Boot Menu

Serial Console OS Booted

Welcome to SUSE Linux Enterprise Server 11 SP2 (x86_64) - Kernel 3.0.13-0.27-default (ttyS0).
Appendix B

Cisco Nexus 9000 Example Configurations of FlexPod for SAP HANA

Cisco Nexus 9000 A

```
hostname NX9K-A
vdc NX9k-A id 1
  allow feature-set fex
  allocate interface Ethernet1/1-48
  allocate interface Ethernet2/1-12
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

cfs eth distribute
feature udld
feature interface-vlan
feature lacp
feature vpc
feature lldp

username admin password 5 $1$vLVKV/5d$bIjkUqsf3kHjKUyJGxZrw1 role
network-admin
no password strength-check
ip domain-lookup
errdisable recovery interval 30
copp profile strict

snmp-server user admin network-admin auth md5
0x3a6326308ce673d7cdb3cf7f0e4b749 priv
0x3a6326308ce673d7cdb3cf7f0e4b749 localizedKey
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
ntp server 172.26.163.254 use-vrf management

vlan 1,110,112,127,201,220-225,510,520,1371-1372,3110-3112

vlan 110
  name HANA-Storage
vlan 112
  name HANA-Admin
vlan 127
  name HANA-Boot
```
vlan 201
   name Temp-Storage
vlan 220
   name HANA-Internal
vlan 221
   name HANA-Backup
vlan 222
   name HANA-Client
vlan 223
   name HANA-AppServer
vlan 224
   name HANA-DataSource
vlan 225
   name HANA-Replication
vlan 510
   name vHANA-Storage
vlan 520
   name vHANA-Access
vlan 1371
   name iSCSI-VLAN-A
vlan 1372
   name iSCSI-VLAN-B
vlan 3110
   name ESX-NFS
vlan 3111
   name ESX-MGMT
vlan 3112
   name ESX-vMotion

cdp timer 5
spanning-tree port type edge bpduguard default
spanning-tree port type edge bpdufilter default
spanning-tree port type network default
vrf context management
   ip route 0.0.0.0/0 172.25.186.1

vpc domain 50
peer-switch
   role priority 10
peer-keepalive destination 177.78.78.2 source 177.78.78.1
delay restore 150
peer-gateway
   auto-recovery

interface port-channel11
   description VPC-Peer
   switchport mode trunk
   switchport trunk allowed vlan 110,112,127,220-225
   switchport trunk allowed vlan add 510,520,1371-1372,3110-3112
   spanning-tree port type network
   vpc peer-link

interface port-channel111
   description VPC to FI-A
   switchport mode trunk
   switchport trunk allowed vlan 110,112,127,220-225
spanning-tree port type edge trunk
mtu 9216
vpc 11

interface port-channel12
  description VPC to FI-B
  switchport mode trunk
  switchport trunk allowed vlan 110,112,127,220-225
  spanning-tree port type edge trunk
  mtu 9216
  vpc 12

interface port-channel21
  description vPC-Backup-FI-A
  switchport mode trunk
  switchport trunk allowed vlan 221
  spanning-tree port type edge trunk
  mtu 9216
  vpc 21

interface port-channel22
  description vPC-Backup-FI-B
  switchport mode trunk
  switchport trunk allowed vlan 221
  spanning-tree port type edge trunk
  mtu 9216
  vpc 22

interface port-channel31
  description VPC to vPC-vHANA-FI-A
  switchport mode trunk
  switchport trunk allowed vlan 510,520,1371-1372,3110-3112
  spanning-tree port type edge trunk
  mtu 9216
  vpc 31

interface port-channel32
  description VPC to vPC-vHANA-FI-B
  switchport mode trunk
  switchport trunk allowed vlan 510,520,1371-1372,3110-3112
  spanning-tree port type edge trunk
  mtu 9216
  vpc 32

interface port-channel41
  description NetApp_CtrlA_OS
  switchport mode trunk
  switchport trunk allowed vlan 127,1371-1372,3110
  spanning-tree port type edge trunk
  vpc 41

interface port-channel42
  description NetApp_CtrlB_OS
  switchport mode trunk
  switchport trunk allowed vlan 127,1371-1372,3110
  spanning-tree port type edge trunk
vpc 42

interface port-channel44
  description NetApp_CtrlA_DATA
  switchport mode trunk
  switchport trunk allowed vlan 110,510
  spanning-tree port type edge trunk
  mtu 9216
  vpc 44

interface port-channel45
  description NetApp_CtrlB_DATA
  switchport mode trunk
  switchport trunk allowed vlan 110,510
  spanning-tree port type edge trunk
  mtu 9216
  vpc 45

interface port-channel112
  description Mgmt-Switch-A
  switchport mode trunk
  switchport trunk allowed vlan 112,127,3111
  spanning-tree port type network
  vpc 112

interface port-channel113
  description Mgmt-Switch-B
  switchport mode trunk
  switchport trunk allowed vlan 112,127,3111
  spanning-tree port type network
  vpc 113

interface Ethernet1/1
  description UPLINK-to-Customer-NetWork

interface Ethernet1/2
  description UCS-FI-A
  switchport mode trunk
  switchport trunk allowed vlan 110,112,127,220-225
  mtu 9216
  channel-group 11 mode active

interface Ethernet1/3
  description UPLINK-to-Customer-NetWork

interface Ethernet1/4
  description UCS-FI-A
  switchport mode trunk
  switchport trunk allowed vlan 110,112,127,220-225
  mtu 9216
  channel-group 11 mode active

interface Ethernet1/6
  description UCS-FI-B
  switchport mode trunk
  switchport trunk allowed vlan 110,112,127,220-225
mtu 9216
channel-group 12 mode active

interface Ethernet1/8
description UCS-FI-B
switchport mode trunk
switchport trunk allowed vlan 110,112,127,220-225
mtu 9216
channel-group 12 mode active

interface Ethernet1/9
switchport mode trunk
switchport trunk allowed vlan 110,112,127,220-225
switchport trunk allowed vlan add 510,520,1371-1372,3110-3112
channel-group 1 mode active

interface Ethernet1/10
description peer-link NX9K-A-1/10--NX9K-B-1/10
switchport mode trunk
switchport trunk allowed vlan 110,112,127,220-225
switchport trunk allowed vlan add 510,520,1371-1372,3110-3112
channel-group 1 mode active

interface Ethernet1/11
description peer-link NX9K-A-1/11--NX9K-B-1/11
switchport mode trunk
switchport trunk allowed vlan 110,112,127,220-225
switchport trunk allowed vlan add 510,520,1371-1372,3110-3112
channel-group 1 mode active

interface Ethernet1/12
description peer-link NX9K-A-1/12--NX9K-B-1/12
switchport mode trunk
switchport trunk allowed vlan 110,112,127,220-225
switchport trunk allowed vlan add 510,520,1371-1372,3110-3112
channel-group 1 mode active

interface Ethernet1/13

interface Ethernet1/14

interface Ethernet1/15
description NetApp_CtrlA_OS
switchport mode trunk
switchport trunk allowed vlan 127,1371-1372,3110
spanning-tree port type edge trunk
channel-group 41 mode active

interface Ethernet1/16
description NetApp_CtrlB_OS
switchport mode trunk
switchport trunk allowed vlan 127,1371-1372,3110
spanning-tree port type edge trunk
channel-group 42 mode active
interface Ethernet1/17
  description NetApp_CtrlA_DATA
  switchport mode trunk
  switchport trunk allowed vlan 110,510
  mtu 9216
  channel-group 51 mode active

interface Ethernet1/18
  description NetApp_CtrlA_DATA
  switchport mode trunk
  switchport trunk allowed vlan 110,510
  mtu 9216
  channel-group 51 mode active

interface Ethernet1/19
  description NetApp_CtrlB_DATA
  switchport mode trunk
  switchport trunk allowed vlan 110,510
  mtu 9216
  channel-group 52 mode active

interface Ethernet1/20
  description NetApp_CtrlB_DATA
  switchport mode trunk
  switchport trunk allowed vlan 110,510
  mtu 9216
  channel-group 52 mode active

interface Ethernet1/29
  description vPC-Backup-6248-A
  switchport mode trunk
  switchport trunk allowed vlan 221
  spanning-tree port type edge trunk
  mtu 9216
  channel-group 21 mode active

interface Ethernet1/30
  description vPC-Backup-6248-B
  switchport mode trunk
  switchport trunk allowed vlan 221
  spanning-tree port type edge trunk
  mtu 9216
  channel-group 22 mode active

interface Ethernet1/31
  description vPC-vHANA-6248-A
  switchport mode trunk
  switchport trunk allowed vlan 510,520,1371-1372,3110-3112
  spanning-tree port type edge trunk
  mtu 9216
  channel-group 31 mode active

interface Ethernet1/32
  description vPC-vHANA-6248-B
  switchport mode trunk
switchport trunk allowed vlan 510,520,1371-1372,3110-3112
spanning-tree port type edge trunk
no buffer-boost
mtu 9216
channel-group 32 mode active

interface Ethernet2/11
  description Link to Mgmt-Switch-A-P1
  switchport mode trunk
  switchport trunk allowed vlan 112,127,3111
  spanning-tree port type network
  channel-group 112 mode active

interface Ethernet2/12
  description Link to Mgmt-Switch-B-P1
  switchport mode trunk
  switchport trunk allowed vlan 112,127,3111
  spanning-tree port type network
  channel-group 113 mode active

interface mgmt0
  vrf member management
  ip address 177.78.78.1/24

---

Cisco Nexus 9000 B

hostname NX9k-B
vdc NX9k-B id 1
  allow feature-set fex
  allocate interface Ethernet1/1-48
  allocate interface Ethernet2/1-12
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

cfs eth distribute
feature udld
feature interface-vlan
feature lacp
feature vpc
feature lldp

username admin password 5 $1$/v261EcG$eLTpE50QHBgBftxGc05xG1 role network-admin
no password strength-check
ip domain-lookup
errdisable recovery interval 30
copp profile strict

snmp-server user admin network-admin auth md5
0x217f517b7927f8292f2297a2065a5636 priv
0x217f517b7927f8292f2297a2065a5636 localizedkey
rmon event 1 log trap public description FATAL(1) owner PMON@FATAL
rmon event 2 log trap public description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 log trap public description ERROR(3) owner PMON@ERROR
rmon event 4 log trap public description WARNING(4) owner PMON@WARNING
rmon event 5 log trap public description INFORMATION(5) owner PMON@INFO
ntp server 172.26.163.254 use-vrf management

vlan 1,110,111,127,201,220-225,510,520,1371-1372,3110-3112

vlan 110
  name HANA-Storage
vlan 112
  name HANA-Admin
vlan 127
  name HANA-Boot
vlan 201
  name Temp-Storage
vlan 220
  name HANA-Internal
vlan 221
  name HANA-Backup
vlan 222
  name HANA-Client
vlan 223
  name HANA-AppServer
vlan 224
  name HANA-DataSource
vlan 225
  name HANA-Replication
vlan 510
  name vHANA-Storage
vlan 520
  name vHANA-Access
vlan 1371
  name iSCSI-VLAN-A
vlan 1372
  name iSCSI-VLAN-B
vlan 3110
  name ESX-NFS
vlan 3111
  name ESX-MGMT
vlan 3112
  name ESX-vMotion

cdp timer 5
spanning-tree port type edge bpdu guard default
spanning-tree port type edge bpdu filter default
spanning-tree port type network default
vrf context management vrf context management
  ip route 0.0.0.0/0 172.25.186.1

vpc domain 50
  peer-switch
  role priority 20
peer-keepalive
destination 177.78.78.1 source 177.78.78.2
delay restore 150
peer-gateway
auto-recovery

interface port-channel1
  description VPC-Peer
  switchport mode trunk
  switchport trunk allowed vlan 110,112,127,220-225
  switchport trunk allowed vlan add 510,520,1371-1372,3110-3112
  spanning-tree port type network
  vpc peer-link

interface port-channel11
  description VPC to FI-A
  switchport mode trunk
  switchport trunk allowed vlan 110,112,127,220-225
  spanning-tree port type edge trunk
  mtu 9216
  vpc 11

interface port-channel12
  description VPC to FI-B
  switchport mode trunk
  switchport trunk allowed vlan 110,112,127,220-225
  spanning-tree port type edge trunk
  mtu 9216
  vpc 12

interface port-channel21
  description vPC-Backup-FI-A
  switchport mode trunk
  switchport trunk allowed vlan 221
  spanning-tree port type edge trunk
  mtu 9216
  vpc 21

interface port-channel22
  description vPC-Backup-FI-B
  switchport mode trunk
  switchport trunk allowed vlan 221
  spanning-tree port type edge trunk
  mtu 9216
  vpc 22

interface port-channel31
  description VPC to vPC-vHANA-FI-A
  switchport mode trunk
  switchport trunk allowed vlan 510,520,1371-1372,3110-3112
  spanning-tree port type edge trunk
  mtu 9216
  vpc 31

interface port-channel32
  description VPC to vPC-vHANA-FI-B
  switchport mode trunk
switchport trunk allowed vlan 510,520,1371-1372,3110-3112
spanning-tree port type edge trunk
mtu 9216
vpc 32

interface port-channel41
  description NetApp_CtrlA_OS
  switchport mode trunk
  switchport trunk allowed vlan 127,1371-1372,3110
  spanning-tree port type edge trunk
  vpc 41

interface port-channel42
  description NetApp_CtrlB_OS
  switchport mode trunk
  switchport trunk allowed vlan 127,1371-1372,3110
  spanning-tree port type edge trunk
  vpc 42

interface port-channel44
  description NetApp_CtrlA_DATA
  switchport mode trunk
  switchport trunk allowed vlan 110,510
  spanning-tree port type edge trunk
  mtu 9216
  vpc 44

interface port-channel45
  description NetApp_CtrlB_DATA
  switchport mode trunk
  switchport trunk allowed vlan 110,510
  spanning-tree port type edge trunk
  mtu 9216
  vpc 45

interface port-channel112
  description Mgmt-Switch-A
  switchport mode trunk
  switchport trunk allowed vlan 112,127,3111
  spanning-tree port type network
  vpc 112

interface port-channel113
  description Mgmt-Switch-B
  switchport mode trunk
  switchport trunk allowed vlan 112,127,3111
  spanning-tree port type network
  vpc 113

interface Ethernet1/1
  description UPLINK-to-Customer-NetWork

interface Ethernet1/2
  description UCS-FI-A
  switchport mode trunk
  switchport trunk allowed vlan 110,112,127,220-225
mtu 9216
channel-group 11 mode active

interface Ethernet1/3
    description UPLINK-to-Customer-NetWork

interface Ethernet1/4
    description UCS-FI-A
    switchport mode trunk
    switchport trunk allowed vlan 110,112,127,220-225
    mtu 9216
    channel-group 11 mode active

interface Ethernet1/6
    description UCS-FI-B
    switchport mode trunk
    switchport trunk allowed vlan 110,112,127,220-225
    mtu 9216
    channel-group 12 mode active

interface Ethernet1/8
    description UCS-FI-B
    switchport mode trunk
    switchport trunk allowed vlan 110,112,127,220-225
    mtu 9216
    channel-group 12 mode active

interface Ethernet1/9
    switchport mode trunk
    switchport trunk allowed vlan 110,112,127,220-225
    switchport trunk allowed vlan add 510,520,1371-1372,3110-3112
    channel-group 1 mode active

interface Ethernet1/10
    description peer-link NX9K-A-1/10--NX9K-B-1/10
    switchport mode trunk
    switchport trunk allowed vlan 110,112,127,220-225
    switchport trunk allowed vlan add 510,520,1371-1372,3110-3112
    channel-group 1 mode active

interface Ethernet1/11
    description peer-link NX9K-A-1/11--NX9K-B-1/11
    switchport mode trunk
    switchport trunk allowed vlan 110,112,127,220-225
    switchport trunk allowed vlan add 510,520,1371-1372,3110-3112
    channel-group 1 mode active

interface Ethernet1/12
    description peer-link NX9K-A-1/12--NX9K-B-1/12
    switchport mode trunk
    switchport trunk allowed vlan 110,112,127,220-225
    switchport trunk allowed vlan add 510,520,1371-1372,3110-3112
    channel-group 1 mode active

interface Ethernet1/13
interface Ethernet1/14

interface Ethernet1/15
    description NetApp_CtrlA_OS
    switchport mode trunk
    switchport trunk allowed vlan 127,1371-1372,3110
    spanning-tree port type edge trunk
    channel-group 41 mode active

interface Ethernet1/16
    description NetApp_CtrlB_OS
    switchport mode trunk
    switchport trunk allowed vlan 127,1371-1372,3110
    spanning-tree port type edge trunk
    channel-group 42 mode active

interface Ethernet1/17
    description NetApp_CtrlA_DATA
    switchport mode trunk
    switchport trunk allowed vlan 110,510
    mtu 9216
    channel-group 51 mode active

interface Ethernet1/18
    description NetApp_CtrlA_DATA
    switchport mode trunk
    switchport trunk allowed vlan 110,510
    mtu 9216
    channel-group 51 mode active

interface Ethernet1/19
    description NetApp_CtrlB_DATA
    switchport mode trunk
    switchport trunk allowed vlan 110,510
    mtu 9216
    channel-group 52 mode active

interface Ethernet1/20
    description NetApp_CtrlB_DATA
    switchport mode trunk
    switchport trunk allowed vlan 110,510
    mtu 9216
    channel-group 52 mode active

interface Ethernet1/29
    description vPC-Backup-6248-A
    switchport mode trunk
    switchport trunk allowed vlan 221
    spanning-tree port type edge trunk
    mtu 9216
    channel-group 21 mode active

interface Ethernet1/30
    description vPC-Backup-6248-B
switchport mode trunk
switchport trunk allowed vlan 221
spanning-tree port type edge trunk
mtu 9216
channel-group 22 mode active

interface Ethernet1/31
  description vPC-vHANA-6248-A
  switchport mode trunk
  switchport trunk allowed vlan 510,520,1371-1372,3110-3112
  spanning-tree port type edge trunk
  mtu 9216
  channel-group 31 mode active

interface Ethernet1/32
  description vPC-vHANA-6248-B
  switchport mode trunk
  switchport trunk allowed vlan 510,520,1371-1372,3110-3112
  spanning-tree port type edge trunk
  no buffer-boost
  mtu 9216
  channel-group 32 mode active

interface Ethernet2/11
  description Link to Mgmt-Switch-A-P1
  switchport mode trunk
  switchport trunk allowed vlan 112,127,3111
  spanning-tree port type network
  channel-group 112 mode active

interface Ethernet2/12
  description Link to Mgmt-Switch-B-P1
  switchport mode trunk
  switchport trunk allowed vlan 112,127,3111
  spanning-tree port type network
  channel-group 113 mode active

interface mgmt0
  vrf member management
  ip address 177.78.78.2/24