

# FlexPod Data Center with VMware vSphere 5.1, and Citrix CloudPlatform 4.2.1

Deployment Guide for FlexPod with VMware vSphere 5.X, and Citrix CloudPlatform 4.2.1 Powered by Apache

Last Updated: February 5, 2014



Building Architectures to Solve Business Problems

# cisco.







# About the Authors



Deepak Natarajan



Ramesh Kamath



Frank Zhang

#### Deepak Natarajan, Technical Marketing Engineer, SAVBU, Cisco Systems

Deepak Natarajan is a Technical Marketing Engineer in Cisco Systems Data Center Group (DCG) and specialist on Data Center Solutions. He has over 11 years of extensive experience on Architecture Design, Capacity Planning and Application Performance to build Data Center Cloud. He has worked as a TME and field enablement, customer and field facing, influencing and building Cloud solutions across Compute, Storage, Network, Cloud Management product portfolio in various organizations. He holds a Bachelor degree in Computer Science and is also an Cisco Certified Network Professional (CCNA). Deepak also has strong background in Cisco UCS Systems, Data Center Network, NetApp Storage and Virtualization domain.

# Ramesh Kamath, Technical Marketing Engineer, Data Center Solutions Group, NetApp Systems

Ramesh Kamath is a Technical Marketing Engineer for Citrix Solutions at NetApp. He is focused on developing, validating and evangelizing Citrix XenServer, ShareFile and XenDesktop based solutions on NetApp Infrastructure. With over 6 years in the Data Storage Industry, Ramesh holds a Bachelor's Degree from R V College Of Engineering, Bangalore.

#### Frank Zhang, CloudPlatform Developer, Cloud Platforms Group, Citrix Systems

Frank Zhang is a core CloudPlatform developer in Citrix. He is responsible for developing Baremetal-as-a-Service as well as Cisco UCS integration in CloudPlatform.







# **Acknowledgment**

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

- Mike Brennan
- Siva Sivakumar
- Vadiraja Bhatt
- Roger Barlow
- Manan Shah
- Troy Mangum
- Abhinav Joshi
- Rachel Zhu
- David La Motta
- Kim White
- Animesh Chaturvedi
- Susan Wu
- Parth Jagirdar
- Karthick Radhakrishnan
- Sridhara C

# 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:

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

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLEC-TIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUP-PLIERS 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.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at <a href="http://www.cisco.com/go/trademarks">http://www.cisco.com/go/trademarks</a>. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2013 Cisco Systems, Inc. All rights reserved.







# FlexPod Data Center with VMware vSphere 5.1, and Citrix CloudPlatform 4.2.1

# **Executive Summary**

This Cisco Validated Design Guide provides design considerations and guidelines for deploying Citrix CloudPlatform 4.2.1 on Cisco Unified Computing System (UCS) and shared NetApp Storage. The document provides information on how to design Compute, Storage, and Network infrastructure layout on Cisco UCS to build Citrix CloudPlatform 4.2.1 over unified protocol (block or file). The deployment scenarios discussed in this document follows the Cisco UCS best practices and recommendations to help ensure that the systems are highly available, scalable, and can be efficiently consolidated and centrally managed in the cloud environment.

# Introduction

Companies everywhere are looking for effective strategies to harness the benefits of cloud computing without disrupting current business models. As the industry ventures into the cloud computing era, service providers and entrepreneurs are seeking more efficient and differentiated cloud solutions to reduce the total cost of ownership of IT, acquire the capability to add capacity on demand, charge-back or show-back for services rendered, and attract and retain customers, and increase market share. They need open and flexible cloud solutions that free them from vendor lock-in so they can take full advantage of existing investments and choose the best possible components for their clouds. They need access to source code and open APIs to innovate and build value-added services, all while still having enterprise-class support and services. Their customers want to choose the architecture and hypervisor that's right for them. At the same time, enterprises are looking to the cloud to enable more agile, elastic, on-demand IT services. In both cases, they need the right solutions to build, scale, and manage cloud services.

This joint solution is comprised of several fundamental building blocks, such as, VMware ESXi 5.1 hypervisor, Citrix CloudPlatform 4.2.1, Cisco Unified Computing System, Nexus physical and virtual switches, UCS B-Series Servers, and NetApp FAS 3270 Storage configured with Cluster Mode Data ONTAP 8.1.2. The combination of these building blocks provide a seamless cloud infrastructure management system.



The reference architecture suggests best practices for configuring and deploying the VMware vSphere ESXi 5.1, Citrix CloudPlatform<sup>TM</sup> Version 4.2.1 powered by Apache CloudStack on the Cisco Unified Computing System<sup>TM</sup> (Cisco UCS®) B200 M3 Blade Servers connected to the NetApp FAS 3270 storage array with Cisco Nexus® 5000 Series Switches. Second and third generation Cisco® UCS hardware and software are used in this solution. Citrix CloudPlatform 4.2.1 is a broad solution that includes a commercially certified and packaged Apache CloudStack product. Cisco UCS is an highly scalable, automated, and programmable infrastructure for cloud deployment.

# Audience

This document is designed to assist solution architects, sales engineers, field engineers, and consultants with evaluation, planning, design, and deployment of Citrix CloudPlatform Version 4.2.1 on Cisco UCS. The reader should have an architectural understanding of Cisco UCS, Cisco Nexus 5500 Series Switches, Citrix CloudPlatform 4.2.1, NetApp FAS 3270 Storage and NetApp Data ONTAP 8.1.2 Cluster Mode, and related software.

# **Solution Components**

The following components are required to deploy the Citrix CloudPlatform 4.2.1 on the Cisco Unified System design:

- Hardware Components
  - Cisco Unified Computing System
  - Cisco Nexus 5500 Series Switches
  - NetApp FAS Storage System
- Software Components
  - VMware vSphere ESXi 5.1 Hypervisor
  - Citrix CloudPlatform 4.2.1
  - Cisco UCS Manager 2.1(2)

# **Cisco Unified Computing System**

## **Overview**

The Cisco UCS is a next-generation approach to blade and rack server computing. It is an innovative data center platform that unites compute, network, storage access, and virtualization into a cohesive system designed to reduce total cost of ownership (TCO) and increase business agility. The system integrates a low-latency; lossless 10 Gigabit Ethernet unified network fabric with enterprise-class, x86-architecture servers. The system is an integrated, scalable, multi-chassis platform in which all resources participate in a unified management domain. Managed as a single system, whether it has one server or 160 servers with thousands of virtual machines, the Cisco UCS decouples scale from complexity. It accelerates the delivery of new services simply, reliably, and securely through end-to-end provisioning and migration support for both virtualized and non virtualized systems.

Many of the concepts that make virtualization the ideal platform for delivering cloud apply to Cisco UCS, thus making Cisco UCS also ideal for cloud deployments. Some of the common concepts are:

- Single point of infrastructure management, which enables complete control
- · Policy-based infrastructure management
- · Using templates to capture desired state and subsequently expedite deployment
- Programmatic control of the entire infrastructure

There are three key areas, inherent in the design, where Cisco UCS excels in comparison to traditional architectures, helping to simplify the design and maintenance of cloud solutions.

The Cisco UCS offers the following features that enable the above concepts in the design solution:

#### **Unified Fabric**

Unified fabric can dramatically reduce the number of network adapters, blade-server switches, cables, and management touch points by passing all network traffic to parent Fabric Interconnects, where it can be prioritized, processed, and managed centrally. This approach improves performance, agility, and efficiency and dramatically reduces the number of devices that need to be powered, cooled, secured, and managed.

#### **Embedded Multirole Management**

The Cisco UCS Manager is a centralized management application that is embedded on the fabric switch. The Cisco UCS controls all the Cisco UCS elements within a single redundant management domain. These elements include all aspects of system configuration and operation, eliminating the need to use multiple, separate element managers for each system component. Massive reductions in the number of management modules and consoles, and in the proliferation of resident agents on all the hardware (which must be separately managed and updated) are important deliverables of Cisco UCS. Cisco UCS Manager, using role-based access and visibility, helps enable cross-functional communication efficiency and promotes collaboration between data center roles for increased productivity.

#### **Cisco Extended Memory Technology**

Significantly enhancing the available memory capacity of some Cisco UCS servers, Cisco Extended Memory Technology helps increase performance for demanding virtualization and large-data-set workloads. Data centers can now deploy very high virtual machine densities on individual servers as well as provide resident memory capacity for databases that need only two processors but can dramatically benefit from more memory. The high-memory dual in-line memory module (DIMM) slot count also lets the users to more cost-effectively scale this capacity using smaller, less costly DIMMs.

#### **Cisco Data Center VM-FEX Virtualization Support and Virtualization Adapter**

With Cisco Data Center VM-FEX, virtual machines have virtual links that allow them to be managed in the same way as physical links. Virtual links can be centrally configured and managed without the complexity of traditional systems, which interpose multiple switching layers in virtualized environments. I/O configurations and network profiles move along with virtual machines, helping increase security and efficiency while reducing complexity. Cisco Data Center VM-FEX helps improve performance and reduce network interface card (NIC) infrastructure.

#### **Dynamic Provisioning with Service Profiles**

The Cisco UCS Manager delivers service profiles, which contain abstracted server-state information, creating an environment in which everything unique about a server is stored in the fabric, and the physical server is simply another resource to be assigned. Cisco UCS Manager implements role-based and policy-based management focused on service profiles and templates. These mechanisms fully provision one or many servers and their network connectivity in minutes, rather than hours or days.

### **Cisco UCS Components**

This section describes the specific Cisco UCS products used in the Citrix CloudPlatform 4.2.1 on UCS design.

The Cisco Unified Computing System<sup>™</sup> with unified fabric dramatically reduces the number of network adapters, blade-server switches, and cables needed as it passes network traffic to parent fabric interconnect. These interconnect process and centrally manage the traffic to improve performance. They also reduce the number of devices that need to be powered, cooled, secured, and managed. The multiple-role management embedded in the Fabric Interconnects to manage configuration and operation, eliminates the need for separate element managers. In addition, Cisco VN-Link Virtualization support gives network links connected to virtual machines the same status as physical links. I/O configurations and network profiles move with the virtual machines, increasing security and efficiency while reducing complexity. This virtual network interface card (vNIC) feature improves performance and reduces NIC infrastructure.



#### Figure 1 Cisco UCS Components

#### **Cisco UCS Fabric Interconnects**

Cisco UCS Fabric Interconnects creates a unified network fabric throughout Cisco UCS. They provide uniform access to both networks and storage, eliminating the barriers to deployment of a fully virtualized environment based on a flexible, programmable pool of resources. Cisco Fabric Interconnects comprise a family of line-rate, low-latency, lossless 10 Gigabit Ethernet, IEEE Data Center Bridging (DCB), and FCoE interconnect switches. Based on the same switching technology as the Cisco Nexus<sup>®</sup> 5000 Series Switches, Cisco UCS 6200 Series Fabric Interconnects provide additional features and management capabilities that make them the central nervous system of Cisco UCS. The Cisco UCS Manager software runs inside the Cisco UCS Fabric Interconnects. The Cisco UCS 6100 Series Fabric Interconnects expand the Cisco UCS networking portfolio and offer higher capacity, higher port density, and lower power consumption. These interconnects provide the management and communication backbone for the Cisco UCS B-Series Blade Servers and Cisco UCS blade server chassis. All chassis and all blades that are attached to interconnect are part of a single, highly available management domain. By supporting unified fabric, the Cisco UCS 6100 Series provides the flexibility to support LAN and SAN connectivity for all blades within its domain at configuration time. Typically deployed in redundant pairs, Cisco UCS Fabric Interconnects provides uniform access to both networks and storage, facilitating a fully virtualized environment.

The Cisco UCS Fabric Interconnects portfolio currently consists of the Cisco 6100 and 6200 Series Fabric Interconnects. In this design we have used the Cisco 6248UP FI:

Cisco UCS 6248UP 48-Port Fabric Interconnect

The Cisco UCS 6248UP 48-Port Fabric Interconnects is a one-rack-unit (1RU) 10 Gigabit Ethernet, IEEE DCB, and FCoE interconnect providing more than 1-terabit-per-second (Tbps) throughput with low latency. It has 32 fixed ports of Fibre Channel, 10 Gigabit Ethernet, IEEE DCB, and FCoE Enhanced Small Form-Factor Pluggable (SFP+) ports.

One expansion module slot can provide up to 16 additional Fibre Channel, 10 Gigabit Ethernet, IEEE DCB, and FCoE SFP+ ports.

#### **Cisco UCS Fabric Extenders**

The Cisco UCS 2100 and 2200 Series Fabric Extenders multiplex, and forward all traffic from blade servers in a chassis to a parent Cisco UCS Fabric Interconnects over 10-Gbps unified fabric links. All traffic, even traffic between blades on the same chassis or virtual machines on the same blade, is forwarded to the parent interconnect, where network profiles are managed efficiently and effectively by the fabric interconnect. At the core of the Cisco UCS Fabric Extenders are application-specific integrated circuit (ASIC) processors developed by Cisco that multiplex all traffic.

Up to two fabric extenders can be placed in a blade chassis. In this design the Cisco UCS 2208XP Fabric Extender

• The Cisco UCS 2208XP Fabric Extender

It has eight 10 Gigabit Ethernet, FCoE-capable, 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.

#### **Cisco UCS Virtual Interface Card**

The Cisco UCS VIC 1240 and 1280 enable a policy-based, stateless, agile server infrastructure that can present up to 256 PCI Express (PCIe) standards-compliant interfaces to the host that can be dynamically configured as either NICs or HBAs. In addition, the Cisco UCS VIC 1280 supports Cisco Data Center VM-FEX technology, which extends the Cisco UCS Fabric Interconnects ports to virtual machines, simplifying server virtualization deployment.

• Cisco UCS VIC 1240

A Cisco innovation, the Cisco UCS VIC 1240 is a four-port 10 Gigabit Ethernet, FCoE-capable modular LAN on motherboard (mLOM) designed exclusively for the M3 generation of Cisco UCS B-Series Blade Servers. When used in combination with an optional port expander, the Cisco UCS VIC 1240 capabilities can be expanded to eight ports of 10 Gigabit Ethernet.

Cisco UCS VIC 1280

A Cisco innovation, the Cisco UCS VIC 1280 is an eight-port 10 Gigabit Ethernet, FCoE-capable mezzanine card designed exclusively for Cisco UCS B-Series Blade Servers.

#### **Cisco UCS 5100 Series Blade Server Chassis**

The Cisco UCS 5108 Blade Server Chassis is a 6RU blade chassis that accepts up to eight half-width Cisco UCS B-Series Blade Servers or up to four full-width Cisco UCS B-Series Blade Servers, or a combination of the two. The Cisco UCS 5108 can accept four redundant power supplies with automatic load sharing and failover and two Cisco UCS 2100 or 2200 Series Fabric Extenders. The chassis is managed by Cisco UCS chassis management controllers, which are mounted in the Cisco UCS fabric extenders and work in conjunction with Cisco UCS Manager to control the chassis and its components.

A single Cisco UCS managed domain can theoretically scale to up to 40 individual chassis and 320 blade servers. At this time, Cisco UCS supports up to 20 individual chassis and 160 blade servers.

Basing the I/O infrastructure on a 10-Gbps unified network fabric allows Cisco UCS to have a streamlined chassis with a simple yet comprehensive set of I/O options. The result is a chassis that has only five basic components:

- The physical chassis with passive midplane and active environmental monitoring circuitry
- Four power supply bays with power entry in the rear and hot-swappable power supply units accessible from the front panel
- Eight hot-swappable fan trays, each with two fans
- Two Cisco UCS Fabric Extenders slots accessible from the back panel
- Eight Cisco UCS Blade Server slots accessible from the front panel

#### Cisco UCS B200 M3 Blade Servers

The Cisco UCS B200 M3 Blade Server delivers performance, versatility, and density without compromise. It addresses the broadest set of workloads, from IT and web infrastructure to distributed databases. Building on the success of the Cisco UCS B200 M2 Blade Server, the enterprise-class Cisco UCS B200 M3 Blade Server further extends the capabilities of the Cisco UCS portfolio in a half-width blade form factor. The Cisco UCS B200 M3 harnesses the power of the latest Intel Xeon processor E5-2600 product family, with up to 384 GB of RAM (using 16-GB DIMMs), two disk drives, and up to dual 4x 10 Gigabit Ethernet throughput. In addition, Cisco UCS has the architectural advantage of not having to power and cool excess switches in each blade chassis. With a larger power budget per blade server, Cisco uCS B200 M3, with its leading memory slot and drive capacity.

# Cisco Nexus 5500 Series Switch

The Cisco Nexus 5000 Series Switch is designed for data center environments with cut-through technology that enables consistent, low-latency Ethernet solutions with front-to-back or back-to-front cooling and data ports in the rear, bringing switching into close proximity with servers and making cable runs short and simple. The switch series is highly serviceable, with redundant, hot-pluggable power supplies and fan modules. It uses data-center-class Cisco NX-OS Software for high reliability and ease of management.

The switch extends the industry-leading versatility of the Cisco Nexus 5000 Series purpose-built 10 Gigabit Ethernet data-center-class switches and provides innovative advances toward higher density, lower latency, and multilayer services. The Cisco Nexus 5500 Series switch is well suited for enterprise-class data center server access layer deployments across a diverse set of physical, virtual, storage-access, and high-performance computing (HPC) data center environments.

• Cisco Nexus 5548UP

The Cisco Nexus 5548UP is a 1RU 10 Gigabit Ethernet (10 GE), Fibre Channel (FC), and Fibre Channel over Ethernet (FCoE) switch offering up to 960 Gbps of throughput and up to 48 ports. The switch has 32 unified ports and one expansion slot supporting modules with 10 Gigabit Ethernet and FCoE ports or connectivity to Fibre Channel SANs with 8/4/2/1 Gbps Fibre Channel switch ports, or both.

# NetApp Storage

The NetApp FAS3270 can handle today's diverse, virtualized workloads and easily respond to future expansion. The NetApp FAS3270 series meets the storage needs of business applications in both virtual and traditional environments in a cost-effective manner. It is ideal for demanding business applications in virtualized environments and dramatically reduces the consumption of raw storage, power, cooling, and space with NetApp FAS3270 highly efficient storage utilization.

NetApp FAS3270 supports the FC, FCoE, IP SAN (iSCSI), NFS, CIFS, HTTP, FTP storage networking. It provides high availability features such as Alternate Control Path (ACP), Ethernet-based service processor and Data ONTAP management interface; redundant hot-swappable controllers, cooling fans, power supplies, and optics. Additionally it supports the highly available controller configurations, such as, active-active controller with controller failover and multipath HA storage, active-active controller with stretch (non switch) and fabric-attached MetroCluster V-Series Storage Acceleration Appliance SA320.

# VMware vSphere ESXi 5.1

Virtualization is a proven technology that enables multiple virtual machines to run on a single physical server. Each virtual machine is completely isolated from other machines and is decoupled from the underlying host by a thin layer of software known as a hypervisor. This allows each virtual machine to run different operating systems and applications. Because the machines have been decoupled from the underlying host, the guest can also be moved from one physical server host to another in production or development environment, this is known as live migration. These attributes have transformed the organization's approach to virtual computing. The range of products offered by VMware meet the business needs of an ever evolving IT Infrastructure.

Built on the powerful vSphere hypervisor, ESXi 5.1 is a complete, managed server virtualization platform. ESXi technology is extensively acknowledged as the fastest and most secure virtualization software in the industry. ESXi efficiently manages virtual servers and provides an economical server consolidation ensuring business continuity.

# **Citrix CloudPlatform 4.2.1**

Citrix CloudPlatform, powered by Apache Cloudstack, is the only future-proofed, application-centric cloud solution proven to reliably orchestrate both existing scale-up enterprise workloads and scale-out cloud-native application workloads within a single unified cloud management platform. Citrix CloudPlatform combines the best private cloud foundation for enterprise workloads like CRM and ERP with true Amazon-style scale, elasticity and operational efficiency for cloud-native application workloads, Big Data and HPC.

# Enabling Scale-up and Scale-out Workloads with CloudPlatform 4.2.1

Citrix CloudPlatform enables organizations to create workload specific availability zones or regions which can support high performance, massively parallel workloads on distributed, low cost infrastructure. Enterprises can run complex enterprise workloads with best in class virtualization and networking to deliver true private cloud isolation, ensure SLA, compliance, security and availability for running mission critical workloads. For organizations that are delivering cloud-native application workloads, Citrix CloudPlatform provides customers with availability, storage and network with proven scalability for public and private clouds with over 40,000 hosts per region.

# **Dedicated Private Cloud Isolation**

Cloud infrastructure layers—zones, pods, clusters and hosts—and virtual machine resources—CPU, memory, storage and network—can be granularly grouped into different isolated logical partitions for true multi-tenant private cloud deployments. Dedicated resources can be applied to any of the infrastructure layers to support virtual private cloud use cases to meet requirements for compliance, security and performance.

## **Logical Isolation**

With CloudPlatform, enterprises can organize their private cloud into multiple discrete logical abstraction layers including availability zones or regions, each comprising resources in one or more physical data centers. CloudPlatform uses a logical user isolation hierarchy that includes Domain, Sub-domain, Account and Users. Usage quotas can be applied to any layer in the hierarchy. This logical isolation hierarchy can be used to model the organizational structure in typical enterprises in a domain to represent a business unit; users can also be grouped into Accounts which could represent a team. A sub-domain could represent a division in a larger business unit. The same isolation hierarchy can be applied to a service provider context in which an Account could represent an individual customer. CloudPlatform ensures that all memory, CPU, network, and storage resources are both available and isolated from one user account to another.

## Regions

Cloud Administrators can define availability regions consisting of multiple zones and/or data centers. The benefits to implementing regions are increased scalability and availability, geographic availability, lower latency and ensuring corporate compliance. Regions enable application workloads to be launched and deployed across multiple availability zones from the same template. Application availability would not impacted if a given zone were to fail because the VMs supporting the service will be running in multiple zones.

## **Hypervisor Agnostic**

CloudPlatform supports the leading commercially supported hypervisors including Citrix® XenServerTM, VMware® vSphere® Oracle® VM (OVM), and KVM. Bare metal infrastructure without a hypervisor is also supported. Customers have complete freedom to choose the right hypervisor or hypervisors for their workload instead of being locked into technology from one single vendor.

Traditional application availability zones typically begin with bare metal or a supported hypervisor, such as VMware® vSphere or Citrix XenServerTM which supports live migration of VMs. CloudPlatform has a two-tier storage hierarchy. Root and data volumes are stored on a primary storage tier that typically resides on host local storage, FC, iSCSI or NFS for performance. VM templates and volume snapshots are stored on a secondary storage tier, typically NFS or object storage.

### Virtual Machine Operations and Management

CloudPlatform provides efficient lifecycle management of virtual machines, including creation and maintenance under a single platform. Root and data volumes reside on the primary storage tier and are created at VM creation. When a VM is destroyed, the root volume is also destroyed. In the case of data volumes that are attached to the VM, they do not get destroyed when the VM is destroyed which means

I

that administrators can take scheduled or adhoc snapshots of the volume to preserve configuration states for backup or data recovery. OS and ISO templates can be imported, created, and stored across zones or regions on the secondary storage tier for optimized storage efficiency.

## Advanced VMware Integration

Virtualization has been broadly adopted by enterprises and service providers alike over the past decade. With the VMware® vCenter® integration, CloudPlatform can help organizations move their enterprise workloads seamlessly from the data center to the cloud and still leverage their existing VMware investments, configurations and expertise. vCenter® features such as virtual hardware hot add, vMotion®, VMware HA & DRS, Storage vMotion, and CPU and RAM overcommit are all enabled in CloudPlatform. CloudPlatform leverages VMware's dvSwitch and PVLAN features to provide further network segmentation and VM isolation on the same network. Additional storage integrations allow for VM level snapshots as well as volume level snapshots.

## **Guest Isolation using Security Groups**

Guest Instances require isolation from other instances running within the same Zone. When guest VMs need to communicate with each other over a network, CloudPlatform provides two isolation methods, Security Groups and VLANs. Although Security Groups can be implemented in both the Basic and Advanced Networking models, VLANs are only available in advanced networking. Advanced Networking allows the cloud administrator to provide custom IP ranges for different accounts. In a Basic Networking setup, the guest instances use the same IP range as the underlying CloudPlatform and Hypervisor architecture.

When using Security Groups, each account has a default Security Group that is automatically created. When new instances are created, they are assigned to one or more Security Groups. Users can create additional Security Groups at any time. Communication between guest instances can happen only if they are assigned to the same security group. The use of Ingress and Egress rules on the Security Group control the flow of traffic, both in and out of the group.

# **Virtual Private Clouds**

Virtual Private Cloud (VPC) is a private, isolated grouping of resources in CloudPlatform. Enterprise applications in traditional data centers have network tiers connected to them for connection to databases, load balancing, and firewalls. A VPC can have its own virtual network topology that resembles a traditional physical network.

Using the VPC feature, cloud administrators can launch VMs in a virtual network containing private addresses to recreate the network architecture of their traditional enterprise applications, including IP ranges and VLANs. The ability to group similar kinds of instances based on IP address range or network tier definition makes the data center transformation to the cloud computing easier. Through the recreation of traditional enterprise network topologies including granular network segmentation for traditional applications, the transition to cloud computing can be simplified.



In traditional multi-tier application, VLANs have been traditionally used to produce network segregation and correct traffic flow. In the above multi-tier example, , the application is composed of a web front end tier, an application tier and a database tier. Each tier is isolated by an individual VLAN. For large scale deployments, administrators using this n-tier application architecture in Citrix CloudPlatform to create granular networks, routing, firewall and load balancing policies, or affinity/anti-affinity rules for individual tiers.

## Advanced Cloud Networking

Cloud operators can create advanced cloud networking configurations and Network-as-a-Service offerings including Portable IP capabilities, global server load balancing (GSLB), and AWS-like Health Checks to ensure application availability. In addition, CloudPlatform has an in-built virtual router that provides granular control of network services like DHCP, Network Address Translation (NAT), load balancing, firewall, and port forwarding.

CloudPlatform integrates with enterprise class Application Delivery Controllers (ADCs) to provide server load balancing. Advanced features such as compression, connection multiplexing, caching, and SSL offload found in ADCs are becoming increasingly helpful off load overburdened networks and servers and increasing application availability. CloudPlatform supports a broad ecosystem of ADCs and networking devices including Citrix Netscaler ®, F5 load balancers, Cisco hardware and software (UCS, Nexus 1000v, ASA1000v), Juniper firewalls and VMware Distributed Virtual Switch. Advanced networking requirements for architecture, scale, SLAs, load balancing can be met using best of breed networking solution for the most demanding cloud-native application workloads and availability requirements.

In particular, the Citrix NetScaler Global Server Load Balancing (GSLB) feature is enabled through CloudPlatform which enables distribution of traffic across multiple sites and helps to manage disaster recovery. GSLB works by controlling how the system routes incoming client requests by directing DNS requests to the best-performing GSLB site in a distributed Internet environment. Pre-defined NetScaler policies and configurations can be orchestrated by CloudPlatform to send traffic. For example, a policy could direct traffic to the closest availability zone, a region with the lowest latency or the least amount of load, or to a secondary data center in case of an outrage.

Intelligent load balancers such as Citrix Netscaler can be configured to perform AWS-style Health Checks on backend services through CloudPlatform. NetScaler will perform periodic checks on backend services based on a set of service level parameters to be monitored. When a VM fails the Health Check, Citrix Netscaler will automatically remove the VM from the load balancer pool and route the incoming requests only onto healthy VMs. Once the VM successfully passes the health checks again, the load balancer will add the VMs back into the resource pool.

CloudPlatform with Citrix NetScaler offers AutoScale technology that automatically expands and contracts the cloud according to business demands. Citrix Netscaler has the ability to monitor CPU usage, server health or application responsiveness. Working in unison with CloudPlatform, changes to application load can prompt Citrix Netscaler to scale up or scale down the corresponding backend services or guest VMs.

Citrix NetScaler comes with a choice of configurations, as a physical appliance or as a Virtual Machine that runs on Citrix XenServer. CloudPlatform treats Citrix NetScaler just like any other infrastructure resource, for which it can be added into the resource pool.

## **Object Storage**

Cloud-native application workloads that make use of object storage will have transparent access to storage objects across geographic and logically defined locations. The ability to access object storage in a region or across multiple zones increases workload availability and operations efficiency. Object Storage can be used to store persistent data given a zone failure. Also the same object storage can provide secondary storage for Infrastructure-as-a Service and Storage-as-a-Service.

## **Cisco and Citrix - Better Together for production clouds**

With over 200+ clouds in production, Citrix CloudPlatform is the trusted cloud management platform to orchestrate the world's most demanding workloads. Leading telecommunications companies and higher education institutions like Bell Canada, BT, COLT, and University of Sao Paulo to web-centric companies like Edmunds.com have chosen Cisco UCS and Citrix CloudPlatform to run their clouds in production and at scale.

# **Cisco UCS Manager**

Cisco UCS Manager is an embedded, unified manager that provides a single point of management for Cisco UCS. Cisco UCS Manager can be accessed through an intuitive GUI, a command-line interface (CLI), or the comprehensive open XML API. It manages the physical assets of the server and storage and LAN connectivity, and it is designed to simplify the management of virtual network connections through integration with several major hypervisor vendors. It provides IT departments with the flexibility to allow people to manage the system as a whole, or to assign specific management functions to individuals based on their roles as managers of server, storage, or network hardware assets. It simplifies operations by automatically discovering all the components available on the system and enabling a stateless model for resource use.

The elements managed by Cisco UCS Manager include:

 CloudPlatform allows to provision bare metal host as a service, in order to enable easy expansion of the cloud by leveraging the programmability of the UCS converged infrastructure. CloudPlatform provides UCS Plugin which can automatically understand the UCS environment, server profiles, etc. so CloudPlatform administrators can deploy a bare metal OS on a Cisco UCS System. An overview of the steps involved in using UCS with CloudPlatform:

- **2.** Set up your Cisco UCS Blade Servers, profiles, and Cisco UCS Manager according to Cisco documentation
- 3. Registering the Cisco UCS Manager with CloudPlatform
- 4. Associate a Service Profile with a UCS blade
- 5. Provision the blade as a bare metal host as described

# **Reference Architecture**

This section presents physical and logical high-level design considerations for Cisco UCS networking and computing with VMware ESXi 5.1 virtualization on NetApp storage with Citrix CloudPlatform to build private cloud deployments.

Using Cisco's Unified Fabric for the networking component of the cloud infrastructure helps to ensure that once cables are connected, they need not be rerouted if there are changes in the cloud workload requirements. The Cisco UCS helps to ensure that the servers can be delivered quickly and in an automated fashion.

# **Citrix CloudPlatform 4.2.1 on FlexPod Overview**

Cisco Flexpod and Citrix CloudPlatform powered by Apache CloudStack combines converged converged compute, networking, and storage solution developed by Cisco and NetApp with a proven, application centric, turn-key orchestration solution from Citrix offers true secure and scalable IT infrastructure with on-demand access to virtual server and storage resources.

Well suited for Enterprise private clouds, CloudPlatform provides a system that allows for delivering capacity on demand, allowing users to provision their own resources based on policy, and charge-back or show back to internal customers, departments or business units.

This document describes design methodology followed to deployment of IaaS (Infrastructure as a Service) based on the components below to build scalable, dynamic and multi-tenant cloud solution deployment models:

- Cisco Unified Computing System
- Cisco Nexus physical and virtual Switches
- NetApp FAS Storage
- VMware vSphere ESXi Hypervisor
- Citrix CloudPlatform 4.2.1

Figure 3 IaaS Cloud Service Model						
laaS Cloud Service						
Discovery Citrix Cloud	<b>Provision</b> IPlatfrom	Service Model	Orchestration			
VMware ES	(i Server		Hypervisor			
Cisco Nexus 5	i000 Switches		Network			
Cisco Unified S	erver System		Compute			
NetApp St	corage		Storage			

# **Cisco Unified Compute System**

ſ

Cisco UCS is designed from the start to be programmable and self-integrating. A server's entire hardware stack, ranging from server firmware and settings to network profiles, is configured through model-based management. With Cisco virtual interface cards (VICs), even the number and type of I/O interfaces is programmed dynamically, making all the servers ready to power up and take any workload at any time.

With model-based management, administrators manipulate a model of a desired system configuration and associate a model's service profile with hardware resources, and the system configures itself to match the model. This automation accelerates provisioning and workload migration with accurate and rapid scalability. The result is increased IT staff productivity, improved compliance, and reduced risk of failures due to inconsistent configurations.

## **Cisco Nexus Unified Network System**

Cisco Unified Fabric delivers reliable, scalable, agile, and cost-effective network services to servers, storage, and applications while improving the user experience. It facilitates better support of virtualization and cloud services with improved staff utilization, more efficient resource utilization (more load on servers and storage), low-latency options, lower TCO, and better resiliency and uptime. It offers high-performance, low-latency, and highly available networks. These networks serve diverse data center needs, including the lossless requirements for block-level storage traffic. A Cisco Unified Fabric network carries multiprotocol traffic to connect storage (Fibre Channel, FCOE, Small Computer System Interface over IP [iSCSI], and network-attached storage [NAS]) as well as general data traffic. Fibre Channel traffic can be on its own fabric or part of a converged fabric with FCoE. Offering the best of both LAN and SAN environments, Cisco Unified Fabric enables storage network users to take advantage of the economy of scale, robust vendor community, and aggressive performance roadmap of Ethernet while providing the high-performance, lossless characteristics of a Fibre Channel network.

## **NetApp Unified Storage System**

NetApp solutions begin with Clustered Data ONTAP 8.2.1, the fundamental software platform that runs on all NetApp storage systems. Data ONTAP 8.2.1 is a highly optimized, scalable operating system that supports mixed NAS and SAN environments and a range of protocols, including Fibre Channel, iSCSI, FCoE, NFS, and CIFS CIFS.

Clustered Data ONTAP offers compelling value to both the enterprise private cloud and public cloud service providers. The software's unified architecture services a range of workloads–from the most demanding to the most unique across virtualized environments, scale-out NAS, and enterprise applications. During the past year companies across all industries have adopted clustered Data ONTAP with a 4x increase in clustered nodes resulting in 100% quarter over quarter growth of deployments. Cloud providers, whose business reputation depends on continuously running operations, are bringing centralized management to the data center with FlexPod® from NetApp and Cisco with clustered Data ONTAP. The new software gives organizations and cloud service providers the capability to rapidly and cost effectively deliver new services and capacity with maximum application uptimeClustered Data ONTAP 8.2 cuts through the performance, availability, and efficiency limits of traditional hardware silos, empowering IT to nondisruptively align the storage infrastructure with changing business and application demands.

Industry leading capabilities in a clustered data ONTAP are:

- Nondisruptive operations with greater than five-9s reliability (99.999%), providing continuous data access during scheduled downtime and dynamic load balancing without disruptive data migrations
- Seamless scalability with up to 69PB of storage and 24 controller nodes, 49,000 LUNs, 12,000 NAS volumes supporting over 100,000 clients and single container up to 20 PB
- Proven storage and operational efficiency within a unified and multi-tenant architecture that meets the needs of enterprises, small, and midsized businesses



#### Figure 4 NetApp Clustered ONTAP Storage Architecture

An array of NetApp tools and enhancements are available to augment the storage platform. These tools assist in deployment, backup, recovery, replication, management, and data protection. This solution makes use of a subset of these tools and enhancements. Through the use of secure multitenancy, cloud deployments can successfully provide shared storage infrastructure, a core component of cloud by providing secure tenant data separation, address space, authentication, high availability and data protection.

## VMware ESXi Server Cloud Hypervisor System

VMware ESXi hypervisor is a complete, managed server virtualization platform built on a powerful ESXi hypervisor. The ESXi technology is widely accredited as the fastest and most secure virtualization software in the industry. ESXi server is designed for efficient management of virtual servers and delivers cost-effective server consolidation and business continuity.

With VMware ESXi Server, Cloud providers can automate key IT processes to improve service delivery and business continuity for virtual environments resulting in both time and money savings while providing more responsive IT services. Some of the important features in a cloud environment are:

- High Availability automatically restarts virtual machines if a failure occurs at the VM, hypervisor, or server level. The auto restart capability allows users to protect all virtualized applications and bring higher levels of availability to the business. Memory Optimization reduces costs and improves application performance and protection by sharing unused server memory between VMs on the host server.
- Dynamic Workload Balancing improves system utilization and increases application performance by automatically balancing two virtual machines within a resource pool. Workload balancing intelligently places VMs on a most suitable host in the resource pool by matching application requirements to the available hardware resources.

- Automated VM- Protection and Recovery cloud administrators can create snapshot and archival
  policies. Regularly scheduled snapshots help to protect against data loss in case of a VM failure. The
  policies established are based on snapshot type, frequency, amount of historical data that is retained,
  and an archive location. Recovering a VM is completed by simply choosing the last good known
  archive.
- Storage ESXiMotion moves live running virtual machines and their associated virtual disk image within and across resource pools leveraging local and shared storage. This enables users to move a VM between tiers of storage when a VM is limited by storage capacity, and perform maintenance and upgrades with zero downtime.
- Site Recovery- provides site-to-site disaster recovery planning and services for virtual environments. Site recovery is easy to set up, fast to recover, and has the ability to frequently test to ensure disaster recovery plans remain valid.
- Host Power management takes advantage of embedded hardware features to lower data center electricity consumption by dynamically consolidating VMs on fewer systems and then powering off under utilized servers as the demand for services fluctuates.

## Citrix CloudPlatform Cloud Orchestrator System

Citrix CloudPlatform allows virtually unlimited computing power in public, private or hybrid deployments, can be accessed on-demand, and provides real-time usage and metering actual data used. It helps to automate the distribution of compute, network, and storage while adhering to defined policies on load balancing, data security, and compliance. It simplifies and accelerates service delivery by combining self-service provisioning with a catalog of custom-built and pre-defined machine images and gain real-time visibility and reporting within your cloud environment to ensure compliance, security and comprehensive customer usage metering.

Build and deploy CloudPlatform includes a management server and the extensions to run industry-standard hypervisor software such as Citrix Xen Server, VMWare vSphere<sup>TM</sup>, and KVM in your cloud. Deployed on a server farm, the management server can manage resources such as hosts, storage devices, and IP addresses.

CloudPlatform provides all that is needed to sell on-demand, self-service VM instances, storage volumes and networking configurations over the Internet, or set up an on-premise private cloud. It manages by offering visibility into the aggregate storage, IP pools, CPU, memory and other resources used by the cloud, as well as a chronological view of events within it. Once the cloud is built, additional accounts can be set up, VMs can be imported, and controls can be developed and monitored.

# **Cisco UCS and Citrix CloudPlatform Network Design**

This section explains Cisco UCS networking design considerations when deploying Citrix CloudPlatform 4.2.1 in a multi-tenant environment. (Multi-tenancy refers to multiple internal customers for Enterprise Private Clouds or to multiple external customers for Service Provider Public Clouds). In this design multi-tenant Management, guest and corresponding storage network traffic is isolated using the same Cisco UCS infrastructure by physically defining ethernet uplink ports and logical VLAN networks to provide data security in cloud environment. This design also reduces OpEx and CapEx compared to a topology in which a separate dedicated physical servers and switches are deployed to handle multi-tenant network traffic.

Figure 5 presents a detailed view of physical topology, identifying the various levels of the architecture and some of the main components of Cisco UCS in a cloud network design.



#### Figure 5 Citrix CloudPlatform 4.2.1 on Cisco UCS Network Topology

Cisco UCS 5108 Chassis

As shown in Figure 5, a pair of Cisco UCS 6248UP Fabric Interconnects carry cloud multi-tenant network traffic from the Cisco UCS Blade Servers with the help Cisco Nexus 5548UP Switches. Both Cisco UCS 6248UP Fabric Interconnects and Cisco Nexus 5548UP Switches are clustered with the peer link between them to provide high availability. There are two virtual Port Channels (vPCs) that are configured to provide network access paths for the Cisco UCS Blade Servers to establish northbound connections with the Cisco Nexus Switches. Each vPC has VLANs created for cloud tenants management, guest, storage network data paths. Two other virtual Port Channels (vPCs) are configured to provide storage network paths from NetApp Controllers on northbound Nexus Switches.

The same cloud network design can be duplicated to provide multiple multi-tenants, network isolation on cloud on a single Cisco UCS, by provisioning separate vPCs with dedicated physical Ethernet uplink ports and logical VLANs to handle network data traffic.

To handle network scalability in cloud, and large multi-tenant network data traffic bandwidth at any given time, Cisco UCS vPCs allow to dynamically add more Ethernet uplink ports on the fly to accommodate cloud network bandwidth on demand.

## **Cabling Information for Network Devices**

The following cabling information is provided as a reference for cabling the physical equipment in a Citrix CloudPlatform 4.2.1. The tables in this section include both local and remote device, and port locations in order to simplify cabling requirements.

This document assumes that the out-of-band management ports are plugged into an existing management infrastructure at the deployment site.

Be sure to follow the cabling instructions provided in this section. Failure to do so will result in necessary changes to the deployment procedures that follow because specific port locations are mentioned.

Figure 6 shows Citrix CloudPlatform 4.2.1 network cabling diagram. The labels indicate connections to the end points rather than the port numbers on the physical device. For example, connection A is a 10 Gb vPC port connected from Cisco Nexus 5548UP switch A to Cisco Fabric Interconnects A and connection P is a 10 Gb vPC peer links connected from Cisco Nexus 5548UP Switch A to Cisco Nexus 5548UP Switch B.



#### Figure 6 Citrix Cloud Network Cabling Diagram

The following table depicts the major cabling sections in the architecture:

**1**. Inter switch links

ſ

- 2. Virtual Port Channel connectivity
- **3.** Infrastructure connectivity.

Table 1 shows the Ethernet cabling information layout on Cisco Nexus 5548UP Switch A, Cisco UCS Fabric Interconnects A and B, local device and NetApp Storage Controller A and B, local port channels and remote device port.

Cable ID on both end	Ethernet Interface	VLAN	Mode	Speed	Port Channel	Remote Device Port
A	Eth1/15	1,602-603,192-193,200 ,300	Trunk	10G	101	Fabric Interconnects A 1/15
С	Eth1/16	1,602-603,192-193,200 ,300	Trunk	10G	102	Fabric Interconnects B 1/15
G	Eth 1/11	1,602-603,1000-1001	Trunk	1G	None	Nexus 1100-A LOM A
Н	Eth 1/12	1,602-603,1000-1001	Trunk	1 <b>G</b>	None	Nexus 1100-B LOM A
Р	Eth1/13	100	Trunk	10G	100	VPC peer link
E	Eth1/17	192	Access	10G	103	NetApp Controller A E1a
F	Eth 1/18	192	Access	10G	104	NetApp Controller B E1a
Not shown	Eth1/14	1,602-603,192-193,200 ,300	trunk	10G	None	Uplink to Infrastructure n/w

1

Table 2 displays the Ethernet cabling information layout on Cisco Nexus 5548UP Switch B, UCS Fabric Interconnects A and B, local device and NetApp Storage Controller A and B, local port channels remote device port.

Table 2	Ethernet	Cabling on	Cisco	Nexus	Switch B
---------	----------	------------	-------	-------	----------

Cable ID on both end	Ethernet Interface	VLAN	Mode	Speed	Port Channel	Remote Device Port
В	Eth1/15	1,602-603,192-193,200, 300	Trunk	10G	101	Fabric Interconnects A 1/16
D	Eth1/16	1,602-603,192-193,200, 300	Trunk	10G	102	Fabric Interconnects B 1/16

Ι	Eth 1/11	1,602-603,1000-1001	Trunk	1G	None	Nexus 1100-A LOM B
J	Eth 1/12	1,602-603,1000-1001	Trunk	1G	None	Nexus 1100-B LOM B
Р	Eth1/ 13	100	Trunk	10G	100	VPC peer link
G	Eth 1/17	192	Access	10G	103	NetApp Controller B E1b
Н	Eth 1/18	192	Access	10G	104	NetApp Controller B E1b
Not shown	Eth1/14	1,602-603,192-193,200, 300	Trunk	10G	None	Uplink to Infrastructure n/w

Table 2 Ethernet Cabling on Cisco Nexus Switch B

Connect all the cables as outlined in the tables and the corresponding images.

Ethernet Cabling on Cisco Nexus Switch Aand Ethernet Cabling on Cisco Nexus Switch B, shows the Cisco Nexus 5548UP vPC configurations with the vPC domains and corresponding vPC names and IDs in the Citrix cloud. To provide Layer 2 and 3 switching, a pair of Cisco Nexus 5548UP Switches with upstream switching are deployed, providing high availability in the event of failure to Cisco UCS to handle management, guest and storage data traffic. In the Cisco Nexus 5548UP topology, a single vPC feature is enabled to provide high availability, faster convergence in the event of a failure, and greater throughput.

# **Cisco UCS and Cloud Storage Design**

This section explains Cisco UCS and cloud storage design considerations when deploying Citrix CloudPlatform 4.2.1 in a multi-tenant environment. In cloud each tenant's storage network traffic is completely isolated physically and logically by creating Virtual Logical SAN Network (VSAN). This allows creation of completely isolated fabric topologies, each with its own set of fabric services, on top of a scalable common physical infrastructure. Since each VSAN possesses its own zoning service, zoning is configured within each VSAN independently and has no effect on other VSANs and zoning services. This design also reduces OpEx and CapEx compared to the topology in which a separate dedicated physical switch is deployed to handle cloud multi-tenant storage traffic.

To support scalability, the Cisco UCS and Cisco Nexus fabric allows aggregation of multiple physical interfaces into one logical interface to provide higher aggregated bandwidth, load balancing, and link redundancy by creating Port Channels.

In this deployment model, we will create VSANs for isolating multi-tenant storage data traffic and create FC Port Channels for link aggregation.

## **Cabling Information for Storage Devices**

The following information is provided as a reference for cabling the physical equipment in a Citrix CloudPlatform 4.2.1 environment. The tables in this section provide both local and remote device and port locations in order to simplify cabling requirements.

This document assumes that out-of-band management ports are plugged into an existing management infrastructure at the deployment site.

The deployment procedures described use specific port locations. Be sure to follow the cabling directions provided in this section. Any change in the port location will result in a consequent change in the deployment procedure.

Before starting, be sure the configuration matches what is described in the tables and figures in this section.

Figure 7 shows Citrix CloudPlatform 4.2.1 network cabling diagram. The labels indicate connections to the end points rather than the port numbers on the physical device. For example, connection A is an FCoE 10-gb unified FCoE port connected from Cisco Nexus 5548UP switch A to Cisco Fabric Interconnects A.

#### Figure 7 Uplink Network Cabling for the Citrix CloudPlatform 4.2.1



# **Cisco UCS Quality-of-Service System and Policy**

In a multi-tenant cloud environment service level availability plays a major role in defining various cloud services which are built on cloud infrastructure. One of the infrastructures is the cloud network for handling data traffic internally and externally. In this paper we will focus on how to define network service level agreements based on Ethernet network bandwidth offered which can later be provisioned to handle cloud multi-tenants data traffic.

Cisco UCS uses IEEE Data Center Bridging (DCB) to handle all traffic within Cisco UCS. This industry-standard enhancement to Ethernet divides the bandwidth of the Ethernet pipe into eight virtual lanes. System classes determine how the DCB bandwidth in these virtual lanes is allocated across the entire Cisco UCS platform.

Each system class reserves a specific segment of bandwidth for a specific type of traffic, providing an assured level of traffic management even in an over-subscribed system. For example, the Fibre Channel priority system class can be configured to determine the percentage of DCB bandwidth allocated to FCoE traffic.

System Class	Description
<ul> <li>Platinum Priority</li> <li>Gold Priority</li> <li>Silver Priority</li> <li>Bronze Priority</li> </ul>	These classes set the Quality of Service (QoS) for all the servers. QoS system classes are defined in the service profile associated to the server. Each of these system classes manages one lane of traffic. All properties of these system classes are available to assign custom settings and policies.
Best-Effort Priority	This class sets the QoS for the lane that is reserved for basic Ethernet traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a drop policy to allow it to drop data packets if required (can we write why the data packets will be dropped? In what circumstances?).
Fibre Channel Priority	This class sets the QoS for the lane that is reserved for FCoE traffic. Some properties of this system class are preset and cannot be modified. For example, this class has a no-drop policy to help ensure that it never drops data packets.

#### Table 3 System Classes defined as per the Quality of Service

To provide network based Service Level Agreement on Citrix CloudPlatform 4.2.1 environment for multi-tenant network requirements, the following system class SLAs have been defined. These SLAs are directly mapped to the cloud network offering which are provided to cloud tenants for choosing network infrastructure based on cost.

• Platinum-Network-SLA

To meet multi-tenant network requirements, to provide higher bandwidth, and lower latency, Cisco UCS QoS system class offers Platinum class with the highest weight (bandwidth) and a maximum transmission unit (MTU) of 9000 defined for handling large Cloud I/O network.

For example, to handle virtual machine migration across server pools in a cluster, define Platinum-Network-SLA policy for management traffic that is applied on Cisco UCS Static vNICs, part of management network bond interfaces.

• Gold-Network-SLA

To provide slightly lower bandwidth, and lower latency network for multi-tenant network requirements compared to Platinum-Network-SLA, Cisco UCS QoS system class offers Gold-Network-SLA with the second highest weight (bandwidth) and a maximum transmission unit (MTU) of 9000 for handling large Cloud I/O network traffic.

• Silver-Network-SLA

On the same cloud network SLA requirements to provide lower bandwidth and lower latency network for multi-tenant network requirements, Silver-Network-SLA is defined. The Cisco UCS QoS system class offers Silver-Network-SLA with the third highest weight (bandwidth) and a Maximum Transmission Unit (MTU) of 9000 for handling large Cloud I/O network traffic.



In this paper we will define Cisco UCS QoS policies based on the described Cloud Network SLA Offerings which are related to specific customer needs and can be altered depending on your cloud network infrastructure offering.

To handle VM migration across server pools in a cluster that requires higher network bandwidth and lower latency, Platinum-Network-SLA policy for management traffic is defined and is later applied on Cisco UCS static vNICs that are part of management network bond interfaces. To handle NFS storage traffic, for handling operation such as cloud VM backup/ restore, templates, ISO or primary storage for storing VMs and so on, which require better bandwidth, Gold-Network-SLA policy for handling all storage related traffic is defined and is later applied on Cisco UCS static vNICs that are part of storage network bond interfaces. To handle VMs' public or private traffic, Silver-Network-SLA policy for such guest traffic is defined and is later applied on Cisco UCS static vNICs that are part of guest network bond interfaces.

After defining cloud network SLAs, Cisco UCS allows to define QoS policies that are assigned to the outgoing traffic for a vNIC. It is required to include a QoS policy with in a vNIC policy, which is then included in a service profile to configure the vNIC.

Table 4 lists the QoS policy name with the corresponding priority, weight, and MTU value. These values are applied to static and dynamic vNICs in the Microsoft SQL Server deployment environment.

Policy Name	Priority	Weight (Percentage)	MTU
Platinum-Net-SLA	Platinum	10	9000
Gold-Net-SLA	Gold	9	9000
Silver-Net-SLA	Silver	8	9000

Table 4 Cisco UCS QoS Policies and Network SLAs

# **Configuring Devices**

This section describes the steps and procedure to configure the hardware devices in the unified design.

This section offers a detail of how to configure and deploy the UCS to make it ready to deploy the storage and CloudPlatform 4.2.1 on UCS:

- Cisco Nexus Switch Configuration
- Cisco UCS Deployment
- Uplink Port Channel Creation
- Storage Configurations

# **Cisco Nexus Switch Configurations**

In this section vPC design is explained as per which the switches and other components will be configured and set up. The following section provides step-by-step procedure to configure the ports, features, VLANS, and Ethernet interfaces on the Nexus switches. The following tasks are detailed in this section:

- vPC Mapping in the Switch
- Configuring the Cisco Nexus Switch
- Enabling feature and Global configuration
- Configuring VLANS
- Configuring Port channel

- Configuring Virtual port channel
- Configuring the Port Channel
- Configuring the Ethernet Interfaces

## vPC Mapping in the Switch

A virtual port channel (vPC) allows links that are physically connected to two different Cisco Nexus 5000 Series devices to appear as a single port channel by a third device. The third device can be a switch, server, or any other networking device that supports port channels. A vPC can provide Layer 2 multipathing, which allows you to create redundancy and increase bisectional bandwidth by enabling multiple parallel paths between nodes and allowing load balancing traffic.

Table 5 shows the Cisco Nexus 5548UP vPC configurations with the vPC domains and corresponding vPC names and IDs in cloud. To provide Layer 2 and 3 switching, a pair of Cisco Nexus 5548UP Switches with upstream switching are deployed, providing high availability in the event of failure to Cisco UCS to handle management, guest and storage data traffic. In the Cisco Nexus 5548UP topology, a single vPC feature is enabled to provide high availability, faster convergence in the event of a failure, and greater throughput.

vPC Domain	vPC Name	vPC ID
100	TenantvPCNetworkA	101
100	TenantvPCNetworkB	102
100	TenantUnifiedStorageA	103
100	TenantUnifiedStorageB	104
100	TenantFCoEFabric	10

Table 5vPC Mapping

In the vPC design table, a single vPC domain, Domain 100, is created across Cisco Nexus 5548UP member switches to define vPCs to carry specific network traffic. This topology defines four vPCs with IDs 101 through 104. vPC IDs 101 and 102 are defined for traffic from Cisco UCS Fabric Interconnects, and vPC IDs 103 and 104 are defined for iSCSI traffic, and vPC 105 and 106 for NFS traffic on NetApp storage. These vPCs are managed within the Cisco Nexus 5548UP, which connects Cisco UCS Fabric Interconnects and the NetApp storage system.

# **Configuring the Cisco Nexus Switch**

The first time that you access Cisco Nexus 5000 Series, it runs a setup program that prompts you for the IP address and other configuration information necessary for the switch to communicate over the Ethernet interface. This information is required to configure and manage the switch.

#### **Preparing to Configure the Switch**

Before you configure Cisco Nexus 5000 Series switch for the first time, you need the following information:

• Administrator password

Note	

If a password is weak (short, easy-to-decipher), your password configuration is rejected. Be sure to configure a strong password.

- If you are using an IPv4 address for the management interface, you need the following information:
  - IPv4 subnet mask for the switch's management interface
  - IPv4 address of the default gateway (optional)
- SSH service on the switch (optional)

To enable this service, select the type of SSH key (dsa/rsa/rsa1) and number of SSH key bits (768 to 2048).

- NTP server IPv4 address (optional)
- SNMP community string (optional)
- Switch name (optional)

This is your switch prompt

• An additional login account and password (optional)



If you are using IPv4, be sure to configure the IPv4 route, the IPv4 default network address, and the IPv4 default gateway address to enable SNMP access.

#### **Default Login**

The switch has the network administrator as a default user (admin). You cannot change the default user at any time.

There is no default password so you must explicitly configure a strong password. If you configure and subsequently forget the password, you have the option to recover the password.

Note

If you enter the write erase command and reload the switch, you must reconfigure the default user (admin) password using the setup procedure.

To set the initial configurations on the Cisco Nexus 5548 switches, follow these steps:

#### For Cisco Nexus A and Cisco Nexus B

The NX-OS setup should automatically start on initial boot and connection to the serial or console port of the switch. Enter the following commands to configure the Cisco Nexus Switch:

- 1. Enter yes to enforce secure password standards: yes
- 2. Enter the password for the administrator (adminuser): <xxxx>
- 3. Enter the password a second time to commit the password; <xxxx>
- 4. Enter yes to enter the basic configuration dialog: yes
- 5. Create another login account (yes/no) [n]: Enter
- 6. Configure read-only SNMP community string (yes/no) [n]: Enter
- 7. Configure read-write SNMP community string (yes/no) [n]: Enter
- 8. Enter the switch name: <Nexus A Switch name> Enter

- 9. Continue with out-of-band (mgmt0) management configuration? (yes/no) [y]: Enter
- 10. Mgmt0 IPv4 address: <Nexus A mgmt0 IP> Enter
- 11. Mgmt0 IPv4 netmask: <Nexus A mgmt0 netmask> Enter
- 12. Configure the default gateway? (yes/no) [y]: Enter
- 13. IPv4 address of the default gateway: <Nexus A mgmt0 gateway> Enter
- 14. Enable the telnet service? (yes/no) [n]: Enter
- **15.** Enable the ssh service? (yes/no) [y]: Enter
- 16. Type of ssh key you would like to generate (dsa/rsa):rsa
- **17**. Number of key bits <768–2048>:1024 Enter
- 18. Configure the ntp server? (yes/no) [y]: n Enter
- **19.** NTP server IPv4 address: *<NTP Server IP>* Enter
- 20. Enter basic FC configurations (yes/no) [n]: Enter
- 21. Would you like to edit the configuration? (yes/no) [n]: Enter

Note

Be sure to review the configuration summary before enabling it.

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

Note

Configuration may be continued from the console or by using SSH. To use SSH, connect to the mgmt0 address of Nexus A or B.



Log in as user admin with the password previously entered.

## **Enabling Features and Global Configuration**

#### **Enabling Features**

To enable the vPC on the devices and define the communication between the linked devices, Link Aggregation Control Protocol (LACP), virtual port channel (vPC), and interface-vlan features must be activated on both the Cisco Nexus switches. To set these features on the two switches follow these steps:

For Cisco Nexus A and Cisco Nexus B:

- **1.** Type configure t to enter the global configuration mode.
- 2. Type feature lacp.
- 3. Type feature interface-vlan.
- 4. Type feature vpc.

#### **Setting Global Configurations**

vPC eliminates the Spanning Tree Protocol (STP) blocked ports, and it is enabled as global configurations, which ensures that all the ports on the Cisco Nexus Switches appear as network port. To set the STP global configurations, follow these steps:

For Cisco Nexus A and Cisco Nexus B:

- 1. From the global configuration mode, type spanning-tree port type network default to make sure that, by default, the ports are considered as network ports with regard to spanning-tree.
- **2.** Type spanning-tree port type edge bpduguard default to enable bpduguard on all edge ports by default.
- 3. Type spanning-tree port type edge bpdufilter default to enable bpdufilter on all edge ports by default.

## **Configuring VLANs**

A VLAN is a group of end stations in a switched network that is logically segmented by function, project team, or application, without regard to the physical locations of the users. VLANs have the same attributes as physical LANs, but the end stations can be grouped even if they are not physically located on the same LAN segment.

This section details how the VLANS can be configured on both the Nexus switches.

In this design the VLANS have been defined as listed in Table 6.

VLAN Name	VLAN Purpose	ID used in this document	Network Address
Management	For Mgmt and VM Migration traffic	602	10.65.121.0/24
BareMetal-VLAN20	For Baremetal host PXE Boot traffic	20	20.1.1.0/24
Guest-VLAN	For guest VM public traffic	603	10.65.122.0/24
Guest-VLAN-1000	For guest VM Private traffic	1000	10.1.0.0/24
Guest-VLAN-1001	For guest VM Private traffic	1001	10.2.0.0/24
NFS	For NFS Storage traffic	193	193.191.1.0/24
vMotion	For vMotion traffic	192	192.191.1.0/24

Table 6 VLANs for Citrix CloudPlatform 4.2.1 setup

#### For Cisco Nexus A and Cisco Nexus B

To configure the VLANS on both the Cisco Nexus Switches, follow these steps:

- 1. Type config-t.
- 2. Type vlan <Management VLAN ID>.
- 3. Type name Management.
- 4. Type exit.
- 5. Type vlan <BareMetal-VLAN20 VLAN ID>.
- 6. Type name BareMetal-VLAN.
- 7. Type exit.

- 8. Type vlan <guest VLAN ID>.
- 9. Type name guest-VLAN.
- 10. Type exit.
- **11.** Type vlan <guest VLAN ID>.
- **12.** Type name guest-VLAN-1000.
- 13. Type exit.
- 14. Type vlan <guest VM VLAN ID>.
- **15.** Type name guest-VLAN-1001.
- 16. Type exit.
- **17.** Type vlan <NFS VLAN ID>.
- 18. Type name NFS.
- 19. Type exit.
- **20.** Type vlan <vMotion VLAN ID>.
- **21**. Type name vMotion.
- 22. Type exit.
- **23.** Type vlan <FCoE VLAN ID>.
- 24. Type name VLAN0200.
- **25**. Type fcoe vsan <ID 200>.
- **26**. Type state <active>.
- **27**. Type no <shutdown> .
- 28. Type exit.
- **29.** Type vlan <FCoE VLAN ID>.
- **30**. Type name VLAN0300.
- **31**. Type fcoe vsan  $\langle ID 300 \rangle$ .
- **32**. Type state <active>.
- **33**. Type no <shutdown>.
- **34.** Type exit.

## **Configuring Port Channels**

This section provides details to create and configure individual port descriptions for troubleshooting steps and verification. To create the port channels to the Cisco Nexus switches A and B, follow these steps:

#### Cisco Nexus 5548 A

I

- 1. From the global configuration mode, type interface Eth1/13.
- 2. Type description <VPC Peer Link>.
- 3. Type exit.
- 4. Type interface Eth1/15.

- 5. Type description <Cisco UCS Manager A:Eth1/5>.
- 6. Type exit.
- 7. Type interface Eth1/16.
- 8. Type description <Cisco UCS Manager B: Eth1/5>.
- 9. Type exit.
- **10.** Type interface Eth1/17.
- **11.** Type description <NetApp Controller Flexpod A:E1a>.
- 12. Type exit.
- **13.** Type interface Eth1/18.
- 14. Type description <NetApp Controller Flexpod B:E1a>.
- 15. Type exit.
- **16.** Type interface Eth1/31.
- 17. Type description <FCoE Uplink To Nexus 5548 B>.
- 18. Type exit.
- **19.** Type interface Eth1/32.
- 20. Type description <FCoE Uplink To Nexus 5548 B>.
- 21. Type exit.

#### Cisco Nexus 5548 B

- 1. From the global configuration mode, type interface Eth1/13.
- **2.** Type description <VPC Peer Link>.
- 3. Type exit.
- 4. Type interface Eth1/15.
- 5. Type description <Cisco UCS Manager A:Eth1/5>.
- 6. Type exit.
- 7. Type interface Eth1/16.
- 8. Type description <Cisco UCS Manager B:Eth1/5>.
- 9. Type exit.
- **10.** Type interface Eth1/17.
- **11.** Type description <NetApp Controller Flexpod A:E1b>.
- 12. Type exit.
- **13**. Type interface Eth1/18.
- 14. Type description <NetApp Controller Flexpod B:E1b>.
- 15. Type exit.
- **16.** Type interface Eth1/31.
- 17. Type description <FCoE Uplink To Nexus 5548 B>.

- 18. Type exit.
- **19.** Type interface Eth1/32.
- 20. Type description <FCoE Uplink To Nexus 5548 B>.
- 21. Type exit.

## **Configuring Virtual Port Channels**

A virtual port channel (vPC) allows links that are physically connected to two different Cisco Nexus 5000 Series devices to appear as a single port channel by a third device. To configure the virtual Port Channels (vPCs) on Cisco Nexus switches A and B, follow these steps:

#### Cisco Nexus 5548 A

- 1. From the global configuration mode, type vpc domain <Nexus vPC domain ID>.
- **2**. Type role priority 10.
- 3. Type peer-keepalive destination <Nexus B mgmt0 IP> source <Nexus A mgmt0IP>.
- 4. Type exit.
- 5. Type interface Port-Channel 100.
- 6. Type vpc peer-link.
- 7. Type exit.
- 8. Type interface Port-Channel 101.
- 9. Type vpc 101.
- **10.** Type exit.
- **11.** Type interface Port-Channel 102.
- 12. Type vpc 102.
- 13. Type exit.
- 14. Type interface Port-Channel 103.
- 15. Type vpc 103.
- **16.** Type exit.
- **17.** Type interface Port-Channel 104.
- **18**. Type vpc 104.
- 19. Type exit.
- **20.** Type interface Port-Channel 10.
- 21. Type exit.
- **22.** Type copy run start.

#### Cisco Nexus 5548 B

I

- 1. From the global configuration mode, type vpc domain <Nexus vPC domain ID>.
- **2.** Type role priority 20.
- 3. Type peer-keepalive destination <Nexus A mgmt0 IP> source <Nexus B mgmt0IP>.
- 4. Type exit.
- 5. Type interface Port-Channel 100.

- 6. Type vpc peer-link.
- 7. Type exit.
- 8. Type interface Port-Channel 101.
- 9. Type vpc 101.
- **10.** Type exit.
- **11.** Type interface Port-Channel 102.
- 12. Type vpc 102.
- 13. Type exit.
- 14. Type interface Port-Channel 103.
- 15. Type vpc 103.
- 16. Type exit
- **17.** Type interface Port-Channel 104.
- **18**. Type vpc 104.
- **19.** Type exit.
- **20.** Type interface Port-Channel 10.
- 21. Type exit.
- **22.** Type copy run start.

#### **Adding Port Channel Configurations**

After the port channels have been created, it is required to configure them individually to meet the design requirements. The ports are configured as per the vPC Mapping defined earlier in Table 6. To add the port channel configurations on the Cisco Nexus Switches A and B, follow these steps:

#### Cisco Nexus 5548 A

- 1. From the global configuration mode, type interface Port-Channel 100.
- **2.** Type switchport mode trunk.
- **3.** Type switchport trunk native vlan <Native VLAN ID>.
- Type switchport trunk allowed vlan <MGMT VLAN ID, BareMetal-VLAN VLAN ID GUESTVM VLAN ID, guest-VLAN-1000 VLANID, guest-VLAN-1001 VLANID, NFS VLAN ID, vMotion VLAN ID>.
- 5. Type spanning-tree port type network.
- 6. Type no shutdown.
- 7. Type exit.
- 8. Type interface Port-Channel 101.
- 9. Type switchport mode trunk.
- 10. Type switchport trunk native vlan <Default VLAN ID>.
- Type switchport trunk allowed vlan <MGMT VLAN ID, BareMetalk-VLAN VLANID, guest-VLAN VLAN ID, guest-VLAN-1000 VLAN ID, guest-VLAN-1001 VLAN ID, NFS VLAN ID, vMotion VLAN ID>.

**12.** Type spanning-tree port type edge trunk.

- 13. Type no shut.
- 14. Type exit.
- **15.** Type interface Port-Channel 102.
- **16.** Type switchport mode trunk.
- 17. Type switchport trunk native vlan <Native VLAN ID>.
- 18. Type switchport trunk allowed vlan <NFS VLAN ID>.
- **19.** Type spanning-tree port type edge trunk.
- 20. Type no shut.
- **21**. Type exit.
- **22.** Type interface Port-Channel 103.
- **23.** Type switchport mode trunk.
- 24. Type switchport trunk native vlan <Native VLAN ID>.
- 25. Type switchport trunk allowed vlan <NFS VLAN ID>.
- 26. Type no shut.
- 27. Type exit.
- **28.** Type interface Port-Channel 104.
- **29.** Type switchport mode trunk.
- 30. Type switchport trunk native vlan <Native VLAN ID>.
- 31. Type no shut.
- 32. Type exit.
- **33.** Type interface Port-Channel 10.
- **34**. Type switchport mode trunk.
- 35. Type switchport trunk native vlan <Native VLAN ID>.
- **36.** Type switchport trunk allowed vlan <200>.
- 37. Type no shut.
- **38.** Type exit.
- **39.** Type copy run start.

#### Cisco Nexus 5548 B

I

- 1. From the global configuration mode, type interface Port-Channel 100.
- 2. Type switchport mode trunk.
- 3. Type switchport trunk native vlan <Native VLAN ID>.
- Type switchport trunk allowed vlan <MGMT VLAN ID, BareMetalVlan VLANID, guestVM VLAN ID, guest-VLAN-1000 VLANID, guest-VLAN-1001 VLANID,NFS VLAN ID, vMotion VLAN ID>.
- 5. Type spanning-tree port type network.
- 6. Type no shutdown.
- 7. Type exit.

- 8. Type interface Port-Channel 101.
- **9.** Type switchport mode trunk.
- 10. Type switchport trunk native vlan <Default VLAN ID>
- Type switchport trunk allowed vlan <MGMT VLAN ID, BareMetalVlan VLANID, guest-VLAN VLAN ID, guest-VLAN-1000 VLANID, guest-VLAN-1001 VLANID, NFS VLAN ID, vMotion VLAN ID>
- **12.** Type spanning-tree port type edge trunk.
- 13. Type no shut.
- 14. Type exit.
- **15.** Type interface Port-Channel 102.
- **16.** Type switchport mode trunk.
- 17. Type switchport trunk native vlan <Native VLAN ID>
- Type switchport trunk allowed vlan <MGMT VLAN ID, BareMetalVlan VLANID, guest-Vlan VLAN ID, guest-VLAN-1000 VLANID, guest-VLAN-1001 VLANID, NFS VLAN ID, vMotion VLAN ID>.
- 19. Type spanning-tree port type edge trunk.
- 20. Type no shut.
- 21. Type exit.
- **22.** Type interface Port-Channel 103.
- **23.** Type switchport mode trunk.
- 24. Type switchport trunk native vlan <Native VLAN ID>.
- 25. Type no shut.
- 26. Type exit.
- 27. Type interface Port-Channel 104.
- **28.** Type switchport mode trunk.
- 29. Type switchport trunk native vlan <Native VLAN ID>.
- 30. Type no shut.
- 31. Type exit.
- **32.** Type interface Port-Channel 10.
- **33**. Type switchport mode trunk.
- 34. Type switchport trunk native vlan <Native VLAN ID>.
- **35**. Type switchport trunk allowed vlan <300>.
- 36. Type no shut.
- 37. Type exit.
- **38.** Type copy run start.

## **Configuring Ethernet Interfaces**

Every port channel created must have their interfaces configured to join with the relevant VLANs. To configure the Ethernet interfaces on the port channels between the devices, follow these steps:

1

#### Cisco Nexus 5548 A

- 1. From the global configuration mode, type interface Eth1/13.
- 2. Type channel-group 100 mode active.
- **3**. Type no shutdown.
- 4. Type exit.
- 5. Type interface Eth1/15.
- 6. Type channel-group 101 mode active.
- 7. Type no shutdown.
- 8. Type exit.
- **9.** Type interface Eth1/16.
- **10**. Type channel-group 102 mode active.
- 11. Type no shutdown.
- 12. Type exit.
- **13**. Type interface Eth1/17.
- 14. Type channel-group 103 mode active.
- 15. Type no shutdown.
- 16. Type exit.
- **17**. Type interface Eth1/18.
- **18**. Type channel-group 104 mode active.
- 19. Type no shutdown.
- 20. Type exit.
- **21**. Type interface Eth1/17.
- **22**. Type channel-group 103 mode active.
- 23. Type no shutdown.
- 24. Type exit.
- **25**. Type interface vfc 17.
- **26.** Type bind interface Ethernet 1/17.
- 27. Type switch port trunk allowed vsan 200.
- **28.** Type exit.
- **29**. Type interface vfc 18.
- **30.** Type bind interface Ethernet 1/18.
- **31**. Type switch port trunk allowed vsan 200.
- 32. Type exit.
- **33.** Type copy run start.

#### Cisco Nexus 5548 B

I

1. From the global configuration mode, type interface Eth1/13.

- 2. Type channel-group 100 mode active.
- 3. Type no shutdown.
- 4. Type exit.
- 5. Type interface Eth1/15.
- 6. Type channel-group 101 mode active.
- 7. Type no shutdown.
- 8. Type exit.
- **9.** Type interface Eth1/16.
- **10**. Type channel-group 102 mode active.
- **11**. Type no shutdown.
- 12. Type exit.
- **13**. Type interface Eth1/17.
- 14. Type channel-group 103 mode active.
- **15.** Type no shutdown.
- 16. Type exit.
- **17**. Type interface Eth1/18.
- **18.** Type channel-group 104 mode active.
- 19. Type no shutdown.
- 20. Type exit.
- **21**. Type interface vfc 17.
- **22.** Type bind interface Ethernet 1/17.
- **23.** Type switch port trunk allowed vsan 200.
- 24. Type exit.
- **25.** Type interface vfc 18.
- **26.** Type bind interface Ethernet 1/18.
- **27.** Type switch port trunk allowed vsan 200.
- 28. Type exit.
- **29.** Type copy run start.

## **Configuring Nexus 1100 Ethernet Ports**

This section provides details to create and configure individual port descriptions for troubleshooting steps and verification. To create the ethernet ports to the Cisco Nexus switches A and B, follow these steps:

#### Cisco Nexus 5548 A

- 1. From the global configuration mode, type interface Eth1/11.
- 2. Type description <Nexus 1100 A LOM A>.
- **3.** Type switchport mode trunk.

- 4. Type switchport trunk allowed vlan 602,603,1000,1001,50.
- 5. Type exit.
- **6.** Type interface Eth1/12.
- 7. Type description <Nexus 1100 B LOM A>.
- 8. Type switchport mode trunk.
- 9. Type switchport trunk allowed vlan 602,603,1000,1001,50.
- 10. Type exit.
- **11**. Type copy run start.

#### Cisco Nexus 5548 B

- 1. From the global configuration mode, type interface Eth1/11.
- 2. Type description <Nexus 1100 A LOM B>.
- 3. Type switchport mode trunk.
- 4. Type switchport trunk allowed vlan 602,603,1000,1001,50.
- 5. Type exit.
- **6.** Type interface Eth1/12.
- 7. Type description <Nexus 1100 B LOM B>.
- 8. Type switchport mode trunk.
- **9.** Type switchport trunk allowed vlan 602,603,1000,1001,50.
- 10. Type exit.
- **11**. Type copy run start.

# FlexPod Cisco Nexus 1000V vSphere

The following sections provide detailed procedures for installing a pair of high-availability (HA) Cisco Nexus 1000V software DVS Switch in a FlexPod configuration. Primary and standby Cisco Nexus 1000V Virtual Supervisor Modules (VSMs) are installed on the separate ESX hosts. By the end of this section, a Cisco Nexus 1000V distributed virtual switch (DVS) will be provisioned.

This procedure assumes that the Cisco Nexus 1000V software version 4.2.1(1)SV2(1.1a) has been downloaded from www.cisco.com and expanded. It also assumes that two ESX host is been installed with VMware vSphere 5.1 with Enterprise Plus licensing and VMware vCenter 5.1 application is installed which is part of Infrastructure Pod.

## Installation of Primary and Secondary Cisco Nexus 1000V VSMs

- 1. Lunch Nexus1000V-install\_CNX.jar file from command prompt on Infrastructure Windows client
- 2. Click the Cisco Nexus 1000V Complete Installation radio button.
- 3. Select Standard Type.
- 4. Click Next
- 5. Enter vCenter IP Address <xx.xx.xx>, Enter User ID <administrator> and Password <XXXXXX>.

- 6. Click Next
- 7. Enter or Browse ESX Host 1 IP Address <xx.xx.xx.xx> and shared Data Store <xxxxxxxx>.

1

- 8. Enter or Browse ESX Host 2 IP Address <xx.xx.xx> and shared Data Store <xxxxxxx>.
- 9. Enter Virtual Machine Name <VSM-TenantA>.
- 10. Browse the path to locate Nexus 1000V software <nexus-1000v.4.2.1.1.SV2.1.1a.ova> file.
- 11. By default Layer 3 radio button will be selected for Layer 2 / Layer 3 Connectivity.

```
Figure 8
```

#### **Cisco Nexus 1000V Standard Configuration Data details**

<u>\$</u>	Cisco Nexus 1	000V Installer App	_ 0			
Steps	Standard Configuration Da	ita				
<ol> <li>Prerequisites</li> <li>vCenter Server Credentials</li> <li>Standard Configuration Data</li> <li>Standard Configuration Review</li> <li>Confirmation</li> </ol>	Import Configuration Host 1 IP Address / Name	10.65.121.20	Browse			
6. Hosts Selection	Data Store	TenantA-FC-PrimaryStorage	Browse			
7. Host Review	Host 2 IP Address / Name	10.65.121.21	Browse			
	Data Store	TenantA-FC-PrimaryStorage	Browse			
	Virtual Machine Name	VSM-TenantA				
	OVA Image Location	VSM\Install\nexus-1000v.4.2.1.SV2.1.1a.ova	Browse			
11 11 11	Layer 2 / Layer 3 Connectivity	🔿 Layer L2	Layer L3			
CISCO.	VSM IP Address	10.65.121.170				
	Subnet Mask	255.255.255.0				
Nexus 1000V	Gateway IP Address	10.65.121.1				
	Domain ID	2				
	Management VLAN	602				
	Migrate Host(s) to DVS	⊖ Yes	● No			

- 12. Click Next
- 13. Check Standard Configuration Review data
- 14. Click Next
- 15. Click No radio button Do you want to add more modules
- 16. Click Next
- 17. Click Next in Host Selection
- 18. Click Finish in Host review

```
Figure 9
```

**Cisco Nexus 1000V Standard Installation Summary details** 

🖆 Cisco Nexus 1000V Installer App 📃 🗖 🗙							
Steps	Summary						
<ol> <li>Prerequisites</li> <li>vCenter Server Credentials</li> <li>Standard Configuration Data</li> <li>Standard Configuration Review</li> <li>Confirmation</li> <li>Hosts Selection</li> <li>Host Review</li> <li>Summary</li> </ol>	Initial Virtual Supervisor Module installation Completed Successfully         connection vcenter         ip address: 10.104.252.107         remote port: 80         protocol: vmware-vim https         certificate: default         datacenter name: Tenant-DC         DV5 uuid: 71 e6 26 50 d1 e7 8d db-de ab e8 70 4a ee 89 f3         config status: Enabled         operational status: Connected         sync status: Complete         version: VMware vCenter Server 5.1.0 build-1064983						
CISCO Nexus 1000V	You can login to VSM using the following credentials: VSM IP: 10.65.121.170 Username: admin Password: <set as="" by="" case="" in="" installation="" is="" of="" or="" same="" standard="" the="" user,="" username=""> Initial VSM Installation has completed. You can install VEM software on other hosts by re-running the installer and selecting the 'VEM Installation' option.</set>						
	< Prev Next > Finish Close						

## **Configure Cisco Nexus 1000V Virtual Appliance**

#### **Cisco Nexus 1000V**

I

To configure Cisco Nexus 1000-V VSM-TenantA-1, follow these steps:

1. Login to VSM-TenantA-1 VM on ESX Host 10.65.121.20 using VMware VI Client

```
Enter the User Name <<admin>>
Enter Password <<admin>>
Enter <<Conf Terminal>>
Enter <<feature ssh>> <<feature telnet>> <<feature http-server>>>
Enter <<Copy run start>>
2. Perform Base Configuration of the Primary VSM
```

- To perform the base configuration of the primary VSM, follow these steps:
- 1. Using an SSH client, log in to the primary Cisco Nexus 1000V VSM as admin.
- 2. Run the following configuration commands.

config t

```
ntp server <<var_global_ntp_server_ip>> use-vrf management
vlan <<var_ib-mgmt_vlan_id 602>>
name IB-MGMT-VLAN
vlan <<var_guest_vlan_id 603>>
name guestVM-VLAN
vlan <<var_guest_vlan_id 1000>>
name guestVM-VLAN1000
vlan <<var_guest_vlan_id 1001>>
name guestVM-VLAN1001
exit
port-profile type ethernet TenantA-guest-Uplink
vmware port-group
switchport mode trunk
switchport trunk native vlan <<var_native_vlan_id>>
switchport trunk allowed vlan <<default 1>>,<<var_ib-mgmt_vlan_id 602>>, <<</pre>
var_guest_vlan_id 603>>, <<var_guest_vlan_id 1000>>, <<var_N1KV_Ctrl_vlan_id 50>>, <<</pre>
var_guest_vlan_id 1001>>
channel-group auto mode on mac-pinning
no shutdown
system vlan <<var_ib-mgmt_vlan_id 602>>, << var_guest_vlan_id 603>>,
<<var_guest_vlan_id 1000>>, << var_guest_vlan_id 1001>>
system mtu 9000
state enabled
port-profile type vethernet TenantA-VSM-VEM-Network
vmware port-group
switchport mode access
switchport access vlan <<var_ib-mgmt_vlan_id 602>>
no shutdown
capability 13control
system vlan <<var_ib-mgmt_vlan_id 602>>
state enable
exit
copy run start
```

# **Cisco UCS Deployment**

The following section provides a detailed procedure for configuring the Cisco Unified Computing System for use in the FlexPod environment. These steps should be followed precisely because a failure to do so could result in an improper configuration.

This section describes how to perform the following tasks that helps in setting up Cisco UCS:

- Configuring Cisco UCS 6248 Fabric Interconnects
- Modifying the Chassis Discovery Policy
- Creating Uplink Port-Channel
- Enabling Jumbo frames
- Enabling QoS Policy in Cisco UCS 6248 Fabric Interconnects
- Enabling QoS Qualifications on Cisco Nexus 5548UP Switch
- Configuring VLAN on Cisco UCS 6248 Fabric Interconnects

## Configuring Cisco UCS 6248 Fabric Interconnects

To perform the initial setup of the Cisco UCS 6248 Fabric Interconnects A and B, follow these steps:

I

#### **Fabric Interconnects A**

- 1. Connect to the console port on the first Cisco UCS 6248 fabric interconnect.
- 2. At the prompt to enter the configuration method, enter console to continue.
- 3. If asked to either do a new setup or restore from backup, enter setup to continue.
- 4. Enter y to continue to set up a new fabric interconnect.
- 5. Enter y to enforce strong passwords.
- 6. Enter the password for the admin user.
- 7. Enter the same password again to confirm the password for the admin user.
- 8. When asked if this Fabric Interconnects is part of a cluster, answer y to continue.
- 9. Enter A for the switch fabric.
- **10.** Enter the cluster name for the system name.
- **11.** Enter the Mgmt0 IPv4 address.
- **12.** Enter the Mgmt0 IPv4 netmask.
- **13**. Enter the IPv4 address of the default gateway.
- **14.** Enter the cluster IPv4 address.
- 15. To configure DNS, answer y.
- **16.** Enter the DNS IPv4 address.
- 17. Answer y to set up the default domain name.
- **18.** Enter the default domain name.
- **19.** Review the settings that were printed to the console, and if they are correct, answer yes to save the configuration.
- 20. Wait for the login prompt to make sure the configuration has been saved.

#### **Fabric Interconnects B**

- 1. Connect to the console port on the second Cisco UCS 6248 fabric interconnect.
- 2. When prompted to enter the configuration method, enter console to continue.
- **3.** The installer detects the presence of the partner Fabric Interconnects and adds this Fabric Interconnects to the cluster. Enter y to continue the installation.
- 4. Enter the admin password for the first Fabric Interconnects.
- 5. Enter the Mgmt0 IPv4 address.
- 6. Answer yes to save the configuration.
- 7. Wait for the login prompt to confirm that the configuration has been saved.

#### **Cisco UCS Manager-Login**

After the Cisco UCS Fabric Interconnects has been configured, the next step would be to download and start using the Cisco UCS Manager software. To login to the Cisco UCS Manager follow these steps:

- 1. Open a Web browser and navigate to the Cisco UCS 6248 Fabric Interconnects cluster address.
- 2. Select the Launch link to access Cisco UCS Manager software.
- 3. If prompted to accept security certificates, accept as necessary.

- 4. When prompted, enter admin for the username and enter the administrative password and click **Login** to log into the Cisco UCS Manager.
- 5. Click the **Equipment** tab in the left pane.
- 6. Select Fabric Interconnects A.
- 7. In the right pane, click the General tab.
- 8. Select Configure Unified Ports.
- 9. Select Yes to launch the wizard.
- **10.** Use the slider tool and move one position to the left to configure the last two ports (31 and 32) as FC uplink ports.
- 11. Ports 31 and 32 now have the "B" indicator indicating their reconfiguration as FC uplink ports.
- 12. Click Finish.
- 13. Click OK.
- 14. The Cisco UCS Manger GUI will close as the primary Fabric Interconnects reboots.
- **15.** Upon successful reboot, open a Web browser and navigate to the Cisco UCS 6248 Fabric Interconnects cluster address.
- 16. When prompted, enter admin as username and enter the administrative password.

#### **Modifying Chassis Discovery Policy**

This section provide details for modifying the chassis discovery policy, as the base architecture includes two uplinks from each Fabric Extender installed in the Cisco UCS chassis.

If the workload on the cloud is expected to be network centric, you may want to provide more bandwidth for the B200 M3 Blade Servers. Increasing the number of links between Fabric Extenders (IOM) on UCS Chassis and Fabric Interconnects would reduce bandwidth oversubscription. Change the number of links in the "Chassis Discovery Policy" under the equipment to match physical number of links. Ideally, the chassis discovery policy should be modified before configuring server ports. If you add or remove links between Fabric Interconnects and Fabric Extender after a chassis is discovered, you need to "Acknowledge chassis".



Acknowledging chassis will not reboot the servers in a chassis.

To modify the chassis discovery policy, login to the Cisco UCS Manager and follow these steps:

- 1. Click the **Equipment** tab in the left pane.
- 2. In the right pane, click the Policies tab.
- 3. Under Global Policies, change the Chassis Discovery Policy to 2-link.
- 4. Click Save Changes.

#### **Configuring Port Channels**

To configure the port channels follow these steps:

- 1. Click the **Equipment** tab in the left pane.
- 2. Select Fabric Interconnects A.
- 3. In the right pane, under Actions click the LAN UpLinks Manager tab.

- 4. Click Create Port Channel then Select Fabric A.
- 5. Specific ID <101> and Name <Tenant1CloudVPCNetworkA>.
- 6. On Add Ports, click **Ports** number <5> and <6>.
- 7. Click Finish.
- 8. By Default Port Channel < Tenant1CloudVPCNetworkB> is disabled, click Enable.
- 9. Click Yes as the warning message display asking to <Enable / Disable> on Fabric.
- **10.** Select Fabric Interconnects B.
- 11. In the right pane, under Actions click the LAN UpLinks Manager tab.
- 12. Right-click Create Port Channel then select Fabric A.
- 13. Specific ID <102> and Name <Tenant1CloudVPCNetworkB>.
- 14. On Add Ports click **Ports** number <5> and <6>.
- 15. Click Finish.
- 16. By Default Port Channel < Tenant1CloudVPCNetworkB> is disabled, click Enable.
- 17. Click Yes as the warning message displays <Enable / Disable> on Fabric B.



I

When configuring the Cisco Nexus 5548UP with vPCs, ensure that the status of all vPCs is "Up" for connected Ethernet ports.

Port Channel Status on Cisco Nexus 5548UP command output:

```
N5548-Switch-A(config-if) # sh vpc brief
Legend:
             (*) - local vPC is down, forwarding via vPC peer-link
vPC domain id
                        : 100
Peer status
                        : peer adjacency formed ok
vPC keep-alive status
                        : peer is alive
Configuration consistency status: success
Per-vlan consistency status : success
Type-2 consistency status
                         : success
Type-2 consistency reason
                         : QoSMgr Qos configuration incompatible
vPC role
                         : primary
Number of vPCs configured
                         : 2
Peer Gateway
                        : Disabled
Dual-active excluded VLANs
                        : -
Graceful Consistency Check
                        : Enabled
vPC Peer-link status
 _____
                     _____
id
   Port Status Active vlans
_ _
    ____
         _____ ____
   Po100 up
1
              1,192-195,602-603,607,20
vPC status
     _____
id Port Status Consistency Reason
                                                  Active vlans
_____ ____
101 Po101 up success success
                                       1,602-603,1000-1001,192-193,20
          up success success
up success success
up success success
                                          1,602-603,1000-1001,192-193,20
102
     Po102
                   success success
                                            1,192-193,200-300
103
     Po103
104
     Po104
                                             1,192-193,200-300
N5548-Switch-B(config-if) # sh vpc brief
Legend:
            (*) - local vPC is down, forwarding via vPC peer-link
vPC domain id
                         : 100
Peer status
                         : peer adjacency formed ok
```

```
: peer is alive
vPC keep-alive status
Configuration consistency status: success
Per-vlan consistency status : success
Type-2 consistency status : success
Type-2 consistency reason : QoSMgr Qos configuration incompatible
vPC role
                                      : primary
vPC role : p
Number of vPCs configured : 2
                                      : Disabled
Peer Gateway

      Dual-active excluded VLANs
      : -

      Graceful Consistency Check
      : Enabled

vPC Peer-link status
_____
id Port Status Active vlans
      ____
             _____
1 Po100 up 1,192-195,602-603,607,20
vPC status
_____
id
        Port
                     Status Consistency Reason
                                                                                Active vlans
_____ _____

        101
        Po101
        up
        success
        success
        1,1000-10001,602-603,192-193,20

        102
        Po102
        up
        success
        success
        1,1000-10001,602-603,192-193,20

        103
        Po103
        up
        success
        success
        1,192-193,200,300

        104
        Po104
        up
        success
        success
        1,192-193,200,300
```

# **Creating the Uplink Ethernet Ports**

LAN traffic enters and departs the Cisco UCS system on the Fabric Interconnects via the use of uplink ports. There are different types of uplink ports and here the uplink port channels are configured to connect to the NetApp storage.

To create and configure the necessary uplink port channels in the Cisco UCS environment login to the Cisco UCS Manager and follow these steps:

### **Fabric Interconnects A**

1. Click the LAN tab in the left pane.



Two Port Channels are created, one from Fabric A to both the Cisco Nexus 5548 switches, and one from Fabric B to both the Cisco Nexus 5548 switches.

- 2. Under LAN Cloud, expand the Fabric A tree.
- 3. In the right pane under General tab click Create Port Channel.



#### Figure 10 Creating Uplink Port Channels

- 4. Enter 101 as the unique ID of the Port Channel.
- 5. Enter Tenant Network A as the name of the Port Channel.
- 6. Click Next.

ſ

😧 🍥 💷 New 👻 🖉 Options 🛛 🚱 🚹 Pending Activities 🛛 🗿 Exit	
>> 🗐 LAN + 🙆 LAN Cloud + 🚥 Fabric A	
General VLANs Uplink Eth Interfaces Port Channels Events	
Actions Create VLANs Create Port Channel Unified Computing System Manager	×
Create Port Channel Set Port Channel Name	•
1. VSEt Port Channel Name         2. Add Ports         ID: 101         Nome: TenantNetworkA]	Cancel
	Create Value     Lukue     Luku

## Figure 11 Naming the Port Channel

7. Select the port with slot ID: 1 and port: 5, and the port with slot ID:1 and port 6, from the Ports list.

1

8. Click >> to add the ports to the Port Channel.

A Cisco Unified Computing System Manager - TM				_				_
Fault Summary	🕒 🍥 🗉 New - 🖓 Options 🛛 🌖	2 1 A Pending Activities	0 Exit					
🛛 🛇 🔻 🛆 🛆			-					
0 42 3 18	>> = LAN + 🕜 LAN Cloud + 🔤 Fabric A							
Equipment Servers LAN SAN VM Admin	General VLANS Uplink Eth Interfaces	Port Channels Events						
Filter: All	Actions	Properties						
• •	📥 Create Port Channel							×
E-= LAN								
E Clud	Unified C	Computing	System N	lan	ader			
						_		_
Uplink Eth Interfaces	Create Port Channel	Add Ports						0
VLAN Optimization Sets								
VLANs	1. V Set Port Channel Name							
Eabric B     Gos System Class	2. √ <u>Add Ports</u>	Ports						_
E = IAN Pin Groups					Ports in the port ch			
		Slot ID Port	MAC 🐺		Slot ID	Port	MAC	
VLAN Groups		1 1	54:7F:EE:98:B		1	5	54:7F:EE:98:BF:6C 54:7F:EE:98:BF:6D	
Herein VLANs     Herein VLANs     Herein VLANs		1 3	54:7F:EE:98:B		1	P	54:7F:EE:90:BF:0D	_
E-I Internal LAN		1 4	54:7F:EE:98:B					
🗄 🚽 Internal Fabric A		1 7	54:7F:EE:98:B					
Internal Fabric B      S     Threshold Policies		1 8	54:7F:EE:98:B					
Inreshold Policies     Policies		1 9	54:7F:EE:98:B					
		1 10		>>				
E-O LAN Cloud		1 11	54:7F:EE:98:B	<<				
Threshold Policies		1 12	54:7F:EE:98:B					
⊕-♠ root     □-♠ Pools		1 13	54:7F:EE:98:B					
E & root		1 15	54:7F:EE:98:B					
IP Pools		1 16	54:7F:EE:98:B					
⊕- IIII MAC Pools ⊕- 🎎 Sub-Organizations		1 17	54:7F:EE:98:B					
Traffic Monitoring Sessions		1 18	54:7F:EE:98:B					
		1 19	54:7F:EE:98:B					
		1 20	54:7F:EE:98:B					
		1 21	54:7F:EE:98:B 💌					<b>_</b>
						< Prev Nex	xt > Finish	Cancel
II								

#### Figure 12 Selecting and Adding the Ports

- 9. Click **Finish** to create the Port Channel.
- 10. Check the Show navigator for Port-Channel 101 (Fabric A) checkbox.
- 11. Click OK.

ſ

- 12. In Actions area, select Enable Port Channel.
- **13.** In the pop-up box, click **Yes**, then click **OK** to enable port-channel.



Enabling the Port Channel



- 14. Wait until the overall status of the Port Channel is Up.
- 15. Click OK to close the navigator.



#### Figure 14 Verifying the Port Channel Status

#### **Fabric Interconnects B**

I

1. Click the LAN tab in the left pane.



Two Port Channels are created, one from Fabric A to both the Cisco Nexus 5548 switches and other from Fabric B to both the Cisco Nexus 5548 switches.

- 2. Under LAN Cloud, expand the Fabric B tree.
- 3. In the right pane under General tab click Create Port Channel.



#### Figure 15 Creating the Port Channel

- 4. Enter 102 as the unique ID of the Port Channel.
- 5. Enter Tenant NetworkB as the name of the Port Channel.
- 6. Click Next.



#### Figure 16 Setting the Port Channel ID and Name

- 7. Select the port with slot ID: 1 and port: 5, and the port with slot ID: 1 and port 6, from the Ports list.
- 8. Click >> to add the ports to the Port Channel.

Figure 17 Selecting and Adding Ports

ſ

Cisco Unified Computing System Manager - TMI		
Fault Summary	🚱 🏐 😐 New 📲 🙀 Options 🛛 🌾	😧 🚯 🔝 Pending Activities 🛛 🔟 Exit
🛛 🛛 🗸 🖉		
0 42 3 10	>> 🗐 LAN I 🙆 LAN Cloud I 🚥 Fabric	k B
Equipment Servers LAN SAN VM Admin	General VLANS Uplink Eth Interfaces	Port Channels Events
Filter: Al	Actions	Properties
	Create Port Channel	10, 0
😑 🕘 LAN Cloud	Unified (	Computing System Manager
E- E- Fabric A		comparing eyetem manager
Filmer Fabric B     GoS System Class		Add Ports
E IAN Pin Groups	Create Port Channel	Add Folts
B→ M Threshold Policies	1. √Set Port Channel Name	
	2. ✓ Add Ports	
E = VLANS		Ports Ports In the port channel
Applances     Internal LAN		Slot ID Port MAC (74) Slot ID Port MAC (74
		1 1 54:7F:EE:A1:0 1 5 54:7F:EE:A1:0F:EC
E - Internal Fabric B		1 2 54:7F:EE:A1:0 1 6 54:7F:EE:A1:0F:ED
Image: Threshold Policies		1 3 54:7F:EE:A1:0
E- S Policies		1 4 54:7F:EE:A1:0
Appliances		1 7 54:7F:EE:A1:0
E C LAN Cloud		1 8 54:2F:EE:A1:0
Inreshold Policies III - 100, root		1 9 54:7F:0E:A1:0
E- Pools		1 10 54:7F:EE:A1:0
E 📣 root		1 11 54:7F:EE:A1:0
() - 飜 IP Pools		1 12 54:7F:EE:A1:0
MAC Pools		1 13 54:27:EE:A1:0
⊕-▲ Sub-Organizations ⊕-☑ Traffic Monitoring Sessions		1 14 54:27:EE:A1:0
E- Minimit Traffic Monitoring Sessions		1 15 54:7F:EE:A1:0
		1 16 54:7F:EE:A1:0
		1 17 54:2F:EE:A1:0
		1 10 54:27:EE:A1:0
		1 19 54:7F:EE:A1:0 1 20 54:7F:EE:A1:0
		1 20 SH7PEEAL0 V
		Prev Next > Finish Cancel

- 9. Click Finish to create the Port Channel.
- 10. Check the Show navigator for Port-Channel 101 (Fabric A) check box.
- 11. Click **OK** to continue.
- 12. In the Actions area, select Enable Port Channel.
- 13. In the pop-up box, click Yes, and then click OK.

#### Figure 18 Enabling the Port Channel



15. Click **OK** to close the navigator.



#### Figure 19 Verifying the Port Channel Status

## **Enabling Jumbo Frames**

I

To set the Jumbo frames (9000-byte frame) for the defined Quality of Service classes in the Cisco UCS Fabric through the Cisco UCS Manager, follow these steps:

- 1. Click the LAN tab in the left pane.
- 2. Choose LAN Cloud > QoS System Class.
- 3. In the right pane, click the General tab.
- 4. Type 9000 in the MTU boxes for the Platinum, Gold, Silver, and Bronze priority value.
- 5. Click Save Changes.
- 6. Click **OK** to continue.

## **Enabling QoS on Cisco UCS 6248 Fabric Interconnects**

In this section the Quality of Service (QoS) Policies-Platinum, Gold, Silver, Bronze, and Fibre Channel, will be created and enabled on the Cisco UCS Fabric in the solution design.

To enable the previously defined Quality of Service Policies on the Cisco UCS Fabric, login to the Cisco UCS Manager and follow these steps:

- 1. Choose LAN > Policies > Root >QoS Policies.
- 2. Right-click the QoS Policies.
- 3. Select Create QoS Policy.
- 4. Enter Platinum-Net-SLA as the QoS Policy name.
- 5. Change the Priority to Platinum. Retain the default values of Burst(Bytes)(10240), Rate (Kbps) (line-rate), and Host Control (None).
- 6. Click OK.

#### Figure 20 Naming and setting the PlatinumQoS Policy

A Cisco Unified Computing System Manager - TM	E-L21	
Fault Summary	🚱 🏐 New - 🛛 😧 Options 🛛 🚱 🕕 🕼 Pending Activities 🗍 💽 Exit	
0 38 3 19	>> 📑 LAN, 🔊 Policies, 🙀 root, 🔊 QoS Policies	
Equipment Servers LAN SAN VM Admin	QoS Policies	
Filter: All	🔍 Filter 🖨 Export 😸 Print	
		Name
• •	🕼 QOS Policy Platinum-Net-SLA	
E⊒ LAN È⊘ LAN Cloud	🗼 Create QoS Policy	X
	Create O.O.B. Key	0
🕂 🚥 Fabric B	Create QoS Policy	•
Qo5 System Class		
LAN Pin Groups		
	Name: Platinum-Net-SLA	
VLAN Groups	Egress	
ULANs	Priority: Platinum	
⊕-⊖ Appliances ⊟-⊒ Internal LAN	Burst(Bytes): 10240	
	Rate(Kbps): line-rate	
	Host Control:  None  Full	
⊡ ··· () Appliances		
Threshold Policies		
⊡		
🗐 Default vNIC Behavior		OK Cancel
Dynamic vNIC Connection Policies     S Flow Control Policies		
LH S Flow Control Policies		
🗄 🗐 Network Control Policies		
🔊 QoS Policies		
wNIC Templates ⊕-ஜ் Sub-Organizations		
Pools		
e root		
IP Pools		
MAC Pools		
⊕-A. Sub-Organizations ⊕-Ø Traffic Monitoring Sessions		
7. Right-click th	e OoS Policies.	

8. Select Create QoS Policy.

- 9. Enter Gold-Net-SLA as the QoS Policy name.
- **10.** Change the Priority to Gold. Retain the default values of Burst(Bytes) (10240), Rate(Kbps) (line-rate), and Host Control (None).
- 11. Click OK.

Figure 21 Naming and Setting the Gold QoS Policy

🚔 Cisco Unified Computing System Manager - TM	F-L21	
Fault Summary	🕒 🔘 🖬 New 🔹 🛃 Options 🛛 🚱 🚺 📥 Pending Activities 🛛 🔟 Exit	
	>>	
	- OoS Policies	
Equipment Servers LAN SAN VM Admin	A Filter - Export - Print	
Filter: All		Name
± =	Create QoS Policy	×
		0
E C LAN Cloud	Create QoS Policy	<b>W</b>
🕀 💼 Fabric A		
🕀 💼 Fabric B		
🗈 🚍 LAN Pin Groups	Name: Gold-Net-SLA	
LAN Pin Group Marketing	Egress	
In a standard matrix and the standard matrix and t		
VLAN Groups	Priority: Gold	
	Burst(Bytes): 10240	
Appliances		
🖨 🚍 Internal LAN	Rate(Kbps): line-rate	
🗈 🖃 Internal Fabric A	Host Control:  None  Full	
Internal Fabric B		
⊞-     S Threshold Policies		
E S Policies		
E C LAN Cloud		
Threshold Policies	OK Car	ncel
Default vNIC Behavior		-
Derault vivic behavior     Solution Policies		
E S Flow Control Policies		
S LAN Connectivity Policies		
S Multicast Policies		
S Network Control Policies		
D- S QoS Policies		
S QOS Policy Platinum-Net-SLA		
VNIC Templates		
Pools		
E A root		
IP Pools		
MAC Pools		
🕀 💓 Traffic Monitoring Sessions		

- 12. Right-click the QoS Policies.
- 13. Select Create QoS policy.
- 14. Enter Silver-Net-SLA as the QoS policy name.
- **15.** Change the Priority to Silver. Retain the default values of Burst(Bytes) (10240), Rate(Kbps) (line-rate), and Host Control (None).
- 16. Click OK.

I

\land Cisco Unified Computing System Manager - TME-	L21
Fault Summary	
	😋 🍥 🗉 New 👻 🛃 Options 🕜 🕕 🦾 Pending Activities 🚺 Exit
	>> 🚍 LAN 🕨 写 Policies 👌 🎄 root 🔸 🗐 QoS Policies
0 36 3 20	
Equipment Servers LAN SAN VM Admin	
Filter: All	🕰 Filter 🗢 Export 😸 Print
• •	🗼 Create QoS Policy
En Cloud	Create QoS Policy
⊕⊶ee Fabric A	
QoS System Class	
🖃 🚍 LAN Pin Groups	Name: Silver-Net-SLA
LAN Pin Group Marketing	Egress
VLAN Groups	Priority: Best Effort
⊕ Appliances	Burst(Bytes): 10240
🕂 🛁 Internal LAN	Rate(Kbps): line-rate
🕀 🗝 🔲 Internal Fabric A	Host Control:  O None  Full
⊕	
⊡… ⑤ Threshold Policies	
🛱 💭 LAN Cloud	
🖻 🦗 root Default vNIC Behavior	
E Flow Control Policies	
🗐 LAN Connectivity Policies	
🕀 🖉 Multicast Policies	
⊕ 🔊 Network Control Policies ⊖ 🔊 QoS Policies	
SQOS Policy Gold-Net-SLA	
S QOS Policy Platinum-Net-SLA	
🗈 ᠫ Threshold Policies	
WIC Templates	
⊡…∰ Sub-Organizations □	
Dep III Pools	
⊕-☆ Sub-Organizations ⊕-☑ Traffic Monitoring Sessions	
<b>17</b> . Right-click the <b>Oos</b>	Deligion

Naming and Setting the Silver QoS Policy Figure 22

1

- **18.** Select Create QoS Policy.
- **19.** Enter FC Net-SLA as the QoS Policy name.
- 20. Change the Priority to FC. Retain the default values of Burst(Bytes) (10240), Rate(Kbps) (line-rate), and Host Control (None).
- 21. Click OK.

A Cisco Unified Computing System Manager - TME-L21	
Fault Summary	<ul> <li>Section Section Pending Activities</li> <li>Exit</li> <li>&gt; ■ LAN * Section Policies * A root * Section QoS Policies</li> </ul>
2 43 8 40 Equipment Servers LAN SAN VM Admin Filter: All Filter: All LAN Cloud Filter: All LAN Cloud Filter: All LAN Cloud Filter: All Cos System Class Filter: All Filter: All Fi	Solicies          QoS Policies       Print         Create QoS Policy         Create QoS Policy         Rame:       FC-Net-SLA         Egress         Priority:         Frate(kbps):         Ine-rate         Host Control:

Figure 23 Naming and Setting the FC QoS Policy

Figure 24 shows Cisco UCS QoS system class and QoS policy configurations defined for application on static and dynamic vNICs for accessing a Microsoft SQL Server iSCSI network.



Γ

Fault Summary 2 Equipment Servers LAN SAN	7 7 VM Admin	20	G     Image: New ▼     Image: Options     Image: Options     Image: Options     Image: Options     Image: Options       >> =     LAN ▷     LAN Cloud ▷     Image: Options     Image: Options     Image: Options       General     Events     FSM							
Filter: All	•	•	Priority	Enabled	Co5	Packet Drop	Weight	Weight (	%) MTU	Multicast Optimized
• •			Platinum		5		10	▼ 22	9000	<b>•</b>
E IAN			Gold		4	<b>V</b>	9	<b>~</b> 20	9000	<b>•</b>
E Cloud			Silver	•	2	<b>V</b>	8	<b>▼</b> 18	9000	<b>•</b>
🕂 🚥 Fabric B			Bronze	•	1	V	7	<b>▼</b> 15	normal	•
			Best Effort		Any		5	<b>-</b> 11	normal	<b>•</b>
EXAMPLE GOODS			Fibre Channel		3		5	▼ 14	fc	▼ N/A

## **QoS Configurations for Cisco Nexus 5548UP Switches**

To apply QoS across the entire system, from Cisco UCS to the upstream switches (Cisco Nexus 5548UP Switches), it is essential to configure similar QoS class and policy types with the right class-of-service (CoS) values that correspond to the Cisco UCS QoS classes.

To set the QoS configurations for all the service classes, follow these steps on each Nexus 5548UP from the system console:

- 1. From the global configuration mode, type spanning-tree port type network default, to ensure that by default, the ports are considered as network ports with regard to spanning-tree.
- **2.** Type spanning-tree port type edge bpduguard default to enable bpduguard on all edge ports by default.
- 3. Type spanning-tree port type edge bpdufilter default to enable bpdufilter on all edge ports by default.

I

4. Type class-map type qos match-any class -- Platinum/Gold/Silver/Bronze/FCoE.

#### Platinum class:

- a. Type description Platinum Class which is mapped to Platinum-Network-SLA.
- **b.** Type match cos 5.
- c. Type exit.

#### Gold class:

- a. Type description Gold Class which is mapped to Gold-Network-SLA.
- **b.** Type match cos 4.
- c. Type exit.

#### Silver class:

- a. Type description Gold Class which is mapped to Silver-Network-SLA.
- **b.** Type match cos 2.
- c. Type exit.

#### FCoE class:

- **a.** Type match cos 3.
- **b**. Type exit.
- 5. Type policy-map type qos system\_qos\_policy.

#### Platinum class:

- a. Type class type qos class-Platinum.
- **b.** Type set qos-group 5.
- c. Type exit.

#### Gold class:

- **a**. Type class type qos class-Gold.
- **b.** Type set qos-group 4.
- **c**. Type exit.

#### Silver class:

- a. Type class type qos class-Silver.
- **b.** Type set qos-group 2.

**c**. Type exit.

## FCoE class:

- **a**. Type class type qos class-fcoe.
- **b.** Type set qos-group 1
- c. Type exit
- 6. Type class-map type queuing match-all class-

## Platinum class:

- a. Type class-map type queuing match-all class-Platinum.
- b. Type description Platinum Class which is mapped to Platinum-Network-SLA.
- **c.** Type match qos-group 5.
- d. Type exit.

#### Gold class:

- a. Type class-map type queuing match-all class-Gold.
- **b.** Type description Gold Class which is mapped to Gold-Network-SLA.
- **c.** Type match qos-group 4.
- d. Type exit

#### Silver class:

- a. Type class-map type queuing match-all class-Silver.
- **b.** Type description Gold Class which is mapped to Silver-Network-SLA.
- **c.** Type match qos-group 2.
- d. Type exit.

#### FCoE class:

- a. Type class-map type queuing match-all class-fcoe.
- **b.** Type match qos-group 1.
- **c.** Type exit.
- 7. Type policy-map type queuing system\_q\_in\_policy.

#### Platinum class:

- **a**. Type class type qos class-Platinum.
- **b.** Type bandwidth percent 30.
- c. Type exit

### Gold class:

- **a**. Type class type qos class-Gold.
- **b.** Type set bandwidth percent 20.
- c. Type exit

### Silver class:

- **a**. Type class type qos class-Silver.
- **b.** Type set bandwidth percent 15.
- c. Type exit

ſ

#### **Default class:**

- a. Type class type qos class-default.
- **b.** Type set bandwidth percent 1.
- c. Type exit

#### FCoE class:

- a. Type class type qos class-FCoE.
- **b.** Type set bandwidth percent 34.
- c. Type exit
- d. Type exit
- **8**. Type policy-map type queuing system\_q\_out\_policy.

#### Platinum class:

- a. Type class type qos class-Platinum.
- **b.** Type bandwidth percent 30.
- **c**. Type exit

#### Gold class:

- a. Type class type qos class-Gold.
- **b.** Type set bandwidth percent 20.
- c. Type exit

## Silver class:

- a. Type class type qos class-Silver.
- **b.** Type set bandwidth percent 15.
- c. Type exit

#### **Default class:**

- a. Type class type qos class-default.
- **b.** Type set bandwidth percent 1.
- c. Type exit

## FCoE class:

- **a**. Type class type qos class-fcoe.
- **b.** Type set bandwidth percent 34.
- **c**. Type exit
- d. Type exit.
- 9. Type class-map type network-qos class-

#### **Platinum class:**

- **a**. Type class-map type network-qos class-Platinum.
- **b.** Type description Platinum Class which is mapped to Platinum-Network-SLA.

- **c.** Type match qos-group 5.
- d. Type exit.

#### Gold class:

FlexPod Data Center with VMware vSphere 5.1, and Citrix CloudPlatform 4.2.1

- a. Type class-map type network-qos class-Gold.
- **b.** Type description Gold Class which is mapped to Gold-Network-SLA.
- **c.** Type match qos-group 4.
- d. Type exit.

#### Silver class:

- a. Type class-map type network-qos class-Silver.
- b. Type description Platinum Class which is mapped to Silver-Network-SLA.
- **c.** Type match qos-group 2.
- d. Type exit.

## FCoE class:

- **a**. Type class-map type network-qos class-fcoe.
- **b.** Type match qos-group 1.
- **c**. Type exit.
- **10.** Type policy-map type network-qos system\_nq\_policy.

#### Platinum class:

- **a**. Type class type qos class-Platinum.
- **b.** Type set.
- c. Type set cos 5.
- d. Type mtu 9000.
- e. Type exit.

### Gold class:

- a. Type class type qos class-Gold.
- **b.** Type set.
- c. Type set cos 4.
- d. Type mtu 9000.
- e. Type exit.

### Silver class:

- a. Type class type qos class-Silver.
- **b.** Type set.
- **c.** Type set cos 2.
- d. Type mtu 9000.
- e. Type exit.

## FCoE class:

- **a**. Type class type qos class-fcoe.
- **b.** Type set.

I

- c. Type set cos 1.
- d. Type mtu 9000.
- e. Type pause no-drop.

f. Type exit.

#### **Default class:**

- **a.** Type class type qos class-defaut.
- **b.** Type set.
- **c.** Type mtu 9000.
- d. Type exit.
- **11.** Type system qos.
- 12. Type service-policy type qos input system\_qos\_policy.
- **13.** Type service-policy type queuing input system\_q\_in\_policy.
- 14. Type service-policy type queuing output system\_q\_out\_policy.
- **15.** Type service-policy type network-qos system\_nq\_policy.
- **16.** Type exit.
- **17.** Type interface port-channel 103.
- **18.** Type service-policy type qos input system\_qos\_policy.
- **19.** Type service-policy type queuing input system\_q\_in\_policy.
- **20.** Type service-policy type queuing output system\_q\_out\_policy.
- **21**. Type interface port-channel 104.
- 22. Type service-policy type qos input system\_qos\_policy.
- **23.** Type service-policy type queuing input system\_q\_in\_policy.
- 24. Type service-policy type queuing output system\_q\_out\_policy.
- **25.** Type copy run start.



Configure the same QoS Policy on Nexus 5548UP Switch B which is part of VPC cluster, repeat steps 1-25 on Nexus 5548UP Switch B.

The commands enumerated below show the QoS configuration output at both Cisco Nexus 5548UP Switch A and B.

```
sh class-map type queuing
  Type queuing class-maps
  _____
  class-map type queuing class-Gold
     match gos-group 4
class-map type queuing class-fcoe
     match qos-group 1
     class-map type queuing class-Silver
     match qos-group 2
    class-map type queuing class-default
     match qos-group 0
    class-map type queuing class-Platinum
     match qos-group 5
    class-map type queuing class-all-flood
     match gos-group 2
    class-map type queuing class-ip-multicast
     match qos-group 2
N5548-L21-A(config) # sh class-map type network-qos
  Type network-gos class-maps
```

\_\_\_\_\_ class-map type network-qos class-Gold match gos-group 4 class-map type network-qos class-fcoe match qos-group 1 class-map type network-gos class-Silver match qos-group 2 class-map type network-qos class-default match qos-group 0 class-map type network-qos class-Platinum match qos-group 5 class-map type network-gos class-all-flood match qos-group 2 class-map type network-qos class-ip-multicast match qos-group 2 N5548-L21-A(config) # sh class-map type queuing Type queuing class-maps \_\_\_\_\_ class-map type queuing class-Gold match qos-group 4 class-map type queuing class-fcoe match gos-group 1 class-map type queuing class-default match qos-group 0 class-map type queuing class-Platinum match qos-group 5 class-map type queuing class-all-flood match gos-group 2 class-map type queuing class-ip-multicast match qos-group 2 sh policy-map type queuing Type queuing policy-maps \_\_\_\_\_ policy-map type queuing default-in-policy class type queuing class-default bandwidth percent 100 policy-map type queuing system\_qos\_policy class type queuing class-Silver priority class type queuing class-default bandwidth percent 100 policy-map type queuing default-out-policy class type queuing class-default bandwidth percent 100 policy-map type queuing system\_q\_in\_policy class type queuing class-Platinum bandwidth percent 30 class type queuing class-Gold bandwidth percent 20 class type queuing class-Silver bandwidth percent 15 class type queuing class-fcoe bandwidth percent 34 class type queuing class-default bandwidth percent 1 policy-map type queuing system\_q\_out\_policy class type queuing class-Platinum bandwidth percent 30 class type queuing class-Gold bandwidth percent 20 class type queuing class-Silver bandwidth percent 15 class type queuing class-fcoe bandwidth percent 34

```
class type queuing class-default
     bandwidth percent 1
  policy-map type queuing fcoe-default-in-policy
   class type queuing class-fcoe
     bandwidth percent 50
    class type queuing class-default
     bandwidth percent 50
  policy-map type queuing fcoe-default-out-policy
    class type queuing class-fcoe
     bandwidth percent 50
    class type queuing class-default
     bandwidth percent 50
sh policy-map type qos
Type qos policy-maps
  ------
policy-map type qos default-in-policy
    class type qos class-default
     set qos-group 0
  policy-map type qos system_qos_policy
   class type qos class-Platinum
     set qos-group 5
    class type qos class_fcoe
     set qos-group 3
    class type qos class-default
     set qos-group 0
  policy-map type qos fcoe-default-in-policy
    class type gos class-fcoe
      set qos-group 1
    class type qos class-default
      set qos-group 0
sh policy-map type network-qos
Type network-gos policy-maps
  policy-map type network-qos system_nq_policy
    class type network-qos class-Platinum
    set cos 5
     mtu 9000
    class type network-gos class-fcoe
   mtu 2158
     set cos 3
     pause no-drop
    class type network-gos class-Gold
     mtu 9000
    class type network-qos class-Silver
    mtu 9000
    class type network-gos class-default
   mtu 1500
  multicast-optimize
  policy-map type network-qos default-nq-policy
    class type network-qos class-default
   mtu 9000
     multicast-optimize
  policy-map type network-qos fcoe-default-nq-policy
   class type network-qos class-fcoe
   pause no-drop
     mtu 2158
    class type network-qos class-default
     mtu 1500
     multicast-optimize
```

## **NetApp Storage QoS Configuration**



On the Cisco Nexus 5548UP upstream switch, ensure that the correct QoS class and MTU value with policy types are applied to the Port Channel Ports (eth19 and eth 20). Port channels are connected to the NetApp FAS3270HA (Controllers Flexpod A and B), 10 Gigabit Ethernet interfaces (e1c and e1d), to allow network packets to be tagged from Nexus 5548 fabric. This is done because NetApp Storage will not tag any network packets with MTU and QoS values.

Following commands shows how to configure the CoS on Nexus 5548 for untagged packets originating from storage on the Port Channels.

## CLI commands on Cisco Nexus 5548UP Application1

```
Switch# Configure Terminal
Switch(Conf)# Interface port channel 105
Switch(Conf-if)#untagged cos 2
Switch# sh policy-map type qos
Switch# Configure Terminal
Switch(Conf)# Interface port channel 106
Switch(Conf-if)#untagged cos 2
Switch# sh policy-map type qos
```

## CLI commands on Cisco Nexus 5548UP Application2

```
Switch# Configure Terminal
Switch(Conf)# Interface port channel 105
Switch(Conf-if)#untagged cos 2
Switch# sh policy-map type qos
Switch# Configure Terminal
Switch(Conf)# Interface port channel 106
Switch(Conf-if)#untagged cos 2
Switch# sh policy-map type qos
Make sure that the MTIL is set to 9000 and that
```

Make sure that the MTU is set to 9000 and that jumbo frames are enabled on the Cisco UCS static and dynamic vNICs, and on the upstream Cisco Nexus 5548UP Switches.

## **Configuring VLANs on Cisco UCS 6248UP Fabric Interconnects**

In multitenant cloud environment, isolation of network data access is a critical requirement to adhere to security measure. Cisco UCS allows creation of logical VLANs that can be dedicated to, and accessed by a specific organization unit.

To configure the necessary dedicated VLANs to an organization unit in Cisco UCS, follow these steps:

- 1. Click the LAN tab in the right pane, click Global Policies.
- 2. In the right pane under Org Permissions area, click Enabled radio button.
- 3. Click Save Changes.



Figure 25 Configuring the VLANS to the Organization Unit

- 4. Click the LAN tab in the left pane.
- 5. Select LAN Cloud.
- 6. Right-click VLANs. (Creating Management VLAN)
- 7. Select Create VLANs.
- 8. Enter Management-VLAN in the Name field.



This VLAN will be used for management traffic.

- 9. Under Multicast Policy Name select default setting.
- 10. Keep the Common/Global option selected for the scope of the VLAN.
- 11. Enter the VLAN ID defined for the management VLAN. Retain the sharing type as none.
- 12. In Permitted Orgs for VLAN(s) select Root & TenantA Organization Unit.
- 13. Click OK.
| <u>A</u>   | Cisco Unified Computing System Manager - TME-L21      |
|--|---|
| 4 13 9 55   Equipment Servers LAN SAN VM Admin   Filter: All   Filter:   All   Filter: All Creation: VLAN Cloud Filter: <th>Cisco Unified Computing System Manager - TME-L21  New</th> | Cisco Unified Computing System Manager - TME-L21  New |

#### Figure 26 Defining the Management VLAN Properties

- **14.** Right-click **VLANs**.(Creating the BareMetal-PXE VLAN)
- 15. Select Create VLANs.
- **16**. Enter BareMetal-VLAN in the Name field.

# <u>Note</u>

ſ

This VLAN will be used for the BareMetal host PXE Boot traffic.

- 17. Under Multicast Policy Name select default setting.
- 18. Keep the Common/Global option selected for the scope of the VLAN.
- **19.** Enter the VLAN ID for the BareMetal-PXE VLAN.
- 20. In Permitted Orgs for VLAN(s) select root organization Unit.
- **21.** Click **OK**.

2	Create VLANs
Create VLAN	٧s
VLAN Name/Prefix:	BareMetal-VLAN20
Multicast Policy Name:	Create Multicast Policy
(	Common/Global O Fabric A O Fabric B O Both Fabrics Configured Differen
You are creating globa	al VLANs that map to the same VLAN IDs in all available fabrics.
Enter the range of V	'LAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")
VLAN IDs: 20	
	one 🔿 Primary 🔿 Isolated
brianing type.	
A service profile's acce permit and group perm	ess to a VLAN is determined by the service profile's organization and the VLAN
Permitted Orgs fo	-
E- 🖌 🎄 root	
🦾 🗹 🎪 Tena	antA

1

Figure 27 Defining BareMetal-PXE VLAN Properties

- 22. Right-click VLANs. (Creating the guest VLAN)
- 23. Select Create VLANs.
- 24. Enter guest-VLAN in the Name field.



This VLAN will be used for the guest VLAN traffic.

- 25. Under Multicast Policy Name select Default setting.
- 26. Keep the Common/Global option selected for the scope of the VLAN.
- 27. Enter the VLAN ID for the guest VLAN.
- 28. In Permitted Orgs for VLAN(s) select Root & TenantA Organization Unit.
- 29. Click OK.

<u>A</u>	Cisco Unified Computing System Manager - TME-L21
Fault Summary	🔰 😋 🏐 🗉 New 🚽 🏹 Options 🕜 🕕 🤷 Pending Activities 🔟 Exit
	>> = LAN > () LAN Cloud > = VLANs
4 13 9 55	>> = LAN , CLAN Cloud , = VLANS
Equipment Servers LAN SAN VM Admin	
Filter: All	
	Create VLANs
LAN Cloud CLAN Cloud CLAN Fin Groups Cost System Class Cost System	VLAN Name/Prefix:       Guest-VLAN         Multicast Policy Name:       Image: Create Multicast Policy         Image: Create Multicast Policy       Image: Creat
30 Right-click VLANs (Cre	ating the quest $VI(\Delta N)$

#### Figure 28 Defining the guest VLAN Properties

- **30.** Right-click **VLANs**. (Creating the guest VLAN)
- 31. Select Create VLANs.
- **32**. Enter guest-VLAN-1000 in the Name field.

### Note

I

This VLAN will be used for the guest VLAN traffic.

- **33**. Under Multicast Policy Name select Default setting.
- 34. Keep the Common/Global option selected for the scope of the VLAN.
- **35**. Enter the VLAN ID for the guest VLAN.
- 36. In Permitted Orgs for VLAN(s) select Root & TenantA Organization Unit.
- 37. Click OK.

<u>A</u>	Cisco Unified Computing System Manager - TME-L21
Fault Summary	🕒 🏐 🗳 New 🤟 🎦 Options 😢 🕕 📥 Pending Activities 🔟 Exit
4 14 9 55	>> 🗐 LAN + 🔿 LAN Cloud + 🗐 VLANs
Equipment Servers LAN SAN VM Admin	VLANs
	🕰 Filter 👄 Export 🎃 Print
	Create VLANs
<ul> <li>AN</li> <li>LAN Cloud</li> <li>Fabric A</li> <li>Goto System Class</li> <li>LAN Pin Groups</li> <li>VLAN Groups</li> <li>VLAN Groups</li> <li>VLANS</li> <li>Appliances</li> <li>Threshold Policies</li> <li>Policies</li> <li>Policies</li> <li>Policies</li> <li>Policies</li> <li>Traffic Monitoring Sessions</li> </ul>	Create VLANS
<b>38.</b> Right-click <b>VLANs</b> . (Creating t	he guest VLAN)

1

#### Figure 29 Defining the guest VLAN 1000 Properties

- **39.** Select Create VLANs.
- **40**. Enter guest-VLAN-1001 in the Name field.

## 

Note This VLAN will be used for the guest VLAN traffic.

- 41. Under Multicast Policy Name select Default setting.
- 42. Keep the Common/Global option selected for the scope of the VLAN.
- 43. Enter the VLAN ID for the guest VLAN.
- 44. In Permitted Orgs for VLAN(s) select Root & TenantA Organization Unit.
- 45. Click OK.

<b>A</b>	Cisco Unified Computing System Manager - TME-L21
Fault Summary	🖁 🕒 🗉 New 🚽 🏹 Options 😧 🚯 🦾 Pending Activities 🔟 Exit
♥         ▲         ▲           4         13         9         54	
Equipment Servers LAN SAN VM Admin	🔍 Filter 👄 Export 🎉 Print
Filter: All	Create VLANs
LAN CLAN Cloud CLAN Cloud Cass Cass Cass Cass Cass Cass Cass Cas	Create VLANS         VLAN Name/Prefix:       Guest-VLAN-1001         Multicast Policy Name:       Image: Contract of the set of th
	⊢ V A TenantA

#### Figure 30 Defining the guest VLAN 1001 Properties

- 46. Right-click VLANs. (Creating the NFS VLAN)
- **47**. Select Create VLANs.
- **48.** Enter NFS-VLAN in the Name field. This VLAN will be used for the Secondary Storage NFS VLAN traffic.
- 49. Under Multicast Policy Name select Default setting.
- **50.** Keep the Common/Global option selected for the scope of the VLAN.
- **51**. Enter the VLAN ID for the NFS VLAN.
- **52.** Keep the Common/Global option selected for the scope of the VLAN.
- 53. In Permitted Orgs for VLAN(s) select TenantA Organization Unit.
- 54. Click OK.

ſ

<u>A</u>	Cisco Unified Computing System Manager - TME-L21
Fault Summary	🕞 🍥 🗉 New 🤟 🎴 Options 😢 🕕 🔺 Pending Activities 🔟 Exit
S V 🛆 🔺	
4 13 9 55	>> = LAN + () LAN Cloud + = VLANs
Equipment Servers LAN SAN VM Admin	VLANS
Filter: All	A Filter = Export Print
	A Create VLANs
LAN LAN LAN Cloud Fabric A Fabric A LAN Pin Groups LAN Pin Groups LAN Pin Groups LAN Pin Groups LAN Groups LAN Groups LAN Fin Groups LAN Fin Groups LAN Groups Finternal LAN Finternal Fabric A Finternal Fabric A Finternal Fabric B Finternal Fabric B	VLAN Name/Prefix:       NFS-VLAN         Multicast Policy Name:       Image: Create Multicast Policy         Image: Common/Global       Fabric A       Fabric B         Both Fabrics       Common/Global       Fabric A         You are creating global VLANs that map to the same VLAN IDs in all available fabrics.         Enter the range of VLAN IDs.(e.g. "2009-2019", "29,35,40-45", "23", "23,34-45")         VLAN IDs:       193         Sharing Type:       None       Primary
	A service profile's access to a VLAN is determined by the service profile's organization and the VLAN permit and group permit settings.  Permitted Orgs for VLAN(s)  Permitted Orgs for VLAN(s)  TenantA  TenantA

1

#### Figure 31 Defining NFS VLAN Properties

- 55. Right-click VLANs.(Creating the vMotion VLAN)
- 56. Select Create VLANs.
- **57.** Enter vMotion-VLAN in the Name field. This VLAN will be used for the VM vMotion VLAN traffic.
- 58. Under Multicast Policy Name select Default setting.
- 59. Keep the Common/Global option selected for the scope of the VLAN.
- 60. Enter the VLAN ID for the vMotion VLAN.
- 61. In Permitted Orgs for VLAN(s) select TenantA Organization Unit.
- 62. Click OK.

LAN   E   E   Create VLANs      Create VLANs Create Multicast Policy VLAN Name/Prefix: vMotion-VLAN Multicast Policy Name: <not set=""> Create Multicast Policy VLAN Sources VLAN Sources VLAN Sources VLAN Sources Internal LAN Internal Fabric A For Policies VLAN IDs: nall available Enter the range of VLAN IDs. (e.g. "2009-2019", "29,35,40-45", "23", "23, "23, "23, "23, "23, "23, "</not>	nager - TME-L21
4       13       9       55         Equipment       Servers       LAN       SAN       VM Admin         Filter:       All       All       All         Image: Constraint of the state of	
Equipment Servers LAN   Filter: All     Filter: All     Filter: All     Filter: Export        Filter: Export        Filter: All     Filter: Export        Filter: Filter:        Filter: Filter:        Filter: Filter:        Filter: Filter:           Filter: Filter: <b>Create VLANs</b> <td></td>	
Equipment SaN VM     Filter: All     Filter: All     Image: Content of	
Filter: All     Image: Content of Conte	
LAN   E   E   Create VLANs      Create VLANs Create Multicast Policy VLAN Name/Prefix: vMotion-VLAN Multicast Policy Name: <not set=""> Create Multicast Policy VLAN Sources VLAN Sources VLAN Sources VLAN Sources Internal LAN Internal Fabric A For Policies VLAN IDs: nall available Enter the range of VLAN IDs. (e.g. "2009-2019", "29,35,40-45", "23", "23, "23, "23, "23, "23, "23, "</not>	
LAN Cloud     Create V LAN S     Create V LAN S     Create Multicast Policy     LAN Pin Groups     LAN Pin Groups     LAN Pin Groups     VLAN Name/Prefix: VMOtion-VLAN     Multicast Policy Name: <a )<="" href="https://www.statestatestatestatestatestatestatestat&lt;/td&gt;&lt;td&gt;Create VLANs&lt;/td&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;Traffic Monitoring Sessions      A service profile's access to a VLAN is determined by the service profile's or permit and group permit settings.      Permitted Orgs for VLAN(s)      Permitted Orgs for VLAN(s)      TenantA&lt;/td&gt;&lt;td&gt;oth Fabrics Configured Differently&lt;br&gt;ble fabrics.&lt;br&gt;23,34-45" td=""></a>	

#### Figure 32 Defining vMotion VLAN Properties

### **Storage Configurations**

ſ

This section details all the configurations and setup steps required to meet the Cisco storage design considerations. In this study we will create Virtual Logical SAN Networks (VSANs) for isolating multi-tenants storage data traffic and create FCoE Port Channel for link aggregation.

The following tasks are described in this section;

- Configure FCoE port
- Create VSAN
- Define VSAN and SAN port channel
- Configure FCoE Port channel on FI

### **Configuring FCoE Ports**

FCoE ports are ports on the 6200 series Fabric Interconnects that can be configured to carry Fibre Channel traffic over Ethernet. These ports are not reserved. They cannot be used by a Cisco UCS domain until you configure them. To modify an unconfigured Ethernet port into a FCoE uplink port in the Cisco UCS environment, follow these steps:

- 1. In the Cisco UCS Manager GUI, click the **Equipment** tab in the left pane. (Configure FCoE Ports on FI A)
- 2. Select Fabric Interconnects A.
- **3.** Select Ethernet Ports.
- 4. Select Port 31.
- 5. In the right pane, click the General tab.
- 6. Select Reconfigure.

#### Figure 33 Reconfigure ethernet port to FCoE Uplink port



7. Select Configure as FCoE Uplink Port



#### Figure 34 Configure as FCoE Uplink port

ſ



#### Figure 35 Configure FCoE Uplink port

- 9. Click OK.
- 10. The Cisco UCS Manger GUI will close as the primary Fabric Interconnects reboots.

11. Click OK.



#### Figure 36 Configure FCoE Uplink port

- 12. Repeat the same steps on Port 32 to configure FCoE Ports on FI A.
- 13. Repeat the same steps on Port 31 and 32 to configure FCoE Ports on FI Creating VSAN.

VSANs help you create multiple logical SANs over a common physical infrastructure. Each VSAN can contain up to 239 switches and has an independent address space that allows identical Fibre Channel IDs (FC IDs) to be used simultaneously in different VSANs. Any application-specific parameters can be configured for a VSAN before creating the VSAN. To create the VSAN, login to the Cisco UCS Manager, and follow these steps:

### **Fabric Interconnects A**

I

- 1. Click the SAN tab in the left pane.
- 2. Expand the SAN Cloud tree.
- 3. Click Fabric A.
- 4. On right pane, under General tab click on Create VSAN.

	Figure 37	Create VSAN	
Fault Summary	20 LAN SAN VM Admin	▲ ▲ 9 55	Cisco Unified Computing System Manager - TME-L21
<ul> <li>→</li></ul>	Port Channels DE Port Channels ink FC Interfaces ink FCE Interfaces ANS a Groups ald Policies oud A A A AN default (1)	•	Image: Section Sect

1

- 5. Enter VSAN300 in the VSAN name field.
- 6. Keep the Disabled option selected for the Default Zoning.
- 7. Click Common/Global radio button.
- 8. Enter the VSAN ID 300.
- **9.** Enter the FCoE VLAN ID 300.
- 10. Click OK.

#### Cisco Unified Computing System Manager - TME-L21 Fault Summary 🔰 🤤 🌐 New 🚽 🋃 Options 🕜 🕕 🦾 Pending Activities 🔟 Exit V ⊗ Δ Δ 55 >> 🚍 SAN + 🙆 SAN Cloud + 💷 Fabric A + 🗮 VSANs 4 20 9 **VSANs** Equipment Servers LAN SAN VM Admin 💼 🖃 💐 Filter 👄 Export 🇞 Print Filter: All • Create VSAN ۸ • = E E SAN **Create VSAN** 🛓 🟉 SAN Cloud Fabric A FC Port Channels Name: VSAN300 FC Zoning Settings -I Uplink FCoE Interfaces E- E VSANs FC Zoning: $\odot$ Disabled $\bigcirc$ Enabled 🕖 🎟 Fabric B Do NOT enable local zoning if fabric interconnect is connected to an upstream FC/FCoE switch. 😑 SAN Pin Groups 🗄 🖅 🗊 Threshold Policies 🗉 🚍 VSANs Common/Global O Fabric A O Fabric B O Both Fabrics Configured Differently USAN default (1) 🟉 Storage Cloud You are creating a global VSAN that maps to the same VSAN ID in all available fabrics. A VLAN can be used to carry FCoE traffic and can be mapped to this VSAN. E - E Fabric A E - E Fabric B Enter the VSAN ID that maps to this VSAN. Enter the VLAN ID that maps to this VSAN. 🗄 🚍 VSANs 😑 VSAN default (1) VSAN ID: 300 FCoE VLAN: 300 S Policies - Ools 🗄 🧔 root 🗄 📈 Traffic Monitoring Sessions

#### Figure 38 Defining the Common/Global VSAN

#### **Fabric Interconnects B**

I

- 1. Click the SAN tab in the left pane. Expand the SAN Cloud tree.
- 2. Click Fabric A.
- 3. On Right Pane Under General tab click on Create VSAN

Δ	Cisco Unified Computing System Manager - TME-L21
Fault Summary	😂 🌑 🗳 New 🚽 🛃 Options 😢 🕕 Antiparticle Structure Exit
4 21 9 55	>> 🚍 SAN + 🙆 SAN Cloud + 🔤 Fabric B
Equipment Servers LAN SAN VM Admin	General VSANs Uplink FC Interfaces Uplink FCoE Interfaces Port Channels Faults Events
Filter: All	Actions
SAN SAN Cloud SAN Cloud SAN Prin Groups SAN Pin Groups SAN Pin Groups SAN S Sorage Cloud Sorage Cloud Sorage Cloud Sorage Cloud Sorage Cloud Sorage Cloud Sorage Cloud Traffic Monitoring Sessions	Create VSAN Create Port Channel Create Port Channels Crea

Figure 39 Create vSAN

- 4. Enter VSAN200 in the VSAN name field.
- 5. Keep the Disabled option selected for the Default Zoning.

- 6. Click Common/Global radio button.
- 7. Enter the VSAN ID 200.
- 8. Enter the FCoE VLAN ID 200.
- 9. Click OK.

#### Figure 40 Defining the Common/Global VSAN

<b>A</b>	Cisco Unified Computing System Manager - TME-L21
Fault Summary	🚱 🏐 🖽 New 🚽 🄀 Options 🕜 🕕 📥 Pending Activities 🔟 Exit
4 21 9 55	>> 🗮 SAN + 🧔 SAN Cloud + 💷 Fabric B
Equipment Servers LAN SAN VM Admin	General VSANs Uplink FC Interfaces Uplink FCoE Interfaces Port Channels Faults Events
Filter: All	Actions Create VSAU Network Type: San
B-= SAN	Create VSAN X
SAN Cloud Fabric A San Pin Groups SAN Pin Groups SAN Pin Groups SAN Cloud San Pin Groups San San Cloud San San San San San San San San San San	Create VSAN         Name:       VSAN200         Ft Zoning Settings         Ft Zoning:       Disabled         Do NOT enable local zoning if fabric interconnect is connected to an upstream FC/FCoE switch.         • Common/Global       Fabric B       Both Fabrics Configured Differently         You are creating a global VSAN that maps to the same VSAN ID in all available fabrics.       A VLAN can be used to carry FCoE traffic and can be mapped to this VSAN.         Enter the VSAN ID that maps to this VSAN.       Enter the VLAN ID that maps to this VSAN.         YSAN ID:       200
	OK Cancel

1

### **Creating Port Channel on Cisco UCS 6248 Fabric Interconnect**

### **Fabric Interconnects A**

- 1. Under SAN Cloud, expand the Fabric A tree.
- 2. Right-click FCoE Port Channels.
- 3. Select Create Port Channel.
- 4. Click Yes.
- 5. Enter 10 in the Port Channel ID field and Tenant-Fabric-A in the Port Channel name field.
- 6. Click Next.



Figure 41 Defining the Name and ID for the FCoE Port Channel

- 7. Select ports 31 and 32 and click >> to add the ports to the FCoE Port Channel.
- 8. Click Finish.

I

A		Cisco Unified Computing System Ma	nager - TME-L21		
Fault Summary         V         A           4         20         9		Intons 😧 🕦 📥 Pending Activities 间 Exat			-
Equipment Servers LAN SAN VM Admin	+ - A Filter + Ex	port 🚕 Print			
Filter: All	Name	Fabric ID	If Type	If Role	Transport
			Create FCoE Port Chan	nel	X
SAN     SAN Cloud     SAN Cloud     Email Fabric A     Image Fabric A     Image Fabric A     Image FCoE Port Channels     Bit → FCoE Port Channels		fied Computing			
es → Content For Charles → Uplink FC Unterfaces → Uplink FC CE Interfaces B → T VANs B → T Fabric B	Create FCoE Port Chan 1. √ <u>Set Port C</u> 2. √Add Port	hannel Name			0
SAN Pin Groups	Haron	Ports		Ports in the port channel	
Bi ≡ VSANs Bi ⊆ VSANs Bi ⊆ Polcies Discos Bi ⊆ Polcies Bi ⊥ <u>A</u> , root		Slok ID Port 1 7 1 10 1 11 1 12	MAC D'1/FIEE1901D 5417F1EE1901B 5417F1EE1901B 5417F1EE1901B	Slot ID         Port           1         31           1         32	MAC C C 54:7F:EE:98:BF:86 A 54:7F:EE:98:BF:87
🗄 💯 Traffic Monitoring Sessions		1 13 1 14 1 15 1 16 1 17	54:7F:EE:98:8 54:7F:EE:98:8 54:7F:EE:98:8 54:7F:EE:98:8 54:7F:EE:98:8		
		1 18 1 19 1 20	54:7F:EE:90:B 54:7F:EE:98:B 54:7F:EE:98:B 54:7F:EE:98:B 54:7F:EE:98:B		
		1 21 1 22 1 23 1 23 1 24	54:7F:EE:98:B 54:7F:EE:98:B 54:7F:EE:98:B		
		1 25 1 26 1 27 1 28	54:7F:EE:98:8 54:7F:EE:98:8 54:7F:EE:98:8 54:7F:EE:98:8 54:7F:EE:98:8		
		1 29 1 30	54:7F:EE:98:B		
			×		<u>~</u>

### Figure 42 Selecting and Adding Ports to the FCoE Port Channel

1

- 9. Click OK to complete creating the FCoE Port Channel.
- 10. In the VSAN pull-down select VSAN300.
- **11.** Click **Save Changes** and then click **OK**.

### Figure 43 Selecting VSAN ID for FCoE Port Channel

Δ	Cisco Unified Computing System Manager - TME-L21
Fault Summary           Image: Summary      <	G ● ■ New - 🕞 Options 🕢 1 📥 Pending Activities 🔟 Exit
Equipment Servers LAN SAN VM Admin	General Ports Faults Events Statistics
Filter: All	Status     Properties       Physical PC State:     Up       ID:     10       Physical PC State Reason:     Fabric ID:
SAN Cloud SAN Cloud Fabric A FCOE Part Channels FCOE Port Channels FCOE Interface 1/31 FCOE Interface 1/32 FCOE Interfaces Uplink FCOE Interfaces SAN Pin Groups SAN Pin Groups SAN Storage Cloud Storage Cloud Folicies Folic	Froble Port State: ↑ Up FCoE PC State: ↑ Up FCoE PC State: ↑ Up FCoE PC State: ↑ Up Factions Factions Finable Port Channel Finable Port Finable Port Fi

#### **Fabric Interconnects B**

- 1. Under SAN Cloud, expand the Fabric B tree.
- 2. Right-click FCoE Port Channels.
- 3. Select Create Port Channel.
- **4.** Click **Yes**, and then enter 10 in the Port Channel ID field and Tenant-Fabric-B in the FCoE Port Channel name field.
- 5. Click Next.

Figure 44 Entering the Name and ID for the FCoE Port Channel



- 6. Select ports 31 and 32 and click >> to add the ports to the FCoE Port Channel.
- 7. Click Finish.

ſ

Figure 45 Selecting and Adding FCoE Ports to the FCoE Port Channel

1

- 8. Click **OK** to complete creating the FCoE Port Channel.
- **9.** In the VSAN pull-down select VSAN200.
- 10. Click Save Changes.

#### Figure 46 FCoE Port Channel Properties

Δ	Cisco Unified Computing System Manager - TME-L21
Fault Summary	🚱 🌑 🗳 New 🚽 🏠 Options 🤣 🚯 📥 Pending Activities 🔯 Exit
4 20 9 55	>> 🗮 SAN > 🜔 SAN Cloud > 🔤 Fabric B > 📲 FCoE Port Channels > 🖶 FCoE Port-Channel 10 (Fabric B)
Equipment Servers LAN SAN VM Admin	General Ports Faults Events Statistics
Filter: All	Status
Image: SAN Cloud         Image: SAN Picture Cloud         Image: SAN Picture Cloud         Image: SAN Picture Cloud         Image: Strate Cloud      <	Physical PC State:  Up Physical PC State Reason: FCOE PC State:  Up FCOE PC State Reason: Actions Consecutive Enable Port Channel Consecutive Enable Port Port Port Port Port Port Port Port

### **Creating SAN Port Channels**

The same pair of Cisco Nexus 5548UP Switches can be used to for accessing Storage. The FCoE ports on Cisco UCS 6248UP Fabric Interconnects are configured with FCoE SAN Port Channel to carry SAN traffic over virtual SAN (vSAN) between Nexus 5548UP Switches. To provide SAN security Zoning was set up on the Cisco Nexus 5548UP switches to access right storage system's logical unit numbers (LUNs) visible to the infrastructure and test servers.

This section provides details for configuring the necessary VSANs and SAN Port Channels on Cisco UCS and Cisco Nexus network cloud environment.

In this deployment model we will create separate FCoE SAN Port Channel VSAN 10 on Tenant-A-Fabric-A, and Tenant-A-Fabric-B for handling cloud Tenant A storage traffic. In similar way various VSANs can be created for multi-tenant s in the Cloud to provide storage network multi-tendency.

#### **Cisco Nexus 5548UP Switch A**

SAN port channels are created with default values. The default configuration can be changed just as any other physical interface. To configure the SAN Port Channel in the global configuration mode, login to the Nexus Switch and, run the following commands.

- 1. Type feature fport-channel-trunk.
- 2. Type vsan database.
- **3.** Type vsan 200.
- 4. Type exit.
- 5. Type interface port-channel 1.
- 6. Type switch mode trunk.
- 7. Type switch trunk allowed vlan 200.
- 8. Type exit
- **9.** Type interface Ethernet 1/31.
- **10.** Type switchport mode trunk.
- **11.** Type switchport trunk allowed vlan 200.
- **12.** Type channel-group 10 mode acive.
- 13. Type exit.
- **14.** Type interface Ethernet 1/32.
- **15.** Type switchport mode trunk.
- 16. Type switchport trunk allowed vlan 200.
- **17.** Type channel-group 10 mode acive.
- 18. Type exit.

#### **Cisco Nexus 5548UP Switch B**

SAN port channels are created with default values. The default configuration can be changed just as any other physical interface. To configure the SAN Port Channel in the global configuration mode, run the following commands.

- 1. Type feature fport-channel-trunk.
- **2.** Type vsan database.

- 3. Type vsan 300.
- 4. Type exit.
- **5.** Type interface port-channel 10.
- 6. Type switch mode trunk.
- 7. Type switch trunk allowed vlan 300.
- 8. Type exit
- 9. Type interface Ethernet 1/31.
- **10.** Type switchport mode trunk.
- **11.** Type switchport trunk allowed vlan 300.
- **12**. Type channel-group 10 mode acive.
- 13. Type exit.
- **14.** Type interface Ethernet 1/32.
- **15.** Type switchport mode trunk.
- **16.** Type switchport trunk allowed vlan 300.
- **17.** Type channel-group 10 mode acive.
- 18. Type exit.

## NetApp Storage

This section presents design considerations of cloud storage layout for deploying storage infrastructure for building Citrix CloudPlatform 4.2.1. To support various service levels of shared storage infrastructure in a multi-tenant cloud environment, NetApp offers various features such as:

- Unified data storage architecture that supports multiple workloads.
- Seamless, multidimensional scaling that meets the dynamic demands of cloud computing.
- Storage efficiency that helps reduce capacity requirements and costs by 50% or more.
- Secure multi-tenancy segments, that isolates and delivers shared server, storage, and network resources.
- Service automation and analytics automate storage provisioning, comprehensive visibility, and monitoring.
- Nondisruptive, continuous operations that enable nonstop data availability for shared cloud storage resources.
- Integrated data protection that helps meet backup, disaster recovery, archiving, compliance, and security service-level agreements.
- Virtual storage tiering that automates data movement based on application affinity and workload.
- Embedded data security that protects data assets through role-based administration, encryption, and antivirus.

The NetApp aggregation layer provides a large virtualized pool of storage capacity and disk IOPS to be used on demand by Citrix CloudPlatform 4.2.1. The aggregation-layer sizing is based on the storage requirements for hosting Citrix CloudPlatform 4.2.1 to store tenant data, to meet the storage capacity, performance, and snapshot copy backup requirements of an assumed workload. When sizing for your environment, perform the necessary planning to determine the exact storage configuration for your

individual requirements. Aggregation layer 0 (Aggr0) is defined for hosting root NetApp flexible volumes (FlexVol® volumes) that use the NetApp clustered Data ONTAP operating system for handling NetApp storage configurations. For details on NetApp storage command options, see http://now.netapp.com/NOW/public/knowledge/docs/ontap/re1732/pdfs/ontap/210-04499.pdf.



In this design, we will create aggregates, flexible volumes, FC and iSCSI LUNs, igroups, and NFS mount points for TenantA hosts to provision primary and secondary storage for hosting virtual machines in a Citrix cloud environment.

### **Storage Configuration**

### **Controller FAS32xx Series**

Requirement	Reference	Comments
Physical site where storage system needs to be installed must be ready	Site Requirements Guide	Refer to the "Site Preparation" section.
Storage system connectivity requirements	Site Requirements Guide	Refer to the "System Connectivity Requirements" section.
Storage system general power requirements	Site Requirements Guide	Refer to the "Circuit Breaker, Power Outlet Balancing, System Cabinet Power Cord Plugs, and Console Pinout Requirements" section.
Storage system model-specific requirements	Site Requirements Guide	Refer to the "FAS32xx/V32xx Series Systems" section.

#### Table 7 Controller FAS32XX series prerequisites

### System Configuration Guides

System configuration guides provide supported hardware and software components for the specific clustered Data ONTAP version. These online guides provide configuration information for all NetApp storage appliances currently supported by the clustered Data ONTAP software. They also provide a table of component compatibilities. The documentation below applies to the clustered Data ONTAP 8.1.2 software that was deployed in this study.

- 1. Make sure that the hardware and software components are supported with the version of Data ONTAP that you plan to install by checking the System Configuration Guides at the NetApp Support site.
- **2.** In the System Configuration Guide, click the appropriate NetApp storage appliance and then click the component you want to view. Alternatively, to compare components by storage appliance, click a component and then click the NetApp storage appliance you want to view.

### Controllers

Follow the physical installation procedures for the controllers in theFAS32xx documentation at the NetApp Support site.

### **Disk Shelves DS2246 Series**

### **DS2246 Disk Shelves**

Follow the procedures in the Disk Shelf Installation and Setup section of the DS2246 Disk Shelf Overview to install a disk shelf for a new storage system.

Follow procedures for proper cabling with the controller model as described in SAS Disk Shelves Universal SAS and ACP Cabling Guide.

The following information applies to DS2246 disk shelves:

- SAS disk drives use software-based disk ownership. Ownership of a disk drive is assigned to a specific storage system by writing software ownership information on the disk drive rather than by using the topography of the storage system's physical connections.
- Connectivity terms used: shelf-to-shelf (daisy-chain), controller-to-shelf (top connections), and shelf-to controller (bottom connections).
- Unique disk shelf IDs must be set per storage system (a number from 0 through 98).
- Disk shelf power must be turned on to change the digital display shelf ID. The digital display is on the front of the disk shelf.
- Disk shelves must be power cycled after the shelf ID is changed for it to take effect.
- Changing the shelf ID on a disk shelf that is part of an existing storage system running Data ONTAP requires that you wait at least 30 seconds before turning the power back on so that Data ONTAP can properly delete the old disk shelf address and update the copy of the new disk shelf address.
- Changing the shelf ID on a disk shelf that is part of a new storage system installation (the disk shelf is not yet running Data ONTAP) requires no wait; you can immediately power cycle the disk shelf.

### **Cisco Nexus 5596 Cluster Network Switch Configuration**

Cisco Nexus 5596 cluster network switch configuration prerequisites.:

- 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.
- Determine switch name.
- Identify SSH key type (dsa, rsa, or rsa1)
- Set up an e-mail server for Cisco Smart Call Home and IP connectivity between the switch and the e-mail server.
- Provide SNMP contact information for Cisco Smart Call Home (name, phone, street address).

 Identify a CCO ID associated with an appropriate Cisco SMARTnet<sup>®</sup> Service contract for Cisco Smart Call Home.

### 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.** Enter appropriate 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.

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 Cisco Nexus 5596 is being used as a cluster network switch with Data ONTAP 8.1.2, it should be running NX-OS version 5.2(1)N1(1). The show version command from the switch command line interface will show the switch version currently running on the switch. If the currently running version is not 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. Make sure both cluster interconnects are running NX-OS version 5.2(1)N1(1).

### 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:
- 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 in which <config file name> is the file name for the switch type. A series of warnings regarding PortFast is displayed as each port is configured.

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.
- 7. 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
- **8.** 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
- **9.** 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
- **10.** Ethernet interface 1/41 through Ethernet interface 1/48.
- 11. Copy the running-config to the startup-config.

copy running-config startup-config

### **Cisco Smart Call Home Setup**

To configure Smart Call Home on a Cisco Nexus 5596 switch, follow these 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)#streetaddress <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
```

### **Clustered Data ONTAP 8.1.2**

### Node 1

1. Connect to the storage system console port. You should see a Loader-A prompt. However, if the storage system is in a reboot loop, press Ctrl-C to exit the autoboot loop when you see this message:

Starting AUTOBOOT press Ctrl-C to abort

**2**. From the Loader-A prompt:

#### printenv

- **3.** If the last-OS-booted-ver parameter is not set to 8.1.2, proceed to step 4 to load Data ONTAP 8.1.2 software. If Data ONTAP 8.1.2 is already loaded, proceed to step 16.
- **4.** Allow the system to boot up.

boot\_ontap

5. Press Ctrl-C when the Press Ctrl-C for Boot Menu message appears.

Note	If Data ONTAP 8.1.2 is not the version of software being booted, proceed with the following steps to install new software. If Data ONTAP 8.1.2 is the version being booted, then select option 8 and $yes$ t reboot the node. Then proceed with step 5.		
	<b>6</b> . To install new software, first select option 7.		
	<ul> <li><sup>7</sup></li> <li>Answer yes to perform a nondisruptive upgrade.</li> </ul>		
	<b>8.</b> Select e0M for the network port you want to use for the download.		
	eom 9. Select yes to reboot now.		
	<b>10.</b> $\stackrel{\text{Y}}{\text{Enter the IP address, netmask, and default gateway for e0M in their respective places.}$		
	< <var_node01_mgmt_ip>&gt; &lt;<var_node01_mgmt_mask>&gt; &lt;<var_node01_mgmt_gateway>&gt; 11. Enter the URL where the software can be found.</var_node01_mgmt_gateway></var_node01_mgmt_mask></var_node01_mgmt_ip>		
Note	This Web server must be pingable.		
	< <var_url_boot_software>&gt; 12. Press Enter for the user name, indicating no user name.</var_url_boot_software>		
	Enter <b>13.</b> Enter yes to set the newly installed software as the default to be used for subsequent reboots.		
	<ul><li><sup>Y</sup></li><li>Enter yes to reboot the node.</li></ul>		
	У		
Note	When installing new software, the system might perform firmware upgrades to the BIOS and adapte cards, causing reboots and possible stops at the LOADER prompt. If these actions occur, the system might deviate from this procedure.		
	<b>15.</b> Press Ctrl-C to exit autoboot when you see this message:		
	Starting AUTOBOOT press Ctrl-C to abort <b>16.</b> From the LOADER-A prompt, enter:		
	printenv		
Note	If bootarg.init.boot_clustered true is not listed, the system is not set to boot in clustered Data ONTA		
	<b>17.</b> If the system is not set to boot in clustered Data ONTAP, at the LOADER prompt, enter the followin command to make sure the system boots in clustered Data ONTAP:		
	<pre>setenv bootarg.init.boot_clustered true setenv bootarg.bsdportname e0M 18. At the LOADER-A prompt, enter:</pre>		
	autoboot 19. When you see Press Ctrl-C for Boot Menu:		
	Ctrl - C 20. Select option 4 for clean configuration and initialize all disks.		

1

v

- **21.** Answer yes to Zero disks, reset config and install a new file system.
- **22.** Enter yes to erase all the data on the disks.

Note

The initialization and creation of the root volume can take 75 minutes or more to complete, depending on the number of disks attached. After initialization is complete, the storage system reboots. You can continue to node 02 configuration while the disks for node 01 are zeroing.

### Node 2

1. Connect to the storage system console port. You should see a Loader-A prompt. However, if the storage system is in a reboot loop, press Ctrl-C to exit the autoboot loop when you see this message:

Starting AUTOBOOT press Ctrl-C to abort ...

2. From the Loader-A prompt, enter:

printenv

- **3.** If the last-OS-booted-ver parameter is not set to 8.1.2, proceed to step 4 to load Data ONTAP 8.1.2 software. If Data ONTAP 8.1.2 is already loaded, proceed to step 16.
- **4.** Allow the system to boot up.

boot\_ontap

5. Press Ctrl-C when Press Ctrl-C for Boot Menu is displayed.

Ctrl-C



If Data ONTAP 8.1.2 is not the version of software being booted, proceed with the following steps to install new software. If Data ONTAP 8.1.2 is the version being booted, then select option 8 and yes to reboot the node. Then proceed with step 15.

- 6. To install new software first select option 7.
- 7. Answer yes to perform a nondisruptive upgrade.
- 8. Select e0M for the network port you want to use for the download.

e0M

- 9. Select yes to reboot now.
- **10.** Enter the IP address, netmask, and default gateway for e0M in their respective places.

```
<<var_node02_mgmt_ip>> <<var_node02_mgmt_mask>> <<var_node02_mgmt_gateway>>
```

**11.** Enter the URL where the software can be found.



This Web server must be reachable.

<<var\_url\_boot\_software>>

**12.** Press Enter for the user name, indicating no user name.

Enter

**13.** Select yes to set the newly installed software as the default to be used for subsequent reboots.

У

car	nen installing new software, the system might perform firmware upgrades to the BIOS and adap rds, causing reboots and possible stops at the LOADER prompt. If these actions occur, the syste ght deviate from this procedure.
15.	Press Ctrl-C to exit autoboot when you see this message:
16.	Starting AUTOBOOT press Ctrl-C to abort From the LOADER-A prompt, enter:
	printenv
If l	pootarg.init.boot_clustered true is not listed, the system is not set to boot in clustered Data ONT
17.	If the system is not set to boot in clustered Data ONTAP, at the LOADER prompt, enter the follo command to make sure the system boots in clustered Data ONTAP:
18.	setenv bootarg.init.boot_clustered true setenv bootarg.bsdportname eOM At the LOADER-A prompt, enter:
19.	autoboot Press Ctrl-C for boot menu when prompted:
20.	Ctrl - C Select option 4 for clean configuration and initialize all disks.
	<sup>4</sup> Answer yes to Zero disks, reset config and install a new file system.
<b>21</b> .	У
	Enter yes to erase all the data on the disks.

1

## **Cluster Create in Clustered Data ONTAP**

Table 8	Cluster create in clustered Data ONTAP prerequisites
14010 0	chaoto, cicato in chaotorea Data ertina proregaionee

Cluster Detail	Cluster Detail Value
Cluster name	< <var_clustername>&gt;</var_clustername>
Clustered Data ONTAP base license	< <var_cluster_base_license_key>&gt;</var_cluster_base_license_key>
Cluster management IP address	< <var_clustermgmt_ip>&gt;</var_clustermgmt_ip>
Cluster management netmask	< <var_clustermgmt_mask>&gt;</var_clustermgmt_mask>
Cluster management port	< <var_clustermgmt_port>&gt;</var_clustermgmt_port>
Cluster management gateway	< <var_clustermgmt_gateway>&gt;</var_clustermgmt_gateway>

Cluster Node01 IP address	< <var_node01_mgmt_ip>&gt;</var_node01_mgmt_ip>
Cluster Node01 netmask	< <var_node01_mgmt_mask>&gt;</var_node01_mgmt_mask>
Cluster Node01 gateway	< <var_node01_mgmt_gateway>&gt;</var_node01_mgmt_gateway>

#### Table 8 Cluster create in clustered Data ONTAP prerequisites

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. 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.
Do you want to create a new cluster or join an existing cluster?
{create, join}:
```

Note

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.

2. Enter the following command to create a new cluster:

```
create
3. The system defaults are displayed.
System Defaults:
Private cluster network ports [e1a,e2a].
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]:
```

4. NetApp recommends accepting the system defaults. To accept the system defaults, press Enter.



The cluster is created; this can take a minute or two.

**5.** 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 additional license key[]:
```

```
<u>Note</u>
```

For this validated architecture we recommend you install license keys for SnapRestore, NFS, FCP, 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 cluster management interface port [e0a]: e0a
Enter the cluster management interface IP address: <<var_clustermgmt_ip>>
Enter the cluster management interface netmask: <<var_clustermgmt_mask>>
Enter the cluster management interface default gateway: <<var_clustermgmt_gateway>>
6. Enter the DNS domain name.
```

FlexPod Data Center with VMware vSphere 5.1, and Citrix CloudPlatform 4.2.1

	Enter the DNS domain names:< <var_dns_domain_name>&gt; Enter the name server IP addresses:&lt;<var_nameserver_ip>&gt;</var_nameserver_ip></var_dns_domain_name>
If y	you have more than one name server IP address, separate them with a comma.
7.	Set up the node.
	Where is the controller located []:< <var_node_location>&gt; Enter the node management interface port [eOM]: eOb Enter the node management interface IP address: &lt;<var_node01_mgmt_ip>&gt; enter the node management interface netmask:&lt;<var_node01_mgmt_mask>&gt; Enter the node management interface default gateway:&lt;<var_node01_mgmt_gateway>&gt;</var_node01_mgmt_gateway></var_node01_mgmt_mask></var_node01_mgmt_ip></var_node_location>
The	e node management interface should be in a different subnet than the cluster management interface. e node management interfaces can reside on the out-of-band management network, and the cluster nagement interface can be on the in-band management network.
8.	Press Enter to accept the AutoSupport message.
9.	Reboot node 01.
	system node reboot < <var_node01>&gt;</var_node01>
10.	y Press Ctrl-C for boot menu when prompted:
	ctrl - c Select 5 to boot into maintenance mode.
40	
	When prompted, Continue with boot?, enter y.
13.	To verify the HA status of your environment, run the following command: ha-config show
	ither component is not in HA mode, use the ha-config modify command to put the components in HA de.
14.	To see how many disks are unowned, enter:
	disk show -a
No	disks should be owned in this list.
15.	Assign disks.
	is reference architecture allocates half the disks to each controller. However, workload design could tate different percentages.
16.	disk assign -n < <var_#_of_disks>&gt; Reboot the controller.</var_#_of_disks>
17	halt
17.	At the LOADER-A prompt, enter:
	autoboot

1

### **Cluster Join in Clustered Data ONTAP**

Cluster Detail	Cluster Detail Value
Cluster name	< <var_clustername>&gt;</var_clustername>
Cluster management IP address	< <var_clustermgmt_ip>&gt;</var_clustermgmt_ip>
Cluster Node02 IP address	< <var_node02_mgmt_ip>&gt;</var_node02_mgmt_ip>
Cluster Node02 netmask	< <var_node02_mgmt_mask>&gt;</var_node02_mgmt_mask>
Cluster Node02 gateway	< <var_node02_mgmt_gateway>&gt;</var_node02_mgmt_gateway>

Table 9 Cluster join in clustered Data ONTAP prerequisites

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. During the 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.
Do you want to create a new cluster or join an existing cluster?
{create, join}:
```

Note

If a login prompt displays instead of the Cluster Setup wizard, start the wizard by logging in using the factory default settings, and then enter the cluster setup command.

- 2. Enter the following command to join a cluster:
- join
- **3.** The system defaults are displayed.

```
System Defaults:
Private cluster network ports [e1a,e2a].
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]:
```

4. NetApp recommends accepting the system defaults. To accept the system defaults, press Enter.

Note

The cluster creation can take a minute or two.

5. The steps to create a cluster are displayed.

Enter the name of the cluster you would like to join [<<var\_clustername>>]:Enter



The node should find the cluster name.

6. Set up the node.

```
Enter the node management interface port [eOM]: eOb
           Enter the node management interface IP address: <<var_node02_mgmt_ip>>
           Enter the node management interface netmask: Enter
           Enter the node management interface default gateway: Enter
        7. 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.
        8. Press Enter to accept the AutoSupport message.
        9. Log in to the Cluster Interface with the admin user id and <<var_password>>.
       10. Reboot node 02.
           system node reboot <<var_node02>>
       11. Press Ctrl-C for boot menu when prompted:
           Ctrl - C
       12. Select 5 to boot into maintenance mode.
       13. When prompted, Continue with boot? enter:
       14. To verify the HA status of your environment, enter:
           ha-config show
Note
       If either component is not in HA mode, use the ha-config modify command to put the components
       in HA mode.
       15. To see how many disks are unowned, enter:
           disk show -a
       16. Assign disks.
Note
       This reference architecture allocates half the disks to each controller. However, the workload design
       could dictate different percentages. Assign all remaining disks to node 02.
           disk assign -n <<var_#_of_disks>>
       17. Reboot the controller:
           halt
       18. At the LOADER-A prompt, enter:
           autoboot
       19. Press Ctrl-C for boot menu when prompted:
```

Ctrl-C

### Log in to the Cluster

Open an SSH connection to cluster IP or host name and log in to the admin user with the password that was 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 Clustered Data ONTAP

Create a management port failover group.

```
network interface failover-groups create -failover-group fg-cluster-mgmt -node
<<var_node01>> -port e0a
network interface failover-groups create -failover-group fg-cluster-mgmt -node
<<var_node02>> -port e0a
```

### Assign Management Failover Group to Cluster Management LIF

Assign the management port failover group to the cluster management LIF.

```
network interface modify -vserver <<var_clustername>> -lif cluster_mgmt
-failover-group fg-cluster-mgmt
```

### Failover Groups Node Management in Clustered Data ONTAP

Create a management port failover group.

```
network interface failover-groups create -failover-group fg-node-mgmt-01 -node
<<var_node01>> -port e0b
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 e0b
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.

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

### Flash Cache in Clustered Data ONTAP

Complete the following steps to enable Flash Cache on each node.

Run the following commands from the cluster management interface:

```
system node run -node <<var_node01>> options flexscale.enable on
system node run -node <<var_node01>> options flexscale.lopri_blocks off
system node run -node <<var_node01>> options flexscale.normal_data_blocks on
system node run -node <<var_node02>> options flexscale.enable on
system node run -node <<var_node02>> options flexscale.lopri_blocks off
system node run -node <<var_node02>> options flexscale.normal_data_blocks on
```

Note

Data ONTAP 8.1 and later does not require a separate license for Flash Cache.



For directions on how to configure Flash Cache in metadata mode or low-priority data caching mode, refer to TR-3832: Flash Cache Best Practices Guide. Before customizing the settings, determine whether the custom settings are required or if the default settings are sufficient.

### 64-Bit Aggregates in Clustered Data ONTAP

A 64-bit aggregate containing the root volume is created during the 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:

```
aggr create -aggregate aggr01 -nodes <<var_node01>> -B 64 -s <<var_raidsize>>
-diskcount <<var_num_disks>>
aggr create -aggregate aggr02 -nodes <<var_node02>> -B 64 -s <<var_raidsize>>
-diskcount <<var_num_disks>>
```

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.



Calculate the RAID group size to allow for roughly balanced (same size) RAID groups of from 12 through 20 disks (for SAS disks) within the aggregate. For example, if 52 disks were being assigned to the aggregate, select a RAID group size of 18. A RAID group size of 18 would yield two 18-disk RAID groups and one 16-disk RAID group. 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.



The aggregate cannot be created until disk zeroing completes. Use the aggr show command to display aggregate creation status. Do not proceed until both aggr01 and aggr02 are online.

1. Disable Snapshot copies for the two data aggregates just created.

node run <<var\_node01>> aggr options aggr01 nosnap on node run <<var\_node02>> aggr options aggr02 nosnap on 2. Delete any existing Snapshot copies for the two data aggregates.

node run <<var\_node01>> snap delete -A -a -f aggr01

```
node run <<var_node02>> snap delete -A -a -f aggr02
3. Rename the root aggregate on node 01 to match the naming convention for this aggregate on node
02.
aggr show
aggr rename -aggregate aggr0 -newname <<var_node01_rootaggrname>>
```

### **Service Processor**

Gather information about the network and the AutoSupport settings before configuring the Service Processor (SP).

Configure the SP using DHCP or static addressing. If the SP uses a static IP address, verify that the following SP prerequisites have been met:

- 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 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.

### Upgrade the Service Processor on Each Node to the Latest Release

With Data ONTAP 8.1.2, you must upgrade to the latest service processor (SP) firmware to take advantage of the latest updates available for the remote management device.

- 1. Using a web browser, connect to http://support.netapp.com/NOW/cgi-bin/fw.
- **2.** Navigate to the Service Process Image for installation from the Data ONTAP prompt page for your storage platform.
- 3. Proceed to the download page for the latest release of the SP firmware for your storage platform.
- **4.** Using the instructions on this page, update the SPs on both nodes in your cluster. You will need to download the .zip file to a web server that is reachable from the cluster management interface. In step 1a of the instructions substitute the following command then execute steps 2–6 on each node.

system image get -node \* -package http://web\_server\_name/path/SP\_FW.zip. Also, instead
of run local, use system node run <<var\_nodename>>,

### **Configure the Service Processor on Node 01**

- **1.** From the cluster shell, enter the following command:
  - system node run <<var\_node01>> sp setup
- 2. Enter the following to set up the SP:

```
Would you like to configure the SP? Y
Would you like to enable DHCP on the SP LAN interface? no
Please enter the IP address of the SP[]: <<var_node01_sp_ip>>
Please enter the netmask of the SP[]: <<var_node01_sp_mask>>
```

Please enter the IP address for the SP gateway[]: <<var\_node01\_sp\_gateway>>

### Configure the Service Processor on Node 02

- 1. From the cluster shell, enter the following command:
  - system node run <<var\_node02>> sp setup
- **2.** Enter the following to set up the SP:

```
Would you like to configure the SP? Y
Would you like to enable DHCP on the SP LAN interface? no
Please enter the IP address of the SP[]: <<var_node02_sp_ip>>
Please enter the netmask of the SP[]: <<var_node02_sp_mask>>
Please enter the IP address for the SP gateway[]: <<var_node02_sp_gateway>>
```

### Storage Failover in Clustered Data ONTAP

Run the following commands in a failover pair to enable storage failover.

1. 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.

- 2. Enable HA mode for two-node clusters only.
- **3.** 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
```

4. 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>>
```

### **IFGRP LACP in Clustered Data ONTAP**

This type of interface group requires two or more Ethernet interfaces and a switch that supports LACP. Therefore, make sure that the switch is configured properly.

Run the following commands on the command line to create interface groups (ifgrps).

```
ifgrp create -node <<var_node01>> -ifgrp a0a -distr-func port -mode multimode_lacp
network port ifgrp add-port -node <<var_node01>> -ifgrp a0a -port e3a
network port ifgrp add-port -node <<var_node01>> -ifgrp a0a -port e4a
ifgrp create -node <<var_node02>> -ifgrp a0a -distr-func port -mode multimode_lacp
network port ifgrp add-port -node <<var_node02>> -ifgrp a0a -port e3a
network port ifgrp add-port -node <<var_node02>> -ifgrp a0a -port e4a
```



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.

## **VLAN in Clustered Data ONTAP**

### **Create NFS VLANs**

Run the following command:

```
network port vlan create -node <<var_node01>> -vlan-name a0a-<<var_nfs_vlan_id>>
network port vlan create -node <<var_node02>> -vlan-name a0a-<<var_nfs_vlan_id>>
```

### Jumbo Frames in Clustered Data ONTAP

To configure a 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:

```
network port modify -node <<var_node01>> -port a0a-<<var_nfs_vlan_id>> -mtu 9000
```

WARNING: Changing the network port settings will cause a serveral second interruption in carrier. Do you want to continue? {y|n}: y network port modify -node <<var\_node02>> -port a0a-<<var\_nfs\_vlan\_id>> -mtu 9000 WARNING: Changing the network port settings will cause a serveral second interruption in carrier. Do you want to continue? {y|n}: y

# **NTP in Clustered Data ONTAP**

To configure time synchronization on the cluster, follow these 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

## **SNMP in Clustered Data ONTAP**

1. 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 DFM server or another fault management system.

snmp traphost add <<var\_oncommand\_server\_fqdn>>

# **SNMPv1 in Clustered Data ONTAP**

1. Set the shared secret plain-text password, which is called a community.

```
snmp community delete all
snmp community add ro <<var_snmp_community>>
```

```
<u>Note</u>
```

Use the delete all command with caution. If community strings are used for other monitoring products, the delete all command will remove them.

## **SNMPv3 in Clustered Data ONTAP**

SNMPv3 requires that a user be 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 in Clustered Data ONTAP

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>>
```

### **Cisco Discovery Protocol in Clustered Data ONTAP**

Enable Cisco Discovery Protocol (CDP) on the NetApp storage controllers by using the following procedure.



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:

1. Enable CDP on Data ONTAP.

node run -node <<var\_node01>> options cdpd.enable on node run -node <<var\_node02>> options cdpd.enable on

### Vserver - Storage Virtual Machine (SVM)

Secure multi-tenancy is the use of secure virtual partitions within a shared physical storage environment for the purpose of sharing the physical environment among multiple distinct tenants. For instance, a storage service provider might configure a storage array in such a way that each of three different customers is provisioned a certain portion of the array's disk capacity and network resources. In a secure multi-tenant environment, each customer would have access only to the resources explicitly provisioned to that customer. The customer would not have access to other customers' data or even be aware of the existence of the other customers or the fact that they share a common physical array.

The secure logical storage partition through which data is accessed in clustered Data ONTAP is known as a vServer, also called Storage Virtual Machine (SVM). A cluster serves data through at least one and possibly multiple vServer's. A vServer is a logical abstraction that represents a set of physical resources of the cluster. Data volumes and logical network interfaces (LIFs) are created and assigned to a vServer and may reside on any node in the cluster to which the vServer has been given access. A vServer may own resources on multiple nodes concurrently, and those resources can be moved non-disruptively from one node to another. It is capable of supporting multiple data protocols concurrently. Volumes within the vServer can be junctioned together to form a single NAS namespace, which makes all of the vServers data available through a single share or mount point to NFS and CIFS clients.



Figure 47 vServer (Storage Virtual Machine)

For more information on vServer (SVM) see TR-4160: Secure Multi-tenancy in Clustered DATA Ontap.

The procedure to create a vServer with name Infra\_Vserver is illustrated below. However, the same procedure can be followed to create additional vServer for isolation in Service Provider or shared environments as required.

To create an infrastructure vServer, follow these 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:Infra\_Vserver
3. Select the vServer data protocols to configure.

Choose the Vserver data protocols to be configured {nfs, cifs, fcp, iscsi}:nfs, fcp 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 {aggr01, aggr02} [aggr01]:aggr01

**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.** Answer no to Do you want to Configure FCP? {yes, no} [yes]: no.
- Do you want to Configure FCP? {yes, no} [yes]: no
- **11**. Add the two data aggregates to the Infra\_Vserver aggregate list for NetApp Virtual Console.

vserver modify -vserver Infra\_Vserver -aggr-list aggr01, aggr02

## Create Load Sharing Mirror of vServer Root Volume in Clustered Data ONTAP

1. Create a volume to be the load sharing mirror of the infrastructure vServer root volume on each node.

```
volume create -vserver Infra_Vserver -volume root_vol_m01 -aggregate aggr01 -size 20MB
-type DP volume create -vserver Infra_Vserver -volume root_vol_m02 -aggregate aggr02
-size 20MB -type DP
```

2. Create the mirroring relationships.

```
snapmirror create -source-path //Infra_Vserver/root_vol -destination-path
//Infra_Vserver/root_vol_m01 -type LS
snapmirror create -source-path //Infra_Vserver/root_vol -destination-path
//Infra_Vserver/root_vol_m02 -type LS
```

**3**. Initialize the mirroring relationship.

snapmirror initialize-ls-set -source-path //Infra\_Vserver/root\_vol

4. Set an hourly (at 5 minutes past the hour) update schedule on each mirroring relationship.

snapmirror modify -source-path //Infra\_Vserver/root\_vol -destination-path \* -schedule
hourly

### FC Service in Clustered Data ONTAP

Create the FC service on each vServer. This command also starts the FC service and sets the FC alias to the name of the vServer.

```
fcp create -vserver Infra_Vserver
```

## **HTTPS Access in Clustered Data ONTAP**

Secure access to the storage controller must be configured.

**1.** Increase the privilege level to access the certificate commands.

```
set -privilege advanced Do you want to continue? {y |n}: y
```

2. Generally, a self-signed certificate is already in place. Check it with the following command:

Note

```
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.
   system services web modify -external true -sslv3-enabled true
   Do you want to continue \{y | n\}: y
   system services firewall policy delete -policy mgmt -service http -action allow
   system services firewall policy create -policy mgmt -service http -action deny
   -ip-list 0.0.0/0
   system services firewall policy delete -policy mgmt -service telnet -action allow
   system services firewall policy create -policy mgmt -service telnet -action deny
   -ip-list 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
```

**3.** Run the following commands as one-time commands to generate and install self-signed certificates:

You can also use the security certificate delete command to delete expired certificates

<<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

security certificate show

```
Note
```

It is normal for some of these commands to return an error message stating that the entry does not exist.

vserver services web access create -name spi -role admin -vserver <<var\_clustername>>

vserver services web modify -name spi|ontapi|compat -vserver \* -enabled true

vserver services web access create -name ontapi -role admin -vserver

vserver services web access create -name compat -role admin -vserver

## NFSv3 in Clustered Data ONTAP

v

У

У

set -privilege admin

<<var clustername>>

<<var\_clustername>>

Run all commands to configure NFS on the vServer.

1. Secure the default rule for the default export policy and create the FlexPod export policy.

```
vserver export-policy rule modify -vserver Infra_Vserver -policyname default
-ruleindex 1 -rorule never -rwrule never -superuser never
vserver export-policy create -vserver Infra_Vserver FlexPod
Create a new rule for the FlexPod export policy.
```

```
<u>Note</u>
```

For each ESXi host being created, create a rule. Each host will have its own rule index. Your first ESXi host will have rule index 1, your second ESXi host will have rule index 2, and so on.

vserver export-policy rule create -vserver Infra\_Vserver -policyname FlexPod -ruleindex 1 -protocol nfs -clientmatch <<var\_esxi\_host1\_nfs\_ip>> -rorule sys -rwrule sys -superuser sys -allow-suid false

**3.** Assign the FlexPod export policy to the infrastructure vServer root volume.

volume modify -vserver Infra\_Vserver -volume root\_vol -policy FlexPod

### FlexVol in Clustered Data ONTAP

The following information is required to create a FlexVol: the volume's name and size, and the aggregate on which it will exist. Create two VMware datastore volumes, a server boot volume, and a volume to hold the OnCommand database LUN. Also, update the vServer root volume load sharing mirrors to make the NFS mounts accessible.

volume create -vserver Infra\_Vserver -volume infra\_datastore\_1 -aggregate aggr02 -size 500g -state online -policy FlexPod -junction-path /infra\_datastore\_1 -space-guarantee none -percent-snapshot-space 0 volume create -vserver Infra\_Vserver -volume infra\_swap -aggregate aggr01 -size 100g -state online -policy FlexPod -junction-path /infra\_swap -space-guarantee none -percent-snapshot-space 0 -snapshot-policy none

```
volume create -vserver Infra_Vserver -volume TenantADataSecNFS_datastore_1 -aggregate
aggr02 -size 20g -state online -policy FlexPod -junction-path / TenantADataSecNFS 1
-space-guarantee none -percent-snapshot-space 0
volume create -vserver Infra_Vserver -volume TenantA-PrimaryNFS-Storage datastore_1
-aggregate aggr02 -size 20g -state online -policy FlexPod -junction-path /
TenantADataSecNFS 1 -space-guarantee none -percent-snapshot-space 0
volume create -vserver Infra_Vserver -volume TenantA_SecondaryNFS-Storage datastore_1
-aggregate aggr02 -size 20g -state online -policy FlexPod -junction-path /
TenantADataSecNFS 1 -space-guarantee none -percent-snapshot-space 0
volume create aggr02 -size 20g -state online -policy FlexPod -junction-path /
TenantADataSecNFS 1 -space-guarantee none -percent-snapshot-space 0
```

volume create -vserver Infra\_Vserver -volume esxi\_boot -aggregate aggr01 -size 100g
-state online -policy default -space-guarantee none -percent-snapshot-space 0
volume create -vserver Infra\_Vserver -volume OnCommandDB -aggregate aggr02 -size 200g
-state online -policy default -space-guarantee none -percent-snapshot-space 0
snapmirror update-ls-set -source-path //Infra\_Vserver/root\_vol

### LUN in Clustered Data ONTAP

Create two boot LUNS: VM-Host-Infra-01 and VM-Host-Infra-02, and a LUN for Bare-metal: VM-BareMetalHost-Infra-02. Run the following comands:

```
lun create -vserver Infra_Vserver -volume esxi_boot -lun VM-Host-Infra-01 -size 20g
-ostype vmware -space-reserve disabled
lun create -vserver Infra_Vserver -volume esxi_boot -lun VM-Host-Infra-02 -size 20g
-ostype vmware -space-reserve disabled
lun create -vserver Infra_Vserver -volume esxi_boot -lun VM-BareMetalHost-Infra-02
-size 20g -ostype vmware -space-reserve disabled
```

### Igroup in Clustered Data ONTAP

Create three igroups: TenantA-ESX-HostA-Platinum-FC-igroup, TenantA-ESX-HostB-Platinum-FC-igroup and TenantA-ESX-BareMetalHostA-Platinum-FC-igroup

```
igroup create -igroup TenantA-ESX-HostA-Platinum-FC-igroup -protocol fcp -ostype
vmware -initiator 20:00:00:25:b5:01:01:02,20:00:00:25:b5:01:01:03 -vserver
Infra_vserver
igroup create -igroup TenantA-ESX-HostB-Platinum-FC-igroup -protocol fcp -ostype
vmware -initiator 20:00:00:25:b5:01:01:04,20:00:00:25:b5:01:01:05 -vserver
Infra_vserver
igroup create -igroup TenantA-ESX-BareMetalHost-Platinum-FC-igroup -protocol fcp
-ostype vmware -initiator 20:00:00:25:b5:04:01:06,20:00:00:25:b5:04:01:05 -vserver
Infra_vserver
```

### **Deduplication in Clustered Data ONTAP**

Enable deduplication on appropriate volumes.

```
volume efficiency on -vserver Infra_Vserver -volume infra_datastore_1
volume efficiency on -vserver Infra_Vserver -volume TenantADataSecNFS
volume efficiency on -vserver Infra_Vserver -volume TenantA-PrimaryNFS-Storage
volume efficiency on -vserver Infra_Vserver -volume TenantA_SecondaryNFS-Storagevolume
efficiency on -vserver Infra_Vserver -volume esxi_boot
volume efficiency on -vserver Infra_Vserver -volume OnCommandDB
```

### Failover Groups NAS in Clustered Data ONTAP

Create an NFS port failover group.

```
network interface failover-groups create -failover-group fg-nfs-<<var_nfs_vlan_id>>
-node <<var_node01>> -port a0a-<<var_nfs_vlan_id>>
network interface failover-groups create -failover-group fg-nfs-<<var_nfs_vlan_id>>
-node <<var_node01>> -port a0a-<<var_nfs_vlan_id>>
```

## **NFS LIF in Clustered Data ONTAP**

Create an NFS logical interface (LIF).

```
network interface create -vserver Infra_Vserver -lif nfs_lif01 -role data
-data-protocol nfs -home-node <<var_node01>> -home-port a0a-<<var_nfs_vlan_id>>
-address 193.191.1.20 -netmask 255.255.255.0 -status-admin up -failover-policy
nextavail -firewall-policy data -auto-revert true -use-failover-group enabled
-failover-group fg-nfs-<<var_nfs_vlan_id>>
```

network interface create -vserver Infra\_Vserver -lif nfs\_lif02 -role data -data-protocol nfs -home-node <<var\_node01>> -home-port a0a-<<var\_nfs\_vlan\_id>> -address 193.191.1.30 -netmask 255.255.255.0 -status-admin up -failover-policy nextavail -firewall-policy data -auto-revert true -use-failover-group enabled -failover-group fg-nfs-<<var\_nfs\_vlan\_id>>

## FCP LIF in Clustered Data ONTAP

Create four FCoE LIFs, two on each node.

network interface create -vserver Infra\_Vserver -lif fcp\_lif01a -role data -data-protocol fcp -home-node <<var\_node01>> -home-port 3a network interface create -vserver Infra\_Vserver -lif fcp\_lif01b -role data -data-protocol fcp -home-node <<var\_node02>> -home-port 4a network interface create -vserver Infra\_Vserver -lif fcp\_lif02a -role data -data-protocol fcp -home-node <<var\_node01>> -home-port 3a network interface create -vserver Infra\_Vserver -lif fcp\_lif02b -role data -data-protocol fcp -home-node <<var\_node01>> -home-port 3a network interface create -vserver Infra\_Vserver -lif fcp\_lif02b -role data -data-protocol fcp -home-node <<var\_node02>> -home-port 4a

### Add Infrastructure vSserver Administrator

Add the infrastructure vSserver administrator and vServer administration logical interface in the out-of-band management network with the following commands:

```
network interface create -vserver Infra_Vserver -lif vsmgmt -role data -data-protocol
none -home-node <<var_node02>> -home-port e0a -address <<var_vserver_mgmt_ip>>
-netmask <<var_vserver_mgmt_mask>> -status-admin up -failover-policy nextavail
-firewall-policy mgmt -auto-revert true -use-failover-group enabled -failover-group
fg-cluster-mgmt
```

network routing-groups route create -vserver Infra\_Vserver -routing-group d<<var\_clustermgmt\_ip>> -destination 0.0.0/0 -gateway <<var\_clustermgmt\_gateway>> security login password -username vsadmin -vserver Infra\_Vserver Please enter a new password: <<var\_vsadmin\_password>> Please enter it again: <<var\_vsadmin\_password>>

security login unlock -username vsadmin -vserver Infra\_Vserver

# **Cloud Infrastructure on Cisco UCS**

This section explains in detail the design considerations for deploying Cisco UCS compute infrastructure for building Citrix CloudPlatform 4.2.1. In a multi-tenant cloud environment management, provisioning, availability, and service levels of shared infrastructure resources are someof the major tasks for the cloud provider.

To build and rebuild Cloud infrastructure within short duration of time is the key challenge in the cloud environment. Cisco Unified Computing System offers data center platform that unites compute, network, storage access, and virtualization into a cohesive system. The Cisco UCS Manager enables Stateless Computing where each compute node has no fixed set of configuration such as, MAC addresses, UUIDs, WWPN, WWNN, adapter policy, firmware and BIOS settings. All configured centrally and applied in the form of Service Profile to the servers. This reduces TCO and increase business agility, allowing consistent configuration and ease of repurposing compute in Citrix CloudPlatform 4.2.1.

This section details the steps to design and deploy the following Cloud components:

- Cloud Management Design and Deployment
- Cloud Compute Design and Deployment

### **Cloud Management Design and Deployment**

The Cisco UCS offers Organizational Units (OUs) which divides large physical infrastructure of the Cisco UCS domain into logical entities where each cloud tenant will be provided with a dedicated and an isolated management domain with unique resources such as policies, pools, service profiles,

templates and quality of service definitions. On compute security operations front, to provide access control Cisco UCS Manager offers OU locales feature where Users can be delegated with roles and privileges.

Note

In this paper we will create single Organization Unit Tenant A with access roles to delegate Cloud User with admin role for performing Cloud operations.

#### **Creating an Organization**

These steps provide details for configuring an organization in the Cisco UCS environment. Organizations are used as a means to organize and control access to various resources like creating Pools (MAC, PWWN, Management IP, and Server), Policy (BIOS, Firmware, and Adapater), and define Service Profile Templates within the IT organization, thereby enabling multi-tenancy of the compute resources. The necessary steps to create these resources are included below.

To create an Organization, login to the Cisco UCS Manager and follow these steps:

4. From the Server tab with the Servers node highlighted in the left pane, choose New > Create Organization from the top control bar which is shown the right pane of the Cisco UCS Manager.



Figure 48 Creating and Configuring the Organization

- 5. Enter a name for the organization in the Name field.
- 6. Enter a description for the organization (optional) in the Description field.



Figure 49 Adding the Name and Description to the Organization

7. Click OK.

ſ

8. Click OK.



#### Figure 50 Confirming Organization Properties

### **Creating Locale for Organization**

To create locales in the Cisco Cisco UCS Manager, follow these steps:

1. In the Admin tab in the left pane, click on User Services under User Management,

- 2. Right-click Locales and click Create Locale.
- 3. Enter a Name TenantA-Locale.



#### Figure 51 Adding the Name for the Locale

- 4. Click Next.
- 5. Select Organizations, expand root, select TenantA and drag to Org-root/org-Tenant A.
- 6. Click Finish.



#### Figure 52 Assigning Organization to the Locales

### **Creating Role for Organization**

To create user roles in the Cisco UCS Manager, follow these steps:

- 7. In the Admin tab in the left pane click User Roles.
- 8. Right-click Create Role.
- 9. Enter a Name TenantAOrgAdmin and select appropriate rights for managing TenantA Organization.

10. Do not check the Aaa, Admin, Operations and Fault Privileges check boxes.

Fault Summ	hary	1000			ions   😢 🕕 🛔 Pending Activities   🔟 Exit	
			Δ	and the second se		
2	18	7	29	>> 🚔 All 🔸 🔒 User Mana	gement 🕨 🏭 User Services 🕴 🏭 Roles 🕨 🌉 TenantAOrgAdmin	
	- Francis		and and a second second	General Events		
Equipment   S	Servers LAN S	SAN WM	Admin	LYCINS		
Filte	r: All		-	Actions	Properties	
10000					Name: TenantAOrgAdmin	
± =				🗂 Delete	Privileges	
	1999-1997 - 19	1001210				
	ults, Events and				Aaa	*
	er Management Authentication				Admin	
	LDAP				Ext Lan Config	E
	RADIUS				Ext Lan Policy	
	TACACS+				Ext Lan Qos	
	User Services				Ext Lan Security	
	Locales				Ext San Config	
1	a Tenani	A-Locale			Ext San Policy	
	- lentar	nca-Locale			Ext San Qos	
	atest-lo				Ext San Security	
Ð		thenticated I	Users		E Fault	•
1	Remotely A	Authenticate	ed Users		Help	
8	Roles		2 C C		Description:	
	Tenan	tAOrgAdmin			e estretion .	
	aaa admin					
		-manager				
	a netwo					
	- a operat					
	read-o					
		-compute				
	- A server	-equipment				
	- 🚜 server	-profile				
	- as server	-security				
	📇 storag	e				
1						
	y Management					
	KeyRing defau					
	mmunication Ma	nagement				
	Call Home Communicatio	- Couries -				
	DNS Managem					
	Management I					
	UCS Central	incertates				
	ats Management					
	ne Zone Manage					
	pability Catalog					
	anagement Exter					
	ense Manageme					

#### Figure 53 Defining the Properties and Privileges

### **Creating User and Assign Role for Organization**

To create users and assign roles to the organizations, login to the Cisco UCS Manager, and follow these steps

- 1. In the Admin tab in the left pane, click on LocallyAuthenticatedUsers.
- 2. Click Create User.
- 3. Enter Tenant A-Admin in the Name field.
- 4. Choose the Roles (TenantAOrgAdmin), the Locales (TenantA-Locale).
- 5. Click OK.



Figure 54 Defining the Properties for the User Profile

## **Cloud Compute Design and Deployment**

In multitenant cloud environment, the Cisco UCS Manager supports data center automation, which helps in increasing operational agility and scalability, while reducing risks. Through its unified, embedded, policy-based, and ecosystem friendly approach, Cisco UCS Manager helps reduce management and administration expenses, which are among the largest items in most IT budgets. The Cisco UCS Manager can manage up to 160 servers and thousands of Cisco UCS components in multiple chassis.

- A unified embedded management interface that integrates server, network, and storage access
- Policy and model-based management, with service profiles, that improves agility and reduces risk
- Auto-discovery to detect, inventory, manage, and provision system components that are added or changed
- Role-based administration that builds on existing skills and supports collaboration across disciplines

Cisco UCS Pools provide predetermined range for an attribute for an UCS blade, such as server UUID, MAC addresses, WWNNs, WWPN and so on which can be defined at the global level with different attributes and applied to the physical blades in the form of service profile template to achieve faster deployment and state less cloud compute environment.

The service profile contains values for a server's property settings such as virtual network interface cards (vNICs), MAC addresses, virtual host bus adapters (vHBAs), WWPN and WWWN address, boot policies, adapter policies, placement policies, firmware revisions, server pools and other elements. By abstracting these settings from the blade server into a profile, a server can be deployed to any blade server in Cisco UCS. Furthermore, the profile can, at any time, migrate from one blade to another in a chassis.

In multi-tenant environment to logically separate compute identities based on the service levels and management configuration, Cisco UCS Manager allows defining UCS Pools for server UUID, MAC, WWPN, WWNN and Servers.

### **Service Level Agreement- Definitions**

To provide compute based Service Level Agreement and separate management configurations on Citrix CloudPlatform 4.2.1 environment for multi-tenants compute requirements, the following compute based offering SLAs have been defined. These SLAs are directly mapped to the cloud network offerings, which are provided to cloud tenants for choosing compute infrastructure based on cost.

• Platinum-Compute

To satisfy multi-tenant cloud compute service level requirements and to provide higher CPU, and memory, a UCS Server Pool is defined with corresponding management identifier for server UUID, MAC, WWPN, WWNN and IP Management.

• Gold-Compute

To satisfy multi-tenant cloud compute service level requirement and to provide slightly lower CPU and memory compared to Platinum-Compute, a UCS Server Pool is defined with corresponding management identifier for Server UUID, MAC, WWPN, WWNN and IP Management.

• Silver-Compute

To satisfy multi-tenant cloud compute service level requirement and to provide slightly lower CPU and Memory compared to Gold-Compute, a UCS Server Pool is defined with corresponding management identifier for Server UUID, MAC, WWPN, WWNN and IP Management.

• Bronze-Compute

To satisfy multi-tenant cloud compute service level requirement and to provide slightly lower CPU and Memory compared to Silver-Compute, a UCS Server Pool is defined with corresponding management identifier for Server UUID, MAC, WWPN, WWNN and IP Management.

In this section we will create different UCS pools, policies and LAN & SAN pin groups for various Compute-SLAs as defined above. These pools and policies will be applied to corresponding gold service profile template in Organization Unit TenantA, which we have already created for cloud TenantA customer.

This section describes the steps and procedures involved to accomplish the following tasks as per the service level definitions listed earlier:

- Creating UUID Suffix Pool
- Creating a MAC Address Pool
- Creating WWNN Pool
- Creating WWPN Pool
- Creating IP Pool
- Creating Server Pool

- Creating Server Pool Qualifications
- Creating Server BIOS Policy
- Creating Local Disk Configuration Policy
- Creating Boot Policies

### **Creating UUID Suffix Pools**

These steps provide details for creating and configuring the necessary UUID suffix pools for the Cisco UCS environment for the Platinum service class:

1

#### Platinum-Compute-UUID

Login to Cisco UCS Manager with User TenantA-Admin created earlier for Organization Tenant A

- 1. Click the Servers tab in the left pane.
- 2. Choose Pools > Sub-Organizations.
- 3. Expand the Sub-Organizations.
- 4. Right-click UUID Suffix Pools.
- 5. Select Create UUID Suffix Pool.



#### Figure 55 Creating the UUID Suffix Pools

- **6.** Name the UUID suffix pool Platinum-Compute-UUID.
- 7. (Optional) Give the UUID suffix pool a description.
- 8. Leave the prefix at the derived option.
- 9. Click Next to continue.



#### Figure 56 Adding Name and Description to UUID

Note

Ensure that sufficient number of blade resources are available.

- 13. Click OK.
- 14. Click Finish.

Cisco Unified Computing System Manager - TME-L2	21			
Fault Summary		G	A Pending Activities	
2 42 3 18		>> 🥪 Servers ' 🚯 Pools ' 👬 root ' 👬 Sub-Or	rganizations 🕴 🎄 TentantA 👌 🎆 UUID Suffix Pool	s
Equipment Servers LAN SAN VM Admin		-UUID Suffix Pools		
Filter: All		🛨 🖃 🕰 Filter 🖨 Export 😓 Print	<b>•</b> • • •	
± =		Name           Name           Image: Image of the second seco	Pool Name Plantinum-Compute-UUID	UUID Prefix Derived
Servers Service Profiles  Service Profiles  Sub-Organizations  Particle Templates  Sub-Organizations  Policies  Policies  Policies  Sub-Organizations  Sub-Organizat		Create UUID Suffix Unifie Create UUID Suffix Pool 1. √Define Name Describtion 2. √Add UUID Fulfixe Create a Block of UUID Suffixe Create a Block of L	Add UUID Blocks Add UUID Blocks  and Blocks Name COODI-00000000001 S UUD Suffixes	System Manager ? ? • 0001-00000001-0000000 • • Add Delete < Prev Next > Finish Cancel

Figure 57 Specifying the UUID Block Size

I

ſ

Follow the steps described above to create the UUID Pool for Gold, Silver, and Bronze service classes as per the UUID and Size noted in the Table 10.

UUID Pool Name	UUID ID	Size
Platinum-Compute-UUID	0001-000000000000	10
Gold-Compute-UUID	0002-00000000000	10
Silver-Compute-UUID	0003-00000000000	10
Bronze-Compute-UUID	0004-000000000000	10

A Cinco Hail		1 System Manager	- TMC 101						
Fault Sum				<b>G</b> 🔵	🖬 New - 🛃 Options 🛛 😢 🕕	Pending Activities			
2 Equipment	42	3 SAN VM Admin	18	UUID S	ervers + 🛞 Pools + 🙏 root + 🗼 Sub-( <b>iffix Pools</b> <b>4</b> Filter 👄 Export 📚 Print	Organizations + 🙏 TentantA + 🎆 UUID Suffix	Pools		
	nicer: Al				Name	Pool Name	UUID Prefix	From	T
± =					ool Bronze-Compute-UUID	Bronze-Compute-UUID	E832BCBA-DFAA-11E1		
E 🥪 Serve	rs					00		0004-000000000001	0004-0000000000A
	ervice Profiles			□ 關 F	ool Silver-Compute-UUID	Silver-Compute-UUID	E832BCBA-DFAA-11E1		
E-1	root			L.	[0003-00000000001 - 0003-00000000	00		0003-00000000001	0003-0000000000A
	8- 🐸 WS2012 8- 🙏 Sub-Organ	instings			ool Gold-Compute-UUID	Gold-Compute-UUID	E832BCBA-DFAA-11E1		
	ervice Profile Ten				[0002-00000000001 - 0002-00000000	00		0002-00000000001	0002-0000000000A
	root	4.4449			ool Platinum-Compute-UUID	Platinum-Compute-UUID	E832BCBA-DFAA-11E1		
B	🗄 🎪 Sub-Organ	izations		L.	[0001-00000000001 - 0001-00000000	00		0001-00000000001	0001-0000000000A
e- 🔊 Po									
<u>⊞-\</u>	root								
e 📀 Po	oois root								
	Server Por	aks							
	UUID Suffi								
E	🗄 👬 Sub-Organ	izations							
	🗄 🛕 Marke	ting							
	E 🙏 Tenan	tA rver Pools							
		ID Suffix Pools							
		b-Organizations							
	🗉 🙆 Windo								
🗄 🚮 Sc	chedules								

#### Figure 58 Summary of all the UUID Pools created

### **Creating a MAC Address Pool**

To configure the necessary MAC address pool for the Cisco UCS environment, follow these steps:

#### **Platinum-Compute-MAC**

Login to the Cisco UCS Manager with User Tenant A-Admin created earlier for Organization Tenant A.

1

- 1. Click the LAN tab in the left pane.
- 2. Choose Pools > Sub Organization.
- 3. Expand Sub-Organization and click TenantA.
- 4. Right-click MAC Pools under the root organization.
- 5. Select Create MAC Pool to create the MAC address pool.



#### Figure 59 Creating the MAC Pool for MAC Addresses

- 6. Enter MAC\_Pool as the name of the MAC pool.
- 7. (Optional) Enter a description of the MAC pool.
- 8. Click Next.



Figure 60 Adding Name and Description to MAC Pool

- 10. Specify a starting MAC address.
- **11**. Specify 10 size of the MAC address pool.





#### Figure 61 Setting the Block Size for the MAC Address Pool

12. Click OK.

ſ

- 13. Click Finish.
- 14. In the message box that displays, click **OK**.

Follow the steps described above to create MAC Pool for Gold, Silver, and Bronze service classes as per the MAC and Size noted in Table 11.

 Table 11
 Block Size and ID for the MAC Pool

UUID Pool Name	UUID ID	Size
Platinum-Compute-UUID	00:25:B5:01:00:00	10
Gold-Compute-UUID	00:25:B5:01:00:00	10
Silver-Compute-UUID	00:25:B5:02:00:00	10
Bronze-Compute-UUID	00:25:B5:03:00:00	10



#### Figure 62 Summary of all the MAC Pools Created

### **Creating WWNN Pools**

To configure the necessary WWNN pools for the Cisco UCS environment, follow these steps:

#### **Platinum-Compute-WWNN**

Login to Cisco UCS Manager with User TenantA-Admin created earlier for Organization TenantA:.

I

- 1. Click the SAN tab in the left pane.
- 2. Choose **Pools > Sub-Organization.** Expand TenantA.
- 3. Right-click WWNN Pools.
- 4. Select Create WWNN Pool.

#### Figure 63 Creating the WWNN Pools



- 5. Enter Platinum-Compute-WWNN as the name of the WWNN pool.
- **6.** (Optional) Add a description for the WWNN pool.
- 7. Click Next to continue.

- 🔾 🍈 💷 New 🕞 Options 🥝 🕕 🧥 Pending Activities 🔯 Exit  $\otimes$ V <u>ک</u> >> 🚍 SAN \* 🛞 Pools \* 🙏 root \* 🙏 Sub-Organizations \* 📩 TentantA \* 🛞 WWNN Pools 2 42 18 WWNN Pools Equipment Servers LAN SAN VM Admin 🛨 🖃 🕰 Filter 👄 Export 😸 Print Filter: All -Na + -E-E SAN SAN Cloud Eac Fabric A
   Eac Fabric B
   Threshold Policies 🗧 Create WWNN Pool × **Unified Computing System Manager** Storage Cloud E E Fabric A **Define Name and Description** 0 reate WWNN Pool 🗄 🗮 VSANs 1. ✓<u>Define Name and</u> Description 2. □<u>Add WWN Blocks</u> E-S Policies E O SAN Cloud Name: Platinum-Compute-WWNN - S Threshold Policies E A root Description: S Default vHBA Behavior Assignment Order: 
   Default 
   Sequential E Sibre Channel Adapter Policies SAN Connectivity Policies Storage Connection Policies Threshold Policies VHBA Templates E A Sub-Organizations Pools E A root IQN Pools • WWPN Pools WWXN Pools A Sub-Organizations 🗛 Marketing Next > Finish Cancel < Prev 🛕 TenantA IQN Pools WWNN Pools WWPN Pools WWXN Pools Traffic Monitoring Sessions
- Figure 64 Defining the Name and Description for the WWNN Pool

- 8. Click Add to add a block of WWNNs 20:00:00:25:B5:01:00:00.
- **9.** Specify size of 10 WWNN block. Ensure that there are sufficient number of blade resources is available.

1



#### Figure 65 Specifying the Size to the WWN Block Created

- **10**. Click **OK** to proceed.
- 11. Click Finish to proceed.
- 12. Click **OK** to finish.

ſ

Follow the same steps above to create WWNN Pool for Gold-Compute-WWNN, Silver-Compute-WWNN and Bronze-Compute-WWNN with below WWNN and Size noted in Table 12.

 Table 12
 UUID IDs and Size for all the Service Classes

UUID Pool Name	UUID ID	Size
Platinum-Compute-WWNN	20:00:00:25:B5:01:00:00	10
Gold-Compute-WWNN	20:00:00:25:B5:02:00:00	10
Silver-Compute-WWNN	20:00:00:25:B5:03:00:00	10
Bronze-Compute-WWNN	20:00:00:25:B5:04:00:00	10



#### Figure 66 Summary of all the WWNN Pools Created

### **Creating WWPN Pools**

To configure necessary WWNN pools for the Cisco UCS environment, follow these steps:

#### **Platinum-Compute-WWPN**

Login to Cisco UCS Manager with User TenantA-Admin which was created earlier for Organization TenantA

- 1. Click the SAN tab in the left pane.
- 2. Choose **Pools > Sub-Organization**. Expand TenantA.
- 3. Right-click WWPN Pools.
- 4. Select Create WWPN Pool.

#### Cisco Unified Computing System Manager - TME-L21 ult Su n' Y 0 $\bigotimes$ V ▲ <u>ک</u> 3 18 2 42 >> w Equipment Servers LAN SAN VM Admin Θ Filter: All Ŧ • = SAN SAN Cloud SAN Cloud SAN Cloud SAN Cloud SAN Pin Groups Shart C B SAN Pin Groups Sorage Cloud Sora 🗄 🧔 SAN Cloud H- S Threshold Policies E A root SAN Connectivity Policies Storage Connection Policies Threshold Policies 🗄 👬 Sub-Organizations A Pools 🗄 🛕 root E WWNN Pools WWPN Pools Ė A Sub-Organization 🛕 Marketing 🛕 TenantA IQN Pools WWPN Pools Show Navigator WWXN Pools Create WWPN Pool ė Z Traffic Monitoring Sessions

#### Figure 67 Selecting Create WWPN Pool option

- 5. Enter Platinum-Compute-WWPN as the name of the WWPN pool.
- 6. (Optional) Add a description for the WWPN pool.
- 7. Click Next to continue.



Figure 68 Adding the Name and Description for the WWPNN Pool

- 8. Click Add to add a block of WWNNs 20:00:25:B5:01:01:00.
- 9. Specify a size of 10 WWNN block (Ensure that sufficient number of blade resources is available).

1



#### Figure 69 Defining the Size of the WWN Block

- 10. Click **OK** to proceed.
- 11. Click Finish to proceed.
- 12. Click **OK** to finish.

ſ

Follow the same steps above to create WWPN Pool for Gold-Compute-WWPN, Silver-Compute-WWPN and Bronze-Compute-WWPN with below WWNN and Size noted in Table 13.

Table 13WWPN UUID Pool name and ID

UUID Pool Name	UUID ID	Size
Gold-Compute-WWPN	20:00:00:25:B5:02:01:00	10
Silver-Compute-WWPN	20:00:00:25:B5:03:01:00	10
Bronze-Compute-WWPN	20:00:00:25:B5:04:01:00	10

🍦 Cisco Unified Computing System Manager - TME-L21					
Fault Summary	🚱 🍥 💷 New - 🎴 Options 🛛 🚱 🚯 Pending Ac	tivities Fxit			
🛛 🔇 🔽 🛆 🔬					
2 42 3 18	>> 🗏 SAN ' 🛞 Pools ' 🙏 root ' 🙏 Sub-Organizations ' 🙏	TentantA 🕨 🎯 WWPN Pools			
Equipment Servers LAN SAN VM Admin	WWPN Pools				
Filter: All	💼 🚍 🕰 Filter 👄 Export 踜 Print				
	Name		Size		Assigned
± =	WWPN Pool Bronze-Compute-WWPN	10		0	
E- = SAN	[20:00:00:25:B5:04:01:00 - 20:00:00:25:B5:04:01:09]				
🛱 🍊 SAN Cloud		10		0	
🕀 🌆 Fabric A	[20:00:00:25:85:02:01:00 - 20:00:00:25:85:02:01:09]				
🕀 💷 Fabric B	WWPN Pool Platinum-Compute-WWPN	10		1	
== SAN Pin Groups ⊕ S Threshold Policies	[20:00:00:25:85:01:01:00 - 20:00:00:25:85:01:01:09]				
	WWPN Pool Silver-Compute-WWPN	10		0	
- O Storage Cloud	[20:00:00:25:85:03:01:00 - 20:00:00:25:85:03:01:09]				
🕀 🎫 Fabric A					
🕀 🔤 Fabric B					
🗄 🚍 VSANs					
E S Policies					
E-O SAN Cloud					
Threshold Policies					
E-A root					
🗐 Default vHBA Behavior 					
SAN Connectivity Policies					
Storage Connection Policies					
Storage Connection Policies					
VHBA Templates					
Sub-Organizations					
E - OP Pools					
A root					
IQN Pools					
🕀 🎯 WWNN Pools					
🖶 💮 WWPN Pools					
Sub-Organizations					
🖽 🧟 Marketing					
E A TentantA					
I QN Pools					
E WWNN Pools					
WWPN Pool Bronze-Compute-Wi					
WWPN Pool Gold-Compute-WWP					
WWPN Pool Platinum-Compute-W					
WWPN Pool Silver-Compute-WW					
- 💮 WWxN Pools					
🚽 🂑 Sub-Organizations					
∰ Mindows2012					
Image: Traffic Monitoring Sessions					

#### Figure 70 Summary of all the four compute UUID Pools

### **Creating IP Pools**

To configure the necessary IP Management pools for the Cisco UCS environment, follow these steps:

1

1

#### **Platinum-Compute-IP**

Login to Cisco UCS Manager with User TenantA-Admin created earlier for Organization TenantA:.

- **1**. Click the **LAN** tab in the left pane.
- 2. Choose Pools > Sub-Organization.
- 3. Expand TenantA.
- 4. Right-click IP Pools.
- 5. Select Create IP Pool.

#### Cisco Unified Computing System Manager - TME-L21 Fault Sum ar y 0 $\bigotimes$ V <u>ک</u> 3 ⚠ 42 18 2 >> IP Equipment Servers LAN SAN VM Admin ± Filter: All • • = E-E LAN LAN Cloud LAN Cloud Lan Cloud Lan Fabric A Fabric B Lan Flabric B LAN Pin Groups LAN Pin Groups VLAN Groups VLAN Groups VLAN Groups Anniances Appliances 南 Appliances Appliances Internal LAN S Policies Appliances Appliances Appliances Appliances Appliances Appliances Appliances Appliances Pools Pools root IP Pools MAC Pool MAC Pools ė Sub-Organization Marketing TenantA Show Navigator MAC P Sub-On Create IP Pool ė 🛕 dows20 Traffic Monitoring Sessions

#### Figure 71 Creating IP Pools for the Storage

- 6. Enter Platinum-Compute-IP as the name of the IP pool.
- 7. (Optional) Add a description for the IP pool.
- 8. Click Next to continue.



Figure 72 Defining the Name and Description to the IP Pool

- 9. Click Add to add a block of IP 10.65.121.50.
- **10.** Specify a size of 10 IP block.

Ensure that sufficient number of blade resources are available.

Specifying the IP Addresses and the Block Size and the DNS

11. Click **OK** to proceed.

Note

- 12. Click Finish to proceed.
- 13. Click OK to finish.

Follow the steps described above to create IP Pool for Gold-Compute-IP, Silver-Compute-IP and Bronze-Compute-IP with WWPN and Size noted in Table 14.

Table 14WWPN and Size for all UUID Pools

UUID Pool Name	UUID ID	Size
Platinum-Compute-WWPN	10.65.121.50	10
Gold-Compute-WWPN	10.65.121.61	10
Silver-Compute-WWPN	10.65.121.71	10
Bronze-Compute-WWPN	10.65.121.81	10

I
Cisco Unified Computing System Manager - TME-L21					
Fault Summary	🕒 🍥 🗳 New - 🛛 🖓 Qptions 🛛 🥹 🕕 🖓 Pending Ac	tivities 🚺 🚺 Exit			
	h de la companya de la				
2 42 3 18	>> = LAN '  Pools '  root '  Sub-Organizations '  IP Pools	TentantA * 19 Pools			
Equipment Servers LAN SAN VM Admin					
Filter: All	🛨 🖃 🕰 Filter 👄 Export 😸 Print				
• •	Name		Size		Assigned
	IP Pool Bronze-Compute-IP	10		0	
E CAN	[10.65.121.71 - 10.65.121.80]				
E - Eabric A	Den IP Pool Gold-Compute-IP	10		0	
Fabric B	[10.65.121.61 - 10.65.121.70]	10		3	
	[10.65.121.50 - 10.65.121.59]	10		3	
LAN Pin Groups     S Threshold Policies	E-W IP Pool Silver-Compute-IP	10		0	
ULAN Groups	10.65.121.71 - 10.65.121.80]			-	
H VLANS					
🕀 🙆 Appliances					
Internal LAN					
E-O LAN Cloud					
S Threshold Policies					
E A root					
⊖ ∲ Pools ⊖ Å root					
E B Pools					
IP Pools     MAC Pools					
E & Sub-Organizations					
A Marketing					
⊡Å, TenantA ⊕-₩₩ [P Pools					
MAC Pools					
- A Sub-Organizations					
Irarric monicoring bessions					

## Figure 73 Summary of all the IP Pools Created

**Creating vNIC and vHBA Template** 

Cisco Cisco UCS Manager provides templates for the primary objects (vNICs and vHBAs) to facilitate reuse and rapid deployment. The vNIC and vHBA resources are always associated with specific FIs (A-side or B-side fabric interconnect) one bound to each side. vNIC (or vHBA) templates can be used to encapsulate both the MAC address pool (or WWPN pool) association.

In this study we will create two sets of vNIC and vHBA templates for Baremetal and Virtual Hosts Service Profile templates.

Note

Create six vNIC templates for handling Management, Application, NFS and vMotion LAN traffic and two vHBA templates for handling SAN traffic to run VMWare ESXi 5.1 hypervisor host for running Virtual Machines on TenantA Zone.

## **Creating vNICS Templates**

This section details the creation off vNIC templates created for BareMetal and VMware ESXi Hosts on Fabric A and Fabric B.

Login to Cisco UCS Manager with User TenantA-Admin created earlier for Organization TenantA::

- 1. Click the LAN tab in the left pane.
- 2. Choose Pools > Sub-Organization.
- 3. Expand TenantA.
- 4. Select vNIC Templates and right click Create vNIC Template.



Figure 74 Creating vNIC Template

- 5. Create vNIC Template window opens.
- 6. Enter Management-A-NIC in the Name field.
- 7. Enter Management Template in the Description filed.
- 8. In Fabric ID click FabricA radio button, do not check Enable Failover check box.
- 9. In Target check Adapater check box.
- 10. In Template Type select Initial Template radio button.
- 11. Under VLANs check Management-VLAN, vMotion-VLAN check box, and choose Native VLAN as Management-VLAN.

- 12. In the MTU field enter 9000.
- 13. Select Platinum-Compute-MAC pool from the MAC Address Assignment list box.
- 14. Select Silver-Net-SLA in QoS Policy list box.
- 15. Select default in Network Control Policy list box.
- 16. Select <not set> in Pin Group list box.
- 17. Select default in Stats Thershold Policy list box.
- 18. Select <not set> in Dynamic vNIC Connection Policy list box.
- 19. Click OK.

	Create vNIC	: Template		×
reate vNIC Te	emplate			0
1	Name: Managment-A-NIC			
Descri	0 ption: Managment Template		_	
Fabr	ric ID: 💿 Fabric A 🕓 Fabric B 🗍	Enable Failover		
	Target			
	Adapter			
	VM			
Template	Type: 💿 Initial Template 🔵 Upd	lating Template		
VLANs				
	Name	Native VLAN	Ę	
VLANs	Name Managment-VLAN	Native VLAN	<b>P</b>	
VLANs Select	Managment-VLAN NFS-VLAN		^	
VLANs Select	Managment-VLAN NFS-VLAN VLAN-Guest-VLAN-1001			
VLANs Select	Managment-VLAN NFS-VLAN		^	
VLANs Select	Managment-VLAN NFS-VLAN VLAN-Guest-VLAN-1001		^	
VLANS Select	Managment-VLAN NFS-VLAN VLAN-Guest-VLAN-1001 vMotion-VLAN		^	
VLANS Select	Managment-VLAN NFS-VLAN VLAN-Guest-VLAN-1001 vMotion-VLAN		^	
VLANS Select Create VLAN Warning Make sure that the MTU h	Managment-VLAN NFS-VLAN VLAN-Guest-VLAN-1001 vMotion-VLAN	m Class	^	
VLANS Select Create VLAN Warning Make sure that the MTU h corresponding to the Egre	Managment-VLAN NFS-VLAN VLAN-Guest-VLAN-1001 VMotion-VLAN MTU: 9000 as the same value in the QoS System ss priority of the selected QoS Policy Pool: Platinum-Compute-MAC(15).	m Class	^	
VLANS Select	Managment-VLAN NFS-VLAN VLAN-Guest-VLAN-1001 VMotion-VLAN MTU: 9000 as the same value in the QoS System spriority of the selected QoS Policy Pool: Platinum-Compute-MAC(15).	m Class	^	
VLANS Select Create VLAN Warning Make sure that the MTU h corresponding to the Egre MAC Qos F	Managment-VLAN NFS-VLAN VLAN-Guest-VLAN-1001 VMotion-VLAN MTU: 9000 as the same value in the QoS System spriority of the selected QoS Policy Pool: Platinum-Compute-MAC(15). Silver-Net-SLA	m Class	^	
VLANS Select Create VLAN Warning Make sure that the MTU h corresponding to the Egre QoS F Network Control F	Managment-VLAN NFS-VLAN VLAN-Guest-VLAN-1001 VMotion-VLAN MTU: 9000 as the same value in the QoS System spriority of the selected QoS Policy Pool: Platinum-Compute-MAC(15/, Policy: Silver-Net-SLA	m Class	^	
VLANS Select Create VLAN Warning Make sure that the MTU h corresponding to the Egre QoS F Network Control F Pin G	Managment-VLAN NFS-VLAN VLAN-Guest-VLAN-1001 VMotion-VLAN MTU: 9000 as the same value in the <u>QoS Syster</u> spriority of the selected QoS Policy Poolicy Silver-Net-SLA Policy: Silver-Net-SLA Policy: default Constraints	m Class	^	
VLANS Select Create VLAN Warning Make sure that the MTU h corresponding to the Egre QoS F Network Control F	Managment-VLAN NFS-VLAN VLAN-Guest-VLAN-1001 VMotion-VLAN MTU: 9000 as the same value in the <u>QoS Syster</u> spriority of the selected QoS Policy Poolicy Silver-Net-SLA Policy: Silver-Net-SLA Policy: default Constraints	m Class	^	

#### Figure 75 Defining the vNIC Properties for Management A-NIC

- 20. Create vNIC Template window opens.
- 21. Enter Management-B-NIC in the Name field.
- 22. Enter Management Template in the Description field.
- 23. In Fabric ID click FabricB radio button, do not check Enable Failover check box.
- 24. In Target check Adapater check box.
- 25. In Template Type select Initial Template radio button.
- **26.** Under VLANs check Management-VLAN, vMotion-VLAN check box, and choose Native VLAN as Management-VLAN.
- **27.** In the **MTU** field enter 9000.

- 28. Select Platinum-Compute-MAC pool from the MAC Address Assignment list box.
- 29. Select Silver-Net-SLA in QoS Policy list box.
- 30. Select default in Network Control Policy list box.
- 31. Select <not set> in Pin Group list box.
- 32. Select default in Stats Thershold Policy list box.
- **33.** Select **<not set>** in **Dynamic vNIC Connection Policy** list box.

## 34. Click OK.

Create vNIC Template	2	Creat	e vNIC Templa	te		x
Name: Managment-B-NIL   Description: Fabric A <ul> <li>Fabric D:</li> <li>Pabric A          <ul> <li>Fabric B          <li>Enable Failover</li> </li></ul> </li> <li> Warning If YM is selected, a port profile by the same name will be created. If YM is selected, a port profile by the same name will be created. If a port profile of the same name exists, and updating template is selected, it will be overwritten Template Type: <ul> <li>Initial Template</li> <li>Updating Template</li> </ul> </li> <li> VLANS Select <ul> <li>Name</li> <li>Native VLAN</li> <li>Network Control Policy:</li> <li>Of Fault</li> <li>Os Policy:</li> <li>Sitver-Net-SLA</li> <li>Discrete VLAN</li> <li>On selected</li> <li>Pin Group:</li> <li>In Group:<th>Create vNIC</th><th>Template</th><th></th><th></th><th></th><th>0</th></li></ul></li></ul>	Create vNIC	Template				0
Description:   Fabric II:   Fabric II:   Target   Adapter   VM      If MM is selected, a port profile by the same name will be created. If a port profile of the same name exists, and updating template is selected, it will be overwritten Template Type: <ul> <li>Initial Template</li> <li>Updating Template</li> </ul> VLANS   Select   NPS-VLAN   NPS-VLAN   NPS-VLAN   VLAN-Guest-VLAN   VLAN-Guest-VLAN   VLAN-Guest-VLAN   Warning   Make sure that the MTU has the same value in the QoS System Class corresponding to the Egress priority of the selected QoS Policy:   Silver-Net-SLA   Network Control Policy:   default   Pin Group:   cost est>   Stats Threshold Policy:			4			^
Pabric ID: Fabric A  Fabric B  Enable Falover     Iarget     I Adapter        If MM is selected, a port profile by the same name will be created.   If a port profile of the same name exists, and updating template is selected, it will be overwritten   Template Type: <ul> <li>Initial Template</li> <li>Updating Template</li> </ul> VLANS   Select Name   NFS-VLAN   NFS-VLAN   NFS-VLAN   NFS-VLAN   NFS-VLAN   VLAN-Guest-VLAN-1001   VLAN-Guest-VLAN-1001   VLAN-Guest-VLAN-1001   VLAN-Guest-VLAN-1001   Varning   Mate sure that the MTU has the same value in the Q05 System Class   corresponding to the Egress priority of the selected Q05 Pokey.   MAC Pool:   Platinum-Compute-MAC(15/)   QoS Policy:   Silver-Net-SLA   Pin Group:   Coto set>   Stats Threshold Policy:   default	Des	<u></u>				
Warning   If VM is selected, a port profile by the same name will be created.   If a port profile of the same name exists, and updating template is selected, it will be overwritten   Template Type:   Initial Template   Updating Template   VLANs   Select   Managment-VLAN   Managment-VLAN   Managment-VLAN   VLANs   Select   Managment-VLAN   VLAN-Guest-VLAN   VLAN-Guest-VLAN   Vulai-Guest-VLAN   V						
Target         Waning         If VM is selected, a port profile by the same name will be created.         If a port profile of the same name exists, and updating template is selected, it will be overwritten         Template Type:         Initial Template         VLANs         Select         Name         NFS-VLAN         NFS-VLAN         NFS-VLAN         VLANs-Guest-VLAN         VLAN-Guest-VLAN         VLAN-Guest-VLAN         VLAN-Guest-VLAN         VLAN-Guest-VLAN         Vtaining         Make sure that the MTU has the same value in the QoS System Class corresponding to the Egress priority of the selected QoS Policy.         MAC Pool:       Platinum-Compute-MAC(15/ ▼         QoS Policy:       Silver-Net-SLA ▼         Network Control Policy:       default         Pin Group:          Stats Threshold Policy:       default	F		pric B Enable Fai	lover		
Warning   If VM is selected, a port profile by the same name will be created.   If a port profile of the same name exists, and updating template is selected, it will be overwritten   Template Type:   Initial Template   VLANs   Select   Name   Nanagment-VLAN   NFS-VLAN   NFS-VLAN   Ntu:   YLANs   Select   Name   Nanagment-VLAN   On the same name exists, and updating template   VLANs   Select   Name   Nanagment-VLAN   On the same name exists, and updating template   VLANs   Select   Name   Native VLAN   Image:   Mut:   9000   Warning Make sure that the MTU has the same value in the QoS System Class Corresponding to the Egress priority of the selected QoS Policy. MAC Pool: Platinum-Compute-MAC(15/ * QoS Policy: Silver-Net-SLA * Network Control Policy: default This Group: Cont set> Stats Threshold Policy: default This Group: Stats Threshold Policy: default This Group: State		Target		7		
Warning         If VM is selected, a port profile by the same name will be created.         If a port profile of the same name exists, and updating template is selected, it will be overwritten         Template Type:       Initial Template         VLANs         Select       Name         WARNS         Select       Name         WAN-Guest-VLAN       Image: Comparent of the same name exists, and updating template         VLANs       Image: Comparent of the same name exists, and updating template is selected, it will be overwritten         Image: Comparent of the same name exists, and updating template is selected, it will be overwritten         Image: Comparent of the same name exists, and updating template is selected, it will be overwritten         Image: Comparent of the same name exists, and updating template is selected, it will be overwritten         Image: Comparent of the same name exists, and updating template         Image: Comparent of the same name exists, and updating template         Image: Comparent of the same name exists, and updating template         Image: Comparent of the same name exists, and updating template         Image: Comparent of the same name exists, and updating template         Image: Comparent of the same name exists, and updating template         Image: Comparent of the same name exists, and updating template         Image: Comparent of the same name exists, and updating template						
If VM is selected, a port profile by the same name will be created. If a port profile of the same name exists, and updating template is selected, it will be overwritten Template Type: Initial Template Updating Template VLANS Select Name Native VLAN Managment-VLAN NFS-VLAN VLAN-Guest-VLAN-1001 VLAN-Guest-VLAN-1001 Create VLAN MTU: S000 Warning Make sure that the MTU has the same value in the QoS System Class corresponding to the Egress priority of the selected QoS Policy. MAC Pool: Platinum-Compute-MAC(15/ QoS Policy: Silver-Net-SLA Network Control Policy: default Pin Group: cnot set> Stats Threshold Policy: default						
If VM is selected, a port profile by the same name will be created. If a port profile of the same name exists, and updating template is selected, it will be overwritten Template Type: Initial Template Updating Template VLANS Select Name Native VLAN Managment-VLAN NFS-VLAN VLAN-Guest-VLAN-1001 VLAN-Guest-VLAN-1001 Create VLAN MTU: S000 Warning Make sure that the MTU has the same value in the QoS System Class corresponding to the Egress priority of the selected QoS Policy. MAC Pool: Platinum-Compute-MAC(15/ QoS Policy: Silver-Net-SLA Network Control Policy: default Pin Group: cnot set> Stats Threshold Policy: default						
If a port profile of the same name exists, and updating template is selected, it will be overwritten  Template Type: Initial Template Updating Template VLANS Select Name Native VLAN  Select Name Native VLAN  Managment-VLAN  NFS-VLAN  NFS-VLAN  VLAN-Guest-VLAN-1001 VLAN-Guest-VLAN-1001 VLAN-Guest-VLAN  TU: 9000 Warning Make sure that the MTU has the same value in the QoS System Class corresponding to the Egress priority of the selected QoS Policy. MAC Pool: Platinum-Compute-MAC(15/  QoS Policy: Silver-Net-SLA Pin Group: Cont set> Stats Threshold Policy: default	Warning	<u> </u>				
Template Type: Initial Template   VLANs   Select   Managment-VLAN   NFS-VLAN   VLAN-Guest-VLAN-1001   VLAN-Guest-VLAN-1001   VLAN-Guest-VLAN   VLAN-Guest-VLAN   VLAN-Guest-VLAN   VLAN-Guest-VLAN						
VLANs         Select       Name         Managment-VLAN         NFS-VLAN         VLAN-Guest-VLAN-1001         VLAN-Guest-VLAN-1001         V         VMotion-VLAN         V         Warning         MAke sure that the MTU has the same value in the QoS System Class corresponding to the Egress priority of the selected QoS Policy.         MAKe sure that the MTU has the same value in the QoS System Class corresponding to the Egress priority of the selected QoS Policy.         MAC Pool:       Platinum-Compute-MAC(15/          QoS Policy:       Silver-Net-SLA          Network Control Policy:       default         Pin Group:       cnot set>         Stats Threshold Policy:       default	If a port profile of the	same name exists, and updatir	ng template is selecti	ed, it will be overw	vritten	
Select       Name       Native VLAN       Image: Select VLAN         Image: Managment-VLAN       Image: Select VLAN       Image: Select VLAN         Image: VLAN-Guest-VLAN-1001       Image: Select VLAN       Image: Select VLAN         Image: VLAN       Image: Select VL	Templa	ate Type: 💿 Initial Template	O Updating Temp	late		
Image: Management-VLAN       Image: Management-VLAN         Image: Management-VLAN       Image: Management-VLAN         Image: With VLAN-Guest-VLAN-1001       Image: Management-VLAN         Image: With VLAN-Guest-VLAN       Image: Management-VLAN         Image: Management-VLAN       Imagement-VLAN         Imagement-VLA	VLANs					
NFS-VLAN         VLAN-Guest-VLAN-1001         VLAN-Guest-VLAN-1001         Image: Vertical and the second seco	Select	Name	Native	VLAN	<b>₽</b>	=
↓       VLAN-Guest-VLAN-1001       ■         ↓       VMotion-VLAN       ↓         ↓       Ymotion-VLAN       ↓         ↓       ↓       ↓         ↓       ↓       ↓         ↓       ↓       ↓         ↓       ↓       ↓         ↓       ↓       ↓         ↓       ↓       ↓         ↓       ↓       ↓	<ul> <li>Image: A start of the start of</li></ul>	Managment-VLAN		۲	^	
Image: Create VLAN       Image: VMotion-VLAN         Image: Create VLAN       Image: VMotion-VLAN         Mark: Sure that the MTU has the same value in the QoS System Class corresponding to the Egress priority of the selected QoS Policy.         MAC Pool:       Platinum-Compute-MAC(15/          QoS Policy:       Silver-Net-SLA         Network Control Policy:       default         Pin Group:       Cnot set>         Stats Threshold Policy:       default		NFS-VLAN		0		
Create VLAN  MTU: 9000  Warning  Make sure that the MTU has the same value in the QoS System Class corresponding to the Egress priority of the selected QoS Policy.  MAC Pool: Platinum-Compute-MAC(15/  QOS Policy: Silver-Net-SLA  QOS Policy: Silver-Net-SLA  Network Control Policy: default  Pin Group: <pre>cnot set&gt;</pre> Stats Threshold Policy: default			001		=	
MTU: 9000 Warning Make sure that the MTU has the same value in the QoS System Class corresponding to the Egress priority of the selected QoS Policy. MAC Pool: Platinum-Compute-MAC(15/ QoS Policy: Silver-Net-SLA QoS Policy: Silver-Net-SLA Network Control Policy: default Pin Group: <a href="https://www.cont.selected">www.control Policy</a> Stats Threshold Policy: default	✓	vMotion-VLAN		0	~	
MTU: 9000 Warning Make sure that the MTU has the same value in the QoS System Class corresponding to the Egress priority of the selected QoS Policy. MAC Pool: Platinum-Compute-MAC(15/ QoS Policy: Silver-Net-SLA QoS Policy: Silver-Net-SLA Network Control Policy: default Pin Group: cnot set> Stats Threshold Policy: default	Teate VLAN					
Warning         Make sure that the MTU has the same value in the QoS System Class corresponding to the Egress priority of the selected QoS Policy.         MAC Pool:       Platinum-Compute-MAC(15/ ▼         QoS Policy:       Silver-Net-SLA ▼         Network Control Policy:       default ▼         Pin Group:          Stats Threshold Policy:       default ▼		MTU: 9000				
Make sure that the MTU has the same value in the QoS System Class corresponding to the Egress priority of the selected QoS Policy. MAC Pool: Platinum-Compute-MAC(15/ ▼ QoS Policy: Silver-Net-SLA ▼ Network Control Policy: default ▼ Pin Group: cnot set> ▼ Stats Threshold Policy: default ▼	Warning					
corresponding to the Egress priority of the selected QoS Policy. MAC Pool: Platinum-Compute-MAC(15/ QoS Policy: Silver-Net-SLA Network Control Policy: default Pin Group: <not set=""> Stats Threshold Policy: default</not>		U has the same value in the O	oS System Class			
QoS Policy: Silver-Net-SLA Network Control Policy: default Pin Group: cnot set> Stats Threshold Policy: default						
QoS Policy: Silver-Net-SLA  Network Control Policy: default Pin Group: <not set=""> Stats Threshold Policy: default</not>	N	IAC Pool: Platinum-Compute-I	MAC(15/ 🔽			
Network Control Policy: default  Pin Group: <not set=""> Stats Threshold Policy: default</not>		0	<b>T</b>			
Pin Group: <not set="">  Stats Threshold Policy: default</not>		0	-			
Stats Threshold Policy: default		0				
			•			
OK Cancel	Stats Thresho	old Policy: default	•			×

## Figure 76 Defining the vNIC Properties for Management- B-NIC

1

- 35. Create vNIC Template window opens.
- 36. Enter guest-A-NIC in the Name field
- **37**. Enter guest Template in the Description field.
- **38.** In **Fabric ID** click **FabricA** radio button, do not check **Enable Failover** check box.
- 39. In Target check Adapater check box.
- 40. In Template Type select Initial Template radio button.
- 41. Under VLANs check guest-VLAN, guest-VLAN-1000, VLAN-guest-VLAN-1001, and choose Native VLAN as guest-VLAN.
- 42. In the MTU field enter 9000.
- 43. Select Platinum-Compute-MAC pool from the MAC Address Assignment list box.
- 44. Select Platinum-Net-SLA in QoS Policy list box.
- 45. Select default in Network Control Policy list box.
- 46. Select <not set> in Pin Group list box.

- 47. Select default in Stats Thershold Policy list box.
- **48.** Select **<not set>** in **Dynamic vNIC Connection Policy** list box.
- 49. Click OK.

Figure 77 Defining the vNIC Properties for guest- A-NIC

Description:       Guest Template         Fabric ID:       Fabric A       Fabric B       Enable Failover         Target <ul> <li>Adapter</li> <li>VM</li> <li>VM</li> <li>Warning</li> <li>If yM is selected, a port profile by the same name will be created.</li> <li>If a port profile of the same name exists, and updating template is selected, it will be overwritten</li> <li>Template Type:</li> <li>Initial Template</li> <li>Updating Template</li> <li>VLANs</li> <li>Select</li> <li>Name</li> <li>Native VLAN</li> <li>Guest-VLAN</li> <li>Guest-VLAN</li> <li>Guest-VLAN</li> <li>MAN-Guest-VLAN-1001</li> <li>NFS-VLAN</li> <li>VLAN-Guest-VLAN-1001</li> <li>VLAN-Guest-VLAN-1001</li> <li>VLAN-Guest-VLAN-1001</li> <li>VLAN-Guest-VLAN-1001</li> <li>Imitial Template</li> <li>Imitial Templat</li></ul>			Create vNIC Tem	plate		x
Guest Template   Fabric ID:   Pabric A   Fabric B   Enable Failover     Target   Adapter   YM     Warning   If YM is selected, a port profile by the same name will be created.   If a port profile of the same name exists, and updating template is selected, it will be overwritten   Template Type:   Initial Template   Updating Template   Select   Name   Native VLAN   Guest-VLAN   Guest-VLAN   Guest-VLAN   VLANs     Select   Name   Native VLAN     Guest-VLAN     Or Guest-VLAN     Warning   Mace sure that the MTU has the same value in the QoS System Class   corresponding to the Egress priority of the selected QoS Policy.     MacPool:   Platinum-Compute-MAC(15/ •   QoS Policy:   Platinum-Compute-MAC(15/ •   QoS Policy:   Platinum-Compute-MAC(15/ •   Network Control Policy:      In Group:	reate vNI	IC Temp	late			0
Description: Guest Template   Fabric ID: Pabric A   Fabric ID: Pabric ID:						^
Target         Adapter         YM         If YM is selected, a port profile by the same name will be created.         If a port profile of the same name exists, and updating template is selected, it will be overwritten         Template Type:       Initial Template         UPdating Template       Updating Template         VLANs       Image: Select         Select       Name         Image: Guest-VLAN       Image: Select VLAN         Image: Guest-VLAN-1000       Image: Select VLAN         Image: Guest-VLAN       Image: Select VLAN         Image: Guest: VLAN       Image: Select VLAN         Image: Guest: VLAN       Image: Select VLAN         Image: Guest: VLAN       Image: Select VLAN         Image: Make sure that the MTU has the same value in the Qood System Class       Image: Select S			2			
Target         Adapter         YM         If YM is selected, a port profile by the same name will be created.         If a port profile of the same name exists, and updating template is selected, it will be overwritten         Template Type:       Initial Template         UPdating Template       Updating Template         VLANs       Image: Select         Select       Name         Image: Guest-VLAN       Image: Select VLAN         Image: Guest-VLAN-1000       Image: Select VLAN         Image: Guest-VLAN       Image: Select VLAN         Image: Guest: VLAN       Image: Select VLAN         Image: Guest: VLAN       Image: Select VLAN         Image: Guest: VLAN       Image: Select VLAN         Image: Make sure that the MTU has the same value in the Qood System Class       Image: Select S		Eshvis TDu	Eabric 0 Cabric B E	nable Failover		
Warning   If VM is selected, a port profile by the same name will be created.   If a port profile of the same name exists, and updating template is selected, it will be overwritten   Template Type:   Initial Template   Updating Template   VLANs   Select   Name   Native VLAN   Image: Select VLAN		Fabric ID;				
If VM is selected, a port profile by the same name will be created. If a port profile of the same name exists, and updating template is selected, it will be overwritten Template Type: Initial Template Updating Template VLANS Select Name Native VLAN I Guest-VLAN I Guest-VLAN I VLAN-Guest-VLAN-1000 I VLAN-Guest-VLAN-1001 I NFS-VLAN I Create VLAN MTU: 9000 Warning Make sure that the MTU has the same value in the QoS System Class corresponding to the Egress priority of the selected QoS Policy. MAC Pool: Platinum-Compute-MAC(15/ • QoS Policy: Platinum-Net-SLA • Network Control Policy: <not set=""> Pin Group: <not set=""></not></not>			✓ Adapter			
If VM is selected, a port profile by the same name will be created. If a port profile of the same name exists, and updating template is selected, it will be overwritten Template Type: Initial Template Updating Template VLANS Select Name Native VLAN I Guest-VLAN I Guest-VLAN I VLAN-Guest-VLAN-1000 I VLAN-Guest-VLAN-1001 I NFS-VLAN I Create VLAN MTU: 9000 Warning Make sure that the MTU has the same value in the QoS System Class corresponding to the Egress priority of the selected QoS Policy. MAC Pool: Platinum-Compute-MAC(15/ • QoS Policy: Platinum-Net-SLA • Network Control Policy: <not set=""> Pin Group: <not set=""></not></not>						
Select Name Native VLAN Guest-VLAN Guest-VLAN Guest-VLAN-1000 VLAN-Guest-VLAN-1001 From VLAN-Guest-VLAN-1001 From VLAN MTU: 9000 Warning Make sure that the MTU has the same value in the QoS System Class corresponding to the Egress priority of the selected QoS Policy. MAC Pool: Platinum-Compute-MAC(15/ QoS Policy: Platinum-Net-SLA Network Control Policy: Crot set > Pin Group: Crot set > Vanta Selected Cos System Class	If a port profile ol	f the same nam	e exists, and updating template i	s selected, it will be overwritt	en	
✓       Guest-VLAN       ●         ✓       Guest-Vlan-1000       ●         ✓       VLAN-Guest-VLAN-1001       ●         ●       NF5-VLAN       ●         ●       NF5-VLAN       ●         ●       NF5-VLAN       ●         ●       NF1       9000         ●       ●       ●      <	VLANs					
Guest-Vlan-1000	Select			Native VLAN	<b>₽</b>	
VLAN-Guest-VLAN-1001       Image: Comparison of the set of					^	
Create VLAN  MTU: 9000  Warning  Make sure that the MTU has the same value in the QoS System Class corresponding to the Egress priority of the selected QoS Policy.  MAC Pool: Platinum-Compute-MAC(15/  QoS Policy: Platinum-Net-SLA  QoS Policy: Platinum-Net-SLA  Network Control Policy: cnot set>  Pin Group: <not set=""></not>		-			- =	
Create VLAN  MTU: 9000  Warning  Make sure that the MTU has the same value in the QoS System Class corresponding to the Egress priority of the selected QoS Policy.  MAC Pool: Platinum-Compute-MAC(15/  QoS Policy: Platinum-Net-SLA  QoS Policy: Platinum-Net-SLA  Network Control Policy: cnot set>  Pin Group: <not set=""></not>		1			_=	
MTU: 9000 Warning Make sure that the MTU has the same value in the <u>QoS System Class</u> corresponding to the Egress priority of the selected QoS Policy. MAC Pool: Platinum-Compute-MAC(15/ • QoS Policy: Platinum-Net-SLA • Network Control Policy:						

- 50. Create vNIC Template window opens.
- 51. Enter guest-B-NIC in the Name field
- 52. Enter guest Template in the Description field.
- 53. In Fabric ID click FabricA radio button, do not check Enable Failover check box.
- 54. In Target check Adapater check box.
- 55. In Template Type select Initial Template radio button.
- 56. Under VLANs check guest-VLAN, guest-VLAN-1000, VLAN-guest-VLAN-1001, and choose Native VLAN as guest-VLAN.
- 57. In the MTU field enter 9000.

- 58. Select Platinum-Compute-MAC pool from the MAC Address Assignment list box.
- 59. Select Platinum-Net-SLA in QoS Policy list box.
- 60. Select default in Network Control Policy list box.

- 61. Select <not set> in Pin Group list box.
- 62. Select default in Stats Thershold Policy list box.
- 63. Select <not set> in Dynamic vNIC Connection Policy list box.

64. Click OK.

Figure 78 Defining the vNIC Properties for guest- B-NIC

7	Create vNIC Te	mplate	x
Create vNIC Te	mplate		0
Na	me: Guest-B-NIC		^
Descript	ion: Guest Template		
Fabric Warning If VM is selected, a port pr	: ID: Target Adapter VM ofile by the same name will be create	Enable Failover	
Template T		ting Template	=
Select	Name	Native VLAN	
✓	Guest-VLAN Guest-Vlan-1000	• ^	
✓	VLAN-Guest-VLAN-1001		
	NFS-VLAN	Ŭ Ū	
• Warning Make sure that the MTU has corresponding to the Egres	TTU: 9000 s the same value in the <u>QoS System</u> s priority of the selected QoS Policy. Pool: Platinum-Compute-MAC(15/		
	olicy: Platinum-Net-SLA		
Network Control Po	0		
	oup: <not set=""></not>		
		ОК	Cancel

- 65. Create vNIC Template window opens.
- 66. Enter NFS-A-NIC in the Name field.
- 67. Enter NFSTemplate in the Description field.
- 68. In Fabric ID click FabricA radio button, do not check Enable Failover check box.
- 69. In Target check Adapater check box.
- 70. In Template Type select Initial Template radio button.
- 71. Under VLANs check NFS-VLAN and choose Native VLAN as NFS-VLAN.
- 72. In the MTU field enter 9000.
- 73. Select Platinum-Compute-MAC pool from the MAC Address Assignment list box.
- 74. Select Gold-Net-SLA in QoS Policy list box.
- 75. Select default in Network Control Policy list box.

- 76. Select <not set> in Pin Group list box.
- 77. Select default in Stats Thershold Policy list box.
- 78. Select <not set> in Dynamic vNIC Connection Policy list box.
- 79. Click OK.

Figure 79 Defining the vNIC Properties for NFS- A-NIC

<b>A</b>	Create vNIC Tem	plate	x
Create vNIC Temp	late		0
Name:	NFS-A-NIC		^
	) NFS Template		
Fabric ID:	D	nable Failover	
rabic ib.			
	Target ✓ Adapter □ VM		
	by the same name will be created le exists, and updating template i Initial Template  O Updatin	s selected, it will be overwritten	
VLANs			
Select	Name	Native VLAN	Ŧ
	Managment-VLAN	0	~
Image: A state of the state	NFS-VLAN	۲	
	VLAN-Guest-VLAN-1001	0	≡
	vMotion-VLAN	0	~
	<b>9000</b> D		
Make sure that the MTU has the corresponding to the Egress price	same value in the <u>QoS System C</u> rity of the selected QoS Policy.	lass	
MAC Pool:	Platinum-Compute-MAC(15/	<b>▼</b>	
QoS Policy:	Gold-Net-SLA		
Network Control Policy:	<not set=""> 💌</not>		
Pin Group:	<not set=""></not>		~
		OK	Cancel

- 80. Create vNIC Template window opens.
- 81. Enter NFS-B-NIC in the Name field.
- 82. Enter NFSTemplate in the Description field.
- 83. In Fabric ID click FabricA radio button, do not check Enable Failover check box.
- 84. In Target check Adapater check box.

- 85. In Template Type select Initial Template radio button.
- 86. Under VLANs check NFS-VLAN and choose Native VLAN as NFS-VLAN.
- **87.** In the **MTU** field enter 9000.
- 88. Select Platinum-Compute-MAC pool from the MAC Address Assignment list box.

1

- 89. Select Gold-Net-SLA in QoS Policy list box.
- 90. Select default in Network Control Policy list box.
- 91. Select <not set> in Pin Group list box.
- 92. Select default in Stats Thershold Policy list box.
- **93.** Select **<not set>** in **Dynamic vNIC Connection Policy** list box.
- 94. Click OK.

7	Create vNIC Tem	plate		X	
Create vNIC Temp	olate			0	
Name:	NFS-B-NIC				^
	) NFS Template				
	🔿 Fabric A 💿 Fabric B 📃 En	able Failover			
c	Target ✓ Adapter ↓ VM				
If a port profile of the same name	by the same name will be created ne exists, and updating template i Initial Template O Updatin	s selected, it will be overwritter	י 		=
Select	Name	Native VLAN	<b>₽</b>		
	Managment-VLAN	0			
✓	NFS-VLAN	۲			
	VLAN-Guest-VLAN-1001	0	≡		
	vMotion-VLAN	0	$\overline{}$		
Warning Make sure that the MTU has the corresponding to the Egress priv MAC Pool:	9000 The same value in the <u>QoS System C</u> prity of the selected QoS Policy. Platinum-Compute-MAC(15/ Gold-Net-SLA				
Network Control Policy:	0				
	<not set=""></not>				~
			ОК	Cancel	]

## Figure 80 Defining the vNIC Properties for NFS- B-NIC

**Baremetal Host vNIC Template** 

Create two vNIC templates for handling PXE and Mangement LAN traffic and two vHBA templates for handling SAN traffic to run Baremetal RHEL 6.3 host on TenantA-BareMetal-Zone.

- 1. Create vNIC Template window opens.
- **2.** Enter PXE-A-NIC in the Name field.
- **3**. Enter PXE Template in the **Description** filed.
- 4. In Fabric ID click FabricA radio button, do not check Enable Failover check box.
- 5. In Target check Adapater check box.

- 6. In Template Type select Initial Template radio button.
- 7. Under VLANs check Baremetal-VLAN20 and choose Native VLAN as BareMetal-VLAN20.

- 8. In the MTU field enter 9000.
- 9. Select Platinum-Compute-MAC pool from the MAC Address Assignment list box.

1

- 10. Select Platinium-Net-SLA in QoS Policy list box.
- 11. Select default in Network Control Policy list box.
- 12. Select <not set> in Pin Group list box.
- 13. Select default in Stats Thershold Policy list box.
- 14. Select <not set> in Dynamic vNIC Connection Policy list box.
- 15. Click OK.

Figure 81 Defining the vNIC Properties for PXE- A-NIC

A	Create vNIC Tem	iplate	x
Create vNIC Temp	olate		0
	PXE-A-NIC		^
Description:	0 PXE Template		
Fabric ID:	0 💿 Fabric A 🔵 Fabric B 🔽 E	nable Failover	
	Target		
Warning	Adapter		
If a port profile of the same nam Template Type: VLANs	e exists, and updating template i  Initial Template 🔿 Updatir		Ξ
Select	Name	Native VLAN	
	default	0 ^	
	BareMetal-VLAN20	• <b>=</b>	
	Guest-VLAN	0	
	Guest-Vlan-1000		
Warning	9000 D same value in the <u>QoS System (</u> rity of the selected QoS Policy.	lass	
	Platinum-Compute-MAC(15/		
	Platinum-Net-SLA		
	D		
	<not set=""></not>		~
		ОК	Cancel

16. Create vNIC Template window opens.

- 17. Enter Bare-MGMT-A-NIC in the Name field.
- 18. Enter Baremtal Magament Template in the Description field.
- 19. In Fabric ID click FabricA radio button, do not check Enable Failover check box.
- 20. In Target check Adapater check box.
- 21. In Template Type select Initial Template radio button.
- 22. Under VLANs check Baremetal-VLAN20 and choose Native VLAN as BareMetal-VLAN20.
- **23.** In the **MTU** field enter 9000.
- 24. Select Platinum-Compute-MAC pool from the MAC Address Assignment list box.
- 25. Select GoldNet-SLA in QoS Policy list box.
- 26. Select default in Network Control Policy list box.
- 27. Select <not set> in Pin Group list box.
- 28. Select default in Stats Thershold Policy list box.
- 29. Select <not set> in Dynamic vNIC Connection Policy list box.
- 30. Click OK.

### Figure 82 Defining the vNIC Properties for Bare-MGMT-A-NIC

	Create vNIC Tem	nplate		
Create vNIC Temp	olate			(
Name:	Bare-MGMT-A-NIC			
Description:	) Baremtal Managment Temp	plate		
Eshvis ID:	● Fabric A 🔵 Fabric B ✔ Er	pable Eailover		
	D			
	Target			
	✓ Adapter VM			
Warning	(			
	by the same name will be created	1		
		 is selected, it will be overwrit	ten	
If a port profile or the same has				
If a port profile of the same har				
	<ul> <li>Initial Template O Updatir</li> </ul>			
Template Type:				
Template Type:	<ul> <li>Initial Template O Updatir</li> </ul>	ng Template		
Template Type:			F	
Template Type:	Initial Template     Updatin Name Managment-VLAN	ng Template		
Template Type: VLANS Select	Initial Template     Updatin Name Managment-VLAN NFS-VLAN	ng Template Native VLAN	F	
Template Type: VLANS Select	Initial Template     Updatin Name Managment-VLAN	ng Template Native VLAN O O O O	F	
Template Type: VLANS Select	Initial Template     Updatin Name Managment-VLAN NFS-VLAN	ng Template Native VLAN		
Template Type:	Initial Template     Updatin Name Managment-VLAN NFS-VLAN VLAN-Guest-VLAN-1001	ng Template Native VLAN O O O O		
Template Type: VLANS Select Create VLAN	Initial Template     Updatin     Managment-VLAN     NFS-VLAN     VLAN-Guest-VLAN-1001     vMotion-VLAN	ng Template Native VLAN O O O		
Template Type: VLANS Select Create VLAN	Initial Template     Updatin Name Managment-VLAN NFS-VLAN VLAN-Guest-VLAN-1001	ng Template Native VLAN O O O		
Template Type:	Initial Template     Updatin Name Managment-VLAN NFS-VLAN VLAN-Guest-VLAN-1001 vMotion-VLAN  9000 0	ng Template		
Template Type:  VLANS Select  Create VLAN  Warning Make sure that the MTU has the	Initial Template Updatin Name Managment-VLAN NFS-VLAN VLAN-Guest-VLAN-1001 vMotion-VLAN  9000 esame value in the QoS System C	ng Template		
Template Type:	Initial Template Updatin Name Managment-VLAN NFS-VLAN VLAN-Guest-VLAN-1001 vMotion-VLAN  9000 esame value in the QoS System C	ng Template		
Template Type:	Initial Template Updatin Name Managment-VLAN NFS-VLAN VLAN-Guest-VLAN-1001 vMotion-VLAN  9000 esame value in the QoS System C	Native VLAN		
Template Type:	Initial Template Updatin     Name     Managment-VLAN     MFS-VLAN     VLAN-Guest-VLAN-1001     vMotion-VLAN     g000     o     o     same value in the QoS System C     ority of the selected QoS Policy.     Platinum-Compute-MAC(15/	Native VLAN		
Template Type:  VLANS Select  Create VLAN  Warning Make sure that the MTU has the corresponding to the Egress prio  MAC Pool: QoS Policy:	Initial Template Updatin     Name     Managment-VLAN     MFS-VLAN     VLAN-Guest-VLAN-1001     vMotion-VLAN     g000     o     same value in the QoS System C     ority of the selected QoS Policy.     Platinum-Compute-MAC(15/     Gold-Net-SLA	Native VLAN		
Template Type:  VLANS Select  Create VLAN  Warning Make sure that the MTU has the corresponding to the Egress pri MAC Pool: QoS Policy: Network Control Policy:	Initial Template Updatin     Name     Managment-VLAN     MFS-VLAN     VLAN-Guest-VLAN-1001     vMotion-VLAN     g000     o     same value in the QoS System C     ority of the selected QoS Policy.     Platinum-Compute-MAC(15/     Gold-Net-SLA	Native VLAN		

**Baremetal / Virtual Host vHBA Template** 

This section details the creation off two vHBA templates for handling SAN traffic to run Baremetal RHEL 6.3 or Hypervisor ESXI 5.1 hosts on TenantA-BareMetal-Zone and TenantA zones respectively.

Login to Cisco UCS Manager with User TenantA-Admin created earlier for Organization TenantA::

- 1. Click the SAN tab in the left pane.
- 2. Choose Pools > Sub-Organization.
- 3. Expand TenantA.
- 4. Select vHBA Templates and right click Create vHBA Template.

## Figure 83 Creating vHBA Template



- 5. Create vHBA Template window opens.
- **6**. Enter TenantAFabricA in the Name field.
- 7. Enter TenantA vHBA Fabric A Template in the Description field.
- 8. In Fabric ID click FabricA radio button.
- 9. Select VSAN300 in VSAN list box.
- 10. In Template Type select Initial Template radio button.
- 11. In the Max Data field Size field enter 2048.
- 12. Select Platinum-Compute-WWPN pool from the WWPN Pool list box.

- 13. Select FC-Net-SLA in QoS Policy list box.
- 14. Select <not set> in Pin Group list box.
- 15. Select default in Stats Thershold Policy list box.
- 16. Click OK.

Create vHBA	•	
	TeantAFabricA	
Description:	TenantA vHBA Fabric A Template	
	• A • B	
Select VSAN:	VSAN300	🛨 Create VS.
Template Type:	Initial Template O Updating Template	
Max Data Field Size:	2048	
WWPN Pool:	Platinum-Compute-WWPN(5/ 💌	
QoS Policy:	FC-Net-SLA	
Pin Group:	<not set=""></not>	
Stats Threshold Policy:	default 🗾	

## Figure 84 Defining the vHBA Properties for TenantAFabricA

- 17. Create vHBA Template window opens.
- **18**. Enter TenantAFabricA in the Name field.
- 19. Enter TenantA vHBA Fabric A Template in the Description field.
- 20. In Fabric ID click FabricA radio button.
- 21. Select VSAN200 in VSAN list box.
- 22. In Template Type select Initial Template radio button.
- 23. In the Max Data field Size enter 2048.
- 24. Select Platinum-Compute-WWPN pool from the WWPN Pool list box.
- 25. Select FC-Net-SLA in QoS Policy list box.
- **26**. Select **<not set>** in **Pin Group** list box.
- 27. Select default in Stats Thershold Policy list box.
- 28. Click OK.

ſ

<b>A</b>	Create vHBA Template	×
Create vHBA	Template	0
Name:	TenantAFabricB	
Description:	TenantA vHBA Fabric B Template	
Fabric ID:	● A ● B	
Select VSAN:	VSAN200	🛨 Create VSAN
Template Type:	Initial Template O Updating Template	
Max Data Field Size:	2048	
WWPN Pool:	Platinum-Compute-WWPN(5/ 💌	
QoS Policy:	FC-Net-SLA	
Pin Group:	<not set=""></not>	
Stats Threshold Policy:	default 👻	
		OK Cancel

## Figure 85 Defining the vHBA Properties for TenantAFabricB

# **Creating IPMI Policy**

Intelligent Platform Management Interface (IPMI) is an open standard technology that defines how administrators monitor system hardware and sensors, control system components and retrieve logs of important system events to conduct remote management and recovery. IPMI runs on the BMC (Baseboard Management Controller) of the server blade and thus operates independently of the operating system. Since IPMI operates independent of the operating system, when sending commands to the BMC over IP, it provides administrators with the ability to monitor, manage, diagnose and recover systems, even if the operating system has hung or the server is powered down.



In the UCS system, the BMC supports IPMI version 2.0 only.

In this study we will create IPMI Access policy in Cisco UCS Manager for CloudPlatfrom 4.2.1 to perform Baremetal host operations like reboot, shutdown, resets and life cyle management in Cloud for Tenants.

Login to Cisco UCS Manager with root user, to configure TenantA Organization Unit:

- 1. Click the Policies ervers tab in the left pane.
- 2. Select Policies, expand root and then Sub-Organization.
- 3. Expand TenantA.
- 4. Right-click on IPMI Access Profile and select Create IPMI Access Profiles.



- 5. Click Add in the IPMI Access Profiles window.
- 6. Enter Baremetal-IPMI in the Name field.
- 7. Enter IPMI Acess in the Description field.
- 8. Click Add in the IPMI Access Profiles window.
- 9. Enter admin in the Name field.
- **10**. Enter <XXXX> in Password field.
- 11. Enter <XXXX> in confirm Password field.
- 12. Select Admin radio button in Role acess.
- **13.** Click **OK**.

ſ

··· 🔊 ··	PMI Profile Baremeral-LPMI				_
	600 600	IPMI Access	s Profiles		
	IPMI Access Profil				
	🛨 🖃 🕰 Filter 🛋	Export 📚 Print			
	Name		Role		[₹
	🖃 👼 IPMI Profile	e Baremetal-IPMI			^
	🏻 🌡 admin		Admin		
	<b>0</b> 000	Create IPMI A	ccess Profile		
		II Access Profile	P		
	Create in it	II Access I Tom			
	Name: Bare	metal-IPMI			
	0				1
	Description: IPMI				
		er 👄 Export 📚 Print			
				Ę	
	E E A Filte	er 👄 Export 📚 Print		E X	
	Name Crea	er 👄 Export 😂 Print Role			
Create I	E E A Filte	er 👄 Export 😂 Print Role		×	
create	Name Crea	er 👄 Export 😂 Print Role		×	
reate	IPMIUser	er 👄 Export 😂 Print Role		× ?	
Sreate Na Passw	IPMIUser	er 👄 Export 😂 Print Role		<b>e</b>	
Na Passw nfirm Passw	IPMI User	er 👄 Export 😂 Print Role		<b>x</b> 0	
Na Passw	IPMIUser	er 👄 Export 😂 Print Role		<b>x</b> 0	
Na Passw nfirm Passw	IPMI User	er 👄 Export 😂 Print Role		<b>x</b> 0	

#### Figure 87 Creating the IPMI Username and Password in Access Profile

# **Creating Server Pool Qualifications and Policy**

A server pool contains a set of servers. These servers typically share the same characteristics, which can be their location in the chassis, or an attribute such as server type, amount of memory, local storage, type of CPU, or local drive configuration. A server can be assigned manually to a server pool, or the server pool policies and server pool policy qualifications can be used to automate the assignment.

To meet compute service levels based on the cloud services offering which includes cost, UCS offers a server pool that enables the Cloud administrator to designate one or more server pools to be used by a specific organization. UCS enables your business to meet the growth demands by facilitating automatic placement of these compute resources to specific server pools by defining Server Pool Qualifications parameters. These parameters include physical CPU and Memory types based on performance and capacity available on the compute blades.

1

In this study we will create four Server Pools with Policy qualifications based on cloud compute offering such as the Memory, CPU, and other attributes, which are automatically assigned to the concerned server pools as and when they are available on cloud compute system.

- 1. Platinum Server Pool
- 2. Gold Server Pool
- 3. Silver Server Pool
- 4. Bronze Server Pool

The steps described in this section provide details to configure the necessary Server Pool Qualifications for Compute-Server-Pool in the Cisco UCS environment.

The Server Pool qualification data mentioned in this paper are based on general usage and can be altered to choose your specific compute needs in the cloud environment

## **Platinum Compute Server Pool and Qualification**

Login to Cisco UCS Manager with root user, to configure TenantA Organization Unit:

- 1. Click the Servers tab in the left pane.
- 2. Select **Policies**, and expand the **root**.
- 3. Right-click Server Pool Policy Qualifications and select Create Server Pool Policy Qualification.

# Figure 88 Creating the Server Pool Policy Qualification



- 4. Name the server pool policy qualification PlatinumSvrQual.
- 5. (Optional) Give description.



### Figure 89 Adding the Name and Description to the Server Pool Policy Qualification

- 6. In the Actions pane, click Create Chassis/Server Qualification.
- 7. Type value 1as the First Chassis ID and value 10 as the Number of chassis.



Figure 90 Defining the ID and Slots for the Server Qualification

8. Under Server Qualifications click ADD (+).



Figure 91 Adding the Server Qualifications for Platinum Server

9. In First Slot ID enter 1 value, and Number of Slots enter 8.

1



### Figure 92 Defining ID and Slots for Server Qualification

- 10. Click Final Stage, and then click Finish.
- 11. In the Actions pane, click Create Chassis/Server Qualification.
- 12. In the First Chassis ID field enter 1 and in Number of Chassis field enter 10.
- 13. In the Actions pane, click Create Memory Qualification.
- 14. For the Clock (MHz) field, click the Unspecified radio button.
- 15. For the Latency (ns) field, click the Unspecified radio button.
- 16. For the Min Cap (MB) field, click select radio button, and enter 128
- 17. For the Max Cap (MB) filed click select radio button enter 256.
- 18. For the Width field, click the Unspecified radio button.
- 19. For the Units field, click the Unspecified radio button.
- 20. Click OK.



### Figure 93 Defining the parameters for the Memory Qualifications

- 21. In the Actions pane click Create CPU Qualifications .
- 22. For the Min Number of Cores field click Select radio button and enter 32
- 23. For the Max Number of Cores field click Select radio button and enter 40.
- 24. Select Any for Processor Architecture, and leave the PID (RegEx) field blank
- 25. For the Min Number of Threads filed click Unspecified radio button.
- 26. For the Max Number of Threads filed click Unspecified radio button.
- 27. For the CPU Speed (MHz) field click Unspecified radio button.
- 28. For the CPU Stepping field, click Unspecified radio button.
- 29. Click Finish.



Figure 94 Defining the Parameters for the CPU Qualifications

Follow the steps described above to create Server Pool Policy Qualifications Gold-Compute-Server, Silver-Compute-Server and Bronze-Compute-Server with Server Pool Policy Qualifications listed in Table 15.

Table 15 Server Pool Policy Qualification Values for all the Service Classes	Table 15	Server Pool Polic	Qualification	Values for all t	he Service Classes
--	----------	-------------------	---------------	------------------	--------------------

ſ

Server Pool Policy Qualifications	Chassis	Memory	CPU
PlatinumSvrQual	ID Range 1 – 10 Server Slot ID range 1 –8	Min Cap 128 – Max Cap 256	Min Number of cores 32 – Max Number of cores 40
GoldSvrQual	ID Range 1 – 10 Server Slot ID range 1 – 8	Min Cap 64 – Max Cap 128	Min Number of cores 32 – Max Number of cores 40
SilverSvrQual	ID Range 1 – 10 Server Slot ID range 1 – 8	Min Cap 32 – Max Cap 64	Min Number of cores 12 – Max Number of cores 16
BronzeSvrQual	ID Range 1 – 10 Server Slot ID range 1 – 8	Min Cap 16 – Max Cap 32	Min Number of cores 12 – Max Number of cores 16

3 🔻 🛆 🔺	🕒 🏐 🗉 New 🔹 😧 Options 🛛 🔞	Pending Activitie	s 🛛 🖸 Exit						
2 42 4 23	>> 🥪 Servers † 🐒 Policies † 🔥 root † 🐒	Server Pool Policy Qualific	ations					🐒 Server Pool Pol	icy Qualifica
ment Servers LAN SAN VM Admin	Server Pool Policy Qualifications								_
	😸 😑 🛃 Filter 👄 Export 🏠 Print								
Filter: Al			Model			0	Architecture	Quantitat	0
-	Name - SS BronzeSvrQual	Max	Prodel	From		To Speed	Architecture	Stepping	1.4
» Servers	Bernzesvruual     Bernzesvruual     Bernzesvruual     Bernzesvruual     Bernzesvruual				10				-
- Service Profiles	- 50 Chassis in range [1 - 10]			1	10	Unspecified			
⊕_0, root	- 30 Memory guaincation					Unspecified		Unspecified	
Service Profile Templates						Unspeched	Any	Unspeched	
⊟-∭, root	E-SilverSwQual								
1 - A Sub-Organizations	Ghassis id range [1 - 10]			1	10				
S Policies	- 55 Memory qualification					Unspecified			
B-A root	- S Processor qualification					Unspecified	Any	Unspecified	
S Adapter Policies	E-S GoldSvrQual								
🕀 🐒 BIOS Defaults	B - S Chassis id range [1 - 10]			1	10				
BIOS Policies	- S Memory gualification					Unspecified			
Boot Policies	Processor qualification					Unspecified	Any	Unspecified	
Host Firmware Packages	E-S PlatinumSvrQual								
- SIPMI Access Profiles	💼 😼 Chassis id range [1 - 10]			1	10				
⊕- S Local Disk Config Policies ⊕- Maintenance Policies	- S Memory gualification					Unspecified			_
- S Management, Firmware Packages	- S Processor gualification					Unspecified	Any	Unspecified	
Source Control Policies							,		
E-S Scrub Policies									
- Serial over LAN Policies									
19- Server Pool Policies									
- Server Pool Policy Qualifications									
BronzeSvrQual									
- 5 GoldSwQual									
- I PlatinumSvrQual									
-SiverSvrQual									
🗐 al-chassis									
Interstold Policies									
<ul> <li>— Si ISCSI Authentication Profiles</li> </ul>									
- S vNIC/vHBA Placement Policies									
⊕-▲ Sub-Organizations									
- 💮 Pools									
E-A root									
🗈 🥪 Server Pools									
UUID Suffix Pools									
Sub-Organizations									

# Figure 95 Summary of the Server Pool Policy Qualifications Created

1

# **Platinum Compute Server Pool**

Login to Cisco UCS Manager with root user to configure Server Pools for TenantA Organization Unit:

- 1. Click the **Servers** tab in the left pane.
- 2. Select Pools, expand root.
- 3. Right-click Server Pool and select Create Server Pool.

#### Figure 96 Create Server Pool



- 4. Enter Platinum-Compute-ServerPool in the Name field.
- **5.** (Optional) Enter a description in the Description field.



Figure 97 Adding the Name and Description for the Server Pool

6. Click Finish.

1

A Cisco Unified Computing System Manager - Th	F-121	
	G 🕘 🗈 New - 😧 Options 🕜 🕕 Andread Control ties 🖸 Exit	
2 42 3 23	>> 🥪 Servers ' 🛞 Pools ' 🗛 root ' 🥪 Server Pools	
Equipment Servers LAN SAN VM Admin	Server Pools	
	🚖 Create Server Pool	×
Filter: All		
± =	Unified Computing System Manager	
E		
E- Service Profiles	Add Servers	0
E- 💑 root	Create Server Pool Aud Server's	
🕀 💐 W52012	1. √Set Name and Description	
🗄 🍌 Sub-Organizations	2. VAdd Servers	
E- Service Profile Templates	Servers Pooled Servers	
E Sub-Organizations	Ch, Slo Ra Us PID Ad, Ad, Serial Cor, 🛱 Cha, Slot ID Rac, Use, PID Ada, Ada	Serial Cor
E- S Policies		
🖻 🛕 root		
🕀 🗐 Adapter Policies		
⊕ ∑ BIOS Defaults	2 UC5N2X FC	
BIOS Policies	4 UCS N2X FC	
Boot Policies	3 UCS., N2X.,, FC.,,	
IPMI Access Profiles	1 4 UCS UCS FC 16	
S Local Disk Config Policies		
Maintenance Policies		
Management Firmware Packages		
😥 🚿 Power Control Policies		
E Scrub Policies		
Serial over LAN Policies		
Server Pool Policies     Server Pool Policy Qualifications		
PlatinumSvrQual		
∬ all-chassis		
⊕ · 🛒 Threshold Policies		•
- 🗐 iSCSI Authentication Profiles		
VNIC/VHBA Placement Policies	Details	
⊕-À Sub-Organizations     ⊖-     ⊕ Pools	Model:	
E- A root	Model:	
E Server Pools	Serial Number: Serial Number:	
UUID Suffix Pools	Vendor: Vendor:	
🕀 👬 Sub-Organizations	venuer:	
🗄 🞯 Schedules		
	<pre> Next &gt; F</pre>	Finish Cancel
	CHEV NEX /	

## Figure 98 Summary of the Servers in the Server Pool

Follow the steps described above to create Server Pools Gold-Compute-ServerPool, Silver-Compute-ServerPool and Bronze-Compute-ServerPool with the Server Pool Policy Qualifications Values listed in Table 16

## Table 16 Server Pool Policy Qualification values for the Server Pools

Server Pool	Blades Values
Platinum-Compute-ServerPool	1 – 8
Gold-Compute-ServerPool	1 - 8
Silver-Compute-ServerPool	1 - 8
Bronze-Compute-ServerPool	1 - 8

ſ

Cisco Unified Computing System Manager - TME-L21				
lt Summary	🕒 🍥 🗉 New 🔹 🛃 Options 🛛 🕢 🕕 Marchine Activities			
🗴 🔻 🛆				
2 42 7 23	>> 🥪 Servers + 🛞 Pools + 👬 root + 🥪 Server Pools			
pment Servers LAN SAN VM Admin	Server Pools			
Filter: All	🛨 🖃 🔍 Filter 👄 Export 😸 Print			
	Name		Size	Assigned
=	Server Pool Bronze-Compute-ServerPool	0	0	
Servers	Server Pool Silver-Compute-ServerPool	0	0	
Service Profiles	Server Pool Gold-Compute-ServerPool	0	0	
	Server Pool Platinum-Compute-ServerPool	0	0	
Service Profile Templates	🗄 🥪 Server Pool default	3	3	
⊡ root ⊞ Sub-Organizations				
- S Policies				
⊟-å root				
Adapter Policies				
BIOS Defaults				
⊞-      S BIOS Policies				
Boot Policies				
Host Firmware Packages				
IPMI Access Profiles				
Local Disk Config Policies      Maintenance Policies				
Management Firmware Packages				
Management Pirmware Packages     S     Power Control Policies				
Scrub Policies				
Serial over LAN Policies				
Server Pool Policies				
⊕				
🗐 ISCSI Authentication Profiles				
🚿 vNIC/vHBA Placement Policies				
🗄 📩 Sub-Organizations				
Pools				
E- Server Pools				
Server Pool Bronze-Compute-ServerPool				
Server Pool Gold-Compute-ServerPool				
Server Pool Platinum-Compute-ServerPool				
Server Pool Silver-Compute-ServerPool				
🖭 🥪 Server Pool default				
🕀 🎆 UUID Suffix Pools				
Gill Schedules				

Figure 99 Summary of all the Server Pools Created

# **Platinum Compute Server Pool Policies**

Login to Cisco UCS Manager with root user to configure Server Pool Policies forTenantA Organization Unit:

1

- 1. Click the **Servers** tab in the left pane.
- 2. Select Policies, expand root.
- 3. Right-click Server Pool Policies and select Create Server Pool Policy.

## Figure 100 Creating Server Pool Policies



4. Enter PlatinumSVRPply in the Name field.

ſ

- 5. (Optional) Enter a description in the Description field.
- 6. In the **Target Pool** list box, select **Server Pool Platinum-Compute-ServerPool** (which was created earlier).
- 7. In the Qualification list box, select PlatinumSvrQual (which was created earlier).



Figure 101 Defining the Server Pool Policy Attributes

Follow the steps described above to create Server Pools Policy Gold-Compute-ServerPool, Silver-Compute-ServerPool and Bronze-Compute-ServerPool with the Server Pool Policies listed in Table 17.

Table 17	Server Pool	Policy	Values
		,	

Server Pool Policies	Target Pool	Qualification
PlatinumSVRply	Server Pool Platinum-Compute-ServerPool	PlatinumSvrQual
GoldSVRply	Server Pool Gold-Compute-ServerPool	GoldSvrQual
SilverSVRply	Server Pool Silver-Compute-ServerPool	SilverSvrQual
BronzeSVRply	Server Pool Bronze-Compute-ServerPool	BronzeSvrQual

Cisco Unified Computing System Manager - TME-L2			
ault Summary	🌀 🍥 🖽 New 🖌 🎴 Options 🛛 🕐 🚯 💧 Amending A	ctivities 0 Exit	
🛛 🗸 🗸			
2 42 8 23	>> 🥪 Servers 🕨 🗊 Policies 👌 🎄 root 🕨 🗐 Server Pool Policies		
quipment Servers LAN SAN VM Admin	Server Pool Policies		
	🔍 Filter 👄 Export 🗞 Print		
Filter: All	• • •		
	Name	Target Pool	Qualificat
	Server Pool Policy BronzeSVRply	org-root/compute-pool-Bronze-Compute-ServerPool	BronzeSvrQual
Servers	Server Pool Policy SilverSVRply	org-root/compute-pool-Silver-Compute-ServerPool	SilverSvrQual
E A root	S Server Pool Policy GoldSVRply S Server Pool Policy PlatinumSVRply	org-root/compute-pool-Gold-Compute-ServerPool	GoldSvrQual
Service Profile Templates	Server Pool Policy PlacinumSvkply	org-root/compute-pool-Platinum-Compute-ServerPool	PlatinumSvrQual
E-A root			
. Sub-Organizations			
🖨 💯 Policies			
🖻 🛕 root			
Adapter Policies			
曲· ⑤ BIOS Defaults 由· ⑤ BIOS Policies			
BIOS Policies			
Host Firmware Packages			
S IPMI Access Profiles			
S Local Disk Config Policies			
Maintenance Policies			
🚿 Management Firmware Packages			
Power Control Policies			
😐 🚿 Scrub Policies			
📓 Serial over LAN Policies			
😑 🚿 Server Pool Policies			
🗐 Server Pool Policy BronzeSVRply			
Server Pool Policy SilverSVRply			
Server Pool Policy Qualifications     Server Pool Policy Qualifications			
S PlatinumSvrQual			
SilverSvrQual			
all-chassis			
S Threshold Policies			
SCSI Authentication Profiles			
😑 🚭 Pools			
🖻 🎪 root			
🕀 🛶 Server Pools			
🕀 🇱 UUID Suffix Pools			
	Dat		

## Figure 102 Summary of all the Server Pool Policies Created

# **Creating a Server BIOS Policy**

ſ

These steps provide details for creating a server BIOS policy for the Cisco UCS environment.

Login to Cisco UCS Manager with User TenantA-Admin created earlier for Organization TenantA::

- 8. Click the Server tab.
- 9. Choose Pools > Sub Organization.
- 10. Expand TenantA and select BIOS Policies.
- 11. Right-click BIOS Policies and select Create BIOS Policy.
- **12.** Enter TenantA-BIOS as the BIOS policy name.
- 13. Check Reboot on BIOS Setting Change check box.
- 14. Change the Quiet Boot property to Disabled.



Figure 103 Defining the BIOS Policy Attributes

- 15. Click Next.
- 16. On Hyper Threading click Enabled radio button.
- 17. On Virtualization Technology (VT) click Enabled radio button.
- 18. Accept default setting and click on Finish.
- 19. Click OK.



### Figure 104 Setting the Processor Attributes

# **Creating a Server Firmware Policy**

These steps provide details for creating a server BIOS policy for the Cisco UCS environment. Login to Cisco UCS Manager with User TenantA-Admin created earlier for Organization TenantA::

- 1. Click Server tab.
- 2. Choose Pools > Sub Organization.
- 3. Expand TenantA and select Firmware Host Firmware Packages.
- 4. Right-click Host Firmware Packages and select Create.
- 5. Enter TenantAFirmware as the BIOS policy name.
- 6. Click Simple radio button on How would you like to configure the Host Firmware Package.
- 7. On Blade Package and Rack Package select the latest Cisco UCS package.
- 8. Click OK.



### Figure 105 Configuring the Host Firmware Package

# **Creating Local Disk Configuration Policy**

These steps provide details for creating a local disk configuration for the Cisco UCS environment, which is necessary if the servers in question do not have a local disk.

۵, Note

This policy should not be used on blades that contain local disks.

Login to Cisco UCS Manager with User TenantA-Admin created earlier for Organization TenantA:

- 1. Click the **Server** tab.
- 2. Choose Pools > Sub Organization.
- 3. Expand TenantA and select Local Disk Configuration Policy.
- 4. Right-click Local Disk Configuration Policy and select Create.
- 5. Enter TenantALocalDisk as the local disk configuration policy name.
- 6. Change the Mode to Any Configuration, and check Protect Configuration check box.
- 7. Click **OK** to complete creating the host firmware package.



## Figure 106 Creating the Local Disk Configuration Policy Properties

# **Creating Boot Policies**

These steps provide details for creating boot policies for the Cisco UCS environment. These directions apply to an environment in which each storage controller 0c port is connected to fabric A and each storage controller 0d port is connected to fabric B.



In this paper we will create two Boot Policies one for ESXi 5.1 Host and second for Baremetal RHEL 6.3 Host.

The first boot policy will define SAN Boot options for booting ESXi 5.1 over FCoE Target

The second boot policy will define PXE Boot options for booting Baremetal RHEL 6.3 over FCoE Target SAN Boot Policy for ESXi 5.1 Host.

Login to Cisco UCS Manager with User TenantA-Admin created earlier for Organization TenantA::

- 1. Click the **Server** tab.
- 2. Select Pools > Sub Organization.

- 3. Expand TenantA and select the **Policies** tab in the right pane.
- 4. Click the Boot Policies sub-tab.
- 5. Click the + symbol at the right edge of the right pane to create a Boot Policy.
- 6. Enter TenantAFCBoot in the Name filed.
- 7. (Optional) Give the boot policy a description.
- 8. Leave Reboot on Boot Order Change unchecked and uncheck Enforce vNIC/vHBA Name.
- 9. Expand the Local Devices drop-down list menu and select Add CD-ROM.
- 10. Expand vHBAs drop-down list menu and select Add SAN Boot.
- 11. Enter TenantAFabricA in the vHBA field of the Add SAN Boot window.
- 12. Ensure that **Primary** is selected as the type.
- **13**. Click **OK** to add the SAN boot initiator.

#### Figure 107 Defining the vHBA Attributes in Primary SAN Boot



- 14. Click Add SAN Boot for the SAN boot initiator for secondary FC Boot Path.
- 15. Enter TenantAFabricB in the vHBA field of the Add SAN Boot window.
- **16**. Click **OK** to add the SAN boot initiator.


### Figure 108 Defining the vHBA attributes in Secondary SAN Boot

- 17. Under Boot Order in right pane select SAN Primary under Storage tree
- **18**. From the vHBA dropdown menu, choose **Add SAN Boot > Add San Boot Target To SAN Primary**.

🔒 Ciso	o Unified Com	puting Syster	n Manager - TM	E-L21						
ımmai	ry		K			D Orkers		Pending	Activities	
		Δ		0	) 🗄 New 🔻	Options	0	🗩   🛆 Pending	J Accivicies	0 <u>E</u> xit
·	<b>V</b>	<u> </u>	40	<b></b>						
	52	8	40	🗐 🌧 Ci	eate Boot Po	licy				
it Ser	vers LAN SAI	V VM Admin				- 4 D - E	_			
c:h	 			i Cr	eate Bo	ot Policy	/			
FIIL	er: All			l n						
	🙀 Dab-Organiza	dons		L L		Name:	Tenant/	AFCBoot		
	ice Profile Templ	ates				Description				
⊡ <mark>.</mark> ģ, r						Description:				
	🙀 Sub-Organiza	ations		R	eboot on Boot C	order Change:				
S Polici				Enf	orce vNIC/vHB4	ViSCSI Name:				
	🗊 Adapter Polic	ies				()	5			
	📓 Muapter Polic 🗐 BIOS Default				ARNINGS: type (primary)	secondary) doe	es not indi	cate a boot order	nresence	
	BIOS Policies							he same device cl		torage/iSCSI) is
	🗑 Boot Policies							elected and the vi		
	Host Firmwar			Ifi	: is not selected	, the vNICs/vH	BAS/ISCSI	are selected if th	iey exist, ol	therwise the vN
	🛐 IPMI Access I						_	Boot Order		
	Local Disk Co				Local Devices	F		Boot Urder		
	📓 Maintenance				-			🛨 🖃 🔍 Filt	er 👄 Expo	ort 😸 Print
	Management Power Control	Firmware Packa	ges 🛛		Add Local D				Name	
	Scrub Policies				Add CD-RC			:@ CD-ROM		
	📓 Serial over LA				🔚 Add Floppy			E Storage		
	🗐 Server Pool F							SAN	nrimary	
÷	Server Pool F	olicy Qualificatio	ns		vNICs		8		secondary	i
	📓 Threshold Po								, increased	
	🛐 iSCSI Authen				vHBAs					
		lacement Policie:			YNDAS		~			
	鶾 Sub-Organiza ፹- 撓 Marketin				💿 Add SAN Bo	pot				
	E 🎎 TenantA				Add San	Boot Target To	SAN prim	arv		
	S Adap					-				
	E S BIOS					Boot Target To	SAN seco	ondary		
	🔊 Boot				iSCSI vNICs	111111	*			
		Firmware Packa	jes 🛛							
	~	Access Profiles								
		Disk Config Polic	ies							
		enance Policies: gement Firmwar	e Packages							
		r Control Policie:								
	Scrub									
		l over LAN Policie	s							
		er Pool Policies								
		er Pool Policy Qu	alifications 🔜				L		_	_
		shold Policies								
		Authentication I								
		/vHBA Placemen Organizations	Policies	<u> </u>						
	- OD-	organizacions	<u> </u>							

1

Figure 109 Adding the SAN Boot Target

- **19.** Type the value as 0 for the Boot Target LUN.
- **20.** Enter the WWPN for the primary FC adapter interface 0c of controller A. To obtain the WWPN, login to controller A and in the command line type network interface show command.
- **21**. Be sure to use the FC portname for 0c and not the FC node name.
- **22**. Keep the type as Primary.
- **23**. Click **OK** to add the SAN boot target.

۵		Create Boot Policy
Create Boot Policy		
Description: Reboot on Boot Order Change: Enforce vNIC/vHBA/iSCSI Name: WARNINGS: The type (primary/secondary) does not The effective order of boot devices wit If Enforce vNIC/vHBA/iSCSI Name	hin the same device class (LAN/Storage is selected and the vNIC/vHBA/iSCSI o	s/ISCSI) is determined by PCIe bus scan order. Joes not exist, a config error will be reported. se the vNIC/vHBA/ISCSI with the lowest PCIe bus sca
Local Devices	Boot Order	rint
Add CD-ROM	Name	Order vNIC/vHBA/iSCSI vNIC
Add Floppy  VNICs  Add LAN Boot	Storage	1 TenantAFabricA ary Add SAN Boot Target
VHBAs	Add SAN Boo	ot Target 🛛 😵
Add SAN Boot Add SAN Boot Target	0	0:05:00:A0:98:37:A0:70
iSCSI vNICs 😵	Type: 0	Primary O Secondary
		OK Cancel

Figure 110 Adding the Boot Target LUN and WWPN Values

I

Γ

- 24. Under Boot Order in right pane select SAN Primary under Storage tree.
- 25. From the vHBA drop down menu, choose Add SAN Boot > Add San Boot Target to SAN Secondary.



Figure 111 Adding the SAN Boot Target to Secondary SAN

- **26.** Type the value 0 as the Boot Target LUN.
- **27.** Enter the WWPN for the primary FC adapter interface 0c of controller B. To obtain WWPN log in to the controller B and in the command line type the network interface show command.

Note

Ensure to use the FC portname for port 0c and not the FC node name.

- **28.** Click **OK** to add the SAN boot target.
- 29. Select Add SAN Boot under the vHBA drop-down menu.
- 30. Enter TenantAFabricB in the vHBA field in the Add SAN Boot window.
- **31.** The type should automatically be set to Secondary and it should be grayed out. This is fine.
- **32.** Click **OK** to add the SAN boot target.

<b>A</b>		Cr	eate Boo	ot Policy	
Create Boot Policy					
Name: Tenar Description: Reboot on Boot Order Change: Enforce vNIC/vHBA/ISCSI Name: WARNINGS: The type (primary/secondary) does not it The effective order of boot devices within If Enforce vNIC/vHBA/ISCSI Name is If it is not selected, the vNICs/vHBA/ISCSI	ndicate a boot order pr n the same device class ; selected and the «NIC	s (LAN/Storage/iSCSI) is de :/vHBA/iSCSI does not exi:	st, a config	error will be reported.	an order is used
Local Devices	Boot Order	▶ Export 😸 Print			_
Add CD-ROM Add Floppy	Name Storage SAN prin	nary	Order 1	VNIC/VHBA/ISCSI VNIC	Type Primary
VNICs		Target primary Target secondary		Boot Target	Primary Secondary
vHBAs 🛞		Add SAN Boo			0
Add SAN Boot Add SAN Boot Target		Boot Target LUN: 0 Boot Target WWPN: 2 Type:		0 Secondary	
				ОК	Cancel

Figure 112 Defining the SAN Boot Secndary Target Properties

- 33. Under Boot Order in right pane select SAN Secondary under Storage tree.
- **34.** From the vHBA drop down menu, choose **Add SAN Boot > Add San Boot Target To SAN primary**.
- **35**. Type the value as 0 for Boot Target LUN.
- **36.** Enter the WWPN for the primary FC adapter interface 0c of controller A. To obtain this information, log in to controller A and run the network interface show command.



ſ

Ensure to use the FC portname for 0c and not the FC node name.

- **37**. Keep the type as Primary.
- **38**. Click **OK** to add the SAN boot target.

<b>A</b>			Cr	eate Bo	ot Policy	
Create Boot Policy						
Name: Tenar Description: Reboot on Boot Order Change: Enforce vNIC/vHBA/iSCSI Name: WARNINGS: The type (primary/secondary) does not i The effective order of boot devices with If Enforce vNIC/vHBA/iSCSI Name is If it is not selected, the vNICs/vHBA/iSCSI	ndicate a boot ord n the same device s selected and the	class (LAN/Stor vNIC/vHBA/iSC	SI does not exis	st, a config	error will be reported.	an order is used.
Local Devices	Boot Order  Boot Order  Filt Name	er 👄 Export	👌 Print	Order	VNIC/VHBA/iSCSI VNIC	Туре
Add Floppy  VNICs  Add LAN Boot	SAN	primary 5AN Target pi 5AN Target se secondary	econdary	1	TenantAFabricA TenantAFabricB	Primary Primary Secondary Secondary
vHBAs		Add S	-		oot Target <b>et</b>	Primary
Add SAN Boot Add SAN Boot Target		Boot Tai	rget LUN: 0 t WWPN: 20:0 Type: • F	6:00:A0:9	8:37:40:70	
					ОК	iancel

### Figure 113 Defining the SAN Boot Target Primary Properties

- **39.** Under **Boot Order** in right pane select **SAN Secondary** under **Storage** tab.
- 40. Choose Add SAN Boot > Add San Boot Target To SAN secondary from the vHBA menu.
- 41. Type the value as 0 for the Boot Target LUN.
- **42.** Enter the WWPN for the primary FC adapter interface 0c of controller B. To obtain this information, log in to the controller B and run the network interface show command.

Note

Ensure to use the FC portname for port 0c and not the FC node name.

- 43. Click OK to add the SAN boot target.
- 44. Select Add SAN Boot under the vHBA drop-down menu.
- 45. Enter TenantAFabricB in the vHBA field in the Add SAN Boot window that displays.
- 46. The type should automatically be set to Secondary and it should be grayed out.
- 47. Click **OK** to add the SAN boot target.

Figure 114	Defining SA	N Boot Secondary	Target Properties

L

Γ

Create Boot Policy					
Name: Tenan Description: Reboot on Boot Order Change: Enforce vNIC/VHBA/ISCSI Name: WARNINGS: The type (primary/secondary) does not in The effective order of boot devices within If Enforce vNIC/VHBA/ISCSI Name is If it is not selected, the vNICs/vHBAs/ISCS	ndicate a boot order 1 the same device cla selected and the vM	ass (LAN/Storage/iSCSI) is d IIC/vHBA/iSCSI does not ex	ist, a config	error will be reported.	an order is used
Local Devices	🛨 🖃 🕰 Filter Name 🖃 💀 Storage	👄 Export 😸 Print	Order 1	VNIC/VHBA/i5CSI VNIC	Туре
vNICs 📚	SA SAN se SAN se	N Target primary N Target secondary econdary N Target primary		TenantAFabricA TenantAFabricB	Primary Primary Secondary Secondary Primary
vHBAs         Image: Constraint of the second s	SA	Add SAN Bo		Boot Target get	Secondary
iSCSI vNICs 😵		Boot Target LUN: 0 Boot Target WWPN: 2 Type:	:0:09:00:A(	0:98:37:A0:70 O Secondary	
				ОК	Cancel

**48.** The final TenantAFCBoot policy.

Figure 115 TenantAFCBpoot SAN Boot Policy Proper
--

1

		Create Bo	ot Policy				
eate Boot Policy							
Name: Te	nantAFCBoot						
Description:							
eboot on Boot Order Change:							
force vNIC/vHBA/iSCSI Name:							
ARNINGS:							
e type (primary/secondary) does n							
	ithin the same device class (LAN/Storage/ e is selected and the vNIC/vHBA/iSCSI do						
	/iSCSI are selected if they exist, otherwise			an order is used.			
Local Devices 🔗	Boot Order	_		_			
_	🔹 🖃 🔍 Filter 👄 Export 📚 Pri	int					
Add Local Disk Add CD-ROM	Name	Order	VNIC/VHBA/ISCSI VNIC	Туре	Lun ID	WWN	
Add Floppy	CD-ROM	1	WIC/WIDA/IDCDI WIC	туре		*****	
Had Hoppy	Storage	2					
	SAN primary	2	TenantAFabricA	Primary			
vNICs 🛞	🛒 SAN Target prima	ry		Primary	0	20:05:00:A0:98:37:A0:70	
(@) Add LAN Boot	SAN Target secon			Secondary	0	20:08:00:A0:98:37:A0:70	
MUG LAN BOOL	🖻 🛒 SAN secondary		TenantAFabricB	Secondary			
	🚽 🗐 SAN Target prima	ry		Primary	0	20:06:00:A0:98:37:A0:70	
vHBAs 🔗	🔤 🗐 SAN Target secon	dary		Secondary	0	20:09:00:A0:98:37:A0:70	
Add CAMP-1							
Add SAN Boot Add SAN Boot Target							
Contra Shiri Sober rangee							
iSCSI vNICs 📎							
iSCSI vNICs 🛛 💝	1						
iSCSI vNICs ⊗	1						
iSCSI vNICs ⊗	1						-
i5C5I vNICs ⊗							
iSCSI vNICs ⊗			🔺 Move Up 🔻 Move Down	Telete			
iSCSI vNICs ⊗			🔺 Move Up 🔻 Move Down	Tolete			

### **PXE Boot Policy for Baremetal RHEL 6.3 Host**

To configure PXE boot policy follow these setps :

- 1. Create Boot Policy TenantAPXEBoot on TenantA Org for SAN Boot Policy with primary and secondary type using two vHBAs as defined above in SAN Boot Policy for ESXi 5.1 host
- **2.** Add LAN Boot option, type PXE-A-NIC in vNIC field (Make sure PXE-A-NIC Static vNIC Name matches with LAN Boot Name (PXE-A-NIC)
- 3. Check Enforce vNIC/vHBA/iSCSI Name check box.

General Events			
Actions	Pronerties		
T Delete		AN Boot	X
Show Policy Usage	Add LAN Boot		0
	vNIC: <b>PXE-vNIC</b>	_	
Warning The type (primary/secondary) The effective order of boot di If Enforce vNIC/vHBA/iSC If it is not selected, the vNIC- order is used.			scan order. reported. west PCIe bus scan
Local De <del>v</del> ices		OK Can	
Add Local Disk	Name	Order	VNIC/VHBA/iSCSI VNIC
Add CD-ROM	CD-ROM	1	mic/mbh/bcbi mic
	Storage	2	
	📮 🗐 SAN primary		TenantAFabricA
vNICs	SAN Target p	-	
💿 Add LAN Boot	SAN Target s	econdary	TenantAFabricB
	SAN secondary	rimary	TenantAradricb
VHBAs	SAN Target s		
		. 3	
Add SAN Boot Add SAN Boot Target	an PXE-yNIC		PXE-vNIC
ACC SHIN BOOT Target			

### Figure 116 Defining the FCoE Boot Policy Properties

- 4. Select SAN in boot order and Move Up to first
- 5. Click Save

I

Γ

### Figure 117 Defining Boot Order Properties

Actions	Properties							
📅 Delete	Name: TenantAPX	EBoot						
Show Policy Usage	Description:							
A Use Global	Owner: Local							
🔲 Ose alobal	Reboot on Boot Order Change:							
	Enforce vNIC/vHBA/iSCSI Name:							
	Enforce WNIC/WHDA/ISCSI Name:							
Warning								
If Enforce vNIC/vHBA/iS0	The type (primary/secondary) does not indicate a boot order presence. The effective order of boot devices within the same device class (LAN/Storage/ISCSI) is determined by PCIe bus scan order. If Enforce vNIC/vHBA/ISCSI Name is selected and the vNIC/vHBA/ISCSI does not exist, a config error will be reported. If it is not selected, the vNICs/vHBA/ISCSI are selected if they exist, otherwise the vNIC/vHBA/ISCSI with the lowest PCIe bus scan order is used.							
Local Devices	Boot Order Boot Order  Contract Contrac	Order	VNIC/VHBA/ISCSI VNIC	Туре	Lun ID	www		
<b>O</b>		1	Witch Hompool Witc	Type	Carrie			
Add LAN Boot	SAN primary	1	TenantAFabricA	Primary				
	SAN Target primary			Primary	0	20:05:00:A0:98:37:A0:70		
vHBAs	SAN Target secondary			Secondary	0	20:08:00:A0:98:37:A0:70		
	⇒ ≡ SAN secondary		TenantAFabricB	Secondary				
iSCSI vNICs	SAN Target primary			Primary	0	20:06:00:A0:98:37:A0:70		
	SAN Target secondary			Secondary	0	20:09:00:A0:98:37:A0:70		
	i LAN	2						
	LAN PXE-A-NIC		PXE-A-NIC	Primary				

# **Configuring Storage Zoning**

After the Cisco UCS service profiles have been created (in the previous steps), the infrastructure blades in the environment each have a unique configuration. To proceed with the FlexPod deployment, specific information must be gathered from each Cisco UCS blade and from the NetApp controllers. Insert the required information in the tables below.

### Table 18 NetApp Controller FC Port FC Portname

Controller B

NetApp Controller	FC Port	FC Portname
Controller A	0c	50:0a:09:83:8d:93:40:7f

50:0a:09:83:9d:93:40:7f

I

# <u>Note</u>

On each NetApp controller CLI type the command show fcp adapters to gather the required information as listed in Table 19.

0c

### Table 19WWPN Values for Tenants A and B

Cisco UCS Service Profile Name	Fabric-A WWPN	Fabric-B WWPN
TenantA-HostA-Platinum-SLA1	20:00:00:25:b5:01:01:09	20:00:00:25:b5:01:01:08
TenantA-HostB-Platinum-SLA1	20:00:00:25:b5:01:01:07	20:00:00:25:b5:01:01:06

To gather the WWPN values for both the fabrics, launch the Cisco UCS Manager GUI, and follow the steps below:

- 1. In the left pane select the Servers tab.
- 2. Choose Servers > Service Profiles > root.
- 3. Click TenantA.
- 4. Click each service profile and then click the Storage tab in the right.
- **5.** Record the WWPN information in the right display window for both Fabric-A-HBA and Fabric-B-HBA for both the Service Profiles.

### **Creating VSANs, Assign FC Ports, Turn on FC Ports**

These steps provide details for configuring the necessary Zoneset and Zone members, to provide FC Initiator and target access to perform SAN Boot on UCS, NetApp Storage on Nexus network cloud environment

Note

This procedure sets up Fibre Channel connections between the Cisco Nexus 5548s and the NetApp storage systems.

### **Creating Zones and Zoneset**

These steps provide details for configuring zones members and Zoneset for the primary and secondary boot path with all target ports.

### Cisco Nexus 5548 A

To create the storage zone and the zoneset for each service profile, login to the Cisco Nexus switch and type the CLI commands listed in these steps:

- 1. Creating Zone.
- 2. Type zone name TenantA-HostA-Plantinum-SLA1 vsan 200.
- **3.** Type member pwwn 20:00:00:25:b5:01:01:01.
- **4.** Type member pwwn 20:05:00:a9:98:37:a0:70.
- **5.** Type member pwwn 20:06:00:a9:98:37:a0:70.
- 6. Type exit.
- 7. Type zone name TenantA-HostB-Plantinum-SLA1 vsan 200.
- 8. Type member pwwn 20:00:00:25:b5:01:01:03.
- **9.** Type member pwwn 20:05:00:a9:98:37:a0:70.
- **10.** Type member pwwn 20:06:00:a9:98:37:a0:70.
- 11. Type exit.
- 12. Type zone name TenantA-BareMetalHostA-Plantinum-SLA1 vsan 200.
- **13**. Type member pwwn 20:00:00:25:b5:04:00:06.
- 14. Type member pwwn 20:05:00:a9:98:37:a0:70.
- **15.** Type member pwwn 20:06:00:a9:98:37:a0:70.
- 16. Type exit.

```
<u>Note</u>
```

After the zone for the primary path of the first Cisco UCS service profiles has been created, create a zoneset to organize and manage them.

- 17. Create the zoneset and add the necessary members.
- **18.** Type zoneset name TenantA vsan 200.
- 19. Type member TenantA-HostA-Plantinum-SLA1.
- 20. Type member TenantA-HostB-Plantinum-SLA2.
- 21. Type exit.
- 22. Type member TenantA-BareMetalHostA-Plantinum-SLA2.
- 23. Type exit.
- 24. Activate the zoneset.
- **25.** Type zoneset activate name TenantA vsan 200.
- 26. Type exit.
- **27.** Type copy run start. The command output is below.

```
N5548-L21-A# sh zoneset vsan 200

zoneset name TenantA vsan 200

zone name TenantA-HostA-Plantinum-SLA1 vsan 200

pwwn 20:00:00:25:b5:01:01:01

pwwn 20:05:00:a9:98:37:a0:70

zone name TenantA-HostB-Plantinum-SLA1 vsan 200

pwwn 20:00:00:25:b5:01:01:03

pwwn 20:05:00:a9:98:37:a0:70

zone name TenantA-BareMetalHostA-Plantinum-SLA1 vsan 200

pwwn 20:00:00:25:b5:04:00:06

pwwn 20:05:00:a9:98:37:a0:70

zone name TenantA-BareMetalHostA-Plantinum-SLA1 vsan 200

pwwn 20:00:00:25:b5:04:00:06

pwwn 20:05:00:a9:98:37:a0:70

pwwn 20:06:00:a9:98:37:a0:70
```

Cisco Nexus 5548 B

- 1. Create the zone for each service profile.
- 2. Type zone name TenantA-HostA-Plantinum-SLA1 vsan 300.
- **3.** Type member pwwn 20:00:00:25:b5:01:01:02.
- **4.** Type member pwwn 20:05:00:a9:98:37:a0:70.
- 5. Type member pwwn 20:06:00:a9:98:37:a0:70.
- 6. Type exit.
- 7. Type zone name TenantA-HostB-Plantinum-SLA1 vsan 300.
- 8. Type member pwwn 20:00:00:25:b5:01:01:04.
- **9.** Type member pwwn 20:05:00:a9:98:37:a0:70.
- **10.** Type member pwwn 20:06:00:a9:98:37:a0:70.
- 11. Type exit.
- 12. Type zone name TenantA-BareMetalHostA-Plantinum-SLA1 vsan 200.
- **13.** Type member pwwn 20:00:00:25:b5:04:00:05.

- 14. Type member pwwn 20:05:00:a9:98:37:a0:70.
- **15.** Type member pwwn 20:06:00:a9:98:37:a0:70.
- 16. Type exit.



After the zone for the primary path of the first Cisco UCS service profiles has been created, create a zoneset to organize and manage them.

- **17.** Create the zoneset and add the necessary members.
- **18.** Type zoneset name TenantA vsan <300>.
- 19. Type member TenantA-HostA-Plantinum-SLA1.
- 20. Type member TenantA-HostB-Plantinum-SLA1.
- 21. Type exit
- **22.** Type member TenantA-BareMetalHostA-Plantinum-SLA2.
- 23. Type exit.
- **24.** Activate the zoneset.
- **25**. Type zoneset activate name TenantA vsan <300>.
- 26. Type exit
- 27. Type copy run start. The command output is below.

```
N5548-L21-A# sh zoneset vsan 10
zoneset name TenantA vsan 10
zone name TenantA-HostA-Plantinum-SLA1 vsan 300
pwwn 20:00:00:25:b5:01:01:02
pwwn 20:05:00:a9:98:37:a0:70
zone name TenantA-HostB-Plantinum-SLA1 vsan 300
pwwn 20:00:00:25:b5:01:01:04
pwwn 20:05:00:a9:98:37:a0:70
pwwn 20:06:00:a9:98:37:a0:70
zone name TenantA-BareMetalHostA-Plantinum-SLA1 vsan 200
pwwn 20:00:00:25:b5:04:00:05
pwwn 20:05:00:a9:98:37:a0:70
pwwn 20:06:00:a9:98:37:a0:70
```

# Citrix CloudPlatform Host Definition

Hosts are like a single computer that provides the computing resources to run the guest virtual machines. Hypervisor software is installed on each host to manage the guest VMs. Cisco Cisco UCS Manager ideally defines the VMware ESXi Server Compute, Storage, and Network cloud infrastructure design required for multi-tenant s to host their services based on the Service Levels Agreements (SLA) defined by the cloud providers.

The host definition design components are discussed below.

# Compute

The compute definition includes CPU, Memory and IO components which are required to support multi-tenants services (Applications) function in terms of performance, dynamic scaling, high availability, manageability and provisioning based on these data points service levels have been defined with associated cost.

To meet these service levels UCS offers Server Pools with qualification policies like CPU speed, and memory capacity definitions for various service levels which are included with Cisco UCS Manager for faster provision time to handle dynamic scaling requirements. UCS offers extended memory technology and 80G IO Virtual Interface Adapters with ether channels to handle multi-tenants services data traffic at any time with no single point of failure it offers high availability in cloud environment.

# Storage

The storage definition involves network scalability, data isolation, high availability and performance to support multi-tenant storage requirements. Based on these data points service levels have been defined with associated cost.

To meet storage requirements, UCS offers virtual Logical SANs to provide storage data isolation in multi-tenant cloud environments. To provide high availability UCS offers SAN Port Channels which takes care of any physically FC ports failures and also can be dynamically expanded to support scalability. On the compute host side each virtual host bus adapter (vHBAs) storage data is pinned to specific SAN Port Channels using SAN PIN Groups depending on the bandwidth service level requirement.

# Network

The network definition involves quality of service, high availability, scalability and performance to support multi-tenant storage requirements. Based on these data points service levels have been defined with associated cost.

To meet network definitions UCS offers virtual port channels and Virtual LANs to provide network data isolations in multi-tenant s cloud environment. To provide high availability UCS offers Ethernet Port Channels which takes care of any physical port failures and also dynamic expansion to support scalability. On the compute host side each virtual Ethernet adapter (vNICs) network data is pinned to specific LAN Port Channels using LAN PIN Groups depending on the bandwidth service level requirement.

# **Creating Service Profile Templates**

The service profile represents a logical view of a single blade server, without the need to know exactly which blade is discussed. The profile object contains the server personality: for example, identity and network information. The profile can then be associated with a single blade at a time. The Compute, Storage, and Network infrastructure components are all provisioned, configured and applied on cloud host server using UCS Service Profile Templates.

The service profile template is a single management configuration window where all of infrastructure components can be defined, configured and applied to multiple cloud hosts in the form of service profile.

The instructions below show creation of different service profile templates based on the service levels which can be later used to instantiate service profiles applied to individual cloud tenant host.

In this section the following tasks are elaborated:

- Compute Definition
- Network Definition
- Storage Definition

# **Compute Definition**

ſ

### **Creating Service Profile Templates**

This section details the creation of two service profile templates: one for Hypervisor ESX Host and second for Baremtal RHEL Operating System.

Hypervisior ESX Host Service Profile Template

Login to Cisco UCS Manager with User TenantA-Admin created earlier for Organization TenantA:

- 1. Click the Servers tab in the left pane.
- 2. Choose Service Profiles > Sub-Organization. Highlight TenantA.
- 3. Select Create Service Profile Templates on the General tab in the right pane.
- 4. The Create Service Profile Template window is displayed.
- 5. Name the service profile template Platinum-Template.
- 6. Select Initial Template.
- 7. In the UUID section, select Platinum-Compute-UUID as the UUID pool.
- 8. Click Next to continue to the next section.

Einung 110	Adding Unique Nome to the Comice Profile Templet	
Figure 118	Adding Unique Name to the Service Profile Templat	e

1

<b>A</b>	Create Service Profile Template
Unified C	Computing System Manager
Create Service Profile Template  1.   1.   1.   1.   1.   1.   1.   1.	Identify Service Profile Template       Image: The service profile template and specify the template type. You can also specify how a UUID will be assigned to this template and enter a description.         Name:       Platinum-Template         The template will be created in the following organization. Its name must be unique within this organization.         Where:       organization. Its name must be unique within this organization.         Type:       Initial Template         UDD       UDD will be assigned to the server associated with the service generated by this template.         UUID       UUID will be assigned from the selected pool.         The UUID will be assigned from the selected pool.       The valiable/total UUIDs are displayed after the pool name.         Optionally enter a description for the profile. The description can contain information about when and where the service profile should be used.
	< Prev Next > Finish Cancel

# **Network Definition**

### **Creating vNICS**

- 1. Leave the Dynamic vNIC Connection Policy field at the default.
- 2. Select Expert for the How would you like to configure LAN connectivity?
- 3. Click Add icon (Specify the desired number of vNICs that the server uses to connect to the LAN).
- 4. Create vNIC window opens.
- 5. Enter Management-A-NIC in the Name field.
- 6. Enable Use vNIC Template check box.
- 7. Select Management-A-NIC in vNIC Template list box.
- 8. Select VMWare in Adapater Policy list box.
- 9. Click OK.

# Create vNIC Create vNIC Name: Managment-A-NIC Use vNIC Template: Create vNIC Template VNIC Template: Managment-A-NIC Adapter Performance Profile Adapter Policy: WMWare Create Ethernet Adapter Policy

### Figure 119 Defining the vNIC Properties for Management A-NIC

- 10. Click Add.
- 11. Enter Management-B-NIC in the Name field.
- 12. Enable Use vNIC Template check box
- 13. Select Management-B-NIC in vNIC Template list box.
- 14. Select VMWare in Adapater Policy list box.
- **15.** Click **OK**.

### Figure 120 Defining vNIC properties for the Management B-NIC



- 16. Click Add
- 17. Enter guest-A-NIC in the Name field.
- **18**. Enable **Use vNIC Template** check box.
- **19.** Select **guest-A-NIC** in vNIC Template list box.
- 20. Select VMWare in Adapater Policy list box.
- 21. Click OK.

I

2	Create
Create vNIC	
Name: Guest-A-NIC	
Use vNIC Template: V Create vNIC Template	
vNIC Template: Guest-A-NIC	-
. 0	
• O Adapter Performance Profile –	

### Figure 121 Defining vNIC Properties for the guest-A-NIC

- 22. Click Add.
- 23. Enter Guest-A-NIC in the Name field.
- 24. Enable Use vNIC Template check box.
- 25. Select guest-A-NIC in vNIC Template list box.
- 26. Select VMWare in Adapater Policy list box.
- 27. Click OK.

### Figure 122 Defining vNIC Properties for the guest-B-NIC



- 28. Click Add.
- 29. Enter NFS-A-NIC in the Name field.
- 30. Enable Use vNIC Template check box
- 31. Select NFS-A-NIC in vNIC Template list box.
- 32. Select VMWare in Adapater Policy list box.
- 33. Click OK.

# Figure 123Defining vNIC Properties for the NFS-A-NIC

▲ Create vNIC
Create vNIC
Name: NFS-A-NIC Use vNIC Template: Create vNIC Template
vNIC Template: NFS-A-NIC
Adapter Performance Profile Adapter Policy: VMWare Create Ethernet Adapter Policy

- 34. Click Add.
- 35. Enter NFS-B-NIC in the Name field.
- 36. Enable Use vNIC Template check box.
- 37. Select NFS-B-NIC in vNIC Template list box.
- 38. Select VMWare in Adapater Policy list box.
- **39.** Click **OK**.

### Figure 124 Defining vNIC Properties for the NFS-B-NIC



# **Storage Definition**

### **Creating vHBAs**

ſ

- 1. Select TenantLocalDisk for Local Storage field.
- 2. Click Expert to define how would you like to configure SAN connectivity field.
- **3.** In the WWNN Assignment field, select Platinum-Compute-WWNN.



Figure 125 Defining the Disk Policies and SAN Storage Properties

- a. Click Add button to add vHBAs to the template.
- b. Enter TenantAFabricA in the Name field.
- c. Select Use vHBA Template check box.
- d. Select TenantAFabricA in vHBA Template.
- e. Select VMWare Adapter Policy list box.
- f. Click OK.

### Figure 126 Defining the vHBA Values for the Fabric-A-HBA

_	
4	Create vHBA
1	Create vHBA
	Name: TenantAFabricA
	vHBA Template: TeantAFabricA
	Adapter Performance Profile
	Adapter Policy: VMWare

- g. Click Add button to add vHBAs to the template.
- **h.** Enter **TenantAFabricB** in the Name field.
- i. Select Use vHBA Template check box.
- j. Select TenantAFabricB in vHBA Template.
- k. Select VMWare Adapter Policy list box.
- I. Click OK.

Figure 127 Defining the vHBA Values for the Fabric-B-HBA

	Create vHBA
C	Create vHBA
	Name: TenantAFabricB Use vHBA Template: ↓ Create vHBA Template
	vHBA Template: TenantAFabricB
ſ	Adapter Performance Profile
	Adapter Policy: VMWare

- 4. Click Next to continue to the next section.
- 5. Zoning section
  - **a**. Accept all values as default.
- 6. Click Next.

Figure 128 Define the Zoning Information

🚖 Cisco Unified Computing System Manager - TME	🗼 Create Service Profile Template	
Fault Summary	Unified	Computing System Manager
2 52 8 40 Equipment Servers LAN SAN VM Admin Filter: Al Servers Servers Servers Service Profiles Service Profiles Service Profile Templates Service Profile Templates Service Profile Templates Service Profile Service Profil	Create Service Profile Template 1. √ Identify Service Profile Template 2. √ Hetworking 3. √ Storage 4. √ Zoning 5. √ HIC/M+BA Placement 6. √ Server Boot Order. 7. √ Maintenance Policy 8. √ Server Assignment, 9. √ Operational Policies	Zoning         Specify zoning information         WARNING: Switch in end-host mode. In end-host mode, zoning configuration will NOT be applied.         Zoning configuration involves the following steps:         1. Select WHBA Initiators ((WHBAs are created on storage page)         2. Select WHBA Initiator Group(s)         Select WHBA Initiator Group(s)         Select WHBA Initiators         Select WHBA Initiators         Name         Storage Connection Policy Name         Pabric-8-HBA         >> Add To >>         Select @ Initiator
7. (	Click Next to contin	nue to the next section.

8. vNIC/vHBA Placement Section

ſ

b. Select the Manual Placement Policy in the Select Placement field.

1

- **c.** Select vCon1 assign the vNICs in the following order:
- Management-A-NIC
- guest-A-NIC
- NFS-A-NIC
- Fabric-A-HBA

Figure 129

Defining the vNIC and vHBA Placement

<b>A</b>		Cisco Unified Compu	iting System Manager - TME-L21			
Fault Summary	A A G	) 🛑 💷 New 🚽 🛃 Options <table-cell> 🚯 📥 Pending A</table-cell>	ctivities 0 Exit			
₩ ¥ 4						x
	<u>A</u>	Create Se	rvice Profile Template			
Equipment Servers LAN SAN VM Admin	Unified (	Computing Syste	m Managor			
Filter: All	Unineu (	somputing Syste	enn manayer			
Servers     Servers     Servers     Servers     Servers     Servers     Servers     Servers     Sub-Organizations     Sub-Organizations     Sub-Organizations     Server Pools     Server Po	Create Service Profile Template  1. √Identify Service Profile 2. √Networking 3. √Sorage 4. √Zoning 5. √ <u>VRUC/VHBA Placement</u> 6. □ Server Boot Order 7. □ Maintenance Policy 8. □ Server Assignment, 9. □ <u>Operational Policies</u>	VNIC/vHBA Placement Specify how vNICs and vHBAs are place VNIC/vHBA Placement specifies how VNICs and vHBAs in a server hardware configuration independent way.	ed on physical network adapters are placed on physical network adapters (nezz are placed on physical network adapters (nezz controlled by placement Policy controlled by placement preferences. e or more VNICs or VHBAs Specific Virtual Network Interfaces (click on a controlled by placement preferences. e or more VNICs or VHBAs Specific Virtual Network Interfaces (click on a controlled by placement preferences. e or more VNICs or VHBAs Specific Virtual Network Interfaces (click on a controlled by placement preferences. e or more VNICs or VHBAs Specific Virtual Network Interfaces (click on a controlled by placement preferences. e or More Specific Virtual Network Interfaces (click on a controlled by placement preferences. e or More Specific Virtual Network Interfaces (click on a controlled by placement preferences. e or More Specific Virtual Network Interfaces (click on a controlled by placement preferences. e or More Specific Virtual Network Interfaces (click on a controlled by placement preferences. e or More Specific Virtual Network Interfaces (click on a controlled by placement preferences. e or More Specific Virtual Network Interfaces (click on a controlled by placement preferences. e or More Specific Virtual Network Interfaces (click on a controlled by placement preferences. e or More Specific Virtual Network Interfaces (click on a controlled by placement preferences. e or More Specific Virtual Network Interfaces (click on a controlled by placement preferences. e or More Specific Virtual Network Interfaces (click on a controlled by placement preferences. e or More Specific Virtual Network Interfaces (click on a controlled by placement preferences. e or More Specific Virtual Network Interfaces (click on a controlled by placement preferences. e or More Specific Virtual Network Interfaces (click on a controlled by placement preferences. e or More Specific Virtual Network Interfaces (click on a controlled by placement preferences. e or More Specific Virtual Network Interfaces (click on a controlled by placement pr	il network adapters s assignment can be 3A or it can be done	selection Preference All All All All	

- d. Select vCon2, and assign the vNICs in the following order:
- Management-B-NIC
- guest-B-NIC
- NFS-B-NIC
- Fabric-B-HBA
- 9. Click Next.



### Figure 130 Assigning the vNICs in the vCon2

- **10.** Server Boot Order Section
  - a. Select TenantAFCBoot Boot Policy.
- 11. Click Next.

I

### Figure 131 Applying TenantFCBoot Boot Policy for the Service Profile Template



- 12. Maintenance Policy Section
  - a. Select default Maintenance Policy.
- 13. Click Next.

Figure 132 Applying default Policies applied for Maintenance Policy During Service Disruptions



- 14. Server Assignment Section
  - a. Select Platinum-Compute-ServerPool for Pool Assignment.

- **b.** Click **Up** radio button to select the power state to be applied when this profile is associated with the server.
- c. Select PlatinumSvrQual for Server Pool Qualification.
- **d.** Do not check Restrict Migration.
- 15. Click Next.

Figure 133 Associating the Server Pool with the Service Profile

📥 Cisco Unified Computing System Manager - TME	🌲 Create Service Profile Template	2	
Fault Summary	Unified	Computing System Manager	
2 52 8 40 Equipment Servers LAN SAN VM Admin	Create Service Profile Template 1. √Identify Service Profile	Server Assignment Optionally specify a server pool for this service profile template.	
Service Profiles	Iemplate       2. √ <u>Networkina</u> 3. √ <u>Storage</u> 4. √ <u>Zonina</u> 5. √ <u>VNIC/VHBA Placement</u> 6. √ <u>Server Boot Order</u> 7. √ <u>Maintenance Policy</u>	You can select a server pool you want to associate with this service profile template. Pool Assignment: Platinum-Compute-ServerPool  Floate Server Pool  Select the power state to be applied when this	
Orbitations     Orbitations     Orbitation     Orbitatio     Orbitatio     Orbitation     Orbitation     Orbitation     O	Server Assignment     Operational Policies	profile is associated with the server.	
⊞ ∰ Schedules		The service profile template will be associated with one of the servers in the selected pool. If desired, you can specify an additional server pool policy qualification that the selected server must meet. To do so, select the qualification from the list. Server Pool Qualification: PlatnumSvrQual	
		Restrict Migration:	
		Firmware Management (BIOS, Disk Controller, Adapter)	8

- **16.** Operational Policies Section
  - a. Select TenantA-BIOS for BIOS Policy.
  - b. Select default for External IPMI Management Configuration
  - c. Select Platinum-Compute-IP for Management IP Address Policy.
  - d. Select default for Monitoring Configuration.
  - e. Select default for Power Control Policy Configuration.
  - f. Select default for Scrub Policy.
- 17. Click Next.

ſ



Figure 134 Defining the attributes for the Operational Policy

Follow the steps described above to create Service Profile Templates for Gold-Template, Silver-Template and Bronze-Template with data values listed in Table 20 and Table 21.

Table 20 Se	rvice Profile Temp	ates
Name	Туре	UUID
Gold-Template	Initial Template	Gold-Compute-UUID
Silver-Template	Initial Template	Silver-Compute-UUID
Bronze-Template	Initial Template	Bronze-Compute-UUID

### Table 20 Service Profile Templates

### Table 21 Ne

Networking Configuration

Dynamic vNIC Connection Policy	Configure LAN Connectivity		
No Dynamic vNIC Policy by default	Expert		

1

Create vNIC For Gold-Template as per the values defined in Table 22.

Name	MAC Address	Fabric ID	VLAN Native VLAN	MTU	Pin Group	Adapter policy	Dynamic vNIC Connection Policy	QoS Policy	Network Control Policy
Manage ment-A -NIC	Gold-Co mpute-M AC	А	Manage ment-VL AN	9000	Tenant A-Net- PIN	default	Not set	Platinum- Net-SLA	default
Manage ment-B -NIC	Gold-Co mpute-M AC	В	Manage ment-VL AN	9000	Tenant A-Net- PIN	default	Not set	Platinum- Net-SLA	default
guest-A -NIC	Gold-Co mpute-M AC	А	guest-VL AN	9000	Tenant A-Net- PIN	default	Not set	Gold-Net -SLA	default
guest-B -NIC	Gold-Co mpute-M AC	В	guest-VL AN	9000	Tenant A-Net- PIN	default	Not set	Gold-Net -SLA	default
NFS-A- NIC	Gold-Co mpute-M AC	А	guest-VL AN	9000	Tenant A-Net- PIN	default	Not set	Silver-Ne t-SLA	default
NFS-B- NIC	Gold-Co mpute-M AC	В	guest-VL AN	9000	Tenant A-Net- PIN	default	Not set	Silver-Ne t-SLA	default

Table 22	vNICs and their Properties for the Gold Service Class

I

Γ

Create vNIC For Silver-Template using the values defined in Table 23.

 Table 23
 vNICs and their Properties for the Silver Service Class

Name	MAC Address	Fabric ID	VLAN Native VLANs	мти	Pin Group	Adapter policy	Dynamic vNIC Connection Policy	QoS Policy	Network Control Policy
Manag ement- A-NIC	Silver-C ompute- MAC	A	Manageme nt-VLAN	9000	Tenant A-Net- PIN	default	Not set	Platinu m-Net- SLA	default
Manag ement- B-NIC	Silver-C ompute- MAC	В	Manageme nt-VLAN	9000	Tenant A-Net- PIN	default	Not set	Platinu m-Net- SLA	default
guest-A -NIC	Silver-C ompute- MAC	A	guest-VL AN	9000	Tenant A-Net- PIN	default	Not set	Gold-N et-SLA	default
guest-B -NIC	Silver-C ompute- MAC	В	guest-VL AN	9000	Tenant A-Net- PIN	default	Not set	Gold-N et-SLA	default

NFS-A -NIC	Silver-C ompute- MAC	А	guest-VL AN	9000	Tenant A-Net- PIN	default	 Silver- Net-SL A	default
NFS-B- NIC	Silver-C ompute- MAC	В	guest-VL AN	9000	Tenant A-Net- PIN	default	Silver- Net-SL A	default

1

 Table 23
 vNICs and their Properties for the Silver Service Class

Create vNIC For Bronze-Template using the values defined in Table 24.

### Table 24vNICs and Their Properties for the Bronze Class

Name	MAC Address	Fabric ID	VLAN Native VLANs	MTU	Pin Group	Adapter policy	Dynamic vNIC Connection Policy	QoS Policy	Network Control Policy
Manag ement- A-NIC	Bronze- Comput e-MAC	А	Managem ent-VLA N	9000	Tenant A-Net- PIN	default	Not set	Platinum- Net-SLA	default
Manag ement- B-NIC	Bronze- Comput e-MAC	В	Managem ent-VLA N	9000	Tenant A-Net- PIN	default	Not set	Platinum- Net-SLA	default
guest- A-NIC	Bronze- Comput e-MAC	А	guest-VL AN	9000	Tenant A-Net- PIN	default	Not set	Gold-Net -SLA	default
guest- B-NIC	Bronze- Comput e-MAC	В	guest-VL AN	9000	Tenant A-Net- PIN	default	Not set	Gold-Net -SLA	default
NFS-A -NIC	Bronze- Comput e-MAC	А	guest-VL AN	9000	Tenant A-Net- PIN	default	Not set	Silver-Ne t-SLA	default
NFS-B -NIC	Bronze- Comput e-MAC	В	guest-VL AN	9000	Tenant A-Net- PIN	default	Not set	Silver-Ne t-SLA	default

### Table 25Storage Configurations

Local Storage	Configure SAN Connectivity	WWNN Assignment
TenantLocalDisk	Expert	Gold-Compute-WWNN

Name	WWPN	Fabric ID	VSAN	Pin Group	Persistent Binding	Max Data field Size	Adapter Policy	QoS Policy
	Gold-Com pute-WWP N	А	10	TenantA-S AN-PIN	Enabled	2048	default	FC-Net- SLA
	Gold-Com pute-WWP N	В	10	TenantA-S AN-PIN	Enabled	2048	default	FC-Net- SLA

### Table 26vSAN values for the Fabric A and B

Table 27

Zoning and vNIC / vHBA Placement

Zoning	vHBA Placement			
Default	Manual			

### Table 28

vNIC and vHBA Placement on vCon1 and vCon2

vCon1	vCon2
Management-A-NIC	Management-B-NIC
guest-A-NIC	guest-B-NIC
NFS-A-NIC	NFS-B-NIC
Fabric-A-HBA	Fabric-B-HBA

Table 29

Values for Server Boot Order and the Maintenance Policy

Boot Policy	Maintenance Policy
TenantAFC-Boot	Default

### Table 30Server Assignment

ſ

Pool Assignment	Power State	Server Pool Qualification	<b>Restrict Migration</b>
Gold-Compute-ServerPool	Up	GoldSvrQual	Un Check
Silver-Compute-ServerPool	Up	SilverSvrQual	Un Check
Bronze-Compute-ServerPool	Up	BronzeSvrQual	Un Check

BIOS Policy	External IPMI Management	Management IP Address	Monitoring Configuration	Power Control Policy	Scrub Policy
TenantA-BIOS	default	Gold-Compute-I P	default	default	default
TenantA-BIOS	default	Silver-Compute- IP	default	default	default
TenantA-BIOS	default	Bronze-Comput e-IP	default	default	default

Table 31	<b>Operational Policies</b>
----------	-----------------------------

### **Baremetal RHELHost Service Profile Template**

This section details the creation of Baremetal Service Profile Template defined to provision blade to host RHEL 6.X Opertaing System using CloudPlatfrom 4.2.1.

For Baremetal as a Service the Service profile Templates, Pools (UUID, MAC, IP, PWWN, WWNN, and Server), vNIC & vHBA Templates, Policies (Boot, IPMI, Adapater, BIOS, Firwware) must be created on root organization.



In this study we do not show steps to create below Pools, Policies, vHBA Templates we expect all are created under root Organization, for more details in creating them see Cloud Compute Design and Deployment section

- **1**. Platinum-Compute-UUID
- 2. Baremetal-Disk
- 3. Platinum-Compute-WWNN
- 4. Platinum-Compute-WWPN

Login to Cisco UCS Manager with User Admin:

- 1. Click the Servers tab in the left pane.
- 2. Choose Service Profiles > root.
- 3. Select Create Service Profile Templates on the General tab in the right pane.
- 4. The Create Service Profile Template window is displayed.
- 5. Name the service profile template Platinum-Baremetal-Template.
- 6. Select Initial Template.
- 7. In the UUID section, select BarePlatinum-Compute-UUID as the UUID pool.

1

8. Click Next to continue to the next section.

### Figure 135 Adding Unique Name to the Service Profile Template

▲ Create Service Profile Template X				
Unified Computing System Manager				
Create Service Profile Template  1. √ Identify Service Profile Template  2. √ Networking  3. √ Storage  4. √ Zoning  5. √ vNIC/VHBA Placement  6. √ Server Boot Order  7. √ Maintenance Policy  8. √ Server Assignment  9. √ Operational Policies	Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Image: Colspan="2">Colspan="2">Image: Colspan="2">Colspan="2"Colspan="2"Colspan="2"Colspan="2"Colspan="2"Colspan="2"Colspan="2"Colspan="2			
	< Prev Next > Finish Cancel			

# **Network Definition**

### **Creating vNICS**

ſ

- 1. Leave the Dynamic vNIC Connection Policy field at the default.
- 2. Select Expert for the How would you like to configure LAN connectivity?
- 3. Click Add icon (Specify the desired number of vNICs that the server uses to connect to the LAN).
- 4. Create vNIC window opens.
- 5. Enter Bare-MGMT-A-NIC in the Name field.
- 6. Enable Use vNIC Template check box.
- 7. Select Bare-MGMT-A-NIC in vNIC Template list box.
- 8. Select Linux in Adapater Policy list box.
- 9. Click OK.



### Figure 136 Defining the vNIC Properties for Bare-MGMT-A-NIC

- 10. Click Add.
- 11. Enter PXE-A-NIC in the Name field.
- 12. Enable Use vNIC Template check box.
- 13. Select PXE-A-NIC in vNIC Template list box.
- 14. Select Linux in Adapater Policy list box.
- 15. Click OK.

### Figure 137 Defining vNIC properties for the PXE-A-NIC



### **Storage Definition**

### **Creating vHBAs**

- 1. Select TenantLocalDisk for Local Storage field.
- 2. Click Expert to define How would you like to configure SAN connectivity field.

- 3. In the WWNN Assignment field, select Platinum-Compute-WWNN
- 4. Click Add.

- 5. Enter TenantAFabricA in the Name field
- 6. Enable Use vHBA Template check box
- 7. Select TenantAFabricA in vHBA Template
- 8. Select Linux in Adapater Policy

Figure 138 Defining the TenantAFabricA vHBA for the Service Profile Template

▲ Create vHE	3A
Create vHBA	
Name: TenantAFabricA Use vHBA Template: Create vHBA Template	
vHBA Template: TenantAlFabricA	
Adapter Performance Profile	
Adapter Policy: Linux Create Fibre Channel Adapter Policy	

- 9. Click Add.
- **10.** Enter TenantAFabricB in the Name field.
- **11.** Enable Use vHBA Template check box.
- **12.** Select TenantAFabricA in vHBA Template.
- 13. Select Linux in Adapater Policy.

Figure 139 Defining the TenantAFabricB vHBA for the Service Profile Template

<b>A</b>	Create vHBA
Create vHBA	
Name: TenantAFabricB Use vHBA Template Create vHBA Template	
vHBA Template: TenantAFabricB	
Adapter Performance Profile Adapter Policy: Linux	Create Fibre Channel Adapter Policy

- 14. Click Next to continue to the next section.
- 15. Zoning section
  - a. Accept all values as default.
- 16. Click Next.

ſ

Figure 140	Define the Zoning	Information
Figure 140	Define the Zoning	information

A		Create Service	Profile Templat	e	X
Unified 0	Computing	System	n Mana	ager	
Create Service Profile Template	<b>Zoning</b> Specify zoning informa	tion			Ø
Template         2. √ <u>Networking</u> 3. √ <u>Storage</u> 4. √ <u>Zoning</u> 5. □ <u>vNIC/vHBA Placement</u> 6. □ <u>Server Boot Order</u> 7. □ <u>Maintenance Policy</u> 8. □ <u>Server Assignment</u> 9. □ <u>Operational Policies</u>	WARNING: Switch in end-ho Zoning configuration involves the 1. Select vHBA Initiator(s) (vl 2. Select vHBA Initiator Group 3. Add selected Initiator(s) to Select vHBA Initiators Name	following <b>steps:</b> HBAs are created on storag (\$) selected Initiator Group(s)			
	TenantAFabricA ^ TenantAFabricB	>> Add To >>	Name	Storage Connection Policy Name	<b>F</b>
				👕 Delete 📑 Add 📑 Modify	~

1

- 17. Click Next to continue to the next section.
- **18.** vNIC/vHBA Placement Section
  - a. Select Let System Perform Placement Policy in the Select Placement field.
- 19. Click Next.

### Figure 141 Defining the vNIC and vHBA Placement

<b>A</b>	Create	e Service Profile Temp	late	
Unified C	Computing Sys	stem Mar	nager	
Create Service Profile Template	vNIC/vHBA Placement Specify how vNICs and vHBAs are	placed on physical netwo	ork adapters	
1. √ <u>Identify Service Profile</u> <u>Template</u> 2. √Networking	vNIC/vHBA Placement specifies how vNICs and vH in a server hardware configuration independent w	BAs are placed on physical n		zanine)
3. $\sqrt{\frac{\text{Storage}}{2\text{oning}}}$				
5. √ <u>vNIC/vHBA Placement</u> 6. □ <u>Server Boot Order</u>	Select Placement: Let System Perform Placen	n 🔻 🚹 Create Placem	nent Policy	
7. <u>Maintenance Policy</u> 8. <u>Server Assignment</u> 9. Operational Policies	System will perform automatic placement of v	/NICs and vHBAs based on PO	II order.	
operacional Policies	Name	Address	Order	₽
	whice Bare-MGMT-A-NIC	Derived	1	^
		Derived	2	
		Derived	3	
		Derived	4	
1				

- 20. Server Boot Order Section
  - a. Select TenantAPXEBoot Boot Policy.

### 21. Click Next.

		Modify Boot F	Policy			
Iodify Boot Policy						
oot Policy: TenantAPXEBoot	Crea	ate Boot Policy				
Name: <b>Te</b>	nantAPXEBoo	ıt				
Description:						
Reboot on Boot Order Change: No						
Enforce vNIC/vHBA/iSCSI Name: Ye	s					
WARNINGS:						
	In the alternative section	aat ardar processo				
The type (primary/secondary) does r	not indicate a bo	ood order presence.				
The effective order of boot devices v	within the same	device class (LAN/Storage/iSCSI) is				
The effective order of boot devices ( If Enforce vNIC/vHBA/iSCSI Nam	within the same <b>ne</b> is selected a	device class (LAN/Storage/iSCSI) is and the vNIC/vHBA/iSCSI does not	exist, a config error	will be reported	ł.	
The effective order of boot devices v	within the same <b>ne</b> is selected a	device class (LAN/Storage/iSCSI) is and the vNIC/vHBA/iSCSI does not	exist, a config error	will be reported	ł.	is used.
The effective order of boot devices on If <b>Enforce vNIC/vHBA/iSCSI Nan</b> If it is not selected, the vNICs/vHBA:	within the same <b>ne</b> is selected a	device class (LAN/Storage/iSCSI) is and the vNIC/vHBA/iSCSI does not	exist, a config error	will be reported	ł.	is used.
The effective order of boot devices u If <b>Enforce vNIC/vHBA/iSCSI Nan</b> If it is not selected, the vNICs/vHBA: Boot Order	within the same ne is selected a s/iSCSI are sele	device class (LAN/Storage/iSCSI) is and the vNIC/vHBA/iSCSI does not	exist, a config error	will be reported	ł.	is used.
The effective order of boot devices on If <b>Enforce vNIC/vHBA/iSCSI Nan</b> If it is not selected, the vNICs/vHBA:	within the same ne is selected a s/iSCSI are sele	device class (LAN/Storage/iSCSI) is and the vNIC/vHBA/iSCSI does not	exist, a config error	will be reported	ł.	is used.
The effective order of boot devices u If <b>Enforce vNIC/vHBA/iSCSI Nan</b> If it is not selected, the vNICs/vHBA: Boot Order	within the same ne is selected a s/iSCSI are sele	device class (LAN/Storage/iSCSI) is and the vNIC/vHBA/iSCSI does not	exist, a config error	will be reported	ł.	is used.
The effective order of boot devices u If Enforce vNIC/vHBA/ISCSI Nan If it is not selected, the vNICs/vHBA: Boot Order Image: Inter Store Export Prime Name Image: Storage	within the same ne is selected a s/iSCSI are sele nt	device class (LAN/Storage/ISCSI) i and the vNIC/VHBA/ISCSI does not cted if they exist, otherwise the vN	exist, a config error NIC/∨HBA/iSCSI with	will be reported the lowest PCI	d. ie bus scan order i	
The effective order of boot devices of If Enforce VNIC/VHBA/ISCSI Nam If it is not selected, the VNICs/VHBA/ Boot Order	within the same ne is selected a s/iSCSI are sele nt Order	device class (LAN/Storage/ISCSI) i and the vNIC/VHBA/ISCSI does not cted if they exist, otherwise the vN	exist, a config error NIC/∨HBA/iSCSI with	will be reported the lowest PCI	d. ie bus scan order i	
The effective order of boot devices u If Enforce VNIC/VHBA/ISCSI Nan If it is not selected, the VNICs/VHBA/ Boot Order	within the same ne is selected a s/ISCSI are sele nt Order 1	device class (LAN/Storage/ISCSI) in and the vNIC/VHBA/ISCSI does not cted if they exist, otherwise the vN vNIC/VHBA/ISCSI vNIC	exist, a config error JIC/vHBA/iSCSI with Type	will be reported the lowest PCI	d. ie bus scan order i	<b>.</b>
The effective order of boot devices of If Enforce VNIC/VHBA/ISCSI Nam If it is not selected, the VNICs/VHBA/ Boot Order The Constant of the Constant of th	within the same ne is selected a s/ISCSI are sele nt Order 1	device class (LAN/Storage/ISCSI) in and the vNIC/VHBA/ISCSI does not cted if they exist, otherwise the vN vNIC/VHBA/ISCSI vNIC	exist, a config error JIC/VHBA/ISCSI with Type Primary	will be reported in the lowest PCI	d. ie bus scan order i wwn	<b>E</b> • •
The effective order of boot devices u If Enforce VNIC/VHBA/ISCSI Nan If it is not selected, the VNICs/VHBA/ Boot Order	within the same ne is selected a s/ISCSI are sele nt Order 1	device class (LAN/Storage/ISCSI) in and the vNIC/VHBA/ISCSI does not cted if they exist, otherwise the vN vNIC/VHBA/ISCSI vNIC	exist, a config error IIC/vHBA/iSCSI with Type Primary Primary	uvill be reported the lowest PCI	d. le bus scan order i WWN 20:05:00:A0	<b>E</b> • •
The effective order of boot devices u If Enforce VNIC/VHBA/ISCSI Nan If it is not selected, the VNICs/VHBA/ Boot Order	within the same ne is selected a s/ISCSI are sele nt Order 1	device class (LAN/Storage/ISCSI) ii and the vNIC/vHBA/ISCSI does not cted if they exist, otherwise the vf vNIC/vHBA/ISCSI vNIC TenantAFabricA	exist, a config error IIC/VHBA/ISCSI with Type Primary Primary Secondary	uvill be reported the lowest PCI	d. le bus scan order i WWN 20:05:00:A0	D:
The effective order of boot devices u If Enforce vNIC/vHBA/ISCSI Nan If it is not selected, the vNICs/vHBA/ Boot Order	vithin the same ne is selected a s/ISCSI are sele nt Order 1	device class (LAN/Storage/ISCSI) ii and the vNIC/vHBA/ISCSI does not cted if they exist, otherwise the vf vNIC/vHBA/ISCSI vNIC TenantAFabricA	exist, a config error IIC/VHBA/iSCSI with Type Primary Primary Secondary Secondary	Lun ID	d. le bus scan order i www 20:05:00:A( 20:08:00:A(	D:
The effective order of boot devices u If Enforce vNIC/vHBA/ISCSI Nan If it is not selected, the vNICs/vHBA: Boot Order	vithin the same ne is selected a s/ISCSI are sele nt Order 1	device class (LAN/Storage/ISCSI) ii and the vNIC/vHBA/ISCSI does not cted if they exist, otherwise the vf vNIC/vHBA/ISCSI vNIC TenantAFabricA	exist, a config error IIC/vHBA/iSCSI with Type Primary Primary Secondary Secondary Primary	ULUN ID	d. le bus scan order i WWN 20:05:00:A( 20:06:00:A( 20:06:00:A(	D:
The effective order of boot devices of If Enforce VNIC/VHBA/ISCSI Nan If it is not selected, the VNICs/VHBA/ Boot Order	within the same ne is selected a s/iSCSI are sele nt Order 1	device class (LAN/Storage/ISCSI) ii and the vNIC/vHBA/ISCSI does not cted if they exist, otherwise the vf vNIC/vHBA/ISCSI vNIC TenantAFabricA	exist, a config error IIC/vHBA/iSCSI with Type Primary Primary Secondary Secondary Primary	ULUN ID	d. le bus scan order i WWN 20:05:00:A( 20:06:00:A( 20:06:00:A(	D:
The effective order of boot devices u If Enforce VNIC/VHBA/ISCSI Nan If it is not selected, the VNICs/VHBA/ Boot Order	within the same ne is selected a s/iSCSI are sele nt Order 1	device class (LAN/Storage/ISCSI) i and the vNIC/VHBA/ISCSI does not cted if they exist, otherwise the v1 vNIC/vHBA/ISCSI vNIC TenantAFabricA TenantAFabricB	exist, a config error JIC/VHBA/ISCSI with Type Primary Primary Secondary Secondary Primary Secondary	ULUN ID	d. le bus scan order i WWN 20:05:00:A( 20:06:00:A( 20:06:00:A(	D:

### Figure 142 Defining the Boot Policy for the Service Profile Template

- 22. Maintenance Policy Section
  - **a**. Select default Maintenance Policy
- 23. Click Next.

Γ

### Figure 143 Defining the Policies applied to Server During Service Disruptions

<u>A</u>	Create Service Profile Template
Unified (	Computing System Manager
Create Service Profile Template 1. <u>√Identify Service Profile</u> <u>Template</u>	Maintenance Policy Specify how disruptive changes such as reboots, network interruptions, and firmware upgrades associated with this service profile.
<ol> <li>√<u>Networking</u></li> <li>√<u>Storage</u></li> <li>√<u>Zoning</u></li> <li>√<u>VNIC/VHBA Placement</u></li> <li>√<u>Server Boot Order</u></li> <li>√<u>Maintenance Policy</u></li> <li>□<u>Server Assignment</u></li> </ol>	Maintenance Policy         Image: Control of the service profile or create a new maintenance policy that will be accessible to all service profiles.
9. D <sub>Operational Policies</sub>	Maintenance Policy: default 🔹 🛨 Create Maintenance Policy
	Name: <b>default</b> Description: Reboot Policy: <b>Immediate</b>

- 24. Server Assignment Section
  - a. Select Platinum-Compute-ServerPool for Pool Assignment.
  - **b.** Click **Up** radio button to select the power state to be applied when this profile is associated with the server.
  - c. Select PlatinumSvrQual for Server Pool Qualification.
  - d. Do not check Restrict Migration.
- 25. Click Next.

### Figure 144 Associating the Server Pool with the Service Profile

<b>A</b>	Create Service Profile Template		
Unified C	Computing System Manager		
Create Service Profile Template 1. √Identify Service Profile	Server Assignment Optionally specify a server pool for this service profile template.		
Template 2. √ <u>Networking</u> 3. √ <u>Storage</u>	You can select a server pool you want to associate with this service profile template.		
4. √ <u>zoning</u> 5. √ <u>vNIC/vHBA Placement</u>	Pool Assignment: Platinum-Compute-ServerPool		
<ol> <li>✓ <u>Server Boot Order</u></li> <li>✓ <u>Maintenance Policy</u></li> <li>✓ <u>Server Assignment</u></li> <li>Doperational Policies</li> </ol>	Select the power state to be applied when this profile is associated with the server.		
	The service profile template will be associated with one of the servers in the selected pool. If desired, you can specify an additional server pool policy qualification that the selected server must meet. To do so, select the qualification from the list.		
	Server Pool Qualification: PlatinumSvrQual Restrict Migration:		

26. Operational Policies Section
- **a.** Select TenantA-BIOS for BIOS Policy.
- b. Select BareMetal for External IPMI Management Configuration.
- c. Select Platinum-Compute-IP for Management IP Address Policy.
- d. Select default for Monitoring Configuration.
- e. Select default for Power Control Policy Configuration.
- f. Select default for Scrub Policy.
- 27. Click Next.

ſ

### Figure 145 Defining the attributes for the Operational Policy

<b>A</b>	Create Service Profile Template	
Unified C	Computing System Manager	
Create Service Profile Template 1. <a href="https://www.ice.com"><u>I</u></a>	Operational Policies Optionally specify information that affects how the system operates.	
. <u>Template</u> 2. √ <u>Networking</u> 3. √ <u>Storage</u>	BIOS Configuration	۲
<ol> <li>√<u>Zoning</u></li> <li>√<u>vNIC/vHBA Placement</u></li> <li>√<u>Server Boot Order</u></li> <li>√<u>Maintenance Policy</u></li> </ol>	If you want to override the default BIOS settings, select a BIOS policy that will be associated with this service profile BIOS Policy: TenantA-BIOS  The service of the BIOS Policy  The service of the BIOS Policy  The service of the	
8. √ <u>Server Assignment</u> 9. √ <mark>Operational Policies</mark>	External IPMI Management Configuration	۲
	If you want to access the CIMC on the server externally, select an IPMI access profile. The users and passwords in that profile will be populated into the CIMC when the profile is associated with the server.	
	IPMI Access Profile: BareMetal Create IPMI Access Profile	
	SoL Configuration Profile: Select a Policy to use (no SoL Access by defa 💌 🛨 Create Serial over LAN Policy	
	This service profile will not have Serial over LAN access.	
	Management IP Address	۲
	Management IP Address Policy: Platinum-Compute-IP(0/0)	
	<ul> <li>Create IP Pool</li> <li>The IP address will be automatically assigned from the selected pool.</li> <li>WARNING: The selected pool does not contain any available entities.</li> <li>You can select it, but it is recommended that you add entities to it.</li> </ul>	



#### Figure 146 Summary of the BareMetal-Platinum Service Profile Template

# **CloudPlatform Host Preparations**

This section outlines VMWare ESXi 5.1 Host preparations required for multi-tenant to host cloud services with cloud based service level definition.

The cloud host preparations can be divided into three major sections as following:

- Creating Host
- Installing Host
- Configuring Host

# **Creating Host**

This section outline steps required to create cloud host compute, network, and storage infrastructure based on the service levels definition required to host cloud services in multi-tenantcloud environment. Cisco UCS offers service profile templates with pre-defined cloud host compute, network and storage resources based on service levels. Four Service Profiles Templates were created to meet the Cloud service level agreement requirements.

The steps below show cloud host creation based on Platinum service levels defined by service profile template Platinum-Template for TenantA Organization unit.

In this section the following tasks are described in detail:

- Create Service Profile based on a Service Profile Template
- Associate the Service Profile with Server

## Creating a Service Profile based on a Service Profile Template

This section details the creation of service profile based on the Service Profile Template we created above.

Login to Cisco UCS Manager with User TenantA-Admin created earlier for Organization TenantA:

- 1. Click the **Server** tab in the left pane.
- 2. Choose Service Profiles > Sub-Organization. Expand TenantA.

3. In the right pane choose Service Profiles > Service Profile Template > Service Template Platinum-Template.



Figure 147 Selecting the Service Profile Template

4. Right-click Create Service Profile from Template.

Figure 148 Selecting the Service Profile Form Template



- **5.** Type TenantA-HostA-Platinum-SLA in Naming Prefix, and type a number corresponding to the number of Service Profiles to be created in the Number text box. In our case, we entered 1.
- 6. Click OK.

I

🐣 Cisco Unified Computing System Manager - TM	IF-121		_
	🕒 🌒 🗉 New 🔹 🔐 Qptions 🛛 🕢 🕘 🖉 Pending Activ	vities 0 Exit	
2 52 8 40 Equipment Servers LAN SAN VM Admin Filter: Al	>> → Servers * Service Profiles * A root * A Sub-Organizations General Sub-Organizations Service Profiles Pools Policies FC Zo Service Profiles Associated Blades Associated Racks Pooled Server	nes Faults Events	-
Servers Service Profiles Service Profiles Sub-Organizations Sub-Organizations A Interaction Sub-Organizations	Name ⊕-III Service Template Bronze-Template ⊕-III Service Template Gold-Template III Service Template Pistinum-Template ⊕-III Service Template Silver-Template	MAC Address	WWPN
⊕ ∰ Service Profile Templates ⊕ ∰ Poldies ⊕ ⊕ Pools ⊕ ∰ Schedules	Creato Naming Pr	Service Profiles From Template e Service Profiles From Templ efic: TenantA -HostA-Platinum-SLA hiber: 11	ate @

#### Figure 149 Adding the Name and Number to the Profile

## Associating the Service Profile with Server

**1.** Under the TenantA the newly created Service Profile TenantA-HostA-Platinum-SLA1 is displayed and will be in associating phase.

1



Figure 150 Displaying the Service Profile Status Details

**2.** After few minutes Service Profile TenantA-HostA-Platinum-SLA will be associated with the available blade defined in the server pool.

ſ



#### Figure 151 Verifying the Service Profile Associated with the Blade

# **Installing Host**

This section outlines steps required to install VMware vSphere ESXi 5.1 operating system on a cloud host. Cisco UCS offers a KVM console which is a video over IP representation of the video output on the blade. The KVM console access to server blades in Cisco UCS is conceptually similar to any industry standard KVM console access to the blade. Once the server profile association is complete; KVM console can be accessed. The KVM console is an interface accessible from the Cisco UCS Manager GUI or the KVM Launch Manager that emulates a direct KVM connection.

The steps below show installation of the ESXi 5.1 hypervisor on newly associated blade serve using service profile TenantA-HostA-Platinum-SLA on TenantA Organization unit.

In this section the following tasks are described:

- Connecting to the blade server KVM console
- Installing the VMware ESXi 5.1 hypervisor

Login to Cisco UCS Manager with User TenantA-Admin created earlier for Organization TenantA:

- 1. Click the Server tab in the left pane.
- 2. Choose Service Profiles expand > Sub-Organization. Expand TenantA.
- **3.** Expand TenantA. Select Tenant A-HostA-Platinum-SLA1.In the right pane under Actions: click **KVM Console**.
- 4. A pop up window /TenantA-HostA-Platinum-SAL1 (Chassis -1 server -2) KVM Console launches.

I



#### Figure 152 Launching the KVM Console

ſ

 On the KVM Console window choose Virtual Media > Add Image > Browse ESX Server 5.1 ISO image. Click Open.



1

Figure 153 Adding the VMWare ESXi Server Image

6. Check Mapped check box, and click the **KVM** tab in the KVM Console.



#### Figure 154 Selecting the VMWare ESXi Image

7. Click Reset button and click OK.

#### Figure 155 Resetting the Server



8. Click Power Cycle radio button and then click OK.

I



Figure 156 Resetting the Power Cycle for the Server Service Profile

9. At the boot menu select Cisco Virtual CD/DVD 1.22 option and press Enter.

Figure 157 Selecting the Boot Device



10. Press enter at the boot prompt. The VMWare ESXi Server is launched.



#### Figure 158 Launching the VMWare ESXi Server

## Installing the VMWare ESXi Server

ſ

To install the VMWare ESXi Server launched at the KVM console, follow these steps:

- 1. Installing the VMWare ESXi Server.
- 2. Press Enter (Continue) key.

Figure 159 Selecting the Enter Option

Welcome to the VMware ESXi 5.1.0 Installation VMware ESXi 5.1.0 installs on most systems but only systems on VMware's Compatibility Guide are supported. Consult the VMware Compatibility Guide at: http://www.vmware.com/resources/compatibility Select the operation to perform. (Esc) Cancel (Enter) Continue

3. Select F11 to Accept and Continue

Figure 160 End User Lic
-------------------------

End User License Agreement (EULA)
VMWARE END USER LICENSE AGREEMENT
PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.
IMPORTANT-READ CAREFULLY: BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE, YOU (THE INDIVIDUAL OR LEGAL ENTITY) AGREE TO BE BOUND BY THE TERMS OF THIS END USER LICENSE AGREEMENT ("EULA"). IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE TO THE VENDOR FROM WHICH YOU ACQUIRED IT WITHIN THIRTY (30) DAYS AND REQUEST A REFUND OF THE LICENSE FEE, IF ANY, THAT
Use the arrow keys to scroll the EULA text
(ESC) Do not Accept (F11) Accept and Continue

1

- 4. Select NetApp LUN C-Mode 20GB
- **5.** Press Enter (Continue).



Select a Disk to I	nstall or Upgrade
* Contains a VMFS partition	
Storage Device	Capacity
Local: (none) Remote: NETAPP LUN C-Mode (naa.60	9a0980443139694a3f3) 20.00 GiB
(Esc) Cancel (F1) Details (	F5) Refresh (Enter) Continue

6. Select US Default.

7. Press (Enter) to Continue.



Please select a keyboard layout
Swiss French Swiss German Turkish US Default US Dvorak Ukrainian United Kingdom
Use the arrow keys to scroll.
(Esc) Cancel (F9) Back (Enter) Continue

8. Enter Password.

Γ

**9.** Press (Enter) to Continue.

## Figure 163 Entering Password

Please enter	a root passwo	rd (recommended)
Root password: Confirm password:		
	Passwords mat	ch.
(Esc) Cancel	(F9) Back	(Enter) Continue

**10.** Enter F11 (Install) to confirm installation

Figure 164 Defining the Disk for ESXi Install



**11.** After installation a reboot is required and VMWare ESXi 5.1 Host Installation Complete information is displayed.

Figure 165 Displaying the VMWare ESXi Installation Status

#### Installation Complete

ESXi 5.1.0 has been successfully installed.

ESXi 5.1.0 will operate in evaluation mode for 60 days. To use ESXi 5.1.0 after the evaluation period, you must register for a VMware product license. To administer your server, use the vSphere Client or the Direct Control User Interface.

Remove the installation disc before rebooting.

Reboot the server to start using ESXi 5.1.0.

(Enter) Reboot

# **Configuring Host**

This section outlines steps required to configure VMWare ESXi 5.1 Server on cloud host after installation is completed with service levels definition required to host cloud services in multi-tenant cloud environment.

The host configuration is divided into two tasks.

• Network task

This will define design and configuration of ESXi Host Networking infrastructure to carry Tenants Management, guest and Primary or Secondary Storage (NFS) network data traffic. Also, it offers Physical and Logical isolation with high availability and load balancing using NIC Teaming and Load balancing features.

• Storage task

This will define design and configuration of ESXi Host Storage infrastructure to create tenants Primary Storage that are later referred by Citrix CloudPlatform to define Zone wide Primary Storage infrastructure for multi-tenants in cloud.

In this section the following tasks have been described in detail:

- Configuring VMWare ESXi Host Network
- Creating VMFS based DataStore on Fibre Channel Storage LUN

## Configuring VMWare ESXi Host Network

This section details the configuration of Virtual Network Switches with VMKernel Interfaces for Management, guest and NFS Storage network traffic.

Each Network Adapaters Uplinked to Virtual Network Switch should be matched with the correct Cisco UCS virtual NIC (vNICs), VLANs defined in Service Profile TenantA-HostA-Platinum-SLA1.

Table 32 provides Citrix ESXi Host Network Bond Ethernet Interfaces mapping with UCS vNICs.

Virtual Network Switch (vSwitch)	VNIC Ethernet Interfaces	UCS Service Profile vNICs
TenantA-Mgmt-Uplink	00:25:B5:01:00:0E	Management-A-NIC 00:25:B5:01:00:0E
	00:25:B5:01:00:0D	Management-B-NIC 00:25:B5:01:00:0D
TenantA-guest-Uplink	00:25:B5:01:00:0B	guest-A-NIC 00:25:B5:01:00:0B
	00:25:B5:01:00:0C	guest-B-NIC 00:25:B5:01:00:0C
TenantA-NFS-Uplink	00:25:B5:01:00:1B	NFS-A-NIC 00:25:B5:01:00:1B
	00:25:B5:01:00:0A	NFS-B-NIC 00:25:B5:01:00:0A

#### Table 32 ESXi vSwitch NIC Interfaces Mapping with UCS vNICs

#### Figure 166 MAC Addresses Corresponding to the Cisco UCS Service Profile vNICs

<b>vNICs</b> 4 Filter 👄 Export 🗞 Print	
Name /	MAC Address
- 🚺 vNIC Guest-A-NIC	00:25:B5:01:00:0B
-1 vNIC Guest-B-NIC	00:25:85:01:00:0C
- 🚺 vNIC Management-A-NIC	00:25:85:01:00:0E
- 🚺 vNIC Management-B-NIC	00:25:85:01:00:0D
-II VNIC NFS-A-NIC	00:25:B5:01:00:1B
- 🚺 VNIC NFS-B-NIC	00:25:85:01:00:0A

#### 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, follow these steps on each ESXi host:

ESXi Host TenantA-ESX-HostA-Platinum-SLA1

To configure the VM-Host-Infra-01 ESXi host with access to the management network, follow these 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. Choose the Configure the Management Network option and press Enter.
- 4. Choose the VLAN (Optional) option and press Enter.
- 5. Enter the <<var\_mgmt\_vlan ID>> 603 and press Enter.



In this guide, we input 603 for var\_mgmt\_vlan ID label

- 6. From the Configure Management Network menu, choose IP Configuration and press Enter.
- 7. Choose the Set Static IP Address and Network Configuration option by using the space bar.
- Enter the IP address for managing the first ESXi host: <<10.65.121.163>> << var\_vm\_host\_infra\_01\_ip>>.

. Note

In this guide, we input 10.65.121.163 for var\_vm\_host\_infra\_01\_ip label

- 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. Choose the IPv6 Configuration option and press Enter.
- 13. Using the spacebar, deselect Enable IPv6 (restart required) and press Enter.
- 14. Choose the DNS Configuration option and press Enter.
- 15. Enter the DNS IP Address for the first ESXi host.

To Configure Management and NFS Virtual Switches, follow these steps:

- 1. Perform SSH to ESXi Host <<10.65.121.163 var\_vm\_host\_infra\_01\_ip>>.
- 2. Provide Root and <Password> credentials
- **3.** Create Virtual Switches and Port Groups <TenantA-Mgmt-Uplink> & <TenantA-NFS-Uplink> with appropriate Network Adapaters defined in Service profile.
  - ~ # esxcfg-vswitch -aTenantA-Mgmt-Uplink
  - ~ #esxcfg-vswitch -a TenantA-NFS-Uplink
  - ~ # esxcfg-vswitch TenantA-Mgmt-Uplink -A TenantA-Mgmt-Uplink
  - ~ # esxcfg-vswitch TenantA-Mgmt-Uplink --link=vmnic3
  - ~ # esxcfg-vmknic -a -i 10.65.121.165 -n 255.255.255.0 TenantA-Mgmt-Uplink
  - ~ # esxcfg-vswitch TenantA-NFS-Uplink -A TenantA-NFS-Uplink
  - ~ # esxcfg-vswitch TenantA-NFS-Uplink --link=vmnic2 vmnic5

Figure 167 ESXi vSwitch TenantA-Mgmt-Uplink and TenantA-NFS-Uplink Creation Commands

₽	10.65.121.163 - PuTTY
~ #	esxcfg-vswitch -a TenantA-Mgmt-Uplink
~ #	esxcfg-vswitch TenantA-Mgmt-Uplink -A TenantA-Mgmt-Uplink
~ #	esxcfg-vswitch TenantA-Mgmt-Uplinklink=vmnic3
~ #	esxcfg-vmknic -a -i 10.65.121.165 -n 255.255.255.0 TenantA-Mgmt-Uplink
~ #	
~ #	esxcfg-vswitch -a TenantA-NFS-Uplink
~ #	esxcfg-vswitch TenantA-NFS-Uplink -A TenantA-NFS-Uplink
~ #	esxcfg-vswitch TenantA-NFS-Uplinklink=vmnic2
~ #	esxcfg-vswitch TenantA-NFS-Uplinklink=vmnic5

Figure 168

ESXi vSwitch TenantA-Mgmt-Uplink and TenantA-NFS-Uplink Pnic Mapping with UCS Service Profile static vNIC

a 1 . I <del>a</del>	
Name	/ MAC Address
-1 vNIC Guest-A-NIC	00:25:85:01:00:0B
-II vNIC Guest-B-NIC	00:25:85:01:00:0C
- 🚺 vNIC Management-A-N	IC 00:25:85:01:00:0E
- VNIC Management-B-N	IC 00:25:85:01:00:0D
VNIC NFS-A-NIC	00:25:85:01:00:1B
-II VNIC NFS-B-NIC	00:25:85:01:00:0A

Name	PCI	Driver	Link	Speed	Duplex	MAC Address	MTU	Description
vmnicO	0000:06:00.00	enic	Up	20000Mbps	Full	00:25:b5:01:00:0e	1500	Cisco Systems Inc Cisco VIC Ethernet NIC 🕈
vmnic1	0000:07:00.00	enic	Up	20000Mbps	Full	00:25:b5:01:00:0b	1500	Cisco Systems Inc Cisco VIC Ethernet NIC
vmnic2	0000:08:00.00	enic	Up	20000Mbps	Full	00:25:b5:01:00:1b	1500	Cisco Systems Inc Cisco VIC Ethernet NIC
vmnic3	0000:85:00.00	enic	Up	20000Mbps	Full	00:25:b5:01:00:0d	1500	Cisco Systems Inc Cisco VIC Ethernet NIC
vmnic4	0000:86:00.00	enic	Up	20000Mbps	Full	00:25:b5:01:00:0c	1500	Cisco Systems Inc Cisco VIC Ethernet NIC
vmnic5	0000:87:00.00	enic	Up	20000Mbps	Full	00:25:b5:01:00:0a	1500	Cisco Systems Inc Cisco VIC Ethernet NIC

- 4. Download VMware vSphere Client and vSphere Remote CLI
  - **a.** Open a Web browser on the management workstation and navigate to the VM-Host-Infra-01 newly created vmkernel management IP address <10.65.121.165> on TenantA-Mgmt-Uplink Port Group.
  - **b.** Download and install both the vSphere Client and the Windows version of vSphere Remote Command Line.
- 5. Log in to VMware ESXi Hosts by Using VMware vSphere Client
  - a. Open the recently downloaded VMware vSphere Client and enter the IP address of VM-Host-Infra-01 as the host you are trying to connect to: <<10.65.121.165 var\_vm\_host\_infra\_01\_ip>>.
  - **b.** Enter root for the user name.
  - c. Enter the root password.
  - d. Click Login to connect.
- 6. Delete default vSwitch0 and add network adapater vmnic0 to TenantA-Mgmt-Uplink
  - a. From each vSphere Client, choose the host in the inventory.
  - **b.** Click the **Configuration** tab.
  - c. Click Networking pane.

- d. On the right pane, click **Remove** on vSwitch0.
- e. Click Properties.
- f. Click Network Adapaters.
- g. Click Add and select vmnic0 under Unclaimed Adapaters.
- h. Click Next and again Next and click Finish to add network adapater
- 7. Add VMKernel interface on TenantA-Mgmt-Uplink virtual switch to access vMotion data traffic
  - **a.** From each vSphere Client, choose the host in the inventory.
  - **b.** Click the **Configuration** tab.
  - c. Click Networking.
  - d. On right pane click Properties on TenantA-Mgmt-Uplink
  - e. Click Add and select VMKernel Connection type radio button.
  - f. Click Next.
  - g. Type vMotion-VMKernel in Network Label text box.
  - h. Type 192 (vMotion ID) in VLANID text box.
  - i. Select Use this port group for vMotion check box.
  - j. Click Use the following IP Setting radio button.
  - k. Type 192.191.1.10 in IP Address text box, and 255.255.255.0 in Subnet Mask.
  - I. Keep the Default Gateway IP Address.
  - m. Click Next.
  - n. Click Finish.

#### Figure 169 Final ESX Virtual Switch Configuration

lardware	View: vSphere Standard Switch vSphere Distribut	ited Switch
Health Status	Networking	
Processors Memory Storage	Standard Switch: TenantA-Mgmt-Uplink	Remove Properties
Networking     Storage Adapters     Network Adapters	VMkernel Port vmK4 : 192.191.1.11	Physical Adapters wmnic0 20000 Full
Advanced Settings Power Management oftware	-VMkemel Port TenarkA-Mgmt-Uplink vmk1:10.65.121.165	2
Licensed Features Time Configuration DNS and Routing	Standard Switch: TenantA-NFS-Uplink	Remove Properties
Authentication Services Virtual Machine Startup/Shutdown Virtual Machine Swapfile Location	Virtual Machine Port Group	Physical Adapters wmnic5 20000 Full wmnic2 20000 Full Physical Adapters
Security Profile Host Cache Configuration		<u>®</u> .+
System Resource Allocation Agent VM Settings Advanced Settings		

8. Add VMKernel interface on TenantA-NFS-Uplink virtual switch to access NFS data traffic

- a. From each vSphere Client, choose the host in the inventory.
- **b.** Click the **Configuration** tab.
- c. Click Networking.
- d. On right pane click Properties on TenantA-NFS-Uplink.
- e. Click Add and Select VMKernel Connection type Radio Button and click Next
- f. Type NFS-VMKernel in Network Label: text box and click Next
- g. Select Use the following IP Setting radio buuton
- h. Type 193.191.1.1.10 in IP Address text box, 255.255.255.0 in Subnet Mask.
- i. Keep the Default Gateway IP Address and click Next.
- j. Click Finish.
- **9.** To load the updated versions of the enic and fnic drivers for the Cisco VIC, follow these steps for the hosts on each vSphere Client:
  - a. From each vSphere Client, choose the host in the inventory.
  - **b.** Choose the **Summary** tab to view the environment summary.
  - c. From Resources Configuration tab choose Storage.
  - d. Right-click datastore1 and choose Browse Datastore.
  - e. Click the fourth button and choose Upload File.
  - f. Navigate to the saved location for the downloaded enic driver version and choose net-enic-2.1.2.38-10EM.500.0.0472560.x86\_64.zip.
  - g. Click Open to open the file.
  - h. Click Yes to upload the .zip file to datastore1.
  - i. Click the fourth button and choose Upload File.
  - j. Navigate to the saved location for the downloaded fnic driver version and choose scsi-fnic-1.5.0.20-10EM.500.0.0.472560.x86\_64.zip.
  - k. Click Open to open the file.
  - I. Click Yes to upload the .zip file to datastore1.
  - **m.** From the management workstation, open the VMware vSphere Remote CLI that was previously installed.
  - **n.** At the command prompt, run the following commands to account for each host (enic):

```
esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> software vib
install --no-sig-check -d
/vmfs/volumes/datastore1/net-enic-2.1.2.38-10EM.500.0.0.472560.x86_64.zip
```

```
o. At the command prompt, run the following commands to account for each host (fnic):
```

```
esxcli -s <<var_vm_host_infra_01_ip>> -u root -p <<var_password>> software vib
install --no-sig-check -d
```

/vmfs/volumes/datastore1/scsi-fnic-1.5.0.20-10EM.500.0.0.472560.x86\_64.zip

- **p.** From the vSphere Client, right-click each host in the inventory and choose Reboot.
- q. Click Yes to continue.
- r. Enter a reason for the reboot and click OK.
- s. After the reboot is complete, log back in to both hosts using the vSphere Client.
- 10. To install the Virtual Ethernet Module (VEM) on the ESXi hosts, follow these steps:

- **a**. Launch a Web browser to http://<<var\_vsm\_mgmt\_ip>>.
- **b.** Right-click the **cross\_cisco-vem-v152-4.2.1.1.2.1.1a.0-3.1.1.vib** hyperlink and choose Save target as.
- **c.** Save the file as cross\_cisco-vem-v152-4.2.1.1.2.1.1a.0-3.1.1.vib, type All Files, on the desktop of the management workstation.
- **d.** From the main window in the vSphere Client connected to vCenter, click the first server in the list under the FlexPod Management cluster.
- e. Click the Summary tab.
- f. Under Storage on the right, right-click infra\_datastore\_1 and choose Browse Datastore.
- **g.** Choose the root folder (/) and click the third button at the top to add a folder.
- h. Name the folder VEM and click OK.
- i. On the left, select the VEM folder.
- j. Click the fourth button at the top and choose Upload File.
- k. Navigate to the cross\_cisco-vem-v152-4.2.1.1.2.1.1a.0-3.1.1.vib file and click Open.
- I. Click Yes. The VEM file should now appear in the VEM folder in the datastore.
- m. Open the VMware vSphere CLI command prompt.
- n. For each ESXi host in the VMware vSphere CLI, run the following command:

esxcli -s <Host Server IP> -u root -p <Root Password> software vib install -v /vmfs/volumes/infra\_datastore\_1/VEM/cross\_cisco-vem-v152-4.2.1.1.2.1.1a.0-3.1.1.vi

- 11. Add TenantA-guest-Uplink VMKernel PortGroup on Cisco Nexus 1000V DVS switch on ESX host
  - a. In the VMware vSphere Client connected to vCenter, choose Home > Networking.
  - b. Expand the vCenter, DataCenter, and Cisco Nexus 1000V folders.
  - c. Choose the Cisco Nexus 1000V switch.
  - d. Under Basic Tasks for the vSphere distributed switch, choose Add a Host.
  - e. Select host <var\_vm\_host\_infra\_01\_ip label> 10.65.121.165.
  - f. Select vmnic1 & vmnic4 network adapaters.
  - g. Select TenantA-guest-Uplink under Uplink port group list box.

#### Figure 170 Adding Host Network Adapaters to Nexus 1000V DVS Switch

	Add Host to vSpher	e Distributed Switch		
Select Hosts and Physical Adapters Select hosts and physical adapters	s to add to this vSphere distributed switc	h.		
Select Host and Physical Adapters			Settings	View Incompatible Host
Network Connectivity	Host/Physical adapters	In use by switch	Settings	Uplink port group
Virtual Machine Networking			View Details	
Ready to Complete	🖃 🔽 📋 10.65.121.165		View Details	
	Select physical adapters			
	🔲 😳 vmnic0	TenantA-Mgmt-Upli	View Details	Select an uplink port gr
	🗹 😳 vmnic1		View Details	TenantA-Guest-Uplink
	🔲 🖽 vmnic2	TenantA-NFS-Uplink	View Details	Select an uplink port gr
	🔲 🖽 vmnic3	TenantA-Mgmt-Upli	View Details	Select an uplink port gr
	Vmnic4		View Details	TenantA-Guest-Uplink

- i. Do not migrate VMKernel adapaters vmk0 and vmk1 interfaces to Nexus 1000V DVS switch.
- j. Click Next.

Γ

#### Figure 171 Do not Migrate VMKernel interfaces

Ø	Add Host to vSphere Distributed Switch								
<b>Network Connectivity</b> Select port group to provide netv	<b>Network Connectivity</b> Select port group to provide network connectivity for the adapters on the vSphere distributed switch.								
Select Host and Physical Adapters	<ol> <li>Assign adapters to a destinati</li> </ol>	on port group to migrat	e them. Ctrl+click to multi-	select.					
Network Connectivity	Host/Virtual adapter	Switch	Source port group	Destination port group					
Virtual Machine Networking	🖃 📋 10.65.121.165								
Ready to Complete	rmk0	TenantA-NFS-Up	NFS-VMkernel	Do not migrate					
	🛄 vmk1	TenantA-Mgmt	TenantA-Mgmt-Uplink	Do not migrate					
k. Cli	ck Next.								

Figure 172
------------

No Virtual Machince network to Migrate

Ø	Add Host to vSphere Distributed Switch
Virtual Machine Networking Select virtual machines or network	k adapters to migrate to the vSphere distributed switch.
Select Host and Physical Adapters	Migrate virtual machine networking
Network Connectivity Virtual Machine Networking Ready to Complete	Host/Virtual machine/Network adapter NIC count Source port group Destination port group
	Network adapter details Assign port group

I. Make sure you have two network adapaters listed under TenantA-guest-Uplink Port Group.

1

1

m. Click Finish.

Ø	Add Host to vSphere Distributed Switch	×	
<b>Ready to Complete</b> Verify the settings for the ne	vSphere distributed switch.		
Select Host and Physical Adapters Network Connectivity Virtual Machine Networking Ready to Complete	VSM-TenantA            © cloud.guest.1000.200.1-T         Virtual Machines (0)             © cloud.guest.1001.200.1-T         ① Virtual Machines (3)             © cloud.guest.1001.200.1-T         ② Virtual Machines (3)             © cloud.guest.1001.200.1-Tena         ② cloud.gublic.603.0.1-Tena         ③ Cloud.gublic.603.200.1-Tena         ③ Virtual Machines (3)         ③         © cloud.gublic.603.200.1-Te         ③ Virtual Machines (1)         ⑤         TenantA-VSM-VEM-Network         ③ Virtual Machines (0)         ④         ① Unused_Or_Quarantine_V         Virtual Machines (0)         ⑤         ①         Unused_Or_Quarantine_V         Virtual Machines (0)         ①         ①         ①		•
Help	< Back Finish	Cancel	

Figure 173 Add Network Adapaters

ſ

**n**. Verfiy virtual adapaters link status is Up and ESX Host <<10.65.121.165>> is been successfully added to Nexus 1000V DVS switch.



- Figure 174 Nexus 1000V DVS switch Configuration
- Distributed Switch: VSM-TenantA

Manage Virtual Adapters... Manage Physical Adapters... Properties...

- 1. Add VMKernel interface Nexus 1000V DVS << VSM-TenantA>> on TenantA-guest-Uplink Port Group to access Tenant guest data traffic
  - a. From each vSphere Client, choose the host in the inventory.
  - b. Click the Configuration tab.
  - c. Click Networking.
  - d. On right pane view click vSphere Distributed Switch Properties on TenantA-NFS-Uplink.
  - e. Click Manage Virtual Adapaters.
  - f. Click Add.
  - g. Click New Virtual adapater radio button.
  - h. Click Next.
  - i. Select VMKernel virtual Adapater Types Click Next
  - j. Select port group TenantA-VSM-VEM-Network in the list box.
  - **k.** Type IP Address <10.65.121.169>, Subnet Mask <255.255.255.0> and leave default gateway field.
  - I. Click Next.
  - m. Click Finish.
  - n. Click Close.
- 2. Verfiy VEM module on Nexus 1000V DVS switch <<10.65.121.170>>
  - a. Telnet to VSM IP Address <<10.65.121.70>>.
  - **b.** At command line type show module vem.

₽				10.65	5.121.170 - PuTTY
VSM- VSM-	TenantÅ( TenantÅ( Ports	Module-Ty			Status
 3			thernet Module	 NA	 ok
Mod			Hw		
3				1.0 Releasebuild-79	99733 (3.1)
Mod		lress (es)		Serial-Num	
3			) to 02-00-0c-00-0		
Mod		IP	Server-UUID		Server-Name
3				1-0001-000000000000	

Figure 175 VEM module on Nexus 1000V DVS

# **NetApp Virtual Storage Console for VMware vSphere**

VSC 4.1 Preinstallation Considerations

The following licenses are required for VSC on storage systems that run clustered Data ONTAP 8.1.2:

- Protocol licenses (NFS and FCP)
- FlexClone (for provisioning and cloning only)
- Install VSC 4.1

To install the VSC 4.1 software, follow these steps:

- Using the instructions in section "Build Microsoft SQL Server VM," build a VSC and an OnCommand virtual machine with 4GB RAM, two CPUs, and one virtual network interface in the <<var\_ib-mgmt\_vlan\_id>> VLAN. The virtual network interface should be a VMXNET 3 adapter. Bring up the VM, install VMware Tools, assign IP addresses, and join the machine to the Active Directory domain. Install the current version of Adobe Flash Player on the VM. Install all Windows updates on the VM.
- 2. Log in to the VSC and OnCommand VM as the FlexPod admin user.
- Download the x64 version of the Virtual Storage Console 4.1 at: http://support.netapp.com/NOW/cgi-bin/software/?product=Virtual+Storage+Console&platform= VMware+vSphere from the NetApp Support site.
- 4. Right-click the file downloaded and choose Run As Administrator.
- 5. Click Yes at the User Access Control warning.
- 6. On the Installation wizard welcome page, click Next.
- 7. Choose the backup and recovery capability.
- 8. Click Next.
- 9. Click Next to accept the default installation location.

## Figure 176 VSC Install Location

Destination	• <b>Virtual Storage Console</b> 4 • Folder • to install to this folder, or div			
	Install NetApp® Virtual Stora C: \Program Files \NetApp \Vir			to: Change
stallShield -				
italishield -		< Back	Next >	Cancel

1

10. Click Install.

NetApp® Virtual Storage Console Ready to Install the Program		Sphere - Install	Shield Wizard	
The wizard is ready to begin installation	on.			1
Click Install to begin the installation.				
If you want to review or change any exit the wizard.	of your installation s	ettings, dick Back.	Click Cancel to	
Virtual Storage Console for VMware v to function. You may register once ins any time by visiting the following URL:	stallation/upgrade co			
https://localhost:8143/Register	r.html			
stallShield				

#### Figure 177 Ready to install VSC 4.1

#### 11. Click Finish.

#### **Register VSC with vCenter Server**

To register the VSC with the vCenter Server, follow these steps:

- **1.** A browser window with the registration URL opens automatically when the installation phase is complete.
- 2. Click Continue to this website (not recommended).
- **3.** In the Plug-in Service Information section, choose the local IP address that the vCenter Server uses to access the VSC server from the drop-down list.
- 4. In the vCenter Server Information section, enter the host name or IP address, user name (FlexPod admin user), and user password for the vCenter Server.
- 5. Click **Register** to complete the registration.

#### **Discover and Add Storage Resources**

To discover storage resources for the Monitoring and Host Configuration and the Provisioning and Cloning capabilities, follow these steps:

- 1. Using the vSphere Client, log in to the vCenter Server as FlexPod admin user. If the vSphere Client was previously opened, close it and then reopen it.
- 2. Click the Home tab in the left side of the vSphere Client window.
- 3. Under Solutions and Applications, click NetApp.

Home				Search Invento
Storage Providers VCenter Service Status				
lanagement				
<b>20</b>	34	-	<b>S</b>	-
Scheduled Tasks Events	Maps	Host Profiles	VM Storage Profiles	Customization Specifications Manager
olutions and Applications	/			
NetApp				
		, Target or Status conta		Clear

#### Figure 178 Adding Storage Resource

- **4.** Click Yes when the security certificate warning appears. To view the certificate, click View Certificate.
- 5. In the navigation pane, choose Monitoring and Host Configuration if it is not selected by default.
- 6. In the list of storage controllers, right-click the first controller listed and choose **Modify** Credentials.
- 7. Enter the storage cluster management IP address in the Management IP address field. Enter admin for the user name, and the admin password for the password. Ensure that Use SSL is selected.
- 8. Click OK.
- 9. Click **OK** to accept the controller privileges.
- **10.** For additional information on storage provisioning, storage efficiency tools, reporting and backup/recovery refer to the VSC Administration Guide

## **Creating Primary Storage on Fibre Channel LUN**

- 1. In the VMware vSphere Client connected to vCenter, choose Home > Hosts and Clusters.
- 2. Expand the vCenter, DataCenter, and ESX Host <var\_vm\_host\_infra\_01\_ip label > 10.65.121.165.

I

- 3. Click Storage under Hardware
- 4. Click Add Storage.
- 5. Select Disk/LUN radio button.
- 6. Click Next.
- 7. Select NetApp LUN =2.
- 8. Click Next.
- 9. Select VMFS-5 radio button.
- 10. Click Next.
- **11.** Click **Next** to create partition.
- 12. Click Next.
- **13.** Type TenantA-FC-PrimaryStorage.
- 14. Click Next.
- 15. Select Maximum available space radio button.
- 16. Click Next.

I

- 17. Click Finish.
- **18.** Verify Datastore << TenantA-FC-PrimaryStorage>> is created under Darastores.

### Figure 179 Datastore TenantA-FC-PrimaryStorage is mapped to NetApp Fiber Channel LUN

View:	Datastores Devices												
Datas	tores									Refresh	Delete	Add Storage	R
Iden	ification /	Status		Device	Drive Type	Capacity	Free	Туре	Last Update	Alarm Act	tions	Storage I/O Con	itrol
	datastore1 (2)	🥏 N	Jormal I	NETAPP Fibre Ch	Non-SSD	10.00 GB	9.14 GB	VMFS5	8/26/2013 4:43:46 AM	Enabled		Disabled	
	TenantA-FC-PrimaryStorage	📀 N	Jormal I	NETAPP Fibre Ch	Non-SSD	179.75 GB	176.68 GB	VMFS5	8/26/2013 4:43:46 AM	Enabled		Disabled	
<						Ш							
Datas	tore Details												Р
Loci Han Refi Sysi	ntA-FC-PrimaryStorage ation: /vmfs/volumes/52038279- dware Acceleration: Unknown resh Storage Capabilities rem Storage Capability: N/A r-defined Storage Capability: N/A	9397ac35-I	f9ee-0025b5	5000001	9.75 GB Capaci 3.07 GB 🔳 Use 5.68 GB 🔲 Fre	ed							
Rou Path: Tota Brok	l: 4 Formatting	ame: Ten Vi	nantA-FC nantA-FC MFS 5.58 MB	Extents NETAPP Fibre Cl Total Formatted		180.00 GB 179.75 GB	Storage I/ Disabled	0 Contro	I				

# **Cloud Deployment Design**

The Management Server manages one or more zones (typically, datacenters) containing host computers where guest virtual machines will run. The cloud infrastructure is organized as follows:

• Zone

Typically, a zone is equivalent to a single datacenter. A zone consists of one or more pods and secondary storage.

٠ Pod

A pod is usually one rack of hardware that includes a layer-2 switch and one or more clusters.

- Cluster
- A cluster consists of one or more hosts and primary storage.
- Host •

A single compute node within a cluster. The hosts are where the actual cloud services run in the form of guest virtual machines.

- Primary storage is associated with a cluster, and it stores the disk volumes for all the VMs running on hosts in that cluster.
- Secondary storage is associated with a zone, and it stores templates, ISO images, and disk volume snapshots.



Figure 180 Logical View of CloudPlatfrom Cloud Provisioning

This section outlines Citrix CloudPlatform Compute, Network and Storage infrastructure design required to create hosted private cloud for multi-tenants.

1

CloudPlatform is a multi-hypervisor, multi-tenant, high-availability Infrastructure as a Service cloud management platform. It provides a cloud infrastructure orchestration layer; giving automation of the creation, provisioning and configuration of IaaS components (such as virtual servers).

It provides role based access features for enterprises to set up utilization charge-backs, user self-administration, approved virtual machine template libraries, and security controls to govern how users utilize the cloud.

To manage and configure cloud infrastructure, Citrix provides CloudPlatform, a software platform that pools computing resources to build public, private, and hybrid cloud network. CloudPlatform manages the network, storage, and compute nodes that make up a cloud infrastructure. Use CloudPlatform to deploy, manage, and configure cloud computing environments.

In this guide, Citrix CloudPlatform 4.2.1 software version is installed on RHEL 6.0.3 Operating System on Cisco B-200 M3 blade server. This paper shows the installation procedure of CloudPlatform 4.2.1 in single user mode.



It is recommended installing CloudPlatfrom in multi user mode to support high availability under any disaster

The below table shows Network Interfaces and their corresponding IP Address (VLAN ID) configured to access Management, NFS and PXE networks.

Make sure the CloudPlatfrom host is able to access internet, pingable and route has been configured correctly to access networks defined below in Table 33.

Ethernet Interface Name	IP Address (VLAN ID)	Network Access		
Eth0	<var_vm_host_infra_01_ip_mgnt></var_vm_host_infra_01_ip_mgnt>	Management Access		
	10.65.121.70 (603)			
Eth 1	<var_host_infra_01_nfs_ip> 193.191.1.10 (193)</var_host_infra_01_nfs_ip>	NFS Access		
Eth2	<var_host_infra-01_pxe_ip> 20.1.1.5 (20)</var_host_infra-01_pxe_ip>	PXE Access		

#### Table 33 Ethenert Interfaces with IP Address (VLAN ID) details

# Install CloudPlatfrom in single user mode

This section describes installing a single Management Server and installing MySQL on the same node.

To prepare The RHEL 6.0.3 OS to host the Management Server follow these steps:

- **1**. Log in to your OS as root.
- 2. Check for a fully qualified hostname: # hostname --fqdn.
- **3.** This should return a fully qualified hostname such as "kvm1.lab.example.org". If it does not, edit /etc/hosts so that it does.
- 4. Set SELinux to be permissive by default.
- 5. In RHEL or CentOS, SELinux are installed and enabled by default. You can verify this with: # rpm -qa | grep selinux.

**6.** Set the SELINUX variable in /etc/selinux/config to "permissive". This ensures that the permissive setting will be maintained after a system reboot.

```
# vi /etc/selinux/config
```

7. Then set SELinux to permissive starting immediately, without requiring a system reboot.

# setenforce 0

8. Make sure that the machine can reach the internet

# ping www.goggle.com

- **9.** Download the CloudPlatform Management Server onto the host from https://www.citrix.com/English/ss/downloads/.
- **10.** Choose CloudPlatform 4.2.1 under the CloudStack 4.2 listing.



You will need a MyCitrix account.

 Install the CloudPlatform packages. You should have a file in the form of "CloudStack-VERSION-N-OSVERSION.tar.gz". Untar the file and then run the install.sh script inside it. Replace the file and directory names below with those you are using:

```
# tar xzf CloudStack-VERSION-N-OSVERSION.tar.gz
# cd CloudStack-VERSION-N-OSVERSION
# ./install.sh
```

**12.** You should see a few messages as the installer prepares, followed by a list of choices.

```
Choose M to install the Management Server software.
Install the Agent
Install BareMetal Agent
Install the Usage Monitor
Install the CloudPlatform packages installed on this computer
Stop any running CloudPlatform services and remove the CloudPlatform packages from
this computer
Remove the MySQL server (will not remove the MySQL databases)
Quit
```

- 13. Wait for a message such as "Complete! Done."
- **14.** When the installation is finished, run the following commands to start essential services (the commands might be different depending on your OS).

```
# service rpcbind start
# service nfs start
```

- # chkconfig nfs on
- $\ensuremath{\texttt{\#}}$  chkconfig rpcbind on
- **15.** Continue with Install and Configure the Database, If you already have a version of MySQL installed on the Management Server node, make one of the following choices, depending on what version of MySQL it is.
  - a. If you already have installed MySQL version 5.1.58 or later, skip to step 18
  - **b.** If you have installed a version of MySQL earlier than 5.1.58, you can either skip to step 18 or uninstall MySQL or proceed to step 10 to install a more recent version.
- **16.** On the same machine where you have installed the CloudPlatfrom Management Server, re-run install.sh

./install.sh

- 17. Choose D to install MySQL server from the distribution's repository.
  - > D

18. Edit the MySQL configuration (/etc/my.cnf or /etc/mysql/my.cnf, depending on your OS) and insert the following lines in the [mysqld] section. You can put these lines below the datadir line. The max\_connections parameter should be set to 350 multiplied by the number of Management Servers you are deploying. This example assumes one Management Server.

```
innodb_rollback_on_timeout=1
innodb_lock_wait_timeout=600
max_connections=350
log-bin=mysql-bin
binlog-format = 'ROW'
```

**19.** Restart the MySQL service, then invoke MySQL as the root user.

```
# service mysqld restart
# mysql -u root
```

**20.** On RHEL and CentOS, MySQL does not set a root password by default. It is very strongly recommended that you set a root password as a security precaution. Run the following commands, and substitute your own desired root password.

```
mysql> SET PASSWORD = PASSWORD('password');
From now on, start MySQL with mysql -p so it will prompt you for the password.
```

- **21.** To grant access privileges to remote users, perform the following steps.
  - **a**. Run the following commands from the mysql prompt:

```
mysql> GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' WITH GRANT OPTION;
mysql> exit
```

- **b.** Restart the MySQL service.
- c. # service mysqld restart
- d. Open the MySQL server port (3306) in the firewall to allow remote clients to connect.

# iptables -I INPUT -p tcp --dport 3306 -j ACCEPT

22. Edit the /etc/sysconfig/iptables file and add the following line at the beginning of the INPUT chain.

-A INPUT -p tcp --dport 3306 -j ACCEPT

- **23.** Set up the database. The following command creates the cloud user on the database for performing DBA activity.
  - **a.** In dbpassword, specify the password to be assigned to the cloud user. You can choose to provide no password.
  - **b.** In deploy-as, specify the username and password of the user deploying the database. In the following command, it is assumed the root user is deploying the database and creating the cloud user.
  - **c.** (Optional) For encryption\_type, use file or web to indicate the technique used to pass in the database encryption password. Default: file..
  - **d.** (Optional) For management\_server\_key, substitute the default key that is used to encrypt confidential parameters in the CloudPlatform properties file. Default: password. It is highly recommended that you replace this with a more secure value.
  - e. (Optional) For database\_key, substitute the default key that is used to encrypt confidential parameters in the CloudPlatform database. Default: password. It is highly recommended that you replace this with a more secure value.

```
# cloud-setup-databases cloud:<dbpassword>@localhost --deploy-as=root:<password>
-e <encryption_type> -m <management_server_key> -k <database_key>
```

**24.** If you are running the KVM hypervisor on the same machine with the Management Server, edit /etc/sudoers and add the following line:

Defaults:cloud !requiretty

**25.** Now that the database is set up, you can finish configuring the OS for the Management Server. This command will set up iptables, sudoers, and start the Management Server.

# cloud-setup-management

**26.** Prepare the System VM Template.

- **a.** Secondary storage must be seeded with a template that is used for CloudPlatform system VMs.
- **b.** On the Management Server, run one or more of the following cloud-install-sys-tmplt commands to retrieve and decompress the system VM template. Run the command for each hypervisor type that you expect end users to run in this Zone.
- **c.** Mount NetApp NFS share on Management Server named /TenantADataSecNFS mount point name.
- **d.** If you set the CloudPlatform database encryption type to "web" when you set up the database, you must use the parameter -s <management-server-secret-key>. This process will require approximately 5 GB of free space on the local file system and up to 30 minutes each time it runs.

For vSphere:

```
# /usr/share/cloudstack-common/scripts/storage/secondary/cloud-install-sys-tmplt -m
/export/TenantADataSecNFSVol -u
http://download.cloud.com/templates/4.2.1/systemvmtemplate-4.2.1-vh7.ova -h vmware -o
```

```
<var_vm_host_infra_01_ip_mgnt> 10.65.121.70 -r admin -d xxxxxx -F
```

Prepare BareMetal Agent and configure PXE on RHEL Linux Operating System for CloudPlatfrom 4.2.1 to perform Baremetal as a Service in cloud



In this paper we have used same system which we have installed CloudPlatfrom 4.2.1.

- 1. Login in as root to RHEL 6.X download and Install PXE, DHCP, TFTP and NFS packages
- **2.** The CloudPlatform-VERSION-N-OSVERSION.tar.gz." is already downloaded and untar as part of CloudPlatfrom 4.2.1 installation which you have preapared as shown in install CloudPlafrom section
- 3. To install BareMetal Agent run the install.sh script found in extracted CloudPlatfrom 4.2.1 directory

```
[root@PXE CloudPlatform-4.2.1.1-rhel6.3]# ./install.sh
Setting up the temporary repository...
Cleaning Yum cache...
Loaded plugins: product-id, refresh-packagekit, security, subscription-manager
Updating certificate-based repositories.
Unable to read consumer identity
Cleaning repos: cloud-temp
0 metadata files removed
Welcome to the CloudPlatform Installer. What would you like to do?
NOTE: For installing KVM agent, please setup EPEL<http://fedoraproject.org/wiki/EPEL>
vum repo first;
  For installing CloudPlatform on RHEL6.x, please setup distribution yum repo either
from ISO or from your registeration account.
 3.We detect you already have MySql server installed, you can bypass mysql install
chapter in CloudPlatform installation guide.
        Or you can use E) to remove current mysql then re-run install.sh selecting D)
to reinstall if you think existing MySql server has some trouble.
       For MySql downloaded from community, the script may not be able to detect it.
   A) Install the Agent
   B) Install BareMetal Agent
    S) Install the Usage Monitor
   U) Upgrade the CloudPlatform packages installed on this computer
   R) Stop any running CloudPlatform services and remove the CloudPlatform packages
from this computer
   E) Remove the MySQL server (will not remove the MySQL databases)
   Q) Quit
Type B option to install BareMetal Agent
> B
```

```
Installing the BareMetal Agent...
Loaded plugins: product-id, refresh-packagekit, security, subscription-manager
Updating certificate-based repositories.
Unable to read consumer identity
cloud-temp
| 1.3 kB
             00:00 ...
cloud-temp/primary
2.5 kB
             00:00 ...
cloud-temp
7/7
Setting up Install Process
Package cloudstack-baremetal-agent-4.2.1.0-2.el6.x86_64 already installed and latest
version
Nothing to do
Done
e. Run the BareMetal setup script after installation of BareMetal Agent. Make sure to note down
   TFTP root directory
    [root@PXE CloudPlatform-4.2.1.1-rhel6.4]# cloudstack-setup-baremetal
   Checking is root
   [ OK ]
   Checking tftp-server
   [ OK ]
   Checking syslinux
   [ OK ]
   Checking xinetd
   [ OK ]
   Checking chkconfig
   [ OK ]
   Checking dhcp
   [ OK ]
   Executing 'chkconfig --level 345 tftp on'
   [ OK ]
   Executing 'chkconfig --level 345 xinetd on'
   [ OK ]
   Executing 'chkconfig --level 345 dhcpd on'
    [ OK ]
   Executing '/etc/init.d/xinetd restart'
   [ OK ]
   Detected iptables is running, need to open tftp port 69
   Executing 'iptables -I INPUT 1 -p udp --dport 69 -j ACCEPT'
   [OK]
   Executing '/etc/init.d/iptables save'
   [ OK]
   Executing 'cp -f /usr/share/syslinux/pxelinux.0 /export'
   [ OK ]
   Setup BareMetal PXE server successfully
   TFTP root directory is: /export
 f. Configure NFS configuration file /etc/exports. Make sure /export (TFTP root) and
```

## /var/www/html/RHEL63 (http root) directories are NFS exported for BareMetal Host to access **PXE** Image

```
[root@PXE ~]# cat /etc/exports
/export *(rw,async,no_root_squash)
/var/www/html/RHEL63 *(rw,async,no_root_squash)
```

#### **g**. Verify that NFS is running on the NFS server

[root@PXE ~]# vi /export/RHEL63.ks				
[root@PXE ~]‡	ŧ rp	cinfo ·	-p	
program ve	ers	proto	port	service
100000	4	tcp	111	portmapper
100024	1	udp	662	status
100011	1	udp	875	rquotad
100005	1	udp	892	mountd

i.

```
2
                           2049 nfs
       100003
                    tcp
h. Download PXE files pxelinux.0, pxelinux.cfg and RHEL63.ks (kickstart image) from RHEL
   6.0.3 Operating System ISO image to shared director /export (TFTP root directory)
   [root@PXE export]# 11
   total 112
   drwxr-xr-x. 2 root root 4096 Oct 11 04:52 pxeimages
   -rw-r--r-. 1 root root 26828 Oct 22 04:16 pxelinux.0
   - drwxr-xr-x. 2 root root 4096 Oct 22 04:55 pxelinux.cfg
   -rwxr-xr-x. 1 root root 1478 Oct 22 04:56 RHEL63.ks
  Verfiy that DHCPD service is started and running on the server. The sample DHCPD.conf file
   can be created to get DHCPD service to run.
   [root@PXE export] # service dhcpd status
   dhcpd (pid 7306) is running...
   Sample file
   # DHCP Server Configuration file.
      see /usr/share/doc/dhcp*/dhcpd.conf.sample
   #
      see 'man 5 dhcpd.conf'
   ignore client-updates;
   authoritative;
  allow booting;
  allow bootp;
   subnet 10.65.121.0 netmask 255.255.255.0
   {
    option routers
                           10.65.121.1:
            option subnet-mask 255.255.0.0;
              option broadcast-address 10.65.121.255;
               option time-offset
                                       -18000;
               default-lease-time
                                       21600;
                max-lease-time 43200;
j. Copy RHEL 6.3 OS Images by extracting ISO to shared directory /export/RHEL6-3.
   [root@PXE RHEL6-3]# 1s
  EFT
  EULA
  GPL
  HighAvailability
```

```
RELEASE-NOTES-es-ES.html RELEASE-NOTES-si-LK.html
                         RELEASE-NOTES-fr-FR.html RELEASE-NOTES-ta-IN.html
                         RELEASE-NOTES-gu-IN.html RELEASE-NOTES-te-IN.html
                         RELEASE-NOTES-hi-IN.html RELEASE-NOTES-zh-CN.html
                         RELEASE-NOTES-it-IT.html RELEASE-NOTES-zh-TW.html
images
isolinux
                         RELEASE-NOTES-ja-JP.html repodata
LoadBalancer
                         RELEASE-NOTES-kn-IN.html ResilientStorage
media.repo
                         RELEASE-NOTES-ko-KR.html RPM-GPG-KEY-redhat-beta
                        RELEASE-NOTES-ml-IN.html RPM-GPG-KEY-redhat-release
Packages
README
                        RELEASE-NOTES-mr-IN.html ScalableFileSystem
RELEASE-NOTES-as-IN.html RELEASE-NOTES-or-IN.html Server
RELEASE-NOTES-bn-IN.html RELEASE-NOTES-pa-IN.html TRANS.TBL
RELEASE-NOTES-de-DE.html RELEASE-NOTES-pt-BR.html
```

k. Start and configure http and tftp server to provide access for CloudPlatfrom BareMetal agent to access RHEL 6.3 kickstart, kernel and initrd files for performing PXE boot.

```
[root@PXE RHEL63] # service httpd start
Starting httpd:
[root@PXE export]# service xinetd status
xinetd (pid 3748) is running...
```

RELEASE-NOTES-en-US.html RELEASE-NOTES-ru-RU.html

4. Create softlinks paths under /var/www/html/RHEL63 which have links created for RHEL 6.3 kickstart image, initrd.img and vmlinuz kernel files for BareMetal Host PXE support.

```
[root@PXE RHEL63]#ln -s /export/RHEL6-3/images/pxeboot/initrd.img initrd.img
[root@PXE RHEL63] #1n -s /export/RHEL63.ks RHEL63.ks
[root@PXE RHEL63]#ln -s /export/RHEL63.ks RHEL6-3/images/pxebooy/vmlinuz vmlinuz
[root@PXE RHEL63]# 11
total 1780
```

1

FlexPod Data Center with VMware vSphere 5.1, and Citrix CloudPlatform 4.2.1
```
lrwxrwxrwx. 1 root root 41 Oct 21 05:45 initrd.img ->
/export/RHEL6-3/images/pxeboot/initrd.img
lrwxrwxrwx. 1 root root 17 Oct 21 07:11 RHEL63.ks -> /export/RHEL63.ks
lrwxrwxrwx. 1 root root 38 Oct 17 02:52 vmlinuz ->
/export/RHEL6-3/images/pxeboot/vmlinuz
```

I. Configure RHEL 6.3 kickstart image file NGS installation media option with NFS IP Address and RHEL 6.3 OS Image.

Note

In this paper we have created **Eth2 (20.1.1.5) VLAN 20** PXE Network for access PXE boot and have NFS export path /export which stores RHEL 6.3 Operating System Installtions files, kickstart, initrd and kernel files.

### Sample RHEL kickstart Image file

```
[root@PXE export]# cat RHEL63.ks
#platform=x86, AMD64, or Intel EM64T
#version=DEVEL
# Firewall configuration
firewall --disabled
# Install OS instead of upgrade
install
# Use NFS installation media
nfs --server=20.1.1.5 --dir=/export/RHEL6-3
# Root password
rootpw --iscrypted $1$rWDxD1lu$iQJek3Co0ivKUEh168CmA/
# System authorization information
auth --useshadow --passalgo=nbv12345
# Use graphical install
graphical
# Run the Setup Agent on first boot
firstboot --enable
# System keyboard
keyboard us
# System language
lang en_US
# Driver Disk
#driverdisk
--source=nfs:20.1.1.50:/var/www/html/RHEL63/dd-fnic-rhel6.3-1.6.0.5.iso
#driverdisk
--source=nfs:192.85.0.2:/home/Delmar-MR1-Driver/RHEL6.3/enic-2.1.1.41-rhel6u3-dd.i
SO
# SELinux configuration
selinux --disabled
# Installation logging level
logging --level=info
# Reboot after installation
#reboot
# System timezone
timezone Asia/Kolkata
# Network information
network --bootproto=dhcp --device=eth0 --onboot=yes --activate
#network --bootproto=dhcp --device=eth2 --onboot=yes --activate
# System bootloader configuration
#bootloader --location=mbr
# Clear the Master Boot Record
#zerombr
# Partition clearing information
#clearpart --none
# Disk partitioning information
#part /boot --fstype="ext4" --size=100
#part swap --fstype="swap" --size=2048
```

```
#part / --fstype="ext4" --grow --size=1
%packages
@base
@network-file-system-client
@network-tools
@server-platform
%end
install
#xconfig --defaultdesktop=GNOME --depth=8 --resolution=800x600
```

# **CloudPlatfrom Advanced Desgin**

The Citrix Cloud Design has been split into the following tasks:

- 1. Creating Zones
- 2. Defining Network
- 3. Adding Pods
- 4. Adding Cluster
- 5. Adding Hosts
- 6. Defining Storage

# **Creating Zones**

A zone is the largest organizational unit within a CloudPlatform deployment. A zone typically corresponds to a single datacenter, although it is permissible to have multiple zones in a datacenter. The benefit of organizing cloud compute, network and storage infrastructure into zones is to provide physical isolation and redundancy.

In order to provide true multi tenant cloud services Tenants cloud infrastructure Compute. Storage and Network for hosting virtual machines resources like CPU, Memory, Network and Storage can be granularly grouped into different isolated logical partitions by creating Zones, Pod, Clusters and Hosts.

I

To create zones using the Citrix CloudPlatform application to host cloud services, login to CloudPlatform with user credentials and follow these steps:

- 1. Access CloudPlatfrom 4.2.1 Management server IP Address on web browser with URL http://10.65.121.70:8080/client/.
- 2. Type the User Name <root>, Password <XXXXX>, and Domain.
- 3. Click Login.

CloudPlatform - Windows Internet Explorer				
🔆 📀 🗢 🔊 http://10.65.121.70:8080/client/				
🖕 Favorites 🛛 🚔 🙋 Suggested Sites 👻 🙋 Web Slice (	Gallery 🔻			
CloudPlatform				
		<b>citrix</b> CloudPlatform	1	admin
		•		•••••
				Domain
				Login
				V

### Figure 181 Logging to the Citrix CloudPlatform

- 4. Click Agree to confirm the End User License Agreement.
- 5. Click I have used CloudPlatform before, skip this guide button.
- **6.** Click **Infrastructure** in the left pane. This shows the currently unconfigured CloudPlatform environment.

Figure 182 Displaying the Infrastructure Page

CloudPlatform™	O N	lotifications Project: Default view	admin	
Dashboard	Global Settings Select view: Global Settin	as 🗸		vswitch
Instances	Name	Description	Value	Actions
Affinity Groups	vmware.use.dvswitch	Enable/Disable Nexus/Vmware dvSwitch in VMware environment	true	<b>√ x</b>
Storage	vmware.use.nexus.vswitch	Enable/Disable Cisco Nexus 1000v vSwitch in VMware environment	true	X 🗸 X

- 7. To handle TenantA Virtual Machines Network access enable vmware use nexus vswitch DVS on CloudPlafrom 4.2.1. Click **Global Settings** in the left pane. In the right pane, with Global Settings in the Select View box selected, type vSwitch in the Search box.
- 8. Press Enter.
- 9. Change Value to True on VMWare.use.dvswitch.
- **10.** Change Value to True on VMWare.use.nexus.vswitch.
- 11. Press Enter.

I

CloudPlatform™		lotifications Project: Default view	admin	
Dashboard	A Global Settings			
-	Select view: Global Settin	gs 🔽		vswitch
( Instances	Name	Description	Value	Actions
Affinity Groups	vmware.use.dvswitch	Enable/Disable Nexus/Vmware dvSwitch in VMware environment	true	× ×
Storage	vmware.use.nexus.vswitch	Enable/Disable Cisco Nexus 1000v vSwitch in VMware environment	ţrue	× 🗸 ×

1

Figure 183 Changing Value to True on Global Setting

- **12**. In search box Type vmware.
- 13. Press Enter.
- 14. Change Value to TenantA-Mgmt-Uplink on vmware.managment.portgroup.
- 15. Press Enter.
- **16.** Restart cloudstack Management service on console by ssh to 10.65.121.70.

[root@cloudstack CloudPlatform-UCS-for-cisco-4.2.1.1-5-rhel6.3]# service cloudstack-management status Stopping cloudstack-management: [ OK ] Starting cloudstack-management: [ OK ]

FlexPod Data Center with VMware vSphere 5.1, and Citrix CloudPlatform 4.2.1

Dashboard	fi Global Settings				
9	Select view: Global Settings	<b>v</b>	vr	nware	
Instances	Name	Description	Value	Actions	
Affinity Groups	router.template.vmware	Name of the default router template on Vmware.	SystemVM Tem plate (vSphere)	2	
Storage	vmware.additional.vnc.portrange.si Ze	Start port number of additional VNC port range	1000	C	
Vetwork	vmware.additional.vnc.portrange.st art	Start port number of additional VNC port range	50000	C	
Templates	vmware.create.full.clone	If set to true, creates VMs as full clones on ESX hypervisor	false	C	
5 Events	vmware.management.portgroup	Specify the management network name(for ESXi hosts)	TenantA-Mgmt-	Uplink 🗙 🗸	×
Projects	vmware.nested.virtualization	When set to true this will enable nested virtualization when this is supported by the hypervisor	false	ß	
	Standard Switch: TenantA-N Virtual Machine Port Grou cloud.private.untagger VMkernel Port TenantA-Mgmt-Uplink vmk1 : 10.65.121.165	d.0.1-TenantA-Mgmt 			
	Standard Switch: TenantA-N -Virtual Machine Port Grou I TenantA-NFS-Uplink				
	-VMkemel Port	vmnic2 20000 Full			

### Figure 184 Changing Value to TenantA-Mgmt-Uplink on Global Setting

- 17. Login to CloudPlatfrom 4.2.1 Management server by providing User Name and Pasword
- 18. Click Infrastructure in the left pane, and then View all under the Zones tile in the right pane.
- **19.** Create Zone for Tenants to provide multtendency by clicking + **Add Zone** at the top right corner of the right pane.

ſ

CloudPlatform		0 Notifications	🗁 Default View	Project View a	dmin cloud 🛛 🔻	CİTRIX
🕢 Dashboard	nfrastructure	Zones				+ Add Zone
Instances	Zone	Network Type	Public	Allocation State	Actions	- Add Zone
Storage	No data to show					
Network						
Templates						
15 Events						
Accounts						
O Domains						
hfrastructure						
Projects						
Global Settings						
Service Offerings						

## Figure 185 Displaying all the Zones in the Infrastructure

1

- **20.** Click **Advanced zone type** radio button.
- 21. Click Next.

Add zone	
Zone Type 🧿 🔶 Setup	Zone 🛛 3 Setup Network 🧿 4 Add Resources 💿 5 Launch
Set up zone type Please select a configuration for	r your zone.
e Basic	Provide a single network where each VM instance is assigned an IP directly from the network. Guest isolation can be provided through layer-3 means such as security groups (IP address source filtering).
Advanced	For more sophisticated network topologies. This network model provides the most flexibility in defining guest networks and providing custom network offerings such as firewall, VPN, or load balancer support.
	Cancel Next

### Figure 186 Defining the Configuration for the Zone

- **22.** Enter TenantA-Zone in the Name field.
- 23. Enter 171.70.168.183 to access public internet in DNS1 field.
- 24. Enter 10.65.121.70 running on CloudPlatfrom Management server in Internal DNS 1 field.
- **25**. In Hypervisor select VMware in list box.
- **26.** Enter 10.1.1.0/24 guest CIDR field which will be assigned to Virtual Machinees communications inside Pod by DHCP server running in Routrer system VM in CloudPlatfrom 4.2.1
- 27. Uncheck Public check box.
- 28. Uncheck Local Storage Enabled check box.
- 29. Click Next.

ſ

Zone Type	2 Setup Zone 2 Setup Network 2 Add Resources 2	Launch
zone is the largest Id redundancy. A zi Irver which is share	organizational unit in CloudPlatform™, and it typically corresponds to a single datacenter. Zones provid one consists of one or more pods (each of which contains hosts and primary storage servers) and a ad by all pods in the zone.	le physical isolation secondary storage
* Name:	TenantA-Zone	[
Pv4 DNS1:	171.70.168.183	
IPv4 DNS2:		
Internal DNS 1:	10.65.121.70	
Internal DNS 2:		
* Hypervisor:	VMware	
letwork Offering:	DefaultSharedNetworkOffering <	
letwork Domain:		
)edicate:		
)omain:	ROOT	
Account:		
.ocal storage enabled:		

1

## Figure 187 Defining the Zone Attributes

# **Defining Network**

After defining zone the next step is to design and define cloud network. There are two types of network definitions-- Basic and Advanced. In the basic networking only one physical network can exist in a zone, however, the advanced networking allows multiple physical networks in a zone. Each physical network can carry one or more traffic types, and CloudPlatform lets you define which type of network traffic will be carried by each network. This solution design implements the advanced networking.

There are three types of traffic which are defined and each is carried using seprate Virtual Switches with corresponding Ethernet Interfaces and Port Group names defined on ESXi Host:

• Management Traffic

It is generated within the CloudPlatform as the internal resources communicate with each other. This includes communication between hosts, system VMs (VMs used by CloudPlatform to perform various tasks in the cloud), and any other component that communicates directly with the CloudPlatform Management Server.

To access Management Traffic a seprate ESX Virtual Switch <<TenantA-Mgmt-Uplink>> with VMKernel Port Group <<TenantA-Mgmt-Uplink>> is created with corresponding Network Adapaters of appropriate network access and QoS definition are created on ESXi 5.1 Host which is managned by vCenter Host.

• guest Private Traffic

It is used and generated by end users running VMs. The guest network results when VMs communicate with each other over a network. guest Public traffic is generated when VMs in the cloud access the Internet. Publicly accessible IPs must be allocated for this purpose. End users can use the CloudPlatform UI to acquire the IPs to implement NAT between their guest network and the public network.

To access guest Public and Private Traffic Cisco Nexus 1000V DVS Switch <<VSM-TenantA>> with VMKernel Port Groups <<TenantA-guest-Uplink>> Uplink is created with corresponding Network Adapaters of appropriate network access and QoS definition

Storage Traffic

It is used for VM templates and snapshots, which is sent between the secondary storage VM and secondary storage servers. CloudPlatform uses a separate Network Interface Controller (NIC) named storage NIC for storage network traffic. Use of storage NIC that always operates on a high bandwidth network allows rapid template and snapshot copying.

To access Storage NFS Traffic a seprate ESX Virtual Switch <<TenantA-NFS-Uplink>> with VMKernel Port Group <<TenantA-NFS-Uplink>> is created with corresponding Network Adapaters of appropriate network access and QoS definition

Table 34	Network Types and Information
----------	-------------------------------

Network Type	ESX vSwitch / Cisco Nexus 1000V DVS	Tag
Management	TenantA-Mgmt-Uplink	TenantA-Mgmt-Uplink
guest	TenantA-guest-Uplink	TenantA-guest-Uplink
Secondary Storage	TenantA-NFS-Uplink	TenantA-NFS-Uplink

To configure the zone advanced network using Citrix CloudPlatform application dedicated for TenantA multi-tenant to host cloud services, follow these steps:

1

1. Drag Public and Guest traffic Types icon to Physical Network 2.

Figure 188 Defining the Advanced Networking Configuration for the Zone

Add zone	_	_		_	-	-	_	_
Zone Type	02	Setup Zone	• 3	Setup Network	• 4	Add Resourc	ces 🛛 🖯	Launch
PHYSICAL NET	WORK >	PUBLIC TRAP	FIC >	• POD >	• GUES	ST TRAFFIC	>	
When adding an ac Each physical netv Drag and drop or					ks. Each netv ions on how	vork correspoi they may be c	nds to a NIC on t ombined.	the hypervisor.
Traffic Types			Physic	cal network name				<b>A</b>
Traine Types			Phys	sical Network 1				
Guest	8			cal network name sical Network 2				×
Storage		2	Edit	C Edit				
				cal network name sical Network 3				
Previous							Cancel	Next

**2**. Drag Storage traffic Type icon to Physical Network 3.

Add zone				_				
1 Zone Type	• 2	Setup Zone	• 3	Setup Network	• 4 Ad	d Resources	05	Launch
PHYSICAL NET	WORK >	PUBLIC TRAF	FIC >	• POD >	• GUEST T	RAFFIC >		
When adding an a Each physical netw Drag and drop of	dvanced zone, you work can carry one <b>ne or more traff</b> i				s. Each network ons on how they	corresponds to may be combir	o a NIC on the ned.	hypervisor.
Traffic Types		8	Edit					
$\bigcirc$				al network name ical Network 2		]		×
Guest	C			$\bigcirc$				
	57	Ø	Edit	🖉 Edit				
Storage				al network name ical Network 3		]		×
		(						
		2	Edit					
Previous			1			Car	ncel	Next

Figure 189 Adding the Traffic Type to Physical Network

- **3.** Rename Physical network Network 1 to <Management>.
- 4. Click Edit enter <TenantA-Mgmt-Uplink> in CloudPlatfrom Traffic label field. In VLAN ID leave blank for Untagged VLANs.
- 5. Select VLAN under Isolation method list box.
- 6. Click OK.

ſ



Figure 190 Labeling the Traffic Type on the Management Network

- 7. Rename Physical network as Network 2 to <guest>.
- 8. Click **Public Edit**, enter <TenantA-guest-Uplink> in CloudPlatfrom Traffic label field. Leave the VLAN ID field blank for Untagged VLANs.
- **9.** Click **Guest Edit**, enter <TenantA-guest-Uplink> in CloudPlatfrom Traffic label field. Leave the VLAN ID field blank for Untagged VLANs.

- **10.** Select VLAN under Isolation method list box.
- 11. Click OK.

Figure 191 Labeling the Traffic Type for guest Network

🕃 Add zone				
1 Zone Type • 2	Setup Zono 🧧 🕄 Selup Nalmurk 🗿 Add Re	sources of Launch	Electriculos Swetch: VIM-TenantA	Manage Virtual Adapters
* STORAGE TRAFFIC >	PUBLIC TRAFFIC > • PGD > • GUEST TRAF	1990 - Tali	VSM-TenantA 0	- Tenartà-Gued-Ibleti 0
Each physical network can carry on	u need to set up one or more physical networks. Each network com e or more types of traffic, with certain restrictions on how they may b	e combined.	Costquest:1000.200.1-T	III C LUCUNOU (1 MC Adapter)
Drag and drop one or more traffic	types onto each physical network			- vnekt 10.65.121.165 0
			coul.quest.1001,200-07.     O     Votual Mechines (0)	E UpLosk01 (1 50C Adapter)
	Physical network name	1100 AL		R Unused_Or_Quarantine_Lighth.
Traffic Types	Managment	Isolation method VLAN V	Coulpuble.603.0.1-Term	suesd'offeranciper O
6			🔮 cloud.public.403.200.1-Te 0 Vintual Machines (0)	
🕒 🕃 Edit traffic typ	oc.		© TenantA-VIIM-VIIM-Metwork 0 %	
			Vehual Machines (0)	
Please specify t this traffic type.	he traffic label you want associated with		T Unused Or_Quarantene_V 0	
uno dunic type.			Watual Machines (0)	
vSwitch Name	TenantA-Guest-Uplink	Isolation method VLAN V		1
Storage VLAN IE				
vSwitch Type	Cisco Nexus 1000y Distributed Virtual Switch			
	VMware vNetwork Standard Virtual Switch VMware vNetwork Distributed Virtual Switch			
Can	cel OK			
	Physical network name Physical Network 3	Isolation method VLAN		
Previous		Cancel Next		

- 12. Rename Physical network Network 3 to <Storage>.
- **13.** Click **Public Edit** enter <TenantA-NFS-Uplink> in CloudPlatfrom Traffic label field. Leave the VLAN ID field blank for Untagged VLANs.
- 14. Select VLAN under Isolation method list box.
- 15. Click OK.

Figure 192 Labeling the Traffic Type for the Storage

🛃 Addizone	E 10.45 (17.00)		. 799123 [Breduction (20 days remaining)
		a land, Renard, State Barry	[7912] Probacka (2) days result day in Streams Martine, Carbourne, Conference, Conference, Stream, Vers.
Zank Type         SolapiZanis         SolapiZanis         SolapiZanis         Add Resources         Lawer           • FHYSICAL NETWORK >         • FUBLIC TRAFFIC >         • FOD >         • COEST TRAFFIC >         •           • STORAGE TRAFFIC >         • FUBLIC TRAFFIC >         • FOD >         • COEST TRAFFIC >         •           • View adding an advanced zone, you need to set up one or more physical networks.         • Cath indexing comparison to a NIC on the hypervicer Each physical network corresponds to a NIC on the hypervicer Each physical network can carry one or more types of Laffe, with certain sector/dons on how they may be combined.           • Drug and drop one or more traffic types onto each physical network.         •		Aver Institution Number	New Conference Service         New Conferee         New Conference Service
Itattic: Lypes     Perskal native/n name:       Bronge     Bronge       Cost     Edit tattic: Label you want associated with this traffic type.       Viewer     Persee specify the traffic label you want associated with this traffic type.       Viewer     Concel       VLAN ID     Instante-NFS-Uplink       Cancel     OK		hank to Donach Hardve Tooman Hardve Mark (Constant) Hardve	Markada Kaba Ka Ang Senata Grid Ang Markada Kaba Ka a Kaba Kaba Kaba Kaba Kaba K

- 16. Under VM Public TRAFFIC enter the below IP Network details.
- **17.** Enter <10.65.122.1 in Gateway field.
- 18. Enter 255.255.255.0 in Network field.
- 19. Leave blank in VLAN (UCS tags VLAN 603).
- **20.** Enter 10.65.122.161 in Start IP.
- **21.** Enter 10.65.122.170 in End IP.
- **22.** Click **ADD** button.
- 23. Click Next.

ſ

Public traffic is on se the CloudPl	generated when VMs i atform™ UI to acquire	in the cloud access the these IPs to impleme	e internet. Publicly-ac int NAT between thei	cessible IPs must be a guest network and the	allocated for this p eir public network	urpose. End users ca
		esses for internet traffic		7. 	20	
ateway	Netmask	VLAN	Start IP	End IP	Add	Actions
					Add	
0.65.122.1	255.255.255.0		10.65.122.161	10.65.122.170		×
	-he	- Ar	he .	he -	h-	- A

### Figure 193 Defining VM Public Traffic Network Details

# **Adding Pods**

Pod is the second-largest organizational unit within a CloudPlatform deployment. Pods are contained within zones. Each zone can contain one or more pods. A pod consists of one or more clusters of hosts and one or more primary storage servers

To add pod network in a zone advanced network configuration using Citrix CloudPlatform application dedicated for TenantA multi-tenant to host cloud services, follow these steps:

I

- 1. Enter TenantA-Pod in Pod Name field.
- 2. Enter <Pod\_VLAN\_603\_Gateway>10.65.121.1 in Reserved System Gateway field.
- 3. Enter 255.255.255.0 in Reserved System netmask field.
- 4. Enter 10.65.121.205 in Start Reserved system IP field.
- 5. Enter 10.65.121.215 in End Reserved system IP field.

## 6. Click Next.

I

Γ

Zone Type	02	Setup Zone	0	3	Setup Netwo	rk 🧿	4,	Add Resou	ces 🤇	5	Launch
UBLIC TRAFFIC	<ul> <li>▶</li> </ul>	0D > •	GUEST	TRAP	FIC > •	STOR	AGE TR	RAFFIC >			
ch zone must contair Il add in a later step. Ist be unique for eac	n in one or m First, configu h zone in the	ore pods, and ure a range of e cloud.	we will ac reserved l	ld the P add	first pod now resses for Clo	. A pod co udStack's	ntains h internal	iosts and p I manageme	rimary stor ent traffic.	age serve The reser	ers, which you ved IP range
*Pod name:	Tentant	A-Pod									
<sup>®</sup> Reserved system gateway:	10.65.1	21.1									
*Reserved system netmask:	255.255	5.255.0									
Start Reserved	10.65.1	21.205									
End Reserved system IP:	10.65.1	21.215									

Figure 194 Adding the Pod to the Zone

8. Click Next.

					ä		
Zone Type			Setup N		Add Resources	<b>9</b> 0	Launch
UBLIC TRAFFIC >	• POD	> • GUE	ST TRAFFIC >	<ul> <li>STORAGE</li> </ul>	GE TRAFFIC >		
Guest network traffic etwork.	is communicati	on between end-u	ser virtual machine	es. Specify a ran	ge of VLAN IDs to ca	rry guest traffic	for each phy
Guest							
VLAN Range:	1000	1001	×				
VEAN Range.	1000		^				

1

### **Adding Storage Traffic**

To add storage network in a zone advanced network configuration using Citrix CloudPlatform application dedicated for TenantA multi-tenant to host cloud services, follow these steps:

- 1. Enter <Storage\_NFS\_VLAN\_Gateway>193.191.1.1 in Gateway field.
- 2. Enter 255.255.255.0 in netmask field.
- **3**. Enter 193 in the VLAN field.
- 4. Enter 193.191.1.50 in Start IP field.
- 5. Enter 193.191.1.80 in End IP field.
- 6. Click Add.
- 7. Click Next.

		1				Launch
UBLIC TRAF	FIC > + POD<	• GUE	ST TRAFFIC > •	STORAGE TRAFF	FIC >	
affic between sts and Cloud	CloudPlatform™\'s inte Platform™ system VM:	rnal resources, in s. Please configu	cluding any components re storage traffic here.	that communicate with	h the Manageme	nt Server, such as
teway	Netmask	VLAN	Start IP	End IP	Add	Actions
3.191.1.1	255.255.255.	193	193.191.1.50	193.191.1.80	Add	
3.191.1.1	255.255.255.0	193	193.191.1.50	193.191.1.80		ж
1.191.1.1	255.255.255.0	193	193.191.1.50	193.191.1.80		×
1.191.1.1	255.255.255.0	193	193.191.1.50	193.191.1.80		x
.191.1.1	255.255.255.0	193	193.191.1.50	193.191.1.80		×
191.1.1	255.255.255.0	193	193.191.1.50	193.191.1.80		×
.191.1.1	255.255.255.0	193	193.191.1.50	193.191.1.80		×
.191.1.1	255.255.255.0	193	193.191.1.50	193.191.1.80		×
.191.1.1	255.255.255.0	193	193.191.1.50	193.191.1.80		×
.191.1.1	255.255.255.0	193	193.191.1.50	193.191.1.80		×
.191.1.1	255.255.255.0	193	193.191.1.50	193.191.1.80		×

### Figure 196 Defining the Storage Traffic Configurations

# **Adding Cluster**

ſ

Cluster provides a way to group hosts. Here to be precise, we have a cluster with a set of VMware clusters, preconfigured in vCenter. By definition all hosts part of cluster should have identical hardware, run the same hypervisor, are on the same subnet, and access the same shared primary storage. Virtual machine instances (VMs) can be live-migrated from one host to another within the same cluster, without interrupting service to the user.

A cluster is the third-largest organizational unit within a CloudPlatform deployment. Clusters are contained within pods, and pods are contained within zones. Size of the cluster is limited by the underlying hypervisor, although the CloudPlatform recommends less in most cases. A cluster consists of one or more hosts and one or more primary storage servers.

To add a cluster in a zone using Citrix CloudPlatform for TenantA, follow these steps:

1. Enter <TenantA-Cluster> in Cluster Name field.

- 2. Enter <vCenter\_IP\_Address>10.104.252.107 in vCenter Host.
- **3**. Enter <administrator> in vCenter Username.
- **4**. Enter <xxxx> in vCenter Password.
- 5. Enter <Tenant-DC> in vCenter Datacenter Name. Make sure naming convention is followed in vCenter Datacenter name.
- 6. Uncheck Override Public and Guest Traffic check boxes.
- 7. Enter <VSM\_IP\_Address>10.65.121.170> Nexus 1000V IP Address.
- 8. Enter <admin> in Nexus 1000V Username.
- 9. Enter <xxxx> in Nexus 1000V Password.
- 10. Click Next.

😌 Add zone		CITRIX	
Zone Type	• 2 Setup Zane • 3 Setup Network • 4 Add Resources • 5 Launch		
CLUSTER >	HOST > PRIMARY STORAGE > • SECONDARY STORAGE >	+ Add Zone	
cluster all have identica	one or more clusters, and we will add the first cluster now. A cluster provides a way to group hosts. The hosts in a all hardware, unit is same hyperivor, are on the same subnet, and access the same shared storage. Each cluster e hosts and one or more primary storage servers.	Quickview	9
		+	Eile Edit View Inventory Administration Plug-ins Help
Hypervisor:	VMware V		🖸 🔯 Atome 🕨 🛃 Inventory 🕨 🛐 Hosts and Clusters
* Cluster Name:	TenantA-Cluster		
* vCenter Host:	10.104.252.107		Getting Started Summary Wrtual Machines Host: Resource Allocation
* vCenter Username:	administrator		What is a Cluster? A cluster is a group of hosts. When you add a host to a
* vCenter Password:			A cluster to a group or notes, when you adult induct to a cluster; the host's resources become part of the cluster's resources. The cluster manages the resources of all hosts within it.
* vCenter Datacenter:	TenantA-DC		Clusters enable the vSphere High Availability (HA) and vSphere Distributed Resource Scheduler (DRS) solutions.
Override Public Traffic:	» D		Basic Tasks
Override Guest Traffic:	• 🗆		
* Nexus 1000v Address:	IP 10.65.121.170		
* Nexus 1000v Username:	admin		
* Nexus 1000v Password:	•	v	
Previous	Cancel	Next	

### Figure 197 Adding the Cluster to the Zone

# **Adding Hosts**

A host provides the computing resources that run the guest virtual machines. Each host has hypervisor software installed on it to manage the guest VMs. The Host here is an ESXi server. The host is the smallest organizational unit within a CloudPlatform deployment. Hosts are contained within clusters, clusters are contained within pods, and pods are contained within zones.

During initial zone creation CloudPlatfrom will automatically sync with VMware vCenter to automatically add hosts which are part of vCenter Cluster.

Later to add or modify hosts in zones CloudPlatfrom allows you to add / remove manually hosts which is explained in Cloud Infrastructure Design section.

I

# **Defining Storage**

## **Primary Storage**

ſ

CloudPlatfrom allows to define Primary Storage on Zone wide basesIt is associated with a cluster, and it stores the Operating System and Data disk volumes for all the VMs running on hosts in that cluster. The Primary Storage can File or Block based Protocol to storage VM data.

To add Primary Storage for zone using Citrix CloudPlatform application dedicated for TenantA multi-tenant to host cloud services, follow these steps:

- 1. Enter <TenantA-PrimaryNFS-Storage> in the Name field.
- 2. Enter Zone-Wide in Scope field.
- **3**. Select nfs under Protocol list box.
- 4. Enter <NetApp\_NFS\_LIF\_IP\_Address>193.191.1.20 in Server field.
- 5. Enter </TenantA\_PrimaryStorage> in Path field.
- 6. Click Next.

Figure 198

Zone Type	• 2	Setup Zone	• 3	Setup Netv	vork 📀	4	Add Resources	0 5	Launch
LUSTER >	HOST >	PRIMA	RY STORA	GE > ·	SECON	DARY	STORAGE >		
ch cluster must co all the VMs runnir	ntain one or r 1g on hosts in	nore primary sto the cluster. Use	rage servers any standar	, and we will a ds-compliant j	dd the first protocol tha	one no t is sup	w. Primary storage ported by the unde	e contains the erlying hyper	e disk volumes visor.
Name:	Tenant	A-PrimaryNF	S-Storage						
cope:	Zone-V	Vide				~			
Protocol:	nfs					~			
Server:	193.19	1.1.20							
Path:	/Tenan	tA_PrimarySt	orage						
itorage Tags:									

**Defining the Primary Storage Properties** 

## **Secondary Storage**

It is associated with a zone, and it stores VM templates used for OS images that can be used to boot VMs and can include additional configuration information, such as installed applications. It provides ISO repository for storing OS images or disc images containing data or bootable media for operating systems. The storage VM disk volume snapshots stores the saved copies of VM data which can be used for data recovery or to create new templates

The items in secondary storage are available to all hosts in the zone.

To add Secondary Storage for zone using Citrix CloudPlatform application dedicated for TenantA multi-tenant to host cloud services, follow these steps:

- 1. Select <NFS> in Provider field
- 2. Enter </TenantA\_SecondaryNFS-Storage> in Name feild.
- 3. Enter <NetApp\_NFS\_LIF\_IP\_Address>193.191.1.20 in NFS Server feild.

- 4. Enter </TenantA\_SecondaryStorage> in Path field.
- 5. Click Next.

Zone Type	02	Setup Zone	• 3	Setup Networ	k 🛛 4	Add Resources	• 5	Launch
USTER > •	HOST >	PRIMA	RY STORA	GE > • \$	SECONDAR	Y STORAGE >		
h zone must have plates, ISO image vide the IP addres			ry storage se hots. This se	rver, and we wi rver must be av	II add the firs ailable to all	t one now. Seconda hosts in the zone.	ary storage sto	res VM
rovider:	NFS				~	]		
ame:	Tenant	A-SecondaryN	IFS-Stora	je				
NFS Server:	193.191	1.1.20						
Path:	/Tenant	A_Secondary	Storage					
								Next

Figure 199 Defining the Name and Path for the Secondary Storage

<u>Note</u>

ſ

After the Zones are created a window appears with message Zone is ready to launch; proceed to the next step. Click **Launch Zone** button, which then launches a window to confirm the Enabling of the Zone. Click **Yes** to enable the Zone.

A	dd zone	
	Zone Type 🔹 2 Set	up Zone 🔹 🕉 Setup Network 🔹 👍 Add Resources 🔹 5 Launch
ase	wait while your zone is being cre	ated; this may take a while
0	Configuring physical netw	orks
0	Creating pod	
0	Configuring public traffic	Confirmation
0	Configuring storage traffic	Zone creation complete. Would you like to enable this zone?
0	Configuring guest traffic	No
9	Creating cluster	
0	Adding host	
0	Creating primary storage	
0	Creating secondary storag	e
9	Zone creation complete	

1

Note

The Cloud Infrastructure Window appears displaying all the components defined in the Zone.

fi Infrastructure			
		Dpda	ate SSL Certificate
Infrastructure			
Zones	Pods 1	Clusters	Hosts
View all	View all	View all	View all
Primary Storage	Secondary Storage	System VMs 2	Virtual Routers
View all	View all	View all	View all

## Figure 201 Displaying the Zones and Other Components

# **Cloud Infrastructure Design**

ſ

This section outlines Citrix CloudPlatform infrastructure offering with service levels provided to multiple tenants to host cloud services. The infrastructure offering includes Compute, Network and Storage resources which are provided in a shared model to tenants; therefore providing Service Levels to these resources with cost based on quality of services.



Figure 202 CloudPlatform Infrastructure Design

COMPUTE CONTROLLER NETWORK CONTROLLER STORAGE CONTROLLER

Citrix CloudPlatform, Cisco UCS and NetApp Storage offer cloud infrastructure resources which are provisioned, configured and deployed based on the service levels definitions with complete integrated, multi-tenant s solution in a cloud. In this section the following infrastructure offerings are enabled, configured and deployed in the Citrix Cloud Platform:

- Cloud Compute
- Cloud Storage
- Cloud Network

# **Cloud Compute**

Cisco UCS System offers Service Profile Templates and Service Profiles with compute server pools and server pool qualification policy definitions based on CPU and Memory requirements which can be related to service level costs definition in service catalog. These SLA definitions can be mapped on Compute by defining server pool qualification definitions, Cisco UCS System will automatically assign compute resources to the correct Service Profile and place the server into its respective server pool. Cisco UCS offers Service Profile Templates and Profiles which provide a single window to configure compute, network and storage definition on host, derived using server pools to provision multi-tenant cloud requirement.

CloudPlatfrom provides single pane of management window to manage, configure and deploy Cloud Compute on Cisco Unified Computing System using a plugin which calls Cisco UCS Manager API to perform compute operations. Once the Cisco UCS Manager Plugin is registerd with CloudPlatrorm, the Cloud Admin can quickly provision and associate Service Profile to relvent B-Series Blade for installing ESXi hypervisior OS server.

Host management for vSphere is done through a combination of vCenter and the CloudPlatform admin UI. CloudPlatform requires all hosts added in a CloudPlatform cluster, are part of VMware vCenter Cluster defined under DataCenter. Clusters of multiple hosts allow for features like vMotion migration. CloudPlafrom allows to perfrom VM Migration operation which will internally call vCenter API to perfrom vMotion opertions on VMs part of Clusters. To perform VM vMotion you require shared FC or NFS storage.

Based on the Service Level definitions Citrix CloudPlatform can define multiple clusters in a Zone to support high availability, resource on demand, performance and capacity .Table 35 shows four sample cluster definitions that can be created on TenantA Zone.

Cluster Name	Host Resources	UCS Service Profile Template	Compute Qualification Min - Max
TenantA-Platinum-Cluster	First Highest CPU & Memory Performance High Availability	Platinum-Template	32 – 40 CPU Core 128 – 256 GB Memory
TenantA-Gold-Cluster	Second Highest CPU and Memory Performance High Availability	Gold-Template	32 – 40 CPU Core 64 – 128 GB Memory
TenantA-Silver-Cluster	Third Highest CPU and Memory Performance High Availability	Silver-Template	12 – 16 CPU Core 32 – 64 GB Memory
TenantA-Bronze-Cluster	Fourth Highest CPU and Memory Performance High Availability	Bronze-Template	12 – 16 CPU Core 16 – 32 GB Memory

Table 35         Cloud Platform Hosts in Cluster Definitions for all the Service L	.evels
--	--------

In this paper VMware Cluster TenantA-Cluster part of vCenter Data Center TenantA-DC with two ESXi host TenantA-HostA and TenantA-HostB ESXi are added to provide high availability, and define Compute Offering for allocating Virtual Machines using Citrix CloudPlatform. The steps below shows creation of Compute Offering with CPU, Memory, Network, Host and High Availability definitions for allocating Virtual Machine using Citrix CloudPlatform application dedicated for TenantA multi-tenant to host cloud services.

To deploy ESXi Server on second host TenantA-HostB refer Cloud Host Preparations for creating service profile based on Platinum-Template with compute, network and storage infrastructure definitions with service levels.

Login to Cisco UCS Manager with User TenantA-Admin created earlier for Organization TenantA:



### Figure 203 Displaying the Service Profile of the Tenant A

- 1. Click the **Server** tab in the left pane.
- 2. Choose Service Profiles > Sub-Organization. Expand TenantA.
- **3.** Follow the steps mentioned in CloudPlatfrom Host Preparation section to create Service Profile <TenantA-HostB-Platinum-SLA2>.

- 4. Click Service Profile < TenantA-HostB-Platinum-SLA2>.
- 5. Click KVM Console in the right pane.



## Figure 204 Displaying the Status of the ESXi Server

- Add ESXi Host <10.65.121.200> to vCenter Cluster <TenantA-Cluster> which is part of vCenter DataCenter <Tenant-DC>. CloudPlatfrom will automatically detect ESXi Host <10.65.121.200> under Hosts tab.
  - a. In the VMware vSphere Client connected to vCenter, choose Home > Host and Clusters.
  - b. Expand the vCenter, DataCenter <Tenant-DC>, and Cluster <TenantA-Cluster> .
  - c. Click Add a host on Basic Tasks.
  - **d.** Enter <10.65.121.200> in Host text box, Enter <root> in Username text box <xxxx> in Password and click **Next**.
  - e. Click Yes to confirm Security Alert.
  - f. Click Next in Host summary.
  - g. Click Assign a new license key to host radio button.
  - h. Click Next.
  - i. Uncheck Enable Lockdown Mode.
  - j. Click Next.
  - k. Click Finish.

I

- Add ESXi Host <10.65.121.200> under Hosts tab in CloudPlatfrom once Cluster <TenantA-Cluster> is added to DataCenter <Tenant-DC> in vCenter.
  - a. Login to CloudPlatfrom with UserName and Password.
  - b. Click Infrastructure tab.

- c. On left pane click on Hosts.
- d. Click Add Host.
- e. Select TenantA-Zone in Zone list box.
- f. Select Tenant-Pod in Pod list box.
- g. Select <10.104.252.107/Tenant-DC/TenantA-Cluster>in Cluster list box.

1

- h. Enter <10.65.121.200> in ESX/ESXi Host Name field.
- i. Click OK.

Figure 205 Adding second cluster host in CloudPlatfrom

* Zone:	TenantA-Zone 🗸
* Pod:	TenantA-Pod 🗸
* Cluster:	10.104.252.107/Tenant-DC/Tenan
Dedicate:	
* ESX/ESXi Host:	10.65.121.200
Host Tags:	

8. Verify host <10.65.121.200> is added on vCenter and CloudPlatfrom.



#### Figure 206 VMWare vCenter DataCenter and Cluster Conifguration

Figure 207

CloudPlatfrom Hosts displaying ESXi Cluster Hosts

CloudPlatform™		1 Notificatio	ons Project:	Default view 🔽 💽	admin cloud 🛛 👻	<b>CITRIX</b>
Dashboard	nfrastruct	ture Hosts			٩	+ Add Host
Instances	Name	Zone	Pod	Cluster	State	Quickview
Affinity Groups	10.65.121.200	TenantA-Zone	TenantA-Pod	10.104.252.107/Tenant-DC/TenantA-Cluster	🔵 Up	+
Storage	10.65.121.165	TenantA-Zone	TenantA-Pod	10.104.252.107/Tenant-DC/TenantA-Cluster	💿 Up	+

# **Defining Tags**

A tag is a text string attribute associated with primary storage, a disk offering, or a compute Offering. Tags allow administrators to provide additional information about the cloud service offering and they are matched against tags placed on compute, service and disk offerings. CloudPlatform allows defining required tags on compute, service and disk offerings to allocate Virtual Machines Host placement and data disks on the primary storage.

## **Host Tags**

I

- 1. Click TenantA-HostA.
- 2. Click Edit icon.
- 3. Enter TenantA-HostA name in Host Tags field.
- 4. Click Apply.

n Infrastructure Hosts	TentantA-Host		
₩			C Refresh
Name Zone	Details	Statistics	
TentantA-Host Tent			
	2 3 4	Vie	w Instances
			-
	Name	TentantA-Host	
	D	e313faed-4e0d-40d5-85fb-0ecee8b8798c	
	Resource state	Enabled	_
	State	Up	
	Туре	Routing	
	Host Tags	TentnatA-HostA	
	OS Preference	None	
	Zone	TentnatA-Zone	
	Pod	TentantA-Pod	
	Apply	Cancel	

## Figure 208 Addi

Adding the Tags to the Host

1

## Storage Tags

- 1. Click the **Infrastructure** tab.
- 2. Click the **Primary Storage** in the right pane.

Vecencencencence				
<b>n</b> Infrastructure				
			Dpdate SSL Certificate	C Refresh
		5. 5.	,	
Infrastructure				
				_
Zones	Pods	Clusters	Hosts	
1		1		
		-		
View all	View all	View all	View a	11
Primary Storage	Secondary Storage	System VMs	Virtual Routers	s
		2		
		2		
				_
View all	View all	View all	View a	
			100	

## Figure 209 Selecting the Primary Storage

- 3. Click TenantAPlatinumNFSStorage.
- 4. Click Edit icon
- 5. Enter Platinum-NFS-Storage in Storage Tags field.
- 6. Click Apply.

Γ

		C Refre
Details	Settings	
24		
Name	TenantAPrimaryNFSStorage	
ID	548f325f-eb3b-3f5c-8ffb-0c2a82c997c9	
State	Up	
Storage Tags	Platinum-NFS-Storage	×
Zone	TenantA-Zone	
Pod	TenantA-Pod	
Cluster	10.104.252.107/Tenant-DC/TenantA-Cluster	
Туре	NetworkFilesystem	

1

### Figure 210 Applying the Tags to the Storage

# **Service Offering**

A service offering is a set of virtual hardware features such as CPU core count and speed, memory, and disk size. The CloudPlatform administrator can set up various offerings, and then end users choose from the available offerings when they create new Virtual Machines with compute, network and storage resources.

CloudPlatform separates service offerings into compute offerings and disk offerings.

The computing service offering specifies:

- Guest CPU
- Guest RAM

- Host Tags
- Storage Tags
- Network rate

The disk offering specifies:

- Disk Size
- Storage Tags

# **Defining the Compute Offering**

1. Click Service Offering tab.

### Figure 211 Displaying the Compute Service Offerings

A Service Offerings - Compute offerings									
elect offering: Compute offe	rings 🔽	٩	+ A	dd cor	npute	offerin			
Name	Description	(	Order						
Plantinum-Compute	TentantA-Plantinum-Compute VM		* *		W	=			
Platinum	Platinum-NFS		\$ ¥		w	=			
Medium Instance	Medium Instance	3	\$ ¥		v	=			
Small Instance	Small Instance		▲ ¥		w	=			

- 2. Select Compute Offering in Select Offering list box.
- 3. Click the Add compute offering button.
- 4. Enter Platinum-Compute in the Name field.
- 5. Enter TenantA-Platinum-Compute VM in the Description field.
- 6. Select shared in Storage Type list box.
- 7. Enter 16 in No of CPU Cores field.
- 8. Enter 2GHz in CPU field.
- 9. Enter 32GB in Memory field.
- **10.** Enter 8G in Network rate field.
- **11.** Check **Offer HA** check box.
- 12. Enter Platinum-NFS-Disk in Storage Tags.
- **13.** Enter TenantA-HostA in Host Tags.
- 14. Check CPU Cap check box.
- 15. Click OK.

ſ

* Name:	Platinum-Compute	* Description:	TenantA-Platinum-Compute-VM
Storage Type:	shared 🗸	*# of CPU Cores:	8
CPU (in MHz):	1000	* Memory (in MB):	32000
Network Rate (Mb/s):	8000	Disk Read Rate (BPS):	11000000
Disk Write Rate (BPS):	110000000	Disk Read Rate (IOPS):	11000000
Disk Write Rate (IOPS):	8000	Offer HA:	
Storage Tags:	Platinum-NFS-Disk	Host Tags:	Platinum-TenantA-HostA
CPU Cap:		Public:	
isVolatile:		Deployment Planner:	FirstFitPlanner V
Planner Mode:	×		

Figure 212 Define the Compute Offerings Attributes

Based on the Service Level definitions Citrix CloudPlatform can define multiple compute offering in a Zone for provisioning tenant's virtual machines to support high availability, resource on demand, performance and capacity. Table 36 shows four compute offering definition that can be created on TenantA Zone.

Table 36	Compute Offering Definitions for Four Service Classes
----------	---

Compute Offering	VM CPU Cores and MHz	Memory	Network Rate	Disk Write / Read IOPS / Rate	Storage / Host Tags
Platinum-Compute	8 Core	32 GB	8GB	11000000	Platinum-Storage
	2 GHz				TenantA-Platinum -Host
Gold-Compute	6 Core	16 GB	6 GB	81000000	Gold-Storage
	2 GHz				TenantA-Gold-Host
Silver-Compute	4 Core	8 GB	4Gb	54000000	Silver-Storage
	1 GHz				TenantA-Silver-Host
Bronze-Compute	2 Core	4 GB	2 Gb	27000000	Bronze-Storage
	1 GHz				TenantA-Bronze-Host

# **Cloud Storage**

This section provides storage design based on service levels definition for hosting multi-tenants data on the cloud. The storage spaces are provisioned by NetApp Storage System based on the service levels cost and exposed to CloudPlatform application as primary storage which allows defining and configuring storage to guest Virtual Machines to store operating system and data files to host multi-tenants.

The Primary storage is associated with a cluster, and it stores the OS and disk volumes for all the virtual machines running on hosts in that cluster which are part of zone. These primary stores can be accessed over Fibre Channel, NFS or iSCSI protocol.

Based on the Service Level definitions Citrix CloudPlatform can define multiple primary storage in a Zone to support high availability, resource on demand, performance and capacity, with these definition as listed in Table 37 shows three primary storage definitions that can be created on clusters on TenantA Zone.

Cluster Name	Primary Storage (Protocol)
TenantA-Platinum-Cluster	TenantA-FC-PrimaryStorage (Fibre Channel)
	TenantA-PrimaryNFS-Storage (NFS)
TenantA-Gold-Cluster	TenantA-Gold-FC-Storage (Fibre Channel)
	TenantA-Gold-NFS-Storage (NFS)
TenantA-Silver-Cluster	TenantA-Silver-FC-Storage (Fibre Channel)
	TenantA-Silver-NFS-Storage (NFS)
TenantA-Bronze-Cluster	TenantA-Bronze-FC-Storage (Fibre Channel)
	TenantA-Bronze-NFS-Storage (NFS)

Table 37 Primary Storage Definitions for the Service Classes

In this paper we will create TenantA-Platinum-Storage, TenantA-Platinum-NFS-Storage and TenantA-Platinum-FC--Storage primary storage in TenantA-Platinum-Cluster for allocating data disks to Virtual Machines using CloudPlatform.

The steps below shows creation of primary storage on Fibre Channel and NFS for allocating data disks to Virtual Machine using Citrix CloudPlatform application dedicated for TenantA multi-tenant to host cloud services.

Login to CloudPlatform with User credentials to configure Primary Storage on TenantA Zone.

## Adding the FC Primary Storage

- 1. Click Add Primary Storage button.
- 2. Select Cluster in Scope list box.
- 3. Select TenantA-Zone in Zone list box.
- 4. Select TenantA-Pod in Pod list box.
- 5. Select <vCenter\_IP\_Address>10.104.252.107/Tenant-DC-/TenantA-Cluster.
- 6. Enter TenantA-FC-PrimaryStorage in the Name field.
- 7. Choose vmfs under Protocol list box.

- 8. Enter <vCenter\_IP\_Address>10.104.252.107 in Server field.
- 9. Enter Tenant-DC in vCenter Datacenter.
- **10.** Enter TenantA-FC-PrimaryStorage in vCenter Datastore.
- 11. Click OK.

### Figure 213 Defining the FC Primary Storage Information

View: Datastores Devices					
Datastores					
Identification	$\sim$	Status	Device	Drive Type	Capacity
548f325feb3b3f5c8ffb0c2a82c997c9		🤣 Normal	193.191.1.20:/Te	Unknown	285.00 GB
😝 datastore1 (2)		🦁 Normal	NETAPP Fibre Ch	Non-SSD	10.00 GB
🔋 TenantA-FC-PrimaryStorage		🤣 Normal	NETAPP Fibre Ch	Non-SSD	179.75 GB

1

CloudPlatform™		11 Notifications Project:	Default view	adn	nin cloud 🛛 🔻	citrix.
Dashboard	nfrastructur	e Primary Storage				
					🔍 🕂 Add P	rimary Storage
Instances	Name	Server	Path	Cluster	Scope	Quickview
Affinity Groups	TenantA-FC- PrimaryStorage	VMFS datastore: /Tenant- DC/TenantA-FC-PrimaryStora	/Tenant-DC/TenantA-FC- PrimaryStorage		CLUSTER	+
Storage	TenantA- PrimaryNF\$	Add Primary Storage			ZONE	+
Network		Scope: Cluster	~			
Templates		* Zone: TenantA-Zor	ne 🗸			
Events		* Pod: TenantA-Pod * Cluster: 10.104.252.1	107/Tenant-DC/Tenan			
Projects			-PrimaryStorage			
Accounts		* Protocolt vmfs	<b>v</b>			
Domains		* Server: 10.104.252. * vCenter Tenant-DC	107			
Regions	* vCe	Datacenter: nter Datastore: TenantA-FC	-PrimaryStorage			
Infrastructure		Storage Tags:				

# **Adding the NFS Primary Storage**

- 1. Provide User Name <root> and Password <XXXXX> and Domain.
- 2. Click Login.
- 3. Click the Infrastructure tab on the left Side Pane.
- 4. Click the View All under Primary Storage in the right pane.
| nfrastructure          |                       | Dpda                      | te SSL Certificate     |
|------------------------|-----------------------|---------------------------|------------------------|
| Infrastructure         |                       |                           |                        |
| Zones<br>1<br>View all | Pods<br>1<br>View all | Clusters<br>2<br>View all | Hosts<br>2<br>View all |
| Primary Storage        | Secondary Storage     | System VMs                | Virtual Routers        |
| View all               | View all              | View all                  | View all               |

## Figure 214 View Primary Storage

# **Add NFS Primary Storage**

ſ

- 1. Click Add Primary Storage.
- 2. Select Cluster in Scope list box..
- **3**. Select TenantA-Zone in Zone list box.
- 4. Select TenantA-Pod in Pod list box.
- 5. Select <vCenter\_IP\_Address> 10.104.252.107/Tenant-DC-/TenantA-Cluster.
- 6. Enter TenantA-PrimaryNFS-Storage in the Name field.
- 7. Choose nfs under Protocol list box.
- 8. Enter <NetApp\_NFS\_LIF\_IP\_Address>193.191.1.20 in Server field.

- **9.** Enter /TenantA\_PrimaryStorage in Path.
- 10. Enter OK.

On successful addition of NFS Primary Storage on CloudPlatfrom, corresponding NFS Datastore will be automatically configured on ESX Hosts part of VMWare Cluster under DataCenter.

Figure 215 Defining NFS Primary Storage Information

nfrastructure	Primary Storage									
				Add	I Primary Storage					
Name	Server	Path	Cluster	Scope	Quickview					
TenantA- PrimaryNFS-Storage	193.191.1.20	/TenantA_PrimaryStorage		ZONE	+					
		1	÷	i.						
	Add Primary Sto	rage								
	Scope: [	Cluster	~							
		TenantA-Zone	~							
	* Pod: [	TenantA-Pod	~			View:	Datastores Devices			
	* Cluster.	10.104.252.107/Tenant-DC/Te	enan 🗸			Datast	ores		-	1
	* Name: (	TenantA-PrimaryNFS-Storag	e				48f325feb3b3f5c8ffb0c2a8	32c997c9	Status	Device 193.191.1.20:/TenantA_PrimaryStorage
	* Protocol:	nfs	~				latastore1 (2)		🦁 Normal	NETAPP Fibre Channel Disk (naa.600a0980443139
	* Server:	193.191.1.20								
	* Path:	/TenantA_PrimaryStorage								
-	Storage Tags: (	•								
		Cancel OK								

## **Cloud Storage Volume**

To provide data storage access to Tenant Virtual Machines based on service levels definition created on primary storage, CloudPlatform offers volume, a unit of storage which can provide additional data disk for a specific VM. CloudPlatform defines a volume as a unit of storage available to a guest VM.

Data disks provide for additional storage (e.g. As "/opt" or "D:"). Every guest VM has a root disk, and VMs can also optionally have a data disk. End users can mount multiple data disks to guest VMs. Users choose data disks from the disk offerings created by cloud administrators.

1

Login to CloudPlatform with user credentials to configure Primary Storage on TenantA Zone

#### **Defining the Disk Offering**

- 1. Click the Service Offering tab.
- 2. Select Offering in Select Offering list box.
- 3. Click Add Disk Offering button.

## Figure 216 Selecting the Disk Offering

elect offering: Disk	Offerings					٩		- Add	Disk	Offerii
Name	Description		Custom Disk Siz	ze	Disk Size (in GB)	Orde	r			
Small	Small Disk, 5 GB	No		5		*	÷		▼	=
Medium	Medium Disk, 20 GB	No		20		*	¥		v	=
Large	Large Disk, 100 GB	No		100		\$	Ť		$\mathbf{v}$	=
Custom	Custom Disk	Yes		N/A		\$	¥		V	=

- 4. Enter Platinum-NFS-Storage in the Name field.
- 5. Enter Platinum-NFS-Disk in the Description field.
- 6. Select shared in Storage Type list box.
- 7. Check Custom Tags check box.
- 8. Leave QoS Type blank
- 9. Enter Platinum-NFS-Storage in Storage Tags.
- **10**. Check the Public check box.
- 11. Click OK.

I

## Figure 217 Defining the Disk Offering Information

🕣 Add Disk Offeri	ng
* Name:	Platinum-NFS-Storage
* Description:	Platinum-NFS-Disk
Storage Type:	shared 🗸
Custom Disk Size:	
QoS Type:	×
Storage Tags:	Platinum-NFS-Storage
Public:	
Cancel	ОК

Based on the Service Level definitions Citrix CloudPlatform can define multiple disk offerings in a Zone for provisioning tenant's virtual machines to support high availability, resource on demand, performance and capacity. Table 38 shows four disk offering definitions that can be created on TenantA Zone.

## Table 38 Disk Offering Definitions for all the Service Classes

Disk Offering	Storage Tags
Platinum-Storage-Disk	Platinum-NFS-Storage
Gold-Storage-Disk	Gold-NFS-Storage
Silver-Storage-Disk	Silver-NFS-Storage
Bronze-Storage-Disk	Bronze-NFS-Storage

#### **Creating Storage Volume**

- 1. Provide User Name <root> and Password <XXXXX> and Domain.
- 2. Click Login.
- 3. Click the Storage tab on the left side pane.
- 4. Click Add Volume in the right pane.
- 5. Enter Platinum-NFS-Data-Vol in the Name field.
- 6. Select TenantA-Zone in Availability Zone list box.
- 7. Select Platinum-NFS-Disk in Disk Offering list box.
- 8. Enter 20 value in Disk Size field.

#### Figure 218 Defining the Volume Data

🕣 Add Volume	
Please fill in the fo	llowing data to add a new volume.
* Name:	Platinum-NFS-Data-Vol
Availability Zone:	TenantA-Zone 🗸
Disk Offering:	Platinum-NFS-Disk
* Disk Size (in GB):	20
Cance	ОК

Based on the Service Level definitions Citrix CloudPlatform can define multiple volumes based on the disk offering requirement in a Zone to support high availability, resource on demand, performance and capacity, with these definitions. Table 39 shows four volume definitions that can be created for allocating data disk to Virtual Machines on TenantA Zone.

I

Volume Name	Disk Offering
Platinum-NFS-Data-Vol	Platinum-NFS-Disk
Gold-NFS-Data-Vol	Gold-NFS-Disk
Silver-NFS-Data-Vol	Silver-NFS-Disk
Bronze-NFS-Data-Vol	Bronze-NFS-Disk

## Table 39 Volume Definition Based on Disk Offering

# **Cloud Network**

To provide network isolation and to offer custom network services based on the service levels definitions for specific Tenants network, CloudPlatform offers advanced zone network traffic types and network offering which can be applied on zone bases.

In this paper the Zones have been configured to use advanced zone networking where multiple physical networks can carry one or more traffic types, and to the admin must define in the CloudPlatform as to what type of network traffic is carried by the network. The traffic types in an advanced zone are mentioned below.

• Guest

When end users run VMs, they generate guest traffic. The guest VMs communicate with each other over a network that can be referred to as the guest network. This network can be isolated or shared. In an isolated guest network, the administrator needs to reserve VLAN ranges to provide isolation for each CloudPlatform account's network (potentially a large number of VLANs). In a shared guest network, all guest VMs share a single network.

• Management

When CloudPlatform's internal resources communicate with each other, they generate management traffic. This includes communication between hosts, system VMs (VMs used by CloudPlatform to perform various tasks in the cloud), and any other component that communicates directly with the CloudPlatform Management Server. You must configure the IP range for the system VMs to use.

• Public

This traffic is generated when VMs in the cloud access the Internet. Publicly accessible IPs must be allocated for this purpose. End users can use the CloudPlatform UI to acquire these IPs to implement NAT between their guest network and the public network

Storage

This traffic such as VM templates and snapshots, which is sent between the secondary storage VM and secondary storage servers. CloudPlatform uses a separate Network Interface Controller (NIC) named storage NIC for storage network traffic.



Refer Cloud Host Preparation and Cloud Host Deployment sections for more details on designing and configuring these network traffic types on different physical network devices on Cisco UCS Compute System.

## **Network Offering**

The CloudPlatform administrator can create any number of custom network offerings, in addition to the default network offerings provided by CloudPlatform. By creating multiple custom network offerings, the cloud is equipped to offer different classes of service on a single multi-tenant physical network and this also ensures various levels of services based on the service levels cost definition.

Example: Considering there are two tenants-- tenant A may require only the simple firewall protection for their website, while tenant B may be running a web server farm and require a scalable firewall solution, load balancing solution, and alternate networks for accessing the database backend.

In this paper default isolated network offering is used that will be defined during zone advanced network configuration. Based on the Service Level definitions and network offering services Citrix CloudPlatform can define multiple networks offering in a Zone.

I

Login to CloudPlatform with User credentials to configure Primary Storage on TenantA Zone

## **Creating Network Offering**

- 1. Provide User Name <root> and Password <XXXXX> and Domain.
- 2. Click Login.
- 3. Click the Service Offering tab.
- 4. Select Network Offering in Select Offering list box.
- 5. Click Add network offering.
- 6. Enter TenantA-Zone-Network in the Name field.
- 7. Enter TenantA Network in the Description field.
- 8. Select Isolated in Guest Traffic list box.
- 9. Check DHCP, DNS, UserData check boxes in Required Services list box.
- 10. Click OK.

* Description: TentantA N Network Rate (MB/s): Guest Type: Isolated Specify VLAN: VPC: Supported Services: DHCP Pr DNS Pr	Zone-Network Network	
* Description: TentantA N Network Rate (MB/s): Guest Type: Isolated Specify VLAN: VPC: Supported Services: DHCP Pr DNS Pr		 
* Description: TentantA N Network Rate (MB/s): Guest Type: Isolated Specify VLAN: VPC: Supported Services: DHCP Pr DNS Pr		-
Network Rate (MB/s): Guest Type: Isolated Specify VLAN: VPC: DHCP Pr DNS Pr	Network	-
Guest Type: Isolated Specify VLAN: VPC: Supported Services: DHCP Pr DNS Pr		-
Specify VLAN:	2	-
Specify VLAN:		
VPC:		
Supported Services: DHCP Pr DNS Pr		
DHCP Pr DNS Pr		
DHCP Pr DNS Pr	VPN: 🗖	-
DNS Pr	DHCP:	L
	rovider: VirtualRot	L
	DNS:	L
Fi	rovider: VirtualRol 💌	
	irewall:	
Load Ba	alancer: 🗖	
Use	er Data: 🔽 🔽	•
System Offering: None		•
Conserve mode: 🔲		
Tags:		
1030.		
Cancel		

Figure 219 Defining the Network Offering Properties

I

Γ

11. Click TenantA-Zone-Network radio button, which is disabled.

Figure 220

Displaying Network Offerings Status

1

ect offering: Network Offerings			<mark>م</mark> ا	🕇 Ad	ld net	work	offerin
lame	State		Orde	r			
TentnatA-Zone-Network	۲	Disabled	*	÷		v	=
DefaultSharedNetworkOfferingWithSGServ ice	0	Enabled	*	÷		v	=
DefaultSharedNetworkOffering	•	Enabled	*	¥		v	=
DefaultIsolatedNetworkOfferingWithSource NatService	۲	Enabled	*	÷		v	=
DefaultIsolatedNetworkOffering	0	Enabled	*	¥		v	=
DefaultSharedNetscalerElPandELBNetwork Offering	۲	Enabled	*	÷		v	=
DefaultisolatedNetworkOfferingFor∀pcNet works	۲	Enabled	*	Ť		v	=
DefaultIsolatedNetworkOfferingFor∀pcNet worksNoLB	۲	Enabled	*	÷		w	=

12. Click Enable icon.

🗌 🕈 Service Offerings - Network O	fferings TentnatA	-Zone-Network	
			C Refresh
Name DefaultSharedNetworkOfferingWith ice	Details		
DefaultSharedNetworkOffering			
DefaultIsolatedNetworkOfferingWith NatService	Name	TentnatA-Zone-Network	<u>^</u>
DefaultIsolatedNetworkOffering			
DefaultSharedNetscalerElPandELBN Offering	ID	408b44a4-c2b0-4c40-9e36-65a7aa91659e	
DefaultIsolatedNetworkOfferingFor\ works	Description	TentantA Network	
DefaultIsolatedNetworkOfferingFor\ worksNoLB	State	Disabled	
TentnatA-Zone-Network	Guest Type	Isolated	
	Availability	Optional	
	Created by system	No	
	Specify VLAN	No	
	Specify IP ranges	No	V

## Figure 221 Enabling the TenantA Zone Network

**13.** Click **OK**.

## Figure 222

Γ

## Confirming the Network Offering Enabling



# **Virtual Machine Configuration and Management**

CloudPlatform provides administrators with complete control over the life cycle of all guest VMs executing in the cloud. CloudPlatform provides several guest management operations for end users and administrators. VMs may be stopped, started, rebooted, and destroyed.

This section explains Virtual Machine (VM) life cycle management design process followed to provision multi-tenants virtual machines on shared cloud infrastructure. The VM management features offered by Citrix CloudPlatform includes, live snapshots, checkpoint, migration, backup, and deletion.

The tasks involved in managing the virtual machine life cycle are listed below:

- VM Infrastructure
- Installing the Operating System on VM
- Configuring VM
- VM Backup and Restore
- VM Migration
- VM Deletion

# **VM Infrastructure**

This section explains how to create compute, network and storage infrastructure for virtual machines which are dedicated for multi-tenant s based on the service levels cost defined. The initial cloud infrastructure designs for compute, network and storage cloud requirements are defined in the previous sections.

In this study we will add Windows 2008 R2 ISO image and create virtual machine with Platinum level compute, network and storage cloud infrastructure using CloudPlatform.

1

Login to CloudPlatform with User credentials to create ISO Image TenantA Zone

## Adding HTTP where Windows 2008 R2 ISO is been placed for CloudPaltfrom to download

- 1. Provide User Name <root> and Password <XXXXX> and Domain.
- 2. Click Login.
- 3. Click Global Setting tab under search type secstorage.allowed.internal.sites.
- 4. Under secstorage.allowed.internal.sites enter << Var\_HTTP\_Server>> 10.65.121.70.
- 5. Restart CloudPlatfrom service.

## Adding ISO Image

- 1. Provide User Name <root> and Password <XXXXXX> and Domain.
- 2. Click Login.
- 3. Click the **Templates** tab.
- 4. Select ISO in Select view list box.

## Figure 223 Displaying the ISO Templates

Templates - ISO				
elect view: ISO	Filter by	All	v 🔍 🗄	Register IS
Name		Zone	Order	Quickview
Linux-VMwareTools		TenantA-Zone	= V A ¥ ±	+
vmware-tools.iso			= V A ¥ 1	+
xs-tools.iso			± ¥ ▲ ▼ =	+

## 5. Click Register ISO.

- 6. Enter Windows2008R2-ISO in the Name field.
- 7. Enter Windows2008R2 in the Description field.
- 8. Enter

http://10.65.121.70/ISO/en\_windows\_server\_2008\_r2\_standard\_enterprise\_datacenter\_and\_web\_ with\_sp1\_x64\_dvd\_617601.iso in URL field.



Ensure to setup http server and stored Windows 2008 R2 ISO image under /etc/www/html path.

- 9. Select TenantA-Zone under Zone list box.
- **10.** Check **Bootable** check box.
- 11. Select Windows 2008 R2 (64-bit) under OS Type list box.
- 12. Select Extractable check box.
- **13**. Select **Public** check box.
- 14. Select Featured check box.
- 15. Click OK.

I

🕀 Register ISO		_
* Name:	Windows2008R2-ISO	
* Description:	Windows2008R2	
* URL:	http://10.65.121.70/ISO/en_	windows
Zone:	All Zones	~
Bootable:		
* OS Type:	Windows Server 2008 R2 (6	4-bit) 🗸
Extractable:		
Public:		
Featured:		

1

## Figure 224 Registering the ISO Properties

## **Creating VM**

- 1. Provide User Name <root> and Password <XXXXX> and Domain.
- 2. Click Login.
- **3**. Click the **Instance** tab.
- 4. Select ISO in Select View list box.
- 5. Click Add Instance.
- 6. Select TenantA-Zone in Select a Zone list box.
- 7. Select ISO radio button.
- 8. Click Next.

Add Instanc	e					
Setup	2 Seletern	cta o Compute offering	Data Disk Offering	Networ	ĸ 🛛 6	Review
Select a z A zone typ the cloud n		a single datacenter. Multiple zones help ma ng physical isolation and redundancy.	ke			
Tena	ntA-Zone	-				
Select IS	O or template				1	
o	Template	OS image that can be used to boot VMs				
o	ISO	Disc image containing data or bootable media for OS				8
						$\geq$
			<			
				с	ancel	Next

## Figure 225 Defining the Name and Image of the Instance

- 9. Click Windows-2008R2 Image radio button.
- **10**. Select ESXiServer in Hypervisor list box.
- 11. Click Next.

I

Γ

Add Instance					
1 Setup 🧿 2 🛔	Select a S Compu emplate S Offerin	te Data Disk g Offering	Affinity	Network 💿	Review
Please select an ISO for your n	ew virtual instance.				
Featured	Community	My ISOs			
● Windows-24 Win2008R2-IS Hypervisor: ▼				05	
Previous				Cancel	Next

## Figure 226 Defining the Hypervisor for the Instance

1

- 12. Select Platinum-Compute.
- 13. Click Next.



## Figure 227 Defining the Compute Offering for the Instance

- 14. Select Platinum-NFS-Storage-Disk.
- 15. Enter 20-GB Value in Disk Size field.
- 16. Click Next.

Γ

Add In		
Setu	Select a Select a Compute A Data Disk offering Offering	Affinity 🛛 Network 🕥 Review
	Medium	
0	Medium Disk, 20 GB	
0	Large Disk, 100 GB	
0	Custom Disk	
۲	Platinum-NFS-Storage: 20 GB	
Disk Size	1 GB 🚱 1024 GB 20 GB	
Previou		Cancel Next

1

## Figure 228 Selecting the Disk Offering and Size

- 17. Check TenantA-Network and Default check boxes under Network.
- 18. Click Next.

Add Instance	_	_	
1 Setup <b>&gt;</b> 2 Select a <b>&gt;</b> 3	Compute offering	Data Disk Offering	twork 🧿 🕜 Review
Please select networks for your virtual machine. VPC:	None 💌		
Networks			
TentnatA-Network Isolated	O Default		
			OS
		0	
Add Network			
Previous			Cancel Next

## Figure 229 Selecting Networks for the Virtual Machine

- **19.** Enter TenantA-Platinum-VM1 in VM Name field.
- 20. Click Launch VM.

I

Γ

e review the following inform e launch.	nation and confirm that your v	irtual instance is correct		
Name (Optional)	TentnatA-Platinum-	VM1		
Add to group (Optional)				
Zone		🖉 Edit		
Hypervisor		🖉 Edit		OS
ſemplate		🖉 Edit		
Compute offering		🖉 Edit		
Data Disk Offering		🖉 Edit	0	
Network		🖉 Edit	0	BLA BLA

#### Figure 230 Verifying the Virtual Instance Information

# **Installing the Operating System**

This section explains how to install guest operating system on virtual machines after provisioning compute, network and storage infrastructure which are dedicated for multi-tenant s to host data.

In this study we will install RHEL 6.2 guest operating system on newly created TenantA-Platinum-VM1 virtual machine with Platinum level compute, network and storage cloud infrastructure using CloudPlatform.

Login to CloudPlatform with User credentials to create ISO Image TenantA Zone:

## **Installing Windows OS**

- 1. Provide User Name <root> and Password <XXXXXX> and Domain.
- 2. Click Login.
- 3. Click the **Instances** tab.
- 4. Click TenantA-Platinum-VM1 under Display name.

5. Click View Console icon.

I

Γ

			C Refres
Name	Details	NICs Statistics	
TenantA-Platinum-VM1	-		
Windows2008r2	× 10 C 0	Ø_ P 🕂 🛱 🗵	C Reset VM
	View Volumes	View Snapshots View Affinity Grou	ps View Hosts
	Display name	TenantA-Platinum-VM1	
	Name	TenantA-Platinum-VM1	
	State	Running	
	Template	Windows2008R2	
	Dynamically Scalable	No	
	OS Type	Windows Server 2008 R2 (64-bit)	
	Hypervisor	VMware	
	Attached ISO	Windows2008R2	
	Compute offering	Small Instance	

6. Click Console button to lunch for installation of Windows OS.

CloudPlatform™	Windows2008r2 - Windows Internet Explorer
	http://10.65.121.70:8080/client/console?cmd=access&vm=09f9c2f7-a744-455a-bd98-57353c205b7e
Dashboard	🚾 Ctrl-Alt-Del 😽 Ctrl-Esc 😽 Keyboard
Instances	
Affinity Groups	🐉 Install Windows
Storage	
Network	
Templates	Windows Server 2008 🐱
15 Events	Languag <u>e</u> to install: English
Projects	Time and currency format: English (United States)
Accounts	Keyboard or input method: US
Domains	Enter your language and other preferences and click "Next" to continue.
Regions	Copyright @ 2009 Microsoft Corporation. All rights reserved.
Global Settings	

Figure 232

#### 32 Launching the VM

7. Click **English** in Language to install, Choose **English** (**United States**) and **US** in keyboard or input method.

1

- 8. Click Next button.
- 9. Click Install Now button.
- 10. Select Windows Server 2008 R2 Enterprise (Full Installation) OS type.
- 11. Click Next button.
- 12. Accept license check box
- 13. Click Next button
- 14. Click Custom Installation method.
- 15. Click Next button.
- 16. Select Disk0.
- 17. Click Next for OS installation.



Figure 233 Windows 2008 R2 OS installation completion into the VM

**18**. Enter **Password** <xxxxx> and **Confirm Password** <xxxx>

ſ



1

## Figure 234 Logging into the VM

## **Detaching ISO on TenantA-Platinum-VM1**

- **1**. Click the **Instance** tab.
- 2. Click Detach ISO icon.

nstances TenantA-Platin	num-VM1		
<b>↔</b>			C Refresh
Name In TenantA-Platinum-VM1	Details	NICs Statistics	
	× 🖾 C 🛇	Ø_ Ø 🕂 🛱 🗖	C Reset VM
	View Volumes	View Snapshots View Affinity Groups View	ew Hosts
	Display name	TenantA-Platinum-VM1	^
	Name	TenantA-Platinum-VM1	
	State	Running	
	Template	Windows 2008 R2	
	Dynamically Scalable	No	
	OS Type	Windows Server 2008 R2 (64-bit)	
	Hypervisor	VMware	
	Attached ISO	vmware-tools.iso	
	Compute offering	Medium Instance	~

Figure 235 Detaching the ISO Image

3. Click Yes in the confirmation window.

# **VM Configuration**

ſ

This section explains Virtual Machine cloud network address translation (NAT) for accessing the public network and provisioning external data disk with ESXi PV Drivers for storing tenants hosted data information.

In this study we will install ESXi PV Driver, provision data disk and attach the newly created virtual machine TenantA-Platinum-VM1, and configure source NAT for accessing Virtual Machine from public access using CloudPlatform.

Login to CloudPlatform with User credentials to install ESXi PV Driver on Virtual Machine on TenantA Zone

# **ESXi PV Driver Installation**

1. Provide User Name <root> and Password <XXXXX> and Domain.

1

- 2. Click Login.
- 3. Click the Instances tab.
- 4. Click Attach ISO icon.

Figure 236 Attaching the ISO

🛱 Instances TenantA-Platin	um-VM1		
		C Rel	resh
Name In TenantA-Platinum-VM1 is	Details	NICs Statistics	
	× DIC 0	04 2 4 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	м
	View Volumes	View Snapshots View Affinity Groups View Hosts	
5	Display name	TenantA-Platinum-VM1	^
	Name	TenantA-Platinum-VM1	
	State	Running	
	Template	Windows 2008 R2	
	Dynamically Scalable	No	
	OS Type	Windows Server 2008 R2 (64-bit)	
	Hypervisor	VMware	
	Attached ISO		
	Compute offering	Medium Instance	~

- 5. Select VMware Tools Installer ISO from ISO list box.
- 6. Click OK.

Figure 237	Selecting the ISO		
•	Attach ISO		
	ISO: VMware Tools Ins	taller ISO	
	Cancel		
7. Launch VM	I Console and login to <tenanta< th=""><th>A-Platinum-VM1&gt;.</th><th></th></tenanta<>	A-Platinum-VM1>.	
8. Enter User	Name <root> and password <x< th=""><th>XXXXX&gt;.</th><th></th></x<></root>	XXXXX>.	
Figure 238	Logging into the VM		
@ http://10.65.121.70:8080/client/con	TenantA-Platinum-VM1 - W sole?cmd=access&vm=899e9cbb-6190-4		
	· Keyboard	1021-9704-9E91B3C1E137	
			R.
			Contraction of the local division of the loc
			1.000
Section 1			
		Administrator	
		ged on remotely from DEEKUMA2-WS	
			$\odot$
			10 19 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
		Gancel	O Activ

L

Γ

- 9. Click Run setup64.exe installer.
- 10. Click Next.
- **11.** Click **Complete** radio button.
- 12. Click Install.
- 13. Click Finish.
- 14. Click Yes to reboot.

Login to CloudPlatform with User credentials to configure VM NAT on TenantA Zone:

## Sourcing the NAT to access VM from Public Access

- 1. Provide User Name <root> and Password <XXXXX> and Domain.
- 2. Click Login.
- 3. Click the Network tab.

#### Figure 239 Displaying the Guest Network

n Network - Guest networks						
Select view: Guest netw	orks 💌			Add guest network		
Name	Account	Туре	VLAN	CIDR		
TentnatA-Network	admin	Isolated	1003	10.1.1.0/24		

- 4. Click **TenantA-Network** tab.
- 5. Click Egress rules.
- 6. Enter 0.0.0.0/0 in Source CIDR and select All in Protocol list box.
- 7. Click ADD button.

#### Figure 240 Displaying the Guest Network Egress Rules

				C Refre
Details	Egress rules			
Source CIDR		Protocol	Add	

- 8. Click TenantA-Network tab.
- 9. Click View IP Address

		C Refi
Details		
2 3 x		Vew IP Addresses
Name	TentnatA-Network	
Ø	b7ea6861-1a84-4422-b8ab-0d3c93073454	
Zone	TentantA-Zone	
Description	TentnatA-Network	
Туре	Isolated	
State	Implemented	
Restart required	No	
VLAN ID	1003	
Network Offering	Offering for isolated networks with Source Nat service enabled	

## Figure 241 Displaying the Network Details

**10.** Click **+Acquire New IP** button.

## Figure 242 Displaying the IP Address for the Guest Network

n Network - Guest networks Ten	natA-Network 🔪 IP Addresse		
			🔦 🕂 Acquire New IP
IPs	Zone	VM name	State
10.65.122.164 [Source NAT]	TentantA-Zone		Allocated

11. Click Yes button.

ſ

			🔍 🕂 Acquire New
<sup>o</sup> s	Zone	VM name	State
10.65.122.164 [Source NAT]	TentantA-Zone		Allocated
Confirma	tion		
	tion In that you would like to acquire ew IP for this network.		

1

## Figure 243 Confirming the IP Address

**12.** IP Address <10.65.122.166> Public IP Address is allocated.

## Figure 244 Displaying the IP Address

			<u> </u>	Acquire New
IPs	Zone	VM name	State	Quickview
10.65.122.166	TenantA-Zone		Allocated	+
10.65.122.165 [Source NAT]	TenantA-Zone		Allocated	-

- **13**. Click **IP Address** <10.65.122.166>.
- **14**. Click the **Configuration** tab.



#### Figure 245 Displaying the Configuration Flow diagram

- 15. Click Firewall tab.
- **16.** Enter  $\langle 0.0.0.0/0 \rangle$  in Source CIDR field.
- **17.** Select TCP Protocol List Value.
- 18. Enter 3389 in (RDP) in Start Port field.
- 19. Enter 3389 in (RDP) End Port field.
- 20. Click Add button.

I

Firewall							
Source CIDR	Protocol	Start Port	End Port	ICMP Type	ICMP Code	Add rule	Action
0.0.0/0	TCP V	3389	3389			Add	

1

## Figure 246 Defining the Firewall Configurations

21. Click Port Forwarding in the flow diagram.



ñ	Network - Guest networks	TenantA-Network	IP Addresses	10.65.122.166	Port Forwarding	
						C Refresh
	Port Forwarding					
	Private Port P	ublic Port	Protocol	Add VM	Action	5
	3389 3389	3389 3389	ТСР	× Add		
	<b>22.</b> Enter 3	3389 in Private Port	field.			

- 23. Enter 3389 in Public Port field.
- 24. Select TCP under Protocol list box.

## Figure 248 Defining the Port Forwarding Configurations

- **25.** Click **Add**.
- 26. Click Select radio button on TenantA-Platinum-VM1.
- 27. Click Apply.

## Figure 249 Adding VMs

						V
Name	Internal name	Display name	Zone name	State	Select	
TenantA-Platinum-	VM1	TenantA-Platinum-VM1	TenantA-Zone	Running	۲	

To configure VM Data Disk on TenantA Zone, login to the CloudPlatform:

### Attaching Data Disk to TenantA-Platinum-VM1

- 1. Provide User Name <root> and Password <XXXXX> and Domain.
- 2. Click Login.
- 3. Click the Service Offerings tab.
- 4. Select Disk Offering in Select offering list box.

#### Figure 250 Displaying the Disk Offerings

Service Offerings - Disk Offerings		
Select offering: Disk Offerings	<u>a</u>	+ Add Disk Offering

Vame	Description		Custom Disk Size	Disk Size (in GB)	Orde	er		
Small	Small Disk, 5 GB	No	E	5	\$	÷	W	=
Medium	Medium Disk, 20 GB	No	4	20	*	¥	w	=
Large	Large Disk, 100 GB	No	1	00	\$	¥	w	=
Custom	Custom Disk	Yes	h	ųγ	\$	÷	V	-

- 5. Enter Platinum-NFS-Storage in the Name field.
- 6. Enter Platinum-NFS-Disk in the Description field.
- 7. Select shared in Storage Type list box.
- 8. Check Custom Tags check box.
- 9. On QoS Type List do not select.
- **10**. Enter Platinum-NFS-Storage in Storage Tags.
- **11**. Select **Public** check box.
- 12. Click OK.

ſ

* Name:	Platinum-NFS-Storage	
Name.	( latinum vi o otorage	
* Description:	Platinum-NFS-Disk	
Storage Type:	shared	~
Custom Disk Size:		
QoS Type:		~
Storage Tags:	Platinum-NFS-Storage	
Public:		

1

Figure 251 Defining the Disk Offerings Information

- **13**. Click the **Storage** tab.
- 14. Select Volumes in Select view list box.

## Figure 252 Displaying the Storage Volume

fi Stora	ge - Volumes				
Select view:	Volumes 💽		Q 1 Upload volume	+ Add Volume	
Name	Туре	Hypervisor	VM display name		
ROOT-11	ROOT	XenServer	TentantA-Platinum-VM1		

- 15. Click Add Volume button.
- 16. Select Volumes in Select view list box.
- **17.** Enter Platinum-NFS-Data-Vol.
- **18.** Select <TenantA-Zone> in Availability Zone list box.
- 19. Select Platinum-NFS-Disk in Disk Offering list box.
- **20.** Enter 20 in Disk Size (in GB) field.

🕒 Add Volume			
Please fill in the following data to add a new volume.			
* Name:	Platinum-NFS-Data-Vol		
Availability Zone:	TenantA-Zone 🗸		
Disk Offering:	Platinum-NFS-Disk V		
* Disk Size (in GB):	20		
Cancel	ОК		

Figure 253 Defining the Volume Information

- **21.** Click <Platinum-NFS-Data-VOL>.
- 22. Click Attach Disk icon.

I

Γ

🐔 🔪 Storage - Volumes 🔪 Pl	atinum-NFS-Data-Vol		
		C Refr	esh
Name ROOT-29 Platinum-NFS-Data-Vol	Details Attach Disk	View Snapshots	>
ROOT-27			
	Name	Platinum-NFS-Data-Vol	î
	ID	7d558754-041f-4f98-a2c7-b94658e72ea0	
	Zone	TenantA-Zone	
	State	Allocated	
	Status		
	Туре	DATADISK	
	Storage Type	shared	
	Hypervisor		
	Size	20.00 GB	~

1

## Figure 254

Displaying Data Disk Details

- **23**. Select <TenantA-Platinum-VM1> in Instance list box.
- **24**. Click **OK**.

A Storage - Volumes Platinum-NFS-Data-Vol			
			C Refresh
Name ROOT-29 Platinum-NFS-Data-Vol	Details		View Snapshots
R00T-27			
KOOTZI	Name	Platinum-NFS-Data-Vol	^
Attach Disk     Attach Disk     Instance:     Cancel	TenantA-Platinum-VI	c7-b94658e72ea0	
	Туре	DATADISK	
	Storage Type	shared	
	Hypervisor		
	Size	20.00 GB	~

#### Figure 255 Attaching Instance to Disk

- 25. Remotely connect to TenantA-Platinum-VM1 <10.65.122.166> (IP Acquired).
- **26.** Login with <administrator> and Password <xxxxxxxx>.
- 27. Open Server Manager.
- 28. Click Storage Under Disk Management .
- 29. Right click Disk 1 Initilize and Online Disk .
- **30.** Select Create simple volume.
- 31. Click Next.
- **32**. Select Assign drive Letter (E).
- 33. Click Next.
- **34**. Select default options.
- 35. Click Next.

ſ

36. Click Finish.

Figure 256	Windows VM displaying Attached Disk info
------------	--

1

1

Eile Action View Help				
(= -> 2 💼 2 💼 2 📾				
Server Manager (WIN-NMNLSJIE4T	Disk Managemen	it Volume List + Graphical View		
<ul> <li>              € ■ Roles      </li> <li>             ∰ Features         </li> </ul>	Volume	Layout Type File System Status		
<ul> <li></li></ul>	📼 (C:)	Simple Basic NTFS Healthy (Boot, Page File, Crash Dump, Primary Partit		
🗄 👬 Configuration	📼 New Volume (E:)			
🖃 🚟 Storage	System Reserved	d Simple Basic NTFS Healthy (System, Active, Primary Partition)		
Windows Server Backup				
	Disk 0     Basic 20,00 GB	System Reserved (C:)		
	Online	100 MB NTFS Healthy (System, Activ Healthy (Boot, Page File, Crash Dump, Primary Partit		
	Disk 1 Basic 20,00 GB Online	New Yolume (E:) 20.00 GB NTF5 Healthy (Primary Partition)		
	CD-ROM 0 DVD (D:) No Media			
	Unallocated	▼ Primary partition		

# **VM Backup and Restore**

This section explains how to configure virtual machine backup and restore policy based on the service levels offering in cloud. The CloudPlatform performs backup of VM OS and Data disks by taking snapshots of disk volumes. Snapshots are a point-in-time capture of virtual machine disks where OS and Data information is stored.

• Backup Methods
There are two methods to take a VM backup, the first method is manual where cloud administrator has to manually take a backup of the disk volumes, and the second method is automatic wherein the recurring snapshots policies can be configured allowing schedule backup time, based on Hourly, Daily, Weekly and Monthly basis with retention numbers. More than one backup policy can be defined according to the requirement.

• Restore Methods

There are two ways to perform snapshot restore, the first method is by creating volume of the snapshot, attaching the snapshot in the form of disk to instance VM. The second method is by creating a template and access the backup VM.

Note

It is recommended to create snapshot restore of Data disk using first method and root disk (Operating System) using second method.

In this study we will create manual backup of TenantA-Platinum-VM1 root and automatic backup of Platinum-NFS-Data-Vol data disk and restore root disk with template and Data disk with volume method using CloudPlatform.

Login to CloudPlatform with User credentials to create TenantA-Platinum-VM1 manual and automatic backup on TenantA Zone

# Manual Backup

- 1. Provide User Name <root> and Password <XXXXXX> and Domain.
- 2. Click Login.
- 3. Click the **Storage** tab.

🐔 🔪 Storage - Volumes 🔪 RO	00T-27		
ŧ			C Refresh
Name Platinum-NFS-Data-Vol	Details		
ROOT-27			View Snapshots
	Name	R00T-27	^
	ID	2e86c19a-4112-43d6-8562-7d685edac131	
	Zone	TenantA-Zone	
	State	Ready	
	Status		
	Туре	ROOT	
	Storage Type	shared	
	Hypervisor	VMware	
	Size	20.00 GB	~

1

#### Figure 257 Displaying the Storage Volume Data

- 4. Click Root-27 under Name in right pane.
- 5. (Manual backup of TenantA-Platinum-VM1 root disk (Operating System)
- 6. Click Take Snapshot icon with single camera.



Ensure you Virtual Machines are powered down to take a Consistent Snapshot copy on ESXi Hypervisor Host.

🛱 🔪 Storage - Volumes 🔪 R	00T-27		
		C Ref	resh
Name Platinum-NFS-Data-Vol ROOT-27	Details Take Snapshot	View Snapshots	
	Name	R00T-27	^
	ID	2e86c19a-4112-43d6-8562-7d685edac131	
	Zone	TenantA-Zone	
	State	Ready	
	Status		
	Туре	ROOT	
	Storage Type	shared	
	Hypervisor	VMware	
	Size	20.00 GB	~

## Figure 258 Displaying Snapshots of Storage Volume

I

Γ

7. Click **Yes** to Confirm.

🛱 🔪 Storage - Volumes 🔪 ROO	T-27			
				C Refresh
Name ROOT-29	Details			
Platinum-NFS-Data-Vol	+ 10 %	j		View Snapshots
R00T-27	-			_
	Name	ROOT-27		^
	nation confirm that you wa napshot of this volu No	ant to take a ume. Yes	12-43d6-8562-7d685edac131	
	Туре	ROOT		
	Storage Type	shared		
	Hypervisor	VMware		
	Size	20.00 GB		~

1

Figure 259 Taking the Snapshot

# **Automatic Backup**

- 1. Provide User Name <root> and Password <XXXXX> and Domain.
- 2. Click Login.
- **3.** Click the **Storage** tab.

🐔 🔪 Storage - Volumes				
Select view: Volumes	$\checkmark$		🔍 🚺 Upload volume	Add Volume
Name	Туре	Hypervisor	VM display name	Quickview
Platinum-NFS-Data-Vol	DATADISK	VMware	TenantA-Platinum-VM1	+
ROOT-27	ROOT	VMware	TenantA-Platinum-VM1	+

# Figure 260 Displaying the Storage Volume

- 4. Click Platinum-NFS-Data-Vol Under Name in the right pane
- 5. (Automatic backup of TenantA-Platinum-VM1 data disk based on every day at midnight and keep 2 weeks backup data).
- 6. Click **Recurring Snapshot** icon with double camera.

ſ

			C Refres
lame	Details		
OOT-29	Setup Recurring	Snapshot	
latinum-NFS-Data-Vol	+ 🖸 🖬	Ø_ 14	ew Snapshots
OOT-27			
	Name	Platinum-NFS-Data-Vol	
	ID	7d558754-041f-4f98-a2c7-b94658e72ea0	
	Zone	TenantA-Zone	
	State	Ready	
	Status		
	Туре	DATADISK	
	Storage Type	shared	
	Hypervisor	VMware	
	Size	20.00 GB	

#### Figure 261

Setting up the Recurring Snapshot Feature

1

- 7. Click **Daily** button in Schedule field.
- 8. Select 12 Hour 00 minutes and PM in Time list box.
- **9.** Select Pacific Standard Time in Timezone list box.
- **10.** Enter 8 value in Keep field.
- 11. Click Add.
- 12. Click Done.

	Dashboard	n Storage - Volumes TentantA-Platinum-VM1-Data-Disk	
Ð	Dasibbaru		C Refres
2	Instances	Name Details	
		Recurring Snapshots	
1	Network	You can setup recurring snapshot schedules by selecting from the available options below and applying your policy preference	View Snapshots
	Templates	Schedule: 💽 Hourty 🔄 Daily 🖅 Weekty 🕮 Monthly	
5	Events	Time 59 - minute(s) Past the Hour	
2	Accounts	Timezone [UTC-08:00] Pacific Standard Time  Keep snapshot(s)	
2	Domains	Add	
2	Infrastructure	Scheduled Snapshots	
2	Projects	Time: 12:00 Time: 12:00 Timezone: [UTC-08:00] Pacific Standard Time Keep: 8 X	
8	Global Settings	Done	
*	Service Offerings	Size 10.00 GB	
		VMID detached	

# Figure 262 Defining the Schedule for Recurring Snapshot

# **Template based Snapshot Restore**

Γ

- 1. Provide User Name <root> and Password <XXXXX> and Domain.
- 2. Click Login.
- 3. Click the **Storage** tab.

Figure 263	Displaying the Storage Volume
------------	-------------------------------

elect view: Volumes	~		V 🔍 👔 Upload volume	+ Add Volun
Name	Туре	Hypervisor	VM display name	Quickview
Platinum-NFS-Data-Vol	DATADISK	VMware	TenantA-Platinum-VM1	+
ROOT-27	ROOT	VMware	TenantA-Platinum-VM1	+

I

1

- 4. Click Root-27 under Storage-Volumes.
- 5. Click View Snapshots.

Figure 264	Displaying th	o Snanchot	Dotaile
rigure 204	Displaying th	e Snapsnot	Details



6. Click Root-27 Snapshot.

#### 7. Click View Snapshots.

#### Figure 265 Viewing the Snapshot Status

🛱 🔪 Storage - Volumes	ROOT-27 Snaps	hots		
				⊽ 🔍
Volume	Interval Type	Created	State	Quickview
ROOT-27	MANUAL	Fri, 20 Sep 2013 08:50:47 UTC	BackedUp	+

8. Click Create Template icon with + symbol.

Figure 266	Creating the New	<sup>,</sup> Template
------------	------------------	-----------------------

Storage - Volume	s > ROOT-27 > Si	napshots	
			v <mark>9</mark>
Volume	Interval Type	Created State	Quickview
ROOT-27	MANUAL	Quickview: ROOT-27	+
		Name       TenantA-Platinum-VM1_ROOT- 27_20130920085047         ID       c4bc5358-45c1-411b-b05c-b00edar         Volume Name       ROOT-27         State       Create template         & Create template       Create Volume       Del Sna	

- 9. Click **Create Template** icon with + symbol.
- **10**. Enter Backup-TenantA-Platinum-VM1.
- **11.** Enter Template based Restore.
- **12.** Select Windows 2008 R2(64-bit) in OS Type list box.
- **13.** Select **Public** check box.

ſ

14. Do not select **Password Enabled** check box.

olume	Interval Type	Created	State	Quickview
ROOT-27	MANUAL	Quickview: ROOT-27		+
<b>3</b>	Create template	Platini 9200:	um-VM1_ROOT- 85047	
	* Name: Backup	-TenantA-Platinum-VM1	-411b-b05c-b00eda11184b	
	* Description: Templa	te Based Backup		
	OS Type: Window Public: 🗹	vs Server 2008 R2 (64-bit) 🗸	/olume 🗙 Delete Snapshot	
Pass	word Enabled:		_	_
	Dynamically Scalable:			
	Cancel	ОК		
	Cancel	ОК		

1

Figure 267 Defining the Template Properties

- **15.** Click the **Instances** tab.
- 16. Click Add Instance button in the right pane.
- **17.** Select TenantA-Zone in Zone list box.
- **18.** Click **Template** radio button.
- 19. Click Next.

Add Instance			
1 Setup 🛛 2 Set	ect a o S Compute of	4 Data Disk o 5	Network o G Review
Select a zone			
1	a single datacenter. Multiple zones help ma ng physical isolation and redundancy.	ke	
Tendate-zone			
Select ISO or template			
Template	OS image that can be used to boot VMs		
○ ISO	Disc image containing data or bootable media for OS		
			Cancel Next

## Figure 268 Selecting the Zone for the Template

- 20. Click My Templates.
- 21. Click Backup-TenantA-Platinum-VM1 radio button.
- 22. Click Next.

I

Γ



#### Figure 269 Selecting the Template for Virtual Interface

I

1

- 23. Click Platinum-Compute radio button.
- 24. Click Next.



## Figure 270 Selecting the Compute Offering

I

Γ

- 25. Click No Thanks radio button.
- 26. Click Next.

Add	Instance					_			
1	Setup 🧧 2	Select a template	<del>9</del> 3	Compute offering	• 4	Data Disk Offering	Netwo	ork o	Review
<ul> <li>N</li> </ul>	o Thanks								
0	Small Small Disk, 5 GB				<u>^</u>			6	
0	<b>Medium</b> Medium Disk, 20 GB				E			OS BRANK	
0	Large Large Disk, 100 GB								
0	Custom Custom Disk								
							~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		

1

Figure 271 Not selecting any Disk Offering

- 27. Check TenantA-Network check box, and click **Default** radio button.
- 28. Click Next.

Setup 🧿 2 Select a 🔹	3 Compute of 2	Data Disk Offering	Network	Review
e select networks for your virtual machine.	c: None 👻			_
works				
TentnatA-Network Isolated	Oefault			
			05	
		C		
i Network				
New				
evious			Cancel	Next

Figure 272 Selecting the Disk Networks for VM

- **29.** Enter Backup-TenantA-Platinum-VM1 in Name (Optional) field.
- 30. Click Launch VM.

Γ

Filter by	All				
Add Instance		_	_		
Setup 92 Set	lect a <b>3</b> Compute <b>3</b>	Data Disk Offering	Affinity <b>2</b> 6	Network 2	7 Review
se review the following inform re launch.	ation and confirm that your virtual in	stance is correct			
Name (Optional)	Backup-TenantA-Platinu	n			
Add to group (Optional)					
Zone	TenantA-Zone	🖉 Edit			
Hypervisor	VMware	🖉 Edit		00	
Template	Backup-TenantA-Platinum- VM1	🖉 Edit			
Compute offering	Platinum-Compute	🖉 Edit			
Data Disk Offering	(None)	🖉 Edit	0		- 6621
Affinity Groups	(None)	🖉 Edit	0		
Network	TenantA-Network	🖉 Edit			
				2	
					db
Previous				Cancel	

Figure 273 Verifying the Virtual Instance Information

1

- **31**. Click the **Instances** tab.
- 32. Click Backup-TenantA-Platinum-VM1.

	C Refresh
Name         Details         NICs         Statistics           Backup-TenantA-Platinum	
VM1	
TenantA-Platinum-VM1         Ø 3 0 × 0+ 2 + 4 E         C Re	eset VM
View Volumes View Snapshots View Affinity Groups View Hosts	×
Display name Backup-TenantA-PlatinumVM1	^
Name Backup-TenantA-PlatinumVM1	
State Running	
Template Backup-TenantA-PlatinumVM1	
Dynamically Scalable Yes	
OS Type Windows Server 2008 R2 (64-bit)	
Hypervisor VMware	
Attached ISO	
Compute offering Platinum-Compute	~

Figure 274 Selecting the Backup VM

I

Γ

**33**. Click **View Console**.

	antA-PlatinumVM1		C Refres
lame Backup-TenantA-Platinum	Details	NICs Statistics View console	
/M1		: @, / + = =	C Reset VM
	View Volumes	View Snapshots View Affinity Groups	View Hosts
	Display name	Backup-TenantA-PlatinumVM1	ŕ
	Name	Backup-TenantA-PlatinumVM1	
	State	Running	
	Template	Backup-TenantA-PlatinumVM1	
	Dynamically Scalable	Yes	
	OS Type	Windows Server 2008 R2 (64-bit)	
	Hypervisor	VMware	
	Attached ISO		
	Compute offering	Platinum-Compute	

1

#### Figure 275 Viewing the Backup VM Details

- **34.** Enter Username <administrator> and password <XXXXX> and login
- **35.** Note: The Password is same has Parent Instance VM is set.

Backup Tenant A-Platinum- 1-2-33-VM Backup Tenant A-Platinum- Tenant A-zone Running Image: Comparison of the state of	BackupTenantA-Platinum- VM1		Display name	Zone name		T
BackupTenantA-Platinum- VM1       i2:33-VM       BackupTenantA-Platinum- VM1       TenantA-Zone       Running       Image: Construction of the constru	BackupTenantA-Platinum- VM1		Display name	Zone name		
VM1 12-33-VM VM1 IPIAIIU-20ne Running Imitu-20ne   Imanu-20ne Running Imitu-20ne Running Imitu-20ne   DackupTenarutA-Platinum-VM1 - Windows Internet Explore Imitu-20ne Imitu-20ne   tp://10.65.121.70.80800/client/console?cmd=access&vm=6s34516b-f4df-4984-b65c-15e100bc33bd Imitu-20ne   CrtI-Att-Del Imitu-20ne CrtI-Esc Imitu-20ne Keyboard Press CTRL + ALT + DELETE to log on	VM1	i-2-33-VM			State	Quickview
BackupTenantA-Platinum-VM1 - Windows Internet Explorer         tp://10.65.121.70:80800/client/console?cmd=access&vm=6a34516b-f4df-4984-b65c-15e100bc33b6         Ctrt-Alt-Det       Ctrt-Esc         Keyboard         Press CTRL + ALT + DELETE to log on	TenantA-VM1			TenantA-Zone	Running	+
tp://10.65.121.70:8080/client/console?cmd=access&vm=6a34516b-f4df-4984-b65c-15e100bc33b6		i-2-25-VM	TenantA-VM1	TenantA-Zone	Running	+
Ctrt-Alt-Del Ctrt-Esc Keyboard Press CTRL + ALT + DELETE to log on		BackupTena	ntA-Platinum-VM1 - Wind	lows Internet Exp	lorer	
Press CTRL + ALT + DELETE to log on	tp:// <b>10.65.121.70</b> :8080/clien	t/console?cmd=acces	ss&vm=6a34516b-f4df-4984-b65	c-15e100bc33b6		
Press CTRL + ALT + DELETE to log on	Ctrl-Alt-Del 🛛 🍓 Ctrl-Es	c 🛛 🍓 Keyboard				
			D CTDI		TTT	
			Press CTRL + A	ALT + DELE	TE to log o	n
				3		

#### Figure 276 Logging into the VM

# **Volume based Snapshot Restore**

ſ

- 1. Provide User Name <root> and Password <XXXXX> and Domain.
- 2. Click Login.
- **3.** Click the **Storage** tab.
- 4. Select Volumes under Select View list box.

lect view: Volumes	$\sim$		V 🔍 🚹 Upload volume	+ Add Volum
Name	Туре	Hypervisor	VM display name	Quickview
Platinum-NFS-Data-Vol	DATADISK		TenantA-VM1	+
ROOT-25	ROOT		TenantA-VM1	+
ROOT-33	ROOT		BackupTenantA-Platinum-VM1	

1

- 5. Click TenantA-Platinum-Data-Disk Volume.
- 6. Click View Snapshots.

🐔 🔪 Storage - Volumes 🔪 Plati	inum-NFS-Data-Vol		
Ð			C Refresh
Name Platinum-NFS-Data-Vol	Details		
ROOT-25		9_ =	View Snapshots
ROOT-33			
	Name	Platinum-NFS-Data-Vol	^
	ID	3984d6e0-3bea-4bec-aa5d-75427f0b9c5c	÷
	Zone	TenantA-Zone	
	State	Ready	
	Status		
	Туре	DATADISK	
	Storage Type	shared	
	Hypervisor		
	Size	20.00 GB	~

## Figure 278 Viewing Snapshot of Virtual Data Disk

I

Γ

- 7. Click TenantA-Platinum-Data-Disk Volume.
- 8. Click View Snapshots.
- 9. Click Create Volume icon.

🐔 🔪 Storage - Volumes 🔪	Platinum-NFS-Data-Vol	Snapshots Platinum-NFS-Data-Vol	
			C Refresh
Volume Platinum-NFS-Data-Vol	Details Create Volume		
	Name	TenantA-VM1_Platinum-NFS-Data- Vol_20131003123941	^
	ID	dcc5fdc0-102f-4c66-9673-8d997fd561de	
	Volume Name	Platinum-NFS-Data-Vol	
	State	BackedUp	
	Interval Type	MANUAL	
	Domain	ROOT	
	Account	admin	
	Created	Thu, 3 Oct 2013 12:39:41 UTC	
	Tags		~
10 Ente	er - Backup Tenant A Pl	latinum-Data-Disk> in the Name field	

1

#### Figure 279 **Creating Volume**

- **10.** Enter <Backup-TenantA-Platinum-Data-Disk> in the Name field.
- 11. Click OK.

🛱 Storage - Volumes Platin	num-NFS-Data-Vol	Snapshots Platinum-NFS-Data-Vol	
			C Refresh
Volume Platinum-NFS-Data-Vol	Details		
	Name	TenantA-VM1_Platinum-NFS-Data- Vol_20131003123941	î
😌 Create Volume		73-8d997fd561de	
* Name:	Backup-TenantA-PI	atinum-Data-Disl	
Cance	I OK		
	Domain	ROOT	
	Account	admin	
	Created	Thu, 3 Oct 2013 12:39:41 UTC	
	Tags		Ň

## Figure 280 Adding Name for the Volume

I

Γ

- 12. Click Storage tab.
- 13. Click Backup-TenantA-Platinum-Data-Disk.

# Figure 281 Displaying the Storage Volume

ect view: Volumes			Vpload volume	🕂 Add Volun
Name	Туре	Hypervisor	VM display name	Quickview
Backup-TenantA-Platinum-Data-Disk	DATADISK			+
Platinum-NFS-Data-Vol	DATADISK		TenantA-VM1	+
ROOT-25	ROOT		TenantA-VM1	+
ROOT-33	ROOT		BackupTenantA-Platinum-VM1	+

1

14. Click Attach Disk icon.

Ð			C Refre
lame Backup-TenantA-Platinum-Data-Di	Details Attach Di	sk	
Platinum-NFS-Data-Vol		년 <del>1</del> × <sup>목</sup>	View Snapshots
ROOT-25			
ROOT-33	Name	Backup-TenantA-Platinum-Data-Disk	
	ID	c91b5270-6f66-4e23-8fc4-36f47d2a61c7	
	Zone	TenantA-Zone	
	State	Ready	
	Status		
	Туре	DATADISK	
	Storage Type	shared	
	Hypervisor		
	Size	20.00 GB	

#### Figure 282 Attaching the Disk

- 15. Select Backup-TenantA-Platinum-VM1 under Instance list box.
- 16. Click OK.

Γ

## Figure 283 Selecting the Disk to the Instance

🕣 Atta	ch Disk		
Attach E	Disk		
	Instance: Backu	pTenantA-Platinum-V	/ <u>M1</u>
ſ	Cancel	ОК	

17. Select Backup-TenantA-Platinum-VM1 under Instance list box.

1

- **18**. Click **View console**.
- **19.** Provide User Name <Administrator> Password <XXXXX>
- 20. Access Disk Manumit Online Disk1.

#### Figure 284 Online snap restored Disk

A Instances					
6	BackupTenant/	A-Platinui	m-VM1 - Win	dows Internet Explorer	. 🗆 X
<i>lefter://10.65.121.70</i> :8080/client/co/	nsole?cmd=access&	vm=6a3451	6b-f4df-4984-b6	5c-15e100bc33b6	Ra Ra
🖡 Server Manager					
File Action View Help					
🗢 🔿 📶 🖬 🖬 🖆 🖆	7 😼				
Server Manager (WIN-GK7KFRUHR	Disk Management	Volume Li:	st + Graphical Viev	v.	
<ul> <li>              € Roles      </li> <li>             € Features         </li> </ul>	Volume	A REAL PROPERTY OF A REAL PROPER	ype File System	Status	Capacity F
Diagnostics	(C:)     New Volume (E:)	Simple Ba	asic NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition) Healthy (Primary Partition)	19.90 GB 5
<ul> <li>Configuration</li> <li>Task Scheduler</li> </ul>	System Reserved	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1		Healthy (System, Active, Primary Partition)	100 MB
🕀 🝻 Windows Firewall with Adva					
Services					
🛨 🌺 Local Users and Groups					
🖃 📇 Storage Windows Server Backup					
Disk Management					
	4				
	Disk 0				
	Basic 20.00 GB	System Re 100 MB NTF:		(C:) 19.90 GB NTFS	
	Online	Healthy (Sys	stem, Active, Prim	Healthy (Boot, Page File, Crash Dump, Primary Partition)	)
				12	
		New Volum			
		20.00 GB NT Healthy (Prir	TFS mary Partition)		
	19005				
	CD-ROM 0			0	
	DVD (D:)			A A	ctivate V
<					to Acyon C

# **VM Migration**

This section explains the configuration steps required to perform the manual migration of the VM from one host to another without interrupting service to users or going into maintenance mode. This is called manual live migration, and can be done under the following conditions:

- The root administrator is logged in. Domain admins and users cannot perform manual live migration of VMs.
- The VM is running. Stopped VMs cannot be live migrated.
- The destination host must be in the same cluster as the original host.
- The VM must not be using local disk storage.
- The destination host must have enough available capacity. If not, the VM will remain in the "migrating" state until memory becomes available.



In this study VM instance TenantA-Platinum-VM1 on Cloud Host TenantA-HostA will be migrated to TenantA-HostB.

Login to CloudPlatform with User credentials to manually live migrate TenantA-Platinum-VM1 to TenantA-Host B:

- 1. Provide User Name <root> and Password <XXXXX> and Domain.
- 2. Click Login.
- **3.** Click the **Instance** tab.
- 4. Click TenantA-Platinum-VM1.

#### Figure 285 Selecting the Tenant A Platinum Host

ilter by All	2			v 🔍	+ Add Instanc
Name	Internal name	Display name	Zone name	State	Quickview
TenantA-Platinum-VM1	i-2-27-VM	TenantA-Platinum-VM1	TenantA-Zone	Running	+

5. Click the migrate instance to another host button.

Iter by All	2			V 🔍	+ Add Instanc
Name	Internal name	Display name	Zone name	State	Quickview
TenantA-Platinum-VM1	i-2-27-VM	Quickview: Te	nantA-Platinum-VM1		+
		Display name Name	TenantA-Platinum-VM1 TenantA-Platinum-VM1		
		State 	Running Windows 2008 R2		
		Ø Stop	3 Reboot	Take VM Snapshot	
		X Destroy		r host Attach ISO	
		View Volumes		View Affinity Groups	

1

#### Figure 286 Migrate Instance

- 6. Select 10.65.121.165 (TenantA-HostB) Host in list box.
- 7. Click OK.

ñ Instances		na en			
Filter by All				v <mark>q</mark> -	Add Instance
Name	Internal name	Display name	Zone name	State	Quickview
TenantA-Platinum-VM1	i-2-27-VM	Quickview: TenantA	-Platinum-VM1		+
		Lispiay name	antA-Platinum-VM1 antA-Platinum-VM1		
		State Run	ining		
🕒 Migrate i	instance to anothe	r host	2008 R2		
	Host: 10.65.121.	165 (Suitable)	boot	Take VM Snapshot	
	Cancel	ОК	set VM	Ø₊ Attach ISO	
			grate to host	Change service offering	
		View console			
		View Volumes View	w Snapshots	/iew Affinity Groups	
		View Hosts			

## Figure 287 Selecting Destination Host for Migration

**8.** VM Migrate task is completed.

Γ

🐔 🔪 Instances 🔪 Ten	antA-Platinum-VM1		
······································			C Refresh
Details	NICs Statistics	Volumes	
0 3 × 0-	₽ ~ + 🗵		View Volumes
Display name	TenantA-Platinum-VM1		-
Internal name	i-2-3-VM		
State	Running		
Hypervisor	XenServer		
Template	RHEL6-0		
OS Type	Red Hat Enterprise Linux 6.0 (64-bit)		
Attached ISO	RHEL6-0		
Compute offering	Platinum-Compute		
HA Enabled	Yes		
			Task completed Migrate instance to another host

1

# Figure 288 Migration Completion

nstances TenantA-Plati	num-VM1		
			C Refresh
Name	Details	NICs Statistics	
TenantA-Platinum-VM1		: 0, 2 + 4 2	C Reset VM
	View Volumes	View Snapshots View Affinity Groups	View Hosts
	Dynamically Scalable	No	î
	OS Type	Windows Server 2008 R2 (64-bit)	
	Hypervisor	VMware	
	Attached ISO		
	Compute offering	Medium Instance	
	HA Enabled	No	
	Group		
	Zone name	TenantA-Zone	
	Host	10.65.121.165	~

#### Figure 289 VM Migration Summary

# **VM Storage Migration**

This section explains the configuration steps required to perform the manual migration of the Virtual Machine Storage from the primary storage to the other primary storage for maintenance, or load balancing mode. The storage migration can be performed on stopped instance only and no disks should be attached to the VM instance.

Note

ſ

In current CloudPlatfrom 4.2.1.1 version Virtual Machine Storage Migration with same Cluster in Zone is not supported using GUI, however you can achieve this by making API Call.

To accomplish this use API "migrateVirtualMachineWithVolume" by specifying a target host for VM & target storage pool for each volume of the VM.

Here is example:

command=migrateVirtualMachineWithVolume&hostid=<TARGET\_HOST>&virtualmachineid=<V M\_IN\_QUESTION>&migrateto[<I>].volume=<VOLUME\_ID>&migrateto[<I>].pool=<TARGET\_POOL \_ID> <TARGET\_HOST> - UUID of target host for the VM to be relocated to. This host can be within or out of cluster. <VM\_IN\_QUESTION> - UUID of VM which need to be migrated out of the current storage pool. <VOLUME\_ID> - UUID of volume of the VM <TARGET\_POOL\_ID> - UUID of target primary storage pool. This pool can belong to current cluster or other cluster)

# **VM Deletion**

This section explains the steps taken for cleaning up virtual machines as part of maintenance efforts by the cloud administrator which releases compute, network and storage resources back to cloud pool for reusability.

Once a virtual machine is destroyed, all the resources used by the virtual machine will be reclaimed by the system. This includes the virtual machine's IP address.



In this study we will delete Backup-TenantA-Platinum-VM1 using CloudPlatform.

Login to CloudPlatform with User credentials to create TenantA-Platinum-VM1 manual and automatic backup on TenantA Zone:

- 1. Provide User Name <root> and Password <XXXXX> and Domain.
- 2. Click Login.
- 3. Click the Global Setting tab under search type secstorage.allowed.internal.sites.
- 4. Under secstorage.allowed.internal.sites enter <<Var\_HTTP\_Server>> 10.65.121.705.
- 5. Restart CloudPlatfrom service.

		C Refr
Details	NICs Statistics Volumes	
0 3 8 6	· / ~ + E	View Volumes
Dest	roy Instance	
Display name	Backup-TentantA-Platinum-VM1	
Internal name	i-2-12-VM	
State	Running	
Hypervisor	XenServer	
Template	Backup-TentantA-Platinmum-VM1	
OS Type	Other (64-bit)	
Attached ISO		
Compute offering	Platinum-Compute	
HA Enabled	No	

#### Figure 290 Destroying the Instance to check the Backup

# **Baremetal Host Cloud Configuration Design**

This section outlines Citrix CloudPlatform 4.2.1 BareMetal host as a service offering which can be provided in private cloud environment. Multiple tenants can install LINUX based operating system on physical compute to run work loads which have performance and security requirement, CloudPlatfrom 4.2.1 provides multi-tendency and life cycle management of these BareMetal hosts.

CloudPlatform 4.2.1 supports the kick start installation method for RPM-based Linux operating system on baremetal hosts in basic zones. Users can provision a baremetal host managed by CloudPlatform as long as they have the kick start file and corresponding OS installation ISO ready.

Kickstart installation eliminates manual intervention during OS installation. It uses a text file as a script to automate installation. The kickstart file contains responses to all the user input prompts that are displayed when you install an operating system. With kickstart installation, you can automate the installation of operating system software on large numbers of hosts.

# **Limitation of Kick Start Baremetal Installation**

- 1. Use in advanced zones is not supported. Use in basic zones only.
- 2. CloudPlatform storage concepts: primary storage, secondary storage, volume, snapshot.
- 3. System VMs: SSVM, CPVM, VR.
- 4. Template copy or template download.
- 5. VM migration.
- 6. Multiple NICs.
- 7. Using host tag for allocating host, capacity (cpu, memory) specifying in service offering.
- 8. A stopped VM (the OS running on host) can only start on the host it was most recently on.

The Citrix BaremetalCloud Design has been split into the following tasks:

- 1. Defining Network and Compute Offerings.
- 2. Defining Zones.
- 3. Defining Network.
- 4. Adding Pods.
- 5. Adding Cluster.
- 6. Adding Hosts.
- 7. Baremetal Host Deployment.

# **Defining Network and Compute Offerings**

A zone is the largest organizational unit within a CloudPlatform deployment. A zone typically corresponds to a single datacenter, although it is permissible to have multiple zones in a datacenter. The benefit of organizing cloud compute, network and storage infrastructure into zones is to provide physical isolation and redundancy.

To create zones using Citrix CloudPlatform application dedicated for TenantA multi-tenant to host cloud services, login to CloudPlatform with user credentials and follow these steps:

admin

Domain Login

-

1

- 1. Type the User Name <root>, Password <XXXXX>, and Domain.
- 2. Click Login.

Figure 291 Logging to the Citrix CloudPlatform

<b>citrix</b> CloudPlatform	

3. Click Agree to confirm the End User License Agreement.

- 4. Click I have used CloudPlatform before, skip this guide button.
- 5. Click **Infrastructure** tab in the left pane.

nfrastructure			
		Dpda	te SSL Certificate 📿 Refresh
Infrastructure			
Zones	Pods O	Clusters	Hosts
View all	View all	View all	View all
Primary Storage	Secondary Storage	System VMs	Virtual Routers
View all	View all	View all	View all

Figure 292 Displaying the Infrastructure Page

- 6. Click Service Offerings in the left pane.
- 7. On the right pane, under Select Offering list box, select Network Offering.
- 8. Click Add Network offering.
- 9. Enter TenantA-BareMetal-Network in the Name field.
- **10.** Enter Network for BareMetal Hosts in the Description field.
- 11. Select Shared in Guest Type list box.
- 12. Check Specify VLAN check box.

ſ

13. In Supported Services, select DHCP check box.

- 14. Select BaremetalDhcpProvider under DHCP Provider list box.
- **15.** Select UserData check box.
- **16.** Select BaremetalUserdataProvider under User Data Provider list box.

1

- 17. Check BaremetalPxeService check box.
- **18.** Click **OK**.

Figure 293 Configuring Baremetal Network Offering

ect offeri	Add network of	fering	Add network offeri				
Name	* Name:	TenantA-BareMet	tal-Network		Order		Quickview
DefaultSha	* Description:	Network for Barel	Metal Hosts	Enabled	* *	A V =	+
DefaultSha	Network Rate (Mb/s):		)	Enabled	* *	A V =	+
Defaultisol	Guest Type:	Shared	~	Enabled	* *	<b>A V =</b>	+
Defaultisol	Persistent :			Enabled	* *	<b>▲ ▼</b> =	+
DefaultSha	Specify VLAN:			Enabled	* *	<b>▲ ▼</b> =	+
Defaultisol	Supported Services:	VPN:		Enabled	* *	<b>A V</b> =	+
Defaultisol		DHCP:		Enabled	* *	A V =	+
Defaultisol		DHCP Provider: DNS:	Baremeta V	Enabled	* ¥	<b>▲ ▼</b> =	•
QuickClou		Firewall:		Enabled	± ¥	<b>▲ ▼</b> =	+
		Load Balancer: User Data: User Data	Baremeta V				
	Conserve mode:						
	Tags: Cance	I ОК					

**19.** Select TenantA-BareMetal-Network and Enable Network.
A Service Offerings - Network	Offerings TenantA-B	areMetal-Network	C Refresh
Name	Details	1	
TenantA-BareMetal-Network DefaultSharedNetworkOfferingWitt	Enable network offering		
DefaultSharedNetworkOffering	Name	TenantA-BareMetal-Network	^
DefaultIsolatedNetworkOfferingWit	Wallie	1 enanti-Datemetal-Network	
DefaultIsolatedNetworkOffering	ID	212d3e2c-de07-4a32-8184-d35c6ba9302b	
DefaultSharedNetscalerEIPandELI	Description	Network for BareMetal Hosts	
DefaultIsolatedNetworkOfferingFor	State	Disabled	
DefaultIsolatedNetworkOfferingFor	Guest Type	Shared	
DefaultIsolatedNetworkOfferingFor	Persistent	No	
QuickCloudNoServices	Egress Default Policy	Allow	
	Availability	Optional	
	Created by system	No	~

#### Figure 294 Enable TenantA-BareMetal-Network offering

- **20**. Click **Service Offerings** in the left pane.
- 21. On right pane, under Select Offering list box, select Compute Offering.
- 22. Click Add Compute offering.
- 23. Enter TenantA-BareMetal-Compute in the Name field.
- 24. Enter Compute Offering in the Description field.
- **25.** Enter Shared in Storage Type field.
- **26.** Enter <Physical\_Blade\_CPU\_Core> 16 in CPU Cores field.
- 27. Enter <Physical\_Blade\_CPU\_Mhz> 1333 in CPU Mhz field.
- **28.** Enter <Physical\_Blade\_Memory> 212992 in Memory (MB) field.
- 29. Click OK.

ſ

* Name:	TenantA-BareMetal-Compute	* Description:	Compute Offerring
Storage Type:	shared 🗸	*# of CPU Cores:	16
CPU (in MHz):	1333	* Memory (in MB):	212992
Network Rate (Mb/s):		Disk Read Rate (BPS):	
isk Write Rate (BPS):		Disk Read Rate (IOPS):	
isk Write Rate (IOPS):		Offer HA:	
Storage Tags:		Host Tags:	
CPU Cap:		Public:	
isVolatile:		Deployment Planner:	<b>~</b>
Planner Mode:	~		

#### Figure 295 Configuring Baremetal Compute Offering

1

#### **Defining Zones**

- 1. With Infrastructure tab selected in the left pane, click View all on Zones in the right pane.
- 2. Click + Add Zone.

#### Figure 296 Displaying the Infrastructure Page

				🔍 🕂 Add Zo
Zone	Network Type	Public	Allocation State	Actions
No data to show				

4. Click Next.

	one type elect a configuration fo	r your zone.
۲	Basic	Provide a single network where each VM instance is assigned an IP directly from the network. Guest isolation can be provided through layer-3 means such as security groups (IP address source filtering).
0	Advanced	For more sophisticated network topologies. This network model provides the most flexibility in defining guest networks and providing custom network offerings such as firewall, VPN, or load balancer support.
1	Isolation Mode	
	Security Groups	Choose this if you wish to use security groups to provide guest VM isolation.

#### Figure 297 Defining the Basic Zone Configuration

- 5. Enter TenantA-BareMetal-Zone in the Name field.
- 6. Enter <Public\_DNS\_IP\_Address>72.163.128.140 in DNS1 field.
- 7. Enter 171.70.168.183 in Internal DNS 1 field.
- 8. In Hypervisor select BareMetal in list box.
- 9. In Network Offering select TenantA-BareMetal-Network.
- 10. Click Next.

ſ

Figure 298

Zone Type	02	Setup Zone	<b>0</b> 3	Setup Network	• 4	Add Resources	05	Launch
zone is the largest o d redundancy. A zo rver which is shared	rganizational ne consists o I by all pods i	unit in CloudPla f one or more po n the zone.	tform™, and ds (each of	d it typically corre which contains h	sponds to a si osts and prima	ngle datacenter. Z ny storage servers	ones provide   s) and a secor	physical isolati idary storage
* Name:	Tenant	A-BareMetal-2	Zone					
* IPv4 DNS1:	72.163.	128.140						
IPv4 DNS2:								
* Internal DNS 1:	171.70.	168.183						
Internal DNS 2:								
* Hypervisor:	BareMe	tal			~			
Network Offering:	Tenant/	\-BareMetal-I	Network		~			
	-				,			

**Defining the Zone Attributes** 

## **Defining Network**

After defining zone the next step is to design and define cloud network. This solution design implements the basic networking, since Baremetal hosts can only be added to zones with basic network support. We will have one physical network defined in a zone which will carry Guest and Management traffic types.

- Management Traffic is generated within the CloudPlatform as the internal resources communicate with each other. This includes communication between hosts
- Guest Private Traffic is used and generated by Baremetal hosts. The guest network results when Baremetal hosts communicate with each other over a network.

To configure the zone basic network using Citrix CloudPlatform application dedicated for TenantA-BareMetal multi-tenant to host cloud services, follow these steps:

- 1. Drag guest Public and Private traffic and Storage Types icon to Physical Network 2.
- 2. Rename Physical network Network 1 TenantA-BareMetal-Network in Physical network name field.

I

#### 3. Click Next.

Figure 299

Add zone	
Zone Type	2 Setup Zone 2 3 Setup Network 2 4 Add Resources 2 5 Launch
PHYSICAL NET	WORK > • POD > • GUEST TRAFFIC > • STORAGE TRAFFIC >
types of traffic.	sic zone, you can set up one physical network, which corresponds to a NIC on the hypervisor. The network carries several and drop other traffic types onto the physical network.
raffic Types	Physical network name TenantA-BareMetal-Network ×
Storage	Management Guest Storage
	Imanagement     Odest     Storage       Imanagement     Imanagement     Odest     Storage       Imanagement     Imanagement     Imanagement     Imanagement       Iman
Previous	Cancel Next

Defining the Basic Networking Configuration for the Zone

## **Adding Pods**

I

Pod is the second-largest organizational unit within a CloudPlatform deployment. Pods are contained within zones. Each zone can contain one or more pods. A pod consists of one or more clusters of hosts and one or more primary storage servers.

To add pod network in a zone advanced network configuration using Citrix CloudPlatform application dedicated for TenantA-BareMetal multi-tenant to host cloud services, follow these steps:

- 1. Enter TenantA-BareMetal-Pod in Pod Name field.
- Enter <Management\_VLAN\_602\_GW\_IP\_Address>10.65.121.1 in Reserved System Gateway field.
- 3. Enter 255.255.255.0 in Reserved System netmask field.

4. Enter 10.65.121.190 in Start Reserved system IP field.

1

- 5. Enter 10.65.121.200 in End Reserved system IP field.
- 6. Click Next.

#### Figure 300 Adding the Pod to the Zone

Zone Type	02	Setup Zone	03	Setup Network	<b>•</b> 4	Add Resources	05	Launch
OD > • GUE ach zone must contain Il add in a later step. Inge must be unique f	n in one or r First, config	nore pods, and y ure a range of re e in the cloud.			∖ pod contair dPlatform™\\	is hosts and prima is internal manage	ary storage ser ement traffic. Ti	vers, which you ne reserved IP
* Pod name:	Tenant	A-BareMetal-	Pod					
* Reserved system gateway:	10.65.1	21.1						
* Reserved system netmask:	255.25	5.255.0						
* Start Reserved system IP:	10.65.1	21.190						
End Reserved system IP:	10.65.1	21.200			×			

#### **Adding Guest Traffic**

To add guest network in a zone basic network configuration using Citrix CloudPlatform application dedicated for TenantA-BareMetal multi-tenant to host cloud services, follow these steps:

- 1. Enter <guest\_VLAN20\_GW\_IP\_Address>20.1.1.1 in Gateway field.
- **2.** Enter 255.255.255.0 in netmask field.
- **3.** Enter 20.1.1.20 in Start IP field.
- 4. Enter 20.1.1.30 in End IP field.
- 5. Click Next.

Add zone	
Zone Type	• 2 Setup Zone • 3 Setup Network • 4 Add Resources • 5 Launch
Guest network traffic	BUEST TRAFFIC > • STORAGE TRAFFIC > ic is communication between end-user virtual machines. Specify a range of IP addresses that CloudPlatform <sup>™</sup> can assign to ure this range does not overlap the reserved system IP range.
Guest Gateway:	20.1.1.1
Guest Netmask:	255.255.255.0
Guest start IP:	20.1.1.20
Guest end IP:	20.1.1.30 ×
Previous	Cancel

Figure 301 Setting the Guest VLAN Range

I

Γ

6. Click **Yes** to Zone creation.

)	Creating zone	
0	Creating physical networks	
2	Configuring physical network	
)	Creating guest network Zone creation complete. Would you like to enable this zone?	
)	Creating pod	
)	Configuring storage traffic No Yes	
2	Configuring guest traffic	
)	Zone creation complete	

#### Figure 302 Zone creation Confirmation

#### Adding Cisco UCS Manager Plugin

You can provision Cisco UCS server blades into CloudPlatform for use as bare metal hosts. The goal is to enable easy expansion of the cloud by leveraging the programmability of the UCS converged infrastructure and CloudPlatform's knowledge of the cloud architecture and ability to orchestrate. CloudPlatform can automatically understand the UCS environment, server profiles and so on such that CloudPlatform administrators can deploy a bare metal OS on a Cisco UCS.

In this study we will register Cisco UCS Manager to CloudPlatfrom using Cisco UCS Manager Plugin. Pefrom hardware inventory to display available blades and their status (Service Profile associated / disassociated).

The CloudPlatfrom admin now can choose blade which is free (unassociated), create Service Profile based on Service Profile Template already defined by Cisco UCS Manager which trigger Cisco UCS Manager API calls to create Service Profile based on Service Profile Template associate blade.

On successfully association of blade CloudPlatfrom performs Baremetal as a Service provisioning by installing RHEL 6.3 Operating System using PXE Boot.

 The CloudPlatfrom needs HTTP and HTTPS protocol to be enabled for accessing Cisco UCS Manager, so make sure Cisco UCS Manager Communication Services for HTTP Admin State is <enabled> & Redirect HTTP to HTTPS is <disabled>.

4					Cisco Unified Com	outing System Manager - TME-L21
Fault Summ	ary			- 16	🕃 💿 🗉 New 🚽 🛃 Options 😢 🕕 🔝 Pending Activities 🚺 Exit	
	$\nabla$		Δ			
4	13	9	55		>> 🛱 All 🕨 🗧 Communication Management 🕨 🔗 Communication Services	
Equipment S	ervers LAN SAN VM	Admin			Communication Services Events FSM	
	Filter: All	•			Web Session Limits Shell Session Limits	
+ =				Ш	Maximum Sessions Per User: 32 Maximum Sessions Per User:	32
= 🙀 All			[		Maximum Sessions: 256 Maximum Sessions:	32
	ults, Events and Audit Log	,				
	Faults Events				(HTTP	Telnet
	Events Audit Logs				Admin State:   Enabled  Disabled	Admin State: O Enabled O Disabled
	Syslog				Admin State:   Enabled  Disabled	Admin State: Enabled   Disabled
	Core Files				Port: 80	
- D	TechSupport Files				Operational Port: 80	
	Settings					
	er Management				Redirect HTTP to HTTPS: O Enabled O Disabled	
	Authentication					
	LDAP				HTTPS	CIM XML
	RADIUS					
	TACACS+				Admin State: <ul> <li>Enabled</li> <li>Disabled</li> </ul>	Admin State: 🔘 Enabled 💿 Disabled
E 🥰	User Services				Port: 443	
±	- Authenticates	d Users			Operational Port: 443	
	Remotely Authentica					
(F)	- Roles	100 03013			Key Ring: KeyRing default 💌	
📄 🔑 Ке	y Management				Cipher Suite Mode: 🕓 High Strength 💿 Medium Strength 🔵 Low Strei	ngth 🔘 Custom
	KeyRing default					
👘 📋 Čo	mmunication Management				Cipher Suite: :XPORT40:!EXPORT56:!LOW:RC4+RSA:+HIGH:+MED:	IUM:+EXP:+eNULL
	) Call Home					
	Communication Services				SNMP	
	DNS Management				Admin State: O Enabled O Disabled	
	Management Interfaces				Admin State: Chabled Isabled	

#### Figure 303 Cisco UCS Manager Communication Services HTTP configuration details

Login to CloudPlatform with User credentials to configure Cisco UCS Manager Plugin on the zone TenantA-BareMetal-Zone:

1. Click Login.

I

- 2. Click the Infrastructure tab on the left pane.
- 3. Click the Zones View All.
- 4. Click <TenatA-BareMetal-Zone> Zone.
- 5. Click Compute and Storage.
- 6. Click UCS View All.



#### Figure 304 Adding Cisco UCS Manager details

- 8. Enter Name <Cisco UCS Manager-Cloud>.
- 9. Enter URL: <10.65.121.14> UCS Cluster IP Address.



- Enter only IP address.
- **10.** Enter UserName <admin>.
- **11.** Enter Password <xxxxx>.
- 12. Click OK.

ager
UCSM-Cloud
10.65.121.14
admin

Figure 305 Displaying the Cisco UCS Manager Plugin Configuration

13. Click Cisco UCS Manager-Cloud.

Figure 306 Access Cisco UCS Manager Plugin

ñ	Infrastructure	Zones	TenantA-BareMetal-Zone	UCS		
					•	Add UCS Manager
1	Vame			URL	ŝ	
	UCSM-Cloud			10.6	55.121.14	

#### 14. Click Blades.

**15.** The current CloudPlatfrom 4.2.1 displays all Blades which are associated with Service Profile or available for association with Service Profile to provision Baremetal host. CloudPlatfrom 4.2.1 allows associating freely available Blade by creating Service Profile derived using Service Profile Template created on Cisco UCS Manager.



I

In current CloudPlatfrom 4.2.1 version the Cisco UCS Manager Plugin allows blade association with Service Profile derived by Service Profile Template created only in Root Org on Cisco UCS Manager, so make sure you have created Service Profile Templates under Root Org for Cisco UCS Manager Plugin to expose in CloudPlatfrom Manager and it is advised to Refresh Blades before starting Baremetal provisioning.

Details	Blades		
			Refresh Blade
Chassis	Blade ID	Associated Profile	Actions
chassis-1	blade-2		e e
chassis-1	blade-1	org-root/org-TentantA/Is-CitrixManagmentServer	C Ø.
chassis-1	blade-4		2 0.
chassis-1	blade-8	org-root/org-TentantA/Is-TenantA-ESX-HostA-Platinum	0.
chassis-1	blade-5	org-root/org-TentantA/Is-N1kVSM	(? <i>O</i> _
chassis-1	blade-7	org-root/org-TentantA/Is-TenantA-ESX-HostC-Platinum1	8 0-

#### Figure 307 Cisco UCS Manager displaying physical Blades available inventory

16. On Blade-2 Under Action, click on Associate Profile to Blade.

#### Figure 308 Select blade -2 to associate with Service Profile in Cisco UCS Manager

Details	Blades		VA
			Refresh B
Chassis	Blade ID	Associated Profile In	stantiate Template and Associate Profile t
chassis-1	blade-2		Ø e.
chassis-1	blade-1	org-root/org-TentantA/ts-CitrixManagmentSe	rver 🕜 @.
chassis-1	blade-4		0 %
chassis-1	blade-8	org-root/org-TentantA/Is-TenantA-ESX-Host	A-Platinum 🕜 🖉
chassis-1	blade-5	org-root/org-TentantA/Is-N1kVSM	8 Ø.
chassis-1	blade-7	org-root/org-TentantA/Is-TenantA-ESX-Host	C-Platinum1 😥 🖉

- 17. Select Platinum-Baremetal-Template in Select Template list box.
- 18. Enter BareMetal-Host1 in Profile Name field.
- 19. Click OK.

				O R
Details	Blades			
				Refresh Bla
Chassis	Blade ID	Associated Profile		Actions
chassis-1	blade-2			<b>C</b> (4)
cha 🕕 Inst	anciate Template	and Associate Profile to B	ade ntServer	@ Ø.
cha				<b>e</b> «.
cha <sup>*</sup> Selec	t Template: org-r	root/ls-Platinum-Baremetal-T	ei V HostA-Platinum	C .
cha	Profile: Bare	Metal-Host1	×	@ Ø.

# Figure 309 Select Platinum-Baremetal-Template to create BareMetal-Host1 Service Profile to associate blade-2

**20.** After Service profile BareMetal-Host1 is associated with Blade 2, Figure 310 shows Cisco UCS Manager and CloudPlatfrom mapping configuration.

Γ



#### Figure 310 Cisco UCS Manager and CloudPlatfrom displaying BareMetal-Host1 Service Profile associated with blade-2

## **Adding Cluster**

Cluster provides a way to group hosts. Here we to be precise, we have cluster with set of Baremetal hosts part of cluster. The hosts in a cluster all have identical hardware, run the same Baremetal operating system, are on the same subnet, and access the same shared primary storage.

A cluster is the third-largest organizational unit within a CloudPlatform deployment. Clusters are contained within pods, and pods are contained within zones. Size of the cluster is limited by the underlying hypervisor, although the CloudPlatform recommends less in most cases. A cluster consists of one or more hosts and one or more primary storage servers.

To add cluster in zone using Citrix CloudPlatform application dedicated for TenantA multi-tenant to host cloud services, follow these steps:

- 1. Select <TenantA-BareMetal-Zone> in Zone Name list box.
- 2. Select <BareMetal> in Hypervisor list box.
- 3. Select <TenantA-BareMetal-Pod> in Pod Name list box.
- 4. Enter <TenantA-BareMetal-Cluster> in Cluster Name field.
- 5. Click Next.

Name	Pod	Hypen	visor	State	Quickview
No data to show					
🕣 A	dd Cluster				
	* Zone Name: Tena	IntA-BareMetal-Zone	~		
	Hypervisor: Bare	Metal	~		
	Pod Name: Tena	antA-BareMetal-Pod	$\sim$		
*(	Cluster Name: Tena	ntA-BareMetal-Cluster			

#### Figure 311 Adding the Cluster to the Zone

## **Adding Hosts**

I

A host provides the computing resources that run the Baremetal Operating System. Each host has Baremetal linux based OS software installed on it to manage Applications. The Host here is an RHEL 6.3 Based server. The host is the smallest organizational unit within a CloudPlatform deployment. Hosts are contained within clusters, clusters are contained within pods, and pods are contained within zones.

To add host in cluster using Citrix CloudPlatform application dedicated for TenantA-BareMetal multi-tenant to host cloud services, follow these steps:

- 1. Select <TenantA-BareMetal-Zone > in Zone Name list box.
- 2. Select <TenantA-BareMetal-Pod > in Pod Name list box.
- **3.** Enter <TenantA-BareMetal-Cluster > in Cluster Name field.
- 4. Enter <UCS-IPMI-IP-Address> 10.65.121.57 in Host Name field.



**Note** The IP Address of Host Name is the CIMC IP Address assigned to physical blade by Cisco UCS Manager which is been added as a Baremetal host to the zone.

5. Enter <admin> in Username field.





I

## **Adding PXE and DHCP Servers**

ſ

CloudPlatfrom 4.2.1 requires external PXE and DHCP servers to access to support Baremetal host PXE installation of Operating System on physical Server. The PXE and DHCP setup and configurations can be referred in Cloud Deployment section.

Login to CloudPlatform with User credentials to create PXE and DHCP servers on the zone TenantA-BareMetal-Zone:

- 1. Provide User Name <root> and Password <XXXXX> and Domain.
- 2. Click Login.
- 3. Click the Infrastructure tab.
- 4. Click Zones View all.
- 5. Click TenantA-BareMetal-Zone.
- 6. Click Physical Network.
- 7. Click TenantA-BareMetal-Network.
- 8. Click Configure Network Service Providers.



#### Figure 313 DHCP and PXE Server configuration Details

- 9. Click **Baremetal PXE** tab.
- **10.** Click **+ ADD** icon to add Baremetal PXE Device.

🕺 👌 Infrastructure 🔪 Zones	TenantA-BareMetal-Zo	ne 🔪 TenantA-BareMetal-Network 📎 Network Service Providers 🔪
		C Refresh
Name	Details	
NetScaler		
Virtual Router	+ ×	View Devices
Nicira Nvp		
BigSwitch Vns	Add Baremetal PX	LE Device
Baremetal DHCP	Name	Baremetal PXE
Baremetal PXE		
Security Groups	State	Enabled

#### Figure 314 Add Baremetal PXE server configuration Details

**11.** Enter < BaremetalAgent\_PXE\_Server\_IP\_Address > http://20.1.1.5 in URL field.

# Note

**e** IP Address 20.1.1.5 is assigned to server which has CloudPlatfrom 4.2.1 Baremetal agent and PXE services configured.

- **12**. Enter < root > in Username field.
- **13**. Enter < XXXXX > in Password field.
- **14**. Enter < **/export** > in Tftp root directory.

## 

ſ

- **Note** /export path is where PXE and Baremetal OS image files are stored and NFS exported for more details refer to Cloud Deployment section.
- 15. Click OK.

ñ	Infrastructure Zones	TenantA-BareMetal-Zone	TenantA-BareMetal-Network	Network Service Providers
				2 Refresh
	Name	Details		
	NetScaler			
	Virtual Router	+ ×		View Devices
	Nicira Nvp			
	BigSwitch Ves			
	Baremetal	PXE Device		
	Baremetal	Lu. (00 1 1 5	×	
	* URL:	http://20.1.1.5		
	* Username:	root		
	* Password:	•••••		
	* Tftp root directory:	/export		
	Cance	і ок		

#### Figure 315 Add Baremetal PXE server and Path configuration Details

1

- 16. Click **Baremetal DHCP** tab.
- 17. Click + ADD icon to add Baremetal DHCP Device.

#### Figure 316 Add Baremetal DHCP server configuration Details

<b>A</b> Infrastructure Zones	TenantA-BareMetal-Zon	e TenantA-BareMetal-Network	Network Service Providers
Ð	-		C Refresh
Name	Details		
NetScaler			
Virtual Router	+ = ×		View Devices
Nicira Nvp			
BigSwitch Vns	Add Baremetal DH	ICP Device	
Baremetal DHCP	Name	Baremetal DHCP	
Baremetal PXE			
Security Groups	State	Enabled	

**18.** Enter <CloudPlatfrom\_Management\_IP\_Address> http://10.65.121.70 in URL field.

# Note IP Address 10.65.121.70 is assigned to server which has DHCP services configured for more details refer to Cloud Deployment section.

- **19.** Enter < **root** > in Username field.
- **20.** Enter < **XXXXX** > in Password field.
- 21. Click OK.

Figure 317 Baremetal DHCP Server Configuration Details

fi Infrastructure Zones	TenantA-BareMetal-Zone	TenantA-BareMetal-Netwo	ork 🔪 Network Service Providers 🔪
			🔍 🕂 Add Baremetal DHCP Device
Add Baremetal	DHCP Device	_	
* URL:	http://10.65.121.70		
* Username:	root		
* Password:		*	
		_	
Cance	ОК		

## **Baremetal Host Deployment**

This section explains how to register Baremetal host template with Linux Operating System PXE Image and create Baremetal instance with Compute and Network offerings.

Bare metal hosts can run any of the following operating systems CentOS 5.5, CentOS 6.2, CentOS 6.3, Fedora 17, RedHat 6.1 – 6.3 and Ubuntu12.04

In this study we will install RHEL 6.3 operating system on newly created Baremetal instance BareMetal-Host1 using PXE method on FCoE NetApp Cluster Target.

Login to CloudPlatform with User credentials to create ISO Image TenantA Zone:

- 1. Provide User Name <root> and Password <XXXXX> and Domain.
- 2. Click Login.
- 3. Click the **Template** tab.

- 4. Select Templates in Select view list box.
- 5. Click Register template.
- 6. Enter BareMetal-RHEL6-3-Template in the Name field.
- 7. Enter RHEL6-3 Image in the Description field.
- 8. Enter URL Path ks=http://20.1.1.5/RHEL63/RHEL63.ks;kernel=20.1.1.5:/var/www/html/RHEL63/vmlinuz;initrd= 20.1.1.5:/var/www/html/RHEL63/initrd.img

Note

Make sure you provide correct path for RHEL6-3 kickstart, kernel and initrd files. The directory /export and /var/www/html/RHEL63 where these files are stored is been NFS exported. For more details refer Cloud Deployment section.

- 9. Select TenantA-BareMetal-Zone in Zone list box.
- 10. Select BareMetal in Hypervisor list box.
- 11. Select **BareMetal** in Format list box.
- 12. Select Red Hat Enterprise Linux 6.3 (64 bit) in OS Type list box.
- **13.** Check **Extractable** check box.
- 14. Check Public check box.
- 15. Check Featured check box.
- 16. Click OK.

fi Templates				
Select view: Templates	Filter by All		V 9	Register template
Name	Zone	Hypervisor	Order	Quickview
No data to 📀 Register ter	mplate			
* Nar	me: BareMetal-RHEL6-	3-Template		
* Descripti				
* UF		HEL63/RHEL63.		
Zo	ne: TenantA-BareMetal-	-Zone 🗸		
Hypervis	Sor: BareMetal	~		
Form	nat: BareMetal	~		
OS Ty		Linux 6.3 (64-t 🗸		
Extractal	_			
Password Enable				
Dynamica Scalab	ally 🔲 ble:			
Pub				
Featur	_			
Routi	ng:			
Са	incel OK			
				Activ

Figure 318 Displaying the Baremetal Template Details

- **17.** Click the **Instances** tab.
- 18. Click Add Instance.
- **19.** Select **TenantA-BareMetal-Zone** in Select a Zone list box.
- 20. Select Template radio button.
- 21. Click Next.

Γ

	Figure 319	Selecting Template	
🕣 Add Instand	ce		
1 Setup	Select a template	Compute Data Disk Affinity Network Review	
		single datacenter. Multiple zones help oviding physical isolation and redundancy.	1
Select IS	O or template		
۲	Template	OS image that can be used to boot VMs	
0	ISO	Disc image containing data or bootable media for OS	
		Cancel Ne	xt

1

- 22. Enter BareMetal-RHEL6-3-Template in the Name field.
- 23. Enter RHEL6-3 Image in the Description field.
- 24. Select BareMetal-RHEL6-3Template in template.
- 25. Click Next.



#### Figure 320 Selecting Template Image

- 26. Select TenantA-BareMetal-Compute in Compute offering.
- 27. Click Next.

Γ

Setu	p <b>02</b> Select a <b>33</b> Compute <b>2</b> Data Disk <b>2</b> Offering <b>2</b>	Affinity O Network O Review
0	Small Instance Small Instance	
۲	TenantA-BareMetal-Compute Compute Offering	
0	Medium Instance Medium Instance	
reviou		Cancel

1

#### Figure 321 Selecting Compute Offering

- **28**. Select **Medium** in Data Disk offering.
- 29. Click Next.



#### Figure 322 Selecting Disk Offering

30. Click Next.

Γ

	Setup	02	Select a template	03	Compute offering	•4	Data Disk Offering	o5	Affinity	O Netwo	rk 🗿	Review
Y	ou do n	ot have	any affin the n	ity gro ext ste	ups. Plea p.	se cor	ntinue to					
									<			
											0.5	
	revious	1								Ca	ncel	Next

1

#### Figure 323 No Affinity Rules Configured

31. Click Next.



#### Figure 324 No Network Configured

32. Click Reboot.

ſ

**33.** Final screen after PXE Boot on host **BareMetal-Host1**.



#### Figure 325 Instance Final Configuration setting

## **Baremetal Blade Deprovision**

This section explains the steps taken for cleaning up Baremetal Instance as part of maintenance efforts by the cloud administrator which releases compute, network and storage resources back to cloud pool for reusability. As part of this process Cisco UCS Manager will disassociate Service Profile on Blade and delete Service Profile,



In this study we will disassociate BareMetal-Host1 using CloudPlatform.

Login to CloudPlatform with User credentials to delete BareMetal-Host1 Instance on the zone TenantA-BareMetal-Zone:

- 1. Provide User Name <root> and Password <XXXXX> and Domain.
- 2. Click Login.
- 3. Click the Infrastructure tab.
- 4. Click the **Zones** and click on **TenantA-BareMetal-Zone**.
- 5. Click UCS ViewAll.



#### Figure 326 Accessing Cisco UCS Plugin

6. Click **TME-L21** and click in **Blades**.

ſ

7. Click Disassociate Profile from Blade icon on blade-2 of chassis-1.

			€ Re
Details	Blades		
Chassis	Blade ID	Associated Profile	Disassociate Profile from Blade
			540 CON
chassis-1	blade-2	org-root/is-BareMetal-Host1	80.
chassis-1	blade-1	org-root/org-TentantA/Is-CitrixManagmentServer	<i>© ©</i> .
	blade-4		<b>C</b> .
chassis-1			
chassis-1 chassis-1	blade-8	org-root/org-TentantA/Is-TenantA-ESX-HostA-Platinum	C Ø.

#### Figure 327 Selecting blade-2 on chassis-1 to Disassociate from BareMetal-Host1 Service Profile in Cisco UCS Plugin

1

8. Enabe Delete Profile check box (This option will delete Service profile on Cisco UCS Manager).

9. Click OK.

			C Re
Details	Blades		
			🖉 Refresh Bla
Chassis	Blade ID	Associated Profile	Actions
chassis-1	blade-2	org-root/is-BareMetal-Host1	8 0.
chassis-1	blade-1	orn-root/orn-TentantA/Is-CitrixMananmentServer	0 0.
cha 🕣 Dis	associate Profile f	rom Blade	<b>C</b> Ø.
<b>cha</b> De	elete Profile: 🔽	HostA-Platinum	C Ø.
cha			0-
	· · · · · · · · · · · · · · · · · · ·		

Figure 328 Enabling Delete Profile check box to delete Service Profile BareMetal-Host1

10. Service Profile BareMetal-Host1 is disassociated with blade-2 and deleted in Cisco UCS Manager.



<b>A</b>	TME-L21 /		Message	x	By: admin)	-	x
	Macros Tools Help ver ॳ Shutdown Server		The server has been disassociated. This session needs to be	closed.			
KVM Consol	e Properties		ОК				
💣 күм 🔤	Virtual Media						
			ux Server release 6.3 (Santiago) x86_64 on an x86_64				
lo	calhost login:	_					

## **Baremetal Instance Life Cycle Management**

I

This section explains the steps taken for providing Baremetal Instance life cycle management as part of maintenance efforts by the cloud administrator which releases compute, network and storage resources back to cloud pool for reusability.

The CloudPlatfrom 4.2.1.1 invokes Cisco UCS Manager API Calls using IPMI interface to start, stop, reboot and destroy RHEL Operating System running on Cisco UCS Blade Server, part of Baremetal host.

#### **Reboot Baremetal Instance**

In this study we reboot BareMetal-Host1 Instance using CloudPlatform.

Login to CloudPlatform with User credentials to reboot BareMetal-Host1 Instance on the zone TenantA-BareMetal-Zone:

- 1. Provide User Name <root> and Password <XXXXX> and Domain.
- 2. Click Login.
- 3. Click the Instances tab.
- 4. Click **Quickview** icon on BareMetal-Host1.
- 5. Click Reboot.

#### Figure 330 Reboot BareMetal-Host1 Instance

A Instances						
Filter by All	~				v <mark>q</mark>	Add Instance
Name	Internal name	Disp	lay name	Zone name	State	Quickview
BareMetal-Host1	i-2-2-VM	Bar	Quickview: B	areMetal-Host1		+
			Display name Name State Template Stop Stop Destroy Reset Passe Change ser offering View Volumes View Hosts	Reboot     Reset VM word     Create template	emplate Take VM Snapshot  C Attach ISO  Migrate to host View Affinity Groups	

6. Click Yes to confirm instance.

fi Instances					
Filter by All	×			v 🔍	- Add Instance
Name	Internal name	Display name	Zone name	State	Quickview
BareMetal-Host1	i-2-2-VM	Bar Quickview	: BareMetal-Host1		+
	Confirmation Please confirm tha in No	Display nam Name Ctate t you want to rebo stance. Yes	BareMetal-Host1 Running JareMetal-RHEL6-3 ot this Reboot Reset VM	-Template Take VM Snapshot Ø <sub>4</sub> Attach ISO	
		Change offering View Volume View Hosts	Service New console		

#### Figure 331 Confirm Reboot BareMetal-Host1 Instance

## **Stop and Start Baremetal Instance**

۵, Note

I

In this study we stop and start BareMetal-Host1 Instance using CloudPlatform.

Login to CloudPlatform with User credentials to reboot BareMetal-Host1 Instance on the zone TenantA-BareMetal-Zone:

- 1. Provide User Name <root> and Password <XXXXX> and Domain.
- 2. Click Login.
- 3. Click the **Instances** tab.
- 4. Click Quickview icon on BareMetal-Host1.
- 5. Click Stop.

Iter by All	~				v 💊 🛛	+ Add Instand
Name	Internal name	Display nar	ne Zo	ne name	State	Quickview
BareMetal-Host1	i-2-2-VM	Bar Qui	ckview: Bare	Metal-Host1		+
		Disp	lay name	BareMetal-Host1 BareMetal-Host1		
		State		Running		
		0	Stop	BareMetal-RHEL6-3-Te	Take VM Snapshot	
		×	Destroy	C Reset VM	Ø₊ Attach ISO	
		P	Reset Password	Create template	🕂 Migrate to host	
		ц.	Change service offering	View console		
		View	v Volumes	View Snapshots	View Affinity Groups	
		1/10	w Hosts			

1

#### Figure 332 Stop BareMetal-Host1 Instance

- 6. Click Yes to confirm Stop instance.
- 7. Uncheck Force Stop instance.

n Instances							
Fifter by All						₹ م	+ Add Instance
Name	Internal name	Disp	lay name	Zone name		State	Quickview
BareMetal-Host1	i-2-2-VM	Bar	Quickview:	BareMetal-Host	1		+
			Display name	BareMetal-He			
			Name	BareMetal-H	ost1		
	op instance	_	_	-R	HEL6-3-Tem	plate	
Please	e confirm that you	want t	o stop this ins	tance.			
	Force Stop:					Snapshot	
		_		set	VM	Ø₄ Attach ISO	
	Cancel		ОК	eat	e template	+ Migrate to hos	st
			Change s offering	ervice 🚬 View (	console		
			View Volumes	View Snapsho	ots 🛛	/iew Affinity Groups	>
			View Hosts	\$: 			

#### Figure 333 Confirm Stop BareMetal-Host1 Instance

8. Stop instance status.

#### Figure 334 Stop status of BareMetal-Host1 Instance

n Instances					
Filter by All				v <mark>q</mark>	Add Instance
Name	Internal name	Display name	Zone name	State	Quickview
BareMetal-Host1	i-2-2-VM	BareMetal-Host1	TenantA-BareMetal-Zone	Stopped	+

- 9. Click the Instances tab.
- 10. Click Quickview icon on BareMetal-Host1.
- 11. Click Start instance

ſ

ilter by All	✓			v 🔍	+ Add Instand
Name	Internal name	Display name	Zone name	State	Quickview
BareMetal-Host1	i-2-2-VM	<sup>Bar</sup> Quickviev	v: BareMetal-Host1		+
		Display nan Name State Start Insta	BareMetal-Host1 Stopped nce BareMetal-RHEL6-3-T	emplate	
		C Reset	Password  Create template e service Assign Instance	* storage	
		View Volume		View Affinity Groups	>

1

#### Figure 335 Start BareMetal-Host1 Instance

**12.** Click **Yes** to confirm start instance.

fi Instances							
Filter by All						V 🔍	- Add Instance
Name	Internal name	Disp	lay name	Zone name		State	Quickview
BareMetal-Host1	i-2-2-VM	Bar	Quickview: E	BareMetal-Host	1		+
			Display name	BareMetal-Ho	ost1		
			Name	BareMetal-Ho	ist1		
	Confirmation		State	Stopped			
	Please confirm	that you	u want to start t	lareMetal-RI		nplate	
		instanc	e.	Take Snaps	/M hot	X Destroy	
	No	)	Yes	₹ Chang	le affinity	Ø₄, Attach ISO	
				Create	e template	Higrate to storage	
			Change se offering	rvice Assigr to And Accou			
			View Volumes	View Snapsho	ts	View Affinity Groups	
			View Hosts				

Figure 336 Start BareMetal-Host1 Instance Confirmation

I

Γ

**13**. Running BareMetal Status after start instance.

Figure 337	BareMetal-Host1 running status after start instance
------------	-----------------------------------------------------

2	Notifications	Project: Default view	·   ▶ 💽 [	admin cloud 🔻	<b>citrix</b> .
n Instances					
Filter by All	~			▼ �	Add Instance
Name	Internal name	Display name	Zone name	State	Quickview
BareMetal-Host1	i-2-2-VM	BareMetal-Host1	TenantA-BareMetal-Zone	Running	+

### **Destroy and Restore Baremetal Instance**

In this study we destroy and restore BareMetal-Host1 Instance using CloudPlatform.

Login to CloudPlatform with User credentials to destroy BareMetal-Host1 instance on the zone TenantA-BareMetal-Zone:

1

- 1. Provide User Name <root> and Password <XXXXX> and Domain.
- 2. Click Login.
- 3. Click the **Instances** tab.
- 4. Click Quickview icon on BareMetal-Host1.
- 5. Click Destory.

#### Figure 338 Destroy BareMetal-Host1 Instance

r Instances							
Filter by All	$\checkmark$					▼ �	+ Add Instance
Name	Internal name	Disp	lay name	Zone name	S	late	Quickview
BareMetal-Host1	i-2-5-VM	Bar	Quickview:	BareMetal-Host1			+
			Display name	BareMetal-Host1			
			Name	BareMetal-Host1			
			State	Running			
			Template	BareMetal-RHEL	6-3-Template		
			Destroy Inst	3 Reboot ance	0	Take VM Snapshot	
			🗶 Destroy	C Reset VM	0,	Attach ISO	
			🔑 Reset Pas	sword 📑 Create ten	nplate 🕂	<ul> <li>Migrate to host</li> </ul>	
			Change se offering	ervice 🚬 View cons	ole		
			View Volumes	View Snapshots	View A	ffinity Groups	
			View Hosts	>			

- 6. Click **OK** to confirm destroy.
- 7. Uncheck Expunge check box



If **Expunge** is checked, the BareMetal-Host1 instance is deleted and cannot be restored.

Figure 339 Confirming Destroying BareMetal-Host1 Instance

n Instances							
Filter by All	V					▼ 🔍	+ Add Instance
Name	Internal name	Disp	lay name	Zone name		State	Quickview
BareMetal-Host1	i-2-1-VM	Bar	Quickview:	BareMetal-	Host1		+
			Display name	BareM	etal-Host1		
			Name	BareM	etal-Host1		
🕀 De	stroy Instance		-	Dunnin			
Please	e confirm that you v	want t	o destroy this	instance	-RHEL6-3-Ter		
	Expunge:				boot	Take VM Snapshot	
	Cancel		ОК		set VM sate template	<ul> <li>Attach ISO</li> <li>Migrate to host</li> </ul>	
			Change se offering	ervice 🚬	View console		
			View Volumes	View S	napshots	View Affinity Groups	
			View Hosts	6			

8. Instance BareMetal-Host1 destroyed.

ſ

#### Figure 340 Destroyed BareMetal-Host1 Instance

E	Notifications	Project: Default view	× •	admin cloud 🔻	Citri
Instances					
iter by All				v <mark>q</mark> [	Add Instanc
	Indexed as see	Display name	Zone name	State	
Name	Internal name	Display name	Zone name	State	Quickview

1

## Restore

- 1. Click the **Instances** tab.
- 2. Click Quickview icon on BareMetal-Host1.
- 3. Click Restore.

#### Figure 341 Restore BareMetal-Host1 Instance

A Instances							
Filter by All	~					⊽ 🔍	+ Add Instance
Name	Internal name	Disp	olay name	Zone name		State	Quickview
BareMetal-Host1	i-2-2-VM	Bar	Quickview:	BareMetal-Host	1		+
			Display name Name State Template X Expunge View Volumes View Hosts	BareMetal-Ho BareMetal-Ho Destroyed Restore Insta C Restor	nce -Temp e	olate ew Affinity Groups	

4. Click Yes to confirm restore on BareMetal-Host1.

		Ű.				
ame	Internal name	Disp	lay name	Zone name	State	Quickviev
areMetal-Host1	i-2-2-VM	Bar	Quickviev	v: BareMetal-Host1		+
			Display nan Name	ne BareMetal-Host1 BareMetal-Host1		
			State	Destroyed		
	Oconfirmation	16	_	areMetal-RHEL	.6-3-Template	
	Please confirm t	hat you instanc	want to rest			
	No	0	Ye	5 View Snapshots	View Affinity Groups	

#### Figure 342 Restore BareMetal-Host1 Instance Confirmation

- 5. Click stopped instance **BareMetal-Host1**.
- Figure 343 Stopped BareMetal-Host1 Instance

•	Notifications	Project: Default view	N 🔽 💽	admin cloud 🔻	<b>citrix</b> .
ñ Instances					
Filter by All	<b>~</b>			v <mark>q</mark>	Add Instance
Name	Internal name	Display name	Zone name	State	Quickview
BareMetal-Host1	i-2-2-VM	BareMetal-Host1	TenantA-BareMetal-Zone	Stopped	+

- 6. Click stopped instance **BareMetal-Host1**.
- 7. Click **Quickview** icon.
- 8. Click Start Instance.

ſ

ilter by All				v <b>Q</b>	+ Add Instance
Name	Internal name	Display name	Zone name	State	Quickview
BareMetal-Host1	i-2-2-VM	Bar Quickvie	w: BareMetal-Host1		+
		Display nar Name State Te Start In Start In	BareMetal-Host1 Stopped stance BareMetal-RHEL6-3-Te	emplate X Destroy	
		C Reset	Password Create template	<ul> <li>∅<sub>+</sub> Attach ISO</li> <li></li></ul>	
		View Volum View Host		View Affinity Groups	,

1

#### Figure 344 Start BareMetal-Host1 Instance

9. Running BareMetal Status after restore instance.

#### Figure 345 BareMetal-Host1 running status after Restore instance

iter by All	$\mathbf{\overline{\mathbf{v}}}$			V <b>Q</b>	+ Add Instan
2276763	Internal name	Display name	Zone name	State	Quickview
Name	internal fiame	Display name	Lono mano		

# Conclusion

Cisco and Citrix are both committed to providing superior cloud solutions to a global clientele. Together, products from both companies enable the flexible and agile delivery of cloud-based services with simplified physical and virtual infrastructure management. Many established enterprises have selected the combination of Cisco and Citrix offerings after analyzing best-in-class cloud products and have built robust and scalable enterprise clouds based on Cisco UCS and Citrix CloudPlatform. The reference architecture in this document further simplifies the deployment of these products by providing best practices for infrastructure and software configurations.

## References

I

Documents listed here provide additional information relevant to implementing Citrix Private Cloud with NetApp Storage System on Cisco UCS B-Series Servers.

- Cisco Nexus QoS Switch Configuration Guide: Cisco Nexus 5000 Series NX-OS SAN Switching Configuration Guide
- Cisco Nexus 5000 Series NX-OS SAN Switching Configuration Guide, Release 5.0(3)N2(1)
- Citrix CloudPlatform Installation and configuration Guides
- Cisco UCS System Hardware and Software Interoperability Matrix
- NetApp Storage Deployment Guide