

VMware Cloud Foundation Overview and Bring-Up Guide

VMware Cloud Foundation 2.3.1



vmware®

You can find the most up-to-date technical documentation on the VMware website at:

<https://docs.vmware.com/>

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2015 – 2018 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

	About the VMware Cloud Foundation Overview and Bring-Up Guide	5
1	About VMware Cloud Foundation	6
	Features and Benefits	7
	Private Cloud Deployment Options	9
	Cloud Foundation Use Cases	9
	Physical Topology	11
	Network Topology	13
	Storage Topology	13
2	Cloud Foundation Architecture	14
	Workload Domains	14
	Architecture Models	15
	Cloud Foundation Components	17
	SDDC Components of Cloud Foundation	19
3	Cloud Foundation Initial Bring-Up	21
	Collect Information Required for Bring-Up	22
	Connect First Rack to Your Power Source	25
	Initiate the Cloud Foundation Bring-Up Process on First Rack	26
	Change SDDC Manager Password	36
	Connect Rack to Corporate Network	37
	Copy Backup File to an Accessible Location	37
	Schedule Backup of Cloud Foundation Components	37
	Login to the SDDC Manager Dashboard	37
4	Adding a Rack to your Cloud Foundation System	39
	Connect Additional Rack to Inter-rack Switches	39
	Power on Additional Rack	40
	Add the Additional Rack to your Cloud Foundation System	40
5	Troubleshooting Cloud Foundation Deployment	42
	Manually Power On SDDC Manager VMs When Setting Up Your Cloud Foundation System	42
	Restart HMS	43
	Retry If Bring-Up Fails During NFS Datastore Creation	43
	Retry If Bring-Up Fails During NSX Power Up	43
6	Additional VMware Product Documentation	45

- 7** Example ToR Switch Output for L3 Configuration on Cisco ToR Switches (9372) 46
- 8** Cloud Foundation Glossary 50

About the VMware Cloud Foundation Overview and Bring-Up Guide

The *VMware Cloud Foundation Overview and Bring-Up Guide* provides an overview of the VMware Cloud Foundation product and its components and describes the steps for setting up and configuring a Cloud Foundation system.

Intended Audience

The *VMware Cloud Foundation Overview and Bring-Up Guide* is intended for data center cloud administrators who deploy a Cloud Foundation system in their organization's data center. The information in this guide is written for experienced data center cloud administrators who are familiar with:

- Concepts of virtualization and software-defined data centers
- Networking and concepts such as uplinks, NICs, and IP networks
- Hardware components such as top-of-rack (ToR) switches, inter-rack switches, servers with direct attached storage, cables, and power supplies
- Methods for setting up physical racks in your data center
- Using the VMware vSphere® Web Client™ to work with virtual machines

Related Publications

The *Administering VMware Cloud Foundation* contains detailed information about how to administer and operate a Cloud Foundation system in your data center.

Your Cloud Foundation system includes various VMware software products and components. You can find the documentation for those VMware software products at docs.vmware.com.

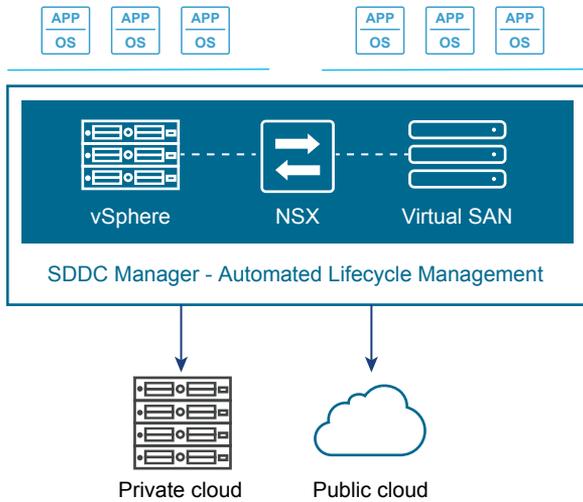
Cloud Foundation Glossary

The Cloud Foundation Glossary defines terms specific to Cloud Foundation.

About VMware Cloud Foundation

1

VMware Cloud Foundation is the unified SDDC platform that brings together vSphere, vSAN, and NSX into a natively integrated stack to deliver enterprise-ready cloud infrastructure for the private and public cloud.



The *VMware Cloud Foundation Overview and Bring-Up Guide* focuses on the private cloud use case.



Deploying VMware Cloud Foundation on qualified vSAN Ready Nodes.

(http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_deploy_cloud_foundation_hardware)

To manage the logical infrastructure in the private cloud, Cloud Foundation augments the VMware virtualization and management components with a new component, SDDC Manager. SDDC Manager is the interface for managing the infrastructure. From this interface, the IT administrator can provision new private cloud resources, monitor changes to the logical infrastructure, and manage lifecycle and other operational activities.

This chapter includes the following topics:

- [Features and Benefits](#)
- [Private Cloud Deployment Options](#)
- [Cloud Foundation Use Cases](#)
- [Physical Topology](#)

- [Network Topology](#)
- [Storage Topology](#)

Features and Benefits

In addition to the core features and capabilities provided by the individual components of the software stack, Cloud Foundation adds several unique capabilities.

Natively Integrated Software-Defined Stack

Cloud Foundation delivers a natively integrated software-defined data center stack that includes the core infrastructure virtualization, vSphere, vSAN and NSX. In addition, Cloud Foundation includes Cloud Foundation, which automates the entire system lifecycle (from initial bring-up, to configuration and provisioning, to upgrades and patching), and simplifies day-to-day management and operations. You can optionally deploy other software components such as VMware Horizon.

Automates Hardware and Software Bring-Up

Cloud Foundation automates the installation of the VMware software stack. Once the physical components have been installed in the rack, cabled, and powered on, SDDC Manager leverages its knowledge of the hardware bill of materials and user-provided environmental information (such as DNS, IP address pool, etc.) to configure the hardware components in the rack and deploy the SDDC software stack. Time savings varies by customer, but software installation time is estimated to be reduced from several weeks to as little as two hours due to the automation of certain previously manual functions. These include provisioning the management domain, including automated provisioning of networks, and allocation of resources based on service needs. When the process completes, you have a virtual infrastructure ready to start deploying vSphere clusters and provisioning workload domains.

Simplifies Resource Provisioning by Creating Workload Domains

Cloud Foundation introduces a new abstraction, workload domains, for creating logical pools across compute, storage, and networking. A workload domain is a policy based resource container with specific availability and performance attributes that combines vSphere, vSAN and NSX into a single consumable entity.

There are two types of workload domains - the management domain (contains the management components to manage the infrastructure) and compute workload domains.

Each workload domain provides the needed capacity with specified policies for performance, availability, and security. For example, a cloud administrator can create one workload domain for test workloads that have balanced performance and low availability requirements, while creating a separate workload domain for production workloads requiring high availability and high performance.

SDDC Manager automatically implements a deployment workflow to translate the workload domain specifications into the underlying pool of resources. Workload domains automate the provisioning of infrastructure in accordance with best practices, making it easy to achieve operational goals.

A workload domain can be created, expanded, and deleted as part of the SDDC lifecycle operations.

Automates Lifecycle Management

Data center upgrades and patch management are typically manual, repetitive tasks that are prone to configuration and implementation errors. Validation testing of software and hardware firmware to ensure interoperability among components when one component is patched or upgraded requires extensive quality assurance testing in staging environments. Often strapped for time, IT must sometimes make the difficult decision to deploy new patches before they are fully vetted or defer new patches, which slows down the roll-out of new feature or security and bug fixes. Both situations increase risk for the private cloud environment.

SDDC Manager automates upgrade and patch management for the SDDC software stack, thereby freeing resources to focus on business critical initiatives, while improving reliability and consistency.

Lifecycle management in SDDC Manager can be applied to the to the SDDC software stack or to individual workload domains, and is designed to be non-disruptive to tenant virtual machines (VMs). By utilizing live VM migration together with vSphere Dynamic Resource Scheduler (DRS), SDDC Manager can patch software to improve infrastructure security and reliability. VMware does extensive validation testing of the software stack prior to releasing software updates, which reduces risk and helps to instill confidence.

Integrates Management of Physical and Virtual Infrastructure

SDDC Manager understands the physical and logical topology of the software defined data center and the underlying components' relation to each other, and efficiently monitors the infrastructure to detect potential risks, degradations and failures. SDDC Manager provides stateful alert management to prevent notification spam on problem detection. Each notification includes a clear description of the problem and provides remediation actions needed to restore service. Degradations or failures are aggregated and correlated to workload domains to enable a clear view of the impact of any issue to the business services being deployed within a domain. Therefore, SDDC Manager can greatly reduce the mean time to resolution across organizational and technology silos.

Scalability and Performance

Cloud Foundation delivers a private cloud instance that can be easily deployed within an existing corporate network. Based on a scale-out, hyper-converged architecture, a Cloud Foundation implementation can start with a single rack containing four servers. Additional capacity and performance can easily be added linearly in increments as small as one server at a time within a single rack, scaling out to eight full racks containing 256 servers. Cloud Foundation adds the new capacity into the larger pool of available capacity for use.

Private Cloud Deployment Options

Cloud Foundation provides flexibility in choosing on-premises deployment options.

Customers begin by sizing their Cloud Foundation deployment to determine the number of physical servers in their rack. You then have two deployment options for Cloud Foundation

- Deploy the Cloud Foundation software on qualified vSAN ReadyNodes in your datacenter.

Customers can start with qualified hardware (qualified ReadyNodes and qualified switches) in their datacenter, wire it up, and deploy the Cloud Foundation software stack on the ready system. For information on qualified hardware, see [VMware Compatibility Guide](#).

- Purchase a fully integrated system that combines software and hardware from select VMware partners.

The partner works with a VMware representative to complete the Site Readiness document. This translates into a bill of materials (BoM) consisting of both hardware and software components. With this BoM in hand, the partner assembles the rack and images it. The partner then ships the system, consisting of physical racks, servers, server sub-components, power distribution units, switching infrastructure and the Cloud Foundation software, to customers.

Cloud Foundation Use Cases

Cloud Foundation includes two pre-packaged workload domain types, Virtual Infrastructure (VI) and Virtual Desktop Infrastructure (VDI). A workload domain is a policy based resource container with specific availability and performance attributes and combining vSphere, vSAN and NSX into single a consumable entity. The following sub-sections discuss how Cloud Foundation implements each of these workload domains.

Virtual Infrastructure

With Cloud Foundation, you have a complete solution to run your SDDC infrastructure. Cloud administrators have the ability to allocate and reclaim the underlying infrastructure to meet their changing business needs. With a cloud that is based on the market leading virtualization platform, lines of business have the flexibility to deploy a wide variety of operating systems and application stacks within the tenant VMs. Virtual infrastructure administrators can integrate with and monitor the underlying infrastructure using a common monitoring tool set that aggregates and correlates across physical and virtual infrastructure. In addition, you have the flexibility to integrate your vSphere compatible tools directly with vCenter Server.

VI configures a flexible virtual datacenter with the ability to deploy and configure OS instances in the form of VMs with vCPUs, memory, and storage including networking resources.

You can acquire modular Cloud Foundation units to match your consumers' data center capacity requirements and offer the resulting virtual infrastructure to your consumers with minimal overhead. SDDC Manager deploys the following for a VI workload:

- Physical compute

The administrator specifies the required capacity and SDDC Manager determines how many servers are needed and decides which servers use.

- Virtual infrastructure

One vCenter Server is deployed per workload domain, which connects to the Platform Services Controller in the management domain for credentials and licenses. SDDC Manager creates workload domains according to your specifications, adding hosts and creating vSAN datastores from the storage on those hosts. It also deploys and configures distributed virtual switches on each host.

- Physical networking

SDDC Manager configures the ToR switches to accept traffic for the VLANs created in the virtual infrastructure and to route traffic for the public logical networks of the workload domain.

- Log Aggregation

Cloud Foundation allows administrators to aggregate logs using vRealize Log Insight.

Virtual Desktop Infrastructure

With Cloud Foundation, you can deliver hosted desktops and applications through a single Virtual Desktop Infrastructure (VDI) platform with VMware VMware Horizon. End users can access all of their desktops and applications through a single unified workspace.

When deploying a VDI workload domain, Cloud Foundation automates the deployment and configuration of all required components. SDDC Manager performs the following tasks during a VDI workload domain creation:

- Physical compute

Hosts for the workload domain are selected from the hosts in the available inventory based upon the sizing requirements for the environment. Each host includes processing, storage, and network connectivity.

- Virtual infrastructure

One vCenter Server is deployed per workload domain, which connects to the Platform Services Controller in the management domain for credentials and licenses. The workload domain is created according your specifications, adding hosts and creating vSAN datastores from the storage on those hosts. Distributed virtual switches are deployed on each host.

- Physical networking

SDDC Manager uses the HMS to configure the switches to accept traffic for the VLANs created in the virtual infrastructure and to route traffic for the public logical networks of the workload domain.

- Log Aggregation

Cloud Foundation allows administrators to aggregate logs using vRealize Log Insight.

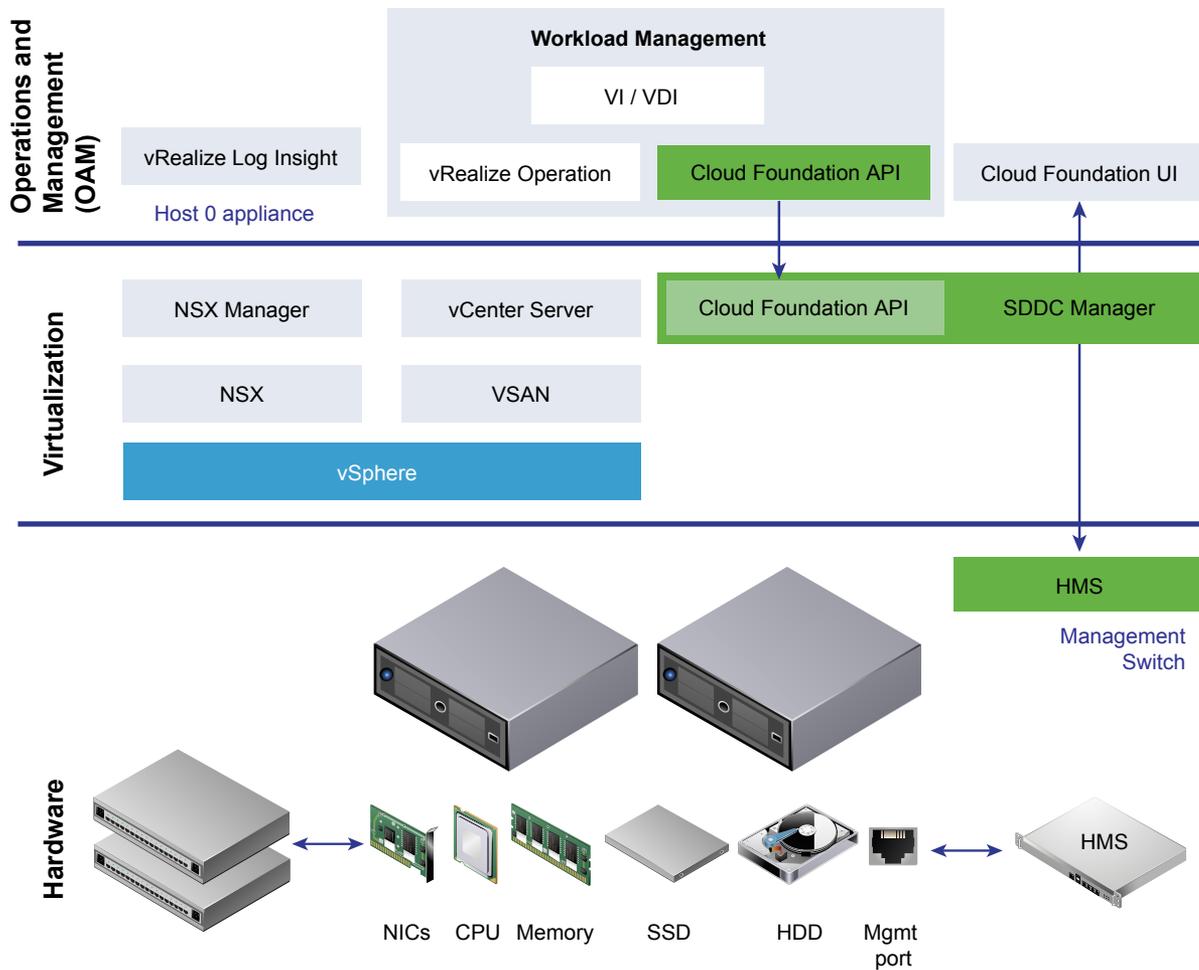
- VDI

VMware Horizon is bundled with Cloud Foundation and automates the deployment of View Connection Servers, security servers, App Volumes, Composer Server, and a DHCP Relay Agent. Cloud Foundation also creates an initial desktop pool.

Physical Topology

A Cloud Foundation system can include up to eight physical racks.

Figure 1-1. Physical Topology



Inter-rack Switches

The Cloud Foundation system contains two inter-rack switches. These switches extend the network fabric of the top of rack (ToR) switches between racks and are used for inter-rack connectivity only. The available uplink ports of the ToR switches are connected to the inter-rack switches.

Inter-rack switches are required only in multi-rack installations of Cloud Foundation and are typically placed in the second rack.

Management Switch

The management network fabric does not carry vSphere management, vSAN, or vMotion traffic. That traffic resides on the network fabric created by the ToR and inter-rack switches. Thus, the management switch is a non-redundant component in the physical rack. If this switch goes down, some functionality such as monitoring may not be available until it comes back up. Workloads will continue to run, but the infrastructure associated with them cannot be modified or controlled.

Top of Rack Switches

A physical rack contains two top of rack (ToR) switches. The ToR and inter-rack switches carry all network traffic from the servers including VM network, VM management, vSAN, and vMotion traffic. The ToR switches in the first rack carry all traffic to the enterprise network via two of the uplink ports. The ToR switches provide higher bandwidth as well as redundancy for continued operation in case one of them goes down.

If the installation has inter-rack switches, two uplink ports from each ToR switch on each rack are connected to each inter-rack switch.

Servers

A Cloud Foundation rack can contain 4 to 32 heterogeneous servers. Servers must be from the same vendor, but can be of different models and sizes with variable CPU, memory, storage size and type, and disk configurations (e.g. hybrid or all flash).

You can select the servers you want to use for the management domain as well as workload domains. This gives you the flexibility to use say hybrid servers for the management domain and all flash servers for workload domains.

For information on supported hardware, see [VMware Compatibility Guide](#).

Table 1-1. Server Configuration for Cloud Foundation

Component	Minimum	Maximum
CPU per server	Dual-socket, 8 cores per socket	Dual-socket, no maximum on cores per socket
Memory per server	256 GB	1.5 TB

Table 1-1. Server Configuration for Cloud Foundation (Continued)

Component	Minimum	Maximum
Storage per server	4 TB for capacity tier. Follow vSAN guidelines for cache tier sizing as described in VMware vSAN Design and Sizing Guide . Each server to be used in the domain must contain at least 3 capacity tier disks. Note Cloud Foundation only supports vSAN RAID controllers in pass-through mode.	8 disks per disk-group and 2 disk-groups per host. Follow vSAN guidelines for cache tier sizing as described in VMware vSAN Design and Sizing Guide .
NICs per server	Two 10 GbE NICs and one 1 GbE BMC NIC	Two 10 GbE NICs and one 1 GbE BMC NIC
Servers per rack	Four 1U or 2U servers A minimum of 7 servers are required for VI and VDI workload creation.	32 1U servers or 16 2U servers
Rack	1	8

Network Topology

Each host in the physical rack is connected to the two ToR switches with separate 10Gb links. On each host, NIC port 1 is connected to ToR switch 1 and NIC port 2 is connected to ToR switch 2 with Link Aggregation (LAG).

In a multi-rack system, both ToR switches are further connected to a pair of inter-rack switches in a dual-LAG configuration using 40 G links. The inter-rack switches are an aggregation layer for connecting multiple racks.

Cloud Foundation is designed to be resilient to certain network failures. The datapath between hosts and ToR switches can tolerate a failure of one link between the host and ToR switches. Between the ToR and inter-rack switches, the system can tolerate the failure of a ToR switch and/or inter-rack switch.

Storage Topology

The primary source of storage for Cloud Foundation is vSAN. For example, a 1U server can have 8 disks in the capacity tier and 2 disks in the caching tier. All disks are claimed by vSAN for storage.

The amount of available physical storage in workload domains depends on the number of physical hosts. The amount of usable capacity depends on availability requirements.

Storage traffic is carried over the 10Gbps links between the hosts and ToR switches. There is a dedicated vSAN port group defined on the vDS. All vSAN members communicate over this 10 Gbps network.

vSphere Network I/O Control (NIOC) can be enabled to allow network resource management to use network resource pools to prioritize network traffic by type.

Cloud Foundation Architecture

Cloud Foundation orchestrates, provisions, and deploys a software defined data center (SDDC). It maps a converged view of physical resources (e.g., CPU, memory, storage, and network) to a logical abstraction. Cloud Foundation overlays a software suite on top of the physical hardware for operations management, event reporting, and auditing. This enables Cloud Foundation to provide consistent hardware management across switches, servers, and storage, as well as a consolidated management solution across your SDDC.

In addition to the SDDC software stack, Cloud Foundation includes SDDC Manager, an application that automates the entire SDDC lifecycle (from initial bring-up, to configuration and provisioning, to upgrades and patching), and simplifies day-to-day management and operations. SDDC Manager offers a web-based interface.

This chapter includes the following topics:

- [Workload Domains](#)
- [Architecture Models](#)
- [Cloud Foundation Components](#)
- [SDDC Components of Cloud Foundation](#)

Workload Domains

A workload domain is a policy based resource container with specific availability and performance attributes that combines compute (vSphere), storage (vSAN) and networking (NSX) into a single consumable entity.

Management Domain

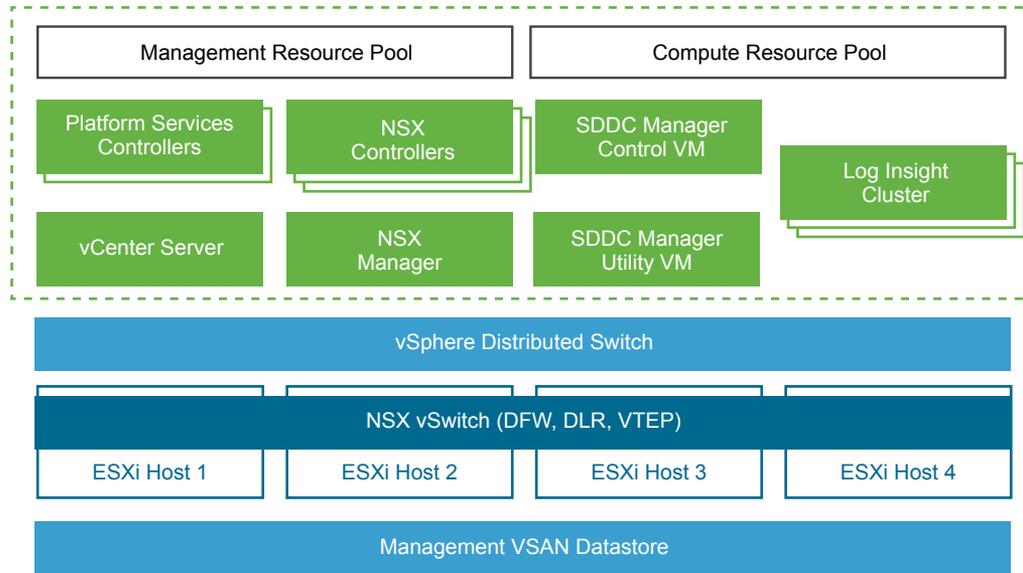
The management domain is a special-purpose workload domain dedicated to infrastructure and management tasks.

During bring-up, the management domain is automatically created on a four host vSAN cluster on the first rack in a Cloud Foundation system. It contains the following management components:

- SDDC Manager
- vCenter Server and Platform Services Controllers

- vRealize Log Insight
- NSX

Figure 2-1. Management Domain Components



Compute Workload Domains

Compute workload domains can be either VI or VDI, and are created on-demand by Cloud Foundation administrators. A compute workload is provisioned on a vSAN with a minimum of three hosts. Each workload domain is created according to user specified size, performance, and availability. For example, a cloud administrator can create one workload domain for test workloads that have balanced performance and low availability requirements, while creating a separate workload domain for production workloads requiring high availability and high performance.

A compute workload domains contains the following software components:

- vCenter Server
- NSX

In addition to the above components, VDI workload domains also contain VMware Horizon.

Architecture Models

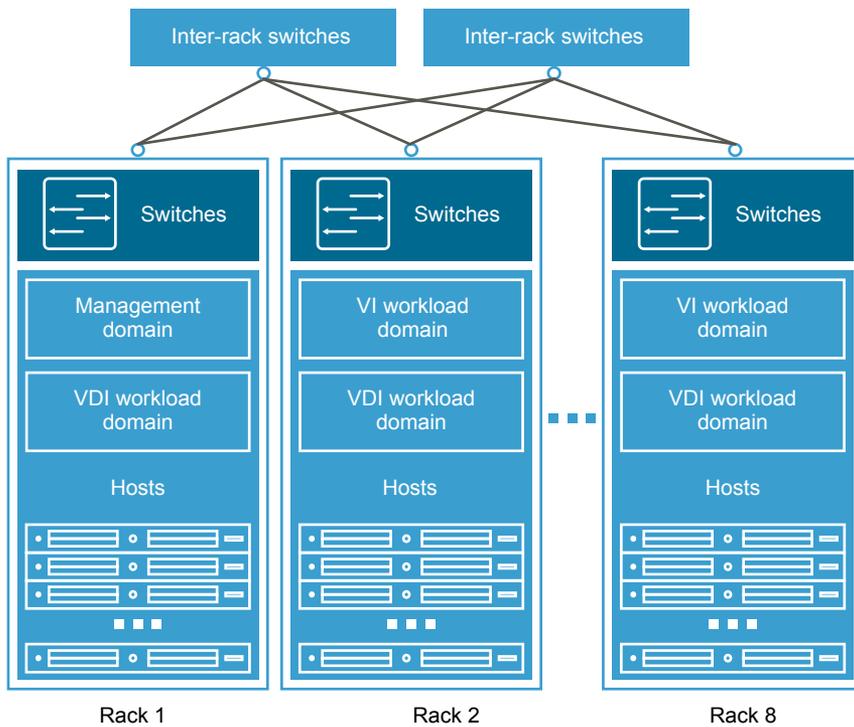
Cloud Foundation supports two architecture models. The architecture model used for your deployment is determined by the number of hosts in your rack.

Standard Architecture Model

When you deploy Cloud Foundation on seven or more hosts, the deployment is based on the standard architecture. A dedicated management domain on the first rack hosts the management components of the SDDC software stack. The remaining capacity in the Cloud Foundation is used for user-created workload domains or for expansion of the management domain. Thus, there is a separation between the infrastructure domains and user-created workload domains.

Standard architecture is recommended for Cloud Foundation deployments.

Figure 2-2. Example Standard Architecture

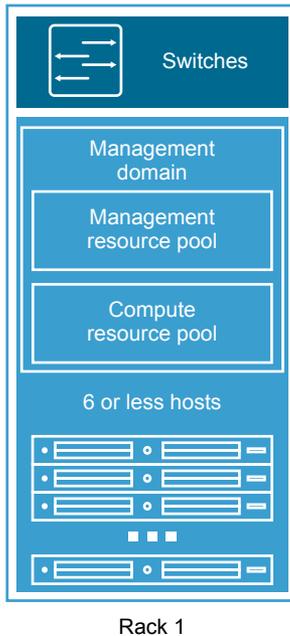


Consolidated Architecture Model

When you deploy Cloud Foundation on six or fewer hosts, deployment is based on the consolidated architecture. In this model, both the infrastructure and compute workload domains run a shared vSphere cluster. Resource pools provide isolation for the different workload types.

As you add additional hosts to a Cloud Foundation system deployed on a consolidated architecture, you can convert to the standard architecture by creating a compute workload domain outside the management domain and moving the workload domain VMs from the compute resource pool to the newly created workload domain. When moving these VMs, you must update shares and reservations on the compute resource pool.

Figure 2-3. Sample Consolidated Architecture



Cloud Foundation Components

VIA

VIA is a virtual appliance used to image the first rack, additional racks, and individual servers. During imaging, VIA pre-configures the SDDC software stack on the rack. For more information, see *VIA User's Guide*.

SDDC Manager

SDDC Manager manages the bring-up of the Cloud Foundation system, creates and manages workload domains, and performs lifecycle management to ensure the software components remain up-to-to date. SDDC Manager also monitors the logical and physical resources of Cloud Foundation.

As you expand your Cloud Foundation system by adding hosts or racks, SDDC Manager allows data center administrators to configure the additional hosts and racks into a logical pool of resources. This consolidates compute, storage, and networking resources of the racks available for assignment to workload domains. Thus, multiple racks can be managed as a single Cloud Foundation system.

SDDC Manager controls these processes by using workflows. Each workflow comprises of a series of tasks, which are executed by SDDC Manager. By doing so, SDDC Manager ensures that if any high level task such as bring-up or upgrade fails, it can identify the exact point of failure, and continue the process from that point onward.

SDDC Manager VMs contain multiple services, each responsible for the different APIs providing lifecycle management for the SDDC.

SDDC Manager Controller VM

The SDDC Manager Controller VM includes the logic for deploying the software stack, managing workload domains, managing hardware tasks, and performing lifecycle management. It provides a persistent data store.

Bring-Up Service

The bring-up service deploys the SDDC software stack on your physical rack. It creates the management domain on the first rack in a Cloud Foundation system. A resource pool is created on the management domain which can contain user-created workload domain VMs.

Manager Service

The Manager Service manages the SDDC stack. It creates, expands, and deletes workload domains according to your specifications.

LCM Service

LCM service performs lifecycle management on the Cloud Foundation software as well as the VMware software components included in the SDDC software stack.

System Controller Service

The System Controller Service starts the other SDDC Manager services and also re-starts them when necessary.

Events Engine

The events engine pushes SDDC Manager events to vRealize Log Insight. The events engine process can also display events information on the SDDC Manager UI dashboard.

Hardware Management Services

The Hardware Management Services (HMS) manages the hardware in the Cloud Foundation system, such as hosts and network switches. It provides the necessary functions required for discovering, bootstrapping, and monitoring the hardware. HMS runs on the SDDC Manager Controller VM, where it can access all hosts and switches on the out-of-band network.

HMS works with both vendor-provided plug-ins and VMware plug-ins, and gives the SDDC Manager the capability to interact with the hardware. The HMS is only accessed through the SDDC Manager and is not visible to system administrators.

SDDC Manager Utility VM

The SDDC Manager Utility VM contains the downloaded LCM update bundles, as well host-level and NSX backup files.

SDDC Components of Cloud Foundation

This section describes how the SDDC software components work within a Cloud Foundation system.

ESXi

ESXi is a type 1 hypervisor used to implement virtualization on bare metal systems. ESXi provides for compute virtualization within the software-defined data center and is a foundational building block for implementing a private cloud.

Cloud Foundation uses ESXi as the foundation for creating workload domains. SDDC Manager groups hosts into vSphere clusters managed by vCenter Server. vSphere HA provides high availability to protect against ESXi host failures.

vCenter Server

vCenter Server provides for management of a VMware virtualized environment with one or more ESXi hosts. SDDC Manager deploys one vCenter Server per workload domain. By default, all vCenter Servers are configured in enhanced linked mode.

Platform Services Controllers

During bring-up, SDDC Manager deploys two Platform Services Controllers in the management domain. These instantiate an SSO domain. All vCenter Servers (management domain and compute workload domains) are registered with the SSO domain and configured in enhanced link mode.

vSAN

vSAN provides storage systems for the SDDC. It pools together local flash devices and/or hard disks to provide a highly resilient shared datastore suitable for a variety of workload domains including business-critical applications, virtual desktops, remote IT, DR, and DevOps infrastructure.

In Cloud Foundation, each workload domain contains one vSphere cluster. The SDDC Manager creates a single vSAN volume spanning all the hosts within each vSphere cluster. It is recommended that you use a minimum of four hosts per workload domain for vSAN.

In an all flash vSAN environment, you must mark flash devices to be used for capacity layer as capacity disks. See the *Administering VMware Cloud Foundation* guide for more information.

NSX

NSX is the network virtualization platform for the SDDC, delivering the operational model of a virtual machine for entire networks. With NSX, network functions including switching, routing, and firewalling are embedded in the hypervisor and distributed across the environment.

NSX comprises of one NSX Manager and three Controllers. NSX Manager maps to a single vCenter Server environment. Therefore, each workload domain includes one NSX Manager instance and three NSX Controller instances.

Data center administrators can use the vSphere Web Client to perform additional NSX configuration required by the specific VMs deployed within the workload domain.

vRealize Log Insight

vRealize Log Insight delivers heterogeneous and highly scalable log management with intuitive, actionable dashboards, sophisticated analytics and broad third-party extensibility, providing deep operational visibility and faster troubleshooting.

Cloud Foundation configures vRealize Log Insight on the management domain in a three node cluster. With vRealize Log Insight, administrators can monitor logs for both the physical and virtual components through a single interface. The default vRealize Log Insight license covers the management domain. You need to provide an additional license for using vRealize Log Insight with workload domains.

Cloud Foundation Initial Bring-Up

3

The initial configuration of a newly deployed Cloud Foundation rack is called bring-up.

During bring-up, the system creates a management cluster and deploys the core management component VMs in the management cluster. You can then create workload domains on your Cloud Foundation system.

The physical rack must contain at least four hosts for bring-up. These are used to create the management domain, which can also be used to host user provided workload domains. To create another workload domain in addition to the initial management domain, another three hosts are required.

The bring-up process involves several steps. If you have multiple racks in your Cloud Foundation system, you must complete bring-up on rack 1 before configuring the remaining racks.

Prerequisites

Verify that you have met the following prerequisites.

- You have an imaged rack (where SDDC software is pre-configured on the rack) with the appropriate number of hosts.
- You have a laptop with a supported web browser, from where you will run the bring-up process. For a list of supported browser versions, see the *VMware Cloud Foundation Release Notes*.

Procedure

1 [Collect Information Required for Bring-Up](#)

During the bring-up process, you are required to provide company domain, management network, and vSAN, VXLAN, vMotion, data center network settings. You must collect this information before starting the bring-up process.

2 [Connect First Rack to Your Power Source](#)

Power on the first rack.

3 [Initiate the Cloud Foundation Bring-Up Process on First Rack](#)

After you provide site specific information for the bring-up process such as rack name, passwords, IP addresses, and DNS and NTP details, SDDC Manager configures your private cloud.

4 [Change SDDC Manager Password](#)

During imaging, the SDDC Manager password is set to `vmware1234`. This is the password used during initial bring-up. For security reasons, you must change this password before connecting the rack to your corporate network.

5 [Connect Rack to Corporate Network](#)

You can now connect the Cloud Foundation rack to your corporate network.

6 [Copy Backup File to an Accessible Location](#)

Copy the files of the backup taken during bring-up to an accessible location.

7 [Schedule Backup of Cloud Foundation Components](#)

Schedule a periodic backup for your Cloud Foundation environment.

8 [Login to the SDDC Manager Dashboard](#)

Collect Information Required for Bring-Up

During the bring-up process, you are required to provide company domain, management network, and vSAN, VXLAN, vMotion, data center network settings. You must collect this information before starting the bring-up process.

Table 3-1. Description of Networks

Title	Description
Management network	Network that provides public access to Cloud Foundation components in the management domain.
vMotion network	Network for vMotion across hosts.
vSAN network	Network for vSAN and vSphere HA inter-host communication.
VXLAN network	Network for internal communication between Cloud Foundation management components.
Data center network	Network used to access customer VMs from your corporate network.

VMware recommends that you print this table and fill in the required values. Keep this printout handy during the bring-up process.

Table 3-2. Information Required for Bring-Up

Category	Information Required	Example
Rack Details	Physical Rack name	ABC
	Rack names allow you to map the IDs SDDC Manager assigns to a host or a switch with the physical rack containing the host or switch. You need to specify the rack name during bring-up and while adding a rack. A best practice is to specify the name affixed to the physical rack along with location details such as the datacenter the rack is located in.	
	Company name	MyCompany
	Company Department	My department
	Root DNS Domain	mycompany.local
	Must be the same as the domain defined in DNS naming system.	
	Cloud Foundation Sub-domain	vcf01-domain.mycompany.local
Each Cloud Foundation system must have a unique sub-domain.		
	SSO Domain	mycompany.local
	VMware Cloud Foundation License Key	11111-11111-1111-111111-11111
Management Network	VLAN ID	24
vMotion Network	Supported VLAN range is 24-3967.	
vSAN Network	Subnet	10.0.24.0
	Subnet Mask	255.255.252.0
	Gateway	10.0.24.1
	Primary DNS (management network only)	10.172.40.1
	Secondary DNS (management network only)	10.172.40.2
	NTP (management network only)	10.172.40.100
	Exclude IP Address Ranges (Optional) If you have already used a set of IP addresses in your data center or do not want to use certain IP addresses, you can exclude them from Cloud Foundation provisioning.	
VXLAN Network	VLAN ID	102
	Supported VLAN range is 24-3967.	
	Subnet	10.0.102.0

Table 3-2. Information Required for Bring-Up (Continued)

Category	Information Required	Example
	<p>Subnet Mask</p> <p>If you intend to specify a large IP subnet mask (for example, /22) for VXLAN during the bring-up phase of installation and subsequently to be used for new VI/VDI workload domain configurations, the following recommendations apply.</p> <ul style="list-style-type: none"> Cloud Foundation uses the NSX Unicast Replication mode by default, which may result in ESXi host overhead when a high number of ESXi hosts belong to a single subnet. VXLAN ESXi host overhead also depends on the amount of multi-destination broadcast, unknown unicast, and multicast (BUM) traffic. High ESXi host overhead may result if, in a subsequent workload domain configuration, the number of VTEP IP addresses exceeds the number supported by the subnet mask in a single IP subnet/VLAN. To avoid high ESXi host overhead, it is recommended that you use a dedicated IP subnet/VLAN for VXLAN for each VI/VDI workload domain. <p>For more information about the NSX Unicast Replication mode, see Add a Transport Zone in the NSX product documentation.</p>	255.255.252.128
	Gateway	10.0.102.1
	<p>Exclude IP Address Ranges (Optional)</p> <p>If you have already used a set of IP addresses in your data center or do not want to use certain IP addresses, you can exclude them from Cloud Foundation provisioning.</p>	
Data Center Network	VLAN ID	225
	Supported VLAN range is 24-3967.	
	Subnet	10.0.225.0
	Subnet Mask	255.255.252.224
	Gateway	10.0.225.1
	<p>Exclude IP Address Ranges (Optional)</p> <p>If you have already used a set of IP addresses in your data center or do not want to use certain IP addresses, you can exclude them from Cloud Foundation provisioning.</p>	
Data Center Uplink	Uplink Type	L2
	Choose L2 or L3. If you choose L3, you will also need the upstream router (next hop) information.	
	Uplink LAG	Yes
	Enable or disable uplink LAG (Link Aggregation Group). LAG aggregates multiple links into a single bundle. You can enable this option if the speeds on the ports in your environment match. For example, if you have 4 uplink ports at 10G, you can get up to 40G with LAG enabled.	

Table 3-2. Information Required for Bring-Up (Continued)

Category	Information Required	Example
	Uplink Ports For 10 Gb ports, specify 43 to 46. For 40 Gb ports, specify 51 to 54.	43, 44
	Uplink speed Specify 1 G, 10 G, or 40 G	10 G

Connect First Rack to Your Power Source

Power on the first rack.

Note Do not connect the rack to your corporate network till after the bring-up process is complete.

Procedure

- 1 Connect the rack's power inlets to your power source.
- 2 Connect port 48 of the first rack's management switch to the laptop from where you will run the bring-up process.
- 3 Configure the laptop NIC to tag VLAN traffic.
- 4 Create a trunked interface on the laptop.
 - a Assign the 192.168.100.248/22 IP address/subnet mask to the untagged interface. The untagged interface will allow private network access to Cloud Foundation hardware and Software components
 - b Tag interface 2 with the management VLAN ID (refer to the table where you had noted these details) and assign an IP address/subnet mask from the upper end of the management network IP address pool used for management workload domains.

This interface will allow for hardware access to the system if there is an uplink mis-configuration and the system is unreachable from the upstream customer network.

What to do next

- 1 Ping the SDDC Manager Controller VM at 192.168.100.40. If you are unable to ping the VM, contact VMware support.
- 2 Open the browser on the laptop and navigate to <http://192.168.100.40:8008/login>. If the browser does not display the setup wizard, the SDDC Manager VMs might not be powered on. Verify whether they are running and, if not, power them on as described in [Manually Power On SDDC Manager VMs When Setting Up Your Cloud Foundation System](#).

Continue with the steps in [Initiate the Cloud Foundation Bring-Up Process on First Rack](#).

Initiate the Cloud Foundation Bring-Up Process on First Rack

After you provide site specific information for the bring-up process such as rack name, passwords, IP addresses, and DNS and NTP details, SDDC Manager configures your private cloud.

If you accidentally log out of the browser while the configuration process is running, the process continues to progress. You can log back in to continue the configuration.

Prerequisites

- 1 Ensure that you have completed the steps in [Connect First Rack to Your Power Source](#).
- 2 Either turn off the firewall on the jump host or ensure that the firewall ports required to access Cloud Foundation are open.

Table 3-3. Inbound Ports for Cloud Foundation

Port	Required for
TCP 8443	SDDC Manager
TCP/UDP 53	DNS resolution to SDDC Manager
TCP 22 (optional)	SSH access to Cloud Foundation and vSphere components

Table 3-4. Outbound Ports for Cloud Foundation

Port	Required for
TCP/UDP 53	Corporate DNS resolution
UDP 123	NTP access to corporate time servers

In addition, other VMware software included in Cloud Foundation may require additional firewall ports to be open.

Login to Cloud Foundation

You begin by logging in to the wizard.

Procedure

- 1 After you power on the rack, wait at least 10 minutes before proceeding to the next step. This ensures that all rack components are powered on.
- 2 In a web browser on the laptop that is connected to port 48 of the rack's management switch, navigate to `https://192.168.100.40:8008/login`.

The Welcome page appears.

- 3 Type the default credentials:

User name: `administrator@vsphere.local`

Password: `vmware1234`

- 4 Click **LOG IN** and then click **START BRING-UP**.

The VMware Cloud Foundation page appears.

Rack Discovery

During the rack discovery phase of the bring-up process, the system communicates with the servers and switches.

If the servers are available and the switches can be accessed, the physical inventory is populated. When this is completed, a green check mark appears next to Rack Discovery on the Welcome page and the Continue button on the bottom of the page is enabled.

- Click **CONTINUE**.

If a hardware issue is detected, you must fix it and click **Re-try**.

Set System Date and Time

After the hardware components on the physical rack have been discovered, you set the date and time for the rack. The specified time is set on all operational hosts, switches, and the SDDC Manager VM.

Procedure

- 1 Select the date on the calendar.

- 2 Set the time.

The specified time should match the current time in your environment.

- 3 Select the time zone for the rack.

- 4 Click **SET TIME**.

The page displays the progress of the set time task. If time set fails on any component other than SDDC Manager VMs, you can either re-try this task or proceed with the rest of the workflow. Time is synced later during the bring-up workflow.

If time set on the SDDC Manager VMs fails, you must retry setting the time. If the retry fails, reboot the SDDC Manager VMs and retry the time set task.

After the time has been set on all Cloud Foundation components, the **CONTINUE** button is enabled.

- 5 Click **CONTINUE**.

The Power On System Validation page is displayed.

Power On System (POSV) Validation

Power On System Validation applies a set of pre-defined rules to assess whether bootstrapping can be started on the rack. Alerts related to hardware issues are displayed so that you can fix the problems before bootstrapping begins. You must ensure that the hardware is healthy before bring-up begins. The bring-up service will skip hosts that cannot be configured.

The status bar on the Power On System Validation page displays the task progress. The Tasks tab displays the date and time that each validation task was performed. After the validation is complete, the Continue button is enabled.

Alert notifications are also displayed here. The Alerts tab displays alert severity and remediation details. You can download or print the task or alert list. After you fix the issue reported by an alert, click **Resolve**. If you cannot take the remediation steps displayed on the alert, you can continue bring-up. Hosts with issues are not configured during bring-up.

Procedure

- 1 Click **CONTINUE**.

If POSV fails, take the necessary action and click **Retry**.

- 2 Click **START DEPLOYMENT**.

Select Hosts for Management Domain

The Host Selection page displays hosts that are suitable for the management domain (healthy hosts that the system can access via SSH).

The primary host (host that contains the management VMs) is selected by default. The page displays hosts that have the same disk type as the primary host (all Flash or hybrid). Though you can add unbalanced hosts (with varying CPU, memory, and storage) to the management domain, it is recommended that you add hosts that have similar processor, memory, storage, and disk types for optimum performance.

Prerequisites

When selecting a host, verify it is healthy by running the SoS health check command. See [Supportability and Serviceability \(SoS\) Tool](#).

Procedure

- 1 Select 3 hosts for the management domain.

The UI displays a notification if you select unbalanced hosts that can potentially affect performance.

- 2 Click **CONTINUE**.

Initial Setup

During initial setup, the rack is bootstrapped and the management cluster is created. The management cluster contains the management component VMs. The remaining hosts in the physical rack are configured for Cloud Foundation.

Accept End User License Agreement (EULA)

Displays EULA for Cloud Foundation.

Procedure

- 1 Read the EULA and accept it.
- 2 Click **NEXT**.

Join Customer Experience Improvement Program

Cloud Foundation participates in VMware's Customer Experience Improvement Program ("CEIP"). When you choose to participate in the Customer Experience Improvement Program (CEIP), VMware receives anonymous information to improve the quality, reliability, and functionality of VMware products and services.

Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at <http://www.vmware.com/trustvmware/ceip.html>.

Procedure

- 1 The **Join the VMware Customer Experience Improvement Program** checkbox is selected by default. If you do not want to join the program, un-select the checkbox.
- 2 Click **Next**.

Create Super User for SDDC Manager Dashboard

You create a super user account to manage the vSphere infrastructure. The super user account has the same privileges as the administrator@vsphere.local account. After the bring-up process is complete, the password for the administrator@vsphere.local account is rotated to a random password, but the password for the super user account does not change. You can, thus, login to SDDC Manager with the super user name and password without having to look up the rotated password for the administrator account.

Procedure

- 1 Type a user name and password for the super user.

The password must be between 8 and 20 characters long and must contain at least one each of the following:

- lowercase letter
- uppercase letter
- number
- special character. Supported special characters are !, %, \$, and ^.

- 2 Click **NEXT**.

Specify Rack and Company Domain Details

Specify information about the physical rack and company domain.

Procedure

- 1 On the General information page, enter the following information.

Field Name	Description
Physical Rack Name	Name by which the physical rack is to be identified Rack names allow you to map the IDs SDDC Manager assigns to a host or a switch with the physical rack containing the host or switch. A best practice is to specify the name affixed to the physical rack along with location details such as the datacenter the rack is located in.
Company Name	Your company name
Company Department	Your department name
Root DNS Domain	Type your root DNS domain (for example, vmware.corp). Must be the same as the domain defined in DNS naming system.
VMware Cloud Foundation Sub-Domain	Cloud Foundation generates this based on the root domain you specified. For example, if you specified the root domain as vmware.corp, the subdomain is auto-populated as subdomain.vmware.corp. You can edit this field. The Cloud Foundation sub-domain must be unique in your organization, otherwise there will be issues when you join Active Directory. The sub-domain is used for all components in Cloud Foundation. So everything is named <i>component.subdomain</i> . Based on our example, the NSX VM would be named rack-1-nsxmanager-1.subdomain.vmware.corp.
SSO Domain	Type the authentication domain to be used by SSO. For example, vsphere.local. The root domain and PSC domain must be different if you plan to join Active Directory. If you will not join Active Directory, they can be the same.
VMware Cloud Foundation License Key	Optionally, type the license key for Cloud Foundation.

- 2 Click **NEXT**.

Specify Management Network Details

Specify network information such as the VLAN identifier and IP subnets for the management, vMotion, vSAN, and VXLAN networks. The VLAN IDs you specify here are configured on the physical switch infrastructure.

Procedure

- 1 On the Management page, enter your management network values. The DNS server here is the DNS server for your management network.

Field Name	Description
VLAN ID	The supported VLAN range is 24-3967.
Subnet	VMware recommends using a /22 network. This is to allow for adequate IP address capacity as you expand your Cloud Foundation deployment by adding racks.
Subnet Mask	VMware recommends using a /22 network.
Gateway	Gateway address.

Field Name	Description
Primary DNS	Primary DNS of your datacenter.
Secondary DNS	Secondary DNS of your datacenter.
NTP	NTP of your datacenter.
Exclude IP Address Ranges	Enter a set of IP address ranges to exclude from the provisioning process. For example, you can exclude a range of IP addresses that you want reserved for other uses in your network. To add multiple address ranges, type an IP address range, click the + sign, and type the next IP address range.

- 2 Click **USE DEFAULTS** to allow Cloud Foundation to specify system generated IP address ranges for vMotion, vSAN, and VXLAN.
- 3 Click **NEXT**.

Specify vMotion Network Settings

If you are using default values, review the system's vMotion network details. Otherwise, specify vMotion network values.

Procedure

- ◆ Review or enter your network addresses for VLAN ID, Subnet, Subnet Mask, Gateway, and excluded IP addresses and IP address ranges.

Note The supported VLAN range is 24-3967. VMware recommends using a /22 network for the subnet and subnet mask. This is to allow for adequate IP address capacity as you expand your Cloud Foundation deployment by adding racks.

Specify vSAN Network Settings

If you are using default values, review the system's vSAN network details. Otherwise, specify vSAN network values.

Procedure

- ◆ On the vSAN Network page, review or enter your vSAN network addresses for the VLAN, Subnet, Subnet Mask, Gateway, and excluded IP address ranges.

Note The supported VLAN range is 24-3967. The subnet and subnet mask must be at least a /22 network. This is to allow for adequate IP address capacity as you expand your Cloud Foundation deployment by adding racks.

Specify VXLAN Network Settings

If you are using default values, review the system's VXLAN network details. Otherwise, specify VXLAN network values.

Procedure

- ◆ On the VXLAN Network page, review or enter your VXLAN network addresses for the VLAN, Subnet, Subnet Mask, Gateway, and excluded IP address ranges.

Note The supported VLAN range is 24-3967. The subnet and subnet mask must be at least a /22 network. This is to allow for adequate IP address capacity as you expand your Cloud Foundation deployment by adding racks.

Specify Datacenter Network Settings

Specify the network settings to connect the Cloud Foundation system to your corporate network.

Procedure

- 1 Type the VLAN ID, Subnet, Subnet Mask, and Gateway for your corporate network.

Note The subnet and subnet mask must be set to /22 or /24.

- 2 Click **NEXT**.

Specify Datacenter Uplink Details

Specify data center uplink information. The uplink is enabled for management and data center networks.

Procedure

- 1 If the uplink is an L2 connection, provide the following information.

Field	Description
Uplink Type	L2
Uplink LAG Enabled	It is recommended that you select this option.
Uplink Ports	Port numbers on the ToR switches that are connected to the uplink network. Enter a value ranging from 43 to 46. If entering multiple values, separate them with a comma. For example, 45,46 .
Uplink Speed	Speed for uplink connections.

Ensure that the management and external VLANs from Cloud Foundation are routable upstream.

- 2 If the uplink is an L3 connection, provide the following information.

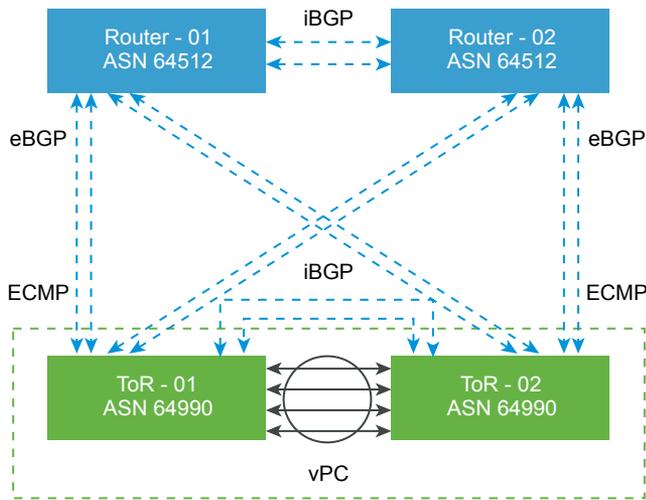
Field	Description
Uplink Type	L3
Uplink LAG Enabled	LAG (Link Aggregation Group) aggregates multiple links into a single bundle. You can enable this option if the speeds on the ports in your environment match. For example, if you have 4 uplink ports at 10G, you can get up to 40G with LAG enabled.
Uplink Ports	Port numbers on the ToR switches that are connected to the uplink network. Enter a value ranging from 51 to 54.
Uplink Speed	Speed for uplink connections.

Field	Description
Uplink IP	IP address of the uplink IP on the ToR switches.
Mask IP	Subnet mask for the uplink IP.
Next Hop IP	IP address of the uplink switch for the data center.

For an L3 uplink, SDDC Manager configures a Switched VLAN Interface (SVI) for each requested VLAN and configures a static route between ToR 1 and the upstream router. The configured SVI and the configuration between the ToR and router is non-HA. You need set up a method to route traffic across the internet. This not automated during bring-up.

You can set up iBGP between the ToR switches and an eBGP between each ToR switch and the upstream router. For information on the required configuration, see [Chapter 7 Example ToR Switch Output for L3 Configuration on Cisco ToR Switches \(9372\)](#).

Figure 3-1. L3 Configuration



3 Click **NEXT**.

Review Configuration Details

Review the configuration details carefully.

Procedure

- 1 On the Review page, review the configuration details carefully. You cannot make any changes after you submit this information.
- 2 Click **FINISH**.

View SDDC Deployment Status

You can see the tasks being completed as the SDDC components are deployed and configured.

Procedure

- ◆ Click **FINISH**.

The system configuration for Cloud Foundation begins. During this process, the following tasks are completed.

- Non-routable IP addresses of all hosts in the rack are reconfigured and the changed IP addresses are updated in the physical inventory.
- ESXi bootbank and state files are backed up.
- PSC, vSphere, vSAN, vRealize Log Insight, and NSX components are deployed.
- The management domain is created, which contains the SDDC Manager, all vCenter Servers, and NSX Managers and Controllers. Hosts that are not in the management cluster are configured for Cloud Foundation as well.
- Each component in the rack is assigned a unique password.

You can search for a task and can also download and print the task list.

The amount of time it takes for the bring up process to be completed depends on the number of servers in the physical rack.

After bring-up is successful, the **SEE IP ALLOCATION** button is enabled.

Dealing with Errors During Bring-Up

During bring-up, SDDC Manager does not configure hosts that are not healthy. You can either fix the corresponding hardware issue and re-try bring-up, or skip these hosts from the bring-up process. You cannot skip a host selected for the management domain.

Hosts with the following alerts are considered not healthy:

- CPU_CAT_FAILURE_ALERT
- CPU_INITIALIZATION_ERROR_ALERT
- CPU_POST_FAILURE_ALERT
- CPU_MACHINE_CHECK_ERROR_ALERT
- CPU_THERMAL_TRIP_ERROR_ALERT
- DIMM_ECC_MEMORY_ERROR_ALERT
- DIMM_THERMAL_TRIP_ALERT
- HDD_DOWN_ALERT
- HDD_EXCESSIVE_WRITE_ERRORS_ALERT
- HDD_WEAROUT_ABOVE_THRESHOLD_ALERT
- HOST_AGENT_NOT_ALIVE_ALERT
- NIC_PORT_DOWN_ALERT

- NIC_PORT_DOWN_ALERT – one of the TOR facing NIC port is down
- SERVER_DOWN_ALERT
- SERVER_PCIE_ERROR_ALERT
- SERVER_POST_ERROR_ALERT
- SSD_DOWN_ALERT
- SSD_EXCESSIVE_READ_ERRORS_ALERT
- SSD_EXCESSIVE_WRITE_ERRORS_ALERT
- SSD_WEAROUT_ABOVE_THRESHOLD_ALERT
- STORAGE_CONTROLLER_DOWN_ALERT

For a description of these alerts, see *Administering VMware Cloud Foundation*. After you resolve an issue, you must clear the corresponding alert. Cloud Foundation does not automatically clear alerts.

Follow the steps below if you see an error during bring-up.

- 1 If a hardware problem is detected, fix the issue. If you see an alert during bring-up that indicates a host is ineligible for configuration, you can skip that host during the bring-up process. After bring-up, you must either repair the faulty host or expand the management domain with one of the successfully configured hosts.
 - a Log in to the SDDC Manager Controller VM with your root credentials.
 - b Run the following script.

```

root@sddc-manager [ /opt/vmware/bringup/webapps/bringup-app/lib ]#
/home/vrack/bin/mark-hosts-ineligible-for-bootstrap.sh
2017-05-17 18:00:58 -----
2017-05-17 18:00:58 Usage:
2017-05-17 18:00:58 /home/vrack/bin/mark-hosts-ineligible-for-bootstrap.sh \
--host-ids=<Host ID(s) separated by comma>
2017-05-17 18:00:58 Example:
2017-05-17 18:00:58 /home/vrack/bin/mark-hosts-ineligible-for-bootstrap.sh \
--host-ids="R1N1,R1N2,R2N5"

```

After bring-up is complete, you can either replace the faulty component or the host.

- 2 click **RETRY**.

The configuration process remembers where it was in the sequence and start over from that point.

- 3 If an error occurs even after you rerun, contact VMware Support.

View IP Addresses and Configure DNS Delegation

The Component IP Allocation page displays IP addresses for VMs that will be deployed for the NSX, Platform Services Controller, SDDC Manager, and vCenter Server software components.

Procedure

- 1 Click **SEE IP ALLOCATION**.
- 2 Note the IP addresses of the component VMs.
- 3 Configure DNS delegation for automatic resolution of all names in Cloud Foundation.

SDDC Manager uses Unbound (a DNS server software) for name resolution during the Cloud Foundation bring-up. You must now configure the corporate DNS server to delegate zone control for the Cloud Foundation domain to SDDC Manager.

For example, if your corporate domain is vmware.corp, and the Cloud Foundation Sub Domain is subdomain. vmware.corp, the corporate DNS server must be configured to delegate control of subdomain.vmware.corp to SDDC Manager.

- a Install DNS on your server by adding a new role through Server Manager and selecting DNS.
- b Ensure that your jump server uses the local DNS for name resolution.
- c Configure the primary zone (vmware.corp) as a zone managed by Windows DNS.
- d Right-click the zone and select **New Delegation**.
- e Enter the name of the sub-domain (subdomain in our example).
- f In the **Server fully qualified domain name (FQDN)** field, type the IP address of SDDC Manager and click **Resolve**.
- g Click **OK**.

The new zone appears as a delegated zone under your primary domain.

- h In a command line window, ping `psc-1.Cloud_Foundation_Sub_Domain` (psc-1.subdomain.vmware.corp in our example).

Change SDDC Manager Password

During imaging, the SDDC Manager password is set to vmware1234. This is the password used during initial bring-up. For security reasons, you must change this password before connecting the rack to your corporate network.

Procedure

- 1 In a command line window, SSH to the SDDC Manager Controller VM on the rack. Use the IP address that you had noted from the IP Allocation page during bring-up.

- 2 Login with these credentials.

User name: root

Password: vmware1234

- 3 Type the following command to change the password:

```
passwd
```

- 4 At the prompt, type and re-type the new password.

The SDDC Manager Controller VM password is changed.

Connect Rack to Corporate Network

You can now connect the Cloud Foundation rack to your corporate network.

Procedure

- ◆ Depending on the switches in your environment, connect two 40 Gbps ports or multiple 10 Gbps ports to your corporate network and configure them appropriately. For wiring information, see *VIA User's Guide*.

Copy Backup File to an Accessible Location

Copy the files of the backup taken during bring-up to an accessible location.

During bring-up, the SoS tool makes backup files of these components' configurations on the rack:

- Switches (management, ToRs, spine)
- ESXi hosts
- SDDC Manager VMs
- HMS configurations on the SDDC Manager

After bring-up is complete, you must copy these files to an accessible location.

Procedure

- 1 In a command line window, SSH to the SDDC Manager Controller VM with your root credentials.
- 2 Navigate to `/var/tmp/`.
- 3 Copy the `backup-xxx` file to a location from where you can conveniently retrieve them for future configuration restoration situations.

Schedule Backup of Cloud Foundation Components

Schedule a periodic backup for your Cloud Foundation environment.

For information on scheduling backups, see *Back Up Component Configurations Using the SoS Tool* in the *Administering VMware Cloud Foundation* document.

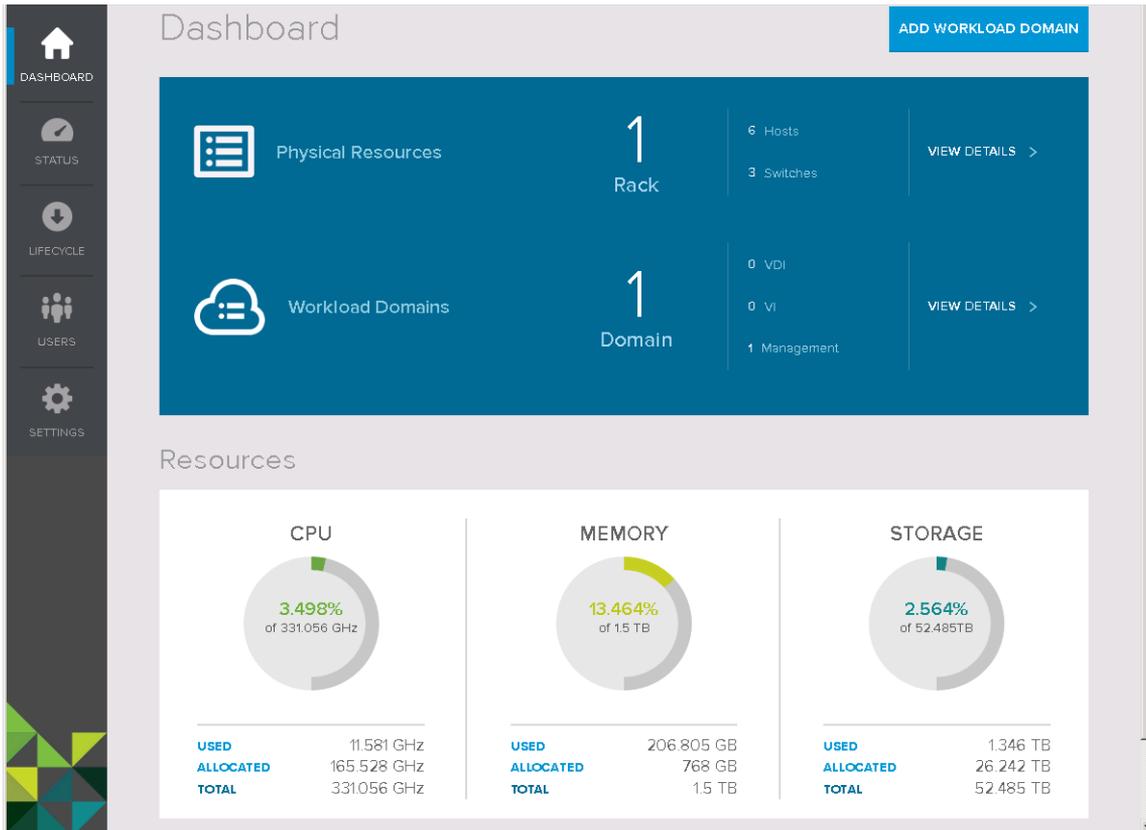
Login to the SDDC Manager Dashboard

Procedure

- 1 Refresh the web browser window where you were running the Initial Setup wizard.

2 Login with the superuser account credentials that you created during the initial setup

The SDDC Manager Dashboard appears.



For information on how to administer and operate your data center's Cloud Foundation system, see the *Administering VMware Cloud Foundation*.

Adding a Rack to your Cloud Foundation System

4

After Cloud Foundation bring-up has been completed on the first rack, you can add additional racks to your environment

Procedure

- 1 [Connect Additional Rack to Inter-rack Switches](#)
Connect the new rack to inter-rack switches.
- 2 [Power on Additional Rack](#)
After the inter-rack switch connections are in place, power on the additional rack.
- 3 [Add the Additional Rack to your Cloud Foundation System](#)
Add the additional rack to your Cloud Foundation system.

Connect Additional Rack to Inter-rack Switches

Connect the new rack to inter-rack switches.

Prerequisites

- 1 Ensure that the additional rack is powered down so that there is no connectivity between the first rack and this rack.
- 2 The bring-up process must have been completed successfully on rack 1. The rack 1 Dashboard must be accessible and the SDDC Manager VMs must be powered on.

Procedure

- ◆ Make the following connections:
 - First rack ToR 1 port 49 to spine 1 port 1 on rack 2
 - First rack ToR 1 port 50 to spine 2 port 1 on rack 2
 - First rack ToR 2 port 49 to spine 1 port 2 on rack 2
 - First rack ToR 2 port 50 to spine 2 port 2 on rack 2

What to do next

Power on the additional rack.

Power on Additional Rack

After the inter-rack switch connections are in place, power on the additional rack.

Procedure

- 1 Power on the additional rack.
- 2 Ensure that you can ping a host on rack 2 from the first rack.
- 3 Verify that the ports on the inter-rack switches on the additional rack are up.
- 4 Verify that the link connectivity LED between the racks is up.

Add the Additional Rack to your Cloud Foundation System

Add the additional rack to your Cloud Foundation system.

Prerequisites

You must have the manifest file for the rack you are adding.

If you bought an integrated system, the partner must have sent you the manifest file along with the imaged rack. If you imaged the additional rack, you must have downloaded and saved the manifest file after imaging the rack. See *VIA Use's Guide*.

Procedure

- 1 On the SDDC Manager Dashboard, click **SETTINGS > Physical Rack Settings**.

- 2 Click the **Add Rack** tab.

The Add a Rack wizard appears.

- 3 Type a name for the rack.
- 4 Upload the manifest file for the rack.

The system discovers and updates the inventory tables for the additional rack. The rack ID and component IDs are generated.

- 5 Click **Continue**.

The system sets the time on each component in the additional rack to match the time on first rack.

- 6 Click **Continue**.

The system performs Power On System Validation (POSV), where it validates that the right hardware and software is installed on the rack and also validates the health of the installed hardware and software applications.

7 Click **Continue**.

The system reconfigures IP addresses on the non-routable network and the OOB network for all hosts and switches. If this is the second rack in your Cloud Foundation system, the system then configures inter-rack network configurations. Then each component in the rack is assigned a unique password.

After configuration is complete, the **Dashboard** button is enabled.

8 Click **Dashboard** to proceed to the SDDC Manager dashboard.

Troubleshooting Cloud Foundation Deployment

5

You can troubleshoot issues that you might experience during deployment of your Cloud Foundation system.

This chapter includes the following topics:

- [Manually Power On SDDC Manager VMs When Setting Up Your Cloud Foundation System](#)
- [Restart HMS](#)
- [Retry If Bring-Up Fails During NFS Datastore Creation](#)
- [Retry If Bring-Up Fails During NSX Power Up](#)

Manually Power On SDDC Manager VMs When Setting Up Your Cloud Foundation System

When you power on a rack, the SDDC Manager Controller VM and SDDC Manager Utility VM that are pre-installed on host 0 are supposed to power on automatically. If this does not happen, you can manually power them on using the vSphere Web Client.

Problem

You open your browser to the address for the SDDC Manager setup wizard, and you do not see the wizard's starting screen. Instead of displaying the wizard, the browser shows there is no connection.

Cause

The setup wizard requires the pre-installed SDDC Manager VMs to be running. If they are not powered on when the ESXi host powers on, the setup wizard cannot run.

Solution

- 1 On the laptop that is connected to port 48 on the management switch, start the vSphere Web Client and open it to the IP address of host 0.
- 2 Log in to the host.
- 3 In the vSphere Web Client, navigate to the Inventory view to see the SDDC Manager Controller VM and SDDC Manager Utility VM. Ensure that they are powered on. If a virtual machine does not have a green arrow icon, it is not powered on.
- 4 If the VMs are not powered on, power them on.

Restart HMS

You may need to restart HMS while deploying the Cloud Foundation system.

Problem

While deploying the Cloud Foundation system, the following error message is displayed:

```
vRack has encountered an error. Problem connecting with HMS host: http://localhost:8080/hms-local at the moment.
```

Cause

HMS may have stopped running.

Solution

- 1 Verify if HMS is running by connecting to the SDDC Manager Controller VM and typing the following commands:

```
jobs
```

```
ps -lef |grep -i hms
```

- 2 If HMS is not running, restart HMS by typing the following commands.

```
cd /opt/vrack/hms
```

```
service starthms.sh start
```

Retry If Bring-Up Fails During NFS Datastore Creation

You might experience an exception during the NFS datastore creation in the bring-up process.

Problem

If intermittent network connectivity occurs during the bring-up process, the process might fail during the ESX: Create NFS Datastore task with the following exception:

```
Exception trying to create NAS DS on host host-ip-address
```

Cause

Intermittent network connectivity to an ESXi host during the bring-up process.

Solution

- ◆ In the bring-up user interface, click the **Retry** button to perform the task and proceed with the bring-up process.

Retry If Bring-Up Fails During NSX Power Up

You might experience an exception during the bring-up process if the NSX nodes fail to power on.

Problem

In a multi-rack system, the management domain creation workflow might fail during the NSX: Deploy NSX Manager task with an error stating that NSX did not power on.

Cause

The bring-up process fails because the NSX Controller virtual machines did not power on during the wait time set in the NSX: Register NSX with VC task.

Solution

- ◆ In the bring-up user interface, click the **Retry** button to perform the task and proceed with the bring-up process.

Additional VMware Product Documentation

6

Refer to the appropriate documentation for help with VMware SDDC products that are part of Cloud Foundation.

Product Name	Documentation
VMware ESXi and vCenter Server	ESXi and vCenter Server 6.5 Documentation at https://docs.vmware.com/en/VMware-vSphere/index.html
vSAN	Administering VMware vSAN at https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.virtualsan.doc/GUID-AEF15062-1ED9-4E2B-BA12-A5CE0932B976.html
NSX	NSX for vSphere Documentation at https://docs.vmware.com/en/VMware-NSX-for-vSphere/index.html
vRealize Log Insight	VMware vRealize Log Insight Documentation at https://docs.vmware.com/en/vRealize-Log-Insight/index.html

Example ToR Switch Output for L3 Configuration on Cisco ToR Switches (9372)

7

Example ToR Switch Output when you set up an iBGP connection between the ToR switches and an eBGP between each ToR switch and the upstream router.

```
TOR-20(config)# show running-config bgp

!Command: show running-config bgp
!Time: Tue Nov  8 00:50:29 2016

version 7.0(3)I2(2d)
feature bgp

router bgp 64990
  router-id 192.168.220.1
  address-family ipv4 unicast
    redistribute direct route-map rmap-bgp
    maximum-paths 4
    maximum-paths ibgp 2
  neighbor 192.168.53.2
    remote-as 64990
    address-family ipv4 unicast
  neighbor 192.168.54.2
    remote-as 64990
    address-family ipv4 unicast
  neighbor 192.168.143.2
    remote-as 64512
    address-family ipv4 unicast
  neighbor 192.168.144.2
    remote-as 64512
    address-family ipv4 unicast
  neighbor 192.168.145.2
    remote-as 64512
    address-family ipv4 unicast
  neighbor 192.168.146.2
    remote-as 64512
    address-family ipv4 unicast

TOR-20(config)# show ip interface brief
IP Interface Status for VRF "default"(1)
Interface          IP Address      Interface Status
Vlan1001           192.168.120.21 protocol-up/link-up/admin-up
Vlan1005           192.168.98.1   protocol-up/link-up/admin-up
Lo0                 192.168.220.1  protocol-up/link-up/admin-up
```

```

Eth1/43      192.168.143.1  protocol-up/link-up/admin-up
Eth1/44      192.168.144.1  protocol-up/link-up/admin-up
Eth1/45      192.168.145.1  protocol-up/link-up/admin-up
Eth1/46      192.168.146.1  protocol-up/link-up/admin-up
Eth1/53      192.168.53.1   protocol-up/link-up/admin-up
Eth1/54      192.168.54.1   protocol-up/link-up/admin-up

```

```
TOR-21(config)# show running-config bgp
```

```
!Command: show running-config bgp
```

```
!Time: Tue Nov 8 00:54:23 2016
```

```
version 7.0(3)I2(2d)
```

```
feature bgp
```

```
router bgp 64990
```

```
router-id 192.168.220.2
```

```
address-family ipv4 unicast
```

```
redistribute direct route-map rmap-bgp
```

```
maximum-paths 4
```

```
maximum-paths ibgp 2
```

```
neighbor 192.168.53.1
```

```
remote-as 64990
```

```
address-family ipv4 unicast
```

```
neighbor 192.168.54.1
```

```
remote-as 64990
```

```
address-family ipv4 unicast
```

```
neighbor 192.168.243.2
```

```
remote-as 64512
```

```
address-family ipv4 unicast
```

```
neighbor 192.168.244.2
```

```
remote-as 64512
```

```
address-family ipv4 unicast
```

```
neighbor 192.168.245.2
```

```
remote-as 64512
```

```
address-family ipv4 unicast
```

```
neighbor 192.168.246.2
```

```
remote-as 64512
```

```
address-family ipv4 unicast
```

```
TOR-21(config)# show ip interface brief
```

```
IP Interface Status for VRF "default"(1)
```

Interface	IP Address	Interface Status
Vlan1001	192.168.120.20	protocol-up/link-up/admin-up
Lo0	192.168.220.2	protocol-up/link-up/admin-up
Eth1/43	192.168.243.1	protocol-up/link-up/admin-up
Eth1/44	192.168.244.1	protocol-up/link-up/admin-up
Eth1/45	192.168.245.1	protocol-up/link-up/admin-up
Eth1/46	192.168.246.1	protocol-up/link-up/admin-up
Eth1/53	192.168.53.2	protocol-up/link-up/admin-up
Eth1/54	192.168.54.2	protocol-up/link-up/admin-up

```
Core1(config-router)# show running-config bgp
```

```
!Command: show running-config bgp
!Time: Tue Nov  8 00:57:53 2016
```

```
version 7.0(3)I4(2)
feature bgp
```

```
router bgp 64512
  router-id 192.168.221.1
  address-family ipv4 unicast
    redistribute direct route-map rmap-bgp
    maximum-paths 4
    maximum-paths ibgp 2
  neighbor 192.168.49.2
    remote-as 64512
    address-family ipv4 unicast
  neighbor 192.168.50.2
    remote-as 64512
    address-family ipv4 unicast
  neighbor 192.168.143.1
    remote-as 64990
    address-family ipv4 unicast
  neighbor 192.168.144.1
    remote-as 64990
    address-family ipv4 unicast
  neighbor 192.168.245.1
    remote-as 64990
    address-family ipv4 unicast
  neighbor 192.168.246.1
    remote-as 64990
    address-family ipv4 unicast
```

```
Core1(config-router)# show ip interface brief
```

```
IP Interface Status for VRF "default"(1)
```

Interface	IP Address	Interface Status
Lo0	192.168.221.1	protocol-up/link-up/admin-up
Eth1/1	192.168.143.2	protocol-up/link-up/admin-up
Eth1/2	192.168.144.2	protocol-up/link-up/admin-up
Eth1/3	192.168.245.2	protocol-up/link-up/admin-up
Eth1/4	192.168.246.2	protocol-up/link-up/admin-up
Eth1/49	192.168.49.1	protocol-up/link-up/admin-up
Eth1/50	192.168.50.1	protocol-up/link-up/admin-up

```
Core2(config-router)# show running-config bgp
```

```
!Command: show running-config bgp
!Time: Tue Nov  8 00:58:04 2016
```

```
version 7.0(3)I4(2)
feature bgp
```

```
router bgp 64512
  router-id 192.168.221.2
  address-family ipv4 unicast
```

```
redistribute direct route-map rmap-bgp
maximum-paths 4
maximum-paths ibgp 2
neighbor 192.168.49.1
  remote-as 64512
  address-family ipv4 unicast
neighbor 192.168.50.1
  remote-as 64512
  address-family ipv4 unicast
neighbor 192.168.145.1
  remote-as 64990
  address-family ipv4 unicast
neighbor 192.168.146.1
  remote-as 64990
  address-family ipv4 unicast
neighbor 192.168.243.1
  remote-as 64990
  address-family ipv4 unicast
neighbor 192.168.244.1
  remote-as 64990
  address-family ipv4 unicast
```

```
Core2(config-router)# show ip interface brief
```

```
IP Interface Status for VRF "default"(1)
```

Interface	IP Address	Interface Status
Lo0	192.168.221.2	protocol-up/link-up/admin-up
Eth1/1	192.168.243.2	protocol-up/link-up/admin-up
Eth1/2	192.168.244.2	protocol-up/link-up/admin-up
Eth1/3	192.168.145.2	protocol-up/link-up/admin-up
Eth1/4	192.168.146.2	protocol-up/link-up/admin-up
Eth1/49	192.168.49.2	protocol-up/link-up/admin-up
Eth1/50	192.168.50.2	protocol-up/link-up/admin-up

Cloud Foundation Glossary

8

Term	Description
add rack	Configure an additional rack for a Cloud Foundation system.
additional rack	Additional racks (added after the first rack) to a Cloud Foundation system.
bring-up	Initial configuration of a newly deployed Cloud Foundation system. .
Cloud Foundation system.	Set of physical racks managed as a unit by a single SDDC Manager.
first rack	First (primary) rack in the Cloud Foundation system. The management domain is deployed on this rack.
Hardware Management System (HMS)	Manages hosts and switches in the Cloud Foundation system.
host	An imaged server.
imaging	During imaging, SDDC software is pre-configured on a physical rack.
integrated system	System that combines hardware and software. Can be purchased from select VMware partners. The partner images the rack before sending it to the customer site.
inter-rack switches	Connects individual ToR switches with each other to provide connectivity across racks. These switches are required only when you have more than one rack in your Cloud Foundation system, and are placed on the second rack.
Lifecycle Manager (LCM)	Automates patching and upgrading of the software stack.
management domain	Cluster of physical hosts (first four hosts in the physical rack) that house the management component VMs
management host	Standalone ESXi server to host the Windows jump VM used for imaging.
primary host	Host on which VIA deploys the SDDC Manager VMs during imaging, and which bootstraps the first rack during bring-up.
SDDC Manager	Software component that provisions, manages, and monitors the logical and physical resources of a Cloud Foundation system.
SDDC ManagerController VM	Contains the SDDC Managerservices and a shell from which command line tools can be run. This VM exposes the SDDC Manager UI.
SDDC Manager Utility VM	Contains the LCM depot, backup repository containing NSX Manager and host backups, and 2nd DNS instance.
server	Bare metal server in a physical rack. After imaging, it is referred to as a host.
Top of Rack (ToR) switch	Connects servers within a rack through 10Gbps links to the NICs on each server. A Cloud Foundation rack contains two ToR switches connected to each other.

Term	Description
unassigned host	Host in the capacity pool that does not belong to a workload domain.
workload domain	A policy based resource container with specific availability and performance attributes and combining vSphere, vSAN and NSX into single a consumable entity. A workload domain can be created, expanded, and deleted as part of the SDDC lifecycle operations.