VMware Cloud Foundation Overview and Bring-Up Guide

VMware Cloud Foundation 2.1.3

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

Contents

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 an 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, spine 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 your data center's deployed Cloud Foundation system.

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

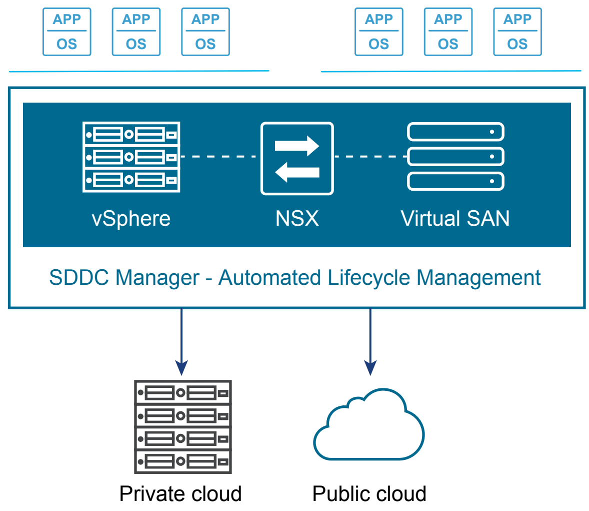
VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

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
- Cloud Foundation Use Cases
- Private Cloud Deployment Options
- 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 starting with the core infrastructure virtualization, vSphere, Virtual SAN and NSX, in addition to the SDDC Manager for lifecycle management automation. Customers can flexibly upgrade individual components in the stack to higher editions and optionally deploy VMware vRealize Suite and VMware Horizon.

Automates Hardware and Software Bring-Up

Cloud Foundation automates the installation of the entire VMware software stack. Once the rack is installed and powered on and the networking is in place, SDDC Manager leverages its knowledge of the hardware bill of materials and user-provided environmental information (e.g. DNS, IP address pool, etc.) to initialize the rack. 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 workloads, including automated provisioning of networks, allocation of resources based on service needs, and provisioning of end points. When the process completes, the customer has a virtual infrastructure ready to start deploying vSphere clusters and provisioning workloads.

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. 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 relieve a cloud administrator from having to research and implement best practices needed 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 entire infrastructure or to specific workload domains and is designed to be non-disruptive to tenant virtual machines (VMs). By utilizing live VM migration, SDDC Manager can patch software to improve infrastructure security and reliability while maintaining tenant uptime.

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 as small as 4servers, and can scale out to multiple racks. 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 8 full racks per SDDC Manager instance. Cloud Foundation automatically discovers any new capacity and adds it into the larger pool of available capacity for use.

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 turnkey solution to run your SDDC infrastructure. Cloud administrators have the ability to expand and contract 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 their vSphere compatible tools directly with vCenter Server.

VI configures a flexible virtual datacenter including the following:

- Ability to deploy and configure OS instances in the form of VMs with vCPUs, memory, and storage including networking resources.
- Internet connectivity with a built-in IPAM (IP Address Management) solution.

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 servers specified by the administrator are deployed. Each server 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. It creates workload domains according to the specifications, adding hosts and creating vSAN datastores from the storage on those hosts. It also deploys and configures NSX vSwitches into the ESXi instance on each host.

- Physical networking

  SDDC Manager uses the Hardware Management Services (HMS) to configure 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.

- Management

  Cloud Foundation allows administrators to monitor and manage the workload domain using vRealize Operations Manager, and vRealize Log Insight.

Virtual Desktop Infrastructure

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

When you deploy a VDI workload, Cloud Foundation reserves the necessary hardware resources and deploys the required SDDC components. Your Cloud Foundation system auto-configures the physical infrastructure. SDDC Manager deploys the following for a VDI workload:

- Physical compute

  The servers specified by the administrator are deployed. Each server 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. It creates workload domains according to the specifications, adding hosts and creating vSAN datastores from the storage on those hosts. It also deploys and configures NSX switches into the ESXi instance 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.

- Management

  Cloud Foundation allows administrators to monitor and manage the workload domain using vRealize Operations Manager, and vRealize Log Insight.

- VDI

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

With VDI, you can:

- Create additional users for access to the VMware Horizon with View environment, connecting it to an LDAP or Active Directory server for authenticating enterprise users.
- Configure desktop environments including persistence, application access, etc.
- Migrate VM templates from VDI infrastructure outside the workload domain into the virtual rack workload domain(s). This is made possible because the SDDC Manager creates the management virtual network as a public one (traffic can flow in and out of the workload domain and physical rack) and vCenter Server 6.0 allows VM migration between vCenter Servers. You cannot migrate VMs being managed by another installation of VMware Horizon with View.

IT Automating IT

vRealize Automation can be optionally added to the Cloud Foundation software stack.

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.

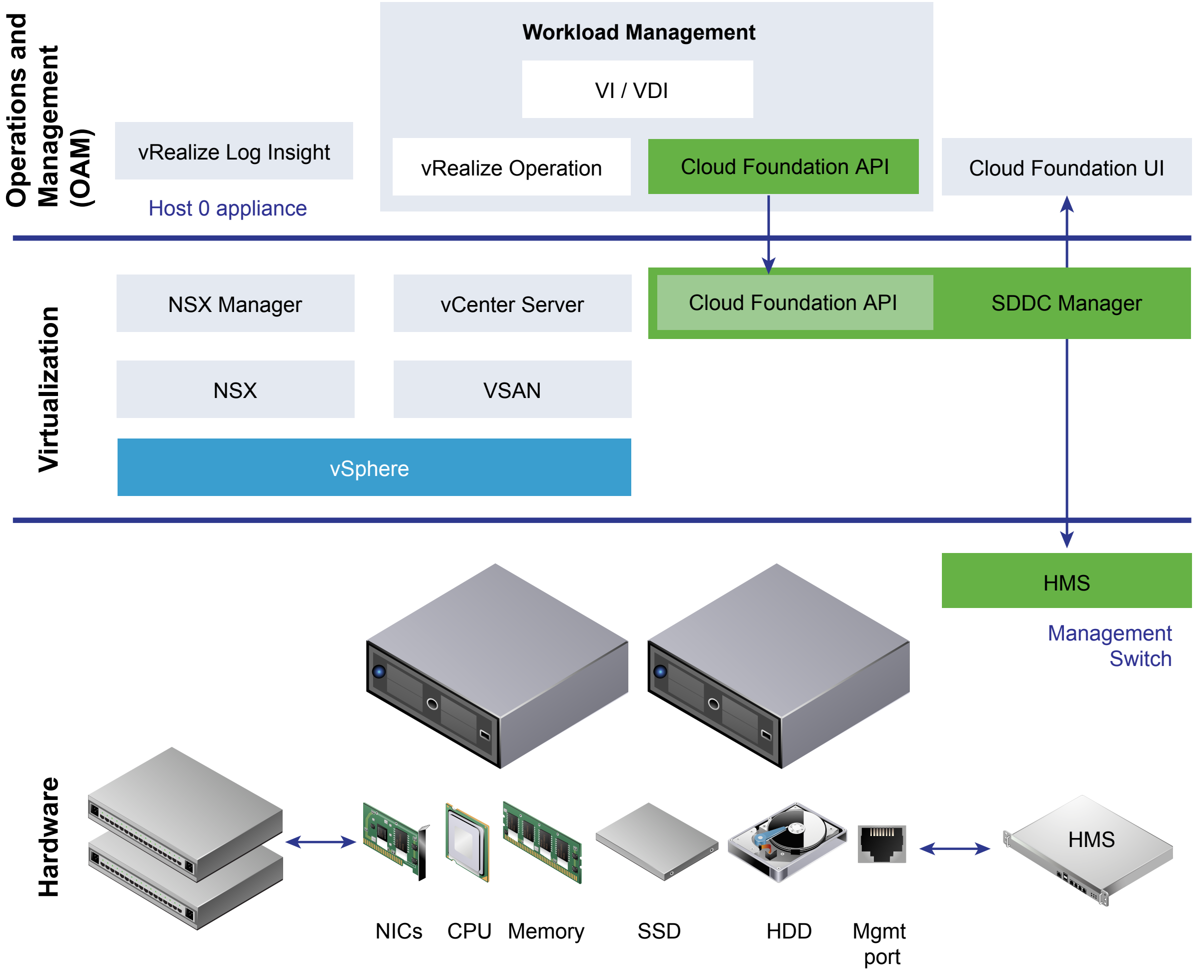
- Purchase a fully integrated system that combines software and hardware from select VMware partners.

  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.

Physical Topology

Cloud Foundation is a logical instance of up to eight physical racks.

Figure 1-1. Physical Topology



Spine Switches

The Cloud Foundation system contains two spine 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 hardware vendor connects the available uplink ports of the ToR switches to the spine switches.

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

Management Switch

The management switch provides Out-Of-Band (OOB) connectivity to the baseboard management controller (BMC) on each server.

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 spine switches. As a result 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, each of which has 48 10GE ports and at least 4 40GE uplink ports. The ToR and spine switches carry all network traffic from the servers including VM network, VM management, vSAN, and vMotion traffic. On rack 1 in a multi-rack Cloud Foundation, the ToRs also carry 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 the ToR switches goes down.

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

Servers

This section contains information about supported server models and component configurations.

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
Storage per server	4 TB for capacity tier. Follow vSAN guidelines for cache tier sizing as described in VMware vSAN Design and Sizing Guide. For high performance workload domains, 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 controller. 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 workload creation.	32 1U servers or 16 2U servers
Rack	1	8

Management Domain

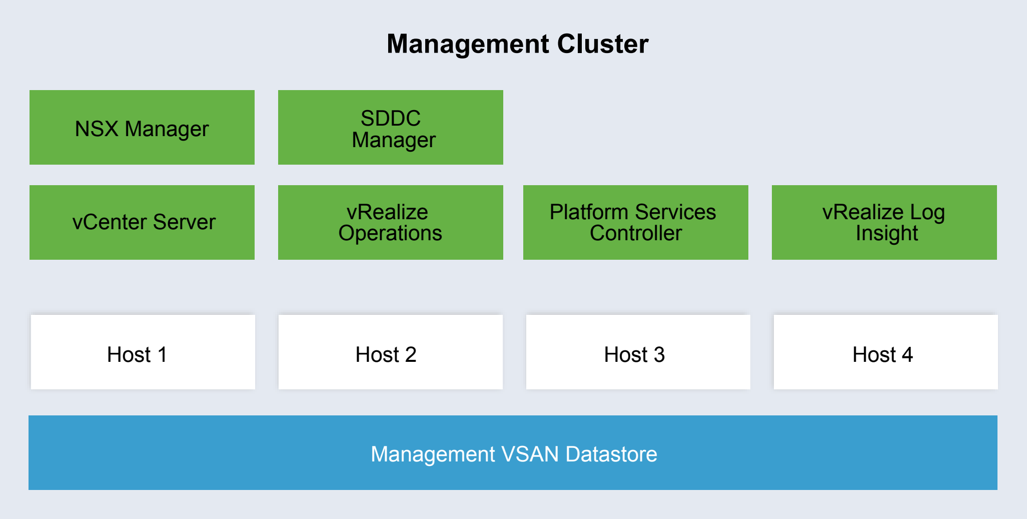
SDDC Manager configures the first four servers in each physical rack into an entity called the management domain. After you deploy Cloud Foundation, you can expand the management domain.

The management domain manages the hosts in that rack. All disk drives are claimed by vSAN.

The management domain contains the following:

- vCenter Server Appliance(including both vCenter Server and Platform Services Controller as separate VMs) managing the vSphere cluster with HA and DRS enabled.
- The following VMs:
  - NSX Manager
  - vRealize Operations
  - vRealize Log Insight
  - SDDC Manager

Figure 1-2. Management Domain Architecture



Network Topology

All hosts in a physical rack are connected to both the two ToR switches with 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).

The BMC on each host is connected to the management switch over a 1G connection. This connection is used for OOB management. Both ToR switches are further connected to a pair of spine switches in a dual-LAG configuration using 40 G links. The spine 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 spine switches, the system can tolerate the failure of a ToR switch and/or spine 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. All vSAN members communicate over this 10Gbps network.

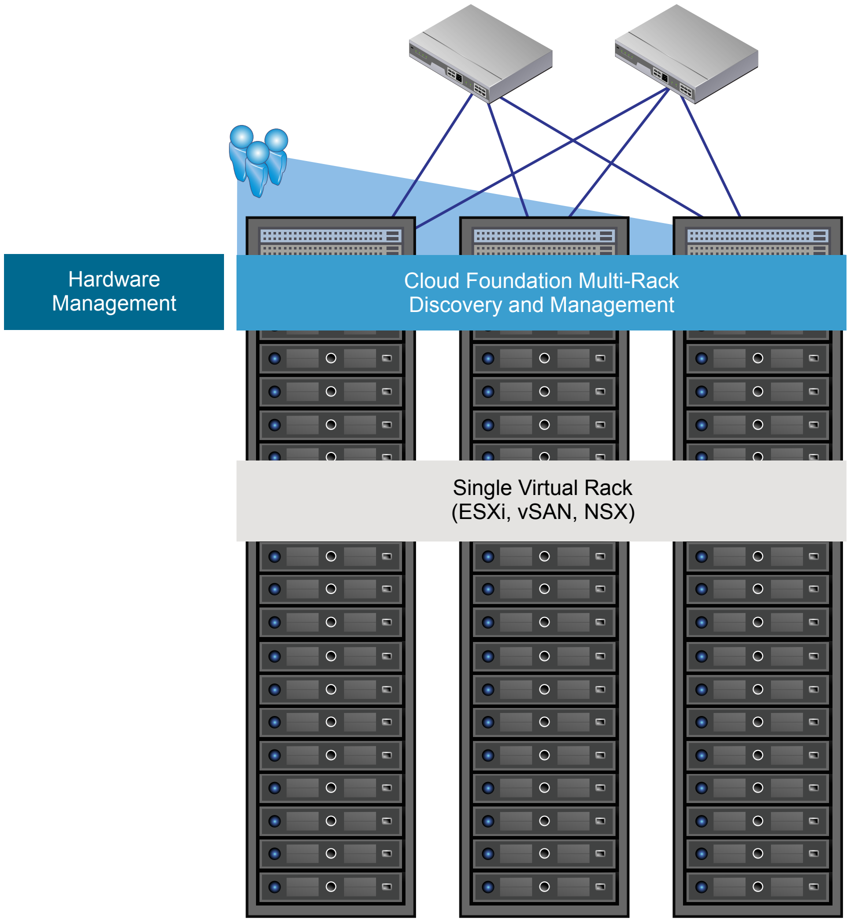
vSphere Network I/O Control (NIOC) can be enabled to allow network resource management to use network resource pools to prioritize network traffic by type.

Cloud Foundation Architecture 2

Cloud Foundation is a logical instance of orchestrating, provisioning, and deploying an 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 distributed management solution across your SDDC.

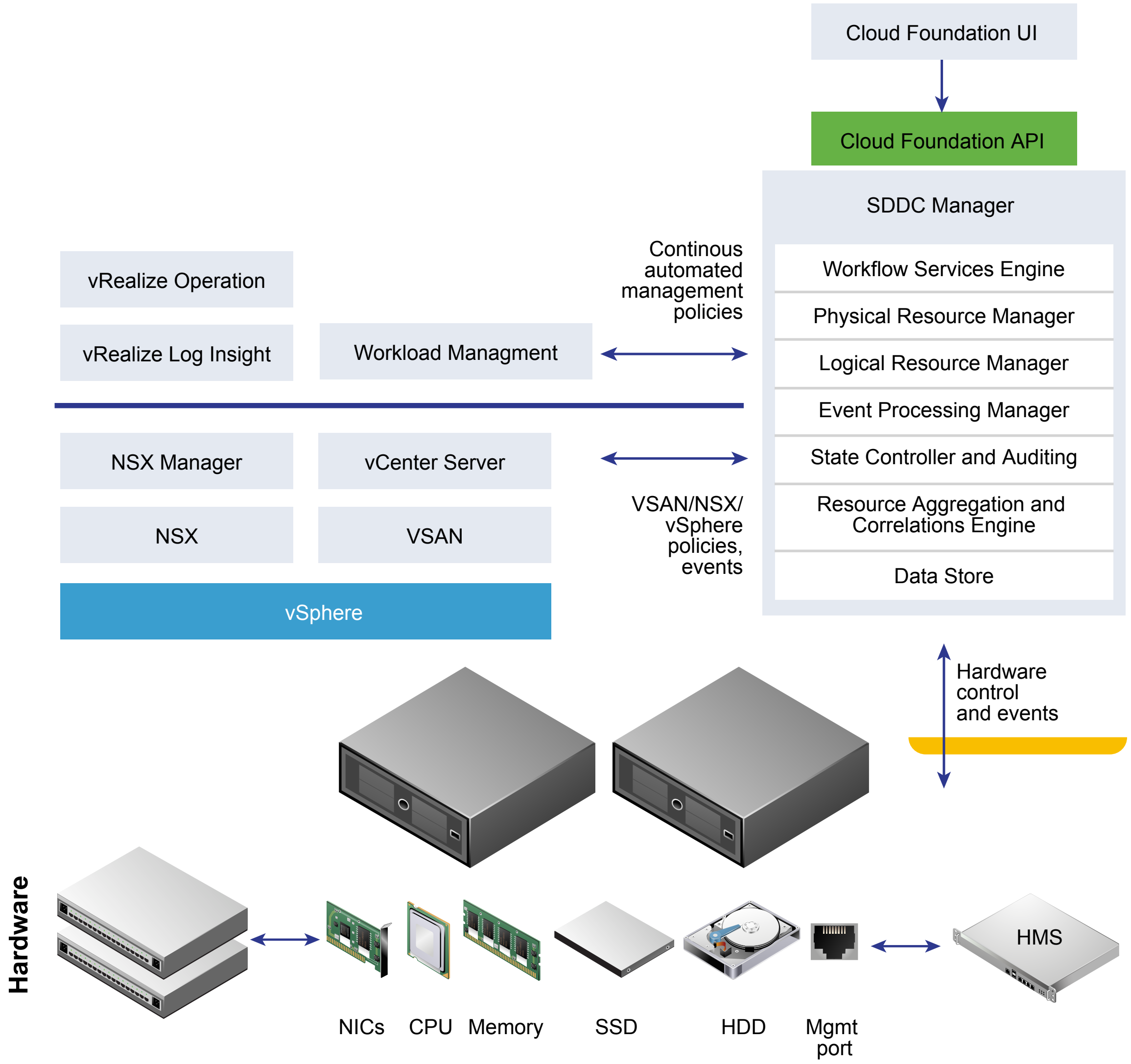
Though there is a management software stack on each physical rack, Cloud Foundation's distributed architecture provides the SDDC Manager as a single point-of-control web-based interface for managing infrastructure and deploying workloads.

Figure 2-1. Multi-Rack Setup



The figure below shows the software components of Cloud Foundation and how they are mapped to the physical hosts and switches in the rack.

Figure 2-2. Cloud Foundation Software Stack



This chapter includes the following topics:

- VIA
- SDDC Manager
- Hardware Management Services and Hardware Plugins
- SDDC Components of Cloud Foundation

VIA

VIA is a virtual appliance used by system integrators or administrators deploying VMware Cloud Foundation to image physical racks. During imaging, VIA pre-configures the Cloud Foundation software stack on the rack. For more information, see *VIA User's Guide*.

SDDC Manager

The SDDC Manager provisions, manages, and monitors the logical and physical resources of Cloud Foundation.

SDDC Manager is responsible for Cloud Foundation configuration, operations, and management functions by:

- Abstracting and aggregating the physical resources of an SDDC into a logical entity.
- Performing physical resource management such as adding and removing hosts or switches to the rack, adding new racks to scale, failure management, and maintaining and upgrading hosts and switches.
- Orchestrating the shutdown and boot-up of logical software and management plane components of Cloud Foundation such as ESXi, vCenter Server, vRealize Operations, vRealize Log Insight, NSX, and vSAN.
- Generating the logical resource mapping structures based on workload profiles, physical events, and physical operations (such as vCenter clusters, vCenter cluster expansion operations, etc.).
- Interacting with the Cloud Foundation software components, such as vCenter Server for cluster and vSAN management, Hardware Management Services for hardware management, vRealize Operations for health monitoring; NSX Manager for network management, and the vRealize Automation suite for workload management.

As you expand your Cloud Foundation environment horizontally by adding physical racks, the SDDC Manager allows data center administrators to configure the additional racks into a single pool of resources. This consolidates compute, storage, and networking resources of the racks available for assignment to workloads.

The SDDC Manager is a multi-threaded execution engine that includes the Physical Resources Manager (PRM), Logical Resources Manager (LRM), and an events engine.

Services Engine

The services engine enables SDDC Manager to perform its management plane functions. The implementation of this engine uses the Java Executor Service framework initialized with a collection of runnable threads and scheduler threads that pull the next threads for execution. SDDC Manager functions are structured as workloads, workflows, and tasks.

Workloads

Workloads are applications deployed on Cloud Foundation. These include initial bring-up of Cloud Foundation as well as VI and VDI workload domains. Workloads consume resources and can lead to multiple software component instantiations during their creation. They are configured with various parameters that specify their resource requirements, software components to be deployed, network configuration details, etc. These details may be stored as workload metadata in the SDDC Manager database or can be directly supplied to the workflow context which is also stored in the SDDC Manager database.

Workflows

Workflows are a long running group of tasks that change the state of a workload. Examples of workflows include creating an instance of a workload, changing the allocated capacity, or removing the workload and reclaiming its associated resources.

Tasks

A task is a unit of work from a workflow. A task can do calculations, allocate resources, and/or request resources. A workflow task obtains the input parameters from either the workflow context or workload metadata and then sets the output parameters. A task can include multiple steps.

If the task fails, it is resumed from right before the point of failure. Since a task can include multiple steps, the step that follows the last successful step in the task can be the point where the task is resumed.

Database

Workload and workflow metadata is stored in the SDDC Manager database. Workload metadata includes information that is always important to the system such as a list of racks, hosts, etc. Workflow data is temporary and stops to exist when a workflow changes a workload or when the workflow is successfully executed.

Physical Resources Manager

The Physical Resources Manager (PRM) manages the physical components of a physical rack and maintains a corresponding software physical rack object.

The PRM does the following:

- defines the interfaces that access the physical resource abstractions.
- retrieves the physical hardware state by interfacing with the HMS layer.
- relays HMS events to the SDDC Manager engine.

Logical Resource Manager

The Logical Resource Manager (LRM) manages the logical resource state of Cloud Foundation.

LRM Controller

The LRM controller is exported as a logical managed view, which is comprised of the deployed vCenters and resource stats per vCenter.

Examples of logical resource types include the following:

- VM
- distributed virtual switch
- distributed virtual portgroup

- host system
- datastore
- total storage

LRM Logical Resources

LRM builds its logical resource view of Cloud Foundation components by interfacing with vCenter using vSphere APIs.

LRM Services

An example of an LRM service is the LRM alarm service that fetches alarms from vCenter periodically.

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.

SDDC Manager in a Multi-Rack Setup

When Cloud Foundation is deployed in a multi-rack environment, bare-metal provisioning and subsequent installation and configuration of software components (e.g., vCenter, NSX, SDDC Manager on host 0) is executed on each rack sequentially. Though there is an instance of SDDC Manager on each physical rack, you can control and manage your Cloud Foundation system through a single interface.

SDDC Manager is highly available. The SDDC Manager instance in the management cluster of the first physical rack is the leader, while the SDDC Manager on each additional physical rack is a secondary instance. To manage this cluster of SDDC Manager services, Cloud Foundation uses Zookeeper and Cassandra as a distributed cluster management service and as shared distributed datastore.

Zookeeper runs as a ZK server process instance within the SDDC Manager VM. The SDDC Manager process communicates with Zookeeper servers using a Zookeeper client handle.

Hardware Management Services and Hardware Plugins

The Hardware Management Services (HMS) provides the necessary functions required for discovering, bootstrapping, and monitoring the hardware in a physical rack in the system. The HMS out of band agent runs on the management switch of each physical rack.

The HMS is an abstracted software mechanism that manages the physical hardware in the physical racks, such as servers and network switches. The HMS provides this abstraction to enable integration of supported hardware from different sources and give 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 directly. With the HMS you can discover, bootstrap, and monitor the hardware by polling received hardware events and handling hardware state changes. The HMS obtains these hardware events and state changes from software plugins that hardware partners create and provide to work with their specific hardware.

SDDC Components of Cloud Foundation

This section describes how the SDDC software components work within an Cloud Foundation system. A virtual rack is a set of physical racks combined into and managed as a single logical entity. A workload domain is a resource group with specific availability and performance attributes.

ESXi

ESXi is a Type I hypervisor that customers use to implement virtualization on bare metal systems to create their own datacenters. Along with certain add-on management products, many customers use ESXi to create private cloud solutions.

Cloud Foundation uses ESXi as a foundation for creating its SDDC architecture by using the hypervisor to run VMs in workload domains as well as the management domain. vCenter Server manages the workload domains using HA and uses internal storage aggregated into a datastore using vSAN.

vCenter Server

vCenter Server provides a single point of management of a VMware virtualized environment with one or more ESXi instances.

Cloud Foundation deploys the vCenter Server Appliance, a preconfigured Linux-based virtual machine optimized for running vCenter Server. The services bundled with the Platform Services Controller and vCenter Server are deployed on different virtual machines. As a result, by default, the management domain consists of a vCenter Server, and two external Platform Services Controllers.

Each vCenter division is configured as follows:

- A vSphere cluster with DRS and HA is enabled.
- Hosts supplying resources to the workload domain are added to the vSphere cluster.
- The capacity tier is aggregated into a vSAN-backed datastore, with the cache tier disk drives in vSAN configured separately to provide additional performance.

vSAN

vSAN pools together server-attached flash devices and/or hard disks to provide a highly resilient shared datastore suitable for a variety of workloads including business-critical applications, virtual desktops, remote IT, DR, and DevOps infrastructure.

In Cloud Foundation, each workload domain contains one or more vSphere clusters. 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.

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.

One NSX Manager maps to a single vCenter Server environment. Therefore, each workload domain includes one NSX Manager instance and one NSX Controller instance.

Beyond this, 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 Operations

vRealize Operations delivers intelligent operations management across physical, virtual, and cloud infrastructure. It correlates data from applications to storage in a unified, easy-to-use management tool that provides control over performance, capacity, and configuration, with predictive analytics driving proactive action, and policy-based automation.

Cloud Foundation configures vRealize Operations so that administrators can monitor operations of both the physical and virtual components through a single interface.

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 so that administrators can monitor logs for both the physical and virtual components through a single interface.

Preparing your Site for the Cloud Foundation System

3

If you are installing Cloud Foundation on qualified vSAN Ready Nodes, you can ignore this topic. If you purchased an integrated system from a VMware partner, you must prepare your datacenter facility for the arrival of the Cloud Foundation system.

Prior to the arrival of the Cloud Foundation system, you completed the *VMware Cloud Foundation Site Readiness Planning Guide*. This document describes the prerequisites and site information you use for planning the deployment of the physical infrastructure. Refer to this document for information on how to prepare your datacenter location for the arrival of the Cloud Foundation system.

Cloud Foundation Initial Bring-Up

4

Once your physical rack is imaged (where the SDDC software is pre-configured on the rack), the rack is powered on, and ToR switches are connected to the datacenter network, you connect a jump box to the ToR switches and log in to the SDDC Manager using a browser on the jump box.

During power on, SDDC Manager completes the configuration of a private cloud in a process called bring-up.

The bring-up process involves multiple steps. Multi-rack configurations require all steps to be completed on the first physical rack before adding additional physical racks

Prerequisites

Verify that you have met the following prerequisites.

- You have your completed copy of the VMware Cloud Foundation Site Readiness Planning Guide along with your VMware representative. This document contains networking and other information that you use in the Cloud Foundation setup wizard.
- You have prepared your site, including power requirements, as described in the *VMware Cloud Foundation Site Readiness Planning Guide*.
- You have physical connectivity to the management switch in the first physical rack and a supported web browser such as Mozilla Firefox and Google Chrome. For the list of supported browser versions, see the *Release Notes*. To run the setup wizard, the browser must be able to connect to port 48 on a rack's management switch. Some methods to accomplish this prerequisite are:
  - On the physical rack, wire the management switch's port #48 to a computer (jump host) that has one of the supported browsers, such as a Windows laptop with its integrated monitor.
  - To use a browser on a remote computer, use a switch to connect the management switch's port #48 to a network that your remote computer can use to access the port.

Procedure

1 Connect Rack 1 to Your Power Source and Network

2 Initiate the Cloud Foundation Bring-Up Process on Rack 1

You initiate the bring-up process on a computer that can access the management switch in the physical rack. The wizard runs in a standard web browser, such as Mozilla Firefox and Google Chrome. After you provide site specific information such as rack name, passwords, IP addresses, and DNS and NTP details, SDDC Manager configures your private cloud.

3 Locate SDDC Manager IP Address

The SDDC Manager IP address changes during bring-up. You need to look up the new IP address so that you can log in to change the password on the rack components.

4 Change Passwords of Rack Components

Cloud Foundation is deployed with factory default passwords. You must replace the default passwords with secure system generated passwords.

5 Change SDDC Manager Password

If you purchased an integrated system, your hardware partner sends you the system generated password for SDDC Manager along with the imaged rack. If you deployed Cloud Foundation on a ready system, you must have saved the SDDC Manager password. This password is not changed during password rotation. VMware strongly recommends that you change this password before creating workloads.

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.

Connect Rack 1 to Your Power Source and Network

Procedure

1 Connect the rack's power inlets to your power source.

2 Connect port 48 of rack 1's management switch to a laptop that has a standard web browser installed, from where you will run the setup wizard.

3 Configure the NIC on the laptop to tag VLAN traffic.

4 Create two interfaces on the laptop - say interfaces 1 and 2.

   a Leave interface 1 untagged and assign the 192.168.100.248/24 IP address/subnet mask to it.

   Interface 1 will allow OOB access to all Cloud Foundation hardware and software components.

   b Tag interface 2 with the management VLAN and assign an unused IP address/subnet mask from the management network IPaddress pool used for management workload domains.

   Interface 2 will allow for OOB access if there is an uplink mis-configuration and the system is unreachable from the upstream customer network.

5 Install a vSphere client application on the jump host.

Your Cloud Foundation system arrives with virtual machines pre-installed on ESX host 192.168.100.50 in the rack. If any of those virtual machines do not power on when you power on the servers in a rack, you can use the vSphere Client application to connect to and manually power on the virtual machine.

What to do next

1. Ping host 0 at 192.168.100.50. If you are unable to ping host 0, contact VMware support.
2. Open a supported browser on the jump host and navigate to https://192.168.100.40:8443/vrm-ui. For a list of the supported browser versions, see the product *Cloud Foundation Release Notes*. If the browser does not display the setup wizard, the required virtual machines might not be powered on. Verify whether the required virtual machines are running and, if not, power them on as described in Manually Power On SDDC Manager VM When Setting Up Your Cloud Foundation System.

Continue with the steps in Initiate the Cloud Foundation Bring-Up Process on Rack 1.

Initiate the Cloud Foundation Bring-Up Process on Rack 1

You initiate the bring-up process on a computer that can access the management switch in the physical rack. The wizard runs in a standard web browser, such as Mozilla Firefox and Google Chrome. After you provide site specific information 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 Rack 1 to Your Power Source and Network.
2. Either turn off firewall on the jump host or ensure that the firewall ports required to access Cloud Foundation on it are open.

Table 4-1. 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 4-2. Outbound Ports for Cloud Foundation

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

In addition, VMware software may require additional firewall ports to be open.

- vRealize Operations

  https://pubs.vmware.com/vrealizeoperationsmanager-6/index.jsp?topic=%2Fcom.vmware.vcom.core.doc%2FGUID-8CEB26FB-9EAF-45D7-A6A5-232A3CED3D6E.html

- vRealize Log Insight

  https://pubs.vmware.com/log-insight-30/index.jsp?topic=%2Fcom.vmware.log-insight.security.doc%2FGUID-14DBC90A-379A-4316-9D76-4850E08437A8.html

- vCenter Server and ESXi

  https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1005189

- VMware Horizon with View

  https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027217

- Platform Services Controller

  https://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.upgrade.doc%2FGUID-925370DD-E3D1-455B-81C7-CB28AAF20617.html

3 Depending on the switches in your environment, ensure that two 40 Gbps ports or multiple 10 Gbps ports are connected to your corporate network and configured appropriately. For details, see *VIA User's Guide*.

4 If your rack has only 4 ports, you must update the `vrm.properties` file before starting bring-up on the rack.

   a In a command line window, SSH to the base IP address for SDDC Manager on the rack.

   b In the `/home/vrack/VMware/vRack/vrm.properties` file, change the `rack.initial.mgmt.hosts=3` parameter to `rack.initial.mgmt.hosts=4` .

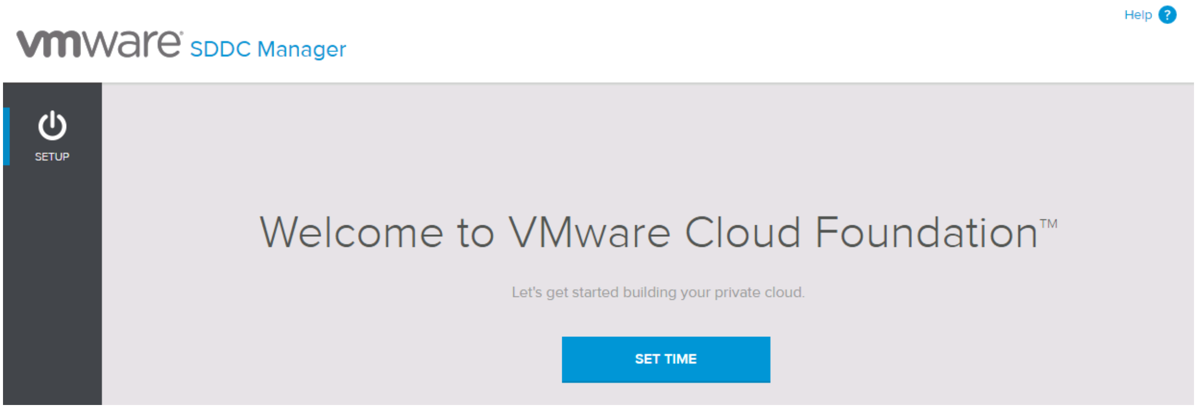
   c In the /home/vrack/vrm/webapps/vrm-ui/web-inf/classes/vrm.properties file, change the `rack.initial.mgmt.hosts=3` parameter to `rack.initial.mgmt.hosts=4` .

Procedure

1 After you connect the Cloud Foundation system to your network, 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 you have connected to port #48 of the rack's management switch, navigate to `https://192.168.100.40:8443/vrm-ui`.

The Welcome page appears.

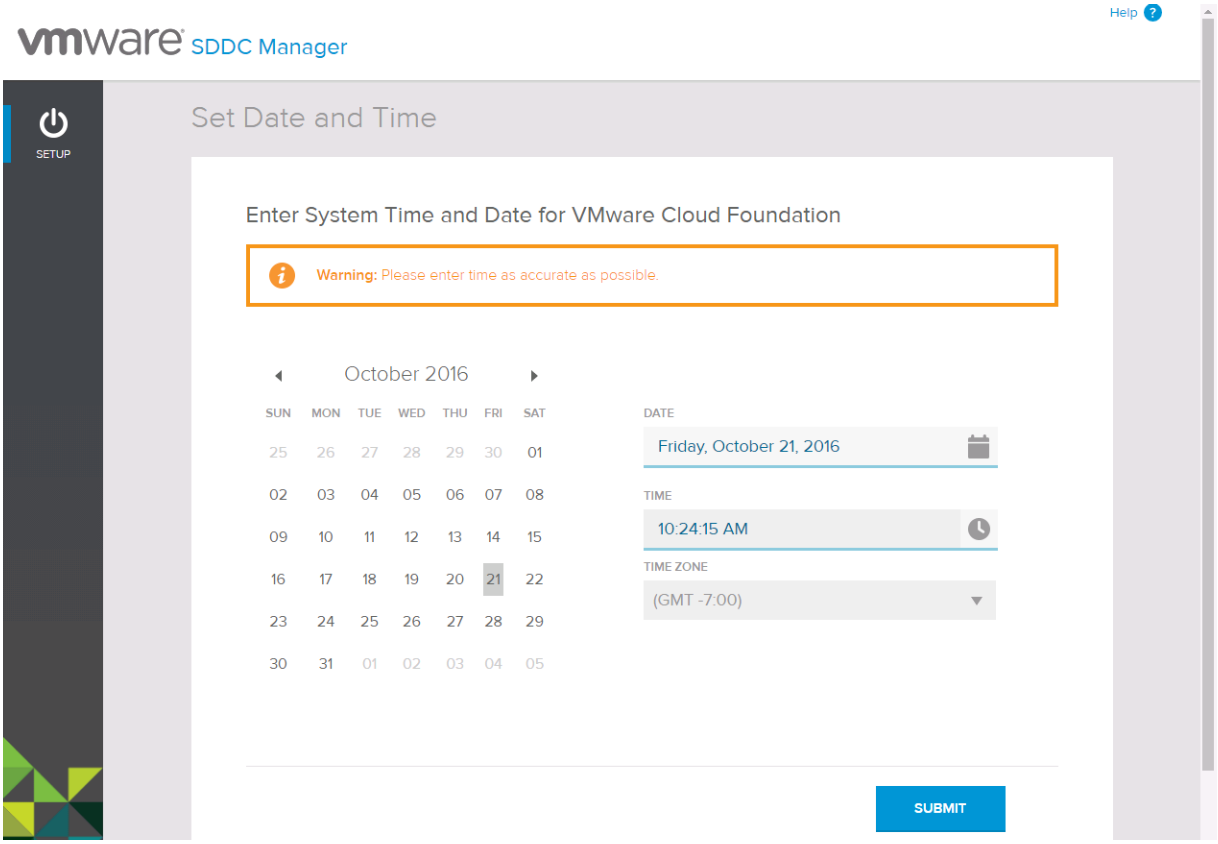


Welcome to VMware Cloud Foundation™

Let's get started building your private cloud.

3 Click **SET TIME**.

The System Time for VMware Cloud Foundation page appears.



Set Date and Time

Enter System Time and Date for VMware Cloud Foundation

Warning: Please enter time as accurate as possible.

October 2016

SUN	MON	TUE	WED	THU	FRI	SAT
25	26	27	28	29	30	01
02	03	04	05	06	07	08
09	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	01	02	03	04	05

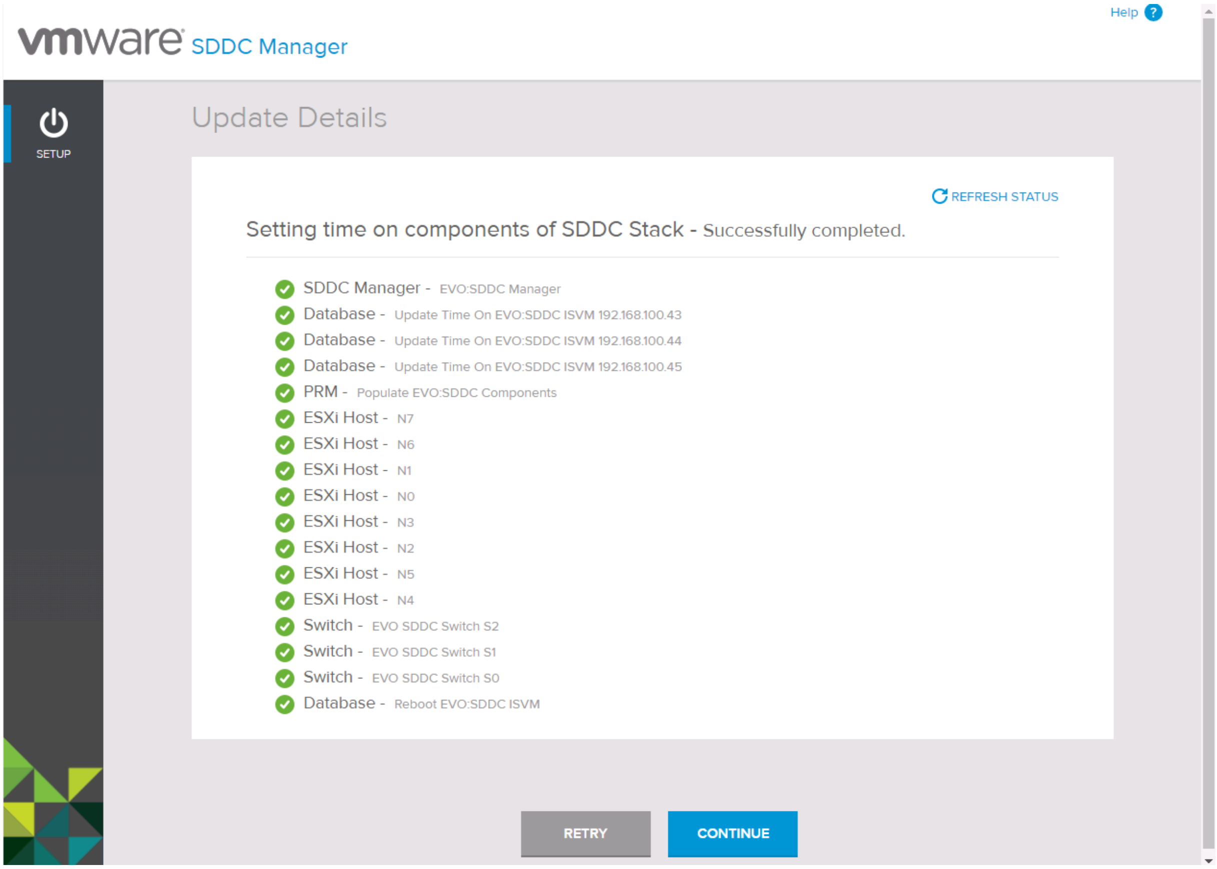
DATE: Friday, October 21, 2016

TIME: 10:24:15 AM

TIME ZONE: (GMT -7:00)

4 Specify the date, time, and time zone for the rack and click **Submit**. The specified time should match the current time in your environment.

All the physical components in the environment are synchronised. After the time has been set on all Cloud Foundation components, the SDDC Manager ISVMs are rebooted and the **CONTINUE** button turns blue.

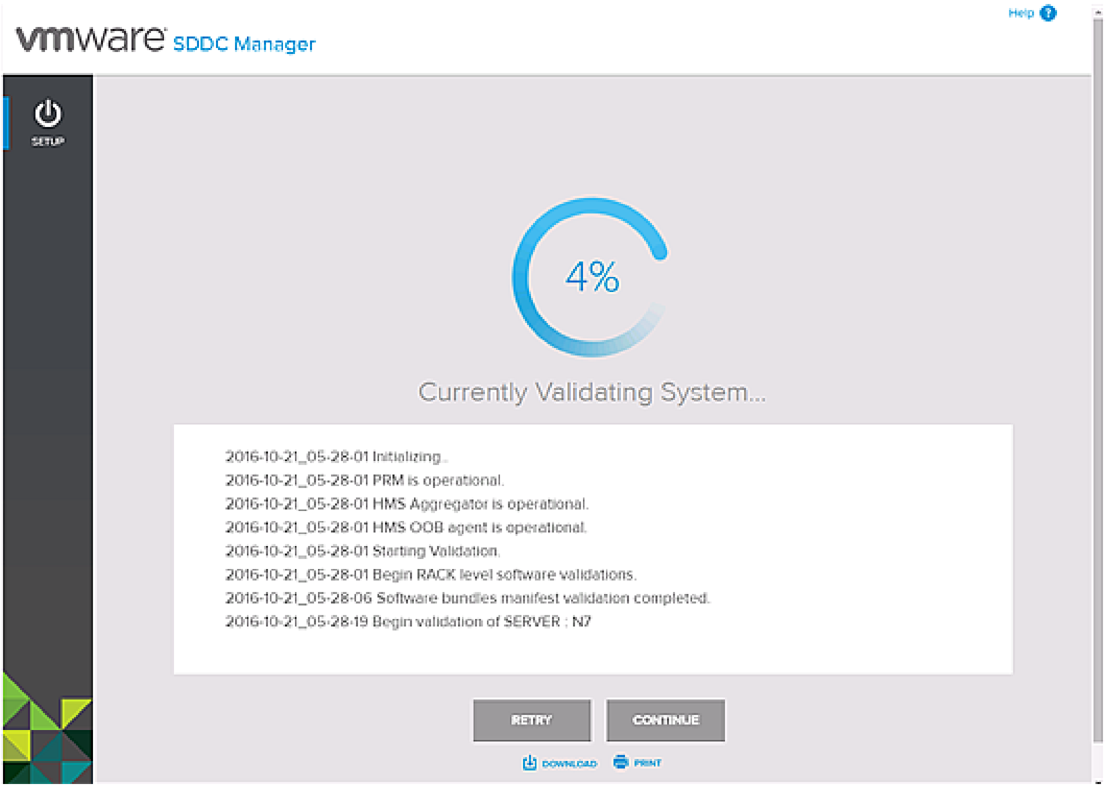


Setting time on components of SDDC Stack - Successfully completed.

- ✓ SDDC Manager - EVO:SDDC Manager
- ✓ Database - Update Time On EVO:SDDC ISVM 192.168.100.43
- ✓ Database - Update Time On EVO:SDDC ISVM 192.168.100.44
- ✓ Database - Update Time On EVO:SDDC ISVM 192.168.100.45
- ✓ PRM - Populate EVO:SDDC Components
- ✓ ESXi Host - N7
- ✓ ESXi Host - N6
- ✓ ESXi Host - N1
- ✓ ESXi Host - N0
- ✓ ESXi Host - N3
- ✓ ESXi Host - N2
- ✓ ESXi Host - N5
- ✓ ESXi Host - N4
- ✓ Switch - EVO SDDC Switch S2
- ✓ Switch - EVO SDDC Switch S1
- ✓ Switch - EVO SDDC Switch S0
- ✓ Database - Reboot EVO:SDDC ISVM

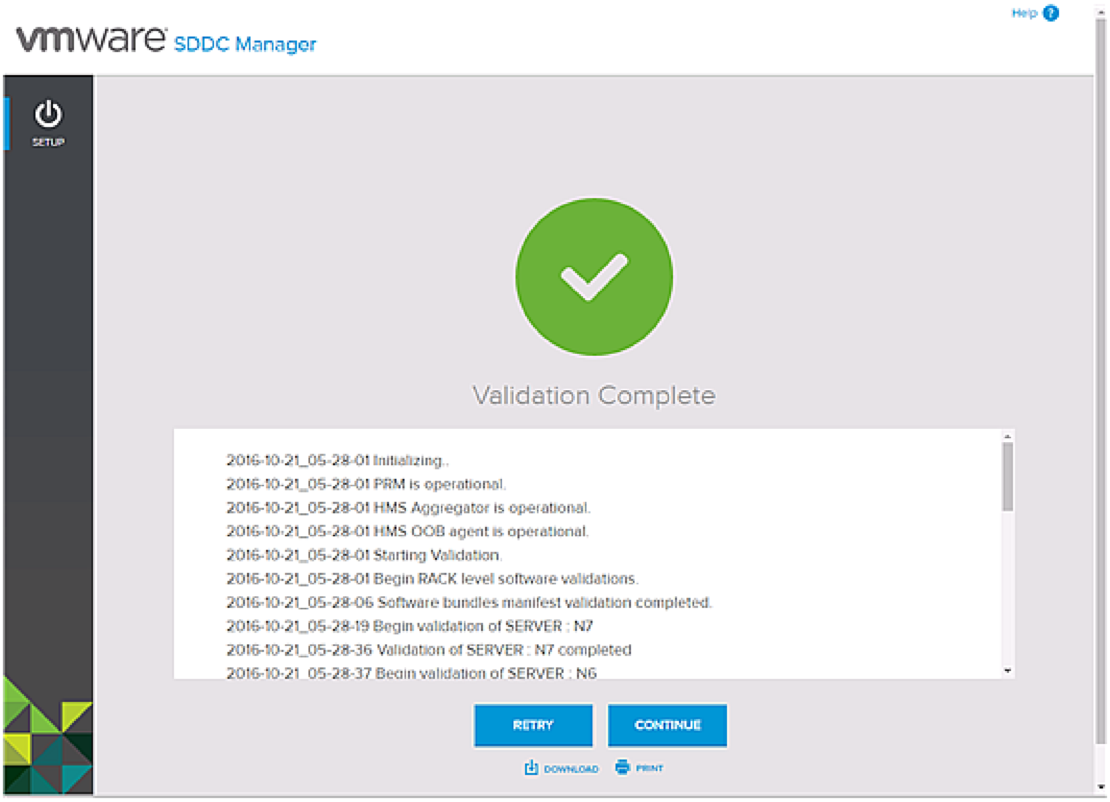
5 Click **CONTINUE**.

The system performs Power On Self Validation (POSV), where it verifies that all the physical components are operational. This includes verifying that everything in the inventory is present, the hardware is healthy, and ensuring that the necessary services are running.



Currently Validating System...

```
2016-10-21_05-28-01 Initializing..
2016-10-21_05-28-01 PRM is operational.
2016-10-21_05-28-01 HMS Aggregator is operational.
2016-10-21_05-28-01 HMS OOB agent is operational.
2016-10-21_05-28-01 Starting Validation.
2016-10-21_05-28-01 Begin RACK level software validations.
2016-10-21_05-28-06 Software bundles manifest validation completed.
2016-10-21_05-28-19 Begin validation of SERVER : N7
```



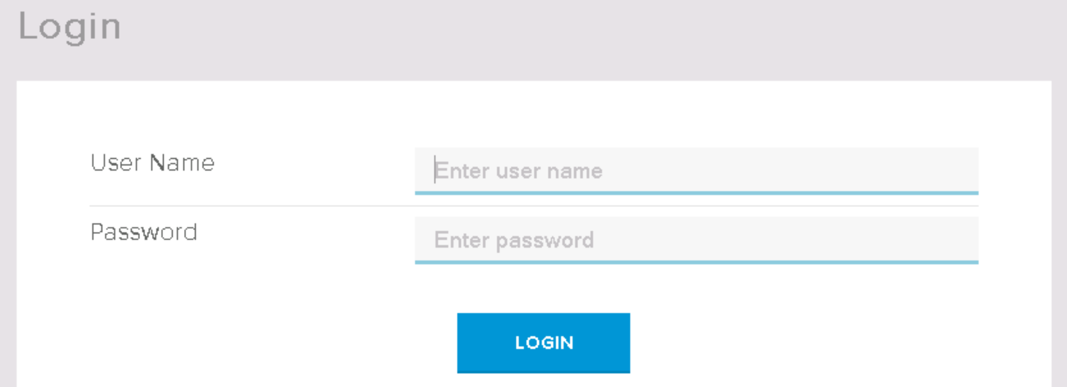
Validation Complete

```
2016-10-21_05-28-01 Initializing..
2016-10-21_05-28-01 PRM is operational.
2016-10-21_05-28-01 HMS Aggregator is operational.
2016-10-21_05-28-01 HMS OOB agent is operational.
2016-10-21_05-28-01 Starting Validation.
2016-10-21_05-28-01 Begin RACK level software validations.
2016-10-21_05-28-06 Software bundles manifest validation completed.
2016-10-21_05-28-19 Begin validation of SERVER : N7
2016-10-21_05-28-36 Validation of SERVER : N7 completed
2016-10-21_05-28-37 Begin validation of SERVER : N6
```

If the validation page displays an error, ensure that all physical connections are in place. Then click **RETRY**.

6 After the validation is complete, click **CONTINUE**.

The Login page appears.



7 Type the default credentials:

User name: **`administrator@vsphere.local`**

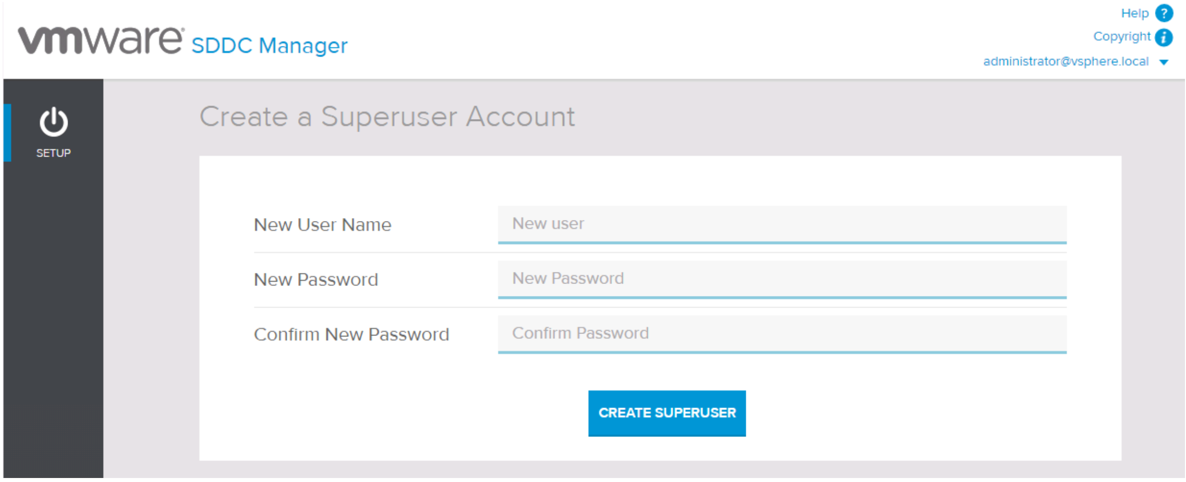
Password: **`vmware123`**

8 Click **LOGIN**.

The Cloud Foundation End User License Agreement (EULA) page appears.

9 Click **AGREE**.

The Create a Superuser Account page appears.



10 Type a user name and password for the superuser.

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

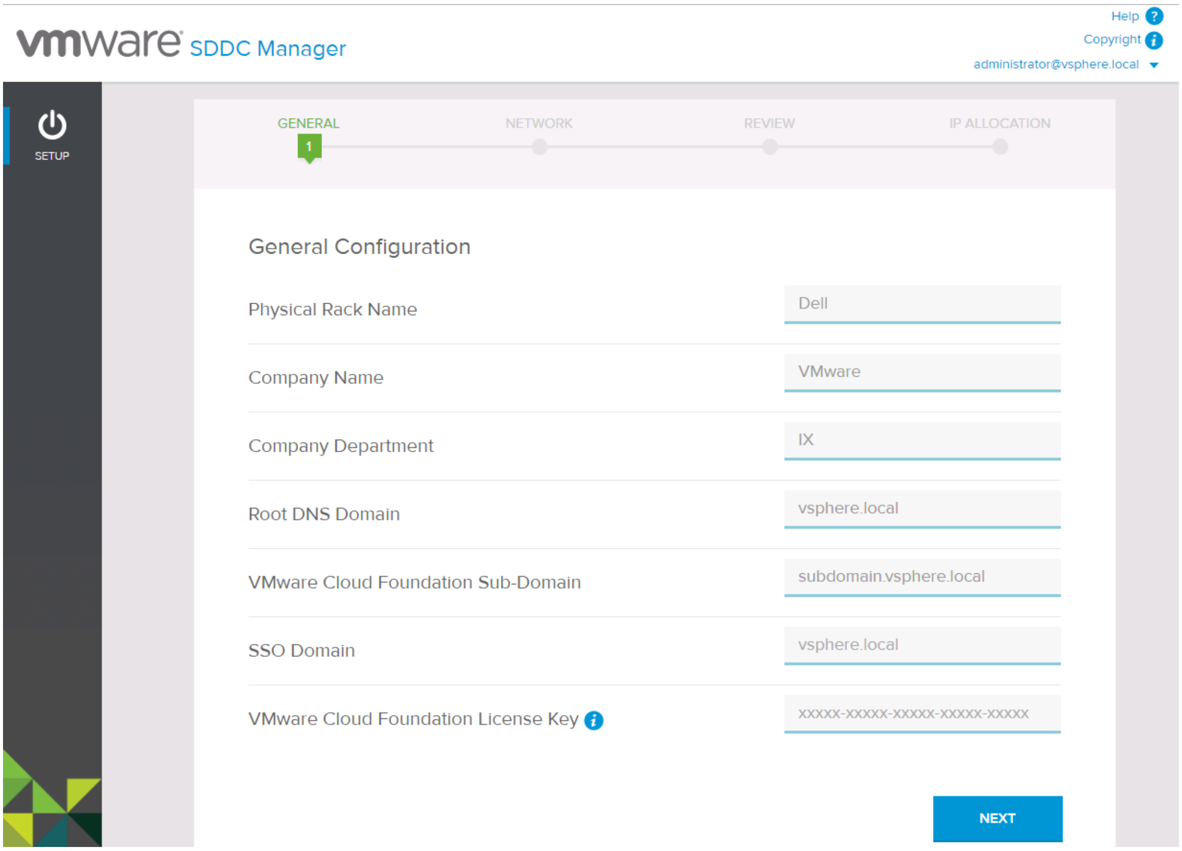
- lowercase letter
- uppercase letter
- number

- special character such as ! or @

The superuser 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 superuser account does not change. You can, thus, login to SDDC Manager with the superuser user name and password without having to look up the rotated password for the administrator account.

11 Click **CREATE SUPERUSER**.

The Initial Setup wizard appears.



General Configuration

Physical Rack Name	Dell
Company Name	VMware
Company Department	IX
Root DNS Domain	vsphere.local
VMware Cloud Foundation Sub-Domain	subdomain.vsphere.local
SSO Domain	vsphere.local
VMware Cloud Foundation License Key	XXXXX-XXXXX-XXXXX-XXXXX-XXXXX

12 On the General information page, enter the following information.

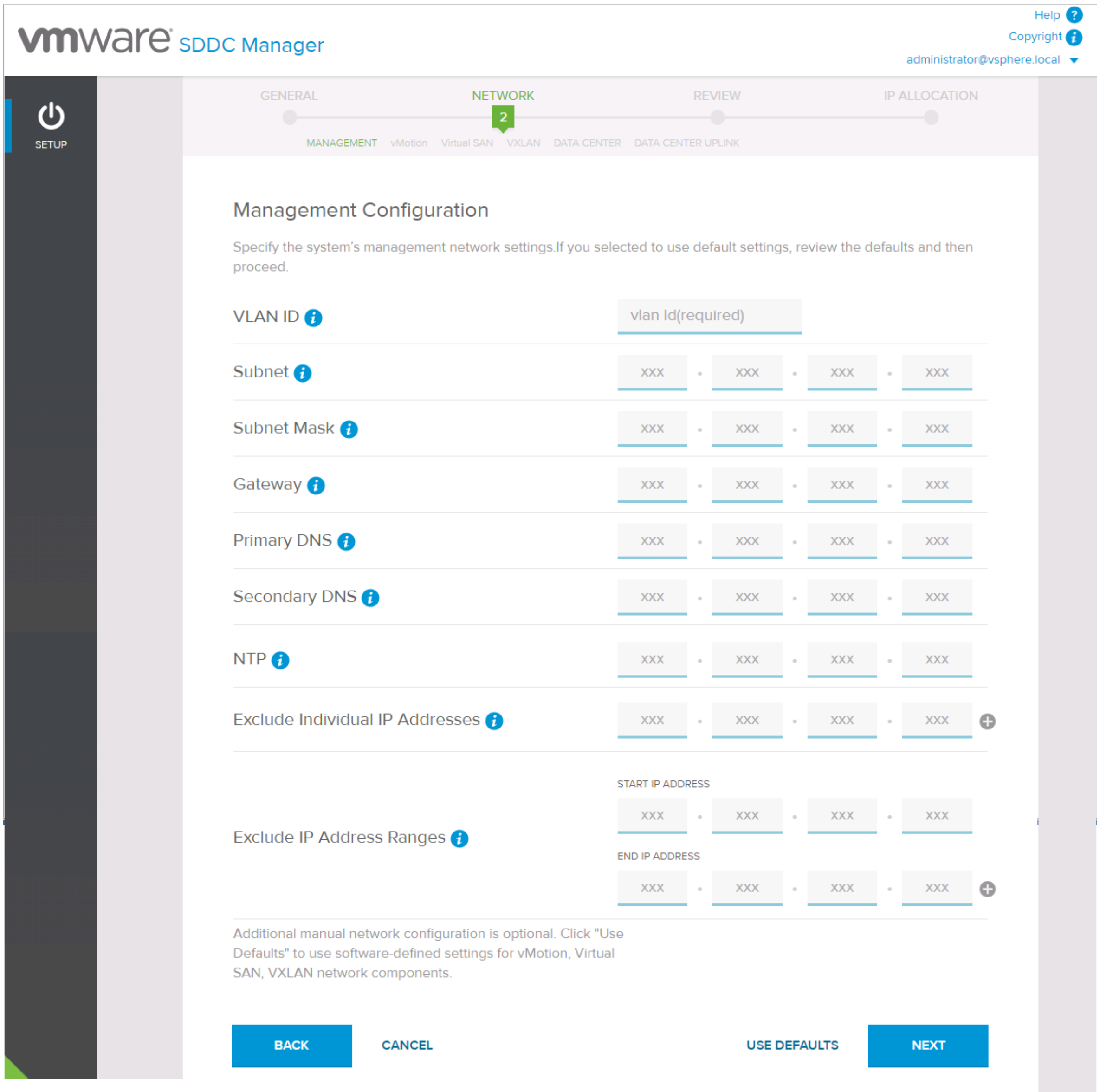
Field Name	Description
vRack Name	Name of the virtual rack
Company Name	Your company name
Company Department	Your department name
Root Domain	Type your root DNS domain (for example, vmware.corp). This should be the same as the Active Directory domain.

Field Name	Description
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 mycompany.example, the subdomain is auto-populated as subdomain.mycompany.example. You can edit this field. The sub domain is used for all components in Cloud Foundation. So everything is named *component*.subdomain. Based on our example, the NSX VM would be named rack-1-nsxmanager-1.subdomain.vmware.com.
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	Type the license key for Cloud Foundation. If you do not have the license key now, you can enter it later on the Cloud Foundation dashboard.

Joining Active Directory during Cloud Foundation bring-up can fail because of unconfigured or mis-configured uplinks, mis-configured upstream firewall, or incorrect corporate DNS configuration. After bring-up, you must identify and correct the cause of the failure. You can then manually connect each PSC to Active Directory. See *ESXi and vCenter Server 6.0 Documentation*.

13 Click **NEXT**.

The Management Configuration page appears. You now provide network information such as the VLAN identifier and IP subnets for the management, vMotion, Virtual SAN, and VXLAN networks. The VLAN IDs you specify here are pre-configured on the physical switch infrastructure.



Management Configuration

Specify the system's management network settings.If you selected to use default settings, review the defaults and then proceed.

VLAN ID: vlan Id(required)

Subnet: xxx . xxx . xxx . xxx

Subnet Mask: xxx . xxx . xxx . xxx

Gateway: xxx . xxx . xxx . xxx

Primary DNS: xxx . xxx . xxx . xxx

Secondary DNS: xxx . xxx . xxx . xxx

NTP: xxx . xxx . xxx . xxx

Exclude Individual IP Addresses: xxx . xxx . xxx . xxx

Exclude IP Address Ranges:
START IP ADDRESS: xxx . xxx . xxx . xxx
END IP ADDRESS: xxx . xxx . xxx . xxx

Additional manual network configuration is optional. Click "Use Defaults" to use software-defined settings for vMotion, Virtual SAN, VXLAN network components.

The following VLANs are configured while setting up networks for the bring-up phase:

a management

b vMotion

c vSAN

d VXLAN

e datacenter (corporate) network

The management and datacenter upstream networks are routable to the datacenter. The vMotion, VSAN, and VXLAN networks are routable only within Cloud Foundation.

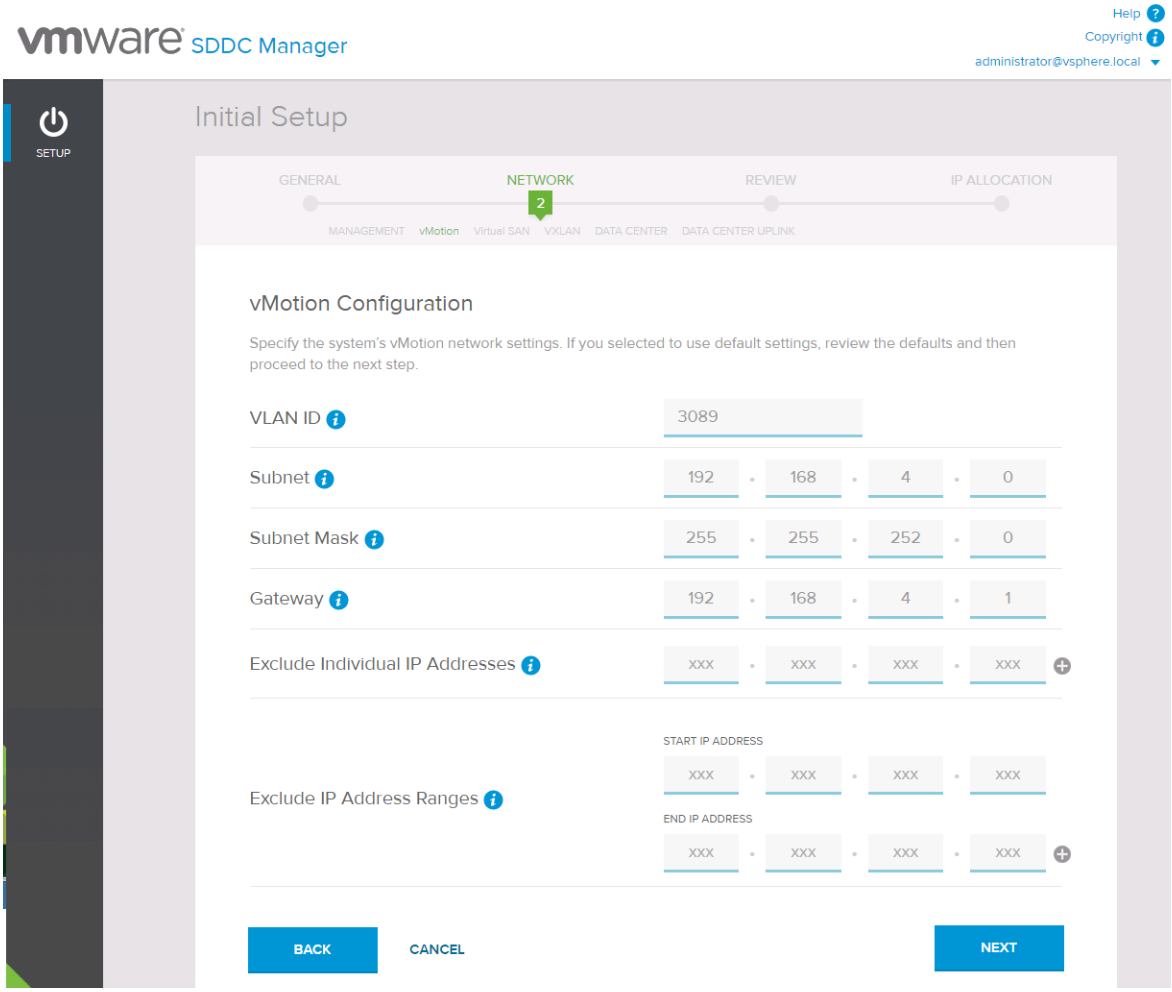
Note that there is a progress bar at the top of the page. To make any changes to a previous screen, click the appropriate page title. After making a change, you must click **NEXT** for the change to take effect.

14 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 21-3299.
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.
DNS	DNS of your datacenter.
NTP	NTP of your datacenter.
Exclude Individual IP Addresses	Enter a set of IP addresses to exclude from the provisioning process. For example, you can exclude those IP addresses that are already assigned to your network availability services such as HSRP. To add multiple addresses, type an IP address, click the + sign, and type the next IP address.
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.

15 Click **USE DEFAULTS** to allow Cloud Foundation to specify system generated IP address ranges for vMOTION, vSAN, and VXLAN. Since the Cloud Foundation network is an enclosed ecosystem, it is recommended that you select this option.

16 Click **NEXT**.

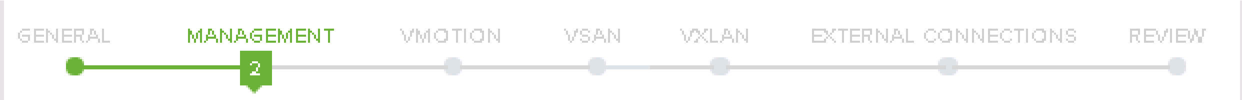


vMotion Configuration

Specify the system's vMotion network settings. If you selected to use default settings, review the defaults and then proceed to the next step.

VLAN ID	3089			
Subnet	192	168	4	0
Subnet Mask	255	255	252	0
Gateway	192	168	4	1
Exclude Individual IP Addresses	xxx	xxx	xxx	xxx
Exclude IP Address Ranges: START IP ADDRESS	xxx	xxx	xxx	xxx
END IP ADDRESS	xxx	xxx	xxx	xxx

The progress bar is displayed with additional wizard steps.



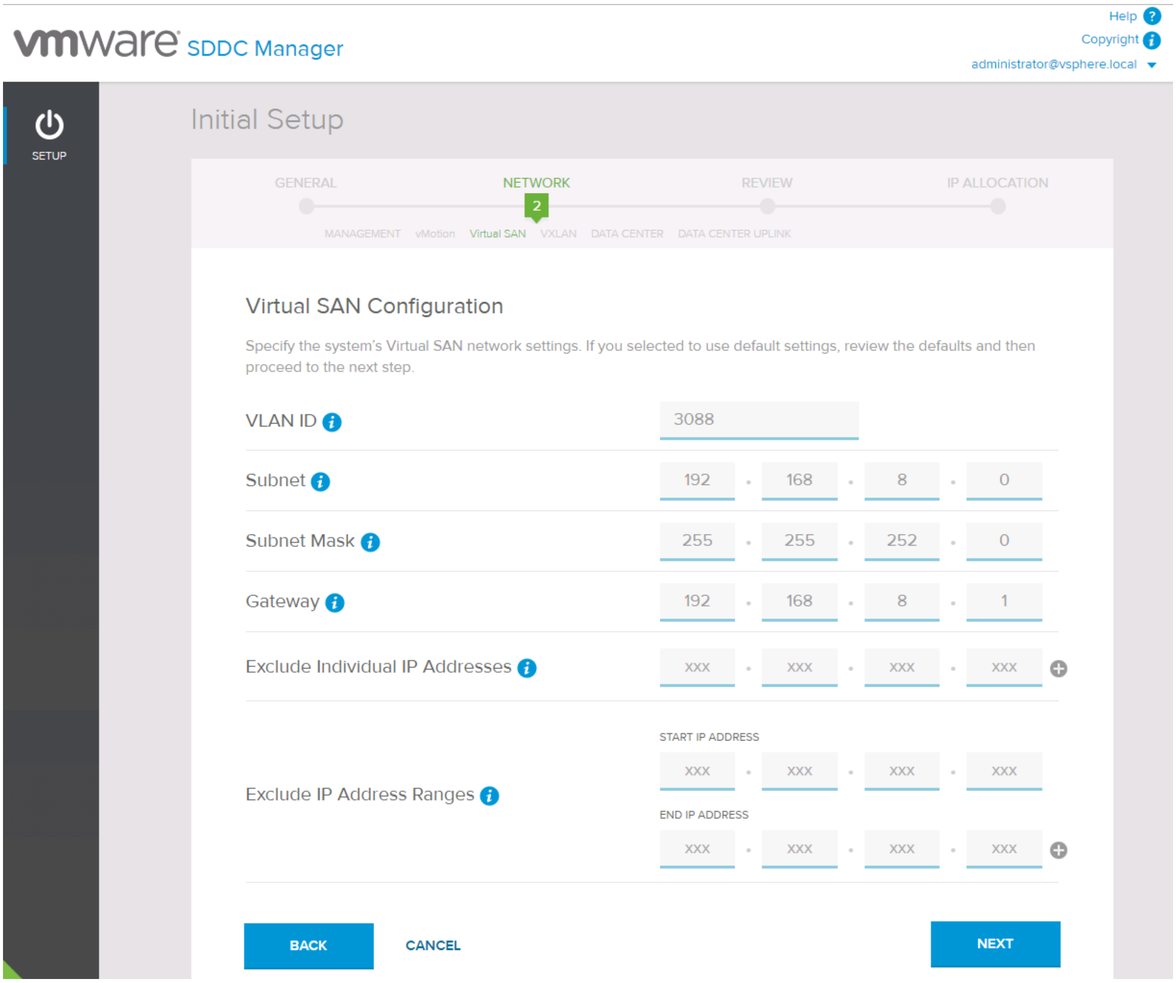
To make any changes to a previous screen, click the appropriate page title. After making a change, you must click **NEXT** for the change to take effect.

17 On the vMotion Configuration page, 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 21-3299. 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.

18 Click **NEXT**.

The VSAN information page appears.



Initial Setup

GENERAL — NETWORK 2 — REVIEW — IP ALLOCATION

MANAGEMENT · vMotion · Virtual SAN · VXLAN · DATA CENTER · DATA CENTER UPLINK

Virtual SAN Configuration

Specify the system's Virtual SAN network settings. If you selected to use default settings, review the defaults and then proceed to the next step.

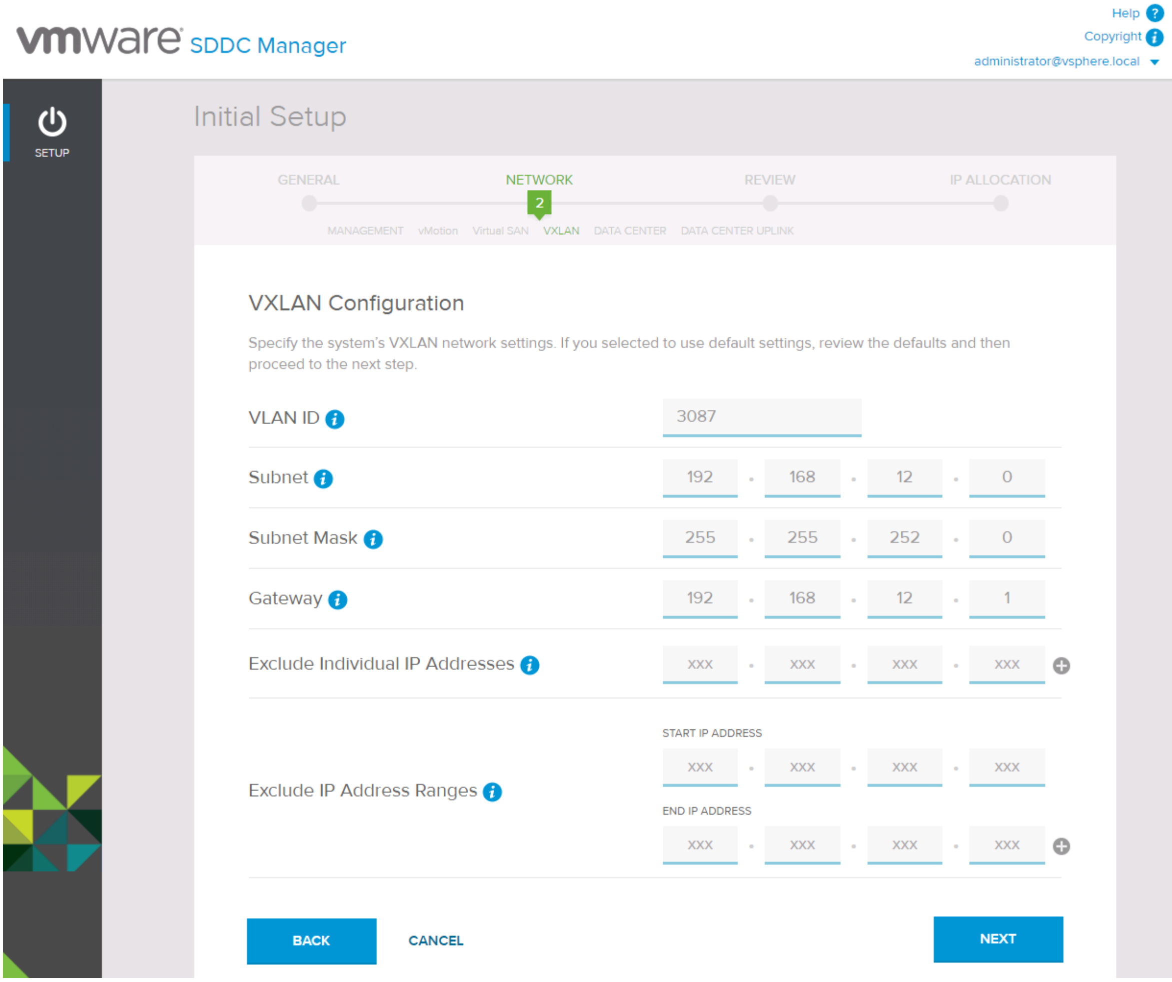
VLAN ID	3088
Subnet	192 . 168 . 8 . 0
Subnet Mask	255 . 255 . 252 . 0
Gateway	192 . 168 . 8 . 1
Exclude Individual IP Addresses	xxx . xxx . xxx . xxx
Exclude IP Address Ranges	START IP ADDRESS xxx . xxx . xxx . xxx END IP ADDRESS xxx . xxx . xxx . xxx

19 On the VSAN Information page, review or enter your Virtual SAN network addresses for the VLAN, Subnet, Subnet Mask, Gateway, and excluded IP addresses and IP address ranges..

Note The supported VLAN range is 21-3299. 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.

20 Click **NEXT**.

The VXLAN information page appears.



Initial Setup

VXLAN Configuration

Specify the system's VXLAN network settings. If you selected to use default settings, review the defaults and then proceed to the next step.

VLAN ID: 3087

Subnet: 192 . 168 . 12 . 0

Subnet Mask: 255 . 255 . 252 . 0

Gateway: 192 . 168 . 12 . 1

Exclude Individual IP Addresses: xxx . xxx . xxx . xxx

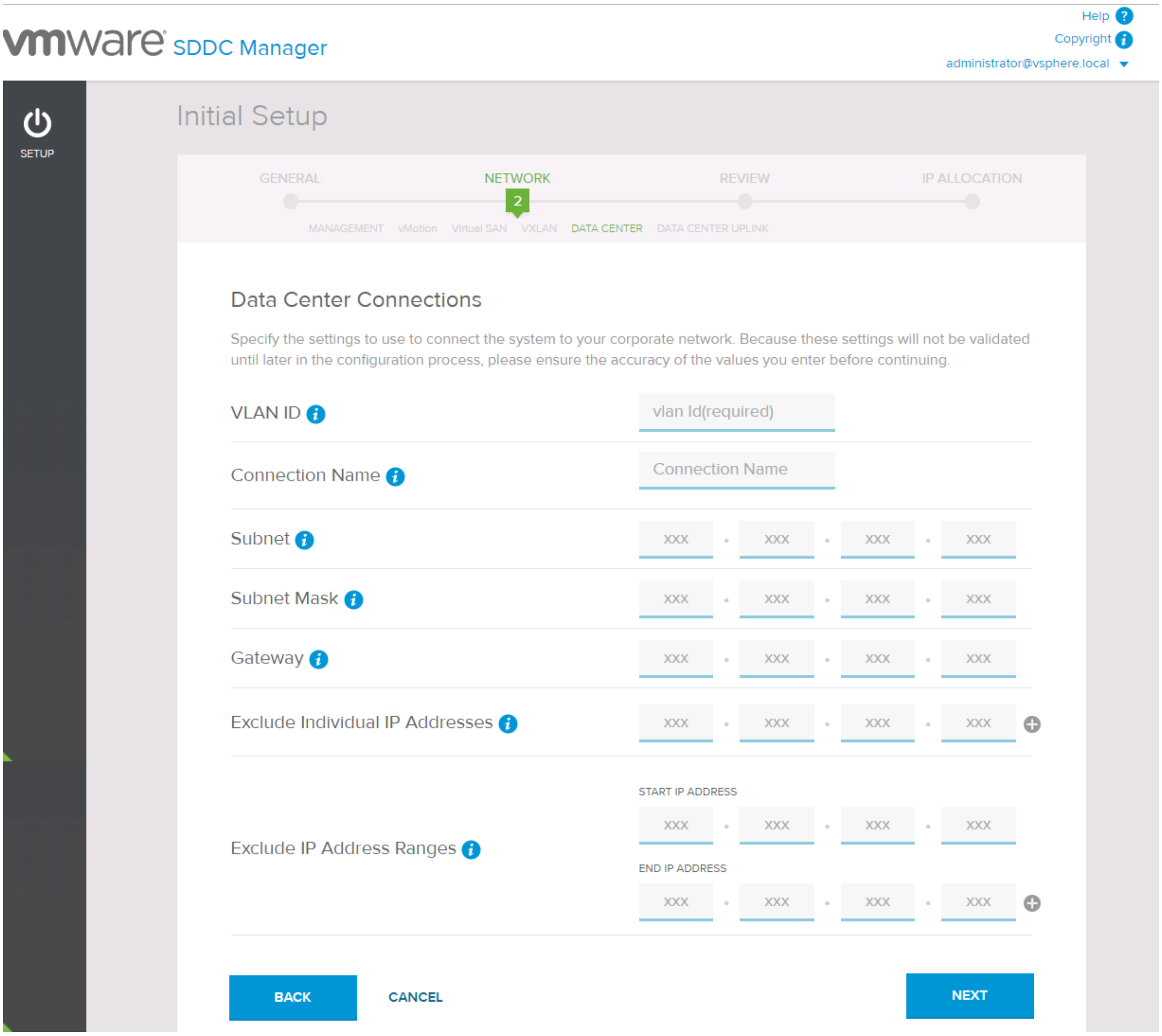
Exclude IP Address Ranges:
START IP ADDRESS: xxx . xxx . xxx . xxx
END IP ADDRESS: xxx . xxx . xxx . xxx

21 On the VXLAN information page, review or enter your VXLAN information for the VLAN ID, Subnet, Subnet Mask, Gateway, and excluded IP addresses and IP address ranges..

Note The supported VLAN range is 21-3299. 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.

22 Click **NEXT**.

The Data Center connections page appears.



Initial Setup

Data Center Connections

Specify the settings to use to connect the system to your corporate network. Because these settings will not be validated until later in the configuration process, please ensure the accuracy of the values you enter before continuing.

VLAN ID: vlan Id(required)

Connection Name: Connection Name

Subnet: xxx . xxx . xxx . xxx

Subnet Mask: xxx . xxx . xxx . xxx

Gateway: xxx . xxx . xxx . xxx

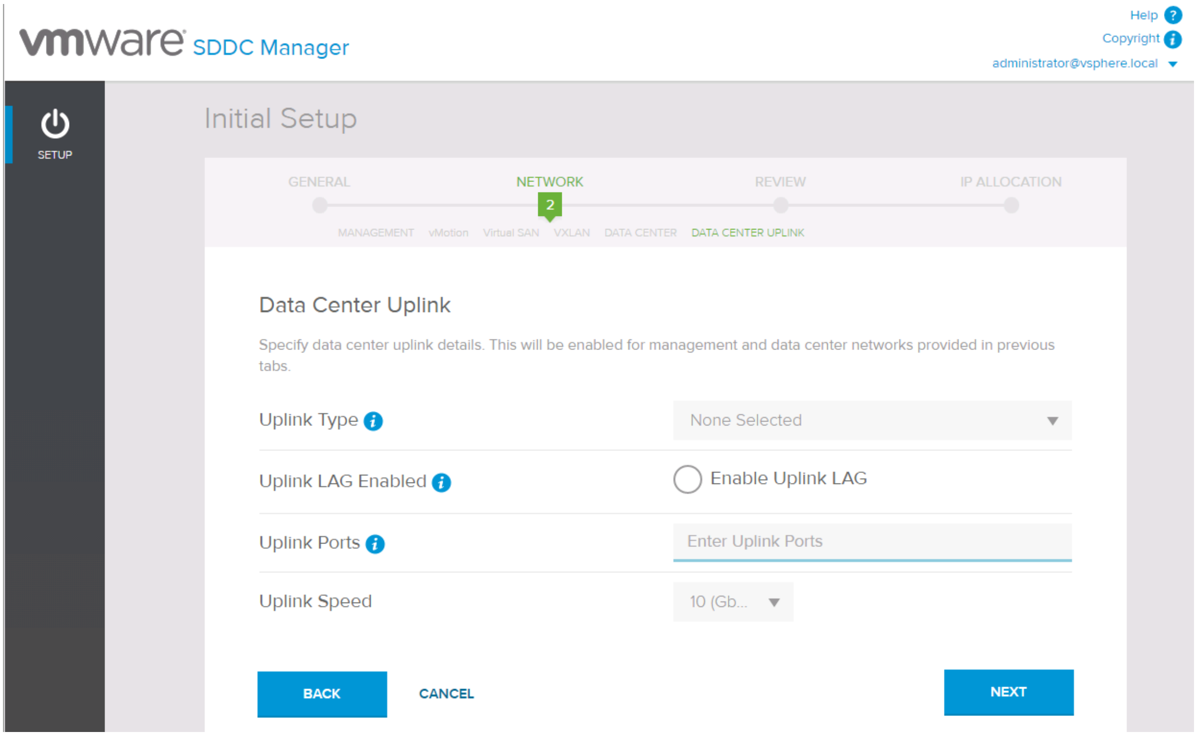
Exclude Individual IP Addresses: xxx . xxx . xxx . xxx

Exclude IP Address Ranges:
START IP ADDRESS: xxx . xxx . xxx . xxx
END IP ADDRESS: xxx . xxx . xxx . xxx

23 The Data Center Connections page contains information for Cloud Foundation to connect to your corporate network. Enter your corporate network information for the VLAN ID, Connection Name, Network Start IP, Subnet Mask, Gateway, DNS, NTP, and excluded IP addresses and IP address ranges.

Important Review these values carefully before clicking **NEXT** because external connections are not validated at this time.

The Data Center Uplink page appears.



Data Center Uplink

Specify data center uplink details. This will be enabled for management and data center networks provided in previous tabs.

Uplink Type: None Selected

Uplink LAG Enabled: ○ Enable Uplink LAG

Uplink Ports: Enter Uplink Ports

Uplink Speed: 10 (Gb...

24 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.
`Uplink Speed`	Speed for uplink connections.

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

Field	Description
`Uplink Type`	L3
`Uplink LAG Enabled`	It is recommended that you select this option.

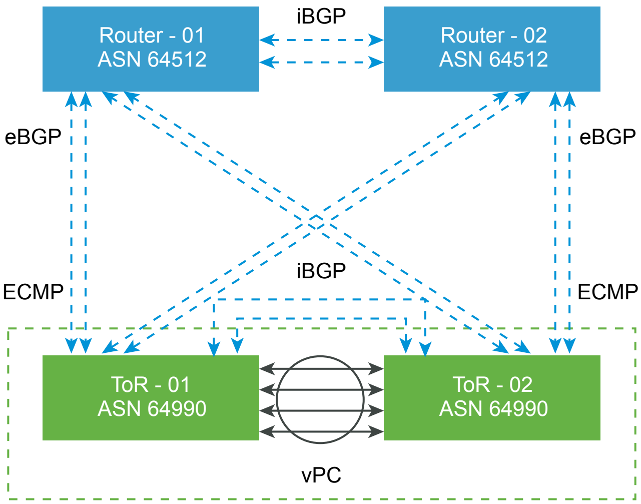
Field	Description
`Uplink Ports`	Port numbers on the ToR switches that are connected to the uplink network.
`Uplink Speed`	Speed for uplink connections.
`Uplink IP`	IP address of the uplink IP on the ToR switches.
`Mask IP`	Subnet mask for the uplink IP.
`Next Hop IP`	IP address of the uplink switch for the data center.

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

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.

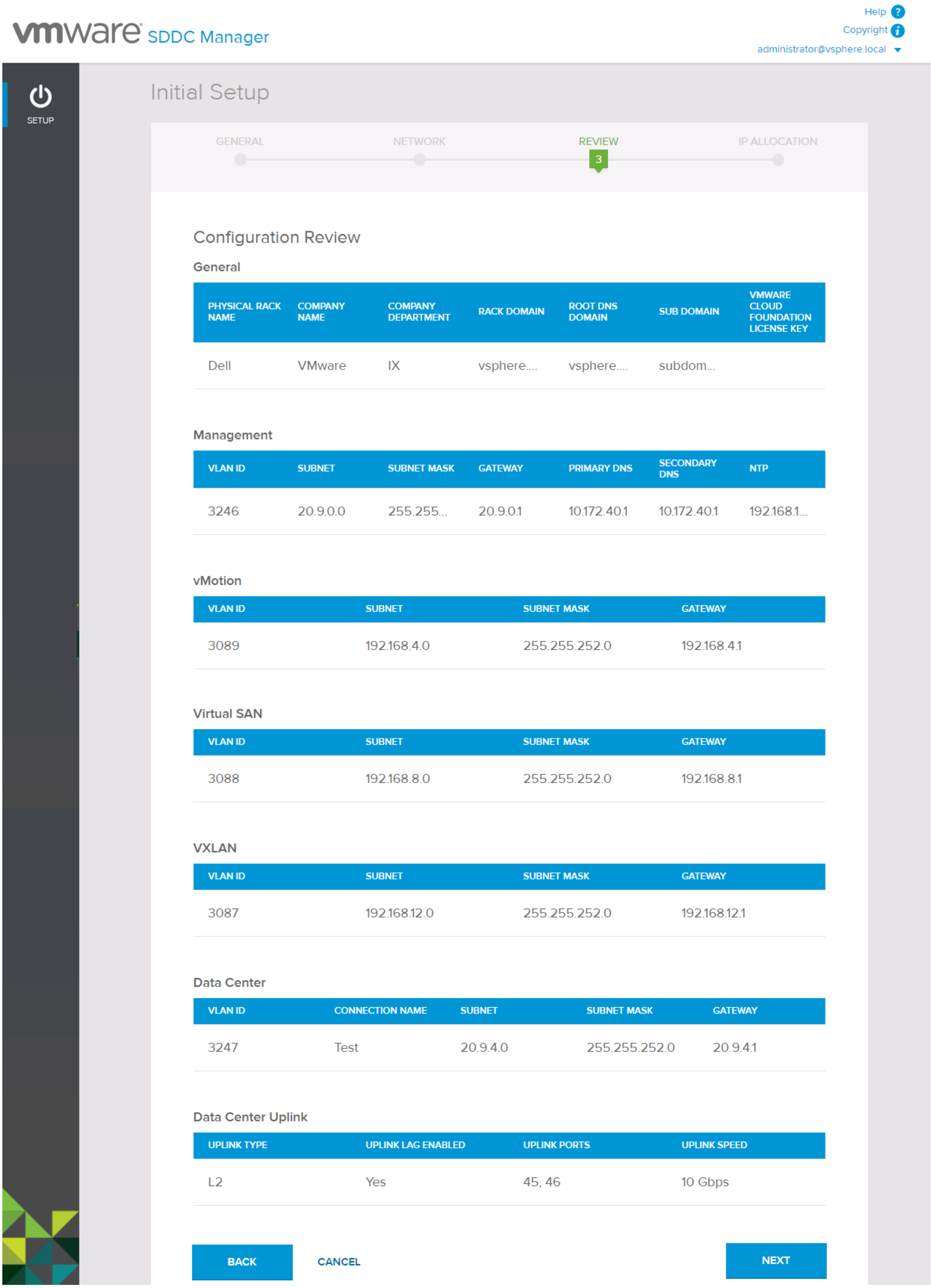
It is recommended that you set up iBGP between the ToR switches and an eBGP between each ToR switch and the upstream router. This not automated. For information on the required configuration, see Chapter 9 Example ToR Switch Output for L3 Configuration on Cisco ToR Switches (9372).

Figure 4-1. L3 Configuration



26 Click **NEXT**.

The Configuration Review page appears.



Configuration Review

General

PHYSICAL RACK NAME	COMPANY NAME	COMPANY DEPARTMENT	RACK DOMAIN	ROOT DNS DOMAIN	SUB DOMAIN	VMWARE CLOUD FOUNDATION LICENSE KEY
Dell	VMware	IX	vsphere....	vsphere....	subdom...	

Management

VLAN ID	SUBNET	SUBNET MASK	GATEWAY	PRIMARY DNS	SECONDARY DNS	NTP
3246	20.9.0.0	255.255...	20.9.0.1	10.172.40.1	10.172.40.1	192.168.1...

vMotion

VLAN ID	SUBNET	SUBNET MASK	GATEWAY
3089	192.168.4.0	255.255.252.0	192.168.4.1

Virtual SAN

VLAN ID	SUBNET	SUBNET MASK	GATEWAY
3088	192.168.8.0	255.255.252.0	192.168.8.1

VXLAN

VLAN ID	SUBNET	SUBNET MASK	GATEWAY
3087	192.168.12.0	255.255.252.0	192.168.12.1

Data Center

VLAN ID	CONNECTION NAME	SUBNET	SUBNET MASK	GATEWAY
3247	Test	20.9.4.0	255.255.252.0	20.9.4.1

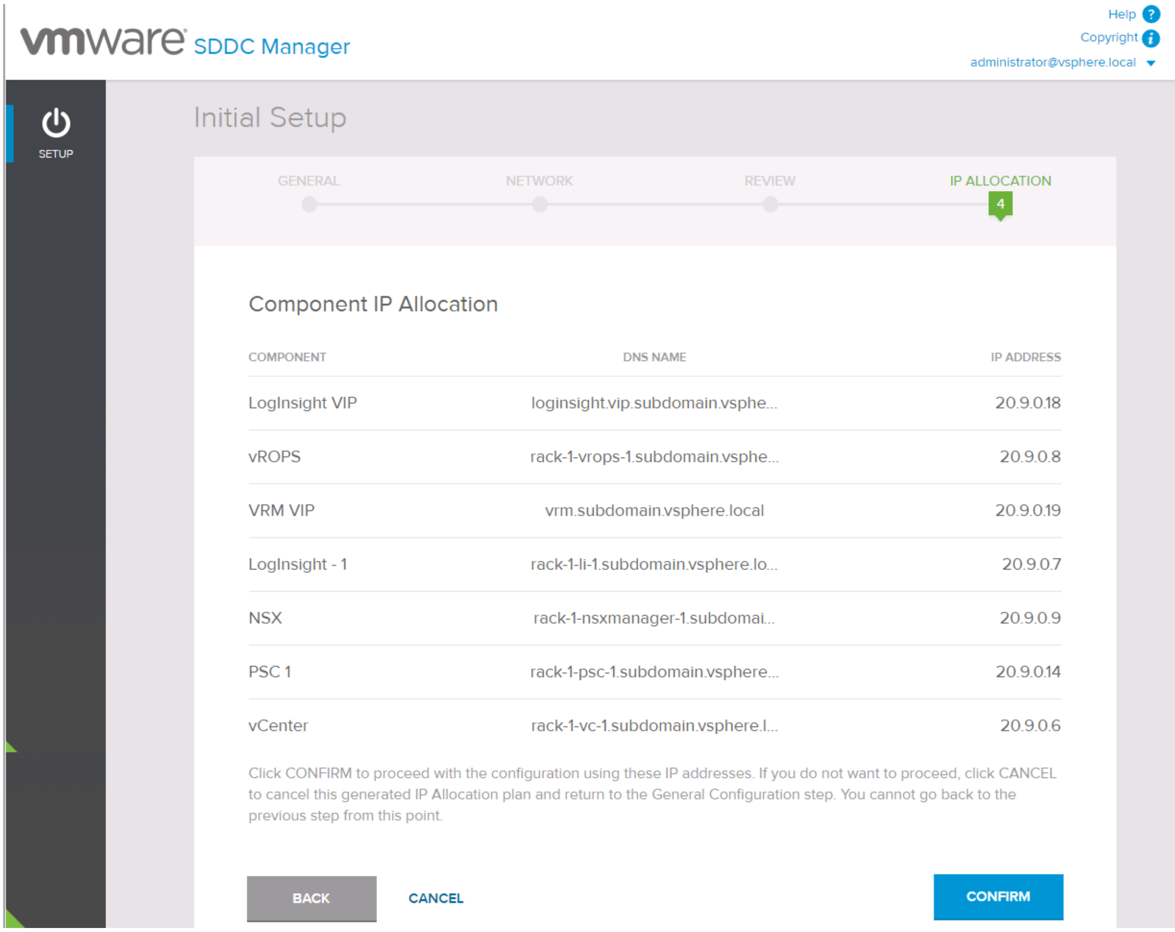
Data Center Uplink

UPLINK TYPE	UPLINK LAG ENABLED	UPLINK PORTS	UPLINK SPEED
L2	Yes	45, 46	10 Gbps

27 On the Configuration Review page, review the information carefully.

28 After you ensure that all values on the Review page are accurate, click **NEXT**.

After a few moments, the Component IP Allocation page appears and displays the IP addresses for the VMs that will be deployed for the vRealize Log Insight, NSX, Platform Services Controller, SDDC Manager, vCenter Server, and vRealize Operations software components.



Component IP Allocation

COMPONENT	DNS NAME	IP ADDRESS
LogInsight VIP	loginsight.vip.subdomain.vsphe...	20.9.0.18
vROPS	rack-1-vrops-1.subdomain.vsphe...	20.9.0.8
VRM VIP	vrm.subdomain.vsphere.local	20.9.0.19
LogInsight - 1	rack-1-li-1.subdomain.vsphere.lo...	20.9.0.7
NSX	rack-1-nsxmanager-1.subdomai...	20.9.0.9
PSC 1	rack-1-psc-1.subdomain.vsphere...	20.9.0.14
vCenter	rack-1-vc-1.subdomain.vsphere.l...	20.9.0.6

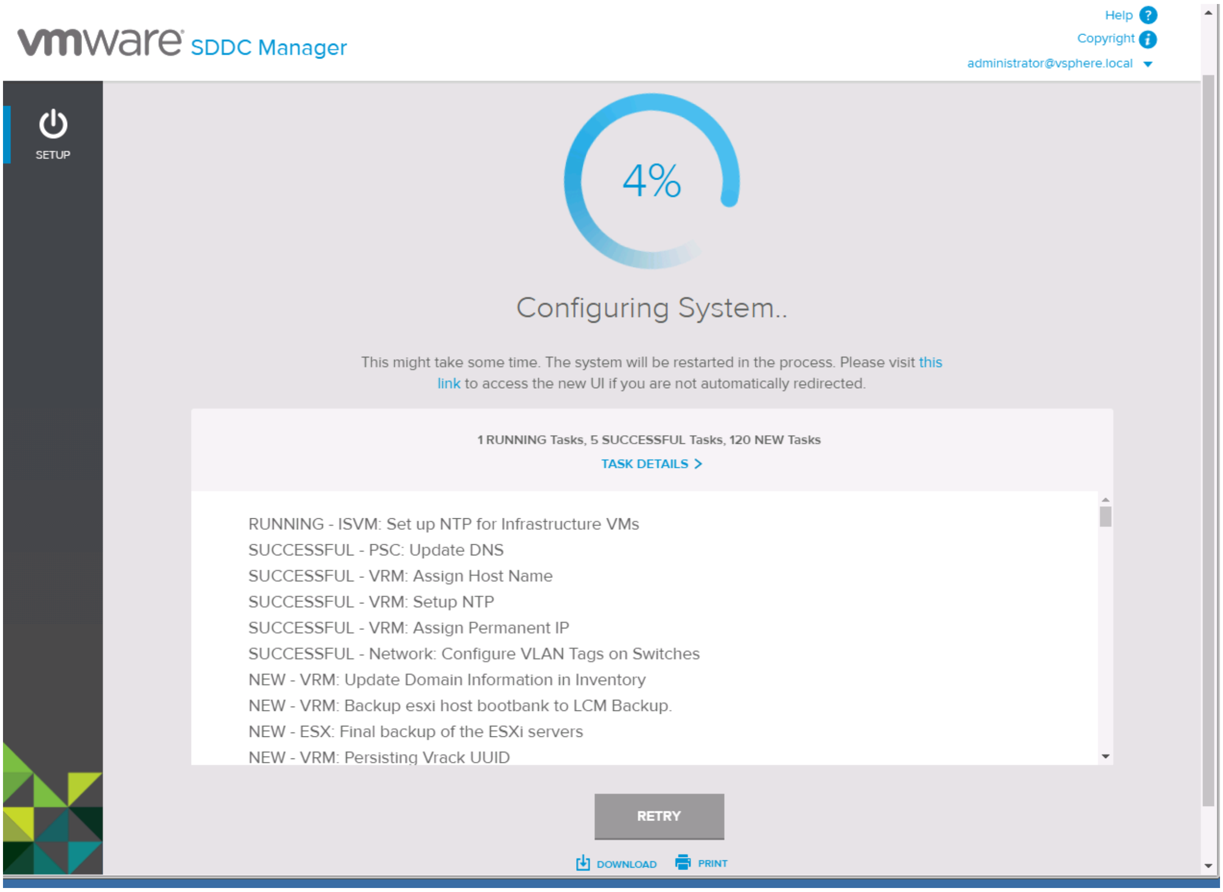
Click CONFIRM to proceed with the configuration using these IP addresses. If you do not want to proceed, click CANCEL to cancel this generated IP Allocation plan and return to the General Configuration step. You cannot go back to the previous step from this point.

If you need to make any change on the IP Reallocation page, click **CANCEL** to make edits as required.

29 Note down the virtual machine IP addresses. You will need these later in the bring-up process.

30 After you ensure that the IP Reallocation values are correct, click **CONFIRM**.

The Cloud Foundation configuration process begins. The amount of time it takes for the bring up process to be completed depends on the number of servers in the physical rack. The average time is approximately 90 minutes.



Configuring System..

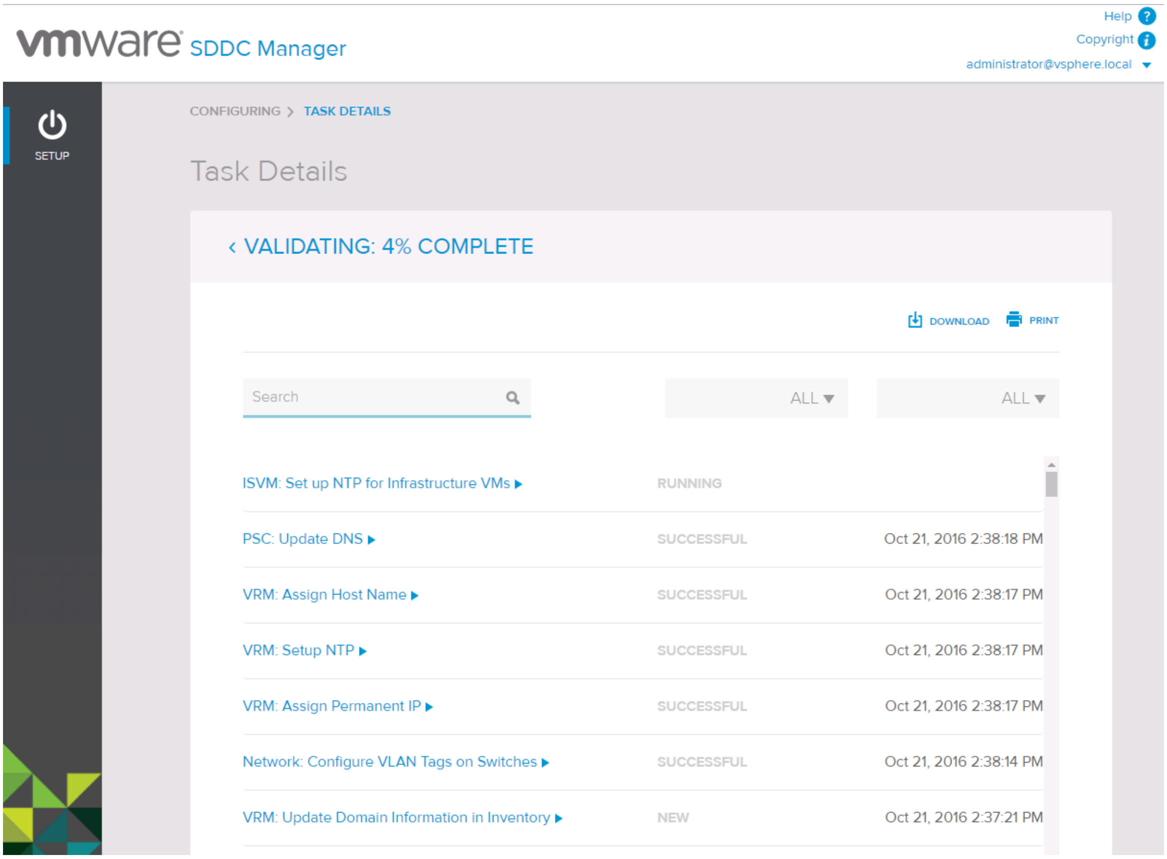
This might take some time. The system will be restarted in the process. Please visit this link to access the new UI if you are not automatically redirected.

1 RUNNING Tasks, 5 SUCCESSFUL Tasks, 120 NEW Tasks

TASK DETAILS >

```
RUNNING - ISVM: Set up NTP for Infrastructure VMs
SUCCESSFUL - PSC: Update DNS
SUCCESSFUL - VRM: Assign Host Name
SUCCESSFUL - VRM: Setup NTP
SUCCESSFUL - VRM: Assign Permanent IP
SUCCESSFUL - Network: Configure VLAN Tags on Switches
NEW - VRM: Update Domain Information in Inventory
NEW - VRM: Backup esxi host bootbank to LCM Backup.
NEW - ESX: Final backup of the ESXi servers
NEW - VRM: Persisting Vrack UUID
```

You can see progress on the individual tasks by clicking **Task Details**.



Task Details

VALIDATING: 4% COMPLETE

ISVM: Set up NTP for Infrastructure VMs ▶	RUNNING	
PSC: Update DNS ▶	SUCCESSFUL	Oct 21, 2016 2:38:18 PM
VRM: Assign Host Name ▶	SUCCESSFUL	Oct 21, 2016 2:38:17 PM
VRM: Setup NTP ▶	SUCCESSFUL	Oct 21, 2016 2:38:17 PM
VRM: Assign Permanent IP ▶	SUCCESSFUL	Oct 21, 2016 2:38:17 PM
Network: Configure VLAN Tags on Switches ▶	SUCCESSFUL	Oct 21, 2016 2:38:14 PM
VRM: Update Domain Information in Inventory ▶	NEW	Oct 21, 2016 2:37:21 PM

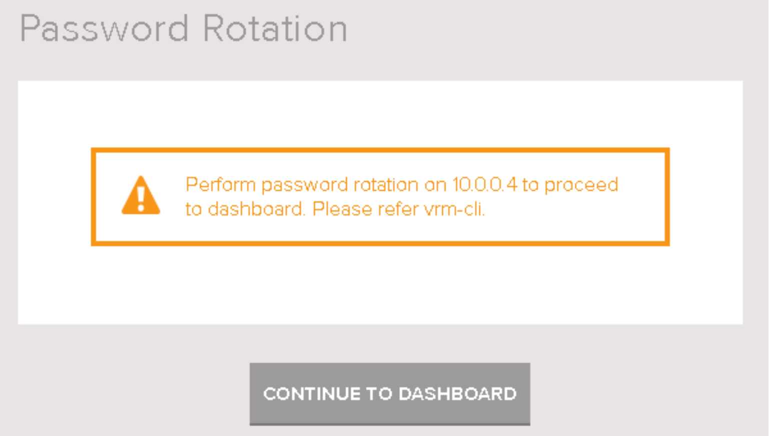
Expand the task by clicking the blue arrow to see additional information. You can filter the tasks by status or time.

If there is an error during the configuration of the system, an error page appears. Click **RETRY**. The configuration process remembers where it was in the sequence and start over from that point. If an error occurs even after you rerun, contact VMware Support.

After the system configuration is completed, the SDDC Manager is restarted and the login screen is displayed.

31 Login with your superuser credentials . When SDDC Manager comes up, the Password Rotation page is displayed. For information on rotating the system passwords, see Change Passwords of Rack Components

The **Continue to Dashboard** button is grayed out till password rotation is completed.



Password Rotation

Perform password rotation on 10.0.0.4 to proceed to dashboard. Please refer vrm-cli.

32 Note the IP address on the URL. If you accidentally close the browser, you will need this IP address to navigate to the Dashboard.

33 Leave this browser window open.

34 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 mycompany.example, and the Cloud Foundation Sub Domain is subdomain. mycompany.example, the corporate DNS server must be configured to delegate control of subdomain. mycompany.example 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 (mycompany.example) 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).

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.*Cloud_Foundation_Sub_Domain* (psc.subdomain. mycompany.example in our example).

Locate SDDC Manager IP Address

The SDDC Manager IP address changes during bring-up. You need to look up the new IP address so that you can log in to change the password on the rack components.

Procedure

1 Look up the vCenter Server IP address from the notes you took when the Component IP Allocation page of the Initial Setup wizard displayed the IP addresses allocated to the virtual machines.

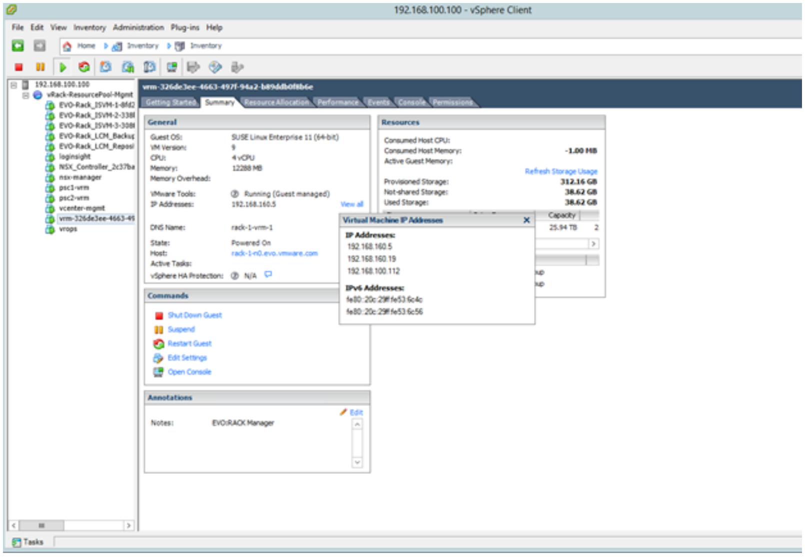
2 Login to this IP address via the vSphere Web Client. Use your superuser account credentials for the user name and password. Append `@vsphere.local` to the user name.

3 Navigate to the **Hosts and Clusters** view and click the SDDC Manager VM in the left pane. The name of the VM appears as **vrm-*UUID***.

4 On the right pane, click the **Summary** tab.

5 The **IP Address** field displays the SDDC Manager IP address.

\



General

Guest OS: SUSE Linux Enterprise 11 (64-bit)
VM Version: 9
CPU: 4 vCPU
Memory: 12288 MB
Memory Overhead:
VMware Tools: Running (Guest managed)
IP Addresses: 192.168.160.5
DNS Name: rack-1-vrm-1
State: Powered On
Host: rack-1-n0.evo.vmware.com
Active Tasks:
vSphere HA Protection: N/A

Resources

Consumed Host CPU:
Consumed Host Memory: -1.00 MB
Active Guest Memory:
Provisioned Storage: 312.16 GB
Not-shared Storage: 38.62 GB
Used Storage: 38.62 GB

Capacity
25.94 TB

Virtual Machine IP Addresses

IP Addresses:
192.168.160.5
192.168.160.19
192.168.100.112

IPv6 Addresses:
fe80::20c:29ff:fe53:6c4c
fe80::20c:29ff:fe53:6c56

Annotations

Notes: EVO:RACK Manager

6 Click **View all** to display all the IP addresses.

7 Identify the base IP addresses for SDDC Manager.

There are three IP addresses displayed for SDDC Manager. The IP address that was displayed for VRM on the IP Allocation page is the virtual IP (VIP) of the SDDC Manager. The other two IP addresses are the base addresses. The private IP address is the 192.168.100.*x*. You need a base IP address for password rotation because the VIP disappears when the vrm-tcserver service is shut down, which will make you lose connectivity when you shut down the service as required during password rotation.

Change Passwords of Rack Components

Cloud Foundation is deployed with factory default passwords. You must replace the default passwords with secure system generated passwords.

Note In a multi-rack setup, you must change the passwords on the first physical rack before bringing-up additional racks.

Prerequisites

You must have completed bring-up on the rack and the Password Rotation blocker screen must have been displayed.

Procedure

1 In a command line window, SSH as root to one of the base IP addresses for SDDC Manager on the rack. See Locate SDDC Manager IP Address.

2 Navigate to `/home/vrack/bin`.

3 Type the following command:

```
./vrm-cli.sh lookup-password
```

The output displays the passwords and IP addresses for all components.

4 Save the output to a secure location so that you can access it later.

5 Save a copy of the `/home/vrack/VMware/vRack/vrm.properties` file to a secure location where you can access it later.

6 In the SDDC Manager console window, navigate to `/home/vrack/bin`.

7 Type the following command:

```
./vrm-cli.sh rotate-all
```

This command changes the passwords of physical and logical components on the rack. Wait for 10 minutes before proceeding to the next step.

8 In the SDDC Manager console window, type the following command again:

```
./vrm-cli.sh lookup-password
```

Save the output. Compare the output file you saved in step 5 with the output file you saved now and ensure that all passwords have been changed. Note the password for the administrator account, which you will need for logging in to the Cloud Foundation dashboard.

9 Refresh the browser window where you were running the Initial Setup wizard.

The **Continue to Dashboard** button is now green. Click this button to display the Cloud Foundation Dashboard.

10 Log out of the Dashboard.

11 Log back in using your superuser credentials.

Change SDDC Manager Password

If you purchased an integrated system, your hardware partner sends you the system generated password for SDDC Manager along with the imaged rack. If you deployed Cloud Foundation on a ready system, you must have saved the SDDC Manager password. This password is not changed during password rotation. VMware strongly recommends that you change this password before creating workloads.

Procedure

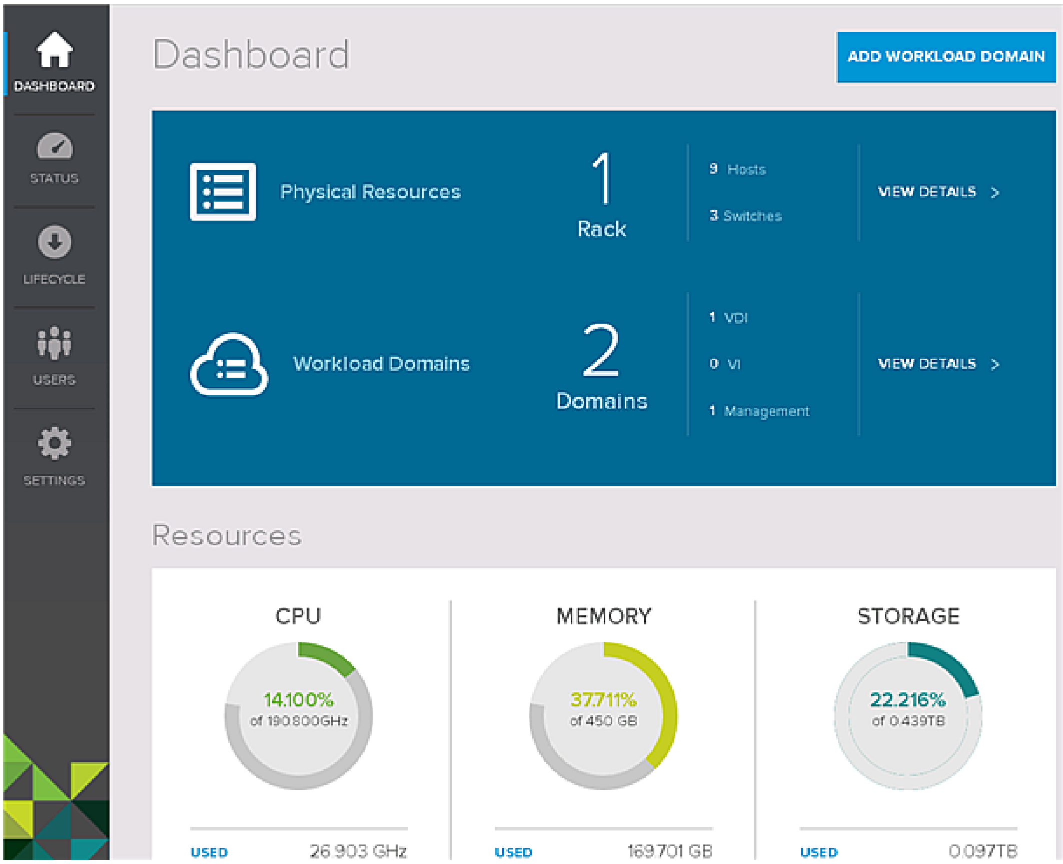
1. In a command line window, SSH to the SDDC Manager on the rack.
2. Login as `root`. Use the password provided to you by the partner (integrated system use case) or the one you saved after imaging the rack(ready system deployment use case.
3. Type the following command to change the password:

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

   The SDDC Manager password is changed.
5. Refresh the web browser window where you were running the Initial Setup wizard.
6. Type in one of the following set of credentials:

   - superuser account username and password that you created during the initial setup
   - `administrator@vsphere.local` user name and the password you noted down afer rotating it (credentials appear in the Single Sign On section in the output of the `lookup-password` command)

   The dashboard page appears.



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

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.

Adding Racks to your Cloud Foundation System

5

Once Cloud Foundation is running on the first physical rack, you can bring up Cloud Foundation on additional physical racks in your environment

Note The SDDC Manager version on the rack you want to add must match the version of the other racks in your environment. If the new rack is a later version, you must upgrade the other racks in your environment before you add it to your Cloud Foundation system.

Procedure

1 Connect Rack 2 to Spine Switches

This procedure refers to the rack being added as rack 2. Follow the same procedure for adding any rack.

2 Power on Rack 2

After the spine connections are in place, you can power on rack 2.

3 Bootstrap Additional Rack

Bootstrap SDDC Manager on rack 2 from SDDC Manager on rack 1.

4 Manual Steps for Rack Addition

Complete these steps before bringing-up the additional rack.

5 Initiate the Bring-Up Process on Additional Rack

Complete bring-up on the rack you are adding to your Cloud Foundation system.

6 Changing Passwords of Rack Components

Cloud Foundation is deployed with factory default passwords. It is highly recommended that you replace the default passwords with secure system generated passwords.

7 Change SDDC Manager Password on Each Additional Rack

If you purchased an integrated system, your hardware partner sends you the system generated password for SDDC Manager along with the imaged rack. If you deployed Cloud Foundation on a ready system, you must have saved the SDDC Manager password. During password rotation, the SDDC Manager is not changed. VMware strongly recommends that you change this password on each rack before creating workloads.

Connect Rack 2 to Spine Switches

This procedure refers to the rack being added as rack 2. Follow the same procedure for adding any rack.

Prerequisites

1. Ensure that rack 2 is powered down so that there is no connectivity between rack 1 and rack 2.
2. The bring-up process must have been completed successfully on rack 1. Rack 1 Dashboard must be accessible and the SDDC Manager VM (VRM) on rack 1 must be powered on.
3. Password rotation must have been completed on rack 1.

Procedure

1. Make the following connections:
   - Rack 1 ToR 1 port 49 to spine 1 port 1 on rack 2
   - Rack 1 ToR 1 port 50 to spine 2 port 1 on rack 2
   - Rack 1 ToR 2 port 49 to spine 1 port 2 on rack 2
   - Rack 1 ToR 2 port 50 to spine 2 port 2 on rack 2
2. While rack 2 is still powered down, verify that the ports on the spine switches on rack 2 are up.
3. Verify that the link connectivity LED between the racks is up.

What to do next

Power on rack 2.

Power on Rack 2

After the spine connections are in place, you can power on rack 2.

Procedure

1. Power on rack 2.
2. Ensure that you can ping SDDC Manager on rack 2 from rack 1.
   a. SSH to SDDC Manager on rack 1 with your superuser account credentials.
   b. Ping SDDC Manager on rack 2 (192.168.100.40).

What to do next

Bootstrap additional rack.

Bootstrap Additional Rack

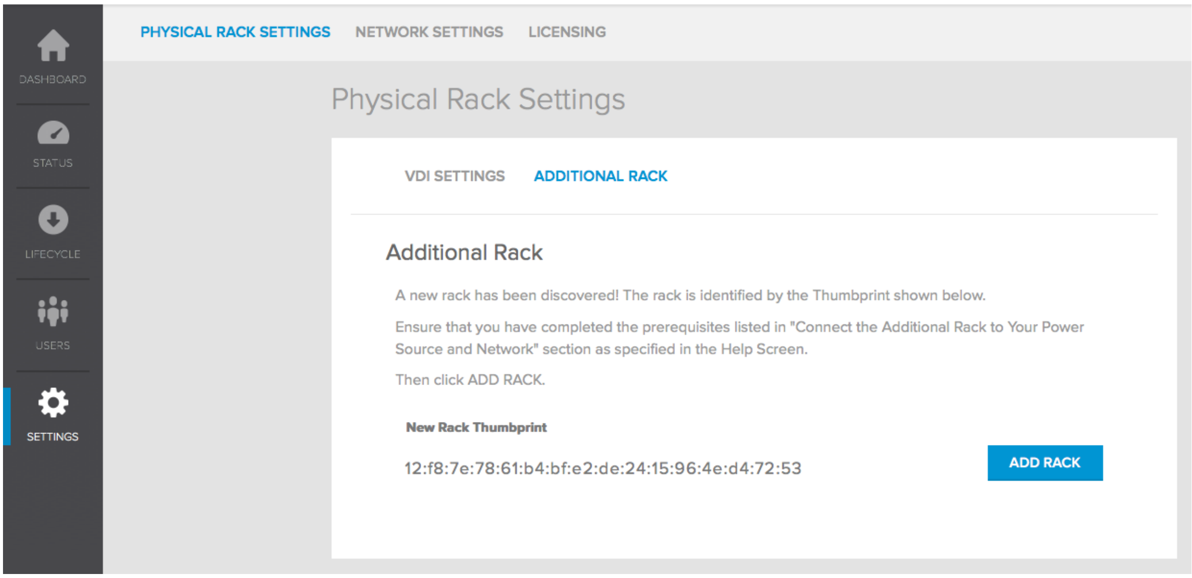
Bootstrap SDDC Manager on rack 2 from SDDC Manager on rack 1.

Procedure

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

2 Click the **Additional Rack** tab.

The thumbprint of rack 2 is displayed here.



Physical Rack Settings

Additional Rack

A new rack has been discovered! The rack is identified by the Thumbprint shown below.

Ensure that you have completed the prerequisites listed in "Connect the Additional Rack to Your Power Source and Network" section as specified in the Help Screen.

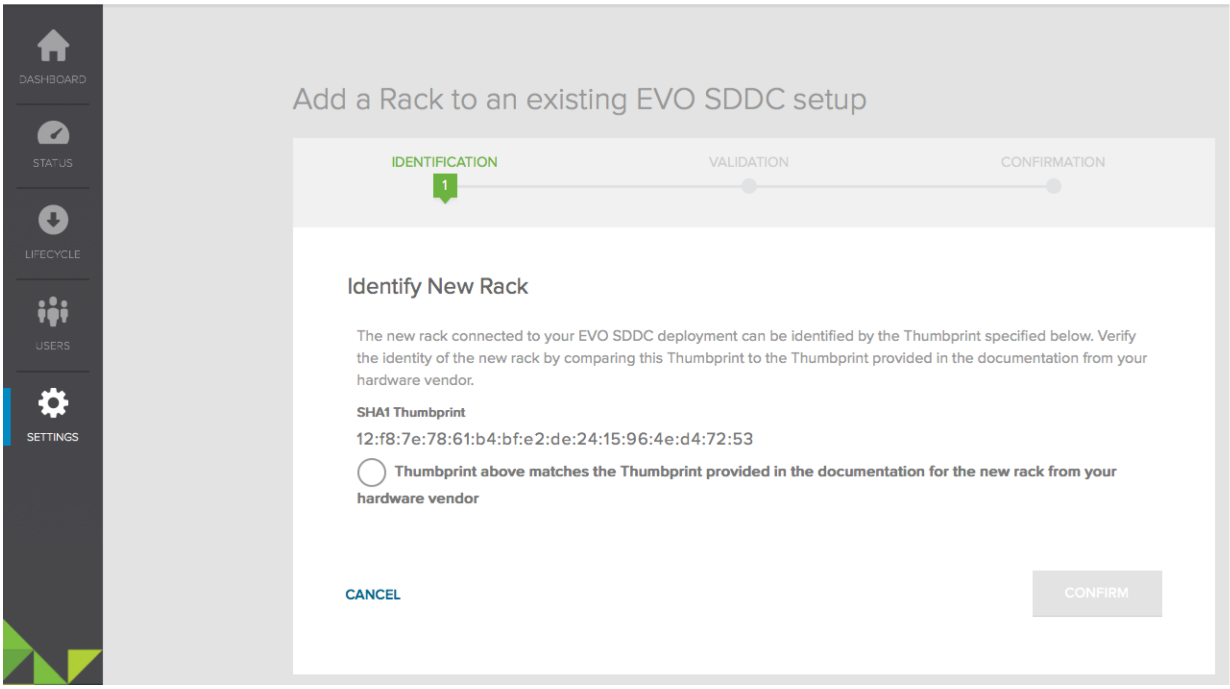
Then click ADD RACK.

New Rack Thumbprint

12:f8:7e:78:61:b4:bf:e2:de:24:15:96:4e:d4:72:53

3 Click **ADD RACK**.

The Add a Rack wizard appears.



Add a Rack to an existing EVO SDDC setup

Identify New Rack

The new rack connected to your EVO SDDC deployment can be identified by the Thumbprint specified below. Verify the identity of the new rack by comparing this Thumbprint to the Thumbprint provided in the documentation from your hardware vendor.

SHA1 Thumbprint

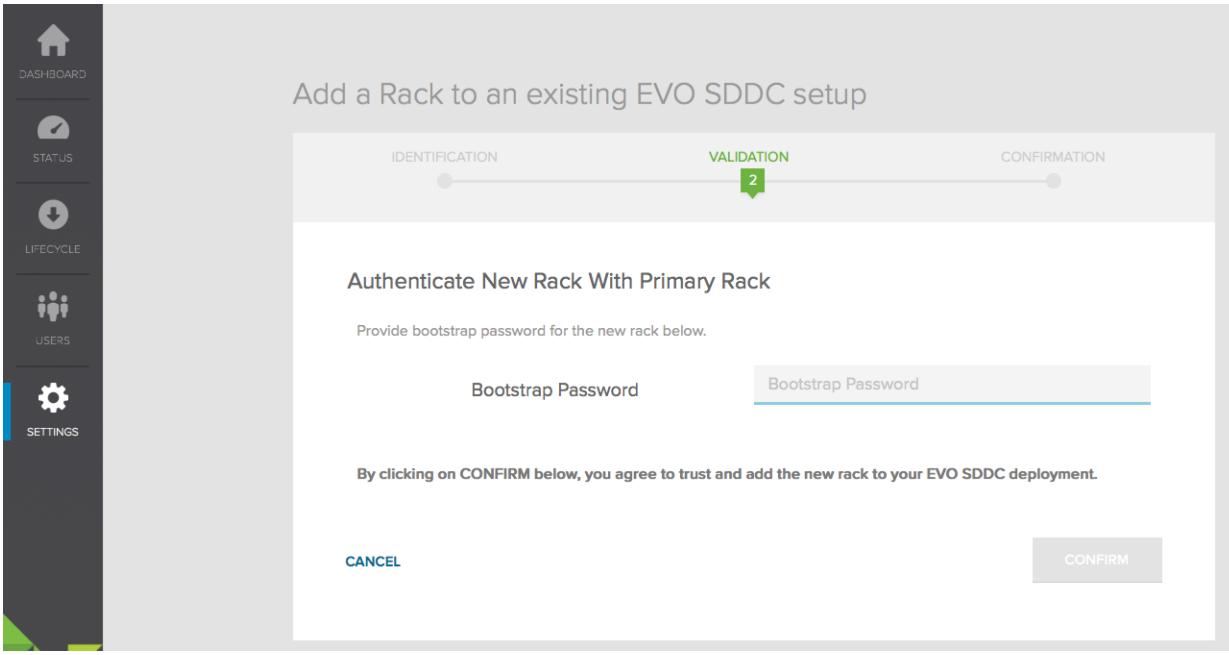
12:f8:7e:78:61:b4:bf:e2:de:24:15:96:4e:d4:72:53

○ **Thumbprint above matches the Thumbprint provided in the documentation for the new rack from your hardware vendor**

4 Compare the thumbprint displayed on the screen with the thumbprint you received from the partner (integrated system use case) or the thumbprint you saved after imaging the rack (ready system use case).

5 If the thumbprints match, click **CONFIRM**.

The Validation page appears.



Add a Rack to an existing EVO SDDC setup

Authenticate New Rack With Primary Rack

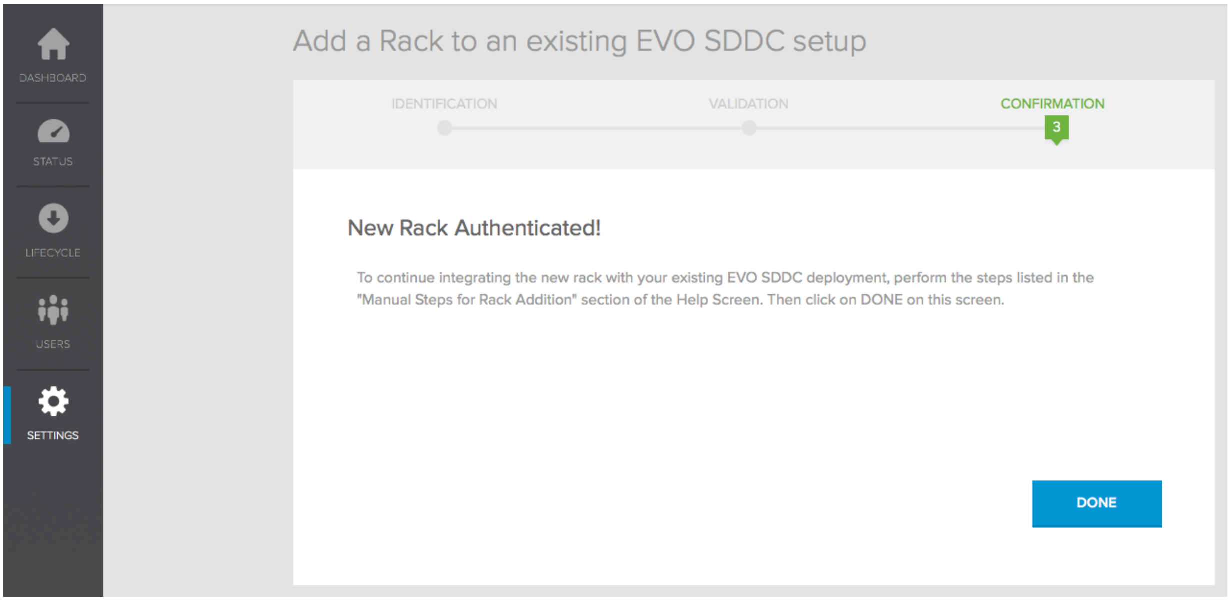
Provide bootstrap password for the new rack below.

Bootstrap Password: Bootstrap Password

By clicking on CONFIRM below, you agree to trust and add the new rack to your EVO SDDC deployment.

6 On the Validation page, type the bootstrap password and click **CONFIRM**.

The Confirmation page confirms that the additional rack has been added to the Cloud Foundation system.



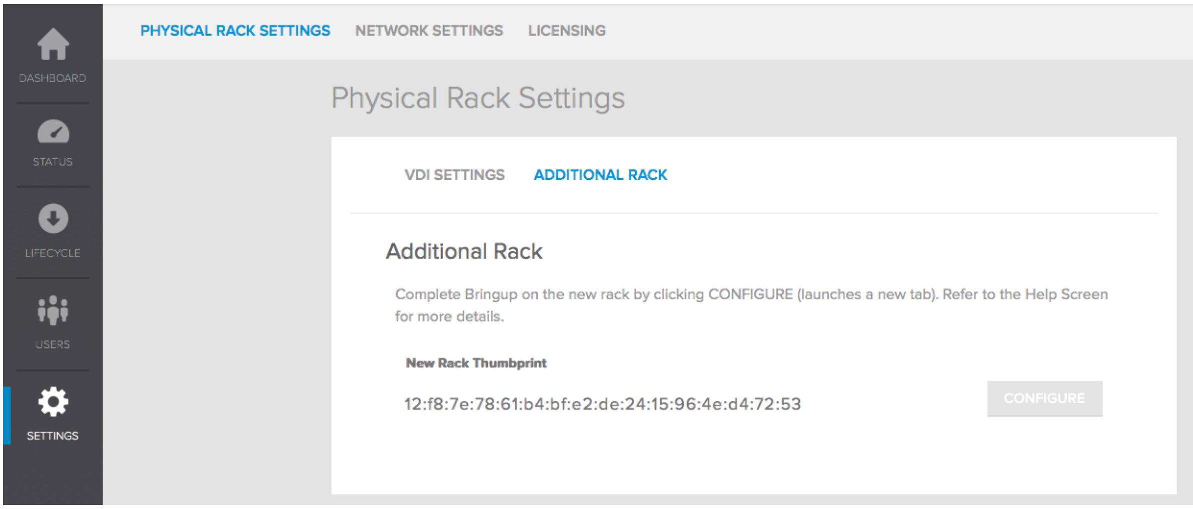
Add a Rack to an existing EVO SDDC setup

New Rack Authenticated!

To continue integrating the new rack with your existing EVO SDDC deployment, perform the steps listed in the "Manual Steps for Rack Addition" section of the Help Screen. Then click on DONE on this screen.

7. Click **DONE**.

   The Additional Rack page displays the thumbprint of the rack you just added. The **CONFIGURE** button is grayed out until you complete the manual steps required at this point. See Manual Steps for Rack Addition.



Physical Rack Settings

Additional Rack

Complete Bringup on the new rack by clicking CONFIGURE (launches a new tab). Refer to the Help Screen for more details.

New Rack Thumbprint

12:f8:7e:78:61:b4:bf:e2:de:24:15:96:4e:d4:72:53

8. Leave this browser window open.

What to do next

Complete manual steps for rack addition.

Manual Steps for Rack Addition

Complete these steps before bringing-up the additional rack.

Procedure

1. Copy the file encryption keys from rack 1 to rack 2. This file will be used to perform encryption and decryption while saving and retrieving the ESXi and PSC passwords to and from Zookeeper.

   a. In a command line window, SSH to the private IP address of SDDC Manager on rack 2.

      For information on retrieving the private IP address of SDDC Manager, see Locate SDDC Manager IP Address.

   b. Run the following script:

      ```
      /home/vrack/VMware/vRack/copycryptokeys.sh
      ```

      The default source and destination paths are displayed.

   c. Type the password of the SDDC Manager on the first physical rack.

   If the files are copied successfully, the message `File copied successfully` is displayed.

2. Confirm that the ISVMs on rack 2 are deleted.

   The additional rack does not contain ISVMs if it was imaged with VIA using the Add-On Rack option.

3 Navigate to `/home/vrack/bin`.

4 Sync the SDDC Manager properties by typing the following command.

```
./vrm-cli.sh sync-properties
```

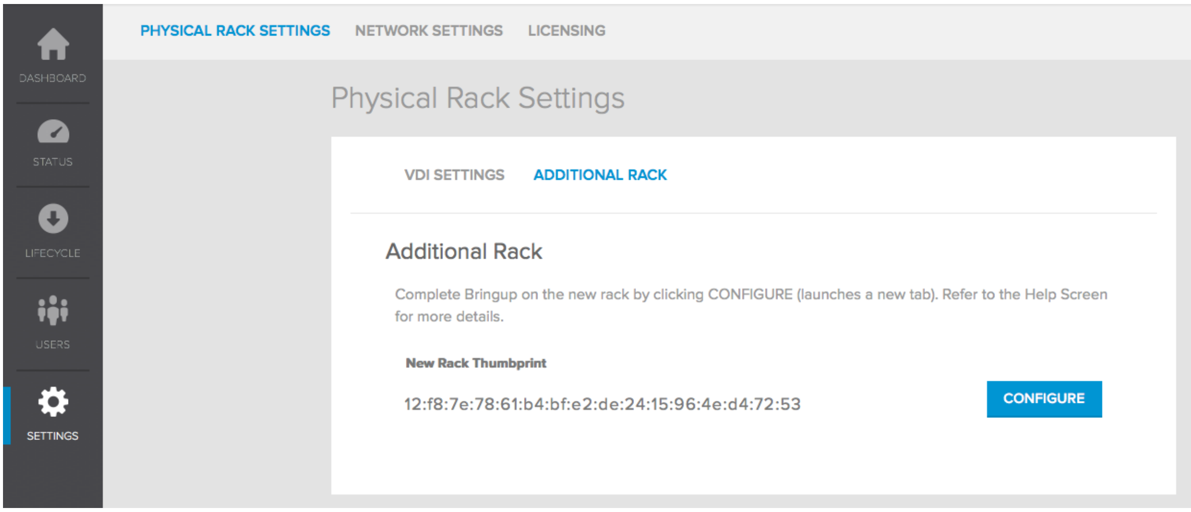
Initiate the Bring-Up Process on Additional Rack

Complete bring-up on the rack you are adding to your Cloud Foundation system.

Procedure

1 Do one of the following to begin bring-up:

- In the Add a Rack wizard that you had left after bootstrapping the additional rack, click **CONFIGURE**.



Physical Rack Settings

Additional Rack

Complete Bringup on the new rack by clicking CONFIGURE (launches a new tab). Refer to the Help Screen for more details.

New Rack Thumbprint

12:f8:7e:78:61:b4:bf:e2:de:24:15:96:4e:d4:72:53

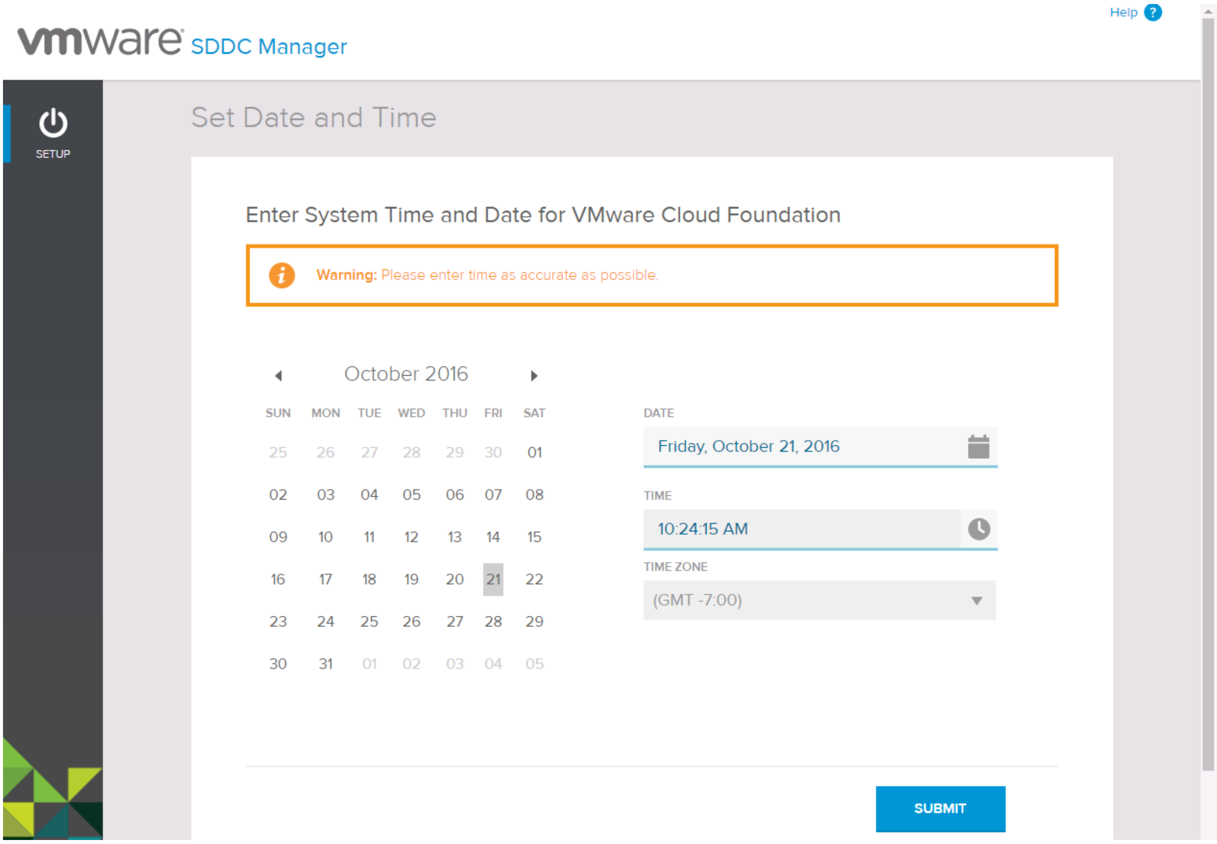
- Open a new browser window and type the following URL:

  https://192.168.100.40:8443/vrm-ui

The Welcome page appears.

2 Click **SET TIME**.

The System Time for VMware Cloud Foundation page appears.



Set Date and Time

Enter System Time and Date for VMware Cloud Foundation

Warning: Please enter time as accurate as possible.

October 2016

SUN	MON	TUE	WED	THU	FRI	SAT
25	26	27	28	29	30	01
02	03	04	05	06	07	08
09	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	01	02	03	04	05

DATE
Friday, October 21, 2016

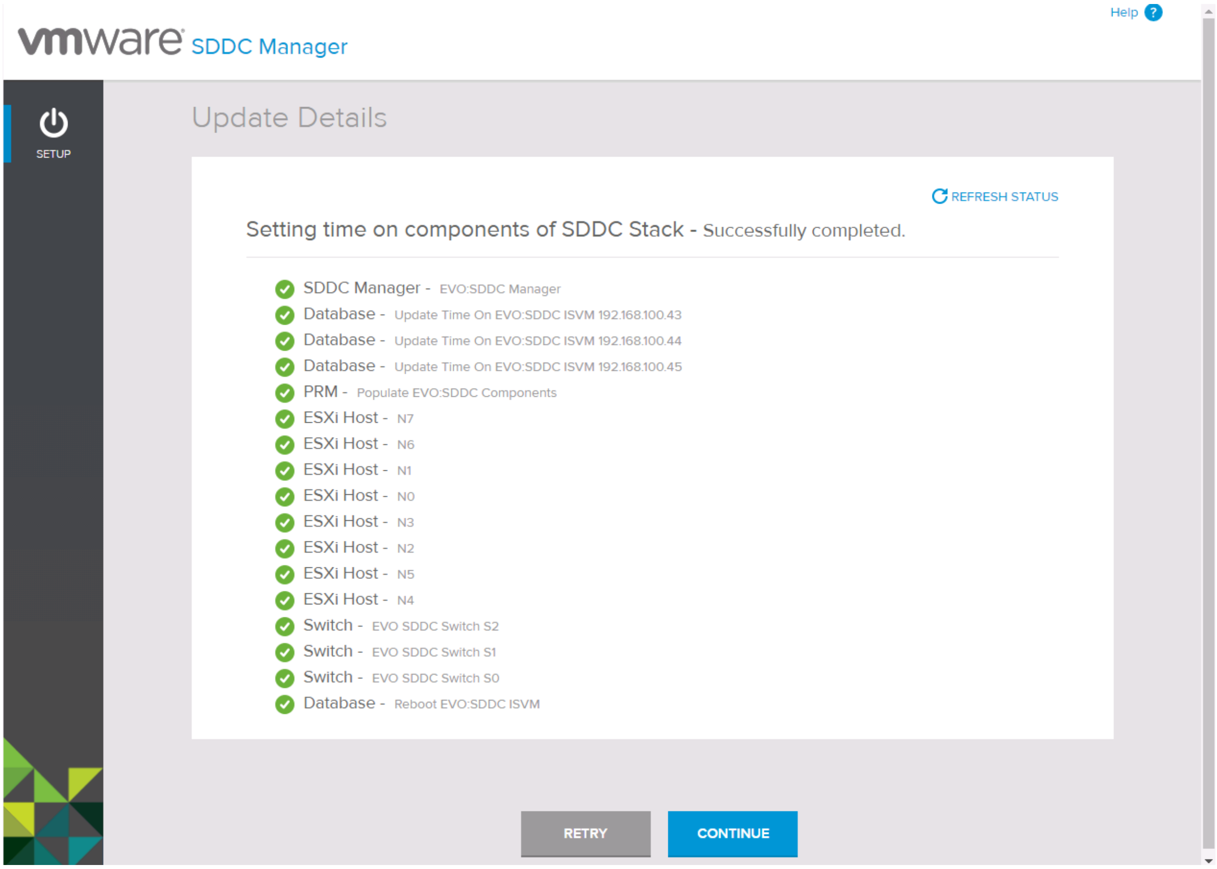
TIME
10:24:15 AM

TIME ZONE
(GMT -7:00)

The date, time, and time zone are fetched from the first physical rack.

3 The system sets the time on each Cloud Foundation component in the additional rack.

After the time has been set on all Cloud Foundation components, SDDC Manager is rebooted and the **CONTINUE** button turns blue.



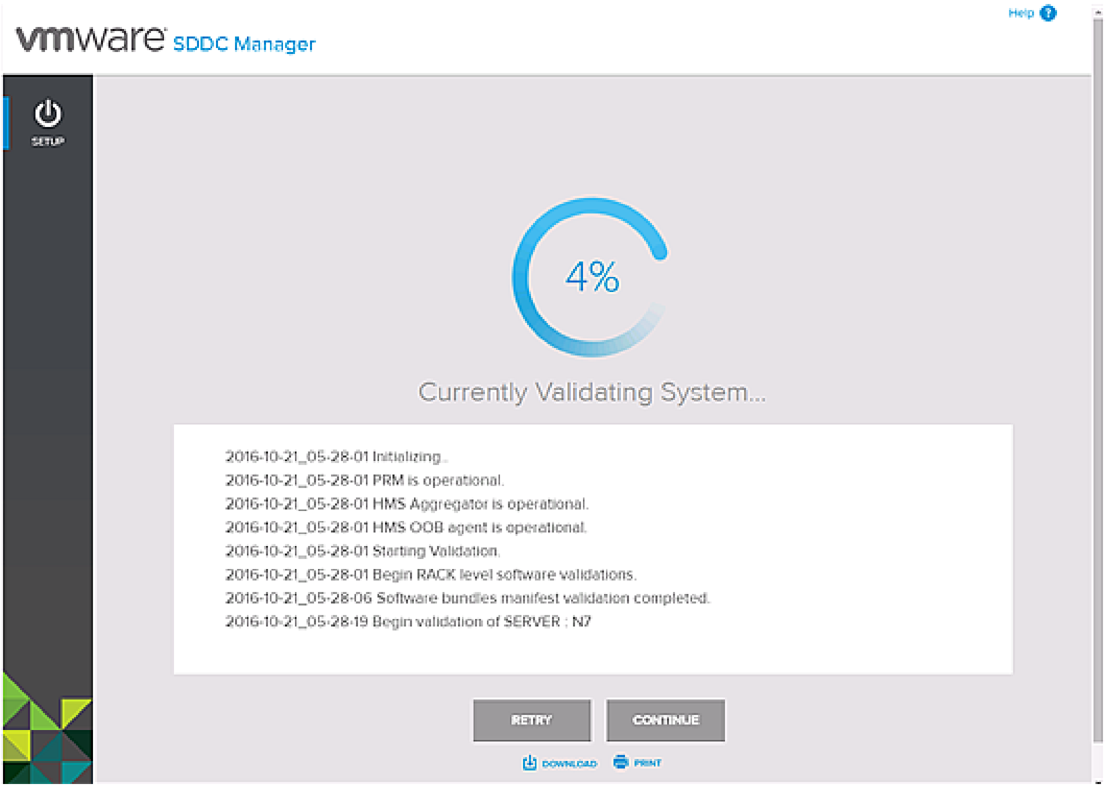
Update Details

Setting time on components of SDDC Stack - Successfully completed.

- ✓ SDDC Manager - EVO:SDDC Manager
- ✓ Database - Update Time On EVO:SDDC ISVM 192.168.100.43
- ✓ Database - Update Time On EVO:SDDC ISVM 192.168.100.44
- ✓ Database - Update Time On EVO:SDDC ISVM 192.168.100.45
- ✓ PRM - Populate EVO:SDDC Components
- ✓ ESXi Host - N7
- ✓ ESXi Host - N6
- ✓ ESXi Host - N1
- ✓ ESXi Host - N0
- ✓ ESXi Host - N3
- ✓ ESXi Host - N2
- ✓ ESXi Host - N5
- ✓ ESXi Host - N4
- ✓ Switch - EVO SDDC Switch S2
- ✓ Switch - EVO SDDC Switch S1
- ✓ Switch - EVO SDDC Switch S0
- ✓ Database - Reboot EVO:SDDC ISVM

4 Click **CONTINUE**.

The system performs Power On System Validation (POSV), where it verifies that the integrated system delivered to the customer is correct and operational. It validates that the right hardware and software is installed in the racks and also validates the health of the installed hardware and software applications.



Currently Validating System...

```
2016-10-21_05-28-01 Initializing..
2016-10-21_05-28-01 PRM is operational.
2016-10-21_05-28-01 HMS Aggregator is operational.
2016-10-21_05-28-01 HMS OOB agent is operational.
2016-10-21_05-28-01 Starting Validation.
2016-10-21_05-28-01 Begin RACK level software validations.
2016-10-21_05-28-06 Software bundles manifest validation completed.
2016-10-21_05-28-19 Begin validation of SERVER : N7
```

If the validation page displays an error, ensure that all physical connections are in place and that the VMs listed in Manually Power On SDDC Manager VM When Setting Up Your Cloud Foundation System are powered on. Then click **RETRY**.

5 Log in using the default credentials:

User name: **`administrator@vsphere.local`**

Password: **`vmware123`**

6 Click **LOGIN**.

The Cloud Foundation EULA page appears.

7 Click **AGREE**.

The Initial Setup wizard appears.

8 Type a name for the rack. It must be different from the name for rack 1. Each rack in the Cloud Foundation system must have a different name.

The company and department name, root domain, sub domain, and PSC domain values are displayed as specified for rack 1. You cannot edit these values.

9 Click **NEXT**.

The Management page displays the network values specified for rack 1.

10 Click **Next**.

The vMotion information page displays the values specified for rack 1.

11. Click **NEXT**.

    The vSAN information page displays the values specified for rack 1.

12. Click **NEXT**.

    The vXLAN information page displays the values specified for rack 1.

13. Click **NEXT**.

    The Data Center Connections page displays the values specified for rack 1.

14. Click **NEXT**.

    The Configuration Review page displays the values specified for rack 1.

15. Click **NEXT**.

    The Review page appears.

16. Review the information.

17. Click **CONNECT**.

    After a few minutes, the Component IP Allocation page appears and displays the IP addresses for the VMs that will be deployed for the NSX, SDDC Manager, vCenter Server, and vRealize Operations software components. Ignore the Log Insight IP address. Log Insight is only deployed on rack 1.

18. After you ensure that the IP Reallocation values are correct, click **CONFIRM**.

    The Configuring System page displays the task that is running and the list of tasks that need to be completed. Click **TASK DETAILS** to view additional details for the tasks. Click ▶ next to the task to see further details. You can filter tasks by status (Running, Successful, or New) or time range.

    In case a task fails, click **RETRY** to run the task again.

    If restarting the `Network: Configure VLAN Tags on Switches` task fails, restart the tcserver on the additional rack.

    a. SSH to the SDDC Manager VM on the additional rack.

    b. Type `service vrm-tcserver stop`.

    c. Type `service vrm-tcserver start`.

19. After the system configuration is completed, the SDDC Manager is restarted. When SDDC Manager comes up, the Password Rotation page is displayed.

20. Leave this browser window open.

21. Rotate passwords on rack 2. See Change SDDC Manager Password on Each Additional Rack.

    You cannot access the SDDC Manager Dashboard on rack 1 till you complete this step.

22. If DNS delegation for automatic resolution is configured in your environment, you are redirected to the login page in the browser window you had left open. Log in using the superuser credentials or the system administrator account name (administrator@domainName) and password that you noted down after password rotation. The Dashboard page appears. The Physical Resources on the Dashboard includes both rack1 and rack 2.

Changing Passwords of Rack Components

Cloud Foundation is deployed with factory default passwords. It is highly recommended that you replace the default passwords with secure system generated passwords.

You must change the passwords on each rack that you add to your Cloud Foundation system.

Note The additional rack must have successfully completed bring-up before you change the passwords.

1 In a command line window, SSH to one of the base IP addresses for SDDC Manager on the rack. See Locate SDDC Manager IP Address.

2 Navigate to `/home/vrack/bin`.

3 Type the following command:

```
./vrm-cli.sh lookup-password
```

The output displays the passwords and IP addresses for all components on rack 1.

4 Save the output to a secure location so that you can access it later.

5 Save a copy of the `/home/vrack/VMware/vRack/vrm.properties` file to a secure location where you can access it later.

6 In the SDDC Manager console window for rack 1, navigate to `/home/vrack/bin`.

7 Type the following command:

```
./vrm-cli.sh rotate-all
```

This command changes the passwords of the physical components on rack 1 and logical components on all racks in your environment.

8 In the SDDC Manager console window, type the following command:

```
./vrm-cli.sh lookup-password
```

Save the output. Compare the output file you saved in step 5 with the output file you saved now and ensure that all passwords have been changed.

9 Refresh the browser window where you were running the Initial Setup wizard.

The Cloud Foundation Dashboard is displayed.

Change SDDC Manager Password on Each Additional Rack

If you purchased an integrated system, your hardware partner sends you the system generated password for SDDC Manager along with the imaged rack. If you deployed Cloud Foundation on a ready system, you must have saved the SDDC Manager password. During password rotation, the SDDC Manager is not changed. VMware strongly recommends that you change this password on each rack before creating workloads.

Procedure

1 In a command line window, SSH to the SDDC Manager on the rack.

2 Login as `root`. Use the password provided to you by the partner (integrated system use case) or the one you saved after imaging the rack (ready system deployment use case).

3 Type the following command to change the password:

```
passwd
```

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

The SDDC Manager password is changed.

Alerts List

6

An alert is a record of a known detected problem. Alerts can be raised at Power On System Validation (POSV), at a set interval when the system polls the alert catalog, or when an event is generated. An event is a record of a system condition that is potentially significant or interesting to you, such as a degradation, failure, or user-initiated configuration change.

Table 6-1. Cloud Foundation Alerts

Alert Name	Short Description	Severity Level	Detected By
BMC_AUTHENTICATION_FAILURE_ALERT	The system is unable to authenticate to the server's out-of-band (OOB) management port.	ERROR	Event
BMC_MANAGEMENT_FAILURE_ALERT	The system failed to perform a management operation using the server's OOB management port.	ERROR	Event
BMC_NOT_REACHABLE_ALERT	The system is unable to communicate with the BMC server's out-of-band (OOB) management port.	ERROR	Event
COORDINATION_SERVICE_DOWN_ALERT	Cannot establish connection with Zookeeper.	ERROR	
CPU_CAT_FAILURE_ALERT	A processor has shut down due to a catastrophic error.	ERROR	Event
CPU_EXTRA_ALERT	Mismatch between CPU spec in manifest file and physical CPU inventory reported by HMS. An extra CPU is present in the physical inventory.	WARNING	Event
CPU_INITIALIZATION_ERROR_ALERT	The system detected that a CPU initialization error has occurred.	ERROR	Event
CPU_INVALID_ALERT	The polling detected a type of CPU in the server that does not match what is expected according to the manifest.	ERROR	POSV and system poll
CPU_MACHINE_CHECK_ERROR_ALERT	A server CPU has failed due to CPU Machine Check Error.	ERROR	Event
CPU_POST_FAILURE_ALERT	A server CPU has shut down due to POST failure.	ERROR	Event
CPU_TEMPERATURE_ABOVE_UPPER_THRESHOLD_ALERT	A CPU temperature has reached its maximum safe operating temperature.	WARNING	Event

Table 6-1. Cloud Foundation Alerts (Continued)

Alert Name	Short Description	Severity Level	Detected By
CPU_TEMPERATURE_BELOW_LOWER_THRESHOLD_ALERT	A CPU temperature has reached its minimum safe operating temperature.	WARNING	Event
CPU_THERMAL_TRIP_ERROR_ALERT	A server CPU has shut down due to thermal error.	ERROR	Yes
CPU_UNDETECTED_ALERT	A CPU matching the manifest was not detected.	ERROR	Event
DIMM_ECC_MEMORY_ERROR_ALERT	The system detected an uncorrectable Error Correction Code (ECC) error for a server's memory.	ERROR	Event
DIMM_TEMPERATURE_ABOVE_THRESHOLD_ALERT	Memory temperature has reached its maximum safe operating temperature.	WARNING	Event
DIMM_THERMAL_TRIP_ALERT	Memory has shut down due to thermal error.	ERROR	Event
EVO_SDDC_BUNDLE_INCOMPLETE_ALERT	The Cloud Foundation ISO file is missing some elements.	CRITICAL	POSV
EVO_SDDC_BUNDLE_INVALID_ALERT	MD5 checksum generated on the Cloud Foundation ISO bundle does not match the MD5 checksum provided by VIA in the vSAN datastore.	CRITICAL	POSV
EVO_SDDC_BUNDLE_MISSING_ALERT	The Cloud Foundation bundle ISO file or MD5checksum file is missing.	CRITICAL	POSV
HDD_DOWN_ALERT	Operational status is down for an HDD.	ERROR	Event
HDD_EXCESSIVE_READ_ERRORS_ALERT	Excessive read errors reported for an HDD.	WARNING	Event
HDD_EXCESSIVE_WRITE_ERRORS_ALERT	Excessive write errors reported for an HDD	WARNING	Event
HDD_EXTRA_ALERT	Additional HDD detected that does not match the manifest.	WARNING	POSV and system poll
HDD_INVALID_ALERT	Detected HDD does not match the manifest.	ERROR	POSV and system poll
HDD_TEMPERATURE_ABOVE_THRESHOLD_ALERT	HDD temperature has reached its maximum safe operating temperature.	WARNING	Event
HDD_UNDETECTED_ALERT	HDD matching the manifest was not detected.	ERROR	POSV and system poll
HDD_WEAROUT_ABOVE_THRESHOLD_ALERT	Wear-out state of an HDD is above its defined threshold.	WARNING	Event
HMS_AGENT_DOWN_ALERT	A physical rack's Hardware Management Services agent is down.	CRITICAL	POSV
HMS_DOWN_ALERT	The HMS is down.	CRITICAL	POSV and event
HOST_AGENT_NOT_ALIVE_ALERT	ESXi on a server in a physical rack is not running.		POSV

Table 6‑1. Cloud Foundation Alerts (Continued)

Alert Name	Short Description	Severity Level	Detected By
MANAGEMENT_SWITCH_DOWN_ALERT	Operational status is down for a physical rack's management switch.	WARNING	POSV, system poll, and event
MANAGEMENT_SWITCH_EXTRA_ALERT	Additional management switch detected that does not match the manifest.	WARNING	POSV, system poll, and event
MANAGEMENT_SWITCH_INVALID_ALERT	Detected management switch does not match the manifest.	CRITICAL	POSV, system poll, and event
MANAGEMENT_SWITCH_PORT_DOWN_ALERT	Operational status is down for a port in a physical rack's management switch.	WARNING	Event
MEMORY_EXTRA_ALERT	Detected additional memory that does not match the manifest.	WARNING	POSV and system poll
MEMORY_INVALID_ALERT	Detected memory type does not match manifest.	ERROR	POSV and system poll
MEMORY_UNDETECTED_ALERT	Memory matching the manifest was not detected.	ERROR	POSV and system poll
PCH_TEMPERATURE_ABOVE_THRESHOLD_ALERT	Platform controller hub (PCH) temperature has reached its maximum safe operating temperature.	WARNING	Event
SERVER_DOWN_ALERT	Server is in the powered-down state.	ERROR	POSV and system poll
SERVER_EXTRA_ALERT	Detected additional server that does not match the manifest.	WARNING	POSV and system poll
SERVER_INVALID_ALERT	Detected server does not match the manifest.	ERROR	POSV and system poll
SERVER_PCIE_ERROR_ALERT	A server's system has PCIe errors.	ERROR	Event
SERVER_POST_ERROR_ALERT	A server has POST failures	ERROR	Event
SERVER_UNDETECTED_ALERT	Server matching the manifest as not detected.	ERROR	POSV and system poll
SPINE_SWITCH_DOWN_ALERT	Operational status is down for a physical rack's spine switch.	ERROR	POSV, system poll, and event
SPINE_SWITCH_EXTRA_ALERT	Detected spine switch does not match the manifest.	WARNING	POSV and system poll
SPINE_SWITCH_INVALID_ALERT	Detected spine switch does not match the manifest.	ERROR	POSV and system poll
SPINE_SWITCH_PORT_DOWN_ALERT	Operational status is down for a port: in a physical rack's spine switch.	WARNING	Event
SSD_DOWN_ALERT	Operational status is down for an SSD.	ERROR	Event
SSD_EXCESSIVE_READ_ERRORS_ALERT	Excessive read errors reported for an SSD.	WARNING	Event

Table 6-1. Cloud Foundation Alerts (Continued)

Alert Name	Short Description	Severity Level	Detected By
SSD_EXCESSIVE_WRITE_ERRORS_ALERT	Excessive write errors reported for an SSD.	WARNING	Event
SSD_EXTRA_ALERT	Detected additional SSD that does not match the manifest.	WARNING	POSV and system poll
SSD_INVALID_ALERT	Detected SSD does not match the manifest.	ERROR	POSV and system poll
SSD_TEMPERATURE_ABOVE_THRESHOLD_ALERT	SSD temperature has reached its maximum safe operating temperature	WARNING	Event
SSD_UNDETECTED_ALERT	SSD matching the manifest was not detected.	ERROR	POSV and system poll
SSD_WEAROUT_ABOVE_THRESHOLD_ALERT	Wear-out state of an SSD is above its defined threshold.	WARNING	Event
STORAGE_CONTROLLER_DOWN_ALERT	Operational status is down for a storage adapter.	ERROR	Event
TOR_SWITCH_DOWN_ALERT	Operational status is down for a physical rack's ToR switch.	ERROR	POSV and system poll
TOR_SWITCH_EXTRA_ALERT	Detected extra ToR switch that does not match the manifest.	WARNING	POSV and system poll
TOR_SWITCH_INVALID_ALERT	Detected ToR switch does not match the manifest.	ERROR	POSV and system poll
TOR_SWITCH_PORT_DOWN_ALERT	Operational status is down for a port in a physical rack's ToR switch.	WARNING	Event

Troubleshooting Cloud Foundation Deployment

7

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 VM When Setting Up Your Cloud Foundation System

When you power on a rack, the SDDC Manager VM (VRM) that is pre-installed on host 0 is supposed to power on automatically. If this does not happen, you can manually power it 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 VM to be running. If it is not powered on when the ESXi host powers on, the setup wizard cannot run.

Solution

1. On the jump host that is connected to port 48 on the management switch, start the vSphere Web Client and open it to IP address 192.168.100.100.
2. Log in to the host.

3. In the vSphere Web Client, navigate to the Inventory view to see the `vrm` VM. Ensure that it is powered on. If a virtual machine does not have a green arrow icon, it is not powered on.

   The LCM Repository and three Zookeeper VMs are also pre-installed. Once the vrm VM is powered on, it powers on the three Zookeeper VMs. The LCM Repository VM is activated during the Cloud Foundation deployment.

4. If `vrm` VM is not powered on, power it 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 management switch 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, a VI workload domain creation workflow might fail during the NSX: Register vCenter 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 vCenter 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

8

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 6.0 Documentation at http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/Welcome/welcome.html
vSAN	Administering VMware Virtual SAN at http://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/virtual-san-61-administration-guide.pdf
NSX	NSX for vSphere Documentation at http://pubs.vmware.com/NSX-62/topic/com.vmware.ICbase/Welcome/welcome.html
vRealize Operations	VMware vRealize Operations Manager Documentation at https://www.vmware.com/support/pubs/vrealize-operations-manager-pubs.html
vRealize Log Insight	VMware vRealize Log Insight Documentation at http://pubs.vmware.com/log-insight-30/topic/com.vmware.ICbase/Welcome/welcome.html

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

9

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
```

Glossary

10

Term	Description
bring-up	Initial configuration of a newly deployed Cloud Foundation system.
host 0	First server in the physical rack.
imaging	During imaging, SDDC software is pre-configured on a physical rack.
management domain	Cluster of physical hosts (first fours hosts in the physical rack) that house the management component VMs
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.