

VIA User's 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/>

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

Copyright © 2015 - 2017 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

About the VIA User's Guide 5

1 About VIA 6

Cloud Foundation Deployment Options 8

Software Bundle 8

VIA Components 9

Database 9

Inventory 9

Services 9

Components of a Physical Rack 10

2 Before You Install VIA 13

Requirements for VIA 13

Setting up your Environment 14

Rack Power 14

Network Cables 14

Rack Wiring 17

Rack Component Ports 22

Physical Servers 24

Network Switches 26

Laptop or Management Host 26

Virtual Machines 28

Pre-Imaging Checklist 30

3 Installing VIA 32

Installing VIA on a Laptop or Desktop 32

Installing VIA on a Management Host 33

4 Imaging Physical Racks 36

Image a Physical Rack 37

Upload Software Bundle 41

Specify Imaging Details 44

Monitor Imaging 47

Verify Inventory 49

Post Imaging Checks 50

Retrieve SDDC Manager Password and Rack Thumbprint 50

Resume Imaging 51

Image Additional Racks 54

- 5 Imaging Individual Devices 55**
 - [Image Individual Server 55](#)
 - [Image New Management Switch 56](#)

- 6 Viewing the VIA Log File 58**

- 7 Viewing Results of an Imaging Run 59**
 - [View Imaging History 59](#)
 - [View Inventory 60](#)

- 8 BIOS Settings 62**
 - [Cisco Settings 62](#)
 - [Dell Settings 63](#)
 - [Hewlett Packard Settings 64](#)
 - [Quanta Settings 65](#)

- 9 Troubleshooting VIA 67**
 - [Host failed to be imaged with error Unable to Establish IPMI v2 / RMCP+ Session 67](#)
 - [ESXi Server has Incorrect BIOS Settings 67](#)
 - [ESXi Server has Bad SD Card 68](#)
 - [Management Switch Boots into EFI Shell 68](#)

About the VIA User's Guide

The *VIA User's Guide* provides information about how to install VIA, manage software bundles, and image physical racks.

Intended Audience

This information is intended for anyone who wants to install or upgrade VIA and image physical racks. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and datacenter operations.

Related Publications

The *VMware Cloud Foundation Overview and Bring-Up Guide* contains detailed information about the Cloud Foundation product, its components, and the network topology of an Cloud Foundation installation.

The *Administering VMware Cloud Foundation* provides information about how to manage a VMware Cloud Foundation™ system, including managing the system's physical and logical resources, managing users, configuring and deploying service offerings, and upgrading and monitoring the system.

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 VIA

1

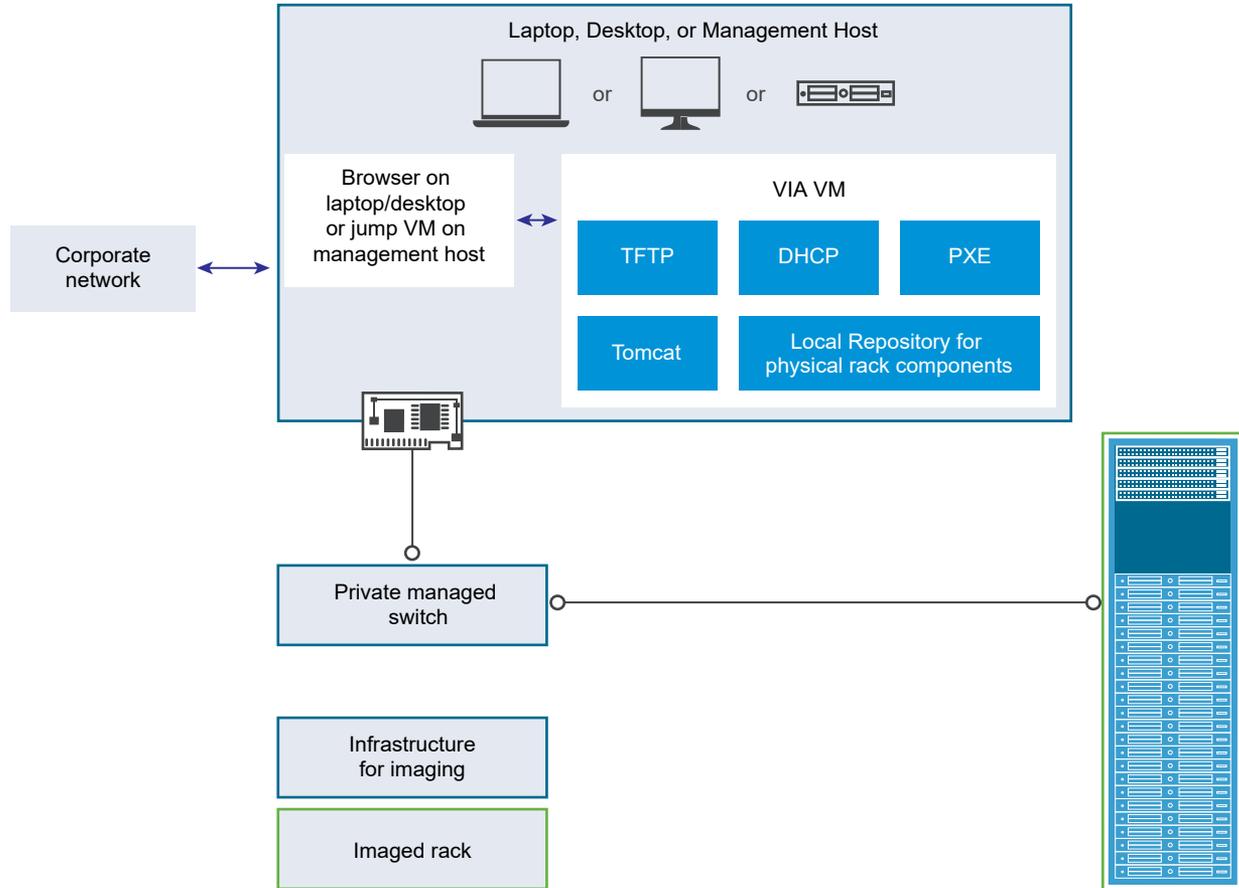
VIA is a virtual appliance used by system integrators or administrators deploying Cloud Foundation to image physical racks. During imaging, VIA pre-configures the Cloud Foundation software stack on the rack.

A physical rack consists of a management switch, two Top of Rack (ToR) switches and 4 to 32 physical servers. If you have multiple physical racks in your datacenter, the second rack must contain two spine switches for inter-rack connectivity.

For imaging the rack, VMware provides the VIA OVF template and the Cloud Foundation software bundle. The software bundle consists of SDDC components - vSphere, NSX, vSAN and management tools vRealize Operations Manager, VMware Horizon with View, vRealize Log Insight, and App Volumes.

The imaging infrastructure at the customer or partner site includes a laptop running Workstation or Fusion, desktop, or ESXi host (referred to as the management host) and a supported 24-port 1GE Managed Switch with RJ45 ports and Cat 5/5E cables. The VIA OVA template is installed on the laptop or management host and the software bundle is uploaded on the VIA VM. The laptop or management host is connected to the corporate network as well as to the private network used by the VIA VM to image the individual hosts and switches. You use a browser (on the laptop) or jump VM (on the management host) to connect to the VIA VM and image the physical rack. The managed switch allows for multiple racks to be simultaneously by creating VLANs.

Figure 1-1. VIA Deployment



During imaging:

- The ToR and spine switches (if applicable) are configured
- The Hardware Management Service (HMS) is installed on the management switch
- VMware ESXi is installed on each server in the physical rack
- The Cloud Foundation software, SDDC Manager, is installed on the first host (node 0) of each physical rack.

After imaging is complete, VIA compiles a manifest file that provides an inventory of the physical rack components. The rack is now ready to be configured for Cloud Foundation.

This chapter includes the following topics:

- [Cloud Foundation Deployment Options](#)
- [Software Bundle](#)
- [VIA Components](#)
- [Components of a Physical Rack](#)

Cloud Foundation 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 and number of racks. Each rack requires a minimum of 4 servers.

Customers have two deployment options for Cloud Foundation

- Deploy the Cloud Foundation software on ready systems in your datacenter.

Customers can start with a ready system (set of qualified vSAN nodes and 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.



Deploying VMware Cloud Foundation on Qualified Hardware

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

Software Bundle

The software bundle is a collection of all the software, configuration files, utilities, and tools used by VIA to image a physical rack. It contains a manifest file that lists the contents of the bundle. The bundle is based on a hardware bill-of-materials (BoM), that includes specific servers, switch models, and their component level configurations.

The bundle contains the following software:

- vSphere (vCenter Server and ESXi)
- NSX
- vSAN
- vRealize Log Insight
- vRealize Operations
- SDDC Manager
- Platform Services Controller
- VMware Horizon with View

- App Volumes

See the *VMware Cloud Foundation Release Notes* for the software component versions.

VIA Components

VIA uses multiple components to track and perform the imaging process. This section describes these components, but you do not need to perform any configuration on them.

Database

VIA stores information about all activities during an imaging run in an HSQLDB database. This includes current imaging information as well as the previous imaging status. All entities utilized by the imaging process are stored as an entry in the database. These entities include the software bundle, imaged component, manifests, user information, and hardware information.

Inventory

VIA maintains a bundle inventory and a rack inventory.

The bundle inventory is an input to the imaging activity, and is created by VIA before it begins an imaging run. The bundle inventory is specific to a vendor and hardware type.

The rack inventory includes configuration details of the hardware imaged by VIA. The configuration details includes credentials to access both the data and the management interfaces of the imaged hardware, as well as the protocols to be used to access the interfaces of the imaged hardware.

Services

In order to handle disparate requests that may be required to service its components, VIA deploys multiple services. Each service has a specific goal, and is instantiated based on the state of the imaging activity.

Bundle Inventory Service

VIA deploys the bundle inventory service before starting an imaging activity. The service creates a bundle inventory using all the information in the bundle manifest. It ensures that the software bundle contains the files listed in the manifest and lists the manufacturer and hardware for which the bundle can be used.

The bundle inventory service includes a bundle manager and bundle controller. They manage the software bundles, mount the active bundle to be used for an imaging run, and set up TFTP and PXE Linux configuration to image the servers.

Device Manifest Service

The device manifest service creates a new manifest file when an imaging activity is performed for the first time. It also tracks changes to the device status and stores hardware information for the rack components.

Imaging Service

The imaging service can start, stop, or cancel an imaging run. It tracks the imaging workflow and maintains the state of the imaging run as well as details about the device being imaged. Details being tracked include the IP address of the device, imaging task being performed, status of the imaging task, and completion time of the imaging task.

DHCP Service

VIA deploys the DHCP service before starting an imaging run. The DHCP service discovers the physical rack components and their PXE images using the DHCP Protocol. It keeps track of the IP addresses allocated to the devices to ensure that a device can be provided with the same IP address in case it needs to be reimaged.

Cipher Service

The imaging service uses a cipher service to generate passwords to access the imaged rack components. The cipher service ensures that each imaged component is always associated with a unique password. However, all ESXi hosts have the same password.

Rack Inventory Service

The rack inventory service is deployed when the components have been successfully imaged. It collects access information for the imaged components such as connection protocol, IP address, and username and password and generates an inventory file. This inventory file is then transferred to the management switch.

Components of a Physical Rack

VMware recommends that you use a white cabinet that is 19" wide with 42 Rack Units (RU) for the physical rack. The cabinet must have a loading capacity of 2000 lbs and have adjustable levelling feet with heavy duty casters and seismic bracing. Since switches do not cover the full shelves, the cabinet must have a grill on one side for proper airflow.

Table 1-1. Rack Components

Component	Rack 1	Additional Racks
PDUs	4	4
Console serial switch	1	1
Spine switches	NA	2 (Rack 2 only)
TOR Switches	2	2
Management switch	1	1
Servers	Up to 32	Up to 32

■ PDUs

Each physical rack must have 4 PDUs (2 primary and 2 standby) even if it contains less than 32 servers. It is recommended that the primary PDUs be blue and the standby be red. The primary PDUs must be placed on the rear left side and the standby PDUs must be placed on the rear right side of the cabinet. The capacity requirements for each PDU are:

- 208 V
- 30 AMP
- 3 phase
- 60 Hz/50 H

The plug type needs to be determined based on the customer's environment.

- Console serial switch

Each physical rack contains a 16-port console serial switch. The console serial switch is connected to all the other switches in the rack and is used for troubleshooting.

- Spine switches

Rack 2 in your Cloud Foundation system contains two 32 x 40 GE spine switches. These switches connect multiple racks by using uplinks from the Top of Rack switches.

Spine switches must not be connected to a corporate network. They are only used for ToR connectivity between physical racks.

- Top of Rack (ToR) switches

Each rack contains two 1RU 48-port 10 GE ToR switches with four 40 GE uplinks. Servers in each rack are connected to both ToRs. The ToRs on rack 1 connect Cloud Foundation to the corporate network.

- Management switch

Each rack contains a 1 GE management switch, which is used for IPMI access and access to the physical switches. The management ports of the ToR switches, Spine switches (on Rack 2 only), and the physical servers are connected to the management switch. The data ports of the ToR switches are also connected to the management switch. This enables the management switch to monitor the data from the servers from both the management network as well as the data network.

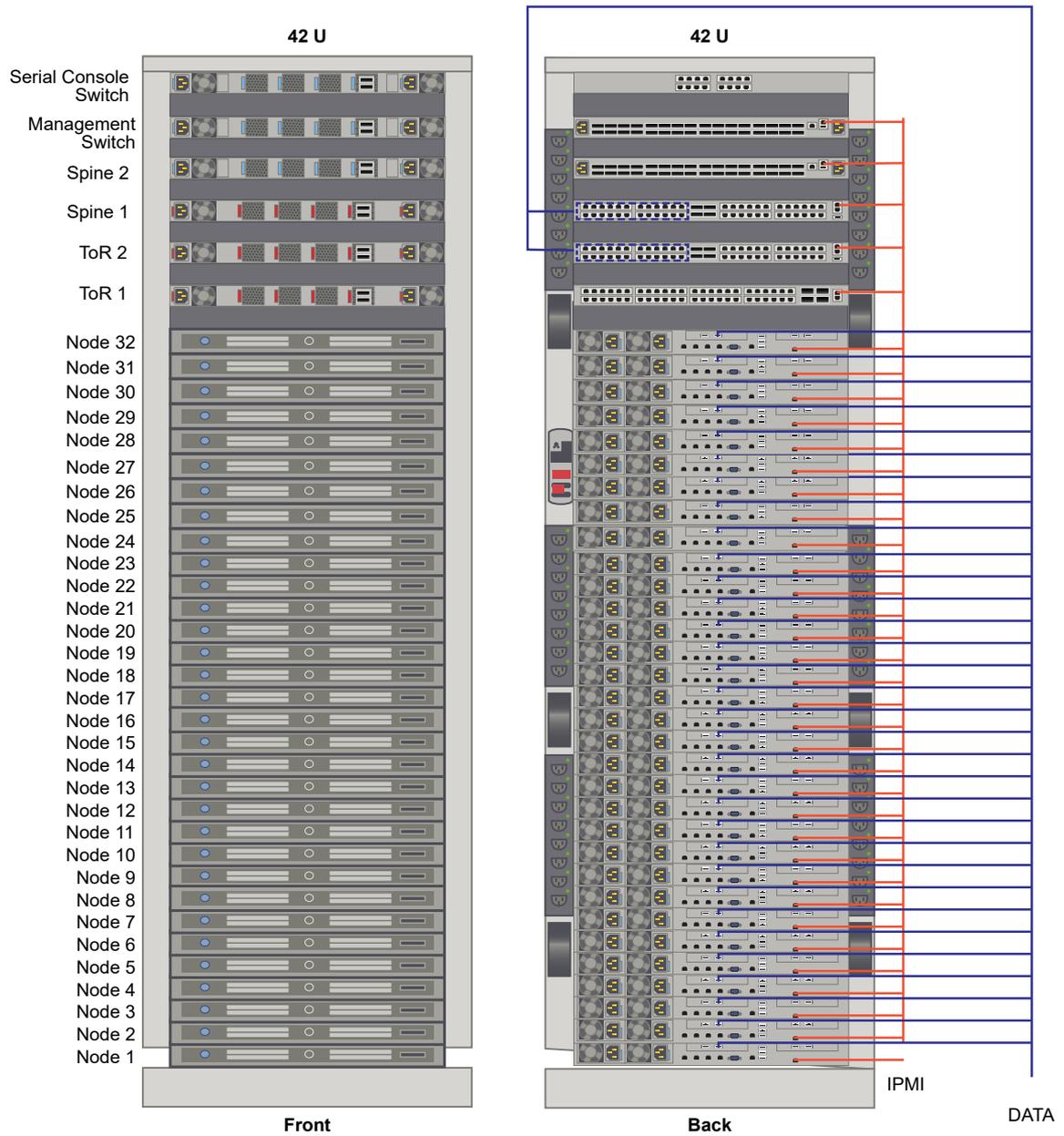
The management switch provides out-of-band (OOB) connectivity for managing switches and servers. The hardware management service (HMS) runs on the management switch.

- Servers

A rack can contain up to 32 two-socket 1U or 16 two-socket 2U servers that are vSAN certified.

All servers within a rack must be of the same model and type. It is recommended that the server disk size and storage configuration be identical. Memory between servers can vary. CPU must be two-socket but the cores can vary.

Figure 1-2. Example Physical Rack Configuration



Before You Install VIA

2

Before you install VIA, ensure that you have all of the required hardware components in place.

This chapter includes the following topics:

- [Requirements for VIA](#)
- [Setting up your Environment](#)

Requirements for VIA

VIA requires the following infrastructure.

- You need a laptop/desktop or an ESXi host (called management host) to run the VIA VM.
A laptop works well for imaging a single rack while a management host is recommended if you are imaging multiple racks. The laptop need to be connected to the management switch of the rack being imaged. If there are multiple racks to be imaged, this would mean physically moving the laptop for imaging each rack. The management host is connected to all the management switches through an internal switch, so the connection to the rack being imaged can be managed remotely.
 - Desktop or laptop (Windows or Mac) with 4 GB memory and a multi core processor to access the jump VM. A Windows laptop must have Workstation 8 or later and a Mac should have Fusion 4 or later installed on it. You also need a network adapter, a cable, and a 4-port unmanaged switch.
 - Management host - a standalone VMware vSphere ESXi 6.0 or later server to host the Windows jump VM. The management host must have at least two NICs, with one NIC connected to the corporate network and one NIC connected to the private network.
- If you are using a management host for imaging, you need a jump VM to access VIA
- Private managed switch. Private indicates that it is being used only by you. A managed switch provides the ability to configure, manage, and monitor your LAN, which gives you greater control over how data travels over the network and who has access to it.

Setting up your Environment

You must inspect the components of the physical rack, verify cable connectivity, and validate BIOS settings before beginning the imaging process.

Review the Bill Of Materials (BOM) from VMware and ensure there are no discrepancies between the BOM and the equipment being used.

Rack Power

Two power strips are supplied with the kits.

Connect a power supply in each server and switch to one of the power strips, and connect the redundant power supply to the other power strip. Connect the power strips to two different power circuits.

- Power cables should not be in an area where there is a risk of touching sharp edges, excessive heat, or subject to pinching between sliding rails.
- Verify that each device in the rack has a connection to each power strip. Power cables must be seated properly.
- VMware recommends that you cable each server to the nearest power port so that the cable length can be kept to a minimum. Length of power cables should be as follows.
 - From the Physical Server: 0.5m
 - From the Top-of-Rack Switch: 1.5m

It is common for power cables within a rack to be longer than required. However, if excess cabling is not managed properly, it may create electromagnetic interference. Avoid bundling of excess cables as this may lead to the cables being damaged due to bending.

Network Cables

Proper management of network cables promotes the elimination of crosstalk and interference, cooler performance, improved maintenance, and easier upgrades. Incorrect cable management may result in damage or failure, which may lead to data transmission errors, performance issues, or system downtime. This section contains cable color and management recommendations. You can adapt the recommendations to suit your environment.

Regardless of the number of servers in each rack, cables must be in place for 32 servers. Ideally, data and power cables must be at opposite ends of the physical rack. If they are aggregated in a bundle or run parallel to each other, induction may introduce electromagnetic interference.

Cable Colors

Using specific colors for cables from each device makes for easier troubleshooting.

- All cables from the management switch (except those going to the ToRs): yellow
- Management switch ports 49 and 50 going to the ToRs: black

- ToR 1 cables to servers: blue
- ToR 2 cables to servers: red
- ToR 1 and ToR 2 connections to spine switches: orange
- Console serial switch connections: grey

Cable Type and Length

The Telecommunications Industry Association (TIA) and the Electronic Industries association (EIA) structured cabling standards define how to design, build, and manage cabling systems. The specification is TIA/EIA-568-A. When used for 10/100/1000BASE-T Category 6 (Cat 6) cable length can be up to 100 meters (328 ft). This distance includes up to 90 meters (295 ft) of horizontal cabling between the patch panel and the wall jack, and up to 10 meters (33 ft) of patch cabling. When used for 10GBASE-T, Cat 6 cable length is reduced to 55 meters (180 ft) assuming minimal exposure to crosstalk. Category 6A (Cat 6A) does not have this limitation and can run at the same distances as 10/100/1000BASE-T.

Ensure that the cable type and length being used in your setup meet the following requirements.

- The cable connecting the physical server baseboard management controller (BMC) port to the management switch is 10 ft.
- The cable connecting the physical server 10 G interfaces to the ToR switches is 1-2 m (3.28-6.56 ft).
- The cable connecting the ToR switches 40G interfaces to the Spine switches is 1-2 m (3.28-6.56 ft).

Cable Bend Radius

Modifying the geometry of a cable can impair data transmission and affect performance. When a cable is tied or tightly looped, the pairs within the cable jacket can be separated impacting the integrity of the cable. Therefore, bend radius should be considered when verifying cable management.

- The minimum bend radius of a twisted pair patch cable is 4x the external cable diameter, and the minimum bend radius of an LC-type fiber optic cable is 0.8" (~2cm) and SC-type fiber optic cable is 1" (~3cm).
- Where articulated arms or rail slides are used, there must be sufficient slack in the cable to allow operation.
- No creases in the sheathing should be visible on any cable.

Cable Routing

Improperly routed cables can contribute to thermal issues, make field replaceable units difficult to access, or impact performance.

Cable ties can damage cables due to excessive over tightening or by violating the bend radius of a cable. Cable ties also increase service time when an add, move, or change request is received. Cables should be bundled with Velcro straps where possible to avoid damage, simplify addition or removal of cables, and reduce service times.

- Use velcro straps instead of cable ties.
- Network cables should not be in an area where there is a chance of contacting sharp edges, excessive heat, or subject to pinching between sliding rails.
- Cables must be free of tension. Where articulated arms or rail slides are used, there must be sufficient slack in the cable to prevent the cables from being stressed.
- Forced air cooling is recommended to draw cool air from the front of the rack and push warm air out the back.
- Ventilation slots, power supplies, and rear fans must be clear of cable obstructions.
- Field replaceable units such as power supplies must be clear of any cable obstructions that may prevent access for service.

Cable Labeling

Partners must label the cables in their datacenter. Properly labeled cables reduce troubleshooting time since it is easier to trace and validate connections.

Cable Testing

Cable testing ensures that the installed cabling links provide the transmission capability to support the data communication required.

Several tools are available for copper testing. Tests fall into three categories: Verification, Qualification, and Certification. Verification tools are used to perform basic continuity, cable length, and open connection verification. Qualification tools can provide information that details the cable capabilities, e.g. supports 10GBase-T. Certification tools determine whether the cable meets TIA standards such as TIA-568-B.

Options for testing SFP+ and QSFP+ cables are limited. Because handheld cable testers are not available, many network administrators typically reserve ports between two adjacent switches, then connect a suspect cable between active ports to determine if the cable is functional.

- Test cables from the physical server baseboard management controller (BMC) port and the management switch.
- Review the test print out to confirm that the cables passed the test.
- Cables from the physical server BMC port to the management switch must be seated properly.
- Cables from the physical server 10G interface to the ToR switches must be tested prior to installation. They must be seated properly.
- Each 10G interface must be connected to a separate ToR switch.

- Inter-switch SFP+ and QSFP+ cables must be tested prior to installation.
- Each 40G QSFP+ cable from the ToR switch must be connected to a separate Spine switch.
- There must be two 40G QSFP+ cable connections between each ToR switch and Spine switch.
- Inter-switch SFP+ and QSFP+ cables must be seated properly.

Rack Wiring

Download VCF Wiremap from the Product Downloads page and connect the wires in your physical rack according to the wiremap. This section contains the logical views of the wiremaps.

Wiring for Rack with Dell Management Switch

Figure 2-1. Wiremap for rack 1 with Cisco ToR Switches and Dell Management Switch

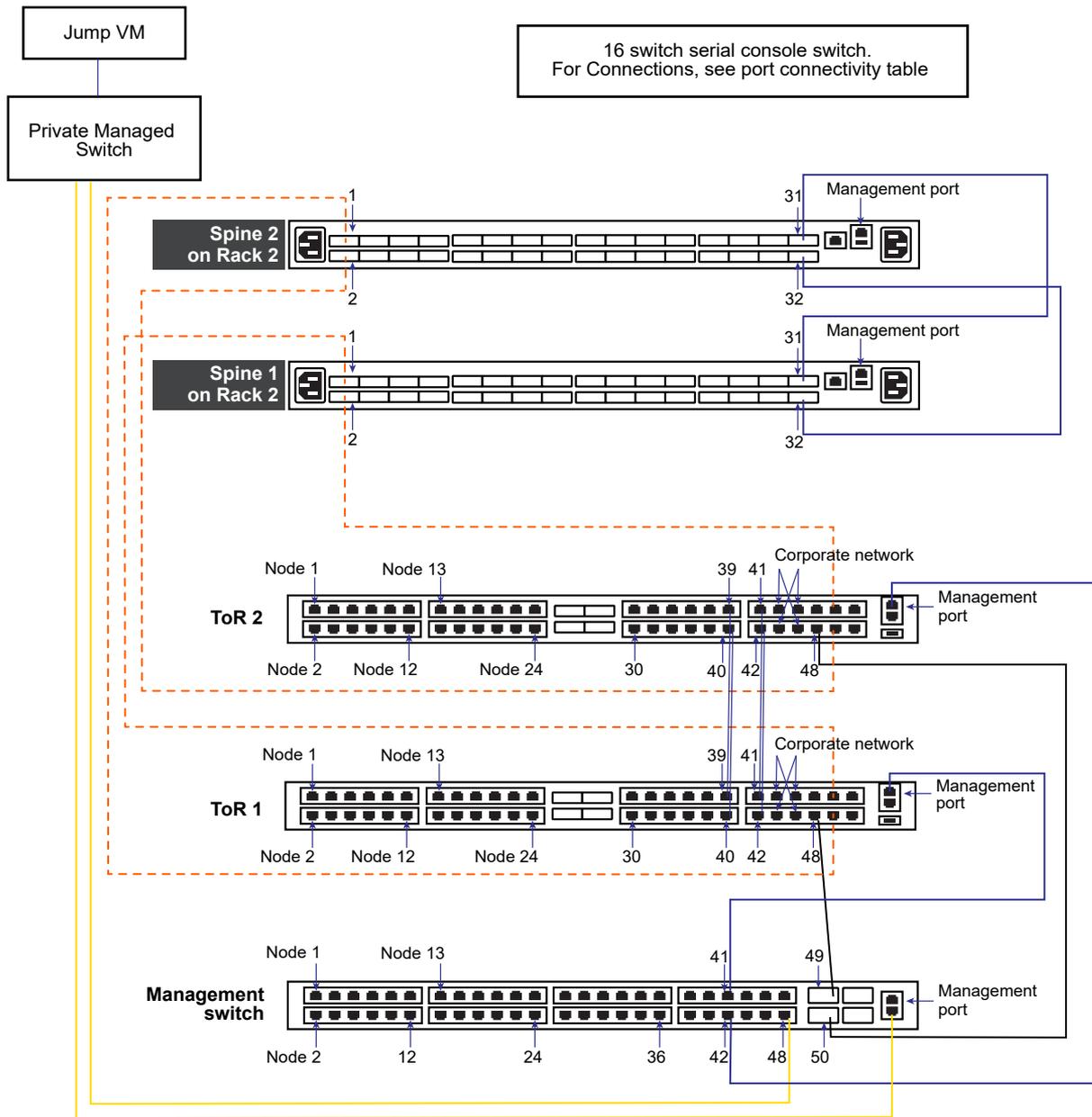
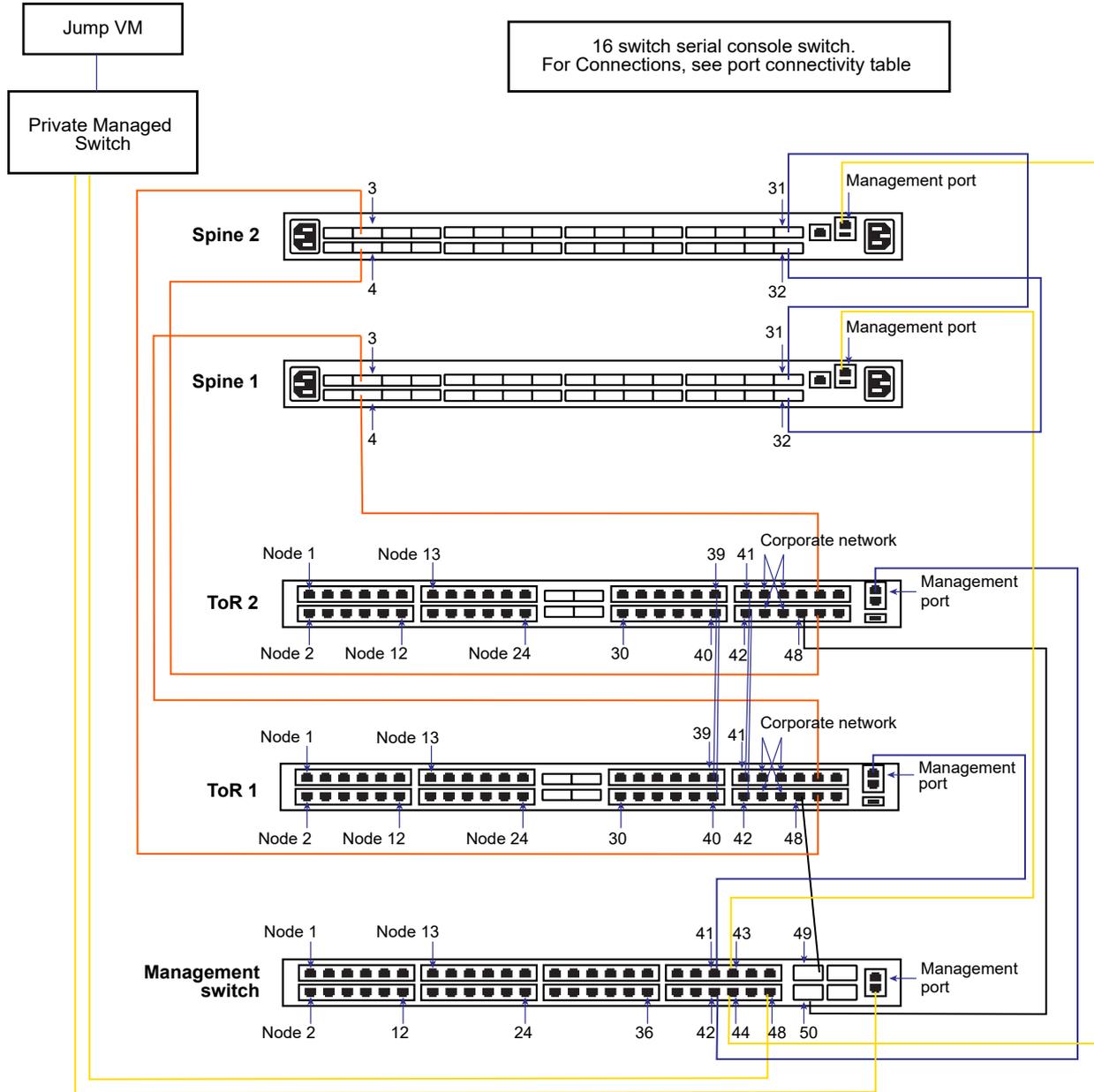


Figure 2-2. Wiremap for rack 2 with Cisco ToR Switches and Dell Management Switch



Wiring for Rack with Quanta Management Switch

Figure 2-3. Wiremap for rack 1 with Cisco ToR Switches and Quanta Management Switch

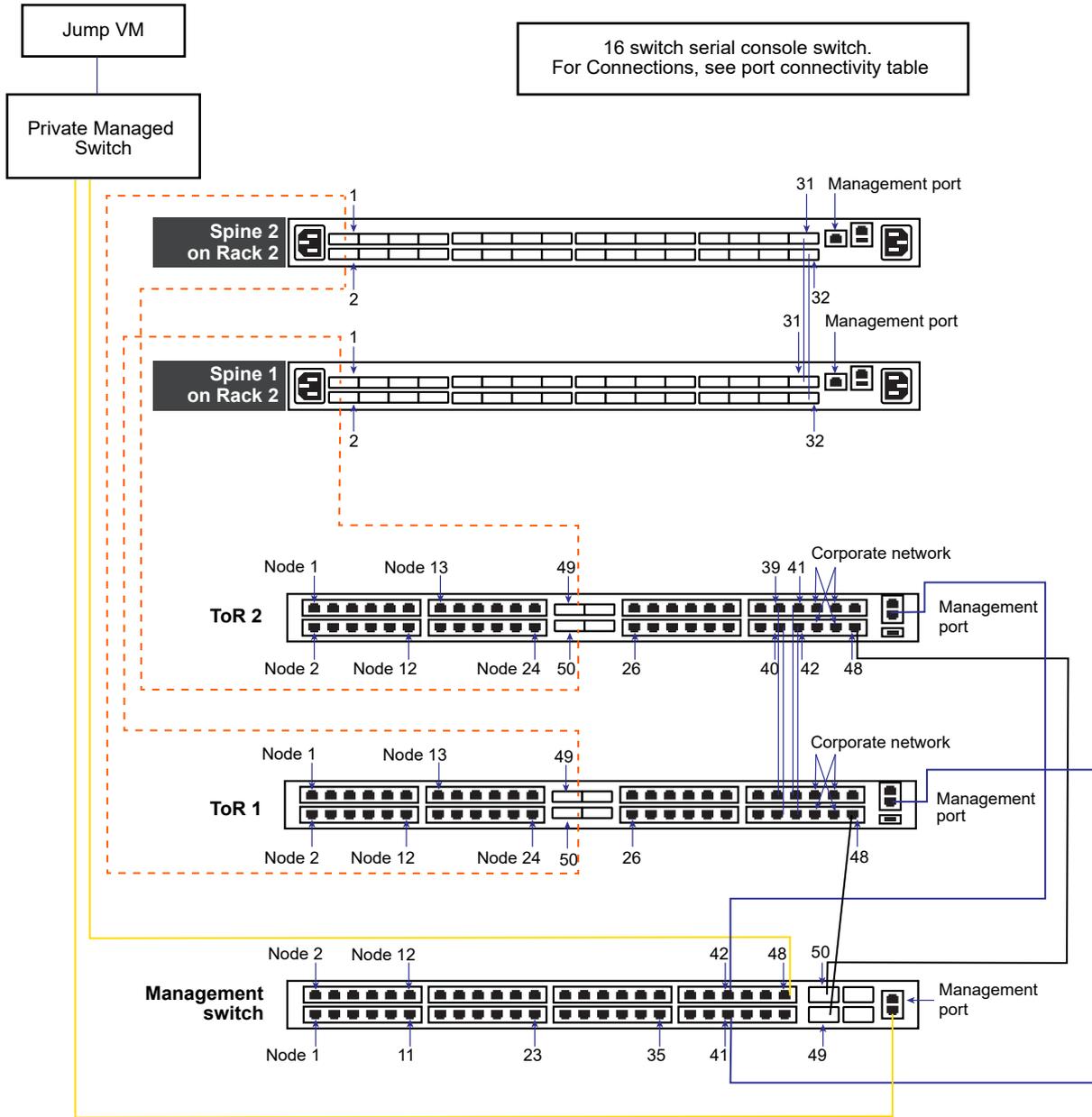
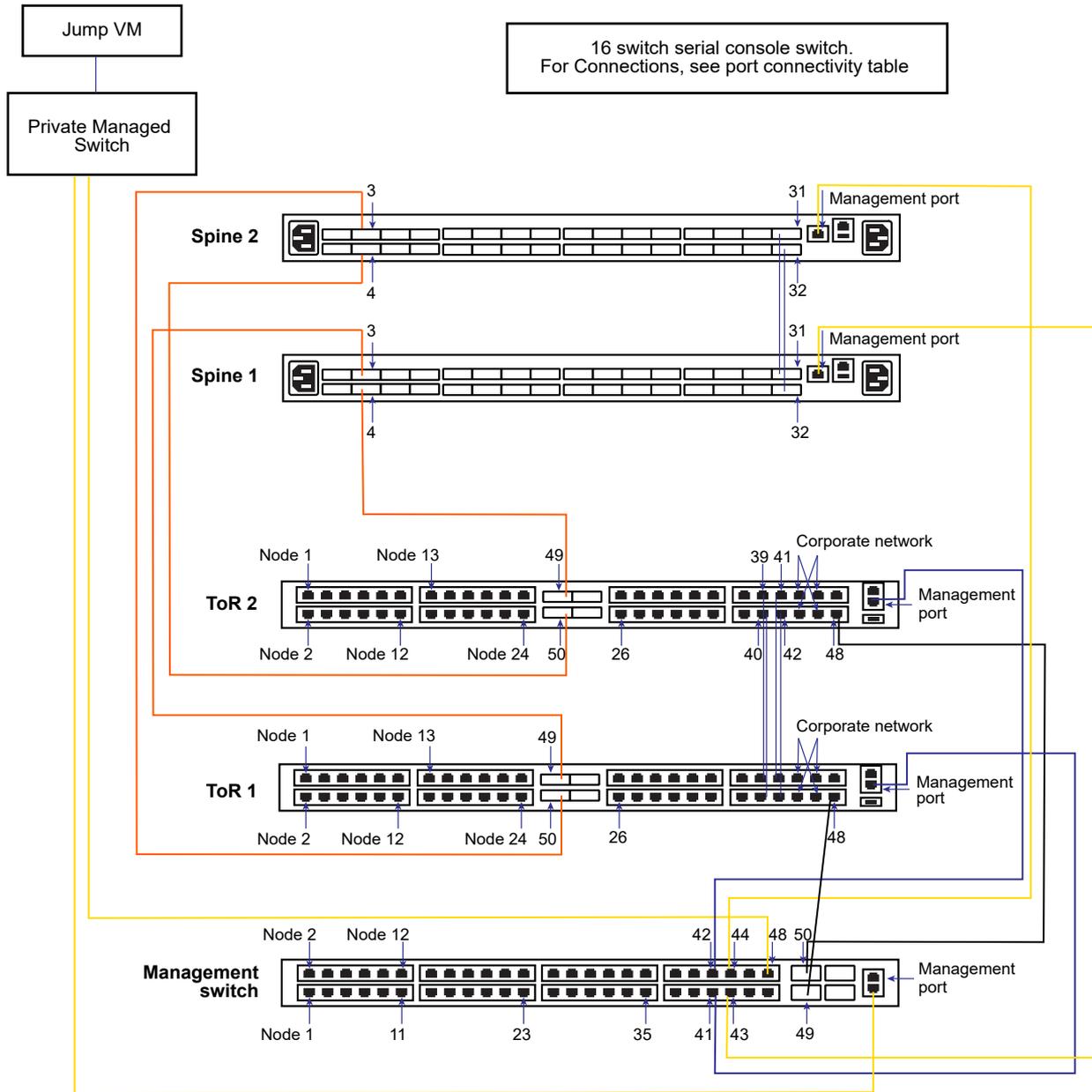


Figure 2-4. Wiremap for rack 2 with Cisco ToR Switches and Quanta Management Switch



Additional Racks

Rack 2 in the integrated system powered by Cloud Foundation must include two spine switches for inter-rack connectivity. The spine switches are connected during the physical environment inspection, but must be disconnected before imaging the rack.

Additional physical racks do not contain spine switches. ToR switches in the additional physical racks are connected to the two spine switches in rack 2.

Rack Component Ports

Refer to the tables below for port connectivity information using Cisco 9372PX as the illustrative example. Connections in your environment may vary based on the actual switches being used.

Console Serial Switch

Port Number	Connects To
1	Management switch console port
2	ToR 1 console port7
3	ToR 2 console port
4	Spine 1 console port
5	Spine 2 console port
6	PDU 1
7	PDU 2
8	PDU 3
9	PDU 4
10 - 16	Not connected

Spine 2 (Rack 2 only)

Port Number	Speed	Connects To
1	40 Gbps	Rack 2 ToR 1 port 50
2	40 Gbps	Rack 2 ToR 2 port 50
3	40 Gbps	Rack 1 ToR 1 port 50
4	40 Gbps	Rack 1 ToR 2 port 50
5	40 Gbps	Rack 3 ToR 1 port 50
6	40 Gbps	Rack 3 ToR 2 port 50
7	40 Gbps	Rack 4 ToR 1 port 50
8	40 Gbps	Rack 4 ToR 2 port 50
9	40 Gbps	Rack 5 ToR 1 port 50
10	40 Gbps	Rack 5 ToR 1 port 50
11	40 Gbps	Rack 6 ToR 1 port 50
12	40 Gbps	Rack 6 ToR 1 port 50
13	40 Gbps	Rack 7 ToR 1 port 50
14	40 Gbps	Rack 7 ToR 1 port 50
15	40 Gbps	Rack 8 ToR 1 port 50
16	40 Gbps	Rack 8 ToR 1 port 50

Spine 1 (Rack 2 only)

Port Number	Speed	Connects To
1	40 Gbps	Rack 2 ToR 1 port 49
2	40 Gbps	Rack 2 ToR 2 port 49
3	40 Gbps	Rack 1 ToR 1 port 49
4	40 Gbps	Rack 1 ToR 2 port 49
5	40 Gbps	Rack 3 ToR 1 port 49
6	40 Gbps	Rack 3 ToR 2 port 49
7	40 Gbps	Rack 4 ToR 1 port 49
8	40 Gbps	Rack 4 ToR 2 port 49
9	40 Gbps	Rack 5 ToR 1 port 49
10	40 Gbps	Rack 5 ToR 1 port 49
11	40 Gbps	Rack 6 ToR 1 port 49
12	40 Gbps	Rack 6 ToR 1 port 49
13	40 Gbps	Rack 7 ToR 1 port 49
14	40 Gbps	Rack 7 ToR 1 port 49
15	40 Gbps	Rack 8 ToR 1 port 49
16	40 Gbps	Rack 8 ToR 1 port 49

ToR 2 (e.g. Cisco 9372PX)

Port Number	Speed	Connects To
1 - 32	10 Gbps	node 1 - node 32 where port 1 connects to node 1, port 2 connects to node 2, and so on
33 - 38	NA	Not connected
39 - 42	10 Gbps	ToR 1 ports 39 - 42
43 - 47	10 Gbps	Corporate network as required (see note below table)
48	1Gbps	Management switch port 50
49	40 Gbps	Spine 1 port 2
50	40 Gbps	Spine 2 port 2
51 - 52	40 Gbps	Corporate network as required (see note below table)
Management	1 Gbps	Management switch port 42

Note Depending on the switches in your environment, connect two 40 Gbps ports or multiple 10 Gbps ports to your corporate network.

ToR 1 (e.g. Cisco 9372PX)

Port Number	Speed	Connects To
1 - 32	10 Gbps	Node 1 - node 32 where port 1 connects to node 1, port 2 connects to node 2, and so on
33 - 38	NA	Not connected
39 - 42	10 Gbps	ToR 2 ports 39 - 42
43 - 47	10 Gbps	Corporate network as required (see note below table)
48	1Gbps	Management switch port 49
49	40 Gbps	Spine 1 port 1
50	40 Gbps	Spine 2 port 1
51 - 52	NA	Corporate network as required (see note below table)
Management	1 Gbps	Management switch port 41

Note Depending on the switches in your environment, connect two 40 Gbps ports or multiple 10 Gbps ports to your corporate network.

Management Switch

Port Number	Speed	Connects To
1 - 32	1 Gbps	Node 1 - Node 32 where port 1 connects to node 1, port 2 connects to node 2, and so on
33 - 40	NA	Not connected
41	1Gbps	ToR 1 management port
42	1Gbps	ToR 2 management port
43	1Gbps	Spine 1 management port
44	1Gbps	Spine 2 management port
45-47	NA	Not connected
48	1Gbps	Private managed switch
49	10 Gbps	ToR 1 port 48
50	10 Gbps	ToR 2 port 48
51-52	NA	Not connected
Management port		Private managed switch

Note PDU ports are not reflected in the table above.

Physical Servers

This section lists the recommended Rack Unit (RU) location of each device.

Hardware Devices

Table 2-1. Physical Device Location in Rack 1 and Rack 3 - Rack n

RU Location	Device
42	Console serial switch
41	Blank
40	Management switch
39	Blank
38	ToR 2
37	Blank
36	ToR 1
33-35	Blank
1-32	Nodes 1-32

Table 2-2. Physical Device Location in Rack 2

RU Location	Device
42	Console serial switch
41	Management switch
40	Spine 2
39	Blank
38	Spine 1
37	Blank
36	ToR 2
35	Blank
34	ToR1
33	Blank
1-32	Nodes 1-32

Power

All servers must have redundant power supplies and each power supply must be connected to a separate rack PDU.

Airflow

Install the servers to allow front-to-back airflow.

BIOS Settings

The Bill of Materials (BOM) specifies the BIOS settings for each device. Ensure that the settings on the physical devices in your environment match the BIOS settings in the BOM. See [Chapter 8 BIOS Settings](#).

During imaging, VIA verifies the BIOS settings of Dell components but not for components from other vendors.

Firmware Settings

Ensure that the firmware settings are set correctly as per the BoM.

Network Switches

Power

- All switches must have redundant power supplies.
- Each power supply must be connected to a separate rack PDU.

Airflow

Switches must be installed to allow front-to-back airflow.

ONIE version

Ensure that the correct ONIE version is installed as per the BOM.

Laptop or Management Host

You need a laptop or management host where you install VIA.

Laptop

You need a desktop or laptop (Windows or Mac) with 4 GB memory and a multi core processor to access the jump VM. A Windows laptop must have Workstation 8 or later and a Mac should have Fusion 4 or later installed on it. You also need a network adapter, a cable, and a 4-port unmanaged switch.

Management Host

If you are using a management host to image the rack, you need a standalone VMware vSphere ESXi 6.0 or later server to host the Windows jump VM. The management host must have at least two NICs, with one NIC connected to the corporate network and one NIC connected to the private network. You also need a 24-port private managed switch.

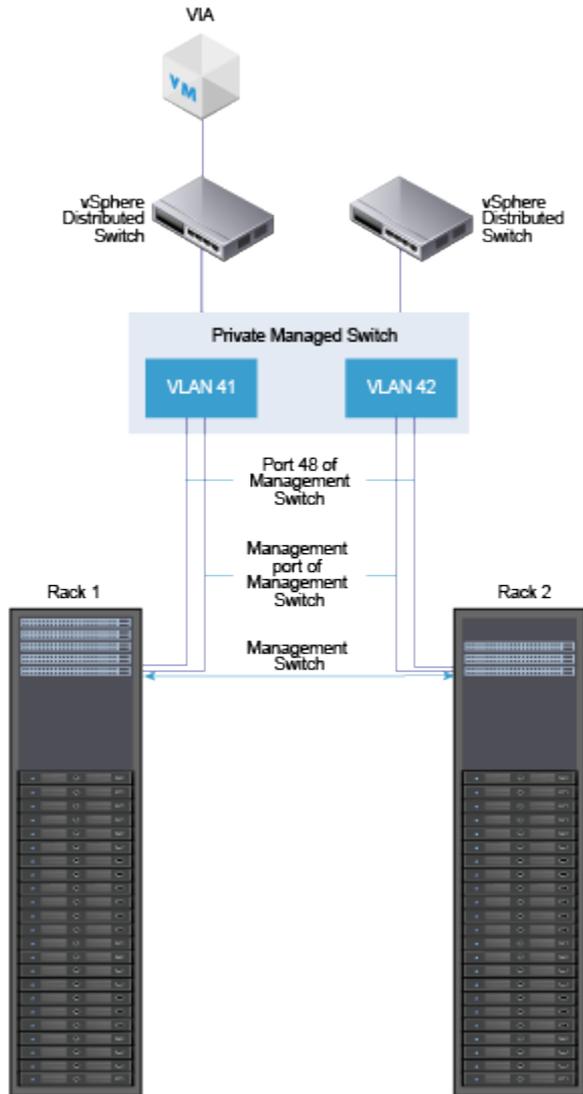
Table 2-3. VLAN Configuration of the Private Managed Switch

Port	Access Ports
1,2,3,4	VLAN 2000
5,6,7,8	VLAN 2001
9,10,11,12	VLAN 2002
13,14,15,16	VLAN 2003

Table 2-3. VLAN Configuration of the Private Managed Switch (continued)

Port	Access Ports
17,18,19,20	VLAN 2004
21,22,23,24	VLAN 2005

Figure 2-5. Management Host Connection



Private Managed Switch

If this is a multi-rack scenario and the private switch is being shared between racks, configure a private VLAN. For example, create two VLANs in a dual rack environment - VLAN 101 and VLAN 102. VLAN 101 is for rack 1 and VLAN 102 is for rack 2. Port 48 and the management port from the imaging management switch in rack 1 are connected to ports 2 and 3 on the private switch which

is configured for VLAN 101. Port 48 and the management port from the imaging management switch in rack 2 are connected to ports 4 and 5 on the private switch which is configured for VLAN 102. The imaging management host is connected to Port 1 which is configured for both VLAN 101 and VLAN 102.

A print out of the VLAN configuration on the imaging management switch should look like this:

```
interface Vlan 1
!untagged GigabitEthernet 0/0-1,6-47
!untagged TenGigabitEthernet 0/48-49
!untagged Port-channel 1-2
!
interface Vlan 2001
no ip address
tagged TenGigabitEthernet 0/48-49
untagged GigabitEthernet 0/2-3
no shutdown
!
interface Vlan 2002
no ip address
tagged TenGigabitEthernet 0/48-49
untagged GigabitEthernet 0/4-5
no shutdown
```

Management Host Settings

Configure the following settings on the imaging management host:

- Install ESXi on the local disk. For the supported version, see the *VMware Cloud Foundation Release Notes*.
- Enable the **Allow virtual machines to start and stop automatically with the system** option.
- Assign the IP address 10.1.0.200 to the vmk0 management network.
- Set the NTP server to 0.vmware.pool.ntp.org.

It is important to ensure that the time on the management host is set correctly.

- Enable SSH on the management host.

In a multi-rack scenario, configure an additional vSphere Standard Switch (vDS) for each additional rack. In a dual rack scenario, vSwitch1 should use vmnic1 and should be configured with two Virtual Machine Port Groups (VIA1 and VIA2). The VIA1 port group should be tagged to use VLAN101, and the VIA2 port group should be tagged to use VLAN102. vmnic1 should be connected to the private switch on a port with VLAN101 and VLAN102 visible.

Virtual Machines

The VIA VM runs on the laptop or management host. A jump VM runs on the management host.

If you have multiple physical racks in your environment, you have the following options:

- Image the racks sequentially - image rack 1 first followed by the remaining racks one at a time.
- Image the racks in parallel by configuring a VIA VM per physical rack.

Hardware Configuration

Table 2-4. Jump VM Hardware Configuration

Virtual Hardware	Value
Memory	4 GB
vCPU	1 virtual socket, 2 cores per socket
Video card	1 display
SSCI Controller 0	LSI Logic SAS bus sharing: none
Hard disk	120 GB, Thin Provision
CD/DVD	Client device
Floppy drive	Removed
Network adapters	2 VMXNET3 vNICs
Operating system	Microsoft Windows 7 64-bit or Win2K12
Virtual Machine version	Hardware version 8
Navigate to Options > Advanced > General	Disable logging keyboard.typematicMinDelay = "2000000"

Software Configuration

Perform the following tasks to prepare the jump VM.

- Install the Windows 2012 Essentials operating system on the VM.
- Install VMware Tools.
- Install the latest Windows patches.
- Enables Windows update using the VMware OS Optimization Tool.
- Install the following applications:
 - Firefox or Chrome web browsers
 - PuTTY
 - WinSCP
 - vSphere Web Client
 - VMware Ruby vSphere Console (RVC)
 - Java Runtime Environment

- If internet access is not available from the Access Virtual Machine, download the executables and binaries for the applications on the VM.
- Verify that Remote Desktop Connection is enabled on the Access Virtual Machine.
- Add a route to allow BMC access to the physical servers. For example,


```
route add 192.168.0.0 mask 255.255.255.0 192.168.100.1 if 16
```

 where *16* is the ID for rack 1. To find the interface number, follow the steps below.
 - a In a command window, type the command **netsh**.
 - b Type the command `int ipv4 show interfaces`.

Pre-Imaging Checklist

You must complete this checklist before beginning the imaging process. It is important that each item in the checklist is set to the specified value, otherwise imaging may fail. You may want to print this checklist and checkmark each row as you verify the setting.

Table 2-5. Pre-Imaging Checklist

Setting	Verified
Review the Bill of Materials (BOM) from VMware and verify that there are no discrepancies between the BOM and the hardware being used. If there is a discrepancy, contact VMware Support.	
Validate that BIOS Settings for all components are correct. See Chapter 8 BIOS Settings . During imaging, VIA verifies BIOS settings for DELL servers and makes appropriate adjustments. But it is recommended that you ensure that they are set correctly before you begin imaging.	
Ensure that the correct ONIE version is installed as per the BoM.	
Verify that firmware settings are set correctly as per the BoM.	
Connect each device in the rack to both PDUs.	
Keep power and network cable lengths to a minimum.	
Use specific colors for cables from each device. See Network Cables .	
Verify that the cable bend radius is proportionate to the external diameter. See Network Cables .	
Verify that cables are properly routed and labeled.	
Test cables to ensure that installed cabling links provide the transmission capability to support the required data communication.	
Verify that the physical racks are wired according to the wiremap. See Rack Wiring .	
Verify that each server has redundant power supplies and that each power supply is connected to a separate rack PDU.	
Ensure that servers and switches have the same airflow.	
Verify that switches have redundant power supplies and each power supply is connected to a separate power strip.	
Ensure that a supported version of ESXi is installed. For the supported version, see the <i>VMware Cloud Foundation Release Notes</i> .	

Table 2-5. Pre-Imaging Checklist (continued)

Setting	Verified
Verify that the Allow virtual machines to start and stop automatically with the system option is enabled.	
Assign IP address 10.1.0.200 to the vmk0 kernel interface.	
Verify that SSH is enabled on the management host.	
Verify that the access VM, VIA VM, and jump VM meet the required hardware configuration. See Virtual Machines .	
Verify that the required software has been installed on the VMs. See Virtual Machines .	

Installing VIA

3

You can install VIA on a desktop, laptop, or an ESXi host, also referred to as the management host. A laptop or desktop is recommended when you are imaging a single rack. A management host is better suited for an environment where you have several physical racks in your datacenter.

This chapter includes the following topics:

- [Installing VIA on a Laptop or Desktop](#)
- [Installing VIA on a Management Host](#)

Installing VIA on a Laptop or Desktop

VIA is a virtual appliance. After you install the VIA VM on your laptop, you copy the software bundle to the VIA VM. You can then access the VIA user interface through a browser on the laptop.

Prerequisites

- Ensure that you have the infrastructure for VIA available and that you have set up your physical environment as described in [Chapter 2 Before You Install VIA](#).
- Download the VIA OVF file, Cloud Foundation software bundle, and the md5sum file on the laptop or desktop.

Procedure

- 1 Connect one port of the network adapter to your laptop and one port to the unmanaged switch.
- 2 Connect two ports of the unmanaged switch as follows:
 - one port to the ethernet management port of the management switch
 - one port to port 48 of the management switch
- 3 Deploy the VIA OVF file on your laptop.

Follow the wizard prompts to specify where to save the OVF file and accept the license agreement.
- 4 Configure time settings on the laptop.

- 5 Upload the Cloud Foundation software bundle on to the VIA VM by pointing the CD /DVD drive to the bundle ISO. Ensure that the CD/DVD drive is connected.
- 6 Configure network settings on the laptop.
 - a Connect one NIC on the laptop to the corporate network and the other to the unmanaged switch.
 - b Manually assign a static IP address to the laptop in the range 192.168.100.151 to 192.168.100.199.

This allows for separation of network traffic between the corporate network and the private network that is established between the physical rack and VIA. It also helps ensure that the DHCP service which is part of is VIA is confined to the private network between the physical rack and VIA.

- 7 For the browser on the laptop that will be used to access VIA, make the following selections.
 - In Network Connection, disable the proxy.
 - Select **Auto-detect proxy settings for this network** so that the browser detects the proxy settings for your network.
- 8 Ensure that you can ping the VIA VM (IP address is 192.168.100.2) from the laptop.
- 9 Power on the VIA VM.
- 10 Ensure that you can ping the management switch (IP address 192.168.100.1) from the VIA VM.

Since the management switch is the first component to be imaged, the VIA VM must be able to talk to the management switch.

What to do next

Open a web browser on the laptop and type the following URL to connect to VIA:

`http://192.168.100.2:8080/via/`

Installing VIA on a Management Host

Prerequisites

- Ensure that you have the infrastructure for VIA available and that you have set up your physical environment as described in [Chapter 2 Before You Install VIA](#).
- Download the VIA OVF file, Cloud Foundation software bundle, and the md5sum file on your local file system.

Procedure

- 1 Deploy the VIA OVF file on the management host.
 - a Login to the vSphere Web Client on the management host.
 - b Right-click the management host and click **Deploy OVF Template**.

- c In source location, select **Local file**. Click **Browse** and select the VIA OVF from your local file system.
 - d Click **Next**.
 - e Review the OVF file details and click **Next**.
 - f Accept the OVF license agreements and click **Next**.
 - g Specify a name and location for the OVF and click **Next**.
 - h Select a resource and click **Next**.
 - i Select the disk format to store the VIA disks and the datastore to store the deployed OVF template and click **Next**.
 - j On the Setup networks page, connect VIA to the private switch connected to rack 1.
 - k Review the deployment details and click **Finish**.
- 2 Copy the Cloud Foundation bundle to the management host.
 - a On the management host, create a single datastore named datastore1.
 - b In datastore1, create a folder named ISO bundle and copy the Cloud Foundation bundle file to this folder.
 - 3 Configure time settings on the management host.
 - a In the vSphere Web Client, navigate to the management host in the vSphere inventory.
 - b Select **Manage** and then select **Settings**.
 - c Under **System**, select **Time configuration** and click **Edit**.
 - d Select **Manually configure the date and time on this host**.
 - e Set the time and date manually.
 - f Click **OK**.
 - 4 Upload the software bundle on to the VIA VM.
 - a Right-click the VIA VM and select **Edit Settings**.
 - b Click the **Hardware** tab and select the CD/DVD drive.
 - c Select the **Connected** check box to connect the CD.
 - d Select **Connect at power on** so that the CD-ROM drive is connected when the virtual machine starts.
 - e Select **Datastore ISO** under **Device Type**.
 - f Click **Select**, browse to the ISO Bundle folder in datastore1 on the management host, and select the bundle.
 - g Click **OK**.

- 5 Create a VM on the management host to serve as the jump VM.

Connect one NIC on the jump VM to the network and the other to the private managed switch.

The jump VM must have a static IP address. The IP range 192.168.100.151 to 192.168.100.199 is usually available for the jump VM. Verify the address that you want to use against the `via.properties` file in the bundle ISO to avoid any conflict.

This allows for separation of network traffic between the datacenter network and the private network that is established between the physical rack and VIA. It also helps ensure that the DHCP service which is part of is VIA is confined to the private network between the physical rack and VIA.

- 6 Copy the `md5sum` file on the jump VM.

- 7 For the browser on the jump VM that will be used to access VIA, make the following selections.

- In Network Connection, disable the proxy.
- Select **Auto-detect proxy settings for this network** so that the browser detects the proxy settings for your network.

- 8 Ensure that you can ping the VIA VM (IP address is 192.168.100.2) from the jump VM.

If you cannot ping the VIA VM, check the route on the jump VM.

- 9 Power on the VIA VM.

- 10 Ensure that you can ping the management switch (IP address 192.168.100.1) from the VIA VM.

Since the management switch is the first component to be imaged, the VIA VM must be able to talk to the management switch.

What to do next

Open a web browser and type the following URL to connect to VIA:

`http://192.168.100.2:8080/via/`

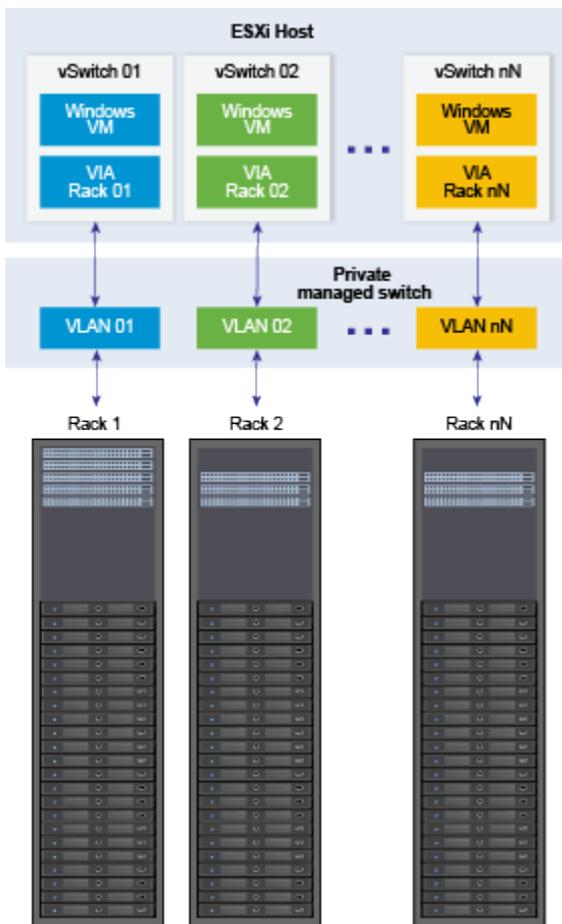
Imaging Physical Racks

4

When you image a physical rack, the software in the manifest bundle is loaded onto the physical rack.

In a multi-rack environment, you can either image all racks in parallel, or image rack 1 first followed by the other racks one at a time. To image multiple racks in parallel, you need a vSphere Distributed Switch and VIA VM for each rack.

Figure 4-1. VIA Setup for Parallel Imaging of Multiple Physical Racks



This chapter includes the following topics:

- [Image a Physical Rack](#)

- [Retrieve SDDC Manager Password and Rack Thumbprint](#)
- [Resume Imaging](#)
- [Image Additional Racks](#)

Image a Physical Rack

VIA images the rack components in a pre-determined order, which is determined by the availability of network route to the different components of the rack. All switches are imaged first. This enables VIA to access the servers through the switches for imaging. The imaging order is as follows.

1 Management switch

The management switch is the main access gateway through which the Cloud Foundation management data is routed. The management ports of the ToR switches, Spine switches, and the physical servers are connected to the management switch. The data ports of the ToR switches are also connected to the management switch. This enables VIA to communicate with the servers over both management and data network through the management switch. VIA is also connected to the rack through a designated port on the management switch. It is therefore required that the management switch is the first component imaged by VIA in order to obtain access to the other components of the rack. VIA currently uses an IPMI connection to image the management switch.

2 Spine switches (rack 2 only) and ToR switches

Spine and ToR switches are imaged in parallel.

Spine switches inter-connect multiple racks enabling a scale out architecture for the datacenter. They create an stretched L2 backplane between racks.

ToR switches provide connectivity to servers in each rack out to spine switches. The first pair of ToR switches provide connectivity to your datacenter network.

3 Servers

The management ports on the servers become accessible to the management switch during the course of imaging/configuration, which in turn make the management ports accessible to VIA through the management switch. Once all the switches are imaged and configured, the data ports of the servers become accessible to VIA through the ToR switches, which then proceeds to image the servers in parallel.

For each component that is being imaged, the following tasks are performed.

1 Discovery

Rack components are discovered using the DHCP service running on the VIA VM. The DHCP Service uses the device type information to identify the device being discovered. Apart from the device type information, the DHCP service also uses hardware vendor specific strings to determine whether the switch being imaged is a management, ToR, or Spine switch.

The first component to be discovered is the management switch. The DHCP service hands out a pre-determined IP address for the management switch followed by a PXE image specific to the management switch.

After the management switch is imaged, the ToR and Spine switches are discovered and imaged. The management switch also discovers the IPMI network of the servers. This allows VIA to initiate imaging of the servers. The ToR switch enables discovery of the data network of the servers which is used to receive the installation image delivered by the DHCP service.

2 Image installation

Image installation refers to installing software on the components to make them operational. The software depends on the component type - an Operating System for switches and a Hypervisor for servers.

3 Configuration

This step in the imaging process ensures that the components of the rack work like a homogenous system. Configuration of each rack component is different. If any configuration step fails for the management, ToR, or spine switches, imaging stops at that point and cannot proceed. If a configuration step fails for the server, imaging for that server cannot be completed but the remaining servers in the rack can be imaged.

Table 4-1. Management Switch Configuration

Number	Step Name	Description
1	Apply license	Apply the relevant license to the installed image
2	Configure ports	<ol style="list-style-type: none"> 1 Configure the ports which allow the management switch to connect to the management interfaces of the ToR and spine switches and the servers. 2 Bridge the ports connected to VIA with the ports connected to the management interfaces of the ToR and spine switches. 3 Create separate subnets for the management network and data network of the rack.
3	Update interface	Ensure that only the management interfaces of ToR and spine switches are enabled while the management interfaces of the servers and the data network interfaces of the ToR switches are disabled before initiating the imaging of ToR switches.
4	Setup persistent network	<ol style="list-style-type: none"> 1 Wait till all ToRs are imaged and bridge the ports connected to VIA with the ports connected to the management interfaces of the ToR and spine switches and servers to enable VIA to listen to DHCP requests. 2 Setup Spanning Tree Protocol (STP) on the IPMI management interfaces of the ToR and spine switches and servers. 3 Setup STP on the Cloud Foundation management interfaces of the ToR switches and the interfaces connected to VIA. 4 Enable LACP on ToR data interfaces. 5 Create separate subnets for the management network and data network for the rack.
5	Setup IPMI DHCP	Set up a DHCP service to discover the IPMI network of the servers.

Table 4-1. Management Switch Configuration (continued)

Number	Step Name	Description
6	Host Power Cycle	Discover all servers and ensure that the minimum required servers are available to ensure that SDDC Manager can be deployed. If the requirement is met, VIA initiates a power cycle of all servers to initiate their imaging. If the required number of servers are not detected, imaging is cancelled.
7	Change Password	Change the default password to connect to the switch and stores the new password in a password store.
8	Generate Manifest	Generate device manifest, which contains the current state of the imaging activity for each rack component.

Table 4-2. ToR Switch Configuration

Number	Step	Description
1	Apply license	Apply the relevant license to the installed image.
2	Configure ports	Configure all ports on the switch to operate in Full Duplex mode with auto negotiation enabled and at 1000Mb/s.
6	Change password	Change the default password to connect to the switch and stores the new password in a password store.
7	Generate Manifest	Generate device manifest, which contains the current state of the imaging activity for each rack component.

Table 4-3. Spine Switch Configuration

Number	Step	Description
1	Apply license	Apply the relevant license to the installed image.
5	Change password	Change the default password to connect to the switch and stores the new password in a password store.
6	Generate Manifest	Generate device manifest, which contains the current state of the imaging activity for each rack component.

Table 4-4. Node 0 Configuration

Number	Step
1	Wait for kickstart delivery.
2	Check host status.
3	Install VIBs.
4	Run storage configuration script.
5	Check VSAN setup.
6	Reboot host.
7	Post- ESXi installation configuration.
8	Verify disk status.
9	Create user task.
10	Check VSAN status after reboot.

Table 4-4. Node 0 Configuration (continued)

Number	Step
11	Deploy LCM.
12	Shutdown LCM.
13	Take LCM snapshot.
14	Deploy LCM backup VM.
15.	Shutdown backup LCM VM.
16	Take backup LCM snapshot.
17	Deploy ISVMs.
18	Shutdown ISVMs.
19	Take ISVM snapshot.
20	Deploy VRM.
21	Post VRM installation configuration.
22	Set VM startup shutdown order.
23	Upload bundle ISO.
24	Add ISO to VRM.
25	Collect inventory.
26	Import SSH public keys.
27	Copy PRM manifest.
28	Copy HMS IB inventory.
29	Create VRM snapshot.
30	Reboot VRM.

Table 4-5. Configuration on Remaining Nodes

Number	Step	Description
1	Install Custom VIBs	Install any custom VIBs that may be necessary to enable vendor specific devices on the server.
2	Reboot server	Reboot the server to complete the installation process.
3	Apply licence	Apply ESXi licence.
4	Create user	Create a new ESXi user with Administrator role.
5	Generate manifest	<p>Generate device manifest, which contains the imaging status of the device, the IP address assigned, the software used to image it, etc.</p> <p>This is performed on all components irrespective of whether the previous steps were successful or not. This allows VIA to track the status of imaging of any given component during any stage of the imaging process.</p>

Imaging is a multi-step process.

Procedure

1 Upload Software Bundle

The software bundle ISO file contains the software bits and scripts to be imaged on the physical rack. You can upload multiple bundles at a time and activate the bundle that is to be used for imaging.

2 Specify Imaging Details

At the Details step of an imaging run, you provide a name and description for the imaging run as well component and port information for the rack.

3 Monitor Imaging

In the Monitor Imaging step of the imaging workflow, you can see the imaging status on all devices in your physical rack.

4 Verify Inventory

In the Verify step of the imaging workflow, the system collects inventory information for each device in the rack.

5 Post Imaging Checks

In the final step of the imaging workflow, VIA creates a rack inventory file.

Upload Software Bundle

The software bundle ISO file contains the software bits and scripts to be imaged on the physical rack. You can upload multiple bundles at a time and activate the bundle that is to be used for imaging.

The bundle contains the following software:

- vSphere (vCenter Server and ESXi)
- NSX
- vSAN
- vRealize Log Insight
- SDDC Manager
- Platform Services Controller
- VMware Horizon with View
- App Volumes

Prerequisites

- Download the Cloud Foundation software bundle and the md5sum file on your laptop, desktop, or jump VM.

- If you are re-purposing hosts in your datacenter, backup the data on the hosts. They are wiped clean during imaging.
- Ensure that the KVM console for servers is closed.
- (Optional) For Dell servers only, install the Dell RACADM utility on VIA.
 - a Download the Dell OpenManage Linux Remote Access Utilities package from <http://www.dell.com/support/home/us/en/04/Drivers/DriversDetails?driverId=X9WN2>.
 - b Unzip the tarball.


```
tar -xzf filename
```
 - c Navigate to the RPM location.


```
cd linux/rac/SLES11/x86_64/
```
 - d Install the package.


```
rpm -Uhv *.rpm
```

The RACADM utility sets most of the BIOS parameters for Dell servers automatically except for DHCP and IPMI.

- For Dell servers only, set the following BIOS parameters.
 - Enable DHCP on the iDRAC/BMC port.
 - Enable IPMI over LAN on BMC.

For servers from other vendors, all BIOS settings need to be set manually. See [Chapter 8 BIOS Settings](#).

- For Cisco UCS servers only, set the following values on the servers before imaging the rack.
 - Out-Band Cisco Integrated Management Controller User Name=admin
 - Out-Band Cisco Integrated Management Controller User Password=password

Procedure

- 1 In a browser window on the jump VM, type <http://192.168.100.2:8080/via>.

2 Click **Bundle**.

VIA 2.0

Bundle | Imaging | Inventory | History | Logs | About | (0)

Upload Bundle

Bundle Location

CD/DVD Drive: CD mounted successfully Refresh

Bundle Hash

MD5SUM File: Browse

Upload Bundle

3 In the **Bundle Location** area, click **Refresh**.

Wait for the message **CD mounted successfully** to be displayed.

4 In the **Bundle Hash** area, click **Browse**, navigate to the directory that contains the MD5SUM file, select the file, and click **Open**.

5 Click **Upload Bundle**.

VIA 2.0

Bundle | Imaging | Inventory | History | Logs | About | (0)

Upload Bundle

Bundle Location

CD/DVD Drive: CD mounted successfully Refresh

Bundle Hash

MD5SUM File: MD5SUM.txt Browse

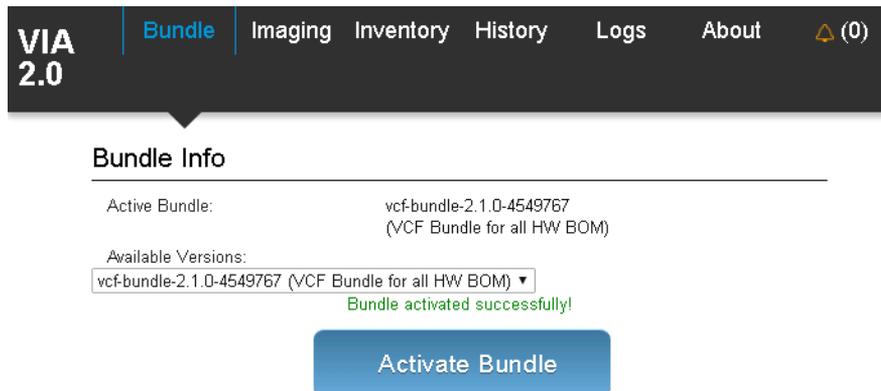
Completed: 7% 4 minutes, 31 seconds remaining

Upload Bundle

The bundle upload can take several minutes. After the upload is complete, the message **Bundle uploaded successfully** is displayed in the Upload Bundle area.

- 6 In the **Bundle Info** area, select the bundle in **Available Versions** and click **Activate Bundle**.

The selected bundle is now the active bundle for imaging and is ready to be used. Active bundle details are displayed next to **Active Bundle**.



VIA 2.0

Bundle | Imaging | Inventory | History | Logs | About (0)

Bundle Info

Active Bundle: vcf-bundle-2.1.0-4549767
(VCF Bundle for all HW BOM)

Available Versions:
vcf-bundle-2.1.0-4549767 (VCF Bundle for all HW BOM) ▼

Bundle activated successfully!

Activate Bundle

- 7 (Optional) Verify that the ISO file and `manifest.xml` file are copied to the VIA VM.

- a In a console window, SSH to the VIA VM.

```
ssh root@192.168.100.2
```

The password is root123.

- b Navigate to the `/mnt/cdrom/` directory.
- c Confirm that the bundle directory and `manifest.xml` are in this directory.

Specify Imaging Details

At the Details step of an imaging run, you provide a name and description for the imaging run as well component and port information for the rack.

Prerequisites

- Software bundle must have been uploaded and activated.
- iDRAC and KVM consoles must be closed. If an iDRAC console is open, imaging may fail.

Procedure

- 1 In the VIA user interface, click **Imaging**.

Ensure that you are in the **Details** tab.

The screenshot shows the VIA 2.0 user interface with the 'Imaging' tab selected. The 'Details' sub-tab is active. The form contains the following sections:

- Name:** Text input field with placeholder 'Provide a name for your new imagin'.
- Description:** Text input field with placeholder 'Provide descriptive text for your ima'.
- Deployment Type:** Dropdown menu set to 'Cloud Foundation Full Deployment'.
- MGMT Switch:** Configuration for a management switch with Vendor: Quanta Computers Inc., Model: Quanta-LB9, IP: 192.168.1.1, and MAC: Optional.
- TOR Switch:** Two configuration entries for TOR switches. Both have Vendor: Quanta Computers Inc., Model: Quanta_LY8-x86, and IP: 192.168.0.2. The first has MAC: Optional.
- Spine Switch:** Configuration with a Number field set to 0.
- Server:** Configuration for servers with 'All Flash' selected and Number: 4. Two entries are shown with Vendor: Dell Inc., Model: PowerEdge R620, and IP: 192.168.1.C. Both have MAC: Optional.

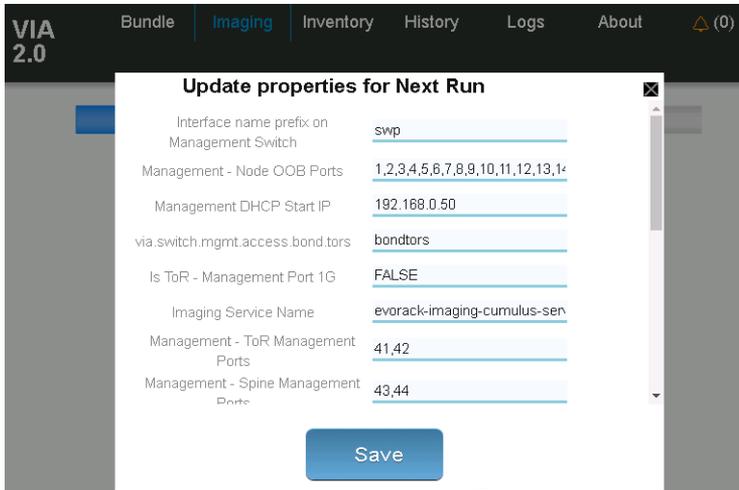
A blue 'Start Imaging' button is located at the bottom of the form.

- 2 (Optional) Type a name and description for the imaging run.
- 3 In **Deployment Type**, select **Cloud Foundation Full Deployment**.
- 4 In **Rack Type**, select **Primary Rack** if you are imaging rack 1. For additional racks, select **Add-On Rack**.
- 5 For the management switch and ToR switches, select the vendor and model.
The IP address for each switch is displayed.
- 6 Type the MAC address of each switch.
- 7 If the physical rack contains spine switches (rack 2 only), type the number of spine switches in the **Number** field in the **Spine Switch** section.
- 8 Select the vendor and model number of the spine switches.
- 9 In the **Server** section, type the number of servers in the physical rack.

- 10 Select the vendor and model number of each server. The IP address for each server is displayed.

Note Ensure that you have selected the component models correctly. VIA enforces a strict matching of the server models selected during imaging against what is discovered by VIA. If they do not match, imaging fails.

- 11 Type the MAC address of each server.
- 12 Click  in any section to view the VIA properties file.

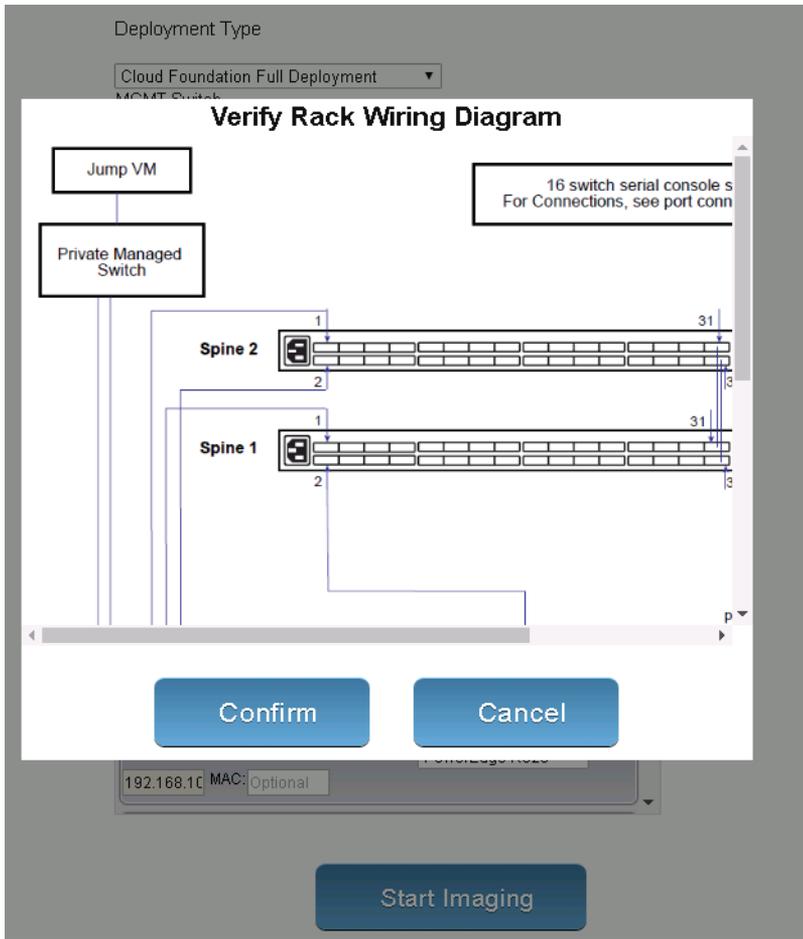


The VIA properties file displays rack specification values from the activated software bundle.

- If required, edit the file as appropriate. For example, delete the ToR OOB ports that you are not using to speed up the imaging process.
- Ensure that the **ESXi Disk-Type** value matches the actual boot device name (scroll to the bottom of the page to see this field). Edit the value if required.
- For Cisco servers, check the default values for VMNIC1 and VMNIC2. If the defaults are not accurate, edit the values based on which 10G port on the server's Network Card is connected to ToR 1 and ToR 2.

- 13 Click **Save**.

14 Click **Start Imaging**. The wiring diagram for the rack is displayed.



Review the wiring diagram to check if your rack is wired according to displayed wiremap. See [Rack Wiring](#).

Click **Confirm** if it is accurate. If you need to make any wiring changes, click **Cancel**.

What to do next

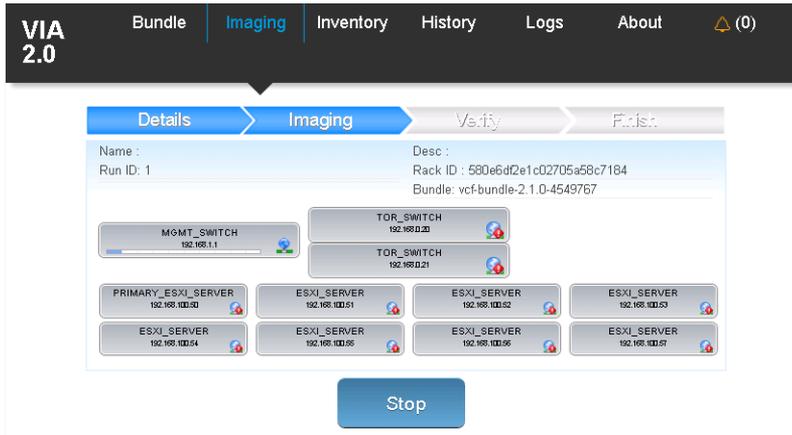
Once imaging starts, notifications (errors, warnings, and information) are displayed in the top right corner of the VIA window. Click the  icon to review the messages so that you can take the appropriate steps to complete the imaging successfully.

Monitor Imaging

In the Monitor Imaging step of the imaging workflow, you can see the imaging status on all devices in your physical rack.

Procedure

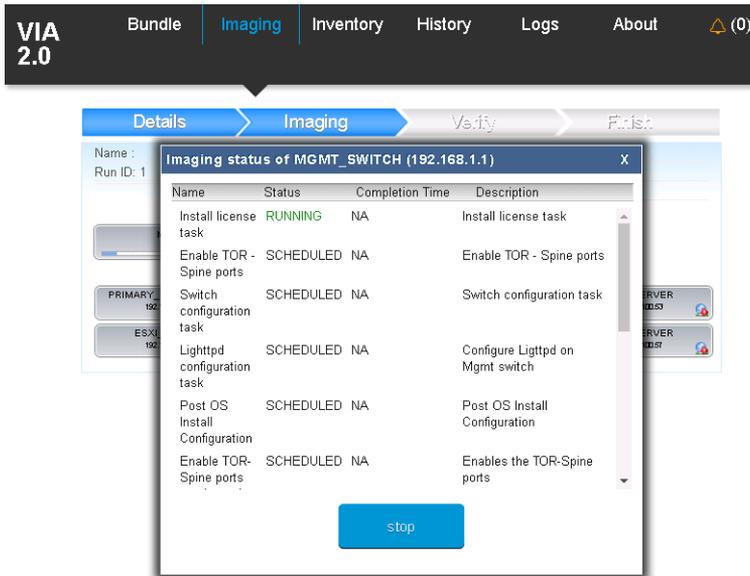
- 1 Click the **Imaging > Imaging** tab.



The run details, rack details, and imaging status for the rack are displayed. The devices in the physical rack are displayed in the order in which they will be imaged.

Note Note the Run ID. You will need it to retrieve the rack thumbprint after imaging is completed.

- 2 Click a device to see information about the imaging tasks completed and in-progress tasks.



It can take approximately 95 minutes for rack 1 to be imaged. After the imaging is completed successfully, the **Imaging > Verify** tab is displayed.

Note During imaging, the password of all rack components except SDDC Manager is set to EvoSddc!2016. The SDDC Manager password is set to a random string, which can be retrieved by an API call.

Note For VCE racks, the ScaleIO VIB needs to be manually installed.

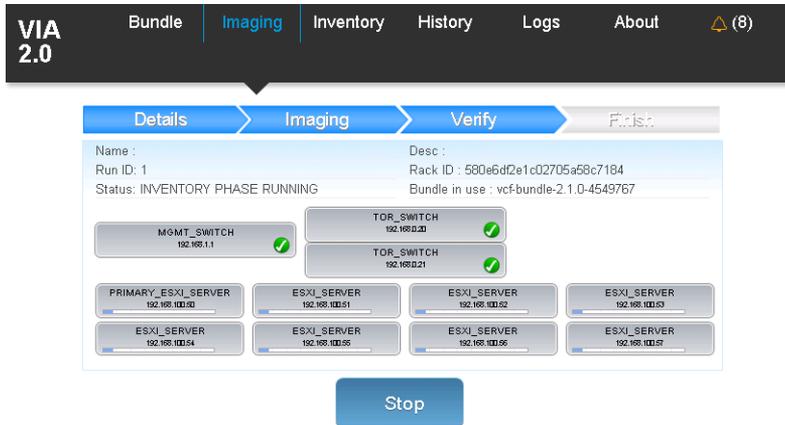
For information on next steps if a device fails to be imaged, see [Resume Imaging](#).

Verify Inventory

In the Verify step of the imaging workflow, the system collects inventory information for each device in the rack.

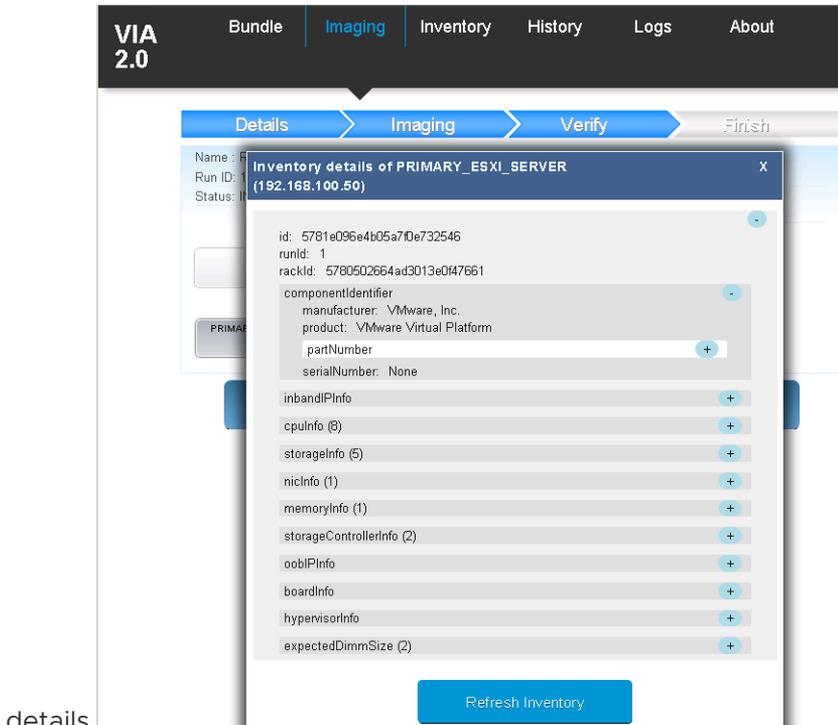
Procedure

- 1 Click the **Imaging > Verify**



The status of inventory collection on each device in the rack is displayed.

- 2 Click a device to see its inventory information. You can expand a component to see more



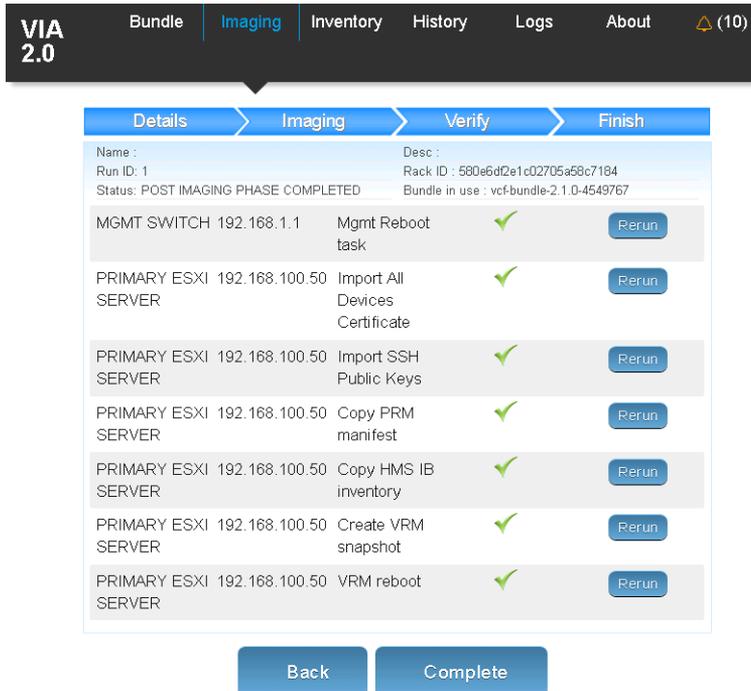
details.

Post Imaging Checks

In the final step of the imaging workflow, VIA creates a rack inventory file.

Procedure

- 1 Click the **Imaging > Finish** tab.



Post imaging tasks are displayed.

- 2 If a task is not completed successfully, click **Rerun**.
- 3 After each displayed task has an ✓ icon next to it, click **Finish**.

The rack inventory file is created for the customer. This file includes the SDDC Manager password generated during imaging. The imaged rack is now ready to be shipped to the customer.

- 4 Power down the primary rack.

It is important to power down the rack even if you are deploying Cloud Foundation on a ready system so that the management switch is rebooted.

Retrieve SDDC Manager Password and Rack Thumbprint

During imaging, VIA generates a password for the root account of SDDC Manager and a thumbprint for the imaged rack. Both of these are required by the customer.

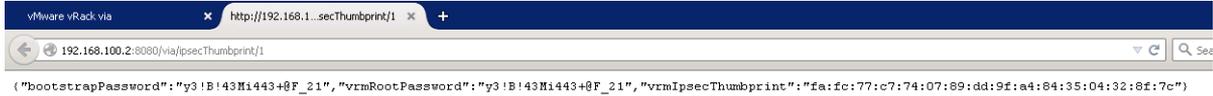
Procedure

- 1 Open a new tab in the browser where you were imaging the rack.

- 2 Type the following:

```
192.168.100.2:8080/via/ipsecThumbprint/runId
```

The browser displays the SDDC Manager password, bootstrap password, and rack thumbprint.



- 3 Print the output.

If you are a partner imaging the rack for a customer, send this print out to the customer along with the imaged rack.

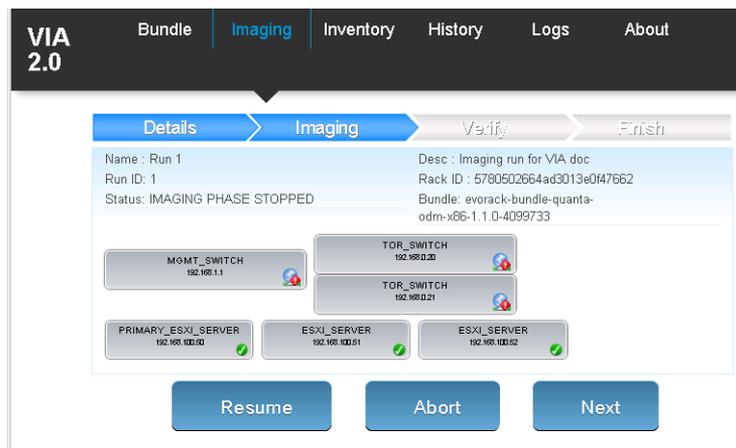
If you are imaging your own rack, keep this print out. You will need this password during bring-up.

Resume Imaging

A device may fail to be imaged because of possible hardware faults or mis-configuration, or network issues. You can take a number of actions that can help in continuing with the imaging run.

Fix Issues During the Monitor If you are able to resolve the hardware problem, click r Imaging Step

During the monitor step in the imaging workflow, you can identify imaging failures by looking at the progress bar on the components in the **Imaging > Imaging** tab. An  icon indicates that it has been imaged successfully. An  icon indicates that one or more imaging tasks on that devices failed.



- 1 Click the component to display the imaging task list for that device. Then do one of the following:
 - Click **Retry** to re-start imaging on that device .

- Click **Remove** to remove that device from the VIA UI and database and then click **Yes** to confirm. The removed device is grayed out and it is not imaged. Ensure that you remove this device from the physical rack before shipping it to the customer. To add a removed device back to the VIA UI, click the device and click **Add to Inventory**. The device is added back to the VIA UI and database.

If the primary ESXi server fails to be imaged, you cannot resume imaging by removing it. It is mandatory for the primary server to be imaged.

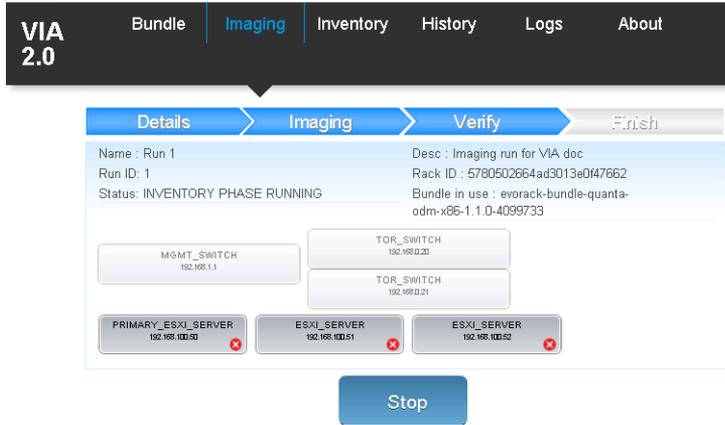
- 2 If you need to resolve a hardware issue before re-trying imaging on that device, close the task list dialog box. In the **Imaging > Imaging** window, click **Stop**.
- 3 If you are able to resolve the hardware problem, click **Resume**. Imaging is resumed from the state where it had stopped. If you need additional time to resolve the hardware issue or there are other hardware problems, click **Abort**. The imaging run is discarded.

If you are unable to resolve the hardware issues, contact VMware Support.

- 4 Click **Next** to proceed to the next step in the workflow.

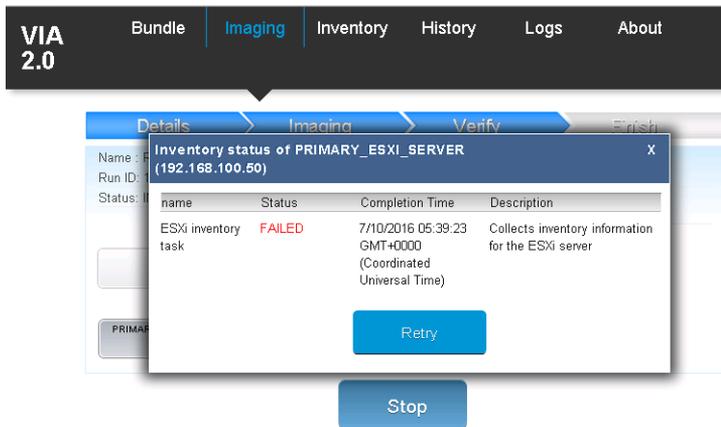
Fix Issues During the Verify Imaging Step

During the verify step in the imaging workflow, you can identify imaging failures by looking at the progress bar on the components in the **Imaging > Verify** tab. An  icon indicates that inventory information has been collected successfully. An  icon indicates that the tasks on that device



failed.

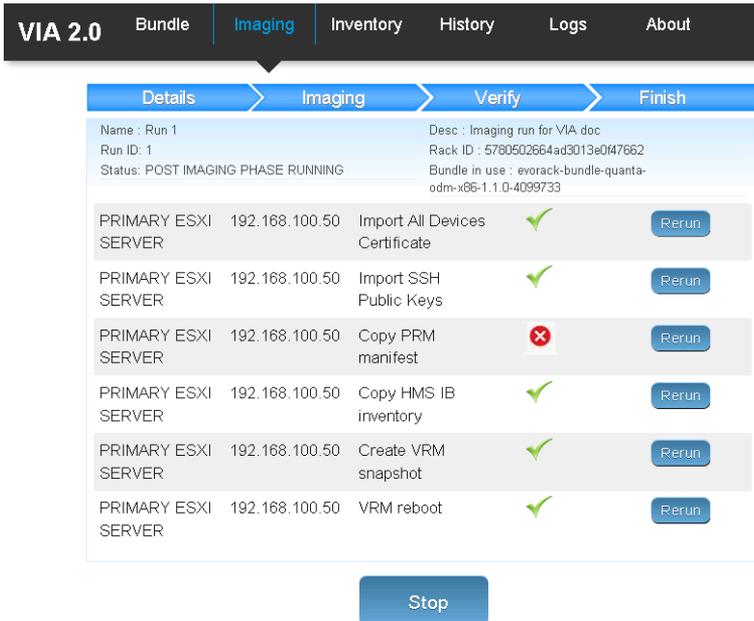
- 1 Click the component to display the verification task list for that device.



- 2 Click **Retry**
- 3 Once the device displays an  icon, click **Next**.

Fix Issues During the Finish Imaging Step

During the finish step in the imaging workflow, failed post-imaging tasks are displayed with an .



Task Name	IP Address	Description	Status	Action
PRIMARY ESXI SERVER	192.168.100.50	Import All Devices Certificate	✓	Rerun
PRIMARY ESXI SERVER	192.168.100.50	Import SSH Public Keys	✓	Rerun
PRIMARY ESXI SERVER	192.168.100.50	Copy PRM manifest	✗	Rerun
PRIMARY ESXI SERVER	192.168.100.50	Copy HMS IB inventory	✓	Rerun
PRIMARY ESXI SERVER	192.168.100.50	Create VRM snapshot	✓	Rerun
PRIMARY ESXI SERVER	192.168.100.50	VRM reboot	✓	Rerun

Stop

icon.

- 1 Click **Rerun** to run the failed task again.
- 2 After all tasks display an  icon, click **Complete**.

Opening a Cancelled Run

If you had accidentally cancelled an imaging run, you can re-open it.

- 1 In the VIA user interface, click **History**.
- 2 In the **Select Run ID** drop-down, select the run ID you want to open.
- 3 Click **Reopen**.

The selected run is opened in the state it was at the time the run had been cancelled.

Image Additional Racks

Follow this procedure for each additional rack if you are imaging racks incrementally in a multi-rack environment.

Procedure

- 1 Disconnect port 48 of the management switch on rack1 from the private managed switch.
- 2 Connect port 48 of the management switch on the next rack to the private managed switch.
- 3 Follow [Image a Physical Rack](#).

Imaging Individual Devices

5

You can image a server or management switch as an individual device.

This chapter includes the following topics:

- [Image Individual Server](#)
- [Image New Management Switch](#)

Image Individual Server

You can use the individual server imaging feature in the following scenarios:

- Imaging fails on a server in a rack
You can image that server as an individual device rather than re-imaging the complete rack.
- You are adding a new host to a Cloud Foundation rack or replacing a dead host.
You can image the new or replacement host with this feature.

Prerequisites

If this is a new or replacement host, do the following.

- Mount the host in the appropriate slot in the physical rack. For a replacement host, mount it in the same slot as the previous host and wire it according to the same wiring connections.
- Depending on whether VIA is installed on a laptop or management host, the NIC port on the laptop must be connected to port 48 of the management switch. Or the management host must be connected to a private managed switch that is connected to port 48 of the management switch.
- VIA must have access to ESXi OOB network (192.168.0.x) and inband network (192.168.100.x).
- Software bundle must have been uploaded.
- BIOS settings must have been set on the server to be imaged.
- For Cisco UCS servers only, set the following values before imaging the rack.
 - Out-Band Cisco Integrated Management Controller User Name=admin
 - Out-Band Cisco Integrated Management Controller User Password=password

Ensure that:

- Server is in ONIE mode.
- iDRAC consoles are closed. If an iDRAC console is open, imaging may fail.

Procedure

- 1 In the VIA user interface, click **Imaging**.

Ensure that you are in the **Details** tab.

- 2 (Optional) Type a name and description for the imaging run.
- 3 In **Deployment Type**, select **Cloud Foundation Individual Deployment**.
- 4 In **Device Type**, select **ESXi_SERVER**.
- 5 In **Rack Type**, select **Primary Rack** if you are imaging a server in rack 1. For a server in an additional racks, select **Add-On Rack**.
- 6 Select the vendor and model number of the server. The IP address of the server is displayed.
- 7 If you want the displayed IP address to be assigned only to the host being imaged, type the MAC address of the server.
- 8 Click  in any section to view the VIA properties file.

The VIA properties file displays rack specification values from the activated software bundle. For Cisco servers, check the default values for VMNIC1 and VMNIC2. If the defaults are not accurate, edit the values based on which 10G port on the server's Network Card is connected to ToR 1 and ToR 2.

- 9 Click **Start Imaging**.
- 10 Power on the server.
The server is discovered and the imaging process begins.
- 11 Open the KVM console to the server.
- 12 For a Dell server, change the boot device for the next boot to **Local SD**.
Do not power cycle or reset the server.

- 13 Monitor the ESXi installation on the console.

The server is rebooted after ESXi installation is complete. Ensure that ESXi is booting from the installed copy of ESXi and not from the network.

After the server boots from the installed copy of ESXi, VIA continues imaging the server.

- 14 After imaging is completed, disconnect VIA and shutdown the laptop or management host.

Image New Management Switch

Imaging the new management switch with VIA installs the necessary software on the switch.

Prerequisites

- Management switch must be connected to the laptop or management host where VIA is installed.
 - If VIA is installed on a laptop, the NIC port on the laptop must be connected to port 48 of the management switch.
 - If VIA is installed on a management host, the management host must be connected to a private managed switch that is connected to port 48 of the management switch.
- Identify the Cloud Foundation version in your environment and ensure that the appropriate bundle and md5sum file is uploaded on VIA.

Note Do not connect the management switch to any host before or during imaging.

Procedure

- 1 In the VIA user interface, click **Imaging**.
Ensure that you are in the **Details** tab.
- 2 (Optional) Type a name and description for the imaging run.
- 3 In **Deployment Type**, select **Cloud Foundation Individual Deployment**.
- 4 In **Device Type**, select **MGMT_SWITCH**.
- 5 Select the vendor and model number of the switch. The IP address is displayed.
- 6 Click **Start Imaging**.
Imaging fails at collect BMC-IP information task. This is expected behavior.
- 7 Disconnect the switch from the laptop or management host.

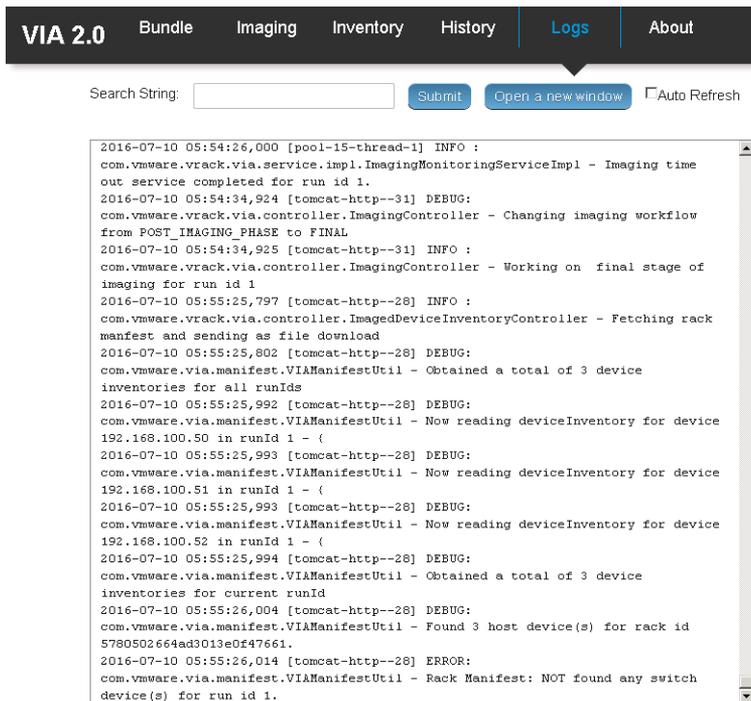
Viewing the VIA Log File

6

The log file displays information for all VIA services.

Procedure

- ◆ On the left navigation bar in the VIA user interface, click **Logs**.



A consolidated log of VIA services is displayed sorted by the time stamp. A maximum of 500 entries is displayed at a time.

You can filter the logs by typing a search string and clicking **Submit**. For example, you can search for activities on the primary ESXi server.

To display the complete log file, click **Open a new window**.

The **Auto Refresh** option is selected by default where the log file automatically scrolls to display the most current information.

Viewing Results of an Imaging Run

7

You can view the imaging history for an imaged rack or the status of individual devices on an imaged rack.

This chapter includes the following topics:

- [View Imaging History](#)
- [View Inventory](#)

View Imaging History

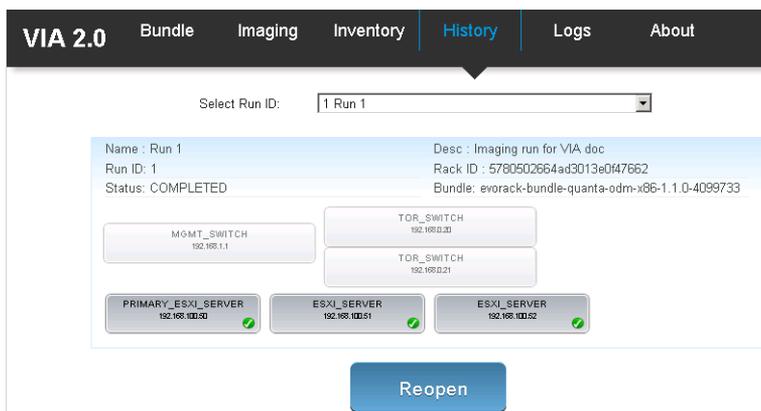
You can view the status of an imaging run by specifying its run ID if the rack state has not changed since that run was completed. If you imaged multiple racks using the same VIA VM, you can view the imaging history of each rack by specifying its run ID.

Prerequisites

Verify that an imaging run is not in progress.

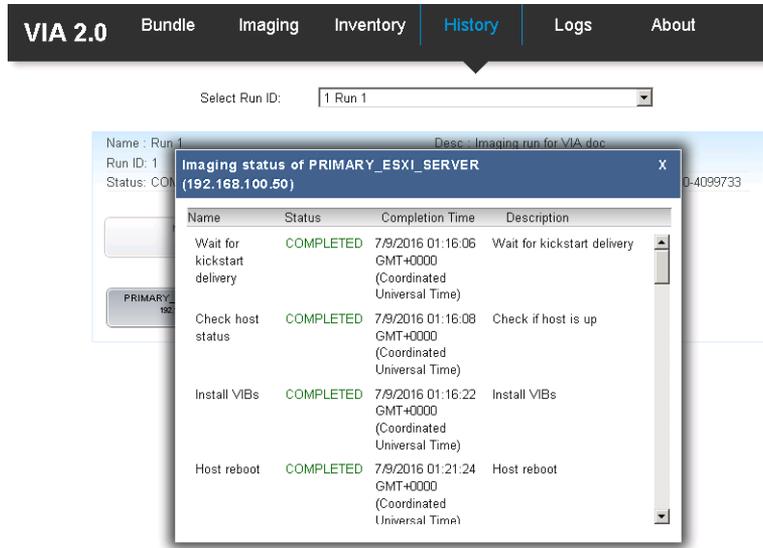
Procedure

- 1 In the VIA user interface, click **History**.



- In **Select Run ID**, select the run ID for which you want to view the imaging history. You can only view the history for a run if the state of the rack has not changed since the run was completed.

Imaging history appears for all devices that are imaged during the specified run.



- To view details for a device, click the expand icon next to the device.
- To reopen a previous run, select the run ID and click **Reopen**.
You can continue imaging a cancelled run by reopening it.

View Inventory

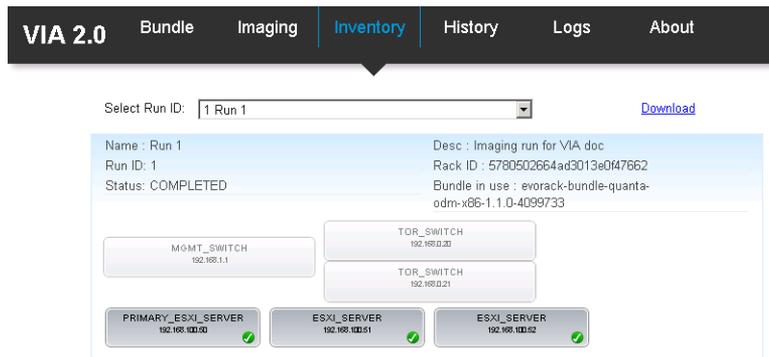
The Inventory page displays a consolidated report of the rack inventory. You can view device details by expanding the appropriate device.

Prerequisites

Verify that an imaging run is not in progress.

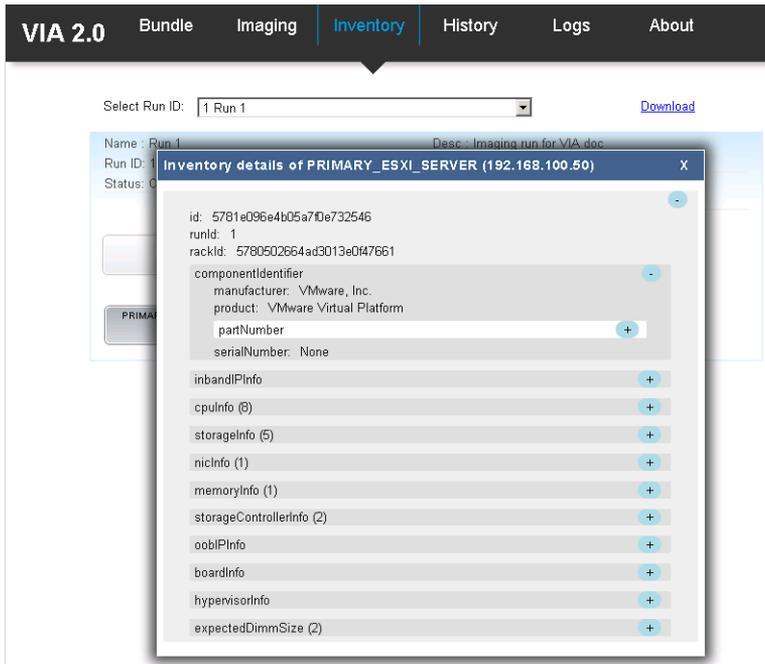
Procedure

- In the VIA user interface, click **Inventory**.



- In Select Run ID, select run ID.

The device inventory for the selected imaging run is displayed.



- To view details for a device, click the expand icon next to the device.
- To download the rack inventory click **Download** and specify the directory where the file is to be saved.

The device inventory is saved as a JSON file.

BIOS Settings

8

The BIOS settings for each device in the physical rack must match the values given below.

This chapter includes the following topics:

- [Cisco Settings](#)
- [Dell Settings](#)
- [Hewlett Packard Settings](#)
- [Quanta Settings](#)

Cisco Settings

Table 8-1. Servers

Setting	Path to Setting	Value
IPMI Over LAN	<ol style="list-style-type: none">1 Connect to OOB.2 Click the Admin tab and click Communication Services.3 In IPMI Over LAN Properties, select Enabled.	Enabled
Enable PXE boot	<ol style="list-style-type: none">1 Connect to OOB.2 Click the Server tab and click Inventory.3 Navigate to Cisco VIC Adapters > vNICs > Properties.4 Select Enable PXE Boot.	Enabled
Boot Option	<ol style="list-style-type: none">1 Reboot the server.2 Press F2.3 Click the Server tab and click BIOS.4 Specify Actual Boot Order.	<ul style="list-style-type: none">■ Boot Option 1 Cisco NIC 6:0.0■ Boot Option 2 Cisco NIC 7:0.0■ Boot Option 3 CiscoVD Hypervisor

Table 8-1. Servers (continued)

Setting	Path to Setting	Value
Network Settings	1 Connect to OOB.	IPv4 enabled
	2 Click the Admin tab and click Network .	Use DHCP enabled
	3 In IPv4 Settings, select Enable IPv4 and Use DHCP .	
SD Card	1 Connect to OOB.	Hypervisor
	2 Click the Storage tab and click Cisco Flex flash .	
	3 In Virtual Drive Info , select Hypervisor .	
	4 In Actions , click Enable/Disable Virtual Drive(s) and click Save .	

Dell Settings

Table 8-2. All components

Setting	Path to Setting
Set BIOS clock to current time	1 Navigate to BIOS > System BIOS Settings > Miscellaneous Setting > System Time..
	2 Click on the right panel to set time.

Table 8-3. Servers

Setting	Path to Setting	Value
Boot order	1 Navigate to System BIOS > System BIOS Settings > Boot Settings > Bios Boot Settings .	Network first
	2 Click Boot Sequence.	
	3 Click the + icon to move Integrated NIC to the top. Use arrow key and + to move SD up to the top of the list	
HDD order	1 Navigate to System BIOS > System BIOS Settings > Boot Settings > Bios Boot Settings .	SD Card first
	2 Click Hard-Disk Drive Sequence .	
	3 Click the + icon to move the Internal SD card to the top.	
Hyperthreading	System BIOS > System BIOS Settings > Processor Settings > Logical Processor Enabled	Enabled
IPMI credentials		Default credentials
IPMI Network Settings		Enabled on LAN
Mode		Legacy
NUMA	System BIOS > System BIOS Settings > Memory Settings > Node Interleaving Disabled Disabling node interleaving enables NUMA	Enabled

Table 8-3. Servers (continued)

Setting	Path to Setting	Value
Power management	<ol style="list-style-type: none"> 1 Navigate to System BIOS > System BIOS Settings > System Profile Settings. 2 Select Performance. This enables Turbo Boost. 	Performance
EIST (P-states)		Enabled
Turbo Mode		Enabled
CPU C3 report		Disabled
CPU C6		Enabled
CPU Advanced PM Tunning / Energy Per BIAS		Balanced performance
PXE on 1G Port 4	<ol style="list-style-type: none"> 1 Navigate to Device Settings > Integrated NIC 1 Port 3 Gigabit > NIC Configuration > Legacy Boot Protocol. 2 Select None. 3 Repeat the above steps on the second integrated 1G NIC. 	Disabled
PXE on 10G Port 2	<ol style="list-style-type: none"> 1 Navigate to Device Settings > Integrated NIC 1 Port 1 10G > NIC Configuration > Legacy Boot Protocol. 2 Select PXE. 3 Repeat the above steps on the second integrated 10 G NIC. 	Enabled
VT	System BIOS > System BIOS Settings > Processor Settings > Virtualization Technology Enabled	Enabled

Hewlett Packard Settings

Setting	Path to Setting	Value
Firmware Version	HP Network First SD card 1st	
Mode	BIOS/Platform Configuration (RBSU) Boot Options > Boot Mode [Legacy BIOS Mode]	Legacy
Boot order	BIOS/Platform Configuration (RBSU) Boot Options > Legacy BIOS Boot Order	Network first
HDD order		SD Card first
PXE on 1G	BIOS/Platform Configuration (RBSU) Boot Options > Network Boot Options Order	Disabled
PXE on 10G	BIOS/Platform Configuration (RBSU) Boot Options > Network Boot Options Order	Enabled
VT	BIOS/Platform Configuration (RBSU) System Options > Virtualization Options > Virtualization Technology	Enabled
Hyperthreading	BIOS/Platform Configuration (RBSU) System Options > Processor Options > Intel(R) Hyperthreading	Enabled

Setting	Path to Setting	Value
IPMI credentials		Default credentials (admin/admin)
IPMI Network Settings	iLO 4 Configuration Utility > Network Options > DHCP Enable [ON]	DHCP
Power: CPU Advanced Tuning / Energy Per BIAS	BIOS/Platform Configuration (RBSU) Power Management > Power Profile [Balanced power and Performance]	Balanced Performance

Quanta Settings

Table 8-4. All components

Setting	Path to Setting
Set BIOS clock to current time	Main > BIOS Information > System Time

Table 8-5. Servers

Setting	Path to Setting	Value
Boot order	System BIOS Settings > Boot > Fixed Boot Order Priorities <ol style="list-style-type: none"> Use arrow key to reach the correct boot order number. Press Enter. The boot devices are displayed. Use arrow key to highlight Network. Press Enter to select it. 	Network first
HDD order	System BIOS Settings > Boot > Hard Disk Drive BBS Priorities <ol style="list-style-type: none"> Press Enter. Press Enter again. The boot devices are displayed. Use arrow key to highlight SATADOM. Press Enter to make it the first device in the boot order. 	SATADOM first
Hyperthreading	<ol style="list-style-type: none"> Navigate to System BIOS Settings > Advanced > CPU Configuration > Hyper-threading. Press Enter to enable. 	Enabled
IPMI credentials		Default credentials
IPMI Network Settings		DHCP
Mode		Legacy
NUMA	<ol style="list-style-type: none"> Navigate to System Bios Settings > Chipset > North Bridge > Numa. Press Enter to enable. Disabling node interleaving enables NUMA 	Enabled

Table 8-5. Servers (continued)

Setting	Path to Setting	Value
Power management	System BIOS Settings > Advanced > CPU Power Management Configuration	
EIST (P-states)		Enabled
Turbo Mode		Enabled
CPU C3 report		Disabled
CPU C6		Enabled
CPU Advanced PM Tunning / Energy Per BIAS		Balanced performance
PXE on 1G	<ol style="list-style-type: none"> 1 Navigate to System BIOS Settings > Advanced > Onboard Device Configuration . 2 Select Enabled Without PXE for both the 1G NICs. 	Disabled
PXE on 10G	10G NICs set by default to PXE. To verify, press Ctrl+s while the server is booting to enter the BIOS.	Enabled
VT	System BIOS Settings > Advanced > Cpu Configuration > Intel Virtualization Technology Press Enter to enable.	Enabled

Troubleshooting VIA

9

This chapter includes the following topics:

- [Host failed to be imaged with error Unable to Establish IPMI v2 / RMCP+ Session](#)
- [ESXi Server has Incorrect BIOS Settings](#)
- [ESXi Server has Bad SD Card](#)
- [Management Switch Boots into EFI Shell](#)

Host failed to be imaged with error Unable to Establish IPMI v2 / RMCP+ Session

VIA was not able to power on a host and failed to image it.

Problem

After a host was powered off, VIA was unable to power it on. The following error was displayed.

Unable to establish IPMI v2 / RMCP+ session Unable to set Chassis Power Control to Up/On

Cause

VIA was unable to establish an IPMI v2 or RMCP+ session with the host.

Solution

- 1 Manually power on the host through DRAC.
- 2 On the **Imaging** tab, click the host that displayed the red icon and click Retry.

Solution

VIA continues imaging the rack.

ESXi Server has Incorrect BIOS Settings

Problem

Host failed to be imaged with the message **Post install reboot ESXi task failed.**

Cause

ESXi server has incorrect BIOS settings.

Solution

- 1 Check the ESXi server console.
- 2 If the console displays a gray screen with the message Unable to find boot device, check that the BIOS setting is SATADOM for Quanta servers and SD card for Dell servers.
- 3 Fix the hardware problem.
- 4 On the **Imaging** tab, click the host that displayed the red icon and click **Retry**.

ESXi Server has Bad SD Card

Problem

Device failed to be imaged with the message **Kickstart image not delivered..**

Cause

ESXi server has bad SD card.

Solution

- 1 Replace the SD flash card in the ESXi server.
- 2 On the **Imaging** tab, click the host that displayed the red icon and click **Retry**.

Management Switch Boots into EFI Shell

Problem

After rebooting, the management switch boots into EFI shell instead of ONIE mode.

Cause

The switch was not in ONIE mode and after rebooting, it boots into an EFI shell.

Solution

- 1 Connect to the management switch with a console cable.
- 2 Press **DEL** to change the boot order.
- 3 Select **P0**.
- 4 Select **Save changes**.

- 5 Select **Save changes and restart**.
- 6 To wipe the switch login as cumulus, type `sudo cl-image-select -k`.