VIA User's Guide

VMware Cloud Foundation 2.2

vmware®

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

https://docs.vmware.com/

Contents

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

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 inter-rack 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 vRealize Log Insight.

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 servers 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 imaged simultaneously by creating VLANs.

Figure 1-1. VIA Deployment
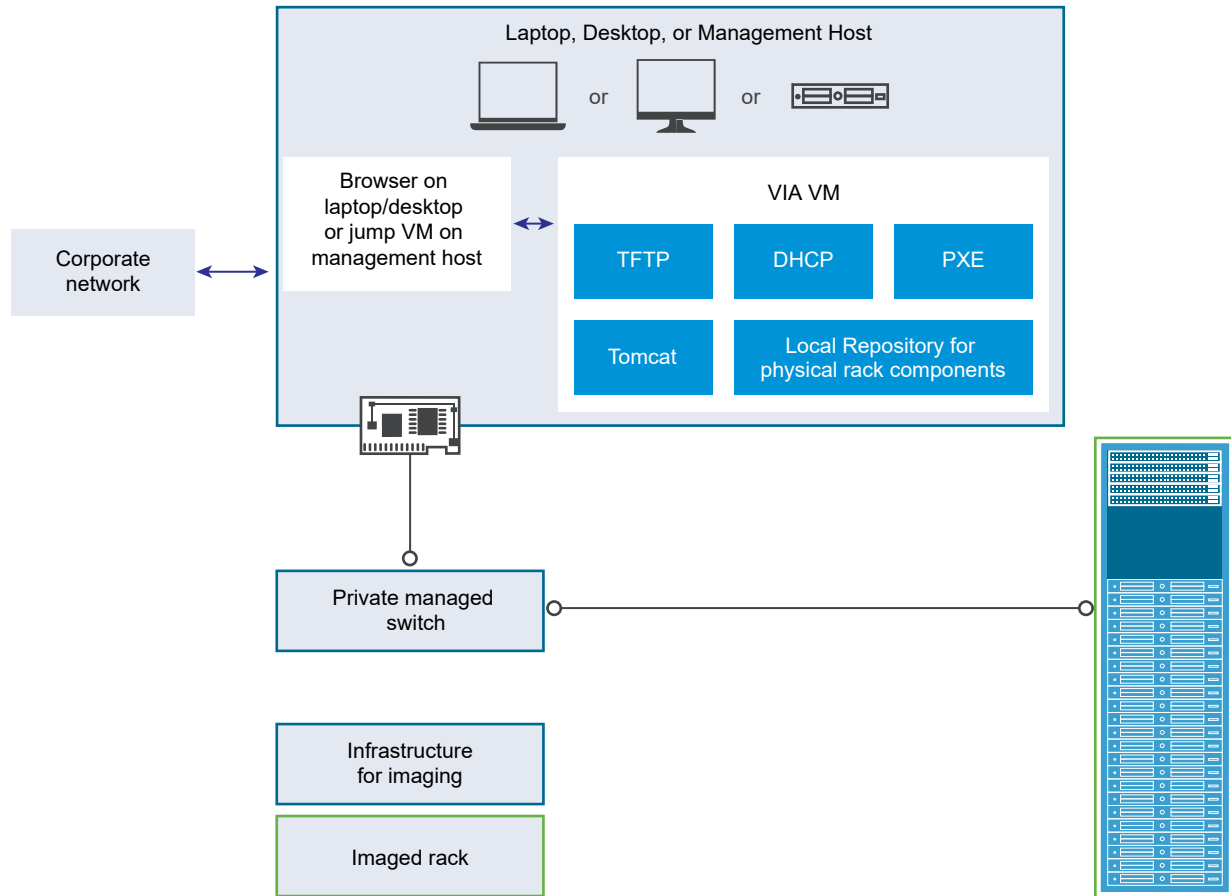
During imaging:

- The ToR and inter-rack switches (if applicable) are configured

- The Hardware Management Service (HMS) VM is installed on the SDDC Manager Controller VM

- VMware ESXi is installed on each host in the physical rack

- The Cloud Foundation software, SDDC Manager, is installed on host 0 of rack 1.

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. You can modify a bundle to add 3rd party VIBs.

The bundle contains the following software:

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

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.

Switch Service

A Switch Service is developed for each switch vendor by using an imaging developer kit. The developer kit provides the imaging orchestration engine, API, data models, and extension points to create imaging tasks (PRE, INTRA, POST, INVENTORY), custom controller, and automated integration tests. VIA loads these services on demand and discovers the switch type (management, ToR, inter-rack) supported by these services.

ESXi Service

The ESXi Service images the servers in the physical rack. It uses the same developer kit as the Switch Service.

Core Platform Service

Core Platform is the main VIA web service which supports external facing API, DHCP, bundle management, imaging workflow orchestration, and UI. This service automatically loads the Switch and ESXi services on demand based on the BOM and bundle and then orchestrates the imaging workflow. This service can image an entire rack as well as individual devices.

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
Inter-rack 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.

- Inter-rack switches

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

  Inter-rack 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, inter-rack 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.

- Servers

  For information on supported hardware, see VMware Compatibility Guide.

  Table 1-2. 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.	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

  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

	42 U	42 U
Serial Console Switch		
Management Switch		
Inter-rack 2		
Inter-rack 1		
ToR 2		
ToR 1		
Server 32		
Server 31		
Server 30		
Server 29		
Server 28		
Server 27		
Server 26		
Server 25		
Server 24		
Server 23		
Server 22		
Server 21		
Server 20		
Server 19		
Server 18		
Server 17		
Server 16		
Server 15		
Server 14		
Server 13		
Server 12		
Server 11		
Server 10		
Server 9		
Server 8		
Server 7		
Server 6		
Server 5		
Server 4		
Server 3		
Server 2		
Server 1		
Front	**Back**	

IPMI

DATA

Requirements for VIA

2

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 for Imaging

3

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.

This chapter includes the following topics:

- Rack Power
- Network Cables
- Rack Wiring
- Rack Component Ports
- Physical Servers
- Network Switches
- Laptop or Management Host
- Virtual Machines

Rack Power

Ensure that rack power meets the following requirements.

- Verify that each device in the rack has a connection to each PDU.

- 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: (9) .5m (3) 1m

  - From the Top-of-Rack Switch: 1.5m

  - From the Inter-rack Switch: .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.

- The power connector from the PDU must match the power connector in the Site Readiness Assessment.

- Power cables must be seated properly from each device to the PDU.

- The cables connect the primary PDUs to the other components must be blue and the cables from the secondary PDUs must be red.

- 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.

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 inter-rack 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.

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.

- Review the test print out to confirm that the cables passed the test.

- 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 inter-rack switch.

- There must be two 40G QSFP+ cable connections between each ToR switch and inter-rack 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

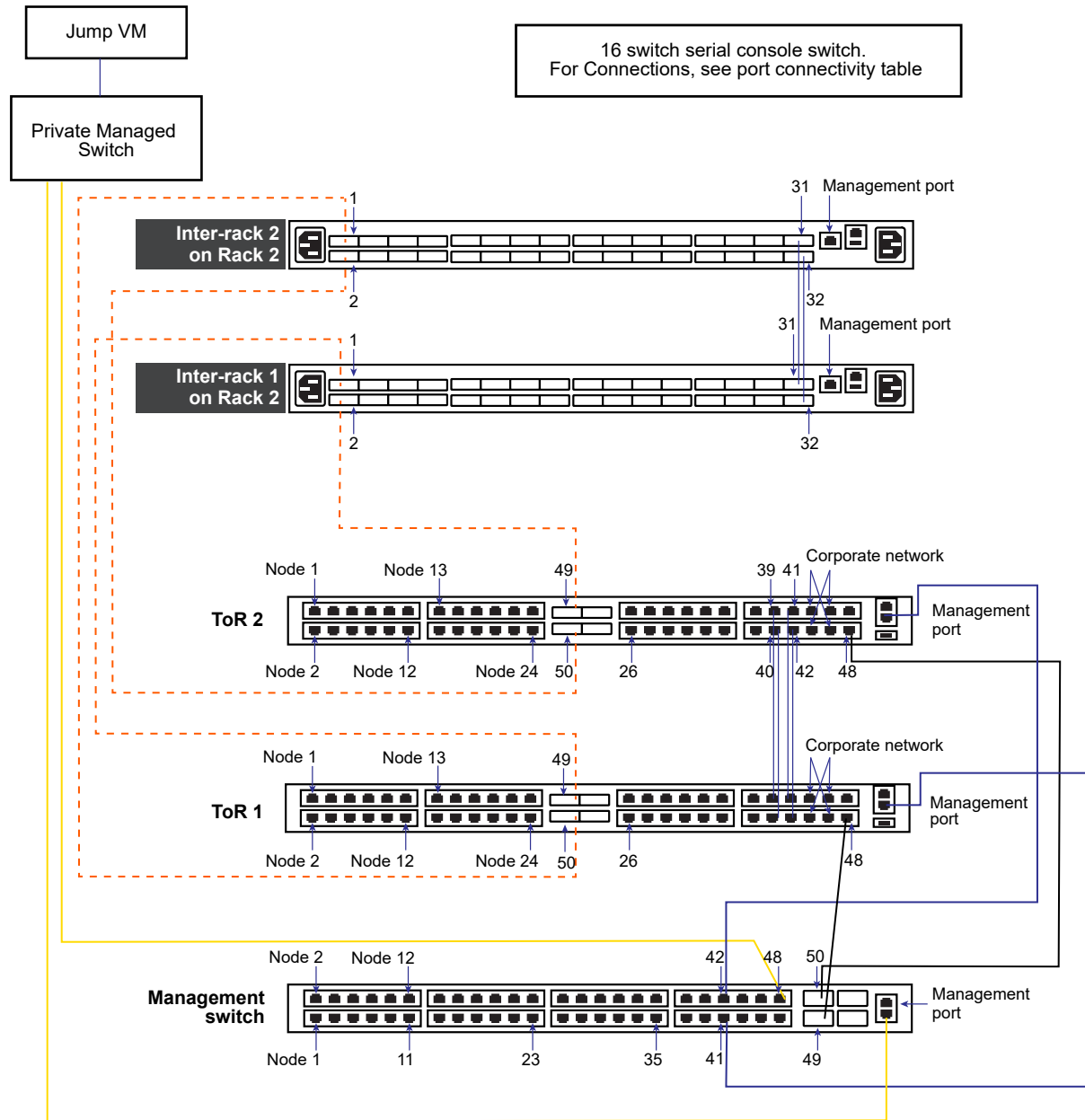**Figure 3-1. Wiremap for rack 1 with Cisco ToR Switches and Dell Management Switch**
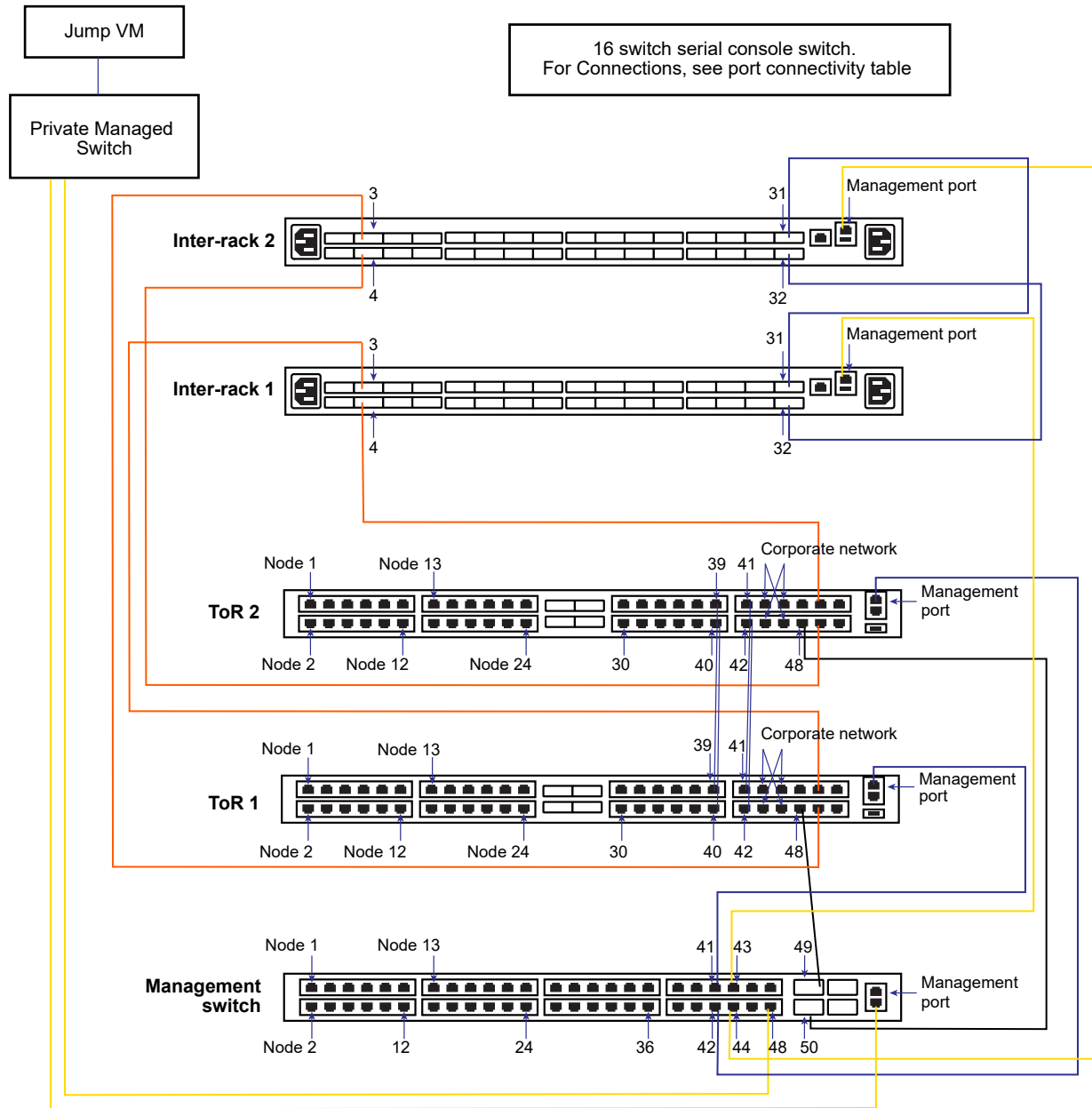
Figure 3-2. Wiremap for rack 2 with Cisco ToR Switches and Dell Management Switch

Wiring for Rack with Quanta Management Switch

Figure 3-3. Wiremap for rack 1 with Cisco ToR Switches and Quanta Management Switch
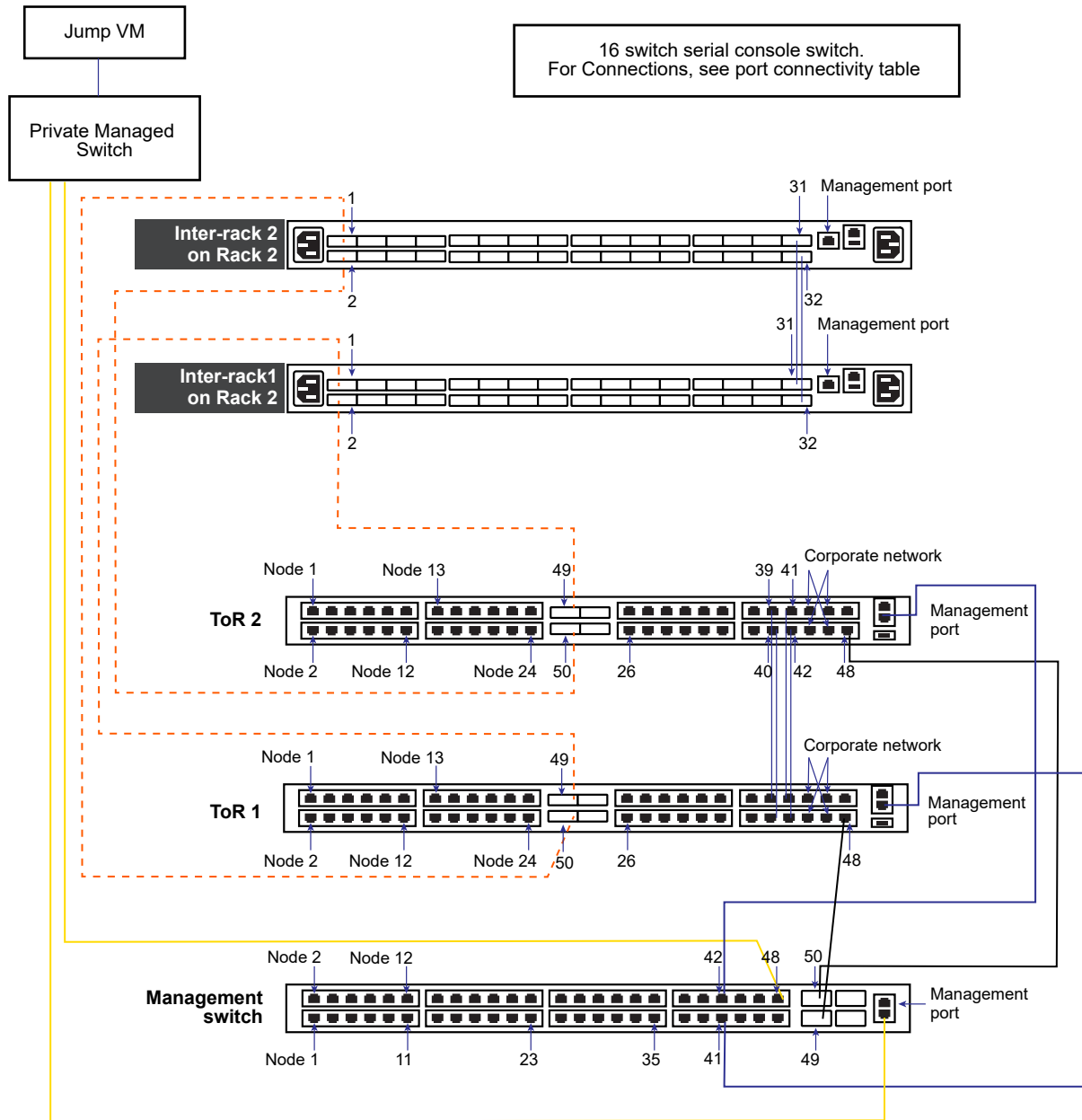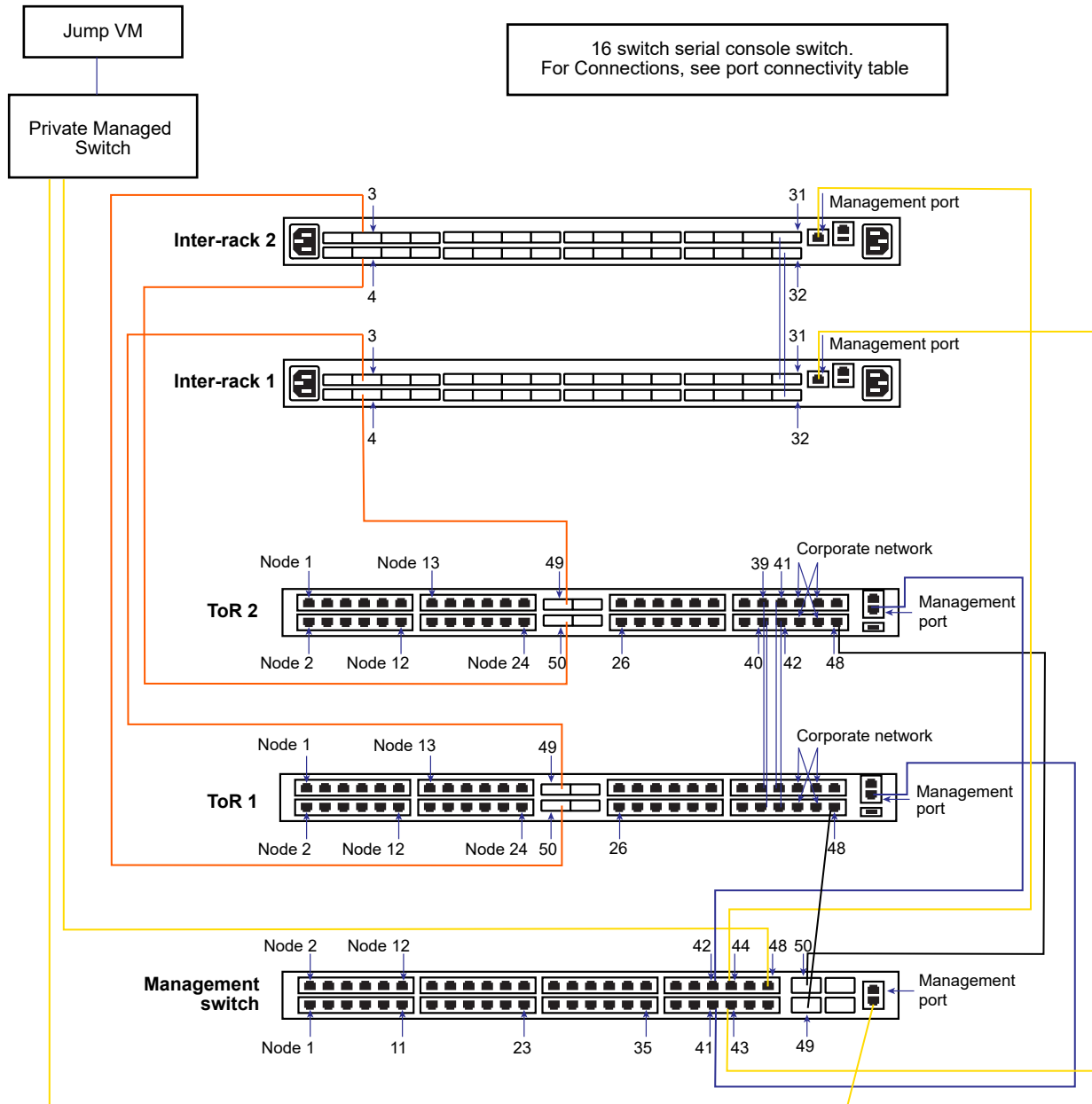
Figure 3-4. Wiremap for rack 2 with Cisco ToR Switches and Quanta Management Switch

Additional Racks

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

Additional physical racks do not contain inter-rack switches. ToR switches in the additional physical racks are connected to the two inter-rack 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	Inter-rack 1 console port
5	Inter-rack 2 console port
6	PDU 1
7	PDU 2
8	PDU 3
9	PDU 4
10 - 16	Not connected

Inter-rack 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

Inter-rack 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 - 46	10 Gbps	Corporate network as required (see note below table)
47	Blank	
48	1Gbps	Management switch port 50
49	40 Gbps	Inter-rack 1 port 2
50	40 Gbps	Inter-rack 2 port 2
51 - 54	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 - 46	10 Gbps	Corporate network as required (see note below table)
47	Blank	
48	1Gbps	Management switch port 49
49	40 Gbps	Inter-rack 1 port 1
50	40 Gbps	Inter-rack 2 port 1
51 - 54	40 Gbps	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	Inter-rack 1 management port
44	1Gbps	Inter-rack 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 3-1. 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 3-2. Physical Device Location in Rack 2

RU Location	Device
42	Console serial switch
41	Management switch
40	Inter-rack 2
39	Blank
38	Inter-rack 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 10 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 3-3. 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
17,18,19,20	VLAN 2004
21,22,23,24	VLAN 2005

Figure 3-5. Management Host Connection
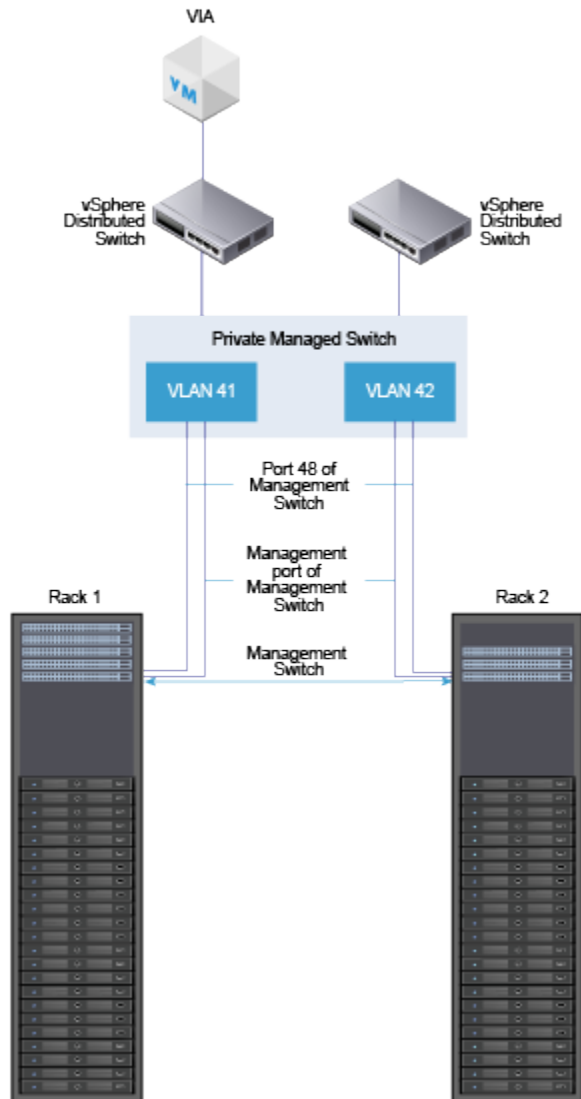
Private Managed Switch

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 managament 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 3-4. 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

4

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 4-1. 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.	
Review the VMware Compatibility Guide and verify you have the supported server models, disk and storage adapter models, and switch models.	
Validate that BIOS Settings for all components are correct. See Chapter 10 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 switch OS or boot environment 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 Cable Colors in Network Cables.	
Verify that the cable bend radius is proportionate to the external diameter. See Cable Bend Radius in 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 direction.	

Table 4-1. Pre-Imaging Checklist (continued)

Setting	Verified
Verify that switches have redundant power supplies and each power supply is connected to a separate power strip.	
If you are using a management host to image your system, ensure that: ■ A supported version of ESXi is installed on the management host. For the supported version, see the *VMware Cloud Foundation Release Notes*. ■ The **Allow virtual machines to start and stop automatically with the system** option is enabled. ■ IP address 10.1.0.200 is assigned to the vmk0 kernel interface. ■ SSH is enabled on the management host. ■ The access VM, VIA VM, and jump VM meet the required hardware configuration. See Virtual Machines. ■ The required software has been installed on the VMs. See Virtual Machines.	

Installing VIA

5

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 #unique_24.

- 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 #unique_24.

- 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

<div style="text-align: right;">6</div>

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 6-1. VIA Setup for Parallel Imaging of Multiple Physical Racks
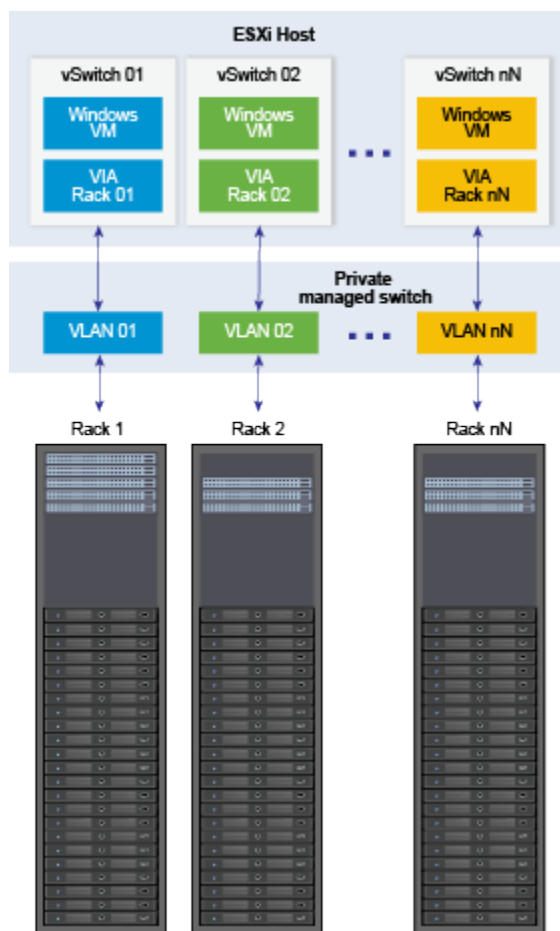
This chapter includes the following topics:

- Image a Physical Rack

- [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, inter-rack 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 ToR switches and Inter-rack switches (inter-rack switches are on rack 2 only)

   Inter-rack and ToR switches are imaged in parallel.

   Inter-rack 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 inter-rack 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 inter-rack 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 inter-rack 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 inter-rack 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.

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   Modify Software Bundle

You can add 3rd party VIBs to a software bundle by modifying it.

3   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.

4   Monitor Imaging

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

5   Verify Inventory

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

6   Post Imaging Checks

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

7 Download Inventory File

You must download and save the inventory file for each imaged rack or host. This file is required during rack bring-up and while adding a host. For the first rack, the inventory file is copied over to the SDDC Manager Controller VM during imaging. However, you must still download the file and save it to an accessible location in case the file on is corrupted for some reason. For additional racks, you must upload this file manually while adding the rack to your system.

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
- 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 10 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**.

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**.

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**.

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.

Modify Software Bundle

You can add 3rd party VIBs to a software bundle by modifying it.

Prerequisites

Download the 3rd party VIBs you want to add to the software bundle.

Procedure

1 In the Bundle tab, click **Modify Bundle**.

2 Select the vendor and model name.

The current VIBs are displayed.

3 In **Select VIB**, select the VIB to be added.

Note Only files with a .vib extension are accepted.

4 Click **Upload VIB**.

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**.

2   (Optional) Type a name and description for the imaging run.

It is recommended that you add the rack serial number or other rack identification details in the Name or Description field. The name and description is recorded in the imaging details JSON file after imaging is complete, which helps identify the rack to which the imaging details file belongs.

3   In **Deployment Type**, select **Cloud Foundation Full Deployment**.

4   In **Rack Type**, select **First Rack** if you are imaging rack 1. For additional racks, select **Additional Rack**.

5   For the management switch and ToR switches, select the vendor and model.

The IP address for each switch is displayed.

6   (Optional) Type the MAC address of each switch.

7   If the physical rack contains inter-rack switches (rack 2 only), type the number of inter-rack switches in the **Number** field in the **Inter-rack Switch** section.

8   Select the vendor and model number of the inter-rack 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 (Optional) Type the MAC address of each server.

After imaging, hosts are numbered based on port connectivity. The host connected to the first port is host 0, the second is N1, and so on. VIA enables switch and server ports and power resets them one by one staggered with a delay. The host that powers on first gets the IP address 192.168.100.50 and becomes the primary host. So host 0 may not necessarily be the primary host.

If you type a MAC address, VIA assigns the IP address 192.168.100.50 to the host with the specified MAC address and makes it the primary host.

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.

13 Click **Save**.

14 Click **Start Imaging**. The wiring diagram for the rack is displayed.
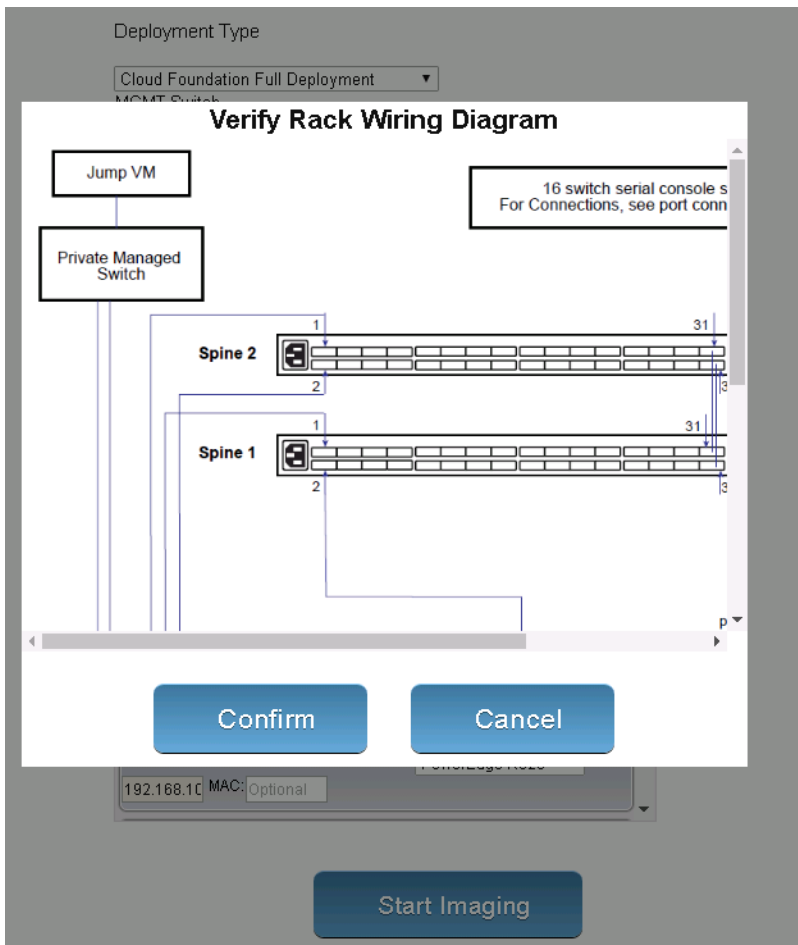
Review the wiring diagram to check if your rack is wired according to the displayed wiremap. See Rack Wiring.

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 ⚠ (8) 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.
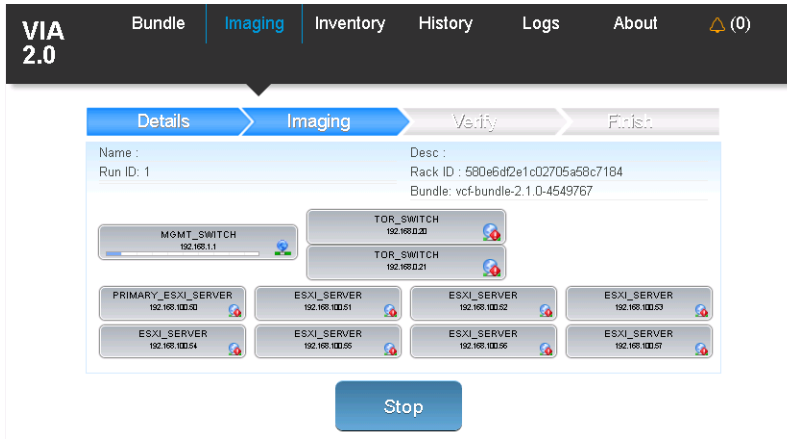
The run details, rack details, and imaging status for switches and servers in the rack are displayed. The devices in the physical rack are displayed in the order in which they will be imaged. IP addresses for each device are displayed as well. The **PRIMARY_ESXI_SERVER** is host 0. You may need to log in to this host, so note down this IP address.

2   Note the **Run ID**.

3   Click a device to see information about the imaging tasks completed and in-progress tasks.
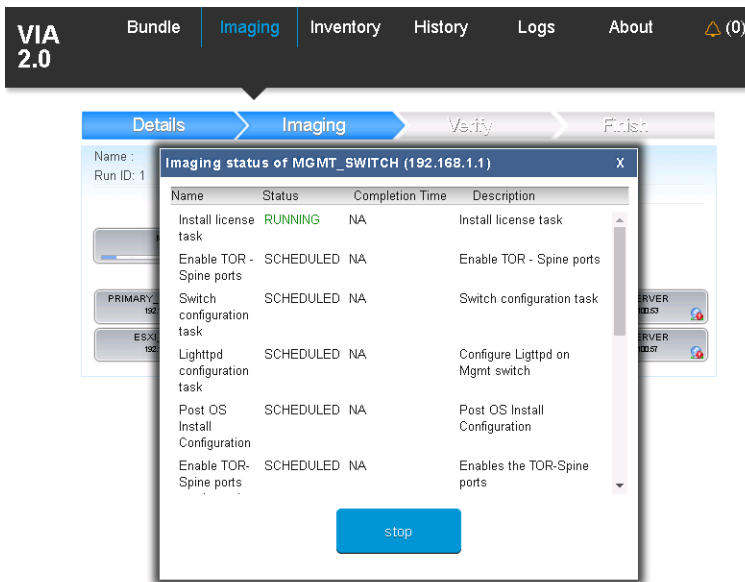
4   Click **Switch to IPMI View** to view progress of the BMC device imaging. This option appears afer the management and ToR switches are imaged.

5   Click **Switch to Default View**.

It is recommended that you switch back to the default view so that you can monitor imaging of all devices, not just the servers.

It can take approximately 95 minutes for rack 1 to be imaged. During imaging, the password of all rack components except SDDC Manager is set to EvoSddc!2016. The SDDC Manager password is set to vmware1234. Note that the ToR and inter-rack switches are named as follows:

- ToR switch connected to port 41 of the management switch is named TOR20

- ToR switch connected to port 42 of the management switch is named TOR21

- Inter-rack switch connected to port 43 of the management switch is named INTER-RACK30

- Inter-rack switch connected to port 44 of the management switch is named INTER-RACK31

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.
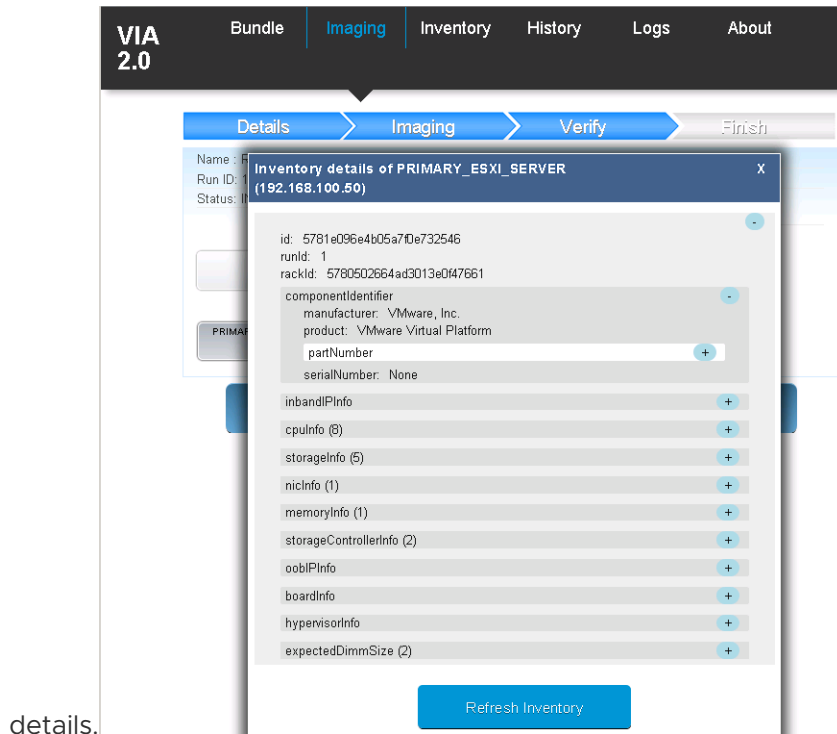
Procedure

1 Click the **Imaging > Verify**
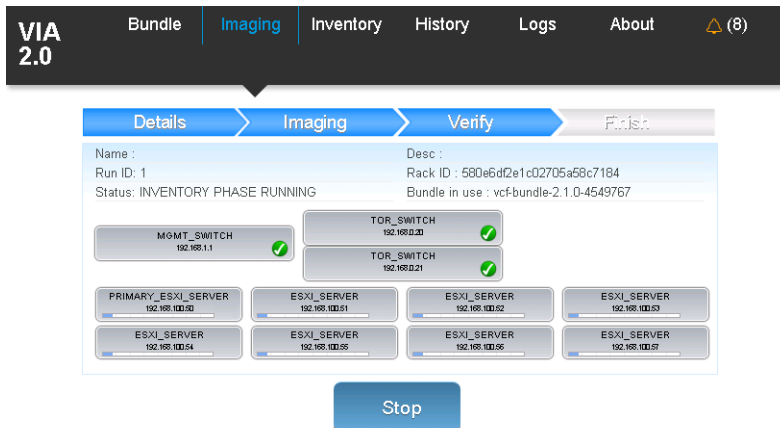
The status of inventory collection on each device in the rack is displayed.

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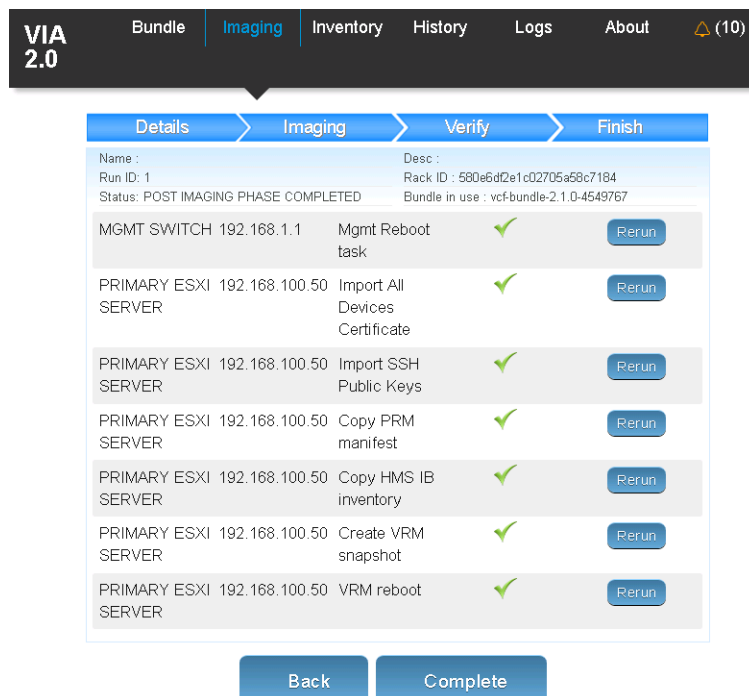

details.

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 **Complete**.

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.

Download Inventory File

You must download and save the inventory file for each imaged rack or host. This file is required during rack bring-up and while adding a host. For the first rack, the inventory file is copied over to the SDDC Manager Controller VM during imaging. However, you must still download the file and save it to an accessible location in case the file on is corrupted for some reason. For additional racks, you must upload this file manually while adding the rack to your system.

Procedure

1 Click the **Inventory** tab.

2 Select the Run ID.

3 Click **Download**.

The file is download on the jump VM. Each inventory file is identified by the ImagingID. The name and description in the file match the details you specified in the Imaging tab.

4 Copy the downloaded file to an accessible location.

5 Rename the file such that the file name indicates the rack or host that the inventory file belongs to.

Resume Imaging

If a device fails to be imaged, you can take a number of actions that can help in continuing with the imaging run.

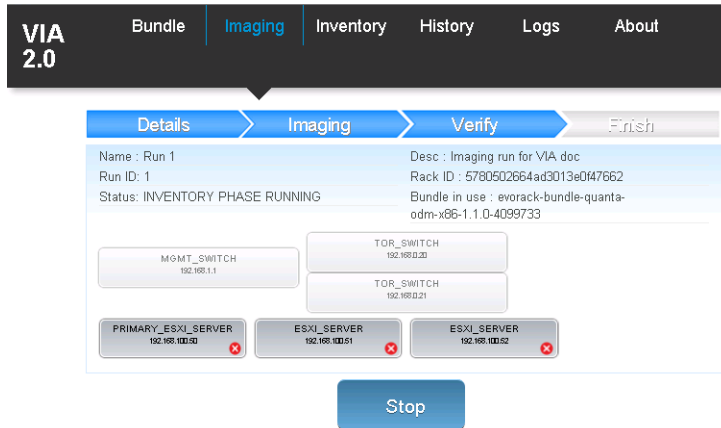## Fix Issues During the Monitor Imaging Step

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.
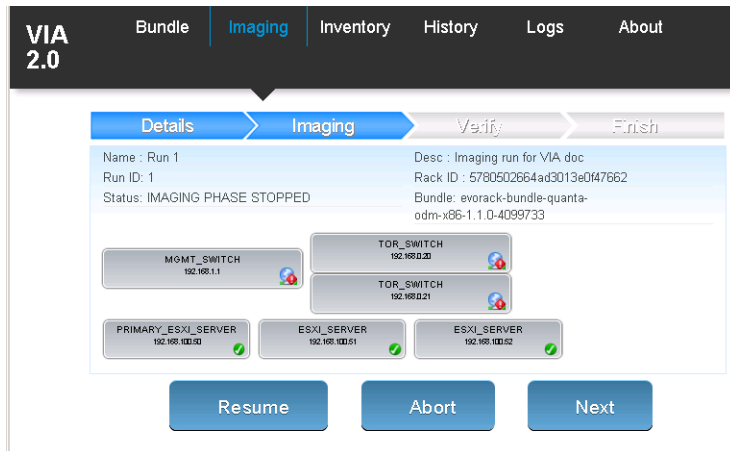
1   Click the component to display the imaging task list for that device. Then do one of the following:

  ■   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.

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.

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.
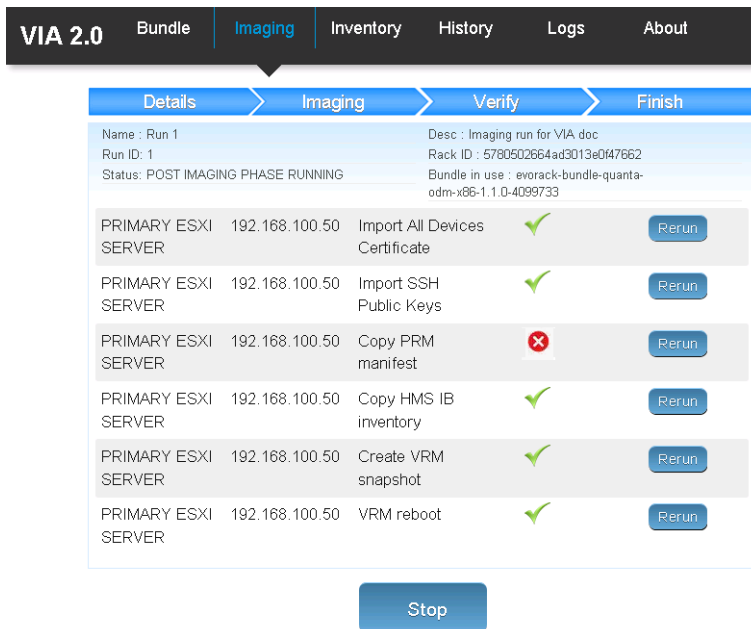
1   Click the component to display the verification task list for that device.
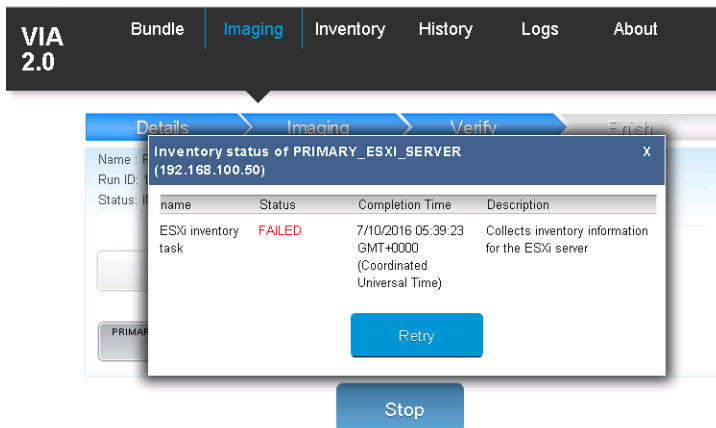
2   Click **Retry**

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 🔴

icon.

1   Click **Rerun** to run the failed task again.

2   After all tasks display an ✅ icon, click **Complete**.

Opening an Aborted Run

If you had accidentally aborted 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 aborted.

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

<div style="text-align: right; font-size: 3em; color: #888;">7</div>

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

If a server fails to be imaged, you can image that server as an individual device rather than re-imaging the complete rack. Or you can image a new or replacement server before adding it to a rack.

Prerequisites

- 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.

- If VIA is installed on a laptop, connect the NIC port on the laptop to port 48 of the management switch on which the host is being imaged. If VIA is installed on a management host, connect the host to a private managed switch that is connected to port 48 of the management switch on which the host is being imaged.

- VIA must have access to the inband network only. The BMC on the server being imaged must be pre-configured with a static IP address in the range 192.168.0.50 - 192.168.0.99. Ensure that the gateway and netmask are set to the same values as the servers that are already in the rack.

- Software bundle must have been uploaded.

- BIOS settings must have been set on the server to be imaged.

- Server must be in PXE boot mode.

- iDRAC 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.

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 are imaging a host for a multi-rack Cloud Foundation deployment, you must type the MAC address of the host being imaged. This ensures that VIA images the correct host.

8   Click **Start Imaging**.

9   Power on the server.

The server is discovered and the imaging process begins.

10   Open the KVM console to the server.

11   Change the boot device for the next boot to **PXE Mode**.

    a   Ina web browser, open the Integrated Dell Remote Access Controller page and login with default credentials (root/calvin).

    b   In the Properties tab, click **Launch** in the Virtual Console Preview.

        The console opens in a new window.

    c   Open the keyboard.

    d   In the Properties tab, click **Power Cycle System** (cold boot) in the Quick Launch Tasks

    e   In the console window, press F11 to access the Boot Manager.

        F11 = Boot Manager is highlighted.

    f   Select One-shot BIOS Boot Method

    g   Select PXE Boot.

    Do not power cycle or reset the server.

12   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.

13   Download the inventory file. You need this file when adding an imaged host to a Cloud Foundation rack.

    a   Click the **Inventory** tab.

    b   Select the Run ID.

    c   Click **Download**.

        The file is download on the jump VM.

    d   Copy the downloaded file to an accessible location.

14 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

8

The log file displays information for all VIA services.

Procedure

◆ On the left navigation bar in the VIA user interface, click **Logs**.
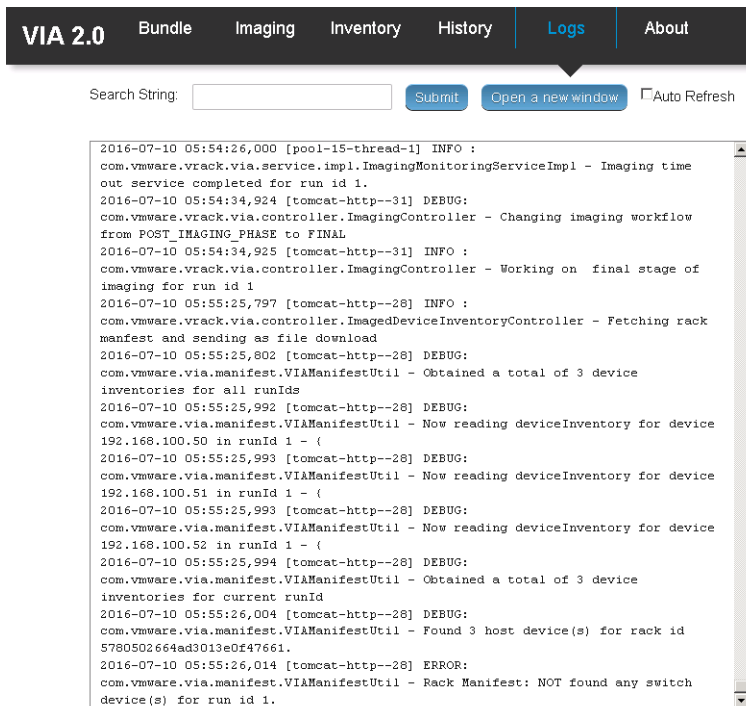
A consolidated log of VIA services is displayed sorted by the time stamp. A maximum of 500 entries is displayed at a time.

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

9

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

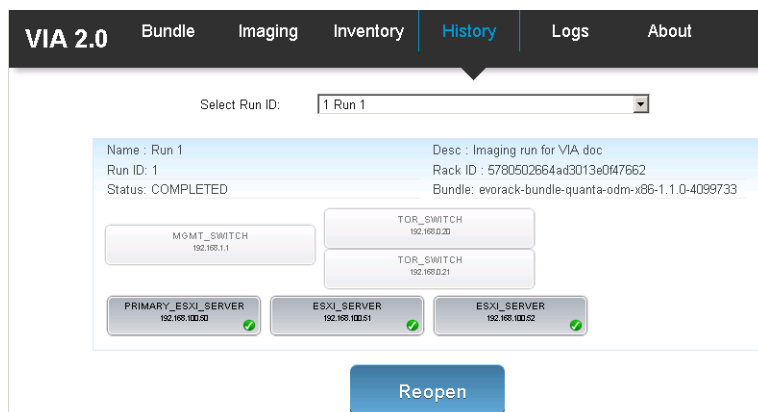You can view the status of an imaging run by specifying its run ID if the rack state has not changed since that run was completed. If you imaged multiple racks using the same VIA VM, you can view the imaging history of each rack by specifying its run ID.

Prerequisites

Verify that an imaging run is not in progress.

Procedure

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

2   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.
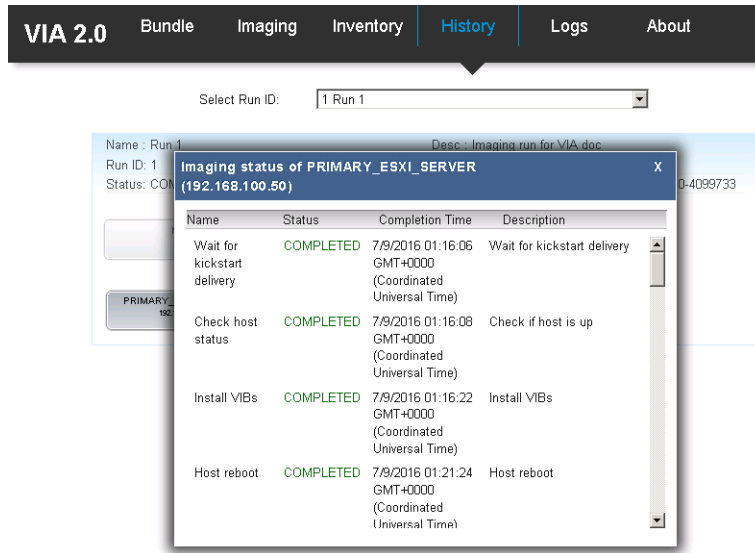
3   To view details for a device, click the expand icon next to the device.

4   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

1   In the VIA user interface, click **Inventory**.
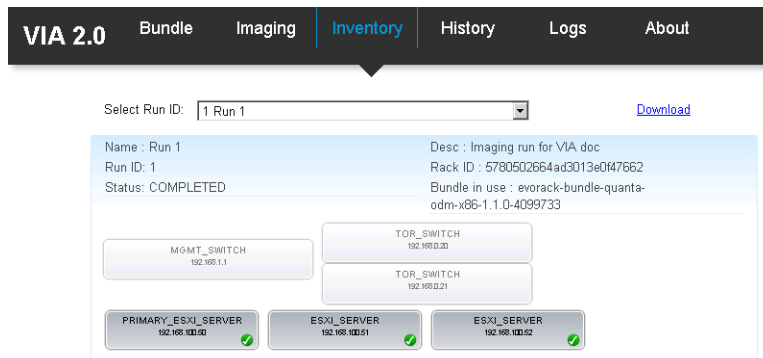
2   In Select Run ID, select run ID.

The device inventory for the selected imaging run is displayed.
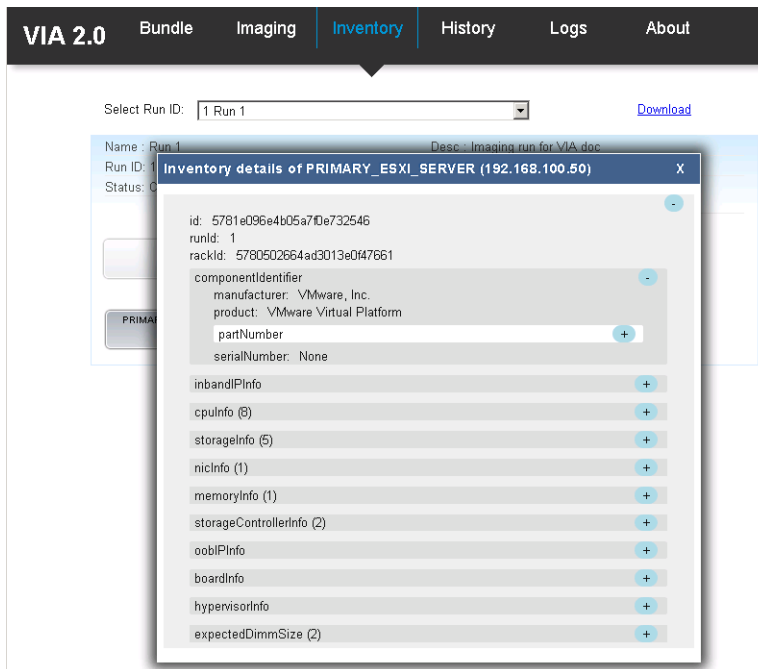
3   To view details for a device, click the expand icon next to the device.

4   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

10

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

This chapter includes the following topics:

- Dell Settings
- Hewlett Packard Settings
- Quanta Settings
- Fujitsu Settings

Dell Settings

Table 10-1. 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 10-2. Servers

| Setting	Path to Setting	Value
Boot order	1 Navigate to **System BIOS > System BIOS Settings > Boot Settings > Bios Boot Settings** . 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	Network first
HDD order	1 Navigate to **System BIOS > System BIOS Settings > Boot Settings > Bios Boot Settings** . 2 Click Hard-Disk Drive Sequence . 3 Click the + icon to move the Internal SD card to the top.	SD Card or SATADOM first
Hyperthreading	**System BIOS > System BIOS Settings > Processor Settings > Logical Processor Enabled**	Enabled
IPMI credentials		Default credentials

Table 10-2. Servers (continued)

Setting	Path to Setting	Value
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
Power management	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	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	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

Setting	Path to Setting	Value
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
IPMI credentials		Default credentials (admin/password)
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 10-3. All components

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

Table 10-4. Servers

Setting	Path to Setting	Value
Boot order	**System BIOS Settings > Boot > Fixed Boot Order Priorities** 1 Use arrow key to reach the correct boot order number. 2 Press Enter. The boot devices are displayed. 3 Use arrow key to highlight Network. 4 Press Enter to select it.	Network first
HDD order	**System BIOS Settings > Boot > Hard Disk Drive BBS Priorities** 1 Press Enter. 2 Press Enter again. The boot devices are displayed. 3 Use arrow key to highlight SATADOM. 4 Press Enter to to make it the first device in the boot order.	SATADOM first
Hyperthreading	1 Navigate to **System BIOS Settings > Advanced > CPU Configuration > Hyper-threading**. 2 Press Enter to enable.	Enabled
IPMI credentials		Default credentials

Table 10-4. Servers (continued)

Setting	Path to Setting	Value
IPMI Network Settings		DHCP
Mode		Legacy
NUMA	1 Navigate to **System Bios Settings > Chipset > North Bridge > Numa** . 2 Press Enter to enable. Disabling node interleaving enables NUMA	Enabled
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	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

Fujitsu Settings

Table 10-5. Servers

Menu Option	Key	Value
Onboad Device Configuration	Onboad CNA	Enabled
	Onboard CNA Oprom	Enabled
	CNA Standy	Enabled
CPU Configuration	Power Technology	Custom
	Override OS Engery Performance	Enabled
	Energy Performance	Performance
Option Rom Configuration	Launch Slot 1 opRom	Disabled
	Launch Slot 2 opRom	Disabled
Boot	Boot Option #1	Emulex PXE 0:0 3 0 0
	Boot Option #2	Emulex PXE 0:0 3 0 1

Table 10-5. Servers (continued)

Menu Option	Key	Value
	Boot Option #3	SATA0 P5: SATADOM-ML 3ME
	Boot Option #4	Disabled
	Boot Option #5	Disabled
	Boot Option #6	Disabled
	Boot Option #7	Disabled
	Boot Option #8	Disabled
	Boot Option #9	Disabled
	Boot Option #10	Disabled
	Boot Option #11	Disabled

Troubleshooting VIA

11

This chapter includes the following topics:

- Host failed to be imaged with error Unable to Establish IPMI v2 / RMCP+ Session
- Servers fail to be Imaged due to Duplicate Port Entries on Management Switch
- 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.

Servers fail to be Imaged due to Duplicate Port Entries on Management Switch

Problem

When there are duplicate port entries on management switch, the OOB network is not accessible and host imaging fails.

Solution

1   Restore the OOB network connection.

2   Click Continue Imaging.

3   Power off all servers with the ipmitool command.

4   Power on the server with IP address 192.168.0.50 followed by the remaining servers with a 30 second gap between each server.

Solution

The rack is imaged successfully.

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 or SATADOM 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.

Note   This issue affects only management switches running the Cumulus OS.

Cause

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

Solution

1   Connect to the management swtich 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`.

Cloud Foundation Glossary

Term	Description
add rack	Configure an additional rack for a Cloud Foundation system.
additional rack	Additional racks (added after the first rack) to a Cloud Foundation system.
bring-up	Initial configuration of a newly deployedCloud Foundation system. .
Cloud Foundation system.	Set of physical racks managed as a unit by a single SDDC Manager.
first rack	First (primary) rack in the Cloud Foundation system. The management domain is deployed on this rack.
Hardware Management System (HMS)	Manages hosts and switches in the Cloud Foundation system.
host	An imaged server.
host 0	First host to be imaged by VIA. This host has the 192.168.100.50 IP address.
imaging	During imaging, SDDC software is pre-configured on a physical rack.
integrated system	System that combines hardware and software. Can be purchased from select VMware partners. The partner images the rack before sending it to the customer site.
inter-rack switches	Connects individual ToR switches with each other to provide connectivity across racks. These switches are required only when you have more than one rack in your Cloud Foundation system, and are placed on the second rack.
Lifecycle Manager (LCM)	Automates patching and upgrading of the software stack.
management domain	Cluster of physical hosts (first fours hosts in the physical rack) that house the management component VMs
management host	Standalone ESXi server to host the Windows jump VM used for imaging.
SDDC Manager	Software component that provisions, manages, and monitors the logical and physical resources of a Cloud Foundation system.
SDDC ManagerController VM	Contains the SDDC Managerservices and a shell from which command line tools can be run. This VM exposes the SDDC Manager UI.
SDDC Manager Utility VM	Contains the LCM depot, backup repository containing NSX Manager and host backups, and 2nd DNS instance.
server	Bare metal server in a physical rack. After imaging, it is referred to as a host.
Top of Rack (ToR) switch	Connects servers within a rack through 10Gbps links to the NICs on each server. A Cloud Foundation rack contains two ToR switches connected to each other.

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