

VMware Cloud Foundation Deployment Guide

23 JUN 2020

VMware Cloud Foundation 4.0

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 - 2020 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

| | |
|------------------------------------------------------------------|----|
| About the VMware Cloud Foundation Deployment Guide | 4 |
| 1 Preparing your Environment for Cloud Foundation | 5 |
| 2 Deploying Cloud Foundation | 6 |
| Deploy VMware Cloud Builder Appliance | 7 |
| Installing ESXi Software on Cloud Foundation Servers | 9 |
| Download ESXi Software and VIBs | 10 |
| Provide Network Information for Imaging | 10 |
| Upload ISOs and VIBs to the VMware Imaging Appliance service | 11 |
| Image Servers with ESXi and VIBs | 12 |
| Post-Imaging Tasks | 14 |
| Initiate the Cloud Foundation Bring-Up Process | 15 |
| Download and Complete the Deployment Parameter Workbook | 15 |
| About the Deployment Parameter Workbook | 16 |
| Upload the Deployment Parameter Workbook and Complete Deployment | 29 |
| 3 Troubleshooting Cloud Foundation Deployment | 31 |
| SoS Tool Options for Cloud Builder appliance | 31 |
| Cloud Builder Appliance Log Files | 35 |
| 4 Cloud Foundation Glossary | 36 |

About the VMware Cloud Foundation Deployment Guide

The *VMware Cloud Foundation Deployment Guide* provides information about installing ESXi software on Cloud Foundation servers and deploying the management domain using the Cloud Builder appliance.

Intended Audience

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

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

Related Publications

The *Introducing VMware Cloud Foundation* document provides a high-level overview of the VMware Cloud Foundation product

The *Planning and Preparation Workbook* provides detailed information about the software, tools, and external services that are required for Cloud Foundation.

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

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

Cloud Foundation Glossary

The Cloud Foundation Glossary defines terms specific to Cloud Foundation.

Preparing your Environment for Cloud Foundation

1

You must prepare your environment for deploying Cloud Foundation. See the *Planning and Preparation Workbook*.

Deploying Cloud Foundation

2

You begin the Cloud Foundation deployment process by deploying the VMware Cloud Builder appliance. The VMware Cloud Builder appliance includes the VMware Imaging Appliance service, which you can use to image your servers with ESXi software. After imaging your servers, you download and complete the deployment parameters workbook from the VMware Cloud Builder appliance to define your network information, host details, and other required information. During the deployment process, this workbook is automatically then converted to a JSON file and uploaded to the VMware Cloud Builder appliance. The provided information is validated, and the automated phase of the bring-up process begins.

Prerequisites

You must prepare your environment for deploying Cloud Foundation. See the *Planning and Preparation Workbook*.

Procedure

1 Deploy VMware Cloud Builder Appliance

The VMware Cloud Builder appliance is a VM which also includes a service called the VMware Imaging Appliance service which can be utilised for installing the base ESXi operating system on your physical servers. After you image the servers, you use the Cloud Builder appliance to deploy and configure the management domain and transfer inventory and control to SDDC Manager. During the deployment process, the Cloud Builder appliance validates network information you provide in the deployment parameter workbook such as DNS, network (VLANs, IPs, MTUs), and credentials.

2 Installing ESXi Software on Cloud Foundation Servers

You can use the VMware Imaging Appliance service (VIA) included with the VMware Cloud Builder appliance to image servers for use in the management domain and VI workload domains. Alternatively, you can install ESXi manually. For the supported ESXi version, see the BOM section of the *VMware Cloud Foundation Release Notes*.

3 Initiate the Cloud Foundation Bring-Up Process

The Cloud Foundation deployment process is referred to as bring-up. You specify deployment information specific to your environment such as networks, hosts, license keys, and other information in the deployment parameter workbook and upload the file to the VMware Cloud Builder appliance to initiate bring-up. During bring-up, the management domain is created on the ESXi hosts specified in the workbook. The Cloud Foundation software components are automatically deployed, configured, and licensed using the information provided.

Deploy VMware Cloud Builder Appliance

The VMware Cloud Builder appliance is a VM which also includes a service called the VMware Imaging Appliance service which can be utilised for installing the base ESXi operating system on your physical servers. After you image the servers, you use the Cloud Builder appliance to deploy and configure the management domain and transfer inventory and control to SDDC Manager. During the deployment process, the Cloud Builder appliance validates network information you provide in the deployment parameter workbook such as DNS, network (VLANS, IPs, MTUs), and credentials.

You must deploy the VMware Cloud Builder appliance on a suitable platform. This can be on a laptop under VMware Workstation or VMware Fusion, or on an ESXi host. The VMware Cloud Builder appliance must have network access to all hosts on the management network.

The procedure here describes deploying the VMware Cloud Builder appliance on an ESXi host. Other deployment methods have different procedures.

Prerequisites

The Cloud Builder appliance requires the following resources.

| Component | Requirement |
|-----------|-------------|
| CPU | 4 vCPUs |
| Memory | 4 GB |
| Storage | 150 GB |

To image servers and automate the deployment, the VMware Cloud Builder appliance must be on the same management network as the hosts to be used. It must also be able to access all required external services, such as DNS and NTP.

Procedure

- 1 Download the VMware Cloud Builder appliance OVA on the Windows machine.
- 2 Log in to the vSphere Host Client.
- 3 In the navigator, select **Host**.
- 4 Click **Create/Register VM**.

- 5 On the Select creation type dialog box, select **Deploy a virtual machine from an OVF or OVA file** and click **Next**.
- 6 Enter a name for the VM.
- 7 Select **Click to select files or drag/drop**. Select the VMware Cloud Builder appliance OVA from your local file system and click **Open**.
- 8 Click **Next**.
- 9 On the Select Storage page, select the storage for the VMware Cloud Builder appliance.
- 10 On the License agreements dialog box, click **I agree** and then click **Next**.
- 11 On the Select networks dialog box, select the port group associated with the VLAN ID used by the ESXi hosts where Cloud Foundation will be deployed and then click **Next**.
- 12 On the Additional settings dialog box, expand **Application** and enter the following information for the VMware Cloud Builder appliance:

| Setting | Details |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Admin Username | <p>The admin user name cannot be one of the following pre-defined user names:</p> <ul style="list-style-type: none"> ■ root ■ bin ■ daemon ■ messagebus ■ systemd-bus-proxy ■ systemd-journal-gateway ■ systemd-journal-remote ■ systemd-journal-upload ■ systemd-network ■ systemd-resolve ■ systemd-timesync ■ nobody ■ sshd ■ named ■ rpc ■ tftp ■ ntp ■ smmsp ■ cassandra |
| Admin Password/Admin Password confirm | The admin password must be a minimum of 8 characters and include at least one uppercase, one lowercase, one digit, and one special character. |
| Root password/Root password confirm | The root password must be a minimum of 8 characters and include at least one uppercase, one lowercase, one digit, and one special character. |
| Hostname | Enter the hostname for the VMware Cloud Builder appliance. |
| Network 1 IP Address | Enter the IP address for the VMware Cloud Builder appliance. |
| Network 1 Subnet Mask | For example, 255.255.255.0. |

| Setting | Details |
|-------------------------|--------------------------------------------------------------------------------------------------------------|
| Default Gateway | Enter the default gateway for the VMware Cloud Builder appliance. |
| DNS Servers | IP address of the primary and secondary DNS servers (comma separated). Do not specify more than two servers. |
| DNS Domain Name | For example, <code>vsphere.local</code> . |
| DNS Domain Search Paths | Comma separated. For example <code>vsphere.local, sf.vsphere.local</code> . |
| NTP Servers | Comma separated. |

- 13 Review the deployment details and click **Finish**.

Note Make sure your passwords meet the requirements specified above before clicking **Finish** or your deployment will not succeed.

- 14 After the VMware Cloud Builder appliance is deployed, SSH in to the VM with the admin credentials provided in step 12.
- 15 Ensure that you can ping the ESXi hosts.
- 16 Verify that the VMware Cloud Builder appliance has access to the required external services, such as DNS and NTP by performing forward and reverse DNS lookups for each host and the specified NTP servers.

Installing ESXi Software on Cloud Foundation Servers

You can use the VMware Imaging Appliance service (VIA) included with the VMware Cloud Builder appliance to image servers for use in the management domain and VI workload domains. Alternatively, you can install ESXi manually. For the supported ESXi version, see the BOM section of the *VMware Cloud Foundation Release Notes*.

Before you can complete the deployment parameter workbook to define your network information, host details, and other required information, you must install ESXi on your servers. If your servers are already installed with a supported version of ESXi, you can skip imaging. Otherwise, you can use VIA.

This guide describes using VIA to image servers prior to bring-up of a Cloud Foundation system. You can also use VIA to image servers prior to adding them to Cloud Foundation as part of the host commissioning process after bring-up is complete. See the *VMware Cloud Foundation Operations and Administration Guide* for more information.

Server Prerequisites

The servers that you image must meet certain prerequisites:

- PXE Boot is configured as primary boot option
- Install device is configured as the second boot option

- Legacy boot mode configured in BIOS

Note Although the VMware Imaging Appliance service does not support UEFI boot mode, Cloud Foundation does support it for servers configured outside of VIA.

- Servers are in the same L2 domain as the VMware Cloud Builder appliance
- Servers are reachable over an untagged VLAN/Network (VLAN ID 0)
- The VMware Cloud Builder appliance is deployed on an untagged VLAN/Network
- Server hardware/firmware should be configured for virtualization and vSAN and match the Cloud Foundation BOM as described in the Release Notes
- Physical hardware health status should be "healthy" without any errors
- Any onboard NICs are deactivate on the servers and only the two 10 GbE NICs reserved for use with Cloud Foundation are enabled in BIOS

The default root credentials for servers imaged with VIA are user **root**, password **EvoSddc!2016**.

Download ESXi Software and VIBs

In order to image your servers, you need to download an ESXi ISO and any vSphere Installation Bundles (VIBs) required to get the servers to a supported version of ESXi. See the BOM section of the VMware Cloud Foundation Release Notes for information about ESXi support.

You can download the ISO and VIBs from My VMware (<https://my.vmware.com>) to any location on the Windows machine that is connected to the VMware Cloud Builder appliance. Make sure to record the MD5 or SHA-1 checksums. You will need them when you upload the ISO/VIB to the VMware Imaging Appliance service.

Provide Network Information for Imaging

You must provide the VMware Imaging Appliance service with certain network information specific to your environment before you can image your servers. This information is contained in the `via.properties` file on the VMware Cloud Builder appliance.

Procedure

- 1 SSH into the VMware Cloud Builder appliance using the credentials specified when you deployed the VM. See [Deploy VMware Cloud Builder Appliance](#).
- 2 Type **su** to switch to the root user.
- 3 Navigate to the `/opt/vmware/evorack-imaging/config/` directory.

4 Update the `via.properties` file with your network information.

- a If the VMware Cloud Builder appliance is using the `eth0` interface (default), then you do not need to modify any of the properties in Section A. If the VMware Cloud Builder appliance has multiple network interfaces and is not using `eth0`, you must update the following properties.

| Property | Description |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>via.network.interface</code> | Interface of the VMware Cloud Builder appliance configured in management network. |
| <code>via.web.url</code> | The IP address used to access the VMware Imaging Appliance service UI. Update this with the IP address of VMware Cloud Builder appliance in the management network. |
| <code>via.network.ifaceaddr</code> | Update this with the IP address of VMware Cloud Builder appliance in the management network. |
| <code>via.dhcp.esxi.tftpServer</code> | IP address of the server where TFTP is running. Update this with the IP address of VMware Cloud Builder appliance in the management network. |
| <code>via.config.remote.pxe=false</code> | Do not modify. |

- b Update Section B with the network information for your environment.

| Property | Description |
|------------------------------------------------|--------------------------------------------------------|
| <code>via.dhcp.netmask</code> | Netmask of the management network. |
| <code>via.dhcp.subnet</code> | Subnet of the management network. |
| <code>via.dhcp.routers</code> | Gateway IP of the management network. |
| <code>via.esxi.firewall.allowed.network</code> | CIDR notation for subnet IP of the management network. |

5 Type `systemctl restart imaging.service` to restart the imaging service.

Wait for the imaging service to restart.

6 Type `systemctl status imaging.service` to verify that the imaging service is running.

What to do next

Log in to the VMware Imaging Appliance service and upload software.

Upload ISOs and VIBs to the VMware Imaging Appliance service

After you have downloaded the required software and updated `via.properties` with your network information, you can upload ISOs and VIBs to the VMware Imaging Appliance service.

Procedure

- 1 In a web browser on the Windows machine that is connected to the VMware Cloud Builder appliance, navigate to `https://Cloud_Builder_VM_IP:8445/via`.

The VMware Imaging Appliance service page displays.

- 2 Enter the admin credentials you provided when you deployed the VMware Cloud Builder appliance and click Log in.
- 3 Click **Bundle** and then click the **ESXi ISOs** tab.
- 4 Click **Browse** to locate and select the ISO.

VMware Imaging Appliance

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

ESXi ISOs | Modify VIBs

Available ISOs :

| Name | Source | Activate |
|----------------------------------------------------------------------------------|--------|----------|
| Select ISO to Add : VMware-VMvisor-Installer-7.0.0-15799291.x86_64.iso | | |
| MD5 Checksum : | | |
| Checksum Type : MD5 <input checked="" type="radio"/> SHA-1 <input type="radio"/> | | |
| ESXi License Key : Optional | | |

Upload ISO

- 5 Select the checksum type and enter the checksum.
- 6 Click **Upload ISO**.
- 7 When the uploaded ISO appears, select **Activate** to use the ISO for imaging servers.
- 8 Click the **Modify VIBs** tab.

The steps for uploading VIBs are optional.

- 9 Click **Browse** to locate and select the VIB.

VMware Imaging Appliance

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

ESXi ISOs | Modify VIBs

Available VIBs :

| Name | In use |
|-------------------------------------------------------------------|--------|
| Select VIB : VMware_bootbank_cpu-microcode_7.0.0-1.0.15799291.vib | |

Upload VIB

- 10 Click **Upload VIB**.
- 11 When the uploaded VIB appears, select **In use** to use the VIB for imaging servers.

What to do next

Use the selected ISO and VIB(s) to image servers for use with Cloud Foundation.

Image Servers with ESXi and VIBs

Once you have uploaded the required ESXi and VIB packages to the VMware Imaging Appliance service, you can begin imaging servers. You can image an individual server, or multiple servers at the same time.

You can use VIA to image servers for use in the management domain and VI workload domains. The management domain requires a minimum of four servers. See the *Planning and Preparation Workbook* for more information about requirements.

Note When you image servers, VIA uses the ESXi ISO that you activated and the VIB(s) that you marked as **In use**.

Procedure

- 1 In a web browser on the Windows machine that is connected to the VMware Cloud Builder appliance, navigate to `https://Cloud_Builder_VM_IP:8445/via`.

The VMware Imaging Appliance service page displays.

- 2 Enter the admin credentials you provided when you deployed the VMware Cloud Builder appliance and click Log in.
- 3 Click Imaging.
- 4 Enter the required information.

Name

Description

ESXI SERVER

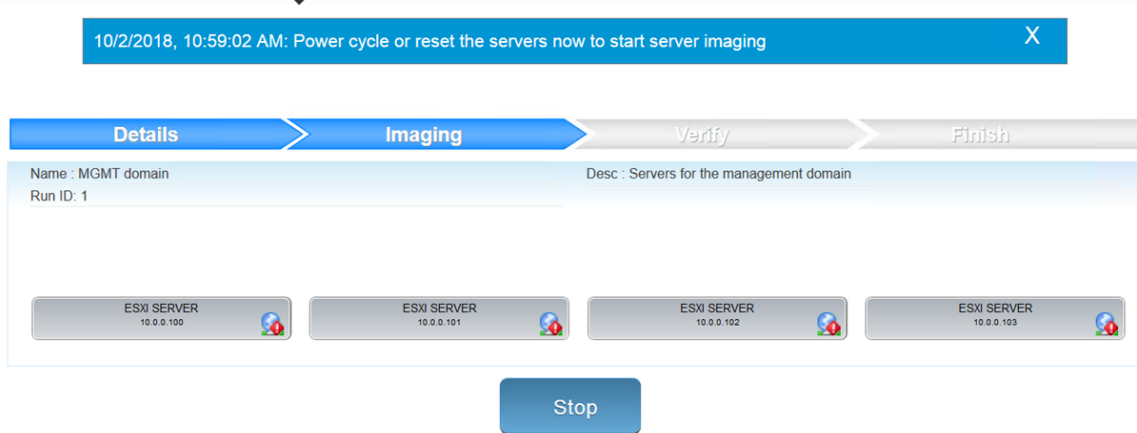
NTP Server: Number:

| | | | | |
|---|---------------------------------------------|-----------------------------------------------------|-------------------------------------------------------------|--------------------------------------------------------------------|
| 1 | IP: <input type="text" value="10.0.0.100"/> | MAC: <input type="text" value="02:00:46:d2:08:73"/> | Hostname: <input type="text" value="esxi-1.vrack"/> | Host FQDN: <input type="text" value="esxi-1.vrack.vsphere.local"/> |
| 2 | IP: <input type="text" value="10.0.0.101"/> | MAC: <input type="text" value="02:00:46:f6:0c:9c"/> | Hostname: <input type="text" value="esxi-2.vrack"/> | Host FQDN: <input type="text" value="esxi-2.vrack.vsphere.local"/> |
| 3 | IP: <input type="text" value="10.0.0.102"/> | MAC: <input type="text" value="02:00:46:7b:c5:0f"/> | Hostname: <input type="text" value="esxi-3.vrack"/> | Host FQDN: <input type="text" value="esxi-3.vrack.vsphere.local"/> |
| 4 | IP: <input type="text" value="10.0.0.103"/> | MAC: <input type="text" value="02:00:46:2c:19:4a"/> | Hostname: <input type="text" value="esxi-4.vrack.vsphere"/> | Host FQDN: <input type="text" value="esxi-4.vrack.vsphere.local"/> |

| Option | Description |
|-------------|-------------------------------------------------------------------------------|
| Name | Enter a name for the imaging job. |
| Number | Enter the number of servers you want to image with the selected ISO and VIBs. |
| Description | Enter a description for the imaging job. |
| NTP Server | Enter the IP address for the NTP server. |
| IP | Enter the IP address for the server. |
| MAC | Enter the MAC address for the server. |
| Hostname | Enter the hostname for the server. |
| Host FQDN | Enter the FQDN for the server. |

- 5 Click **Start Imaging**.

- 6 When prompted, power cycle the server(s) to continue imaging.



VIA displays information about the progress of imaging. Click a server to view details. Once imaging is complete, VIA performs verification of the servers.

- 7 When verification is finished, click **Complete**.

What to do next

Perform post-imaging tasks before you download the deployment parameter workbook and begin the bring-up process.

Post-Imaging Tasks

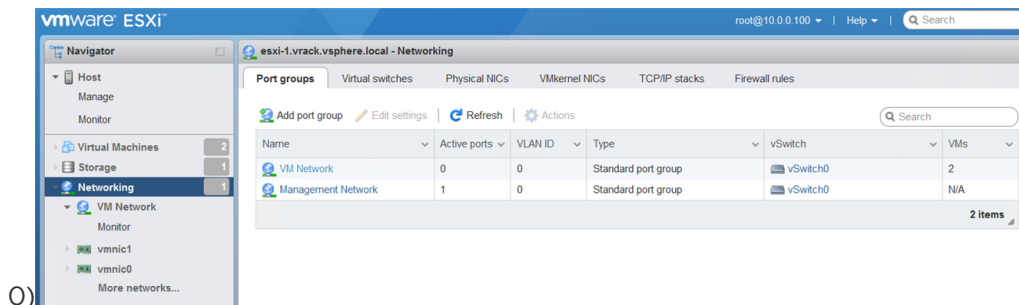
After you image your servers with ESXi and VIBs, you must perform some post-imaging tasks, depending on whether you use an untagged or a tagged management VLAN.

For imaging servers, the VMware Imaging Appliance service requires an untagged VLAN. You can continue to use an untagged VLAN for management, or you can use a tagged VLAN.

Untagged Management VLAN

In this scenario, you use the same network for provisioning and management.

- Ensure that the Management Network and VM Network port groups on each host use the untagged VLAN (VLAN ID



- Verify that your DNS and NTP server are routable to the management network and ESXi hosts can reach them. To configure a default gateway or static routes on your ESXi hosts, see <https://kb.vmware.com/kb/2001426>.

Tagged Management VLAN

In this scenario, you use an untagged VLAN for provisioning and a tagged VLAN for management.

- Modify the Management Network and VM Network port groups on each host to use the tagged VLAN
- Migrate the hosts from the provisioning network to the management network on the TOR switches
- Verify that your DNS and NTP server are routable to the management network and ESXi hosts can reach them. To configure a default gateway or static routes on your ESXi hosts, see <https://kb.vmware.com/kb/2001426>.

Initiate the Cloud Foundation Bring-Up Process

The Cloud Foundation deployment process is referred to as bring-up. You specify deployment information specific to your environment such as networks, hosts, license keys, and other information in the deployment parameter workbook and upload the file to the VMware Cloud Builder appliance to initiate bring-up. During bring-up, the management domain is created on the ESXi hosts specified in the workbook. The Cloud Foundation software components are automatically deployed, configured, and licensed using the information provided.

Download and Complete the Deployment Parameter Workbook

The deployment parameter workbook provides a mechanism to specify infrastructure information specific to your environment. This includes information about your networks, hosts, license keys, and other information. The workbook is downloaded from the VMware Cloud Builder appliance and the completed workbook is uploaded back to the VM. The deployment parameter workbook can be reused to deploy multiple Cloud Foundation instances of the same version.

Cloud Foundation supports isolating VMkernel traffic (management, vSAN, vMotion, or overlay) across multiple physical NICs (pNICs). However, you cannot use the deployment parameter sheet for bring-up of hosts with more than two pNICs. To perform bring-up with hosts with more than two pNICs, use the [VMware Cloud Foundation API](#).

Procedure

- 1 In a web browser on the Windows machine that is connected to the VMware Cloud Builder appliance, navigate to `https://Cloud_Builder_VM_IP`.
- 2 Enter the admin credentials you provided when you deployed the VMware Cloud Builder appliance and then click **Log In**.
- 3 Read the End-User License Agreement and accept it. Click **Next**.
- 4 Select **VMware Cloud Foundation** on the Supported Platform page and click **Next**.

- 5 Review the prerequisites checklist and ensure the requirements are met before proceeding. If there are any gaps, ensure they are fixed before proceeding to avoid issues during the the bring-up process.

Select the check box at the bottom of the page to acknowledge that your environment meets the listed requirements. You can download or print the prerequisite list as well.

- 6 Click **Next**.
- 7 In the Download Deployment Parameter Workbook section, click **Download**.
- 8 Complete the workbook. See [About the Deployment Parameter Workbook](#).

About the Deployment Parameter Workbook

The deployment parameter workbook contains tabs categorizing the information required for deploying Cloud Foundation. The information provided is used to create the management domain.

The fields in yellow contain sample values that you should replace with the information for your environment. If a cell turns red, the required information is missing, or validation has failed.

Prerequisites Checklist Tab

This tab is a summary of infrastructure configuration requirements that need to be satisfied before deploying Cloud Foundation.

The Cloud Builder appliance runs a platform audit before starting deployment to check if the requirements listed on this tab are met. If the audit fails, you cannot proceed with the deployment.

Physical Network

- Top of Rack switches are configured. Each host and NIC in the management domain must have the same network configuration. No Ethernet link aggregation technology (LAG/VPC/LACP) is being used.
- IP ranges, subnet mask, and a reliable L3 (default) gateway for each VLAN.
- Jumbo Frames (MTU 9000) are recommended on all VLANs. At a minimum, an MTU of 1600 is required on the NSX-T Host Overlay (Host TEP) and NSX-T Edge Overlay (Edge TEP) VLANs end-to-end through your environment.
- VLANs for management, vMotion, vSAN, NSX-T Host Overlay (Host TEP), NSX-T Edge Overlay (Edge TEP), and NSX uplink networks are created and tagged to all host ports. Each VLAN is 802.1q tagged. NSX-T Host Overlay (Host TEP) VLAN and NSX-T Edge Overlay (Host TEP) VLAN are routed to each other.
- Management IP is VLAN-backed and configured on the hosts. vMotion and vSAN IP ranges are configured during the bring-up process.
- DHCP with an appropriate scope size (one IP per physical NIC per host) is configured for the NSX Host Overlay (Host TEP) VLAN.

- To use Application Virtual Networks (AVNs) for vRealize Suite components you also need:
 - Top of Rack (ToR) switches configured with the Border Gateway Protocol (BGP), including Autonomous System (AS) numbers and BGP neighbor passwords, and interfaces to connect with NSX-T Edge nodes.
 - Two VLANs configured and presented to all ESXi hosts to support the uplink configuration between the (ToR) switches and NSX-T Edge nodes for outbound communication.

Servers must be racked and cabled. ESXi version as mentioned in the *VMware Cloud Foundation Release Notes* must be installed on each host.

For detailed planning guidance, see the *Planning and Preparation Workbook*.

Physical Hardware and ESXi Hosts

- All servers are vSAN-compliant and certified on the [VMware Compatibility Guide](#), including BIOS, HBA, SSD, HDD, and so on.
- Identical hardware (CPU, Memory, NICs, SSD/HDD, and so on) within the management cluster is highly recommended. Refer to vSAN documentation for minimum configuration.
- Hardware and firmware (including HBA and BIOS) is configured for vSAN.
- One physical NIC on each host is configured and connected to the vSphere Standard switch. The second physical NIC is not configured.
- Physical hardware health status is "healthy" without any errors.
- ESXi is freshly installed on each host. The ESXi version matches the build listed in the Cloud Foundation Bill of Materials (BOM). See the *VMware Cloud Foundation Release Notes* for the BOM.
- The default port group, VM Network, is configured with the same VLAN ID as the management network.
- TSM-SSH service is running on each ESXi host with the policy configured to `Start and stop with host`.
- All hosts are configured and in synchronization with a central time server (NTP). NTP service policy set to `Start and stop with host`.
- Each ESXi host is running a non-expired license. The bring-up process will configure the permanent license.

If you used the VMware Imaging Appliance service to install ESXi on your hosts and you completed the [Post-Imaging Tasks](#), then your hosts are already configured properly and are ready for bring-up.

DNS Configuration

Host names for the following components must be resolvable for forward, reverse, short name, and long name resolution.

- ESXi hosts

- vCenter Server
- NSX-T Management cluster
- SDDC Manager

Management Workloads Tab

This tab provides an overview of the components deployed by the VMware Cloud Builder appliance. The sizes and versions are not editable and are provided for reference only.

Input required:

- In column L, update the red fields with your license keys. Ensure the license key matches the product and version listed in each row. The license key audit during bring-up validates both the format of the key entered and the validity of the key.

The required license keys are:

- ESXi
- vSAN
- vCenter Server
- NSX-T Data Center
- SDDC Manager

If you do not enter license keys for these products, you will not be able to create or expand VI workload domains.

Users and Groups Tab

This tab details the accounts and initial passwords for the Cloud Foundation components. You must provide input for each yellow box. A red cell may indicate that validations on the password length has failed.

Input Required

Update the Default Password field for each user (including the automation user in the last row). Passwords can be different per user or common across multiple users. The tables below provide details on password requirements.

Table 2-1. Password Complexity

| Password | Complexity |
|--------------------------------------------------|----------------------------------------------------------------------------------|
| ESXi Host root account | This is the password which you configured on the hosts during ESXi installation. |
| Default Single-Sign on domain administrator user | SSO |
| vCenter Server virtual appliance root account | Standard |
| NSX-T virtual appliance root account | NSX-T |

Table 2-1. Password Complexity (continued)

| Password | Complexity |
|----------------------------------------------------|------------|
| NSX-T user interface and default CLI admin account | NSX-T |
| NSX-T audit CLI account | NSX-T |
| SDDC Manager | |
| SDDC Manager appliance root account | SSO |
| SDDC Manager super user | SSO |
| SDDC Manager REST API user | SSO |

Table 2-2. Password Requirements based on Complexity

| Password Type | Requirements Based on Complexity |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Standard | <ol style="list-style-type: none"> Length 8-12 characters Must include: <ul style="list-style-type: none"> ■ mix of upper-case and lower-case letters ■ a number ■ a special character such as @ ! # \$ % ^ or ? Cannot include: * { } [] () / \ ' " ~ , ; : . < > |
| SSO (accounts in SSO vsphere.local) | <ol style="list-style-type: none"> Length 8-20 characters Must include: <ul style="list-style-type: none"> ■ mix of upper-case and lower-case letters ■ a number ■ a special character |
| NSX-T | <ol style="list-style-type: none"> At least 12 characters Must include: <ul style="list-style-type: none"> ■ mix of upper-case and lower-case letters ■ a number ■ a special character ■ at least five different characters |

Hosts and Networks tab

In this tab, specify details of your existing networking infrastructure. This information is configured on the appropriate Cloud Foundation components.

Management Domain Networks

This section covers the VLANs, gateways, MTU, and expected IP ranges and subnet mask for each network you have configured on the Top of Rack switches in your environment.

Table 2-3. Input Required

| VLAN | Portgroup Name | CIDR Notation | Gateway | MTU |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|-----------------------------------------------------------------------|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Enter VLAN ID for management network. The VLAN ID can be between 0 and 4094. Note Enter 0 if you imaged the servers with VIA. VLAN 0 means the management network is untagged. | Enter a portgroup name for the management network. | Enter CIDR notation for management network | Enter gateway IP for management network | Enter MTU for management network. The MTU can be between 1500 and 9000. |
| Enter VLAN ID for vMotion network The VLAN ID can be between 0 and 4094. | Enter a portgroup name for the vMotion network. | Enter CIDR notation for vMotion network | Enter gateway IP for vMotion network | Enter MTU for vMotion network The MTU can be between 1500 and 9000. |
| Enter VLAN ID for vSAN network The VLAN ID can be between 0 and 4094. | Enter a portgroup name for the vSAN network. | Enter CIDR notation for vSAN network | Enter gateway IP for vSAN network | Enter MTU for vSAN network The MTU can be between 1500 and 9000. |
| Enter VLAN ID for the NSX-T host overlay network The VLAN ID can be between 0 and 4094. | Enter a portgroup name for the NSX-T host overlay network. | N/A Cloud Foundation uses DHCP for VTEPs, so CIDR is not required. | N/A Cloud Foundation uses DHCP for VTEPs, so a gateway is not required. | Enter MTU for the NSX-T host overlay network The MTU can be between 1500 and 9000. |
| Enter VLAN ID for the first uplink. The VLAN ID can be between 0 and 4094. | Enter a portgroup name for the first uplink. | Enter CIDR notation for the first uplink | Enter gateway IP for the first uplink | Enter MTU for the first uplink The MTU can be between 1500 and 9000. |
| Enter VLAN ID for the second uplink. The VLAN ID can be between 0 and 4094. | Enter a portgroup name for the second uplink. | Enter CIDR notation for the second uplink | Enter gateway IP for the second uplink | Enter MTU for the second uplink The MTU can be between 1500 and 9000. |
| Enter VLAN ID for the NSX-T Edge overlay network The VLAN ID can be between 0 and 4094. | Enter a portgroup name for the NSX-T Edge overlay network. | Enter the CIDR notation for the NSX-T Edge overlay network | Enter the gateway IP for the NSX-T Edge overlay network | Enter the MTU for the NSX-T Edge overlay network. The MTU can be between 1500 and 9000. |

Management Domain ESXi Hosts

Specify the IP addresses of the ESXi hosts for the management domain. In a standard deployment, only four hosts are required in the management domain. Cloud Foundation can also be deployed with a consolidated architecture. In a consolidated deployment, all workloads are deployed in the management domain instead of to separate workload domains. As such, additional hosts may be required to provide the capacity needed. In this section, only enter values for the number of hosts desired in the management domain.

Table 2-4. Input Required

| Host Name | IP Address |
|---------------|-------------------------------------------------------------------------------|
| sfo01m01esx01 | Enter IP address of first ESXi host where Cloud Foundation is to be deployed. |
| sfo01m01esx02 | Enter IP address of second ESXi host |
| sfo01m01esx03 | Enter IP address of third ESXi host |
| sfo01m01esx04 | Enter IP address of fourth ESXi host |

Inclusion Ranges

Specify IP inclusion ranges for the vSAN and vMotion networks of the management domain. IP addresses from the specified range are automatically assigned to hosts. Ensure that the IP ranges include sufficient IP addresses for the initial deployment. The number of IP addresses must be at least equal to the number of hosts deployed as part of Cloud Foundation.

As an example, if you specify the range start value as 192.168.1.1 and end as 192.168.1.20, a total of 20 IP addresses would be used.

Do not use special IP addresses, such as the network or broadcast address.

IPs for the vMotion range must be part of the VLAN configured with the vMotion portgroup. IPs for the vSAN range must be part of the VLAN configured for the vSAN portgroup. All IPs within the range must be available for use or IP conflicts will occur. It is a good practice to validate this prior to starting a deployment.

Table 2-5. Input Required

| Network | Start IP | End IP |
|---------|------------------------------------------------------|--------------------------------|
| vMotion | Enter start of IP address range for vMotion network. | Enter end of IP address range. |
| VSAN | Enter start of IP address range for vMotion network. | Enter end of IP address range. |

ESXi Host Security Thumbprints

If you want bring-up to validate the SSH fingerprint and SSL thumbprints of the hosts before connecting to them, select **Yes** in the **Validate ESXi Thumbprints** field.

If you set **Validate ESXi Thumbprints** to **Yes**, follow the steps below.

- 1 Open the DCUI screen for each server.

- 2 From the View Support Information tab, copy the SSH RSA Key Fingerprint and SSL Thumbprint.
- 3 Replace the example values in the deployment parameter workbook with these values.

Virtual Networking (Cloud Foundation 4.0.1 only)

Cloud Foundation 4.0.1 provides three vSphere Distributed Switch profiles that allow you to perform bring-up of hosts with two or four pNICs and to create up to two vSphere Distributed Switches for isolating VMkernel traffic. The information that you are required to provide depends on the profile that you select.

| vSphere Distributed Switch Profile | Description |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Profile 1 | <ul style="list-style-type: none"> ■ One vSphere Distributed Switch (vDS): Traffic for Management, vMotion, vSAN, Host Overlay, Edge Overlay, and Uplink networks using specified pNICs. ■ Two or four physical NICs (pNICs) |
| Profile 2 | <ul style="list-style-type: none"> ■ Two vSphere Distributed Switches (vDS) ■ Four physical NICs (pNICs) ■ Primary vDS: Traffic for Management, vMotion, and vSAN networks using specified pNICs. ■ Secondary vDS: Traffic for Host Overlay, Edge Overlay, and Uplink networks using specified pNICs. |
| Profile 3 | <ul style="list-style-type: none"> ■ Two vSphere Distributed Switches (vDS) ■ Four physical NICs (pNICs) ■ Primary vDS: Traffic for Management, vMotion, Host Overlay, Edge Overlay, and Uplink networks using specified pNICs. ■ Secondary vDS: Traffic for vSAN network using specified pNICs. |

After you select a vSphere Distributed Switch Profile, enter the required information for that profile.

| | |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vSphere Standard Switch Name | Enter a name for the vSphere Standard Switch. |
| Primary vSphere Distributed Switch - Name | Enter a name for the primary vSphere Distributed Switch (vDS). You can modify the portgroup names of the management domain networks to make it clear which vDS each network uses. |
| Primary vSphere Distributed Switch - pNICs | Select the physical NICs to assign to the primary vDS. |
| Primary vSphere Distributed Switch - MTU Size | Enter the MTU size for the primary vDS. Default value is 9000. |
| Secondary vSphere Distributed Switch - Name | <p>Enter a name for the secondary vSphere Distributed Switch (vDS). You can modify the portgroup names of the management domain networks to make it clear which vDS each network uses.</p> <p>Note If you are not creating a secondary vDS, enter n/a.</p> |

| | |
|-------------------------------------------------|------------------------------------------------------------------|
| Secondary vSphere Distributed Switch - pNICs | Select the physical NICs to assign to the secondary vDS. |
| Secondary vSphere Distributed Switch - MTU Size | Enter the MTU size for the secondary vDS. Default value is 9000. |

Deploy Parameters Tab: Existing Infrastructure Details

Your existing DNS infrastructure is used to provide forward and reverse name resolution for all hosts and VMs in the Cloud Foundation SDDC. External NTP sources are also utilized to synchronize the time between the software components.

Table 2-6. Infrastructure

| Parameter | Value |
|---------------|---------------------------------------------------------------------------------------------------------|
| DNS Server #1 | Enter IP address of first DNS server. |
| DNS Server #2 | Enter IP address of second DNS server. If you have only one DNS server, enter n/a in this cell. |
| NTP Server #1 | Enter IP address or FQDN of first NTP server. |
| NTP Server #2 | Enter IP address or FQDN of second NTP server. If you have only one NTP server, enter n/a in this cell. |

Table 2-7. DNS Zone

| Parameter | Value |
|---------------|-------------------------------------------------------------|
| DNS Zone Name | Enter root domain name for your SDDC management components. |

Table 2-8. CEIP

| Parameter | Value |
|---------------------------------------------------------|------------------------------------------------------------------------------------------|
| Enable Customer Experience Improvement Program ("CEIP") | Select an option to turn on or off CEIP across vSphere, NSX-T, and vSAN during bring-up. |

Deploy Parameters Tab: vSphere Infrastructure

Specify details for the vSphere infrastructure.

This section of the deployment parameter workbook contains sample host names, but you can update them with names that meet your naming standards. This host name is one part of the FQDN - the second part of the FQDN is the root or child DNS zone name provided above.

The specified host names and IP addresses must be resolvable using the DNS servers provided earlier, both forward (hostname to IP) and reverse (IP to hostname), otherwise the bring-up process will fail.

Table 2-9. Management Cluster

| Parameter | Host Name | IP Address |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vCenter Server | Enter a host name for the vCenter Server. | Enter the IP address for the vCenter Server that is part of the management VLAN. This is the same VLAN and IP address space where the ESXi management VMKernels reside. |
| vCenter Server Appliance Size (Default Small) | This parameter defines the size of the vCenter Server to be deployed. Default size is Small. Additional options are: tiny, medium, large, and xlarge. | |

Table 2-10. vCenter Datacenter and Cluster

| Parameter | Value |
|---------------------|--------------------------------------------------------------------------------------------------------------------------|
| Datacenter Name | Enter a name for the management datacenter. |
| Cluster Name | Enter a name for the management cluster. |
| Cluster EVC Setting | To enable EVC on the management cluster, select the CPU chipset that should be applied to enhance vMotion compatability. |

In the Virtual Networking - ESXi Hosts section below, the default settings are appropriate for hosts with two physical NICs (pNICs). To perform bring-up with hosts with more than two pNICs, use the [VMware Cloud Foundation API](#).

Table 2-11. Virtual Networking - ESXi Hosts

| Parameter | Value |
|--------------------------------------------|-------------------------------------------------------------|
| vSphere Standard Switch - Management | Do not modify. |
| vmnic Allocated to vSS - Management | Select the physical NIC to assign to the management vSS. |
| Physical NIC to Assign to vDS - Management | Select the physical NIC to assign to the management vDS. |
| vSphere Distributed Switch Name | Enter a name for the management vSphere distributed switch. |
| vSphere Distributed Switch MTU Size | Enter the MTU size. Default value is 9000. |

Table 2-12. vSphere Resource Pools

| Parameter | Value |
|-------------------------------|-------------------------------------------------------------------------------------------------------|
| Resource Pool SDDC Management | Specify the vSphere resource pool name for management VMs. |
| Resource Pool SDDC Edge | Specify the vSphere resource pool name for NSX-T VMs. |
| Resource Pool User Edge | Specify the vSphere resource pool name for user deployed NSX-T VMs in a consolidated architecture. |
| Resource Pool User VM | Specify the vSphere resource pool name for user deployed workload VMs in a consolidated architecture. |

Table 2-13. vSphere Datastore

| Parameter | Value |
|-------------------------------------------|--------------------------------------------------------------------|
| vSAN Datastore Name | Enter vSAN datastore name for your management components. |
| Enable vSAN Deduplication and Compression | Select Yes to turn on Dedupe and Compression capabilities of vSAN. |

Deploy Parameters Tab: NSX-T Data Center

Enter IP addresses and host names for NSX-T installation.

Table 2-14. NSX-T Management Cluster

| Parameter | Value |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NSX-T Management Cluster VIP | <p>Enter the host name and IP address for the NSX Manager VIP.</p> <p>The host name can match your naming standards but must be registered in DNS with both forward and reverse resolution matching the specified IP.</p> <p>The IP address must be part of the management VLAN. This is the same VLAN and IP address space where the vCenter and ESXi management VMKernels reside.</p> |
| NSX-T Virtual Appliance Node #1 | Enter the host name and IP address for the first node in the NSX Manager cluster. |
| NSX-T Virtual Appliance Node #2 | Enter the host name and IP address for the second node in the NSX Manager cluster. |
| NSX-T Virtual Appliance Node #3 | Enter the host name and IP address for the third node in the NSX Manager cluster. |
| NSX-T Virtual Appliance Size | Select the size for the NSX Manager virtual appliances. The default is medium. |

Application Virtual Networking

Application virtual networks (AVNs) are virtual networks, backed by overlay segments using the encapsulation protocol of NSX-T, that use a single IP network address space to span across data centers. By default, Cloud Foundation deploys and configures AVNs during bring-up. If you do not want to deploy and configure AVNs, select **No** from the drop-down menu. Deselect AVNs if you want to deploy vRealize Suite components to VLAN-backed networks.

A two-node NSX-T Edge cluster routes traffic between the AVNs and the public network. Routing to the management network and external networks is dynamic and based on the Border Gateway Protocol (BGP).

Table 2-15. NSX-T Edge Nodes with ECMP

| Parameter | Value |
|---------------------------------------|--------------------------------------------------------------|
| NSX-T Edge Cluster Name | Enter a name for the Edge cluster. |
| NSX-T Edge Nodes Autonomous System ID | Enter the AS ID of the Edge nodes to peer with ToR switches. |
| NSX-T Edge Node Appliance Size | The default size is medium. |

Table 2-16. North-South Routing Edge Node 1

| Parameter | Value |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Edge Name Node 1 | Enter a name for the first Edge node. The Edge node name must match the short hostname reserved for the VM. Combined with the DNS Zone Name this should match the FQDN reserved for the VM in the DNS server. |
| Edge Management IP Address Node 1 | Enter a management IP address for the first node. The IP address must be part of the management VLAN. |
| Edge Uplink 1 IP Address Node 1 | Enter the first uplink IP address to use for Node 1. This is the IP address connected to the first ToR switch. The IP address must be part of the NSX-T Edge Uplink 1 VLAN. |
| Edge Uplink 2 IP Address Node 1 | Enter the second uplink IP address to use for Node 1. This is the IP address connected to the second ToR switch. The IP address must be part of the NSX-T Edge Uplink 2 VLAN. |
| Edge Overlay IP Address #01 Node 1 | Enter the first Edge overlay IP address to use for Node 1. The IP address must be part of the NSX-T Edge Overlay VLAN. |
| Edge Overlay IP Address #02 Node 1 | Enter the second Edge overlay IP address to use for Node 1. The IP address must be part of the NSX-T Edge Overlay VLAN. |

Table 2-17. North-South Routing Edge Node 2

| Parameter | Value |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Edge Name Node 2 | Enter a name for the second Edge node. The Edge node name must match the short hostname reserved for the VM. Combined with the DNS Zone Name this should match the FQDN reserved for the VM in the DNS server. |
| Edge Management IP Address Node 2 | Enter a management IP address for the second node. The IP address must be part of the management VLAN. |
| Edge Uplink 1 IP Address Node 2 | Enter the first uplink IP address to use Node 2. This is the IP address connected to the first ToR switch. The IP address must be part of the NSX-T Edge Uplink 1 VLAN. |
| Edge Uplink 2 IP Address Node 2 | Enter the second uplink IP address to use for Node 2. This is the IP address connected to the second ToR switch. The IP address must be part of the NSX-T Edge Uplink 2 VLAN. |

Table 2-17. North-South Routing Edge Node 2 (continued)

| Parameter | Value |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| Edge Overlay IP Address #01 Node 2 | Enter the first Edge overlay IP address to use for Node 2. The IP address must be part of the NSX-T Edge Overlay VLAN. |
| Edge Overlay IP Address #02 Node 2 | Enter the first Edge overlay IP address to use for Node 2. The IP address must be part of the NSX-T Edge Overlay VLAN. |

Prepare your top of rack (ToR) switches by configuring Border Gateway Protocol (BGP) on the switches, defining the Autonomous System (AS) number, BGP password, Router ID, and creating interfaces to connect with Edge nodes.

Table 2-18. Top of Rack Switches for BGP Peering

| Parameter | Value |
|---------------------------------------|------------------------------------------------------------------------------------------|
| Top of Rack 1 - IP Address | Enter the IP address of the first ToR switch. |
| Top of Rack 1 - Autonomous System ID | Enter the AS ID for the first switch. |
| Top of Rack 1 - BGP Neighbor Password | Enter the BGP neighbor password for the first switch. |
| Top of Rack 2 - IP Address | Enter the IP address of the second ToR switch. |
| Top of Rack 2 - Autonomous System ID | Enter the AS ID for the second switch. This should match the AS ID for the first switch. |
| Top of Rack 2 - BGP Neighbor Password | Enter the BGP neighbor password for the second switch. |

Prepare your top of rack (ToR) switches to announce the subnets configured on the logical segments over BGP to make the segments routable in the data center.

Table 2-19. Application Virtual Networks

| Parameter | Value |
|----------------------------|-------------------------------------------------------------------------|
| Region A - Logical Segment | Enter a name to use for the Region A logical segment. |
| Region A - Networks | Enter the gateway IP and CIDR notation to use for the Region A network. |
| xRegion - Logical Segment | Enter a name to use for the xRegion logical segment. |
| xRegion - Networks | Enter the gateway IP and CIDR notation to use for the xRegion network. |

The following example shows how the NSX-T Data Center parameters (with AVNs) that you specify in the deployment parameter workbook map to the network topology in NSX Manager.

Figure 2-1. NSX-T Data Center Deployment Parameters

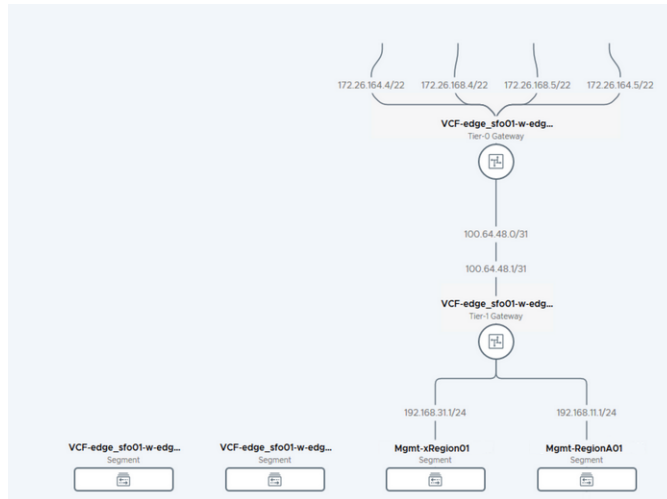
| NSX-T Data Center on vSphere | | NSX-T Management Cluster | | Hostname | IP Address | Do you want to deploy and configure Application Virtual Networks? <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No |
|------------------------------------------------------------------------------------|--|-----------------------------------------------|--|------------|---------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> NSX-T Nodes - Resolvable in DNS | | NSX-T Management Cluster VIP | | nsx-mgmt | 172.17.210.30 | |
| <input checked="" type="checkbox"/> NSX-T Nodes - Hostnames and Static IPs Defined | | NSX-T Virtual Appliance Node #1 | | nsx-mgmt-1 | 172.17.210.31 | |
| | | NSX-T Virtual Appliance Node #2 | | nsx-mgmt-2 | 172.17.210.32 | |
| | | NSX-T Virtual Appliance Node #3 | | nsx-mgmt-3 | 172.17.210.33 | |
| | | NSX-T Virtual Appliance Size (Default Medium) | | medium | 172.17.210.33 | |

| Application Virtual Networks Used to Deploy Solutions on VMs are Cloud Foundation | | | |
|-----------------------------------------------------------------------------------|--|-----------------------|-------|
| NSX-T Edge Nodes (vCMP) | | Value | Value |
| NSX-T Edge Cluster Name | | nsx-tv-edge-cluster01 | |
| NSX-T Edge Nodes Autonomous System | | 65003 | |
| NSX-T Edge Node Appliance Size (Default Medium) | | medium | |
| North-South Routing Edge Node 1 | | Value | Value |
| Edge Name Node 1 | | nsx-edge-node1 | |
| Edge Management IP Address Node 1 | | 172.17.210.50 | |
| Edge Uplink IP Address Node 1 | | 172.26.164.4 | |
| Edge Uplink 2 IP Address Node 1 | | 172.26.164.4 | |
| Edge Overlay IP Address #01 Node 1 | | 172.26.160.12 | |
| Edge Overlay IP Address #02 Node 1 | | 172.26.160.13 | |
| North-South Routing Edge Node 2 | | Value | Value |
| Edge Name Node 2 | | nsx-edge-node2 | |
| Edge Management IP Address Node 2 | | 172.17.210.51 | |
| Edge Uplink IP Address Node 2 | | 172.26.164.5 | |
| Edge Uplink 2 IP Address Node 2 | | 172.26.164.5 | |
| Edge Overlay IP Address #01 Node 2 | | 172.26.160.14 | |
| Edge Overlay IP Address #02 Node 2 | | 172.26.160.15 | |

| Top of Rack Switches for BGP Peering | | | |
|--------------------------------------|--|----------------|--|
| Top of Rack 1- IP Address | | 172.26.164.251 | |
| Top of Rack 1- Autonomous System ID | | 65001 | |
| Top of Rack 1- BGP Neighbor Password | | VM@ne#t | |
| Top of Rack 2- IP Address | | 172.26.168.251 | |
| Top of Rack 2- Autonomous System ID | | 65001 | |
| Top of Rack 2- BGP Neighbor Password | | VM@ne#t | |

| Application Virtual Networks | | | |
|-----------------------------------------------|----------------------------------|-----------------|-----------------|
| Region | Specific Application Virtual Net | Gateway | CIDR Notation |
| Region A - Logical Segment | | VM@ne-RegionA01 | |
| Region A - Network | | 172.168.1.11 | 172.168.1.11/24 |
| Cross Region Specific Application Virtual Net | | VM@ne-RegionA01 | |
| Region - Logical Segment | | VM@ne-RegionA01 | |
| Region - Network | | 172.168.1.11 | 172.168.1.11/24 |

Figure 2-2. Post-Deployment Network Topology Viewed in NSX Manager



Deploy Parameters Tab: SDDC Manager

Enter the host name, IP address, and subnet mask of the SDDC Manager VM.

Table 2-20. SDDC Manager

| Parameter | Value |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SDDC Manager Host name | Enter a host name for the SDDC Manager VM. The specified host name must be registered with your DNS server for both forward and reverse resolution, and it must be resolvable from the Cloud Builder appliance. |
| SDDC Manager IP Address | Enter an IP address for the SDDC Manager VM. The IP address must be registered with your DNS server for both forward and reverse resolution, and must be part of the management VLAN. |
| Network Pool Name | Enter the network pool name for the management domain network pool. |
| Cloud Foundation Management Domain Name | Enter a name for the management domain. This name will appear in Inventory > Workload Domains in the SDDC Manager UI. |

Upload the Deployment Parameter Workbook and Complete Deployment

You upload the completed deployment parameter workbook to complete bring-up.

Procedure

- 1 In the Download Deployment Parameter Workbook section, click **Next**.
- 2 In the Complete Deployment Parameter Workbook section, click **Next**.
- 3 In the Upload File section, click **Select File**. Select the completed deployment parameter workbook and click **Open**.
- 4 After the file is uploaded, click **Next** to begin validation of the uploaded file. You can download or print the validation list.

The following audit tasks are performed and validation results are displayed on the UI.

| Task | Validation |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| JSON validation | Validates JSON correctness, syntax, null values, and missing fields or components |
| Host and IP DNS records | Validates forward and reverse lookup for all hosts in bring-up JSON. |
| ESXi Host Readiness | Validates SSH access and policy, NTP configuration and policy, DNS configuration, VMNIC availability, vSwitch availability, VM network portgroup, and VLAN check on each host. |
| vSAN Disk Availability | Validates that required disks for vSAN are available for use. |
| License Key Format | Validates format, validity, and expiry for ESX, vSAN, vCenter Server, and NSX-T license keys. |
| Password Validation | Validates specified passwords. Checks for minimum length, invalid characters, and format. |
| Network Configuration | Validates CIDR to IP address validity, IP addresses in use, gateways, invalid or missing VLANs, invalid or missing MTU, IP pools, and network spec availability for all components. |
| Network Connectivity | Validates that the vSAN and vMotion VLANs, MTUs, and gateways specified in the deployment parameter workbook are correctly configured. |
| Time Synchronization | Validates NTP configuration for all ESX hosts. |
| Network IP Pools | Validates the following: <ul style="list-style-type: none"> ■ Pool defines enough IP addresses such that there is one IP address available for each host used for bring-up. ■ Start and end of IP inclusion pools are within the subnet specified for vSAN and vMotion. ■ IP addresses provided in inclusion pool are not in use. |
| Cloud Builder Readiness | Validates that Cloud Builder appliance has the correct NTP and DNS configuration. |
| ESXi Host Version | Validates ESXi version installed on the hosts and compares against the VCF-EMS manifest located in <code>/opt/evosddc/bundle/scripts/manifest.json</code> on the Cloud Builder appliance. |

To access the bring-up log file, SSH to the VMware Cloud Builder appliance as root and open the `/opt/vmware/bringup/logs/vcf-bringup-debug.log` file.

If there is an error during the validation and the Next button is grayed out, you can either make corrections to the environment or edit the JSON file and upload it again. Then click **Re-Try** to perform the validation again.

If any warnings are displayed and you want to proceed, click **Acknowledge** and then click **Next**.

5 Click **Deploy SDDC**.

During the bring-up process, the following tasks are completed.

- vCenter Server, vSAN, and NSX-T components are deployed.
- The management domain is created, which contains the management components - SDDC Manager, vCenter Server, and NSX-T components.

The status of the bring-up tasks is displayed in the UI.

After bring-up is completed, a green bar is displayed indicating that bring-up was successful. A link to the SDDC Manager UI is also displayed.

If there are errors during bring-up, see [Chapter 3 Troubleshooting Cloud Foundation Deployment](#) for guidance on how to proceed.

6 Click **Download** to download a detailed deployment report. This report includes information on assigned IP addresses and networks that were configured in your environment.

7 After bring-up is completed, click **Finish**.

8 In the SDDC Deployment Completed dialog box, click **Launch SDDC Manager**.

9 Verify the following:

- View management domain details.
- Log in to vCenter Server and verify the management cluster, vSAN cluster, and deployed VMs.

10 Power off the VMware Cloud Builder appliance.

The VMware Cloud Builder appliance includes the VMware Imaging Appliance service, which you can use to install ESXi on additional servers after bring-up is complete. You can delete the VMware Cloud Builder appliance to reclaim its resources or keep it available for future server imaging.

Caution Do not modify or delete any vDS or port groups, or modify the default configuration.

Troubleshooting Cloud Foundation Deployment

3

You can run the SoS tool and review bring-up log files to troubleshoot deployment issues.

This chapter includes the following topics:

- [SoS Tool Options for Cloud Builder appliance](#)
- [Cloud Builder Appliance Log Files](#)

SoS Tool Options for Cloud Builder appliance

You can run SoS tool operations in the VMware Cloud Builder appliance to debug a failed bring-up of Cloud Foundation.

Note After a successful bring-up, run the SoS tool only through SDDC Manager. See [Supportability and Serviceability \(SoS\) Tool](#) in the *VMware Cloud Foundation Operations and Administration Guide*.

To run the SoS utility in Cloud Builder appliance, SSH in to the VMware Cloud Builder appliance using the **admin** administrative account, then enter **su** to switch to the root user, and navigate to the `/opt/vmware/sddc-support` directory and type `./sos` followed by the options required for your desired operation.

```
./sos --option-1 --option-2 ... --option-n
```

SoS Tool Help Options

Use these options to see information about the SoS tool itself.

| Option | Description |
|-------------------------------------------|------------------------------------------------------|
| <code>--help</code> <code>-h</code> | Provides a summary of the available SoS tool options |
| <code>--version</code> <code>-v</code> | Provides the SoS tool's version number. |

SoS Tool Generic Options

These are generic options for the SoS tool.

| Option | Description |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>--configure-sftp</code> | Configures SFTP for logs. |
| <code>--debug-mode</code> | Runs the SoS tool in debug mode. |
| <code>--force</code> | Allows SoS operations from the VMware Cloud Builder appliance after bring-up. Note It is recommended that you do not use this option. |
| <code>--history</code> | Displays the last twenty SoS operations performed. |
| <code>--log-dir LOGDIR</code> | Specifies the directory to store the logs. |
| <code>--log-folder LOGFOLDER</code> | Specifies the name of the log directory. |
| <code>--setup-json SETUP_JSON</code> | Custom setup-json file for log collection. SoS prepares the inventory automatically based on the environment where it is running. If you want to collect logs for a pre-defined set of components, you can create a <code>setup.json</code> file and pass the file as input to SoS. A sample JSON file is available on the Cloud Builder appliance in the <code>/opt/vmware/sddc-support/</code> directory. |
| <code>--skip-known-host-check</code> | Skips the specified check for SSL thumbprint for host in the known host. |
| <code>--zip</code> | Creates a zipped tar file for the output. |

SoS Tool Options for JSON Generator

| Option | Description |
|---------------------------------------------------------------|------------------------------------------------------------------|
| <code>--jsongenerator</code> | Invokes the JSON generator utility. |
| <code>--jsongenerator-input JSON_GENERATOR_INPUT</code> | Specify the input file to be used by the JSON generator utility. |
| <code>--jsongenerator-design JSON_GENERATOR_DESIGN</code> | Specify the design file for the SDDC architecture. |
| <code>--jsongenerator-supress</code> | Supress confirmation to force cleanup directory. |
| <code>--jsongenerator-logs JSONGENERATORLOGS</code> | Set the directory to be used for logs. Optional. |

SoS Tool Options for Platform Audit

| Option | Description |
|-----------------------------------------|------------------------------------------------------------------|
| <code>--platformaudit</code> | Invokes the platform audit operation. |
| <code>--platformaudit-dependency</code> | Executes audit tests with dependencies. |
| <code>--platformaudit-input FILE</code> | Specify the input file to be used by the platform audit utility. |
| <code>--platformaudit-kill</code> | Stops all running platform audit processes. |

| Option | Description |
|------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| <code>--platformaudit-modules</code> <i>MODULE1,MODULE2,MODULE3</i> | Specify the specific audit tests to run. If specifying multiple tests, separate the modules with commas. |
| <code>--platformaudit-output</code> <i>OUTPUT</i> | Saves the output to the specified file. |
| <code>--platformaudit-reason</code> | Outputs reasons for failed or skipped tests. |
| <code>--platformaudit-tree</code> | Displays a list of available audit tests. |

SoS Tool Options for Health Check

These SoS commands are used for checking the health status of various components or services, including connectivity, compute, and storage.

| Option | Description |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>--certificate-health</code> | Verifies that the component certificates are valid (within the expiry date). |
| <code>--connectivity-health</code> | Performs a connectivity health check to inspect whether the different components of the system such as the ESXi hosts, vCenter Servers, NSX Manager VMs, and SDDC Manager VM can be pinged. |
| <code>--compute-health</code> | Performs a compute health check. |
| <code>--general-health</code> | Verifies ESXi entries across all sources, checks the Postgres DB operational status for hosts, checks ESXi for error dumps, and gets NSX Manager and cluster status. |
| <code>--get-host-ips</code> | Returns server information. |
| <code>--health-check</code> | Performs all available health checks. |
| <code>--ntp-health</code> | Verifies whether the time on the components is synchronized with the NTP server in the VMware Cloud Builder appliance. |
| <code>--services-health</code> | Performs a services health check to confirm whether services are running |
| <code>--run-vsan-checks</code> | Runs proactive vSAN tests to verify the ability to create VMs within the vSAN disks. |

SoS Tool Log File Options

| Option | Description |
|-----------------------------------|----------------------------------------------------------------------------------------------------------------|
| <code>--api-logs</code> | Collects output from APIs. |
| <code>--cloud-builder-logs</code> | Collects Cloud Builder logs. |
| <code>--esx-logs</code> | Collects logs from the ESXi hosts only. Logs are collected from each ESXi host available in the deployment. |

| Option | Description |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>--no-clean-old-logs</code> | Use this option to prevent the tool from removing any output from a previous collection run. By default, before writing the output to the directory, the tool deletes the prior run's output files that might be present. If you want to retain the older output files, specify this option. |
| <code>--no-health-check</code> | Skips the health check executed as part of log collection. |
| <code>--nsx-logs</code> | Collects logs from the NSX Manager instances only. |
| <code>--rvc-logs</code> | Collects logs from the Ruby vSphere Console (RVC) only. RVC is an interface for ESXi and vCenter. Note If the Bash shell is not enabled in vCenter, RVC log collection will be skipped . Note RVC logs are not collected by default with <code>./sos log</code> collection. |
| <code>--sddc-manager-logs</code> | Collects logs from the SDDC Manager only. |
| <code>--test</code> | Collects test logs by verifying the files. |
| <code>--vc-logs</code> | Collects logs from the vCenter Server instances only. Logs are collected from each vCenter server available in the deployment. |
| <code>--vm-screenshots</code> | Collects screen shots from all VMs. |

Sample Output

The following text is a sample output from an `--ntp-health` operation.

```
root@cloud-builder [ /opt/vmware/sddc-support ]# ./sos --ntp-health --skip-known-host --force
Welcome to Supportability and Serviceability(SoS) utility!
```

```
User passed --force flag, Running SOS from Cloud Builder VM, although Bringup is completed
and SDDC Manager is available. Please expect failures with SoS operations.
```

```
Health Check : /var/log/vmware/vcf/sddc-support/healthcheck-2020-02-11-23-03-53-24681
```

```
Health Check log : /var/log/vmware/vcf/sddc-support/healthcheck-2020-02-11-23-03-53-24681/
sos.log
```

```
SDDC Manager : sddc-manager.vrack.vsphere.local
```

```
NTP : GREEN
```

```
+-----+-----+-----+-----+
| SL# |           Area           | Title   | State |
+-----+-----+-----+-----+
| 1 | ESXi : esxi-1.vrack.vsphere.local | ESX Time | GREEN |
| 2 | ESXi : esxi-2.vrack.vsphere.local | ESX Time | GREEN |
| 3 | ESXi : esxi-3.vrack.vsphere.local | ESX Time | GREEN |
| 4 | ESXi : esxi-4.vrack.vsphere.local | ESX Time | GREEN |
| 5 | vCenter : vcenter-1.vrack.vsphere.local | NTP Status | GREEN |
+-----+-----+-----+-----+
```

```
Legend:
```

```

GREEN - No attention required, health status is NORMAL
YELLOW - May require attention, health status is WARNING
RED - Requires immediate attention, health status is CRITICAL

```

```
Health Check completed successfully for : [NTP-CHECK]
```

The following text is sample output from a `--vm-screenshots` log collection operation.

```

root@cloud-builder [ /opt/vmware/sddc-support ]# ./sos --vm-screenshots
--skip-known-host --force
Welcome to Supportability and Serviceability(SoS) utility!

User passed --force flag, Running SOS from Cloud Builder VM, although Bringup is completed
and SDDC Manager is available. Please expect failures with SoS operations.
Logs : /var/log/vmware/vcf/sddc-support/sos-2018-08-24-10-50-20-8013
Log file : /var/log/vmware/vcf/sddc-support/sos-2018-08-24-10-50-20-8013/sos.log
Log Collection completed successfully for : [VMS_SCREENSHOT]

```

Cloud Builder Appliance Log Files

The VMware Cloud Builder appliance contains various log files for different components of the system. The following table describes the important log files that can be used for troubleshooting.

| Component | Log Name | Location |
|-----------------|---------------------------------|-------------------------------------------------------------------|
| JsonGenerator | <i>jsongenerator-timestamp</i> | <i>/var/log/vmware/vcf/sddc-support/</i> |
| PlatformAudit | <i>platform-audit-timestamp</i> | <i>/var/log/vmware/vcf/sddc-support/</i> |
| Bringup Service | <i>vcf-bringup.log</i> | <i>/var/log/vmware/vcf/bringup/</i> |
| | <i>vcf-bringup-debug.log</i> | <i>/var/log/vmware/vcf/bringup/</i> |
| | <i>rest-api-debug.log</i> | <i>/var/log/vmware/vcf/bringup/</i> |
| SoS | <i>sos.log</i> | <i>/var/log/vmware/vcf/sddc-support/</i> <i>sos-timestamp/</i> |

Cloud Foundation Glossary

4

| Term | Description |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| availability zone | Collection of infrastructure components. Each availability zone is isolated from other availability zones to prevent the propagation of failure or outage across the data center. |
| Application virtual networks (AVNs) | Virtual networks backed by overlay segments using the encapsulation protocol of NSX-T. Virtual Networks use a single IP network address space, to span across data centers. |
| bring-up | Initial configuration of a newly deployed Cloud Foundation system. During the bring-up process, the management domain is created and the Cloud Foundation software stack is deployed on the management domain. |
| cluster image | Precise description of the software, components, vendor add-ons, and firmware to run on a host. With this new functionality, you set up a single image and apply it to all hosts in a cluster, thus ensuring cluster-wide host image homogeneity. |
| commission host | Adding a host to Cloud Foundation inventory. The host remains in the free pool until it is assigned to a workload domain. |
| composability | Ability to dynamically configure servers to meet the needs of your workloads without physically moving any hardware components. You bind disaggregated hardware components (compute, network, storage, and offload components) together to create a logical system based on the needs of your applications. |
| dirty host | A host that has been removed from a cluster in a workload domain. A dirty host cannot be assigned to another workload domain until it is cleaned up. |
| decommission host | Remove an unassigned host from the Cloud Foundation inventory. SDDC Manager does not manage decommissioned hosts. |
| Edge cluster | A logical grouping of Edge nodes. These nodes run on a vSphere cluster, and provide north-south routing and network services for the management and VI workload domains. |
| free pool | Hosts in the Cloud Foundation inventory that are not assigned to a workload domain |
| host | An imaged server. |
| inventory | Logical and physical entities managed by Cloud Foundation. |
| Kubernetes - Workload Management | With Kubernetes - Workload Management, you can deploy and operate the compute, networking, and storage infrastructure for vSphere with Kubernetes workloads. A vSphere with Kubernetes workload is an application with containers running inside vSphere pods, regular VMs, or Tanzu Kubernetes clusters. |
| Lifecycle Manager (LCM) | Automates patching and upgrading of the software stack. |

| Term | Description |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| management domain | Cluster of physical hosts that contains the management component VMs |
| network pool | Automatically assigns static IP addresses to vSAN and vMotion vmkernel ports so that you don't need to enter IP addresses manually when creating a VI workload domain or adding a host or cluster to a workload domain. |
| patch update bundle | Contains bits to update the appropriate Cloud Foundation software components in your management or VI workload domain. |
| region | A Cloud Foundation instance. |
| SDDC Manager | Software component that provisions, manages, and monitors the logical and physical resources of a Cloud Foundation system. |
| SDDC Manager VM | Virtual machine (VM) that contains the SDDC Manager services and a shell from which command line tools can be run. This VM exposes the SDDC Manager UI. |
| server | Bare metal server in a physical rack. After imaging, it is referred to as a host. |
| unassigned host | Host in the free pool that does not belong to a workload domain. |
| vSphere Lifecycle Manager (vLCM) | A vCenter service, which is now integrated with Cloud Foundation, that enables centralized and simplified lifecycle management of ESXi hosts. |
| workload domain | A policy based resource container with specific availability and performance attributes that combines vSphere, storage (vSAN, NFS, or VMFS on FC) and networking (NSX-T) into a single consumable entity. A workload domain can be created, expanded, and deleted as part of the SDDC lifecycle operations. It can contain cluster(s) of physical hosts with a corresponding vCenter to manage them. The vCenter for a workload domain physically lives in the management domain. |