Dell EMC VMware Cloud Foundation 4.0 for PowerEdge Rack Server

Deployment Guide

May 2020
Rev. A02

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

1

Audience and scope

This deployment guide includes step-by-step instructions for deployment of VMware Cloud Foundation (VCF) on Dell EMC PowerEdge RX740xd rack servers. Any deviation from the listed configurations may negatively impact functionality.

This deployment guide makes certain assumptions about the prerequisite knowledge of the deployment personnel. This includes the prerequisite knowledge of:

- Dell EMC products including the location of buttons, cables, and components in the hardware
- Functional knowledge of the items in the Dell EMC owner's manuals for the products being used
- VMware products and the components or features of VMware vSphere
- Data center infrastructure best practices in the areas of server, storage, networking, and environmental considerations such as power and cooling

The scope of this document excludes existing infrastructure components outside of the specific hardware and software that is mentioned in this guide. Dell EMC takes no responsibility for any issues that may be caused to existing infrastructure during deployment.

2

Overview

Deployment of VMware VCF on the PowerEdge R740xd platform provides a hyperconverged infrastructure solution incorporating best-in-class hardware from Dell EMC with core VMware products including vSphere, vSAN, NSX, vRealize Log Insight, and SDDC Manager. Virtualization of compute, storage, and networking is delivered on a single cluster of PowerEdge R740xd servers.

Dell EMC has determined the compatibility and established certification across hardware and software. The combination of VMware VCF software on the Dell EMC PowerEdge hardware that is described in this document has been validated in Dell EMC labs and certified by VMware. The PowerEdge R740xd systems that are described within are certified as vSAN and VCF Ready Nodes, as shown in the VMware Compatibility Guide (VCG).

Some of the key benefits of the PowerEdge server platform include:

- Dell EMC iDRAC9 provides a full-featured management console. iDRAC9 enables the configuration of all aspects of PowerEdge servers. Multiple license tiers are available but the example provided in this guide assumes that you have the Enterprise license.
- Powerful compute and storage capability in an economical 2U footprint
- Dell EMC Networking switches provide both throughput and reliability with minimum latency

NOTE: VCF builds a strong infrastructure foundation which you can expand with additional products. You can enable a true private cloud consumption model in your environment with optional add-on products from the VMware vRealize suite of software. For more information about these products, see www.vmware.com/products/vrealize-suite.html.

Deploying VCF includes several steps. The following figure lists the steps and their sequence, providing a high-level visualization of the overall deployment workflow.

In the figure and throughout the deployment process, the term SDDC bring-up refers to the software-defined data center (SDDC) which is built as the result of the steps documented in this guide.

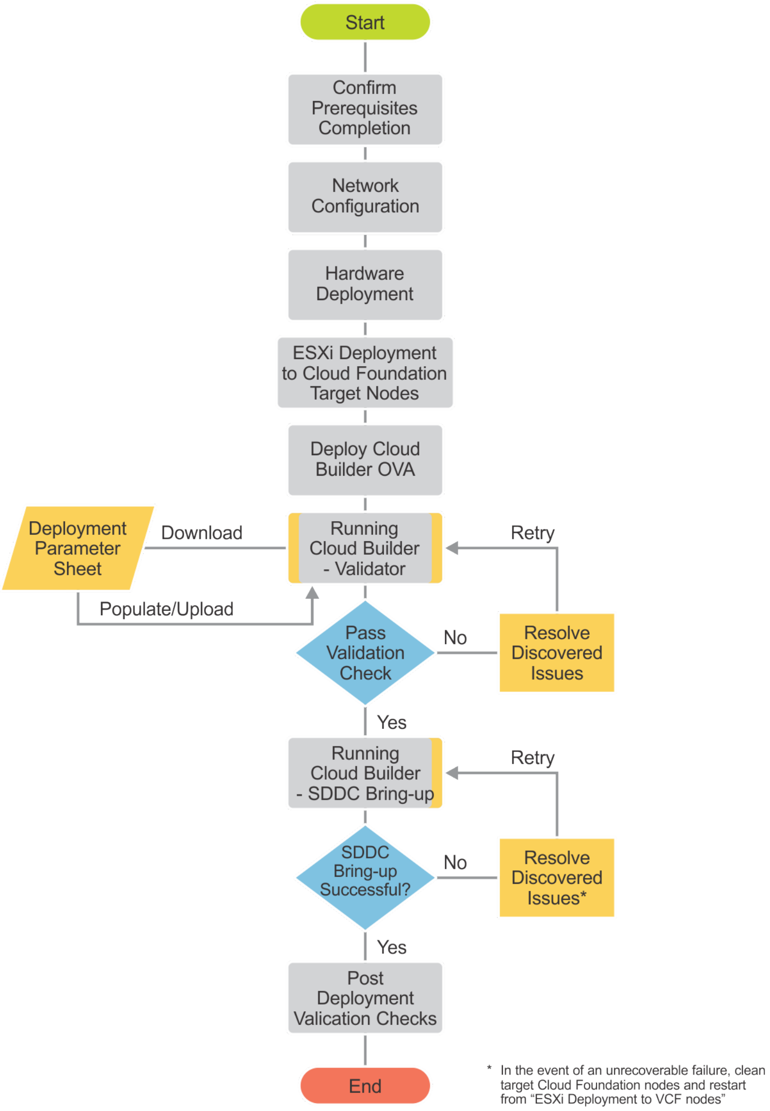

Start
Confirm Prerequisites Completion
Network Configuration
Hardware Deployment
ESXi Deployment to Cloud Foundation Target Nodes
Deploy Cloud Builder OVA
Deployment Parameter Sheet
Download
Running Cloud Builder - Validator
Retry
Populate/Upload
Pass Validation Check
No
Resolve Discovered Issues
Yes
Running Cloud Builder - SDDC Bring-up
Retry
SDDC Bring-up Successful?
No
Resolve Discovered Issues*
Yes
Post Deployment Valication Checks
End
* In the event of an unrecoverable failure, clean target Cloud Foundation nodes and restart from "ESXi Deployment to VCF nodes"

Figure 1. VCF workflow diagram

3

Pre-deployment requirements

Management host

The deployment of VMware Cloud Foundation is executed by a Cloud Builder VM that is deployed using an Open Virtualization Appliance (OVA). The virtual machine must be deployed on an ESXi host or cluster that is not a part of the Cloud Foundation cluster. If the management network is a private network ensure that the Cloud Builder VM and the Cloud Foundation management hosts have access to the same DNS and NTP services.

In this example, a host in an existing vSphere environment is used to run the services that are required to install Cloud Foundation. The management VLAN and VXLAN VLAN are extended to this management host. An NTP time server is installed on the management VLAN and a DHCP server on the VXLAN VLAN.

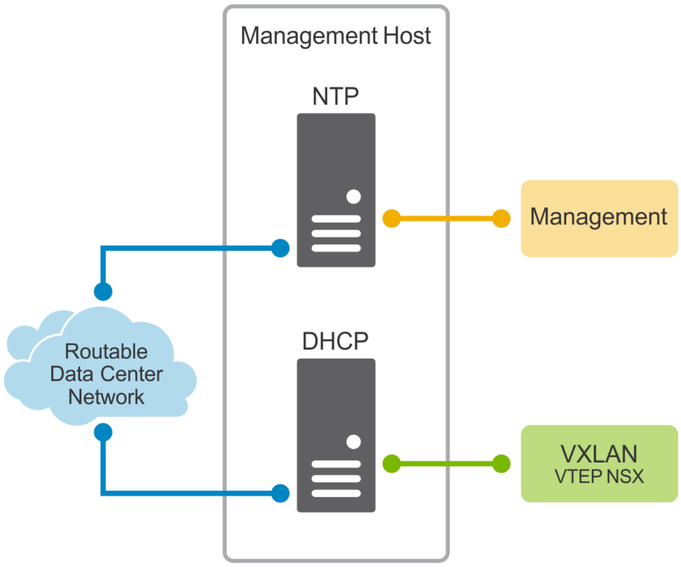


Figure 2. Management host in an existing vSphere environment

Connectivity

The Cloud Builder VM must be able to communicate with the hosts that become the Cloud Foundation management cluster. In this example, the new cluster hosts were given IP addresses on the 172.30.11.0/24 subnet and placed on the management VLAN (3011). A port group on the management host that was tagged with VLAN 3011 was created and connected to a port on a switch that accepted (ingress) traffic. The switchports between that initial ingress port and the new hosts were tagged with VLAN 3011.

Network services

There are three network services that are essential for Cloud Foundation deployment.

ⓘ **NOTE: Misconfiguration or lack of one of these services causes the validation portion of the installation to fail.**

The information pertaining to the network services are inserted into the Cloud Builder Deployment Parameter Sheet. The parameter sheet is a spreadsheet that contains the details of the deployment and information specific to these prerequisites.

Domain Name Service

Domain Name Service (DNS) is required to provide both forward and reverse name resolution. The IP addresses of name servers, search domains, and hostnames of all the VCF VMs must be inserted into the cloud builder deployment parameter sheet. Forward and reverse DNS entries of any hostname that are indicated in the parameter sheet should be tested and retested for both forward and reverse lookups. Test the DNS entries using their Fully Qualified Domain Name (FQDN) and their short name (hostname).

ⓘ NOTE: **Every DNS hostname and corresponding IP address that is specified in the parameter sheet are tested during the validation phase.**

Dynamic Host Configuration Protocol

The Dynamic Host Configuration Protocol (DHCP) provides network addresses to the VXLAN tunnel end points (VTEP). A VTEP is a software-based endpoint of a VXLAN connection that communicates over these IP addresses and are on the same Layer 2 network. An address pool large enough to provide an address to every host connection on the VXLAN network--one address per NIC per host--is required.

ⓘ NOTE: **Software-based VTEPs could transition to hardware-based VTEPs with the launch of new features included in future switch operating systems.**

Whenever a new cluster node is added to the Cloud Foundation, a new VTEP is created which requires DHCP to obtain IP addressing information. The DHCP service is not only a prerequisite for deployment but an ongoing requirement as well. Place the DHCP server (or VM) on a reliable and well-maintained part of your infrastructure.

The validation process checks to ensure that DHCP is available on the VXLAN network that is specified in the parameter sheet. Validation fails if there is no positive DHCP response on the VXLAN network.

Network Time Protocol

Time synchronization is critical to the Cloud Foundation stack. All hosts and the Cloud Builder VM are synchronized to a reference time source before attempting to run the validation phase of the Cloud Builder process. Network Time Protocol (NTP) traffic is routed from client to source or it can travel over the same L2 network.

Validated components

Validated components refer to the hardware components, and the software and firmware versions that have been validated. VMware no longer maintains the VMware Compatibility Guide (VCG) for Cloud Foundation. Since VSAN is an underlying requirement of Cloud Foundation, any hardware that is specified as a vSAN Ready Node is approved for Cloud Foundation.

Topics:

Hardware components

The following hardware components were used in the validation of this solution.

NOTE: VCF automatically configures vSAN disk groups, which requires following a few rules for drive population:

- **Identical drive configurations in each target host**
- **There must be one size for all cache drives, as well as one size for all capacity drives**
- **The number of capacity drives in a host is cleanly divisible by the number of cache drives (that is, the result is a whole number)**

Table 1. Hardware components

Manufacturer	Model	Description	Specifications
Dell EMC	PowerEdge R740xd	Cluster hosts	2x Xeon Gold processor, 256 GB 2x Xeon Gold processor, 256 GB RAM, Cache drives and Capacity drives as per the VSAN VCG. This server was selected as an example device for the purpose of this documentation.
Dell EMC	Broadcom 57414 10/25GbE rNDC Broadcom 57414S 10/25GbE NIC	NIC to support connectivity to chosen top-of-rack switches	Need to match speed and form factor of upstream switch ports
Dell EMC	PowerConnect S5248F-ON	Top-of-rack switches selected as an example for this document.	Any top-of-rack switch can be used. These switches were selected as an example device supporting VLT and operating system version 10.

Software and firmware

NOTE: The VMware Compatibility Guide (VCG) is the system of record for versions of certain types of firmware and drivers which are certified to be compatible with vSphere and vSAN. These include server platform, vSAN disk controllers, and network interface cards. For more information about other components, see https://www.dell.com/support.

Software

This document was written for Dell EMC VMware Cloud Foundation 4 running on ESXi 7. The exact version and build of ESXi is specified by the version of Cloud Foundation being installed. It is critical to identify and install the corresponding Cloud Foundation and ESXi versions.

Hardware overview

This section provides additional information about the hardware platform used in the development of this deployment guide.

Topics:

- Dell EMC PowerEdge R740xd server
- Dell EMC Networking S5248F-ON Switch

Dell EMC PowerEdge R740xd server

The PowerEdge R740xd server provides the benefit of scalable storage performance and data set processing. This 2U, 2-socket platform brings you scalability and performance to adapt to a variety of applications. You can choose up to 24 NVMe drives, or a total of 32 x 2.5", or 18 x 3.5" drives. As you scale your deployments, scale your productivity with embedded intelligence and automation from iDRAC9 and the entire OpenManage portfolio that is designed to simplify the IT lifecycle from deployment to retirement.

- 24 DIMM slots of DDR4 memory (RDIMM or LRDIMM)
- Up to 24 SAS or SATA SSD or hard drive and NVMe PCIe SSDs
- Boot device options such as BOSS-S1
- 4 x 1GE or 2 x 10GE + 2 x 1GE or 4 x 10GE or 2 x 25GE

Front view of the PowerEdge R740xd server

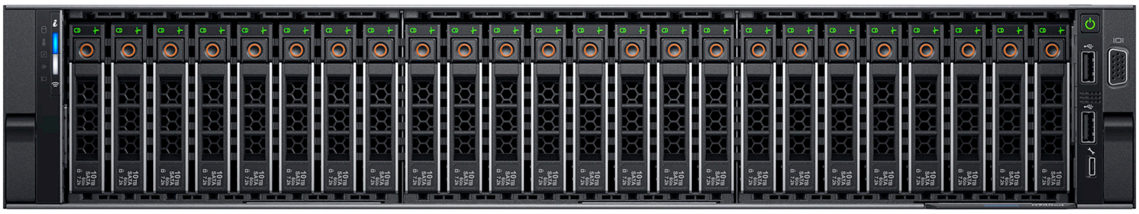


Figure 3. PowerEdge R740xd server—front view

Back view of the PowerEdge R740xd server

Figure 4. PowerEdge R740xd server—back view

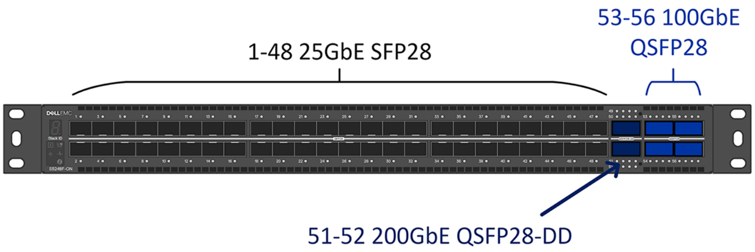
Dell EMC Networking S5248F-ON Switch

The Dell EMC Networking S4048-ON Switch is a high-performance, low latency 10 GbE switch designed for flexibility and high performance for today's demanding modern workloads and applications. This switch supports both Virtual Link Trunking (VLT) and OS10 making it a good example of switches that can be used at the top of the rack. In addition to 48 10 GbE ports, the S4048-ON provides:

- 48 10 GbE SFP+ ports
- Six 40 GbE QSFP+ ports

The QSFP28 or QSFP28-DD ports can be used for Ethernet uplink connectivity. For more information, see the Management host section. The SFP28 ports can be used for connections to both Cloud Foundation management and Cloud Foundation workload domains.

Figure 5. Dell EMC Networking S5248F-ON Switch



6

Physical layout

The configuration of Cloud Foundation on PowerEdge R740xd is described in this document. The Cloud Foundation software addresses the host servers using their IP Address. The physical layout and resulting cabling are determined by the number of R740xd servers and the number of available ports on the top-of-rack switches. Cloud Foundation 4.0 incorporates NSX-T where the 3.x versions of Cloud Foundation incorporate NSX. The move from NSX to NSX-T has an impact on the network topology. The NSX-T Edge Nodes should use a standard LACP LAG where the VSAN, VMotion, VRealize, and Management networks can share the same MLAG if wanted.

Topics:

Management Host Network Cabling

The configuration for the management cluster of a Cloud Foundation deployment includes:

- Four Dell EMC PowerEdge R740xd servers
- Two Dell EMC Networking S5248F-ON switches (sample data switch)
- One Dell EMC Networking 3048 switch (sample out of band management switch)

Each management host in the management domain has four connections to their Top of Rack (leaf) switches. The Connections can be either 10 GbE or 25 GbE, in this example the connections are all 25 GbE. Each NIC in each host should have one port that is connected to each top of rack switch to ensure redundancy.

These connections should not be aggregated in any way. The ESXi 7.0 hypervisor should be allowed to manage these connections. This diagram shows the distribution of ports across both of the top of rack switches.

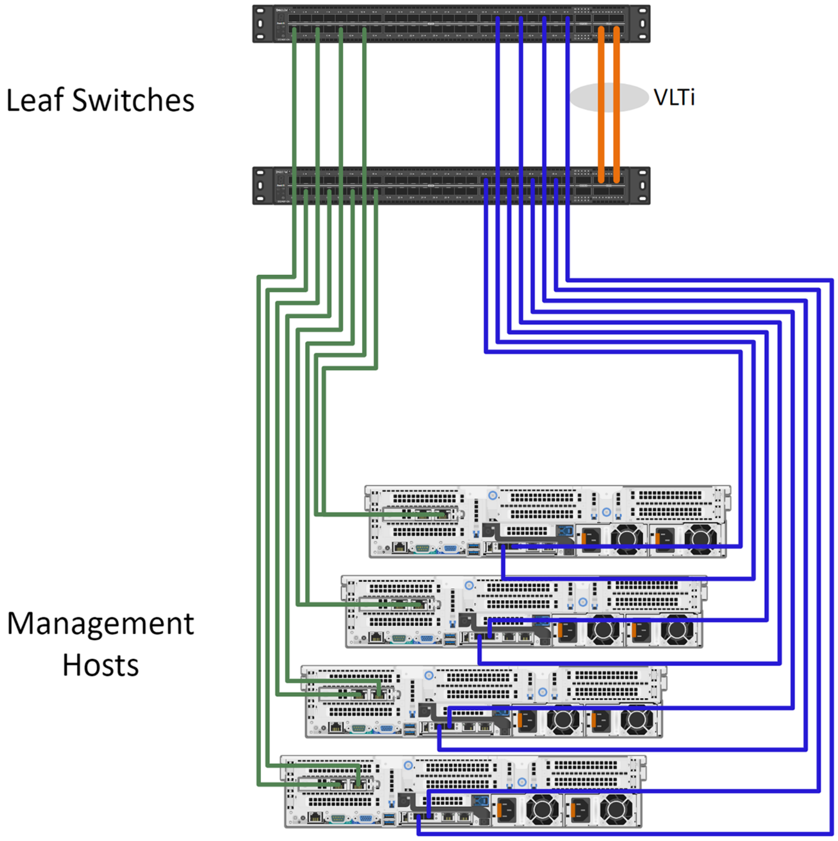


Figure 6. Management Host Network Cabling

Top of Rack Connectivity to Spine

The uplinks from the Top of Rack Leaf switches include separate uplinks for support of NSX-T edge node networking. To accommodate all the connections, we can utilize ports 51 and 52 on the S5248F-ON switches. These ports are 200GbE Double Density ports. Utilizing the Dell EMC DAC-Q28DD-2Q28-100G cables the 200GbE ports can be broken out into two 100GbE QSFP connections

This diagram shows a conceptual view of the different uplinks from the top of rack switches to the spine. The MLAG is a VLT port channel that includes connections from both top of rack switches to multiple devices in the spine layer. The two NSX-T LAG connections are standard LACP link aggregations which will connect the NSX-T edge nodes back to the spine layer. The connections shown are for conceptual illustration purposes only and are not accurate to any specific model of switch.

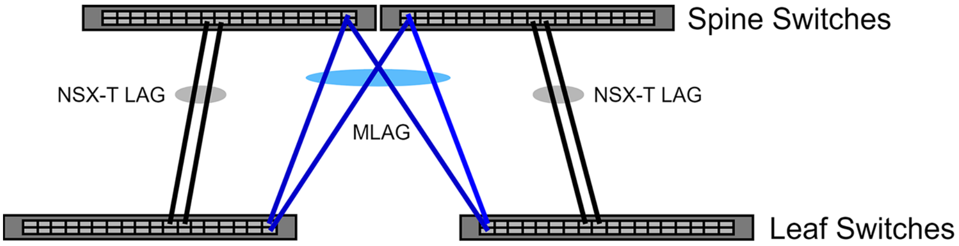


Figure 7. Top of rack connectivity

Out of Band Management Connectivity

While the Out of Band management network is not used by VCF, it is worth noting that a flat network running on a Dell EMC Networking S3048-ON switch was used to help with the remote configuration and deployment of switches and servers.

7

VCF and SDDC design considerations

VMware Cloud Foundation relies on a set of key infrastructure services to be made available externally. You must configure these external services before you begin deployment.

NOTE: This section is universal for VCF deployments regardless of hardware platform. The content in this section is also available in the VMware Cloud Foundation Planning and Preparation Guide, and is included here for reference. The original content in the VMware website includes additional sections which are not in the scope of this document.

Topics:

External services overview

Many external services are required for the initial deployment of Cloud Foundation and for the deployment of other optional components such as vRealize Operations or vRealize Automation. The following table lists the required and optional external services and dependencies:

Table 2. Required and optional external services and dependencies

Service	Purpose
Active Directory (AD)	(Optional) Provides authentication and authorization. **NOTE: AD is required if you are deploying vRealize Automation.**
Dynamic Host Configuration Protocol (DHCP)	Provides automated IP address allocation for VXLAN Tunnel Endpoints (VTEPs).
Domain Name Service (DNS)	Provides name resolution for the various components in the solution.
Network Time Protocol (NTP)	Synchronizes time between the various components.
Simple Message Transfer Protocol (SMTP)	(Optional) Provides method for email alerts.
Certificate Authority (CA)	(Optional) Allows replacement of the initial self-signed certificates that are used by Cloud Foundation. **NOTE: A CA is required if you are deploying vRealize Automation.**

Active Directory

Cloud Foundation uses Active Directory (AD) for authentication and authorization to resources. The Active Directory services must be reachable by the components that are connected to the management and vRealize networks.

You must configure user and group accounts in AD before adding them to the SDDC manager and assigning privileges.

NOTE: If you plan to deploy vRealize Automation, Active Directory services must be available. For more information on AD configuration, see the vRealize Automation documentation.

Dynamic Host Configuration Protocol

Cloud Foundation uses Dynamic Host Configuration Protocol (DHCP) to automatically configure each VM kernel port of an ESXi host that is used as a VTEP with an IPv4 address. One DHCP scope must be defined and made available for this purpose.

The DHCP scope that is defined must be large enough to accommodate all the initial and future servers that are used in the Cloud Foundation solution. Each host requires two IP addresses, one for each VTEP configured.

Domain Name System

During deployment, you must provide the DNS domain information to be used to configure the various components. The root DNS domain information is required and, optionally, you can also specify subdomain information.

DNS resolution must be available for all the components that are contained within the Cloud Foundation solution, which includes servers, virtual machines, and any virtual IPs that are used. For more information on the components that are required for DNS resolution before starting a Cloud Foundation deployment, see Host names and IP addresses.

Ensure that both forward and reverse DNS resolutions are functional for each component before deploying Cloud Foundation or creating any workload domains.

Network Time Protocol

All components must be synchronized against a common time by using the Network Time Protocol (NTP) on all nodes. Important components of Cloud Foundation, such as vCenter Single Sign-On (SSO), are sensitive to a time drift between distributed components. Synchronized time between the Cloud Builder appliance VM and the Cloud Foundation components is required and the deployment fails if they are not synchronized to the same time source.

If you identify your time sources as IP addresses when you configure Cloud Builder, then you should specify those same IP addresses in your deployment parameter file. Similarly, if you specify by DNS name(s) then you should specify the same DNS name(s) in the parameter file.

Requirements for the NTP sources include the following:

- The IP addresses of two NTP sources are provided during the initial deployment.
- The NTP sources must be reachable by all the components in the Cloud Foundation solution.
- Time skew is less than 5 minutes between NTP sources.

Simple Mail Transfer Protocol mail relay (optional)

Certain components of the SDDC, such as vCenter, Log Insight, and vRealize Automation, can send status messages to users by email. To enable this functionality, a mail relay that does not require user authentication must be available through SMTP. As a best practice, limit the relay function to the networks allocated for use by Cloud Foundation.

Certificate Authority (optional)

The components of the SDDC require SSL certificates for secure operation. During deployment, self-signed certificates are used for each of the deployed components. These certificates can be replaced with certificates that are signed by an internal enterprise CA or by a third-party commercial CA.

Physical network requirements

Before deploying Cloud Foundation, configure the physical network to enable the following features:

- VLAN Tagging (802.1Q)
- Jumbo frames
  - A minimum MTU value of 9000 is required.

Network pools

Cloud Foundation uses a construct that is called a network pool to automatically configure VM kernel ports for vSAN, NFS, and vMotion.

Cloud Foundation uses an Internet Protocol Address Management (IPAM) solution to automate the IP configuration of VM kernel ports for vMotion, vSAN, and NFS (depending on the storage type being used).

When a server is added to the inventory of Cloud Foundation, it goes through a process called host commissioning. During this process, the hosts are associated with an existing network pool. When the host is provisioned during the create VI workload domain, add cluster, or add host workflow, it automatically configures the VMkernel ports and allocates IP addresses for vMotion, vSAN, and NFS from the network pool the host was associated with.

You can expand the included IP address range of a network pool at any time, however you cannot modify the other network information. Ensure that you have defined each subnet in the network pool to account for current and future growth in your environment.

VLANs and IP subnets

Network traffic types within Cloud Foundation are isolated from each other by using VLANs. Before deploying your SDDC, you must allocate VLAN IDs and IP subnets for each required traffic type. Configure the VLAN IDs and IP subnets in your network to pass traffic through your network devices. Before you start the Cloud Foundation deployment, verify that the allocated network information is configured and does not conflict with pre-existing services.

The number and size of the subnets that are required for a deployment depends on:

- The number of workload domains that are created
- The number of clusters defined
- The optional components that are installed

The following table lists the basic allocation of VLANs and IP subnets for a sample deployment.

Table 3. VLANs and IP subnets for a sample deployment

Domain	Cluster	VLAN Function	VLAN ID	Subnet	Gateway
Management	Cluster-01	Management	1811	172.18.11.0/24	172.18.11.1
		vMotion	1812	172.18.12.0/24172.18.13.0/24	172.18.12.1
		VSAN	1813	172.18.13.0/24	172.18.13.1
		VxLAN	1814	172.18.14.0/24	172.18.14.1
		vRealize Suite	1815	172.18.15.0/24	172.18.15.1
		NSX 1	2711	172.27.11.0/24	172.27.11.1
		NSX 2	2712	172.27.12.0/24	172.27.12.1

NOTE: Cloud Foundation deploys vRealize Suite products to a dedicated VLAN-backed vSphere Distributed Port Group. The IP subnet must be routable to the Cloud Foundation management network and the firewall. Also, the networks should be disabled or configured as prescribed in the Cloud Foundation documentation.

Host names and IP addresses

Before deploying a Cloud Foundation, or creating or expanding a workload domain, you must define the hostnames and IP addresses for various system components.

The defined hostnames and IP addresses need to exist in DNS and be resolvable, through forward and reverse lookups.

The required hostnames and IP addresses are categorized as follows:

- External services—services that are external to the Cloud Foundation solution and are required for proper operation.
- Virtual infrastructure layer—components that provide for the basic foundation of the Cloud Foundation solution.
- Operations management layer—components used for day-to-day management of the environment, for example, vRealize Operations.
- Cloud management layer—services that use the infrastructure layer resources, for example, vRealize Automation.

Host names and IP addresses for external services

External services such as Active Directory (AD) and NTP must be accessible and resolvable by IP Address and Fully Qualified Domain Name (FQDN). Acquire the hostnames and IP addresses for AD and NTP before deploying Cloud Foundation.

Allocate hostnames and IP addresses to the following components:

- NTP
- AD
- DNS
- Certificate Authority (CA)

The following table provides sample information for the external services. This example uses a DNS domain called `osevcf18.local` for illustration purposes only. Modify the sample information to conform to the configuration of your site.

Table 4. Configuration for external services

Component Group	Hostname	DNS	IP Address	Description
DNS	dc01sfo	sfo01.osevcf18.local	172.18.11.5	AD and DNS server for the sfo01 subdomain
NTP	Ntp	sfo01.osevcf18.local		Round-robin DNS pool containing the NTP servers
	0.ntp	sfo01.osevcf18.local	172.18.11.251	First NTP server
	1.ntp	sfo01.osevcf18.local	172.18.11.252	Second NTP server
AD, DNS or CA	dc01rpl	sfo01.osevcf18.local	172.18.11.4	Windows host that contains the AD configuration, the DNS

Host names and IP addresses for the virtual infrastructure layer

Most of the virtual infrastructure components that are installed by Cloud Foundation require their hostnames and IP addresses to be defined before deployment.

During the initial deployment of Cloud Foundation, the management domain is created and you must define components specific to the management domain before installation.

After the initial deployment, additional workload domains are created and you must define components specific to each additional workload domain.

Planning ahead for the initial deployment and the workload domains to be created avoids delays in deployment.

The following table provides an example of the information for the virtual infrastructure layer using the standard deployment model with a single workload domain. This example uses a DNS domain called `osevcf18.local` for illustration purposes. Modify the sample information to conform to the configuration of your site.

Table 5. Configuration for the virtual infrastructure layer

Workload Domain	Hostname	DNS Zone	IP Address	Description
Management	sddc-manager	osevcf18.local	100.71.101.7	SDDC Manager VM
	vcenter-m01-18	osevcf18.local	100.71.101.20	vCenter VM
	sddc18-m01-nsx01	osevcf18.local	100.71.101.31	NSX-T Management Cluster
	sddc18-m01-nsx02	osevcf18.local	100.71.101.32	NSX-T Virtual Appliance 1
	sddc18-m01-nsx03	osevcf18.local	100.71.101.33	NSX-T Virtual Appliance 2
	sddc18-m01-nsx04	osevcf18.local	100.71.101.34	NSX-T Virtual Appliance 3
	vcfmgmthost01	osevcf18.local	100.71.101.111	Management Host 1
	vcfmgmthost02	osevcf18.local	100.71.101.112	Management Host 2
	vcfmgmthost03	osevcf18.local	100.71.101.113	Management Host 3
	vcfmgmthost04	osevcf18.local	100.71.101.114	Management Host 4

8

Networking requirements

This section covers the networking requirements from both the Cloud Foundation software perspective and from a networking hardware connectivity perspective using the Dell EMC Networking S5248F-ON as an example.

Topics:

VMware Cloud Foundation networking

A successful VMware Cloud Foundation deployment relies heavily on networks that are constructed and allocated to Cloud Foundation. The networks are used by Cloud Builder during the installation and configuration process and then used by Cloud Foundation to carry out various activities. The different networks are allocated to specific purposes and have different requirements.

VMware Cloud Foundation requires six networks and at least one connection to a customer network (for external access to your Cloud Foundation stack). In the following example, a private IP address range is used for all connectivity within the management stack. There is also an IP network that connects back to an external network.

Each of these networks is propagated to the Cloud Foundation stack using tagged VLANs. Using tagged VLANs enables mapping of port groups to VLANs allowing access to resources as needed. All these networks are routable to and from each other. In this example, the routing task is executed at some layer above the access level switched fabric that is deployed here.

The networks required to deploy Cloud Foundation are listed in the following table:

Table 6. Networks required to deploy Cloud Foundation

Network	Description
Management	Dedicated to communication between all the deployed resources and services. When the SDDC Manager Utility needs to communicate to any other service or resource, it uses the management network.
vSAN	Used to communicate and synchronize vSAN storage traffic across multiple hosts to ensure data integrity and resiliency.
vMotion	Used to quickly redistribute virtual machine state and or storage between hosts.
VXLAN	VMware NSX uses VXLAN to extend NSX networking constructs from host to host. This network is sometimes referred to as the VTEP Network.
Uplink 1 and Uplink 2	VMware VCF uses these networks for northbound and southbound traffic when an NSX Edge Gateway is deployed.

Network connectivity

When deploying Dell EMC Networking S5248F-ON switches, the switches are configured as VLT peers. VLT enables the creation of a single link aggregation across two discrete switches. Two switches provide a redundant connection to each of the PowerEdge R740xd servers. The connection between the R740xd servers and the switches must not use any kind of link aggregation protocol. The connections are separate network connections that are managed by the Cloud Foundation stack.

The connections from the switches to the external network are implemented using both Virtual Link Trunking (VLT) link aggregation and standard LACP link aggregations. VLT allows you to create a single LACP-managed link aggregation from the two rack switches to an LACP-managed aggregation in the external network. The standard LACP link aggregations are used for NSX-T traffic so the VLT link aggregation will not carry the NSX underlay network. Use these link aggregation only on the links between the rack switches and the customer network.

Deploying Cloud Foundation on the R740xd servers and S5248F-ON switches follows the network connectivity as shown in Figure 6. Management Host Network Cabling.

Networking and NSX-T

Version 4.0 of Cloud Foundation changes to NSX-T from NSX or NSX-V in Cloud Foundation 3.9. The move to NSX-T drives changes in the physical and logical networking architecture. NSX-T introduces the concept of an Edge Node Cluster. An Edge Node Cluster is a resilient cluster of NSX-T edge nodes that are used to connect to upstream networks. All NSX traffic leaving the cluster passes through these edge nodes and the edge nodes rely on physical NICs.

Each member of an Edge Node Cluster contains identical configurations of physical NICs. This way, the NSX network constructs can fail over during a node failure. This diagram shows a conceptual view of the different uplinks from the top of rack switches to the spine. The MLAG is a VLT port channel that includes connections from both top of rack switches to multiple devices in the spine layer. The two NSX-T LAG connections are standard LACP link aggregations which connect the NSX-T edge nodes back to the spine layer. The connections that are shown are for conceptual illustration purposes only and are not accurate to any specific model of switch. If an MX7000 modular is deployed, the MX9116n IOMs are the Top or Rack or leaf switches. The connections shown in Figure 7. Top of rack connectivity are for conceptual illustration purposes only and are not accurate to any specific model of switch.

Manual switch configuration

This section describes the configurations that are made on the S5248F-ON switches. The configuration information includes two Dell EMC Networking S5248F-ON switches. These switches get the same configuration except for the hostname, IP address, the VLT Backup Destination IP Address and the NSX-specific uplink VLANs.

The management IP address of each switch was initially assigned using a serial console.

.

Topics:

VLANs and subnets for manual switch configuration

NOTE: Complete switch documentation is available from support.dell.com. Enter the service tag of your device to locate your device.

Here are the VLANs created on the S5248F-ON switch that is required for Cloud Foundation. These VLANs and subnets are created on both switches.

```
interface vlan1811
 description 1811-Mgmt
 no shutdown
 mtu 9216

interface vlan1812
 description 1812-VMotion
 no shutdown
 mtu 9216

interface vlan1813
 description 1813-VSAN
 no shutdown
 mtu 9216

interface vlan1814
 description 1814-VXLAN
 no shutdown
 mtu 9216

interface vlan1815
 description Log_Insight
 no shutdown
 mtu 9216
```

NOTE: All these VLANs are created on both Top of Rack switches (see Networking Requirements for more details).

NSX switch specific VLANs

These VLANs are switch-specific and should not be created on both switches. On the first switch, we create VLAN 2711 and on the second switch, create VLAN 2712 on the second switch.

On switch one:

```
interface vlan2711
 description 2711-NSX
 no shutdown
 mtu 9216
```

On switch two:

```
interface vlan2712
 description 2712-NSX
 no shutdown
 mtu 9216
```

NOTE: These VLANs are created on different Top of Rack switches.

Uplink and VLTi ports

VLT synchronizes Layer 2 table information between two switches and enables them to display as a single logical unit from outside the VLT domain. The VLT interconnect (VLTi) between two Dell EMC Networking S5248F-ON switches is a port group that is generated by configuring a VLT domain and specifying the discovery interfaces.

VLTi ports are specified during the configuration of the VLT domain by specifying the wanted interconnect ports as discovery interfaces. The resulting VLTi portgroup cannot be managed manually. The VLT domain would be created on both VLT peer switches.

Configure the ports for VLTi

The VLTi ports for this example are ethernet1/1/49 and 1/1/51. These ports are placed into a link aggregation by the VLT configuration process. Do not create the link aggregation manually.

To configure the ethernet1/1/49 and 1/1/51 ports, ensure that the:

- Ports are pre-configured correctly.
- Ports are set to the correct frame size.
- Ports are not set in any switchport (VLAN) mode.
- Ports are not shut down.

```
interface ethernet1/1/49
 no shutdown
 no switchport
 mtu 9216
 flowcontrol receive off
```

Configure VLT domain

The next step is to configure a VLT domain on each switch. It contains the exact same VLT domain on each switch. In this case, create a VLT domain '10' on each switch. The backup destination for the first switch is the management IPv4 address of the second switch. Similarly, the backup destination for the second switch is the management IPv4 address of the first switch. Ensure that the VLT domain is configured on each of the two switches.

```
S5248-bottom(config)#
S5248-bottom(config)# vlt-domain 10
S5248-bottom(conf-vlt-100)# discovery-interface ethernet1/1/49,1/1/51
S5248-bottom(conf-vlt-10)# backup destination 100.71.242.220
S5248-bottom(conf-vlt-10)# exit
```

Verify VLT settings

Verify the VLT settings by running the following command on each switch:

```
r10-24-s5248# show vlt 10
Domain ID                  : 10
Unit ID                    : 2
Role                       : secondary
Version                    : 2.3
Local System MAC address   : 3c:2c:30:80:a8:80
Role priority              : 32768
VLT MAC address            : aa:bb:cc:11:11:11
IP address                 : fda5:74c8:b79e:1::2
Delay-Restore timer        : 90 seconds
Peer-Routing               : Disabled
Peer-Routing-Timeout timer : 0 seconds
VLTi Link Status
    port-channel1000       : up

VLT Peer Unit ID    System MAC Address    Status    IP Address             Version
----------------------------------------------------------------------------------
  1                 3c:2c:30:80:aa:80      up       fda5:74c8:b79e:1::1     2.3
r10-24-s5248# show port-channel summary

Flags:  D - Down    I - member up but inactive    P - member up and active
        U - Up (port-channel)    F - Fallback Activated
--------------------------------------------------------------------------------
Group Port-Channel           Type     Protocol  Member Ports
--------------------------------------------------------------------------------
1    port-channel1    (D)     Eth      DYNAMIC   1/1/56(I)
1000 port-channel1000 (U)     Eth      STATIC    1/1/49(P) 1/1/51(P)
```

Verify the VLTi (port-channel)

To view the port channel summary, enter the following command on each switch:

```
r10-24-s5248#
r10-24-s5248# show port-channel summary

Flags:  D - Down    I - member up but inactive    P - member up and active
        U - Up (port-channel)    F - Fallback Activated
--------------------------------------------------------------------------------
Group Port-Channel           Type     Protocol  Member Ports
--------------------------------------------------------------------------------
1000 port-channel1000 (U)     Eth      STATIC    1/1/49(P) 1/1/51(P)
r10-24-s5248#
```

Configure Link Aggregation Control Protocol

After the VLT is enabled, create the uplinks to the network layer above the S5248F-ON switches. The connections will be a Link Aggregation Control Protocol (LACP) active link aggregation of two or more ports.

A VLT link aggregation is created by creating a VLT port-channel on each of the S5248F-ON switches. First create the uplink VLT port-channel on both switches and assign the appropriate VLANs.

Create a second LACP link aggregation, one on each switch, that are standard uplinks (not VLT uplinks). These links will only carry the NSX underlay and management VLANs.

Here are the port-channels created on switch one:

```
r10-24-s5248# show running-configuration interface port-channel 1
!
interface port-channel1
 description "Uplink to DataCenter"
 no shutdown
 switchport mode trunk
 switchport trunk allowed vlan 96,1811-1813,1815
 mtu 9216
 vlt-port-channel 1
r10-24-s5248# show running-configuration interface port-channel 11
!
interface port-channel11
 description NSX_Uplink_1
 no shutdown
 switchport mode trunk
 switchport trunk allowed vlan 2711,1814
 mtu 9216
r10-24-s5248# show port-channel summary

Flags:  D - Down    I - member up but inactive    P - member up and active
        U - Up (port-channel)    F - Fallback Activated
--------------------------------------------------------------------------------
Group Port-Channel           Type     Protocol  Member Ports
--------------------------------------------------------------------------------
1    port-channel1    (D)     Eth      DYNAMIC   1/1/56(I)
11   port-channel11   (U)     Eth      DYNAMIC   1/1/53(P) 1/1/54(P)
1000 port-channel1000 (U)     Eth      STATIC    1/1/49(P) 1/1/51(P)
r10-24-s5248#
```

Here are the port-channels created on switch two:

```
r10-25-s5248# show running-configuration interface port-channel 1
!
interface port-channel1
 description "Uplink to DataCenter"
 no shutdown
 switchport mode trunk
 switchport access vlan 1
 switchport trunk allowed vlan 96,1811-1813,1815
 mtu 9216
 vlt-port-channel 1
r10-25-s5248# show running-configuration interface port-channel 12
!
interface port-channel12
 description NSX_uplink_2
 no shutdown
 switchport mode trunk
 switchport trunk allowed vlan 2712,1814
 mtu 9216
r10-25-s5248# show port-channel summary

Flags:  D - Down    I - member up but inactive    P - member up and active
        U - Up (port-channel)    F - Fallback Activated
--------------------------------------------------------------------------------
Group Port-Channel           Type     Protocol  Member Ports
--------------------------------------------------------------------------------
1    port-channel1    (U)     Eth      DYNAMIC   1/1/56(P)
12   port-channel12   (U)     Eth      DYNAMIC   1/1/53(P) 1/1/54(P)
1000 port-channel1000 (U)     Eth      STATIC    1/1/49(P) 1/1/51(P)
r10-25-s5248#
```

Configure the host facing ports

To support multiple VLANs, you must place the server facing ports in trunk mode. All the VLANs assigned to the ports are tagged to allow the port groups to identify and direct traffic appropriately.

On switch one:

```
S5248-top(config)#
S5248-top(config)# interface range ethernet 1/1/1-1/1/16
S5248-top(conf-range-eth1/1/1-1/1/16)# switchport mode trunk
S5248-top(conf-range-eth1/1/1-1/1/16)# switchport trunk allowed vlan 96,1811-1815,2711
S5248-top(conf-range-eth1/1/1-1/1/16)# mtu 9216
S5248-top(conf-range-eth1/1/1-1/1/16)# no shutdown
S5248-top(conf-range-eth1/1/1-1/1/16)# exit
S5248-top(config)#
```

On switch two:

```
S5248-top(config)#
S5248-top(config)# interface range ethernet 1/1/1-1/1/16
S5248-top(conf-range-eth1/1/1-1/1/16)# switchport mode trunk
S5248-top(conf-range-eth1/1/1-1/1/16)# switchport trunk allowed vlan 96,1811-1815,2712
S5248-top(conf-range-eth1/1/1-1/1/16)# mtu 9216
S5248-top(conf-range-eth1/1/1-1/1/16)# no shutdown
S5248-top(conf-range-eth1/1/1-1/1/16)# exit
S5248-top(config)#
```

Save your switch configuration on each S4048-ON switch by running the following command:

```
ToR-Top-220#write mem
```

Verify switch configuration

The S5248F-ON switches are now configured with the minimum required settings to support the deployment of Cloud Foundation. Each of the following should now be configured:

- All required VLANs and subnets
- VLT Domain
- VLTi
- VLT Link Aggregations
- Link Aggregations
- Host facing ports

10

Deploy ESXi to cluster nodes

Perform the following steps to install VMware ESXi on each of the PowerEdge R740xd hosts that are part of the management cluster. This guide covers the steps to install VMware ESXi remotely using iDRAC Virtual Console with Virtual Media. In this example, a static IP address is assigned to the management interface of the ESXi hosts, which is required for Cloud Foundation.

ⓘ **NOTE: This guide assumes that the steps in this document are being followed comprehensively and sequentially. The tasks of previous sections are prerequisites for this section.**

Topics:

- Prerequisites
- Installation of ESXi

Prerequisites

The following items are required to complete this section of the deployment guide:

- iDRAC IP addresses or FQDNs
- iDRAC credentials
- iDRAC enterprise license that is applied on all nodes
- Dell EMC customized ESXi image
- Host names, Management VLAN ID, IP address information
- Credentials for vSphere
- Hostnames added to DNS server

Installation of ESXi

Complete the following steps on each physical compute node targeted for Cloud Foundation deployment before moving on to the next section.

Connect to iDRAC and boot installation media

- The virtual console should be in HTML5 mode, which is the default setting.
- The location of the Dell EMC customized ESXi image (ISO image) file should not be changed during the installation process.

1. Connect to the iDRAC web interface.
2. Log in with your credentials.

   ⓘ **NOTE: The default user name is `root` and the password is `calvin`.**

3. Click **Launch Virtual Console**, and then enable the support in the pop-up window for each iDRAC device.

   ⓘ **NOTE: When the virtual console is launched for the first time, repeating this step may be necessary due to browser pop-up blocker.**

   Figure 8. Virtual console preview

4. The mapping screen for the virtual media is displayed on the **Virtual Media** menu.
5. In the **Map CD/DVD** section, click **Choose File**.
6. Browse and select the required Dell EMC customized ESXi image (ISO image) file.
7. Click **Map Device** and then click **Close**.
8. From the **Virtual Console** menu, click **Boot**, and then click **Virtual CD/DVD/ISO**.
9. Click **Yes**.

10. From the **Power** menu, click **Power on System**.
11. If the system is not turned on, click **Power on System**. If the system is ON, click **Power Cycle System (cold boot)**.

The server is connected to the iDRAC devices and boots into the ESXi installer.

Install VMware ESXi

Before installing VMware ESXi, you must connect to the iDRAC devices and boot into the ESXi installer. For more information, see Connect to iDRAC and boot installation media.

1. In the **Welcome to ESXi Installation** window, press Enter.
2. Review the End User License Agreement (EULA), and then press F11 to accept and continue.
3. On the **Select a Disk to Install or Upgrade** page, select the **DELLBOSS VD** device, and then press Enter.

   NOTE: If DELLBOSS VD device has been used for previous ESXi installation, in the ESXi/VMFS Found dialog box, choose to overwrite the existing VMFS datastore, and then press Enter.

4. Select the required keyboard layout, and then press Enter.
5. Enter the root password, and then press Enter.
6. In the **Confirm Install** window, press F11 to install the VMware ESXi.
7. In the **Installation Complete** window, press Enter to reboot the server.
   The installation completes and the server boots into ESXi.
8. From the **Virtual Media** menu, click **Disconnect Virtual Media**.

VMware ESXi is installed in the server.

Configure ESXi settings using Direct Console User Interface

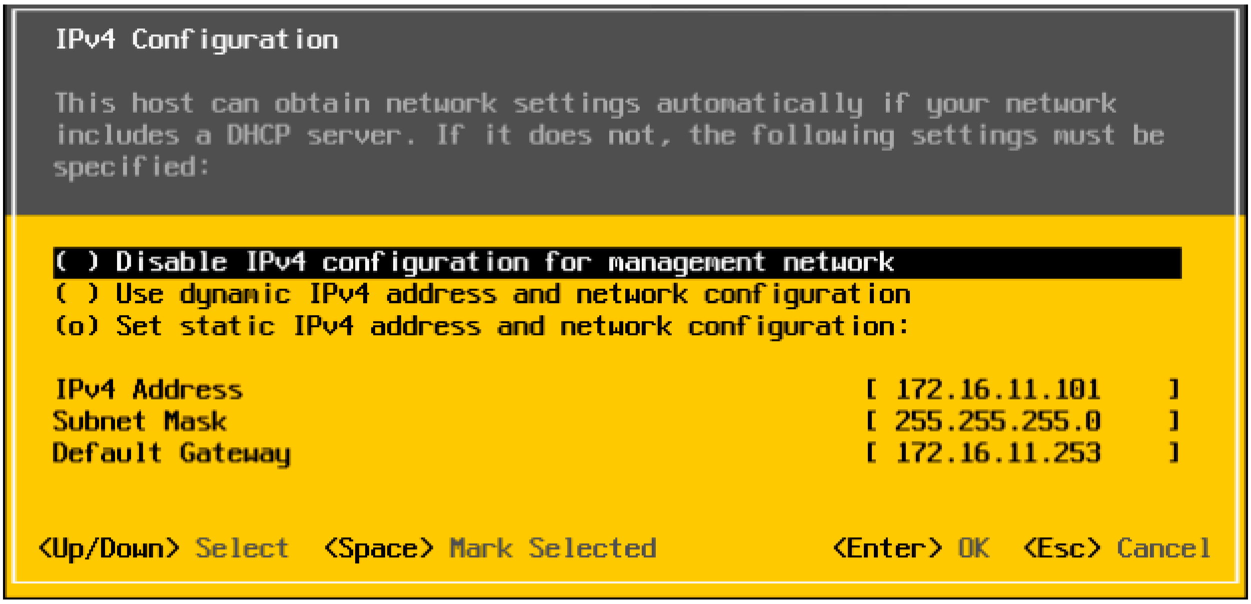
The Direct Console User Interface (DCUI) is a menu-based interface that is accessed from the host console and used to configure ESXi running on vSphere hosts.

NOTE: You must configure the ESXi settings using both DCUI and the web interface.

1. After the server reboots and fully loads ESXi, press F2 to log in to the DCUI.
2. Enter the credentials that were created during the ESXi installation, and then press Enter.
3. From the **System Customization** menu, select **Configure Management Network**.
4. From the **VLAN (Optional)** menu, press Enter.

   NOTE: Step 4 is mandatory although the name of the menu item includes the word optional.

5. Enter the required **management VLAN ID**, and then press Enter.
6. Select **IPv4 Configuration** and press Enter.
7. Select **Set static IPv4 address** and press the spacebar.



```
IPv4 Configuration

This host can obtain network settings automatically if your network
includes a DHCP server. If it does not, the following settings must be
specified:

( ) Disable IPv4 configuration for management network
( ) Use dynamic IPv4 address and network configuration
(o) Set static IPv4 address and network configuration:

IPv4 Address                                    [ 172.16.11.101    ]
Subnet Mask                                     [ 255.255.255.0    ]
Default Gateway                                 [ 172.16.11.253    ]

<Up/Down> Select   <Space> Mark Selected          <Enter> OK   <Esc> Cancel
```

Figure 9. IPv4 configuration page

8. Enter the **IPv4 Address**,**Subnet Mask**, and the **Default Gateway**, and then press Enter to confirm.
9. Select **DNS Configuration**, and then press Enter.
10. Enter the IP addresses of the DNS servers and FQDN of the host.
11. Press Esc to return to the main menu, and then press Y to confirm the changes and restart the management network.
12. From the main menu, click **Test Management Network**.
    The target IP addresses and DNS hostname are pre-populated.
13. Press Enter to perform the network test, and after the test is completed, press Enter to return to the main menu.

    △ CAUTION: **If the network test fails, troubleshoot and resolve the issues before proceeding further.**

14. From the main menu, select **Troubleshooting Options** > **Enable ESXi Shell**, and then select **Enable SSH** (required during validation and deployment phases) to enable the ESXi shell.
15. Press Esc to return to the main menu.

Configure ESXi settings using web interface

Before configuring ESXi settings using web interface, you must configure the ESXi settings using DCUI. For more information, see Configure ESXi settings—using DCUI.

ⓘ NOTE: **You must configure the ESXi settings using both DCUI and the web interface.**

1. Using a web browser, go to the ESXi host-level management web interface at **https://<ESXi Host Address>/ui**.
2. Enter the credentials that were created during the ESXi installation, and then click **Log in**.
3. In the **Navigator** pane, click **Networking**.
   The current port groups on the host are displayed by default. One is configured with VLAN information that is entered during installation and the other is still at zero.
4. Right-click **VM Network** and then click **Edit settings**.

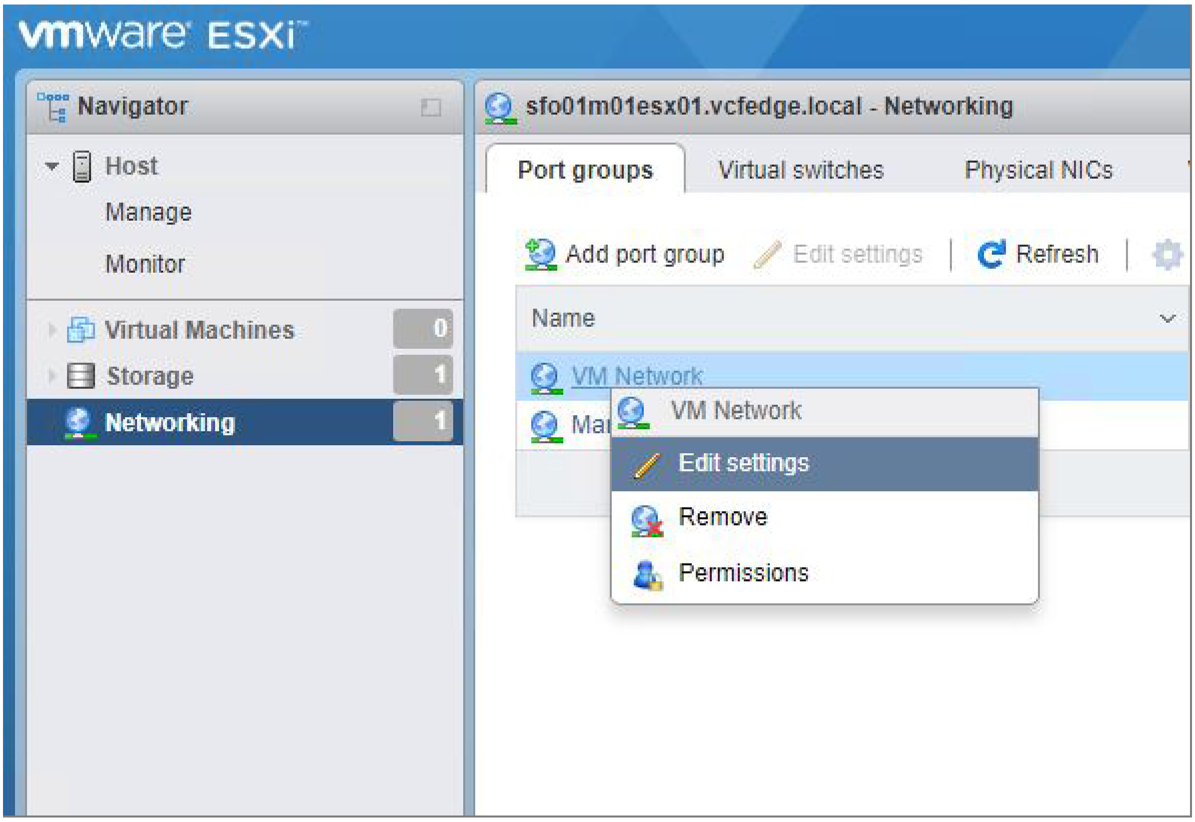


Figure 10. ESXi web interface—Edit settings page

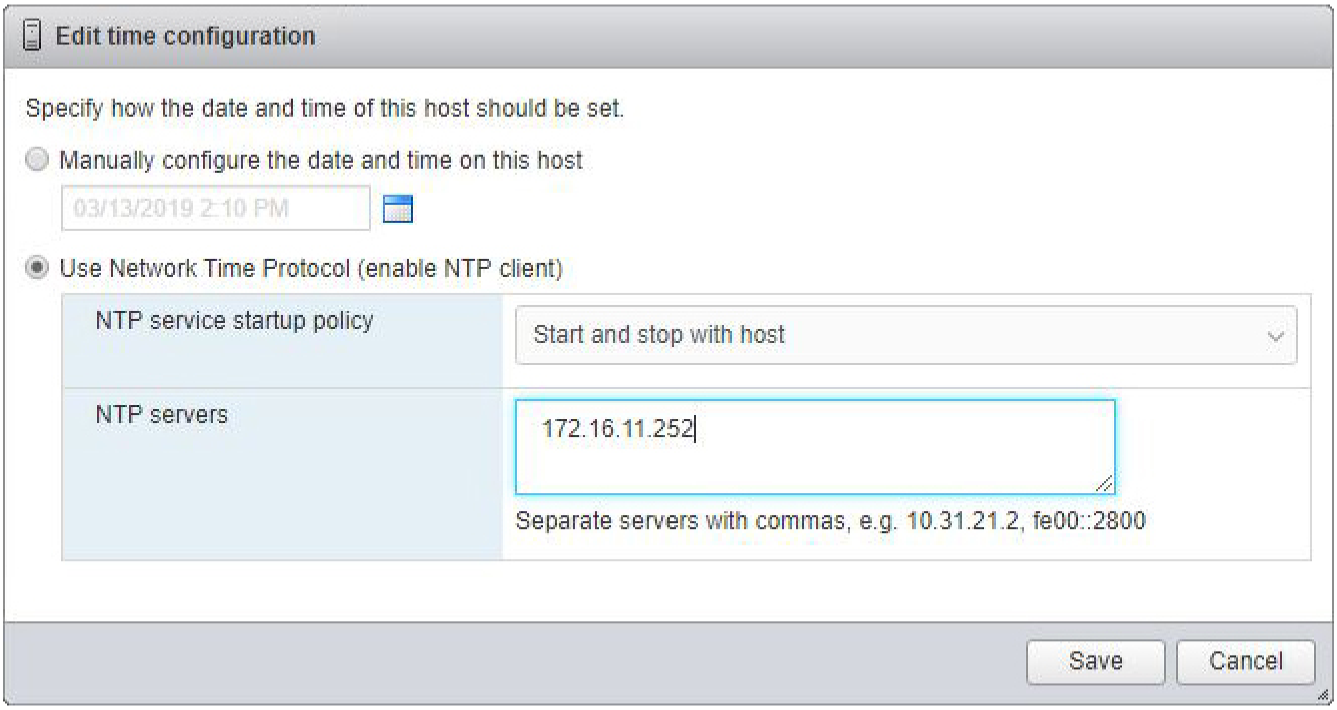
5. In the **Edit Port Group** window, enter the **Management VLAN ID**, and then click **Save**.

   CAUTION: **Leaving the VLAN ID at default setting causes pre-deployment validation to fail during a later step.**

6. In the **Navigator** pane, click **Manage** to set up the NTP.
7. In the right pane, click **Time & Date**.
8. Click **Edit Settings** and then select **Use Network Time Protocol (enable NTP client)**.
9. In the **NTP Servers** box, enter the NTP server IP addresses.

   NOTE: **If multiple IP addresses are provided, separate the IP addresses with commas.**

10. Click **Save**.



Edit time configuration

Specify how the date and time of this host should be set.

○ Manually configure the date and time on this host

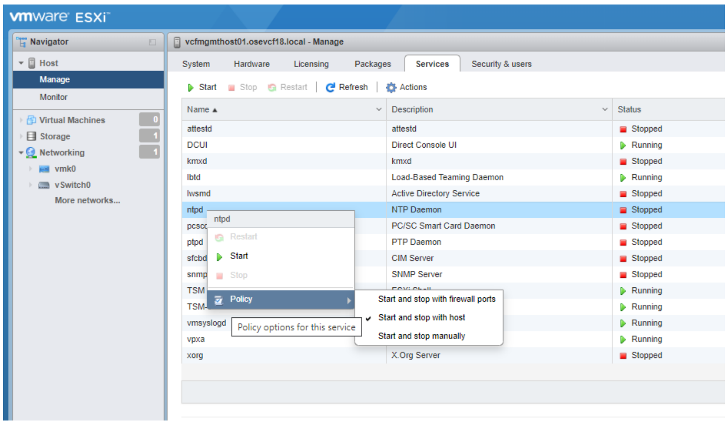
03/13/2019 2:10 PM

● Use Network Time Protocol (enable NTP client)

NTP service startup policy	Start and stop with host
NTP servers	172.16.11.252 Separate servers with commas, e.g. 10.31.21.2, fe00::2800

Figure 11. ESXi web interface—Edit time configuration page

11. In the **Manage** pane, select the **Services** tab and right click on the **ntpd service**. Set the Policy to **Start and stop with the host**. The resulting page is as shown in the following figure:



Name ▲	Description	Status
attestd	attestd	🟥 Stopped
DCUI	Direct Console UI	▶ Running
kmxd	kmxd	🟥 Stopped
lbtd	Load-Based Teaming Daemon	▶ Running
lwsmd	Active Directory Service	🟥 Stopped
ntpd	NTP Daemon	🟥 Stopped
pcscd	PC/SC Smart Card Daemon	🟥 Stopped
ptpd	PTP Daemon	🟥 Stopped
sfcbd	CIM Server	🟥 Stopped
snmp	SNMP Server	🟥 Stopped
TSM	ESXi Shell	▶ Running
TSM-		▶ Running
vmsyslogd		▶ Running
vpxa		▶ Running
xorg	X.Org Server	🟥 Stopped

Figure 12. ESXi settings web interface—Manage pane

Once the policy is set, start the ntpd service. If the ntpd service is already running, restart the service.

Repeat all the steps for each host targeted for Cloud Foundation management domain deployment. Validate that each ESXi host can access the NTP servers by establishing an SSH connection to each host and executing the `ntpq -p` command. A reach value of 377 indicates that time synchronization is functioning properly.

11

Cloud Builder and SDDC deployment

The primary software installation tool for Cloud Foundation 4.x is Cloud Builder. It is delivered as a virtual appliance in the standard OVA format. This section describes the steps to deploy the OVA. The Cloud Builder VM is a temporary tool to facilitate deployment of Cloud Foundation. It can be discarded after the deployment.

Topics:

Deploy Cloud Builder

The prerequisites to deploy Cloud Builder are as follows:

- Cloud Builder OVA file with version and build numbers that are specified in Validated components section
- The following steps must be deployed to an ESXi host outside of the Cloud Foundation target nodes and have network access to the Cloud Foundation Management VLAN on which the Cloud Builder VM resides.
- All prior sections are reviewed and any listed steps completed

1. Using a web browser, go to the vCenter or ESXi web client at https://<ip address> .
2. In the **Navigator** pane, on the **Hosts and Clusters** tab, locate an available ESXi host.
3. Right-click the ESXi host and select **Deploy OVF Template**.
4. Locate the OVA file locally or from the URL, and then click **Next**.
5. Select the required ESXi server to host the Cloud Builder VM, and then click **Next**.

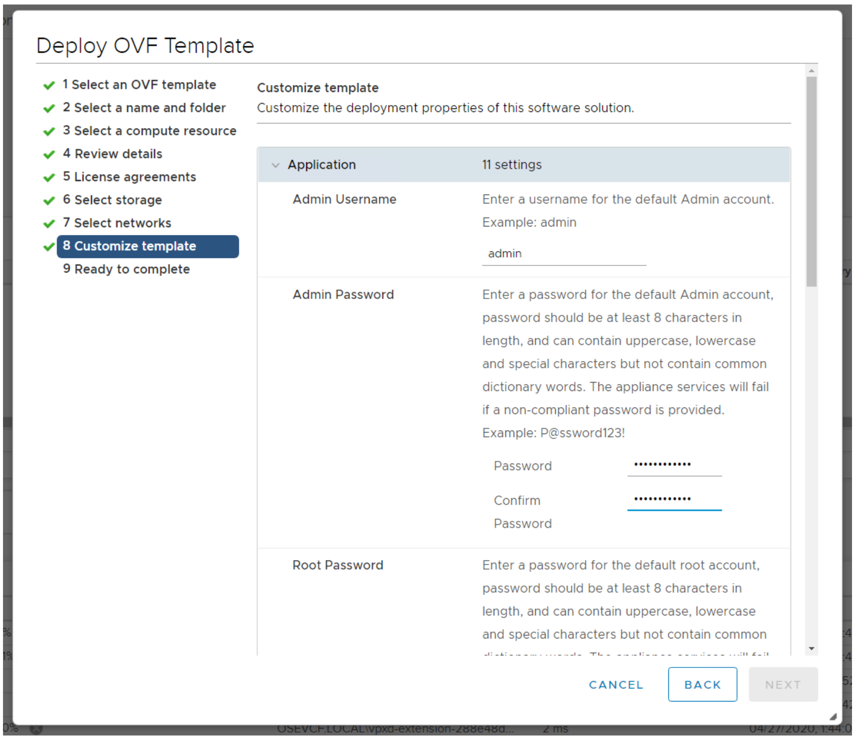
   NOTE: The selected EXSi server should not be targeted for Cloud Foundation deployment.

6. Click **Next**.
7. Review the EULA, and if you agree, click **Accept**, and then click **Next** to continue.
8. Select the required datastore and then click **Next**.
9. Select the required network and then click **Next**.
10. In the **Customize Template** page, enter username, password, network 1 IP address and subnet mask, default gateway, hostname, DNS, and NTP resources in the appropriate fields, and then click **Next**.

    CAUTION: You must adhere to the following password rules that are listed on the screen:

    - **Noncompliant passwords cause an unrecoverable error when attempting to access and use the Cloud Builder VM in the next section of the document.**
    - **The password rules vary for different user accounts. For example, minimum 8-character rule is applicable to some users and minimum 12-character rule is applicable to other users.**
    - **You must not enter dictionary words as passwords.**

    NOTE: IP Address and related fields must align with the IP subnet of the Cloud Foundation Management VLAN.



Customize template

Customize the deployment properties of this software solution.

Application 11 settings

Admin Username: Enter a username for the default Admin account. Example: admin

admin

Admin Password: Enter a password for the default Admin account, password should be at least 8 characters in length, and can contain uppercase, lowercase and special characters but not contain common dictionary words. The appliance services will fail if a non-compliant password is provided. Example: P@ssword123!

Password: ••••••••••••

Confirm Password: ••••••••••••

Root Password: Enter a password for the default root account, password should be at least 8 characters in length, and can contain uppercase, lowercase and special characters but not contain common

Figure 13. OVF customize template page

11. Review the **Ready to Complete** final configuration page, and then click **Finish**.
12. In the **Recent Tasks** pane, check the OVA deployment status.
    When the OVA deployment is complete, turn on the Cloud Builder VM.

Check Time Synchronization

After the Cloud Builder VM is started it will take some time to for all of the services to start and for time synchronization to complete. It is recommended that you access the command line of the Cloud Builder VM and verify time synchronization status using Linux “ntpq” commands.

```
root@vcloudbuilder# ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*100.71.100.2    143.166.255.32   2 u  113 1024  377    0.218   -0.755   0.037
+ntp-cent-3.osev 143.166.226.32   2 u  510 1024  377    0.205    0.612   0.443
```

12

VCF Deployment using Cloud Builder

In the previous section, you deployed the Cloud Builder virtual appliance. In this section, the software within the virtual machine is used to validate the target environment and deploy the entire Cloud Foundation stack.

ⓘ **NOTE: Before proceeding with the Cloud Builder validation process, take a snapshot of your Cloud Builder VM.**

Topics:

Prerequisites

The prerequisites to deploy the Cloud Foundation stack are as follows:

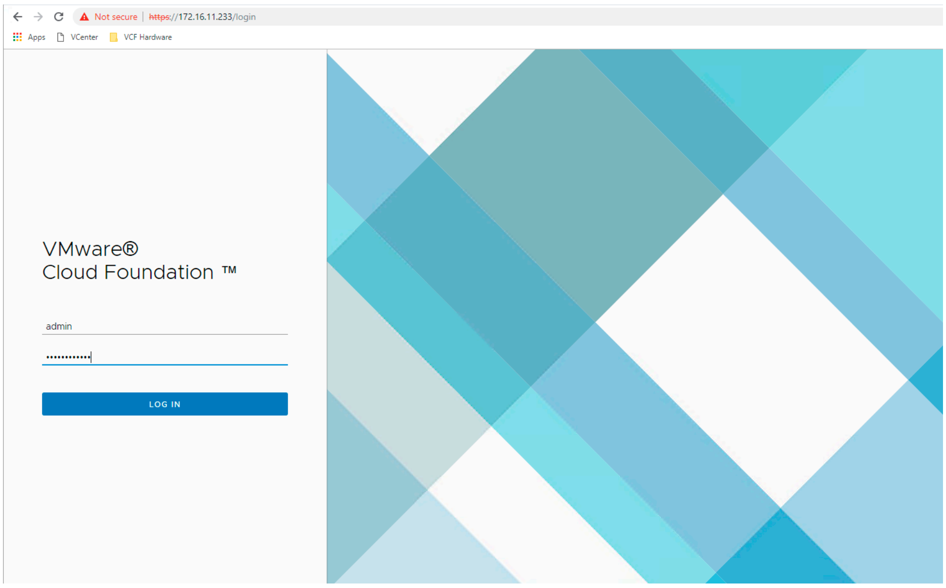
- Cloud Builder OVA file with version and build numbers that are specified in the Validated components section must be deployed to an available ESXi host outside of the Cloud Foundation target nodes with network access to the Cloud Foundation Management VLAN.
- Target hardware certified on VMware Compatibility Guide (VCG) with appropriate firmware versions is specified in the Validated components section.
- Clean install of ESXi on each target server node, with SSH/NTP/DNS enabled and configured.
- Physical switches that are configured with jumbo frames and necessary VLANs.
- All prior sections are reviewed and any listed steps completed.
- A completed parameter sheet. (can be downloaded during the CloudBuilder Deployment Wizard)

Launch Cloud Builder web interface

Complete the following steps to launch the Cloud Builder web interface:

1. Turn on **Cloud Builder VM**.
   The VM must finish booting up and load the application stack.

   ⓘ **NOTE: You can monitor the progress of Cloud Builder VM from a VM console session.**
2. Using a web browser, go to the Cloud Builder web interface at **https://<Cloud Builder IP Address>**.



VMware®
Cloud Foundation ™

admin

Figure 14. Cloud Builder web interface

3. Log in using the credentials that you specified during OVA deployment.
4. Click **Check All** to review the checklist of pre-bring-up steps and confirm that all the steps that are completed, and then click **Next**.
5. Review the EULA, and if you agree, click **Agree to End User License Agreement**, and then click **Next**.
6. If you have not obtained and completed the Cloud Foundation Information Spreadsheet, click **Download Deployment Parameter Sheet**.

Cloud Builder Deployment Parameter Sheet

All parameters that are needed for Cloud Builder to deploy your Cloud Foundation stack are passed to the tool using the deployment parameter sheet. It is critical that you complete the sheet fully and accurately. The configuration details that you enter into the deployment parameter sheet should be tied to existing services and records before proceeding. For example, the DNS servers you specify in the deployment parameter sheet must correspond to DNS servers running in your infrastructure.

NOTE: This guide covers the process to deploy Cloud Foundation using a spreadsheet, for example, .xlsx format. However, Cloud Builder also supports the use of a .json file for uploading deployment parameters. The latter is outside the scope of this document.

This worksheet is incorporated into the Cloud Builder VM and specific version of Cloud Foundation that is deployed. Save the worksheet to a safe location and edit the file modifying the information to match your deployment environment.

Note the following points before deploying Cloud Foundation using the deployment parameter sheet:

- Do not deploy Cloud Foundation using the deployment parameter sheet intended for a different version of Cloud Foundation.
- Any parameter field with a yellow background indicates that data format validation rules for that field have been specified.
- If when adding information to the parameter sheet your font turns red, you have not entered the right information.
- Do not copy and paste data between fields as different fields may have different requirements.
- Copying fields can change or delete the specified input data validation for that data.

Cloud Builder parameters

Some of the Cloud Builder parameters are:

- Management Workload tab
- Users and Groups tab
- Hosts and Networks tab
- Deploy Parameters tab

Management Workload tab

License keys are required for the following items:

- ESXi hosts
- vSAN
- vCenter
- NSX-T
- SDDC Manager Appliance

Users and Groups tab

In the **Users and Groups** tab, you can set the passwords for your initial Cloud Foundation components.

⚠ **CAUTION: Do not make a mistake on this page because if any of the passwords do not meet the indicated specifications, you must redeploy your Cloud Builder VM, unless you elected to create a snapshot after you created your VM.**

ⓘ **NOTE: Minimum password length should be 12 characters for NSX controllers.**

Hosts and Networks tab

In the **Hosts and Networks** tab, perform the following steps:

- Specify the VLAN IDs, subnets, gateways, and MTU for the networks that are used for the four required Cloud Foundation networks.
  - The MTU value should be the MTU size that can be tested during validation. For an actual MTU value of 9000 set this value to 8972.
- Specify the management IP addresses of the deployed hosts which are on the Cloud Foundation management VLAN.
- Specify the range of IP addresses for both the vSAN and vMotion networks.
- Host names that you enter in the **Management Domain ESXi Hosts** section are also autopopulated in the **ESXi Host** column of the **ESXi Host Security Thumbprint** section.

By default, use of DSA fingerprints as a more secure method to validate a host's authenticity is optional and disabled. Unique fingerprints are automatically generated on each host during installation. You can view the fingerprints using the **DCUI** under **View Support Information**. Due to the complexity of fingerprints, it is easier to access the hosts using SSH where they can be copied and pasted into the cloud builder deployment parameter sheet. Change the **Validate ESXi Thumbprints** option to **Yes** to enable fingerprint validation.

Deploy Parameters tab

The **Deploy Parameters** tab contains all the IP addresses and hostnames that must be added to DNS.

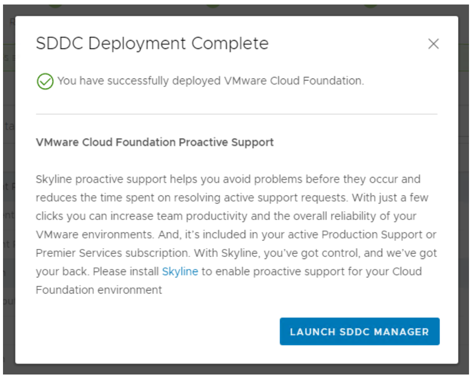
- All the hostnames must be configured for forward and reverse lookups.
- Test all the hostnames before attempting validation.
- Ensure that all of the values provided are consistent with the values used to deploy the Cloud Builder VM
- The NTP server would have already been tested as the ESXi hosts have already been configured to this same NTP server(s).
- Change the hostnames that are listed and the domain that meets the customer required specifications.
- For a simplified network installation where a multi-tiered BGP environment is not available make sure that field **K27** is set to **No**.

Run Cloud Builder Deploy SDDC

Complete the following steps to launch the Cloud Builder web interface:

1. Turn on Cloud Builder VM.
2. The VM must finish booting up and load the application stack.
3. Using a web browser, go to the Cloud Builder web interface at https://<Cloud Builder IP Address>.
4. Log in using the credentials that you specified during OVA deployment.
5. Review the **EULA**, and if you agree, click **Agree** to End User License Agreement, and then click **Next**.
6. Select **VMware Cloud Foundation**. Be sure not to select VMware Cloud Foundation on VxRAIL.
7. Review the list of **Prerequisites** and ensure that they have all been completed

8. **Place a checkmark** to indicate that the prerequisites have been met and select **Next**
9. If you have not obtained and completed the Cloud Foundation Information Spreadsheet, click **Download Deployment Parameter Sheet**. If you have the parameter sheet click **Next** to move forward
10. If you have not completed your parameter sheet do it now. If the parameter sheet is complete, click **Next** to continue.
11. Click **Select File** to browse to your completed parameter sheet.
12. Locate your completed parameter sheet and click **Open**.
13. Click **Next** to begin the validation phase.
    If validation discovers any issues in your configuration or parameter file it will show an error and provide clear and detailed information on the issue. Read the message provided, correct the issue(s) and run the validation again. Validation can be run as many times as necessary to obtain a successful result.
14. Once Validation has passed, and you have the **green banner** indicating that 'Configuration file validated successfully', click **Next**
15. A pop-up will appear on the screen to Deploy SDDC Manager.
16. Click **DEPLOY SDDC** to continue
    The deployment process will begin. The deployment will take in excess of an hour. A successful deployment will result in the **SDDC Deployment Complete** pop-up message. If there were any issues you can identify them in the **VMware Cloud Foundation** deployment screen.
17. Review any task failures and correct the issue. You can restart the deployment when you have resolved the issue(s).
18. Click **LAUNCH SDDC MANAGER**



SDDC Deployment Complete

✓ You have successfully deployed VMware Cloud Foundation.

VMware Cloud Foundation Proactive Support

Skyline proactive support helps you avoid problems before they occur and reduces the time spent on resolving active support requests. With just a few clicks you can increase team productivity and the overall reliability of your VMware environments. And, it's included in your active Production Support or Premier Services subscription. With Skyline, you've got control, and we've got your back. Please install Skyline to enable proactive support for your Cloud Foundation environment

Figure 15. Pop-up window on successful SDDC deployment

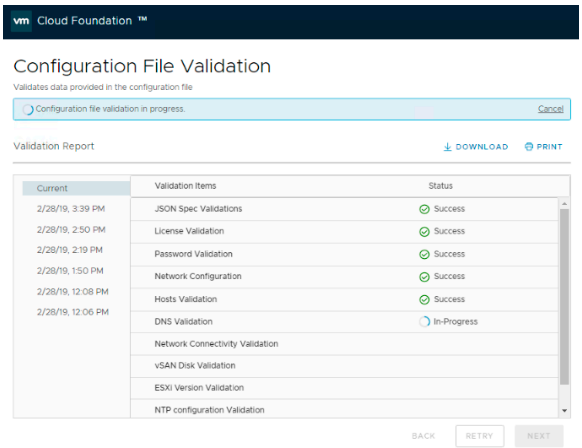
VMware Cloud Foundation on Dell EMC servers and networking hardware is now successfully deployed.

Cloud Builder Configuration Validation

The Cloud Builder Configuration Validation is a critical step in the Cloud Foundation deployment process. It probes your target servers, required services, and network environment to detect potential issues.

NOTE: The validation may fail initially and can be run as many times as necessary to address any issues.

1. After you have completed the deployment parameter spreadsheet, click **Upload**, select the file, and then click **Open**.
   A message is displayed to acknowledge successful upload of the parameter sheet.
2. Click **Validate** and monitor progress on the **Configuration File Validation** page.



Configuration File Validation

Validates data provided in the configuration file

Configuration file validation in progress.

Validation Report

Current
2/28/19, 3:39 PM
2/28/19, 2:50 PM
2/28/19, 2:19 PM
2/28/19, 1:50 PM
2/28/19, 12:08 PM
2/28/19, 12:06 PM

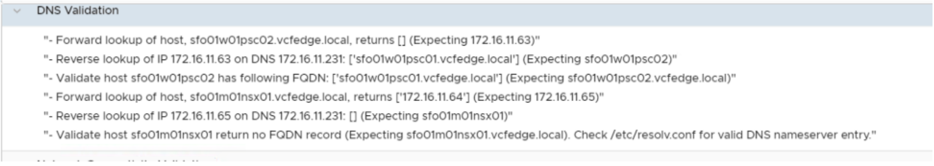
Validation Items	Status
JSON Spec Validations	✓ Success
License Validation	✓ Success
Password Validation	✓ Success
Network Configuration	✓ Success
Hosts Validation	✓ Success
DNS Validation	In-Progress
Network Connectivity Validation	
vSAN Disk Validation	
ESXi Version Validation	
NTP configuration Validation	

Figure 16. Configure Cloud Builder validation

NOTE: Validation may take 15 minutes or more. However, if there are issues such as the DNS server being down or if you provided a wrong IP address, validation may take longer.

NOTE: On the Validation Report page, you can access the information about previous validation attempts. Each validation attempt is tracked with an entry that is designated by the date and time of execution.

3. If the validation fails, expand the failed line item and review the detailed error messages. Some of the possible validation failures are shown in the following example.



DNS Validation

```
"- Forward lookup of host, sfo01w01psc02.vcfedge.local, returns [] (Expecting 172.16.11.63)"
"- Reverse lookup of IP 172.16.11.63 on DNS 172.16.11.231: ['sfo01w01psc01.vcfedge.local'] (Expecting sfo01w01psc02)"
"- Validate host sfo01w01psc02 has following FQDN: ['sfo01w01psc01.vcfedge.local'] (Expecting sfo01w01psc02.vcfedge.local)"
"- Forward lookup of host, sfo01m01nsx01.vcfedge.local, returns ['172.16.11.64'] (Expecting 172.16.11.65)"
"- Reverse lookup of IP 172.16.11.65 on DNS 172.16.11.231: [] (Expecting sfo01m01nsx01)"
"- Validate host sfo01m01nsx01 return no FQDN record (Expecting sfo01m01nsx01.vcfedge.local). Check /etc/resolv.conf for valid DNS nameserver entry."
```

Figure 17. Configuration validation error messages

4. Resolve all the reported failures within the targeted servers, required services, network environment, or parameter spreadsheet, and then re-run validation in Cloud Builder by clicking **Retry**.
5. Repeat Steps 1-4, until the validation is successful.

SDDC bring-up

Perform the following steps for the SDDC bring-up:

1. In the **Bringing Up the SDDC** page, click **Next** to start the deployment of Cloud Foundation.

   NOTE: You can monitor the deployment progress on the Bringing Up the SDDC page and this deployment process may require two hours or more, depending on your environment.

2. If a bring-up failure occurs, expand the failed line item, review the detailed error messages. Depending on the nature of the error, resolve all the reported failures and click **Retry**.

   NOTE: If an unrecoverable failure occurs during SDDC bring-up, it is necessary to resolve the root cause issue, wipe the Cloud Foundation target servers including all disk partitions, and then restart from the Deploy ESXi to cluster nodes section.

3. The SDDC bring-up process is completed when the Cloud Builder reports that the **SDDC has been successfully created**. When the SDDC bring-up process is complete, this indicates that the Cloud Foundation is successfully deployed.
4. Access the recently deployed SDDC Manager by clicking the link on the page.
5. Confirm deployment of vCenter, vSAN, NSX, and vRealize Log Insight.

   NOTE: Hostnames and IP addresses are in the Cloud Foundation Deployment Parameters spreadsheet.

   The Cloud Builder VM can now be discarded.

13

Post-install validation

Cloud Foundation cluster verification

After installing Cloud Foundation, perform the steps in the following sections to verify that the components are installed and available.

SDDC Manager

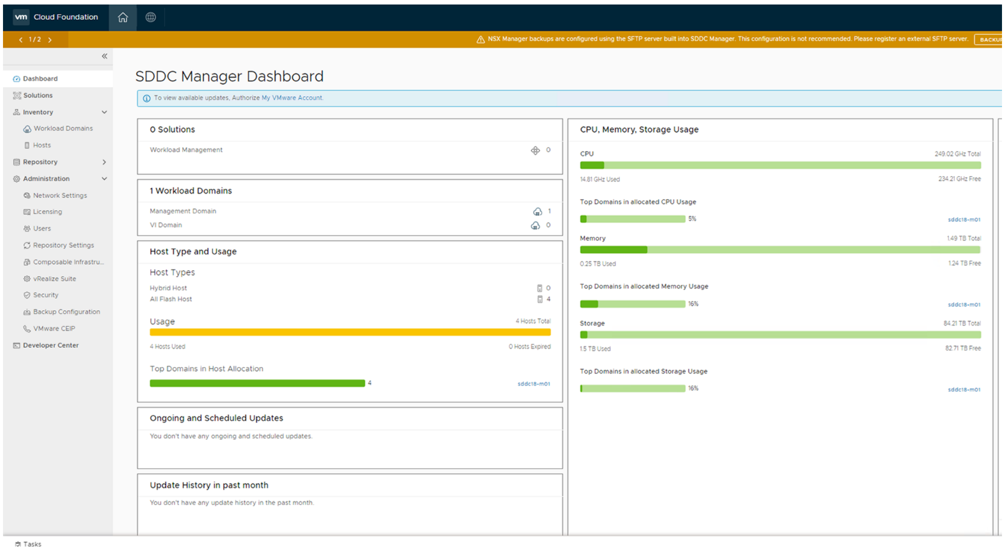
Log in to SDDC Manager using a web browser at: **https://<ip address or DNS name>**. The SSO user ID is `administrator@vsphere.local` and the password is the one you specified during installation.

NOTE: Use the domain `vsphere.local`. Do not use the DNS domain that was used for the Cloud Foundation deployment.

Customer Experience Improvement Program

Join Customer Experience Improvement Program (CEIP) when prompted. CEIP provides statistical data to SDDC Manager, allowing for improved performance and troubleshooting.

The following figure shows a sample SDDC Manager dashboard. In this example, the host usage is yellow because the management cluster has consumed all of the hosts currently available to Cloud Foundation.



NSX Manager backups are configured using the SFTP server built into SDDC Manager. This configuration is not recommended. Please register an external SFTP server.

SDDC Manager Dashboard

To view available updates, Authorize My VMware Account.

0 Solutions

Workload Management: 0

1 Workload Domains

Management Domain: 1

VI Domain: 0

Host Type and Usage

Host Types

Hybrid Host: 0

All Flash Host: 4

Usage: 4 Hosts Total, 4 Hosts Used, 0 Hosts Expired

Top Domains in Host Allocation: 4 sddc18-m01

Ongoing and Scheduled Updates

You don't have any ongoing and scheduled updates.

Update History in past month

You don't have any update history in the past month.

CPU, Memory, Storage Usage

CPU: 249.02 GHz Total, 14.81 GHz Used, 234.21 GHz Free

Top Domains in allocated CPU Usage: 5% sddc18-m01

Memory: 1.49 TB Total, 0.25 TB Used, 1.24 TB Free

Top Domains in allocated Memory Usage: 16% sddc18-m01

Storage: 84.21 TB Total, 1.5 TB Used, 82.71 TB Free

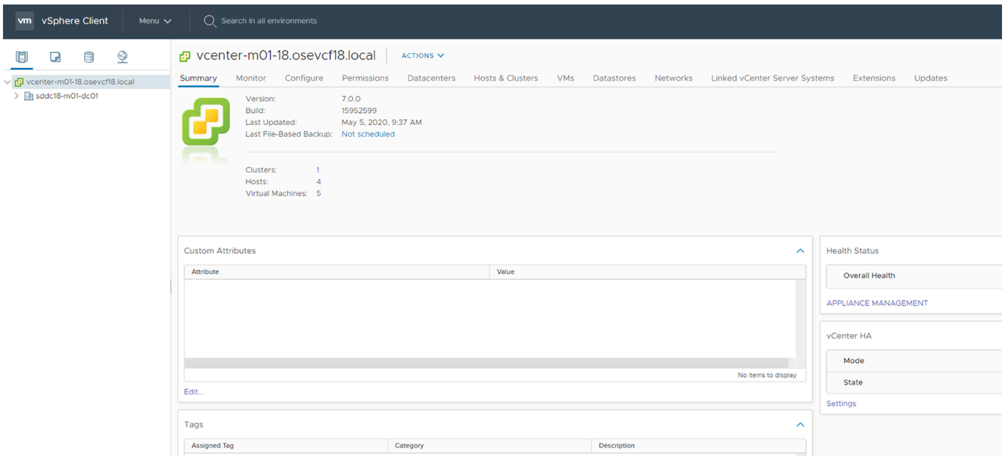
Top Domains in allocated Storage Usage: 16% sddc18-m01

Figure 18. SDDC Manager dashboard

vCenter

Log in to vCenter using the same SSO credentials—`administrator@vsphere.local`. Verify that the cluster appears healthy and that there are no warnings.

Validate that the VMs created during deployment are all up and running. Validate that your VSAN is running and available. Look at the disk groups that are created and ensure they are consistent with the disks available in the hosts. Look at the virtual networking components that are deployed to vCenter.



vcenter-m01-18.osevcf18.local

Version: 7.0.0
Build: 15952599
Last Updated: May 5, 2020, 9:37 AM
Last File-Based Backup: Not scheduled

Clusters: 1
Hosts: 4
Virtual Machines: 5

Attribute	Value

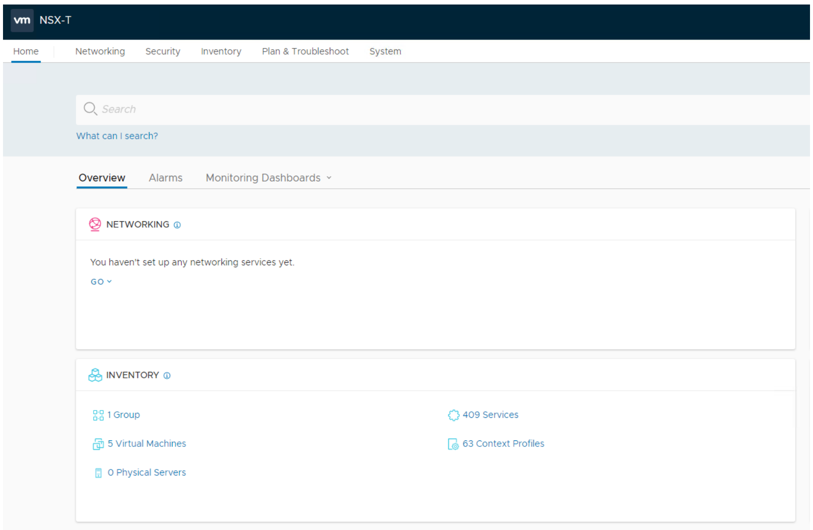
No items to display

Assigned Tag	Category	Description

Figure 19. vCenter dashboard

NSX Manager

Log into the NSX Manager through your browser using the admin credentials set in your parameter sheet.



You haven't set up any networking services yet.

1 Group
5 Virtual Machines
0 Physical Servers
409 Services
63 Context Profiles

Figure 20. NSX dashboard

VMware Cloud Foundation installation complete

Cloud Foundation has been successfully deployed and is ready for use. Typical tasks from this point would be:

- Configure your VMware account credentials in SDDC manager.
- If you chose simplified networking configure your SDDC for VLAN backed Application Virtual Networks.
- Install additional products such as:
  - Life Cycle Manager.
  - vRealize Suite.
  - Other licenced bundles.
- Deploy a Workload Domain.