

VMware Cloud Foundation Planning and Preparation Guide

VMware Cloud Foundation 3.0



vmware®

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

<https://docs.vmware.com/>

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

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

Copyright © 2018 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

	About the VMware Cloud Foundation Planning and Preparation Guide	4
1	Minimum Hardware Requirements	5
2	Software Requirements	8
	Cloud Foundation Builder VM Support	8
	Third-Party Software	9
	VMware Software Licenses	9
	Passwords	10
3	External Services	11
	External Services Overview	11
	Physical Network Requirements	13
	Network Pools	13
	VLANs and IP Subnets	14
	Host Names and IP Addresses	15
4	Capacity Planning for Management and Workload Domains	21
	Virtual Infrastructure Layer Footprint	21
	Operations Management Layer Footprint	22
	Cloud Management Layer Footprint	23
5	Virtual Machine Placement	25

About the VMware Cloud Foundation Planning and Preparation Guide

The *VMware Cloud Foundation Planning and Preparation Guide* provides detailed information about the software, tools, and external services that are required prior to using VMware Cloud Foundation to implement a Software-Defined Data Center (SDDC).

This document should be reviewed in its entirety, prior to beginning a VMware Cloud Foundation deployment to ensure a successful deployment. Review this document several weeks prior to the start of the deployment in order to provide enough time to realize all the requirements.

VMware Cloud Foundation can be deployed in one of two different architecture models - Standard or Consolidated.

- In the standard architecture model, the SDDC management workloads are separated from the tenant workloads by using multiple workload domains.
- In the consolidated architecture model, only one workload domain containing both the management and tenant workloads is created and resource pools are used to isolate workloads.

Although this document focuses on the standard architecture model, the general requirements provided are applicable to both.

Intended Audience

The *VMware Cloud Foundation Planning and Preparation Guide* is intended for cloud architects, infrastructure administrators, and cloud administrators who are familiar with VMware software and want to quickly deploy and manage an SDDC.

Required VMware Software

The *VMware Cloud Foundation Planning and Preparation Guide* is compliant and validated with certain product versions. See the VMware Cloud Foundation release notes for more information about supported product versions.

Minimum Hardware Requirements

1

To implement an SDDC with VMware Cloud Foundation, your hardware must meet certain minimum requirements.

This topic provides general guidance on the minimum requirements for a management domain and a virtual infrastructure workload domain in a Cloud Foundation system. For more details about sizing a Cloud Foundation system for your environment, see [Chapter 4 Capacity Planning for Management and Workload Domains](#).

Management Domain

The management domain contains infrastructure workloads. The management domain requires a minimum of four servers. The management domain can be expanded in order to provide more resources for additional workloads or increased availability.

In the standard architecture deployment model, the infrastructure workloads contained within the management domain are kept isolated from tenant workloads through the creation of additional workload domains. In the consolidated architecture model, both infrastructure and tenant workloads are contained within the management domain. Workloads are kept separated in this model through the implementation of resource pools. Regardless of the deployment model used, ensure the servers provide ample resources to support the deployed workloads. This includes being able to support availability and maintenance actions where the workloads on a server need to be transferred to the other servers in the workload domain.

Cloud Foundation supports the use of vSAN ReadyNodes that are certified with supported versions of ESXi. Refer to <https://kb.vmware.com/s/article/52084> for guidance on what components can be modified in a vSAN ReadyNode. See the [VMware Cloud Foundation Release Notes](#) for information about supported versions of ESXi.

The management domain contains a management cluster which must meet or exceed the following minimum hardware requirements.

Table 1-1. Minimum Hardware Requirements for the Management Cluster

Component	Requirements
Servers	<ul style="list-style-type: none"> Four vSAN ReadyNodes <p>For information about compatible vSAN ReadyNodes, see the VMware Compatibility Guide.</p>
CPU per server	<ul style="list-style-type: none"> Dual-socket, 8 cores per socket minimum requirement for all-flash systems Single-socket, 8 cores per socket minimum requirement for hybrid (flash and magnetic) systems <p>Note Cloud Foundation also supports quad-socket servers for use with all-flash or hybrid systems.</p>
Memory per server	<ul style="list-style-type: none"> 192 GB
Storage per server	<ul style="list-style-type: none"> 16 GB Boot Device, Local Media; see https://kb.vmware.com/s/article/2004784 One NVMe or SSD for the caching tier <ul style="list-style-type: none"> Class D Endurance Class E Performance Two SSDs or HDDs for the capacity tier <p>See Designing and Sizing a vSAN Cluster for guidelines about cache sizing.</p>
NICs per server	<ul style="list-style-type: none"> Two 10 GbE (or higher) NICs (IOVP Certified) (Optional) One 1 GbE BMC NIC <p>Note Servers cannot have more than two NICs for primary communication, plus one BMC NIC for out-of-band host management.</p>

Virtual Infrastructure Workload Domains

A virtual infrastructure (VI) workload domain is used in the standard architecture deployment model to contain the tenant workloads. A VI workload domain consists of a minimum of one cluster consisting of three or more servers. Additional clusters can be added to a VI workload domain as required. A Cloud Foundation solution can include a maximum of 15 workload domains, in accordance with vCenter maximums.

Workloads in each cluster utilize vSphere High Availability (HA) to coordinate the failover to other servers in the event of a failure. To provide for the best levels of availability, all servers in a given cluster must be of the same model and type. A cluster does not need to have servers of the same model and type as other clusters. For example, all servers in Cluster 1 must be homogeneous; all servers within Cluster 2 must be homogeneous; servers in Cluster 1 do not need to have the same model and type as servers in Cluster 2.

Cloud Foundation supports the use of most vSAN ReadyNodes. Refer to <https://kb.vmware.com/s/article/52084> for guidance on what components can be modified in a vSAN ReadyNode.

The servers used for a VI workload domain must meet or exceed the following minimum requirements.

Table 1-2. Minimum Hardware Requirements for a VI Workload Domain

Component	Requirements
Servers	<ul style="list-style-type: none"> ■ Three supported servers <p>For information about compatible vSAN ReadyNodes, see the VMware Compatibility Guide.</p>
CPU, memory, and storage per server	<ul style="list-style-type: none"> ■ Supported configurations
NICs per server	<ul style="list-style-type: none"> ■ Two 10 GbE (or higher) NICs (IOVP Certified) ■ (Optional) One 1 GbE BMC NIC <p>Note Servers cannot have more than two NICs for primary communication, plus one BMC NIC for out-of-band host management.</p>

Primary Storage Options

VMware Cloud Foundation utilizes and is validated against vSAN as primary storage. Familiarize yourself with the vSAN documentation on docs.vmware.com, if you have not done so already.

With any vSAN deployment, it is imperative that you maintain the firmware and drivers across the entire storage path, including the storage controller, any SSD drives, and ESXi. Use the vSAN HCL, <https://www.vmware.com/resources/compatibility/search.php?deviceCategory=vSAN>, to validate driver and firmware versions for associated components. Ensure the hardware is updated to supported levels before starting the deployment.

Software Requirements

Additional software is required in order to deploy and manage VMware Cloud Foundation.

The required software depends on the configuration options you choose.

This chapter includes the following topics:

- [Cloud Foundation Builder VM Support](#)
- [Third-Party Software](#)
- [VMware Software Licenses](#)
- [Passwords](#)

Cloud Foundation Builder VM Support

In order to deploy Cloud Foundation, you first need to deploy the Cloud Foundation Builder VM.

The Cloud Foundation Builder VM takes your configuration inputs and provides the automated workflows that instantiate the management domain. The host for the Cloud Foundation Builder VM can be any supported system capable of running Cloud Foundation Builder. A dedicated ESXi host, workstation, or a laptop running VMware Fusion or Workstation are examples of supported systems. You can download the Cloud Foundation Builder VM through your MyVMware account.

The Cloud Foundation Builder VM requires the following resources.

Table 2-1. Cloud Foundation Builder VM Resource Requirements

Component	Requirement
CPU	4 vCPUs
Memory	4 GB
Storage	350 GB

The Cloud Foundation Builder VM requires network connectivity to the ESXi management network, so that it can communicate to all ESXi hosts added to the solution. The Cloud Foundation Builder VM also needs to be able to communicate to the DNS and NTP servers used in the VMware Cloud Foundation environment so that it can validate the deployment inputs provided. The DNS and NTP settings used when deploying the Cloud Foundation Builder VM must be the same as the settings configured on the hosts.

Once the management domain is created, you can delete the Cloud Foundation Builder VM and reclaim its resources.

Third-Party Software

Additional third-party software may be required in order to support the VMware Cloud Foundation solution.

In order to access the Cloud Foundation Builder VM UI to begin the Cloud Foundation deployment, you will need a host with a supported web browser. You will use the same host and browser to access the Cloud Foundation UI after deployment. See the VMware Cloud Foundation release notes for information about supported web browsers.

In addition, this host must have connectivity to the management network. When implementing a network specific to the out-of-band management of the servers through the BMC ports, the host should be multi-homed and able to access the configured out-of-band network as well.

Finally, the host should have enough storage space available to support the transfer of applications, log bundles, and, optionally, vRealize Automation template images.

You can use Cloud Foundation to automate the deployment of vRealize Automation. If you choose this option, the following additional products are required in order to complete the deployment. See the *VMware Cloud Foundation Operations and Administration Guide* for more information about deploying vRealize Automation.

Table 2-2. Third-Party Software Required to Automate the Deployment of vRealize Automation

SDDC Layer	Required by VMware Component	Vendor	Product Item	Product Version
Cloud Management	vRealize Automation	Microsoft	Windows Server	Windows Server 2012 R2 or Windows 2016 Standard (64-bit)
		Microsoft	SQL Server 2012	SQL Server 2012 or SQL Server 2016 Standard or higher (64-bit)

VMware Software Licenses

Before you deploy VMware Cloud Foundation, ensure that you have appropriate license keys for the required VMware software.

You will need a license key for each of the following:

- SDDC Manager
- VMware vSphere
- VMware vCenter Server
- VMware vSAN
- VMware NSX for vSphere
- VMware vRealize Log Insight
- VMware vRealize Automation (optional)
- VMware vRealize Operations (optional)

Passwords

You must specify the passwords to be used for the various accounts used during the deployment of Cloud Foundation.

Refer to the deployment parameter spreadsheet for a list of accounts for which you must define passwords. See the *VMware Cloud Foundation Architecture and Deployment Guide* for details about the deployment parameter spreadsheet and the password requirements.

External Services

VMware Cloud Foundation relies on a set of key infrastructure services to be made available externally. These external services must be configured and accessible before beginning a deployment.

This chapter includes the following topics:

- [External Services Overview](#)
- [Physical Network Requirements](#)
- [Network Pools](#)
- [VLANs and IP Subnets](#)
- [Host Names and IP Addresses](#)

External Services Overview

A variety of external services are required for the initial deployment of Cloud Foundation and for the deployment of other optional components like vRealize Operations or vRealize Automation.

The following table lists the required and optional external services and dependencies.

Table 3-1. External Services

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 Services (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 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 connected to the management and vRealize networks.

User and Group accounts must be configured in AD prior to adding them to the SDDC Manager and assigning privileges.

If you plan to deploy vRealize Automation, Active Directory services must be available. See the vRealize Automation documentation (<https://docs.vmware.com/en/vRealize-Automation/index.html>) for more information about its AD configuration.

DHCP

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

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

DNS

During deployment, you will need to 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 of the components contained within the Cloud Foundation solution. This includes servers, virtual machines, and any virtual IPs used. See [Host Names and IP Addresses](#) for details on the components requiring DNS resolution prior to starting a Cloud Foundation deployment.

Ensure that both forward and reverse DNS resolution is functional for each component prior to deploying Cloud Foundation or creating any workload domains.

NTP

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 various components also assists troubleshooting efforts.

Requirements for the NTP sources include the following:

- The IP addresses of two NTP sources can be 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

SMTP 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 signed by an internal enterprise CA or by a third-party commercial CA.

If you plan to replace the self-signed certificates, the CA must be able to sign a Certificate Signing Request (CSR) and return the signed certificate. All endpoints within the enterprise must also trust the root CA of the CA.

If you plan to deploy vRealize Automation, a Certificate Authority is required, and the installation workflow will request certificates.

Physical Network Requirements

Before you start deploying Cloud Foundation, you must configure your physical network.

Prior to deploying Cloud Foundation, configure your physical network to enable the following functionality.

- VLAN Tagging (802.1Q)
- Jumbo Frames
 - A minimum MTU value of 1600 is required, however it is recommended that you set the MTU to 9000.

Network Pools

Cloud Foundation uses a construct called a network pool to automatically configure VMkernel ports for vSAN and vMotion.

Cloud Foundation uses an Internet Protocol Address Management (IPAM) solution to automate the IP configuration of VMkernel ports for vSAN and vMotion. A network pool contains network information details for each network. Each network pool includes network information details for vSAN and vMotion. For example:

vSAN Network Information		vMotion Network Information	
VLAN ID	<input type="text" value="1633"/>	VLAN ID	<input type="text" value="1632"/>
MTU ⓘ	<input type="text" value="9000"/>	MTU ⓘ	<input type="text" value="9000"/>
Network	<input type="text" value="172.16.33.0"/>	Network	<input type="text" value="172.16.32.0"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>	Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="172.16.33.253"/>	Default Gateway	<input type="text" value="172.16.32.253"/>
Included IP Address Ranges Once a network pool has been created, you are not able to edit or remove IP ranges from that pool.		Included IP Address Ranges Once a network pool has been created, you are not able to edit or remove IP ranges from that pool.	
<input type="text" value="172.16.33.101"/>	To <input type="text" value="172.16.33.104"/>	<input type="text" value="172.16.32.101"/>	To <input type="text" value="172.16.32.104"/>
	<input type="button" value="ADD"/>		<input type="button" value="ADD"/>

When a server is added to the inventory of Cloud Foundation, it goes through a process called host commissioning. During this process, vSphere ESXi servers 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 used for vSAN and vMotion based on the network pool information and allocates IP addresses for vSAN and vMotion from the network pool it 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 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 through the use of VLANs. Before deploying your SDDC, you must allocate VLAN IDs and IP subnets for each required traffic type.

You must configure the VLAN IDs and IP subnets in your network in order to pass traffic through your network devices. Verify the allocated network information is configured and does not conflict with pre-existing services before starting your Cloud Foundation deployment.

The number and size of the subnets required for a deployment will depend on the number of workload domains created, the number of clusters defined, and the optional components installed.

The following table demonstrates the basic allocation of VLANs and IP subnets for a sample deployment. Utilize this sample to define the actual VLANs and IP subnets according to your environment.

Table 3-2. Sample VLAN and IP Subnet Configuration

Workload Domain	Cluster	VLAN Function	VLAN ID	Subnet	Gateway
Management	cluster-01	Management	1611	172.16.11.0/24	172.16.11.253
		vSphere vMotion	1612	172.16.12.0/24	172.16.12.253
		vSAN	1613	172.16.13.0/24	172.16.13.253

Table 3-2. Sample VLAN and IP Subnet Configuration (Continued)

Workload Domain	Cluster	VLAN Function	VLAN ID	Subnet	Gateway
		VXLAN (NSX VTEP)	1614	172.16.14.0/24	172.16.14.253
		vRealize (Optional)	1616	172.16.16.0/24	172.16.16.253
VI Workload #1	cluster-01	Management (ESXi)	1711	173.17.11.0/24	173.17.11.253
		vSphere vMotion	1712	173.17.12.0/24	173.17.12.253
		vSAN	1713	173.17.13.0/24	173.17.13.253
		VXLAN (NSX VTEP)	1714	173.17.14.0/24	173.17.14.253
		Uplink	1716	173.17.15.0/24	173.17.15.253
	cluster-02	Management (ESXi)	1811	174.18.11.0/24	174.18.11.253
		vSphere vMotion	1812	174.18.12.0/24	174.18.12.253
		vSAN	1813	174.18.13.0/24	174.18.13.253
		VXLAN (NSX VTEP)	1814	174.18.14.0/24	174.18.14.253
		Uplink	1816	174.18.15.0/24	174.18.15.253

Host Names and IP Addresses

Before you deploy Cloud Foundation, or before you create or expand a workload domain, you must define the hostnames and IP addresses for various system components.

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

The hostnames and IP addresses required 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 solution.
- Operations management layer: Components used for day-to-day management of the environment.
- Cloud management layer: Services that consume the infrastructure layer resources.

Host Names and IP Addresses for External Services

External services, like Active Directory and NTP, need to be accessible and resolvable by IP Address and fully qualified domain name (FQDN). Acquire the hostnames and IP addresses for these external services prior to deploying Cloud Foundation.

Allocate hostnames and IP addresses to the following components:

- NTP
- Active Directory (AD)

- Domain Name System (DNS)
- Certificate Authority

The following table provides an example of the information to be collected for the external services. This example uses a fictional DNS domain called `rainpole.local` for illustration purposes. Modify the sample information to conform to your site's configuration.

Table 3-3. Sample External Services Hostname and IP Information

Component Group	Hostname	DNS	IP Address	Description
NTP	ntp	sfo01.rainpole.local		Round robin DNS pool containing the NTP servers
	0.ntp	sfo01.rainpole.local	172.16.11.251	First NTP server
	1.ntp	sfo01.rainpole.local	172.16.11.252	Second NTP server
AD/DNS/CA	dc01rpl	rainpole.local	172.16.11.4	Windows 2012 R2 host that contains the Active Directory configuration, the DNS server for the <code>rainpole.local</code> domain, and the Certificate Authority for signing management SSL certificates
	dc01sfo	sfo01.rainpole.local	172.16.11.5	Active Directory and DNS server for the <code>sfo01</code> subdomain

Host Names and IP Addresses for the Virtual Infrastructure Layer

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

During the initial deployment of Cloud Foundation, the management domain is created. Components specific to the management domain need to be defined prior to installation.

After the initial deployment, you can create additional workload domains as required. Components specific to each additional workload domain need to be defined prior to their creation.

Planning ahead for the initial deployment and the workload domains to be created will avoid delays in a deployment.

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

Table 3-4. Sample Host Names and IP Addresses for the Virtual Infrastructure Layer

Workload Domain	Hostname	DNS Zone	IP Address	Description	
Management	sfo01m01sddcmgr	sfo01.rainpole.local	172.16.11.60	SDDC Manager	
	sfo01m01psc01	sfo01.rainpole.local	172.16.11.61	Platform Services Controller 01	
	sfo01m02psc02	sfo01.rainpole.local	172.16.11.63	Platform Services Controller 02	
	sfo01m01vc01	sfo01.rainpole.local	172.16.11.63	vCenter Server	
	sfo01m01esx01	sfo01.rainpole.local	172.16.11.101	ESXi host 01	
	sfo01m01esx02	sfo01.rainpole.local	172.16.11.102	ESXi host 02	
	sfo01m01esx03	sfo01.rainpole.local	172.16.11.103	ESXi host 03	
	sfo01m01esx04	sfo01.rainpole.local	172.16.11.104	ESXi host 04	
	sfo01m01nsx01	sfo01.rainpole.local	172.16.11.64	NSX Manager	
	sfo01m01nsxc01		172.16.11.65	NSX Controller 01	
	sfo01m01nsxc02		172.16.11.66	NSX Controller 02	
	sfo01m01nsxc03		172.16.11.67	NSX Controller 03	
	VI Workload #1	sfo01w01vc01	sfo01.rainpole.local	172.16.11.68	vCenter Server
		sfo01w01esx01	sfo01.rainpole.local	172.16.17.101	ESXi host 01
sfo01w01esx02		sfo01.rainpole.local	172.16.17.102	ESXi host 02	
sfo01w01esx03		sfo01.rainpole.local	172.16.17.103	ESXi host 03	
sfo01w01esx04		sfo01.rainpole.local	172.16.17.104	ESXi host 04	
sfo01w01nsx01		sfo01.rainpole.local	172.16.11.69	NSX Manager	
sfo01w01nsxc01			172.17.17.120	NSX Controller 01	
sfo01w01nsxc02			172.17.17.121	NSX Controller 02	
sfo01w01nsxc03			172.17.17.122	NSX Controller 03	

Host Names and IP Addresses for the Operations Management Layer

The operations management layer focuses on the components used for day-to-day management of the Cloud Foundation environment.

Cloud Foundation automatically deploys vRealize Log Insight in the management domain during a deployment. Other components within the management domain are automatically configured to utilize this vRealize Log Insight instance. With the appropriate licensing in place, this vRealize Log Insight Instance can also be utilized by other workload domains. You must define the hostnames and IP addresses for the vRealize Log Insight components prior to beginning the deployment of Cloud Foundation.

Cloud Foundation automates the deployment of vRealize Operations. This optional component is deployed within the management domain. Deployment of vRealize Operations also deploys a virtual machine for vRealize Suite Lifecycle Manager (vRSLCM) and a edge device used for load balancing within the management domain. These two components are shared between vRealize Operations and vRealize Automation and are automatically installed if either product is deployed. Hostname and IP information is required to be defined for the vRealize Operations components to be installed within the solution and the shared components if not previously deployed.

The following table provides an example of the information to be collected for the operations management layer, including the shared components with vRealize Automation. If you are deploying both vRealize Operations and vRealize Automation, the shared components are only installed once. This example uses a fictional DNS domain called `rainpole.local` for illustration purposes. Modify the sample information to conform to your site's configuration.

Table 3-5. Sample Host Names and IP Addresses for Operations Management Layer

Component Group	Hostname	DNS Zone	IP Address	Description
vRealize Log Insight	sfo01vrli01	sfo01.rainpole.local	172.16.11.70	Virtual IP address of the vRealize Log Insight integrated load balancer
	sfo01vrli01a	sfo01.rainpole.local	172.16.11.71	Master node of vRealize Log Insight
	sfo01vrli01b	sfo01.rainpole.local	172.16.11.72	Worker node 1 of vRealize Log Insight
	sfo01vrli01c	sfo01.rainpole.local	172.16.11.73	Worker node 2 of vRealize Log Insight
vRealize Operations Manager (Optional)	vrops01svr01	rainpole.local	172.16.11.74	Virtual IP address of load balancer for the analytics cluster of vRealize Operations Manager
	vrops01svr01a	rainpole.local	172.16.11.75	Master node of vRealize Operations Manager
	vrops01svr01b	rainpole.local	172.16.11.76	Master replica node of vRealize Operations Manager
	vrops01svr01c	rainpole.local	172.16.11.77	Data node 1 of vRealize Operations Manager

Table 3-5. Sample Host Names and IP Addresses for Operations Management Layer (Continued)

Component Group	Hostname	DNS Zone	IP Address	Description
	vrslcm01	rainpole.local	172.16.11.7 8	vRealize Suite Lifecycle Manager (shared component with vRealize Automation)
	vredge01	rainpole.local	172.16.11.7 9	vRealize Edge load balancer (shared component with vRealize Automation)

Host Names and IP Addresses for the Cloud Management Layer

If you plan to have Cloud Foundation automate the deployment of vRealize Automation for cloud management, you must define hostnames and IPs prior to deployment.

vRealize Automation requires specific external services to be available prior to deployment. This includes a Microsoft SQL Server instance which can be deployed within the management domain or externally to the solution. Regardless of the location, vRealize Automation deployment requires the hostname and IP information for the SQL Server instance before beginning deployment. See "Deploy vRealize Automation in Cloud Foundation" in the *VMware Cloud Foundation Operations and Administration Guide*.

Deployment of vRealize Automation also deploys a virtual machine for vRealize Suite Lifecycle Manager (vRSLCM) and a edge device used for load balancing within the management domain. These two components are shared between vRealize Operations and vRealize Automation and are automatically installed if either product is deployed. Hostname and IP information is required to be defined for the vRealize Automation components to be installed within the solution and the shared components if not previously deployed.

During the deployment wizard for vRealize Automation, you are given the opportunity to select the number of nodes to be deployed. The samples shown within this document reflect a three node deployment. You will need to adjust accordingly if you deploy more than three nodes.

The following table provides an example of the information to be collected for the cloud management layer, including the shared components with vRealize Operations. If you deploy both vRealize Operations and vRealize Automation, the shared components are only installed once. This example uses a fictional DNS domain called `rainpole.local` for illustration purposes. Modify the sample information to conform to your site's configuration.

Table 3-6. Sample Hostnames and IP Addresses for the Cloud Management Layer

Component Group	Hostname	DNS Zone	IP Address	Description
vRealize Automation	vra01svr01	rainpole.local	172.16.11.80	Virtual IP address of the vRealize Automation Appliance
	vra01svr01a	rainpole.local	172.16.11.81	vRealize Automation Appliance
	vra01svr01b	rainpole.local	172.16.11.82	vRealize Automation Appliance
	vra01svr01c	rainpole.local	172.16.11.83	vRealize Automation Appliance
	vra01iws01	rainpole.local	172.16.11.84	Virtual IP address of the vRealize Automation IaaS Web Server

Table 3-6. Sample Hostnames and IP Addresses for the Cloud Management Layer (Continued)

Component Group	Hostname	DNS Zone	IP Address	Description
	vra01iws01a	rainpole.local	172.16.11.85	vRealize Automation IaaS Web Server
	vra01iws01b	rainpole.local	172.16.11.86	vRealize Automation IaaS Web Server
	vra01ims01	rainpole.local	172.16.11.87	Virtual IP address of the vRealize Automation IaaS Manager Service
	vra01ims01a	rainpole.local	172.16.11.88	vRealize Automation IaaS Manager Service and DEM Orchestrator
	vra01ims01b	rainpole.local	172.16.11.89	vRealize Automation IaaS Manager Service and DEM Orchestrator
	vra01dem01a	rainpole.local	172.16.11.90	vRealize Automation DEM Worker
	vra01dem01b	rainpole.local	172.16.11.91	vRealize Automation DEM Worker
	sfo01ias01a	sfo.rainpole.local	172.16.11.92	vRealize Automation Proxy Agent
	sfo01ias01b	sfo.rainpole.local	172.16.11.93	vRealize Automation Proxy Agent
	vrslcm01	rainpole.local	172.16.11.78	vRealize Suite Lifecycle Manager (shared component with vRealize Automation)
	vredge01	rainpole.local	172.16.11.79	vRealize Edge load balancer (shared component with vRealize Automation)
Microsoft SQL Server (external)	vra01mssql01	sfo.rainpole.local	10.0.0.10	Microsoft SQL Server for vRealize Automation

Capacity Planning for Management and Workload Domains

4

Before deploying Cloud Foundation, you must ensure that your environment has enough available compute and storage resources to accommodate the footprint of the management domain, any additional workload domains, and any optional components you plan to deploy.

Use the VMware Cloud Foundation Capacity Planner to assist you in identifying hardware to match your capacity requirements. See <https://vcf-planner.cfapps.io/>.

Note Storage footprint shows allocated space. Do not consider it if you use thin provisioning.

This chapter includes the following topics:

- [Virtual Infrastructure Layer Footprint](#)
- [Operations Management Layer Footprint](#)
- [Cloud Management Layer Footprint](#)

Virtual Infrastructure Layer Footprint

The resources required by the virtual infrastructure layer will vary depending on which deployment model you choose and the number of workload domains you plan to create.

The following table displays the amount of resources the virtual infrastructure layer components consume for a management domain and a single virtual infrastructure workload domain. Duplicate the resource consumption shown for each additional workload domain.

This table does not factor in additional storage requirements to account for availability or maintenance considerations. In a production environment, you need to account for adequate resources to allow for the failure of hosts, virtual machine snapshots, and backups.

It also does not consider additional workloads deployed to the virtual infrastructure layer outside of Cloud Foundation. This can include virtual machines you deploy that provide backup, antivirus, or other security services to the environment.

Table 4-1. Virtual Infrastructure Layer Footprint

Domain	Component	Operating System	vCPUs	Memory (GB)	Storage (GB)
Management	SDDC Manager	Virtual appliance	4	16	800
	vCenter Server	Virtual appliance	4	16	290
	Platform Services Controller	Virtual appliance	2	4	60
	Platform Services Controller	Virtual appliance	2	4	60
	NSX Manager	Virtual appliance	4	16	60
	NSX Controller 01	Virtual appliance	4	4	20
	NSX Controller 02	Virtual appliance	4	4	20
	NSX Controller 03	Virtual appliance	4	4	20
Virtual Infrastructure Workload #1	vCenter Server	Virtual appliance	8	24	400
	NSX Manager	Virtual appliance	4	16	60
	NSX Controller 01	Virtual appliance	4	4	20
	NSX Controller 02	Virtual appliance	4	4	20
	NSX Controller 03	Virtual appliance	4	4	20
TOTAL			52 vCPU	120 GB	1,850 GB

Operations Management Layer Footprint

The amount of resources required to support the operations management layer depends on the components installed.

A vRealize Log Insight instance is required and is automatically deployed as part of the management domain. Installation of vRealize Operations is optional.

Refer to the following table for information on the minimum resource requirements for the operations management layer components.

Table 4-2. Operations Management Layer Footprint

Product	Component	Operating System	vCPUs	Memory (GB)	Storage (GB)
	vRealize Operations Manager Analytics Node1	Virtual Appliance	8	32	1,024
vRealize Operations (Optional)	vRealize Operations Manager Analytics Node 2	Virtual Appliance	8	32	1,024
	vRealize Operations Manager Analytics Node 3	Virtual Appliance	8	32	1,024
	vRealize Log Insight Node 1	Virtual Appliance	8	16	1,312
	vRealize Log Insight Node 2	Virtual Appliance	8	16	1,312
	vRealize Log Insight Node 3	Virtual Appliance	8	16	1,312
TOTAL			48 vCPU	144 GB	7,008 GB

Cloud Management Layer Footprint

vRealize Automation is an optional component that can be deployed as part of the cloud management layer.

During the deployment wizard for vRealize Automation, you are given the opportunity to select the number of nodes to be deployed. The samples shown within this document reflect a three node deployment. You will need to adjust accordingly if you deploy more than three nodes.

The following table depicts the resources required to support the deployment of vRealize Automation.

Note Not all of the components listed need to consume resources within the Cloud Foundation environment. The Microsoft SQL server instance can be deployed within the management domain or at an external location accessible over the network. Review the vRealize Automation documentation (<https://docs.vmware.com/en/vRealize-Automation/index.html>) for more information on the resource requirements.

Table 4-3. Cloud Management Layer Footprint

Product	Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
vRealize Automation	vRealize Automation Appliance 1	Virtual Appliance	4	18	140
	vRealize Automation Appliance 2	Virtual Appliance	4	18	140
	vRealize Automation Appliance 3	Virtual Appliance	4	18	140
	vRealize Automation IaaS Web Server	Windows VM	2	8	60

Table 4-3. Cloud Management Layer Footprint (Continued)

Product	Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
	vRealize Automation IaaS Manager Server 1	Windows VM	2	8	60
	vRealize Automation IaaS Manager Server 2	Windows VM	2	8	60
	vRealize Automation DEM Worker 1	Windows VM	2	8	60
	vRealize Automation DEM Worker 2	Windows VM	2	8	60
	vRealize Automation Proxy Agent 1	Windows VM	2	8	60
	vRealize Automation Proxy Agent 2	Windows VM	2	8	60
	Microsoft SQL Server (external)	Windows VM	8	16	200
	Total		34 vCPU	126 GB	1,040 GB

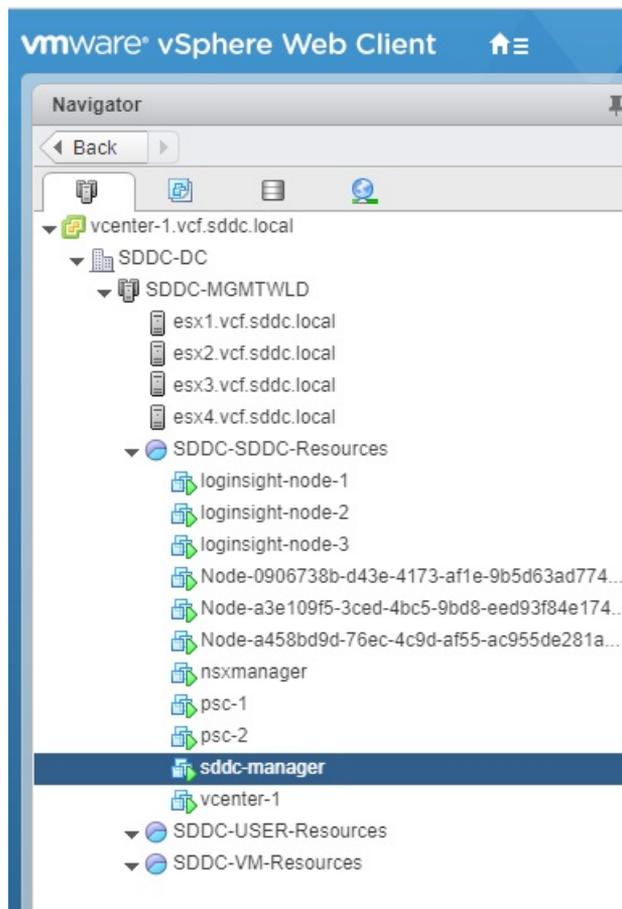
Virtual Machine Placement

Administrators familiar with vSphere will benefit from being able to visualize the placement of the deployed virtual machines.

This section provides some examples of various basic configurations.

Management Domain

This example illustrates the environment after the initial deployment of VMware Cloud Foundation. The configuration shown depicts four hosts, which are contained in a cluster. These four hosts make up the management domain. No other workload domains have been deployed.



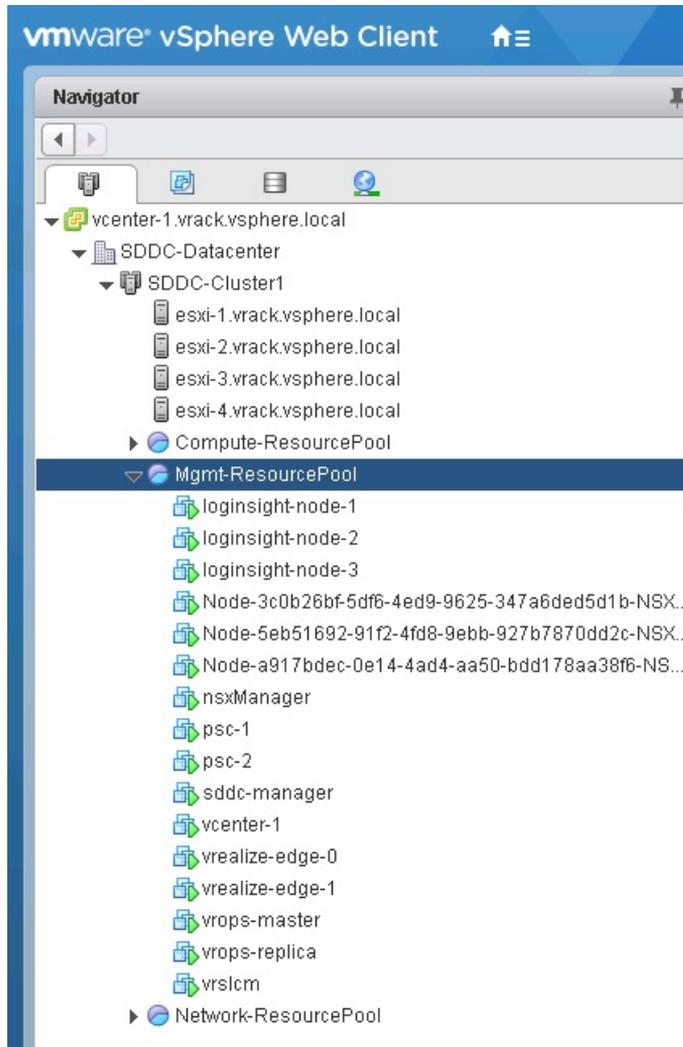
Within this cluster are a series of virtual machines that have been automatically deployed by Cloud Foundation. These include:

- SDDC Manager
- vCenter Server
- Platform Services Controllers
- NSX Manager
- NSX Controllers
- vRealize Log Insight

This example could provide the basis for either a consolidated or standard deployment architecture. If this was a consolidated deployment, the resource pools shown would be used to separate tenant workloads from the infrastructure workloads. If this was a standard deployment model, additional workload domains would be added and additional components would be automatically deployed.

Management Domain with vRealize Operations

This example illustrates a Cloud Foundation environment that consists of a management domain after an automated deployment of vRealize Operations Manager. No additional workload domains have been added in this example.

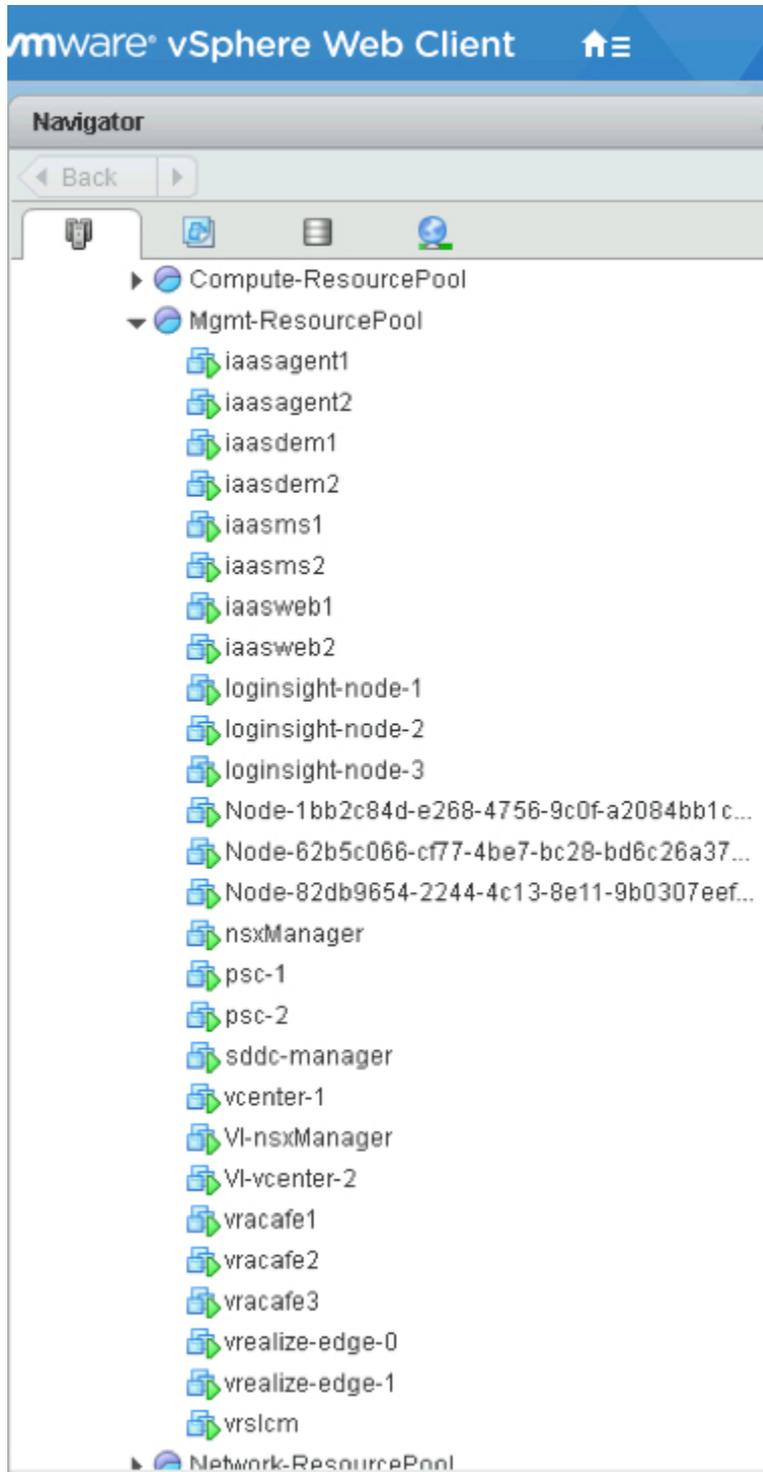


The deployment of vRealize Operations Manager within the environment is optional. In this example, vRealize Operations Manager was deployed with two nodes. You can define the number of nodes to be deployed as part of vRealize Operations Manager. See the *VMware Cloud Foundation Operations and Administration Guide* for more information on deploying vRealize Operations Manager within Cloud Foundation.

In the example, you can see the vRealize Operations Manager components that were deployed, including the vRealize Life Cycle Management (VRLCM) appliance and the NSX edge devices. These components are shared with vRealize Automation and are only deployed once, even if you deploy both vRealize Operations Manager and vRealize Automation.

Multiple Workload Domains with vRealize Automation

This example includes a management domain and a VI workload domain. In this scenario, there are multiple vCenter Servers and NSX managers deployed; one instance each for the management domain and the VI workload domain.



In addition, vRealize Automation has been deployed. Deploying vRealize Automation is optional. A vRealize Life Cycle Management (VRLCM) appliance and NSX edge devices are deployed for vRealize Automation. These components are shared with vRealize Operations and are only deployed once, even if you deploy both vRealize Operations Manager and vRealize Automation.

Note vRealize Automation requires a Microsoft SQL server. Although it can be installed within the management domain, it is an external component and can exist outside of the VMware Cloud Foundation environment, as long as it is reachable over the network. IN this example, the Microsoft SQL server is not installed in the management domain.
