VMware Cloud Foundation Planning and Preparation Guide

VMware Cloud Foundation 3.8

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

Contents

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 5 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 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 that 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 must 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 in the management domain. 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	■ Four vSAN ReadyNodes For information on compatible vSAN ReadyNodes, see the VMware Compatibility Guide.
CPU per server	Aligns with minimum requirements for vSAN ReadyNodes. For more information, refer to the VMware vSAN Documentation.

Table 1-1. Minimum Hardware Requirements for the Management Cluster (continued)

Component	Requirements
Memory per server	■ 192 GB
Storage per server	Aligns with minimum requirements for vSAN ReadyNodes. For more information, refer to the VMware vSAN Documentation.
NICs per server	■ Two 10 GbE (or faster) NICs (IOVP Certified) ■ (Optional) One 1 GbE BMC NIC **Note** Servers cannot have more than two NICs for primary communication, plus one BMC NIC for out-of-band host management.

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 use vSphere High Availability (HA) to coordinate the failover to other servers if there is 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, consider a VI workload domain that has two clusters:

- All servers in Cluster 1 must be homogeneous.
- All servers in 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 for vSAN backed VI workload domains. Refer to https://kb.vmware.com/s/article/52084 for guidance on what components can be modified in a vSAN ReadyNode. For NFS backed workload domains, you can use vSAN ReadyNodes or servers compatible with the vSphere version included with the Cloud Foundation Bill of Materials (BOM).

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	■ For vSAN backed VI workload domains, three compatible vSAN ReadyNodes are required. For information about compatible vSAN ReadyNodes, see the VMware Compatibility Guide. ■ For NFS backed VI workload domains, three servers compatible with the vSphere version included with the Cloud Foundation BOM are required. For information about the BOM, see the *Cloud Foundation Release Notes*. For compatible servers, see the VMware Compatibility Guide. Servers within a cluster must be of the same model and type.
CPU, memory, and storage per server	■ For vSAN backed VI workload domains, supported vSAN configurations are required. ■ For NFS backed VI workload domains, configurations must be compatible with the vSphere version included with the Cloud Foundation BOM. For information about the BOM, see the *Cloud Foundation Release Notes*.
NICs per server	■ Two 10 GbE (or faster) NICs (IOVP Certified) ■ (Optional) One 1 GbE BMC NIC **Note** Servers can have a maximum of two NICs for primary communication, plus one BMC NIC for out-of-band host management.

Storage Options

VMware Cloud Foundation uses and is validated against vSAN and NFSv3. The management domain uses vSAN for storage. You can use vSAN or NFSv3 for VI workload domains. The type of storage used by a VI workload domain is defined when the VI workload domain is created. After the VI workload domain is created and the storage type has been selected, you cannot change to another storage type. The storage type selected during the VI workload domain creation applies to all clusters that are created within the VI workload domain.

You must configure a network pool for the desired storage type before you create the VI workload domain.

If using vSAN 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 that the hardware is updated to supported levels before starting the deployment.

Networking Platform Options

The management domain includes NSX for vSphere. For VI workload domains, you can select either NSX for vSphere or NSX-T.

Software Requirements

2

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 Builder VM Support

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

The Cloud Builder VM takes your configuration inputs and provides the automated workflows that instantiate the management domain. The host for the Cloud 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 Builder VM through your MyVMware account.

The Cloud Builder VM requires the following resources.

Table 2-1. Cloud Builder VM Resource Requirements

Component	Requirement
CPU	4 vCPUs
Memory	4 GB
Storage	350 GB

The Cloud 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 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 Builder VM must be the same as the settings configured on the hosts.

VMware Imaging Appliance

The Cloud Builder VM includes the VMware Imaging Appliance (VIA). You can use VIA to install ESXi and VIBs on servers for use in the management domain and VI workload domains. Using VIA is optional, and if your servers are already installed with a supported version of ESXi, you do not need to use VIA.

You can use VIA to image servers prior to bring-up of a Cloud Foundation system and to image additional servers post-bring-up.

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 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 2016 Standard (64-bit)
		Microsoft	SQL Server	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. The license keys must match with the version of the product installed. See the Bill of Materials (BOM) in the VMware Cloud Foundation Release Notes for information on the specific product versions supported in each release.

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 NSX-T uses an evaluation license for 60 days. After that time period, a license is required.
- VMware vRealize Log Insight
- VMware vRealize Automation (optional); you can also use a vRealize Suite or vCloud Suite license key.
- VMware vRealize Operations (optional); you can also use a vRealize Suite or vCloud Suite license key.

Note Although part of the platform deployed by Cloud Foundation, vCenter Server is sold and licensed separately and you must provide a separate vCenter Server license for Cloud Foundation. Only one vCenter Server license is needed per Cloud Foundation instance, regardless of the number of workload domains in the environment.

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.

Port Requirements

3

This section lists the firewall ports required to access Cloud Foundation.

Cloud Foundation Builder

Table 3-1. Inbound Ports

Port	Protocol	Description
22	TCP	SSH access to vSphere components
67	TCP/UDP	VIA - DHCP server on Cloud Foundation Builder
8445	TCP	VIA UI
9080	TCP	Bring-up APIs

Table 3-2. Outbound Ports

Port	Protocol	Description	Notes
22	TCP	SSH to all ESXi hosts and vRealize network	Two dynamic ports are selected from the range for `mountd` and `statd`
53	TCP/UDP	DNS name resolution	
68	TCP/UDP	ESXi hosts	
123	TCP/UDP	Time sync on Cloud Foundation Builder	
443	TCP	Bring-up - vSphere API	
902	TCP	Bring-up - OVF deploy	
123	NTP	Upstream NTP	

SDDC Manager

Table 3-3. Inbound Ports

Port	Protocol	Description
22	TCP	SSH access into SDDC Manager
111	TCP/UDP	RPC - for NFS server on SDDC Manager
123	TCP/UDP	Time sync - NTP server on SDDC Manager
135	TCP	DCE RPC Daemon (dcerpcd)
443	TCP	Access to SDDC Manager UI
2020	TCP	VMware Authentication Service (vmafdd)

Table 3-3. Inbound Ports (continued)

Port	Protocol	Description
2049	TCP/UDP	NFS Daemon (nfsd) This daemon is used for client file-system requests.
4045	TCP/UDP	NFS Lock Manager (lockd) This daemon is used for record-locking operations on NFS files. It sends and manages locking requests from the client to the NFS server.
32766	TCP/UDP	NFS RPC Listen (statd) This daemon works with (lockd) to provide crash and recovery functions for the lock manager.
32767	TCP/UDP	NFS (mountd) This is a remote procedure call (RPC) server that handles file-system mount requests from remote systems and provides access control.

Table 3-4. Outbound Ports

Port	Protocol	Description
22	TCP	SSH
53	TCP/UDP	DNS
123	TCP/UDP	NTP
443	TCP	HTTPS
514	UDP	Syslog output to vRealize Log Insight
9000	TCP	vRealize Log Insight agent to access vRealize Log Insight

External Services

4

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

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 4-1. 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.

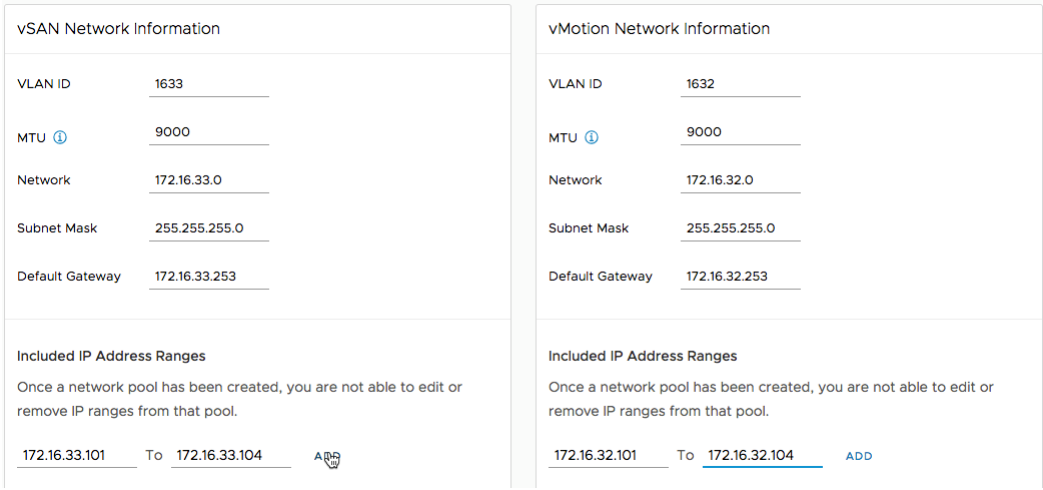
Prior to deploying Cloud Foundation, configure your physical network to enable the following functionality.

- 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, NFS, and vMotion.

Cloud Foundation uses an Internet Protocol Address Management (IPAM) solution to automate the IP configuration of VMkernel ports for vMotion, vSAN, and NFS (depending on the storage type being used). A network pool contains network information details for each network. For example:



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 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 4-2. 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
		VXLAN (NSX VTEP)	1614	172.16.14.0/24	172.16.14.253
		vRealize Suite	1616	172.16.16.0/24	172.16.16.253

Table 4-2. Sample VLAN and IP Subnet Configuration (continued)

Workload Domain	Cluster	VLAN Function	VLAN ID	Subnet	Gateway
		Uplink 1	2711	172.27.11.0/24	172.27.11.253
		Uplink 2	2712	172.27.12.0/24	172.27.12.253
VI Workload #1 (NSX for vSphere)	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 1	1716	173.17.15.0/24	173.17.15.253
		Uplink 2	1717	173.17.16.0/24	173.17.16.253
	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 1	1816	174.18.15.0/24	174.18.15.253
		Uplink 2	1817	174.18.16.0/24	174.18.16.253
VI Workload #2 (NSX-T with shared NSX-T Edge cluster)	cluster-01	Management (ESXi)	1911	175.19.11.0/24	175.19.11.253
		vSphere vMotion	1912	175.19.12.0/24	175.19.12.253
		vSAN	1913	175.19.13.0/24	175.19.13.253
		Hosts TEP	1914	175.19.14.0/24	175.19.14.253
		NSX-T Edge TEP	1915	175.19.15.0/24	175.19.15.253
		NSX-T Edge Uplink 1	1916	175.19.16.0/24	175.19.16.253
		NSX-T Edge Uplink 2	1917	175.19.17.0/24	175.19.17.253

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, if any, between the networks should be disabled or configured per the Cloud Foundation documentation.

The first NSX-T VI workload domain needs additional VLANs for the NSX-T Edge cluster, which is shared among the other NSX-T VI workload domains. Subsequent NSX-T workload domains will not need these VLANs.

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, for example, vRealize Operations.
- Cloud management layer: Services that consume the infrastructure layer resources, for example, vRealize Automation.

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 4-3. 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

Table 4-3. Sample External Services Hostname and IP Information (continued)

Component Group	Hostname	DNS	IP Address	Description
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 `rainpole.local` 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 sfo01 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 4-4. 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-V Manager

Table 4-4. Sample Host Names and IP Addresses for the Virtual Infrastructure Layer (continued)

Workload Domain	Hostname	DNS Zone	IP Address	Description
	sfo01m01nsxc01		172.16.11.65	NSX-V Controller 01
	sfo01m01nsxc02		172.16.11.66	NSX-V Controller 02
	sfo01m01nsxc03		172.16.11.67	NSX-V Controller 03
	sfo01w01vc01	sfo01.rainpole.local	172.16.11.68	Additional vCenter Server for VI Workload #1
	sfo01w01nsx01	sfo01.rainpole.local	172.16.11.69	Additional NSX-V Manager for VI Workload #1
	sfo01w02vc01	sfo01.rainpole.local	172.16.11.70	Additional vCenter Server for VI Workload #2
	sfo01w02nsx01	sfo01.rainpole.local	172.16.11.71	NSX-T Manager for Workload #2
	sfo01w02nsxc01		172.16.11.120	NSX-T Controller 01 for Workload #2
	sfo01w02nsxc02		172.16.11.121	NSX-T Controller 02 for Workload #2
	sfo01w02nsxc03		172.16.11.122	NSX-T Controller 03 for Workload #2
VI Workload #1 (NSX for vSphere)	sfo01w01esx01	sfo01.rainpole.local	172.16.17.101	ESXi host 05
	sfo01w01esx02	sfo01.rainpole.local	172.16.17.102	ESXi host 06
	sfo01w01esx03	sfo01.rainpole.local	172.16.17.103	ESXi host 07
	sfo01w01esx04	sfo01.rainpole.local	172.16.17.104	ESXi host 08
	sfo01w01nsxc01		172.17.17.120	NSX-V Controller 01
	sfo01w01nsxc02		172.17.17.121	NSX-V Controller 02
	sfo01w01nsxc03		172.17.17.122	NSX-V Controller 03
VI Workload #2 (NSX-T)	sfo01w02esx01	sfo01.rainpole.local	172.16.18.101	ESXi host 09
	sfo01w02esx02	sfo01.rainpole.local	172.16.18.102	ESXi host 10
	sfo01w02esx03	sfo01.rainpole.local	172.16.18.103	ESXi host 11
	sfo01w02esx04	sfo01.rainpole.local	172.16.18.104	ESXi host 12
	sfo01w02nsxe01	sfo01.rainpole.local	172.16.18.201	NSX-T Edge 01
	sfo01w02nsxe02	sfo01.rainpole.local	172.16.18.202	NSX-T Edge 02

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. In order to deploy vRealize Operations, you must first deploy vRealize Suite Lifecycle Manager. When you deploy vRealize Automation or vRealize Operations, Cloud Foundation deploys an NSX Edge used to load balance vRealize Suite product services within the management domain. vRealize Suite Lifecycle Manager and the NSX Edge are shared between vRealize Automation and vRealize Operations. You must define hostname and IP information for the vRealize Operations components to be installed within the solution and the shared components if not previously deployed.

vRealize Operations and vRealize Automation are not supported for NSX-T workload domains yet.

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 4-5. Sample Host Names and IP Addresses for Operations Management Layer

Component Group	Hostname	DNS Zone	IP Address	Network	Description
vRealize Log Insight	sfo01vrli01	sfo01.rainpole.local	172.16.11.70	Management	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	172.16.16.74	vRealize	Virtual IP address of load balancer for the analytics cluster of vRealize Operations Manager
	vrops01svr01a	rainpole.local	172.16.16.75		Master node of vRealize Operations Manager
	vrops01svr01b	rainpole.local	172.16.16.76		Master replica node of vRealize Operations Manager
	vrops01svr01c	rainpole.local	172.16.16.77		Data node 1 of vRealize Operations Manager

Table 4-5. Sample Host Names and IP Addresses for Operations Management Layer (continued)

Component Group	Hostname	DNS Zone	IP Address	Network	Description
	vrslcm01svr01a	rainpole.local	172.16.16.78		vRealize Suite Lifecycle Manager (shared component with vRealize Automation)
	sfo01m01lb01	rainpole.local	172.16.16.79		vRealize Edge load balancer (shared component with vRealize Automation)

Host Names and IP Addresses for the Cloud Management Layer

Before you add vRealize Automation to Cloud Foundation you must prepare the host names and IP addresses for the each of the vRealize Automation components. Each must be added in DNS with a fully qualified domain name (FQDN) that maps the host name to the IP address.

Ensure that you create the prerequisite forward (A) and reverse (PTR) DNS records for vRealize Automation and its shared components.

Note Before you can deploy vRealize Automation, you must deploy vRealize Suite Lifecycle Manager. When you deploy vRealize Automation or vRealize Operations, Cloud Foundation deploys an NSX Edge used to load balance vRealize Suite product services within the management domain. vRealize Suite Lifecycle Manager and the NSX Edge are shared between vRealize Automation and vRealize Operations.

The following components require host names and IP addresses:

- All vRealize Automation virtual appliances and vRealize Automation IaaS virtual machines.

  Important Host names for IaaS VMs should be 15 characters or less due to limitations in the Windows OS. If the host names are longer they will be trimmed during the installation and installation will fail.

- Microsoft SQL Server for the vRealize Automation IaaS database server instance.

  For more infomation, see Configure Microsoft SQL Server for vRealize Automation .

- The NSX Edge used to load balance vRealize Suite product services.

  This is required only if you have not previously configured it for use with vRealize Operations in your Cloud Foundation system.

- All vRealize Automation virtual servers configured on the NSX Edge load balancer.
- vRealize Suite Lifecycle Manager virtual appliance.

  This is required only if you have not previously configured it for use with vRealize Operations in your Cloud Foundation system.

The following table provides an example of the information to be collected for the cloud management layer. For illustration purposes, this example uses a fictional DNS root domain named `rainpole.local`. Modify the example information for your organization's configuration.

Table 4-6. Example Host Names and IP Addresses for vRealize Automation

Component Group	Hostname	DNS Zone	IP Address	Network	Description
vRealize Automation	vra01svr01	rainpole.local	172.16.16.80	vRealize	Virtual IP address of the vRealize Automation Appliance
	vra01svr01a	rainpole.local	172.16.16.81		vRealize Automation Appliance
	vra01svr01b	rainpole.local	172.16.16.82		vRealize Automation Appliance
	vra01svr01c	rainpole.local	172.16.16.83		vRealize Automation Appliance
	vra01iws01	rainpole.local	172.16.16.84		Virtual IP address of the vRealize Automation IaaS Web Servers
	vra01iws01a	rainpole.local	172.16.16.85		vRealize Automation IaaS Web Server
	vra01iws01b	rainpole.local	172.16.16.86		vRealize Automation IaaS Web Server
	vra01ims01	rainpole.local	172.16.16.87		Virtual IP address of the vRealize Automation IaaS Manager Service
	vra01ims01a	rainpole.local	172.16.16.88		vRealize Automation IaaS Manager Service and DEM Orchestrator
	vra01ims01b	rainpole.local	172.16.16.89		vRealize Automation IaaS Manager Service and DEM Orchestrator
	vra01dem01a	rainpole.local	172.16.16.90		vRealize Automation DEM Worker
	vra01dem01b	rainpole.local	172.16.16.91		vRealize Automation DEM Worker
	sfo01ias01a	rainpole.local	172.16.11.92	Management	vRealize Automation Proxy Agent
	sfo01ias01b	rainpole.local	172.16.11.93		vRealize Automation Proxy Agent
	vrslcm01svr01a	rainpole.local	172.16.16.78	vRealize	vRealize Suite Lifecycle Manager (Shared component with vRealize Automation and vRealize Operations)
	sfo01m01lb01	rainpole.local	172.16.16.79		NSX Edge Load Balancer (Shared component with vRealize Automation and vRealize Operations)
Microsoft SQL Server	vra01mssql01	rainpole.local	10.0.0.10	Any accessible network	Microsoft SQL Server for vRealize Automation

Requirements for vRealize Automation

Before you begin the procedure to add vRealize Automation to Cloud Foundation, plan for and verify that the following configurations are established in addition to the prerequsites for both the VLANs and IP subnets and the host names and IP addresses.

Active Directory Service Accounts for vRealize Automation

Before you deploy and configure vRealize Automation in Cloud Foundation, you must provide specific configuration for an Active Directory user. This user acts as a service account for authentication in cross-application communication.

The service account provides non-interactive and non-human access to services and APIs to the vRealize Automation components of Cloud Foundation.

The service account is a standard Active Directory account that you configure in the following way:

- The password never expires.
- The user cannot change the password.

Source	Destination	Description	Required Role
vRealize Automation	Active Directory	Service account for performing Active Directory domain join operations for computer accounts used by vRealize Automation IaaS components.	■ Account Operators Group ■ Delegation to Join Computers to Active Directory Domain
vRealize Automation	■ vRealize Automation ■ Microsoft SQL Server	Service account for access from vRealize Automation to vCenter Server and the Microsoft SQL Server instance.	■ Administrator ■ vRealize Orchestrator Administrator

Note Delegation to Join Computers to Active Directory Domain is only required to deploy vRealize Automation. After deployment, it is no longer required.

Certificates for vRealize Automation

Before you add vRealize Automation to Cloud Foundation, you must prepare the certificates for the vRealize Automation components. In the vRealize Automation installation wizard, you will provide the certificates signed by a certificate authority (CA) that will be used for the vRealize Automation deployment.

- If using Microsoft CA-signed certificates for vRealize Automation in Cloud Foundation, verify that the certificate service template is properly configured for basic authentication.

Create and Add a Microsoft Certificate Authority Template

If your organization plans to use a Microsoft Certificate Authority instead of an external third party certificate authority, you must set up the Microsoft Certificate Authority template on the Microsoft Certificate Authority servers. The template contains the certificate authority (CA) attributes for signing

certificates for the Cloud Foundation solutions. After you create the new template, you add it to the certificate templates in the Microsoft Certificate Authority.

Setting up a Microsoft Certificate Authority template involves creating a template and then adding that template to the certificate templates of the Microsoft Certificate Authority.

Procedure

1. Log in to the Microsoft Certificate Authority server by using a Remote Desktop Protocol (RDP) client.
2. Click **Windows Start** > **Run**, enter `certtmpl.msc`, and click **OK**.
3. On the **Certificate Template Console**, under **Template Display Name**, right-click **Web Server** and click **Duplicate Template**.
4. In the **Properties of New Template** dialog box, leave **Windows Server 2003** selected for backward compatibility.
5. Click the **General** tab.
6. In the **Template display name** text box, enter `VMware` as the name of the new template.
7. Click the **Extensions** tab and specify extensions information.
   a. Select **Application Policies** and click **Edit**.
   b. Select **Server Authentication**, click **Remove**, and click **OK**.
   c. Select **Client Authentication**, click **Remove**, and click **OK**.

      If **Client Authentication** does not appear in **Application Policies**, then you can skip this step.
   d. Select **Key Usage** and click **Edit**.
   e. Select the **Signature is proof of origin (nonrepudiation)** check box.
   f. Leave the default for all other options. Click **OK**
8. Click the **Subject Name** tab, ensure that the **Supply in the request option** is selected, and click **OK** to save the template.
9. To add the new template to your Microsoft Certificate Authority, click **Windows Start** > **Run**, enter `certsrv.msc`, and click **OK**
10. In the **Certification Authority** window, expand the left pane if it is collapsed.
11. Right-click **Certificate Templates** and select **New** > **Certificate Template to Issue**.
12. In the **Name** column of the **Enable Certificate Templates** dialog box, select the **VMware** certificate that you created and click **OK**.

Generating Certificates for vRealize Automation

Before you can deploy vRealize Automation for use with Cloud Foundation, you must generate certificates for all the vRealize Automation components. In the vRealize Automation installation wizard, you will provide the certificates signed by a certificate authority (CA) that will be used for the vRealize Automation deployment.

vRealize Automation supports certificates that are signed by a Microsoft Certificate Authority, as well as certificates that are signed by a non-Microsoft Certificate Authority. The procedure for generating certificates varies depending on the Certificate Authority that you are using in your environment.

Generate vRealize Automation Certificates for Use with a Non-Microsoft Certificate Authority

Use the SDDC Manager VM to generate a certificate request and private key. Your Certificate Authority uses the certificate request to generate a certificate you can use when you deploy vRealize Automation.

Procedure

1. Using SSH, log in to the SDDC Manager VM with the user name `vcf` and password you specified in the deployment parameter sheet.
2. Enter **`su`** and the password you specified in the deployment parameter sheet.
3. Navigate to the `/opt/vmware/vcf/operationsmanager/scripts/cli` directory.
4. Run the following command.

   ```
   ./generate_certificate.sh
   ```
5. Enter **`1`** to generate a certificate signing request.
6. Press Enter to accept the default resource type (**`vra`**).
7. Enter the information for use with your certificate request.

   For example, Country Name, State or Province Name, and so on.
8. Enter the subject alternative names (SANs) for each of the vRealize Automation components.

   Add the FQDN and hostname for each component as a separate SAN entry.

Component	Sample SANs
vRealize Automation Appliance Load Balancer VIP	vra01svr01.rainpole.local
	vra01svr01
vRealize Automation Appliance	vra01svr01a.rainpole.local
	vra01svr01a
vRealize Automation Appliance	vra01svr01b.rainpole.local
	vra01svr01b
vRealize Automation Appliance	vra01svr01c.rainpole.local
	vra01svr01c
vRealize Automation IaaS Web Server VIP	vra01iws01.rainpole.local
	vra01iws01
vRealize Automation IaaS Web Server	vra01iws01a.rainpole.local
	vra01iws01a

Component	Sample SANs
vRealize Automation IaaS Web Server	vra01iws01b.rainpole.local
	vra01iws01b
vRealize Automation IaaS Manager Service VIP	vra01ims01.rainpole.local
	vra01ims01
vReaize Automation IaaS Manager Service and DEM Orchestrator	vra01ims01a.rainpole.local
	vra01ims01a
vReaize Automation IaaS Manager Service and DEM Orchestrator	vra01ims01b.rainpole.local
	vra01ims01b
vRealize Automation DEM Worker	vra01dem01a.rainpole.local
	vra01dem01a
vRealize Automation DEM Worker	vra01dem01b.rainpole.local
	vra01dem01b

9 Enter **done**.

```
Enter SAN : vra01dem01a
Enter SAN : vra01dem01b.rainpole.local
Enter SAN : vra01dem01b
Enter SAN : done
```

10 Enter the file path to copy the private key.

The default path is `/tmp/private_key.pem`.

11 Enter the file path to copy the csr file.

The default path is `/tmp/csr.pem`.

What to do next

Send the certificate signing request to your Certificate Authority to get a certificate. You will need the server certificate, root CA certificate, and your private key to deploy vRealize Automation.

Generate vRealize Automation Certificates for Use with a Microsoft Certificate Authority

Use the SDDC Manager VM to generate a certificate and private key. Use the certificate and private key when you deploy vRealize Automation.

Prerequisites

You have configured a Microsoft Certificate Authority. See "Configure Certificate Authority" in the *VMware Cloud Foundation Operations and Administration Guide*.

Procedure

1. Using SSH, log in to the SDDC Manager VM with the user name `vcf` and password you specified in the deployment parameter sheet.
2. Enter **`su`** and the password you specified in the deployment parameter sheet.
3. Navigate to the `/opt/vmware/vcf/operationsmanager/scripts/cli` directory.
4. Run the following command.

   ```
   ./generate_certificate.sh
   ```
5. Enter **`2`** to generate a certificate.
6. Press Enter to accept the default resource type (**`vra`**).
7. Enter the information for use with your certificate request.

   For example, Country Name, State or Province Name.
8. Enter the subject alternative names (SANs) for each of the vRealize Automation components.

   Add the FQDN and hostname for each component as a separate SAN entry.

Component	Sample SANs
vRealize Automation Appliance Load Balancer VIP	vra01svr01.rainpole.local
	vra01svr01
vRealize Automation Appliance	vra01svr01a.rainpole.local
	vra01svr01a
vRealize Automation Appliance	vra01svr01b.rainpole.local
	vra01svr01b
vRealize Automation Appliance	vra01svr01c.rainpole.local
	vra01svr01c
vRealize Automation IaaS Web Server VIP	vra01iws01.rainpole.local
	vra01iws01
vRealize Automation IaaS Web Server	vra01iws01a.rainpole.local
	vra01iws01a
vRealize Automation IaaS Web Server	vra01iws01b.rainpole.local
	vra01iws01b
vRealize Automation IaaS Manager Service VIP	vra01ims01.rainpole.local
	vra01ims01
vReaize Automation IaaS Manager Service and DEM Orchestrator	vra01ims01a.rainpole.local

Component	Sample SANs
	vra01ims01a
vReaize Automation IaaS Manager Service and DEM Orchestrator	vra01ims01b.rainpole.local
	vra01ims01b
vRealize Automation DEM Worker	vra01dem01a.rainpole.local
	vra01dem01a
vRealize Automation DEM Worker	vra01dem01b.rainpole.local
	vra01dem01b

9 Enter **done**.

```
Enter SAN : vra01dem01a
Enter SAN : vra01dem01b.rainpole.local
Enter SAN : vra01dem01b
Enter SAN : done
```

10 Enter the file path to copy the private key.

The default path is `/tmp/private_key.pem`.

11 Enter the file path to copy the csr file.

The default path is `/tmp/csr.pem`.

12 Enter the file path to copy the server certificate.

The default path is `/tmp/server.pem`.

13 Enter the file path to copy the root CA certificate.

The default path is `/tmp/rootca.pem`.

What to do next

Deploy vRealize Automation. You will need the private key, server certificate, and root CA certificate.

Configure Microsoft SQL Server for vRealize Automation

Before you deploy vRealize Automation in Cloud Foundation, configure the Microsoft SQL Server as a prerequisite.

Microsoft SQL Server Recommendations

vRealize Automation uses Microsoft SQL Server on Windows Server as the database management system (DBMS) to store data for the vRealize Automation IaaS components. The specific configuration of SQL Server for use in your environment is not addressed in this guide. High-level guidance is provided to ensure more reliable operation of your vRealize Automation deployment.

Review the vRealize Automation Support Matrix (PDF) for supported Microsoft SQL Sever versions for vRealize Automation.

Note If using Microsoft SQL Server 2016 or 2017, use 100 or 120 compatibility level.

To provide optimal performance for the vRealize Automation IaaS database, configure the Microsoft Windows Server virtual machine for Microsoft SQL Server with a minimum of 8 vCPU and 16 GB vRAM.

Microsoft SQL Server binaries should be installed in the operating system VMDK. Microsoft SQL Server, even if another drive is selected for binary installation, will still install components on the operating system drive. Separating Microsoft SQL Server installation files from data and transaction logs also provides better flexibility for backup, management, and troubleshooting.

Place Microsoft SQL Server data files (system and user), transaction logs, and backup files into separate VMDKs. For example:

- Operating System
- SQL User Database Data Files
- SQL User Database Log Files
- SQL TempDB
- SQL Backup Files

Utilize the VMware Paravirtualized SCSI (PVSCSI) Controller as the virtual SCSI Controller for data and log VMDKs. The PVSCSI Controller is the optimal SCSI controller for an I/O-intensive application on vSphere allowing not only a higher I/O rate but also lowering CPU consumption compared with the LSI Logic SAS. In addition, the PVSCSI adapters provide higher queue depth, increasing I/O bandwidth for the virtualized workload.

Use multiple PVSCSI adapters. VMware supports up to four (4) adapters per virtual machines and as many as necessary, up to this limit, should be leveraged. Placing operating system, data, and transaction logs onto a separate vSCSI adapter optimizes I/O by distributing load across multiple target devices and allowing for more queues on the operating system level. Consider distributing disks between controllers.

For more information, refer to the Architecting Microsoft SQL Server on VMware vSphere Best Practices Guide.

Assign the Server Role to vRealize Automation Service Account

Assign the Microsoft SQL Server **sysadmin** server role to the vRealize Automation service account.

vRealize Automation uses the Microsoft SQL Server **sysadmin** server role privilege to create and run scripts on the SQL Server database. By default, only users who are members of the **sysadmin** server role, or the **db_owner** and **db_ddladmin** database roles, can create objects in the database.

Procedure

1 Log in to the Microsoft SQL Server virtual machine as an administrative account by using a Remote Desktop Protocol (RDP) client.

2 From the **Start** menu, click **All Programs**, click **Microsoft SQL Server**, and click **SQL Server Management Studio**.

Note If Microsoft SQL Server Management Studio does not appear in your **All Programs** menu, the component might not have successfully installed. Verify that you have successfully installed Microsoft SQL Server Management Studio, and then continue with this procedure.

3 In the **Connect to Server** dialog box, leave the default value of the **Server Name** text box, select **Windows Authentication** from the **Authentication** drop-down menu, and click **Connect**.

Note During the Microsoft SQL Server installation, the **Database Engine** configuration wizard prompts you to provide the user name and password for the SQL Server administrator. If this user was not added during the installation, select **SQL Authentication** from the **Authentication** drop-down menu, and enter the user name **`sa`** in the **User name** text box, and the password ***`sa_password`*** in the **Password** text box.

4 In the **Object Explorer** pane, expand the server instance (for example, **vra01mssql01**).

5 Right-click the **Security** folder, click **New**, and click **Login**.

6 In the **Login Properties** dialog box, click the **General** page and enter the service account name (for example, **`rainpole\svc-vra`**) in the **Login name** text box.

7 Click the **Server Roles** page, select the **sysadmin** check box, and click **OK**.

Configure Network Access for Distributed Transaction Coordinator

Configure network access and security between vRealize Automation and your Microsoft SQL Server instance using Microsoft Distributed Transaction Coordinator (MSDTC). MSDTC coordinates transactions that update two or more transaction-protected resources, such as databases, message queues, file systems. These transaction-protected resources may be on a single computer, or distributed across many networked computers.

Procedure

1 Log in to the Microsoft SQL Server virtual machine as an administrative account using a Remote Desktop Protocol (RDP) client.

2 From the **Start** menu, click **Run**, type **`comexp.msc`** in the **Open** text box, and click **OK**.

The **Component Services** manager displays. Component Services lets you manage Component Object Model (COM+) applications.

3 In the navigation tree, select **Component Services > Computers > My Computer > Distributed Transaction Coordinator > Local DTC**.

4 Right-click **Local DTC** and click **Properties**.

The **Local DTC Properties** dialog box displays.

5 Click the **Security** tab in the **Local DTC Properties** dialog box.

6 In the **Security** tab, configure the following values, and click **OK**.

Setting	Value
Network DTC Access	Selected
Allow Remote Clients	Selected
Allow Remote Administration	Selected
Allow Inbound	Selected
Allow Outbound	Selected
Mutual Authentication Required	Selected
Enable XA Transactions	Deselected
Enable SNA LU 6.2 Transactions	Selected
Account	Leave the default setting (NT AUTHORITY\NetworkService)
Password	Leave blank

7 Click **Yes** to restart the MSDTC Service, click **OK** to confirm that the service has successfully restarted, and close the **Component Services** manager.

Allow Microsoft SQL Server and MSDTC Access through the Windows Firewall for vRealize Automation

Configure the Windows Firewall to allow inbound access for Microsoft SQL Server and the Microsoft Distributed Transaction Coordinator (MSDTC).

Procedure

1 Log in to the Microsoft SQL Server virtual machine with an administrative user by using a Remote Desktop Protocol (RCP) client.

2 From the **Start** menu, click **Run**, type `WF.msc` in the **Open** text box, and click **OK**.

The **Windows Firewall with Advanced Security** dialog box appears to configure firewall properties for each network profile.

3 Allow Access for Microsoft SQL Server on TCP Port 1433.

a In the navigation pane, under **Windows Firewall with Advanced Security**, select and right-click **Inbound Rules**, and click **New Rule** in the action pane.

The **New Inbound Rule Wizard** appears.

b On the **Rule Type** page of the **New Inbound Rule Wizard**, select the **Port** radio button, and click **Next**.

c On the **Protocol and Ports** page, select **TCP** and enter the port number `1433` in the **Specific local ports** text box, and click **Next**.

d On the **Action** page, select **Allow the connection**, and click **Next**.

e On the **Profile** page, select the **Domain**,**Private**, and **Public** profiles, and click **Next**.

f On the **Name** page, enter a **Name** and a **Description** for this rule, and click **Finish**.

4 Allow access for Microsoft Distributed Transaction Coordinator.

a In the navigation pane, under **Windows Firewall with Advanced Security**, select and right-click **Inbound Rules**, and click **New Rule** in the action pane.

b On the **Rule Type** page click **Predefined**, click **Distributed Transaction Coordinator**, and click **Next**.

c On the **Predefined Rules** page, select all rules for **Distributed Transaction Coordinator (RPC-EPMAP)**, **Distributed Transaction Coordinator (RPC)**, **Distributed Transaction Coordinator (TCP-In)**, and click **Next**.

d On the **Action** page, select **Allow the connection**, and click **Finish**.

5 Exit the **Windows Firewall with Advanced Security** wizard.

6 Right click **Powershell**, select **Run as Administrator**, and run the following commands. These commands adjust the **User Account Controls**, disable IPv6, and restart the server to activate these changes.

Command
`set-ItemProperty -Path "HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\System" -Name "EnableLUA" -Value "0"`
`set-ItemProperty -Path "HKLM:\System\CurrentControlSet\Services\TCPIP6\Parameters" -Name "DisabledComponents" -Value 0xff`
`Restart-Computer`

Configure a Microsoft SQL Server Database for vRealize Automation IaaS Components

Create and configure the Microsoft SQL Server database for the vRealize Automation IaaS Components.

Prerequisites

- A supported version of Microsoft SQL Sever for vRealize Automation is installed per the vRealize Automation Support Matrix (PDF).
- The vRealize Automation service account has been added to Microsoft SQL Server with the **sysadmin** server role.
- Microsoft Distributed Transaction Coordinator has been configured.
- The Windows Firewall inbound access has been configured for Microsoft SQL Server (TCP port 1433) and the Microsoft Distributed Transaction Coordinator.

Procedure

1 Log in to the Microsoft SQL Server virtual machine as an administrative account by using a Remote Desktop Protocol (RDP) client.

2 From the **Start** menu, click **All Programs**, click **Microsoft SQL Server**, and click **SQL Server Management Studio**.

Note If Microsoft SQL Server Management Studio does not appear in your **All Programs** menu, the component might not have successfully installed. Verify that you have successfully installed Microsoft SQL Server Management Studio, and then continue with this procedure.

3 In the **Connect to Server** dialog box, leave the default value of the **Server Name** text box, select **Windows Authentication** from the **Authentication** drop-down menu, and click **Connect**.

Note During the Microsoft SQL Server installation, the **Database Engine** configuration wizard prompts you to provide the user name and password for the SQL Server administrator. If this user was not added during the installation, select **SQL Authentication** from the **Authentication** drop-down menu, and enter the user name **`sa`** in the **User name** text box, and the password ***`sa_password`*** in the **Password** text box.

4 In the **Object Explorer** pane, right-click **Databases** and choose **New Database**.

5 The **New Database** dialog box, select the **General** tab and enter the database name, for example, **`vRADB01`**.

6 Set **Database Owner** to the same value as the service user name, for example **`svc-vra`**.

7 Select the **Options** tab and configure the following settings:

a Set **Recovery Model** option to **`Simple`**.

b If using Microsoft SQL Server 2016 or 2017, set **Compatibility Level** as 100 or 120.

c Under **Other options**, change the **Allow Snapshot Isolation** option to **true**.

d Under **Other options**, change the **Is Read Committed Snapshot** option to **true**.

8 Click **OK**.

Prepare the IaaS Windows Server OVA Template for vRealize Automation

Before you deploy vRealize Automation in Cloud Foundation, prepare a Microsoft Windows Server OVA template for the vRealize Automation IaaS components.

Creation of the Microsoft Windows Server OVA template is one of the prerequisites for deploying vRealize Automation in Cloud Foundation, as described in the *VMware Cloud Foundation Operations and Administration Guide*.

Prerequisites

- Verify that you have a Microsoft Windows Server virtual machine to serve as the template for the vRealize Automation IaaS components. It must have the following configuration:

Attribute	Value	
Operating System	Microsoft Windows Server 2016 (64-bit)	
vCPU	Two	
Memory	8 GB	
Disk	50 GB LSI	
Network	VMXNET3	
Other	**Browser**	In Internet Explorer, disable the Enhanced Security Configuration feature.
	Remote Desktop	Enable Remote Desktop Connections.

- Verify that the virtual machine is not joined to Active Directory.
- Verify that you can access and download Java Runtime Environment (JRE) executable: `jre-8u201-windows-x64.exe` or later version.

Procedure

- On the Microsoft Windows Server virtual machine, launch the PowerShell console as an administrator and run the following commands:
  a Set the PowerShell Execution Policy

```
Set-ExecutionPolicy Unrestricted
```

  b Disable User Account Control (UAC)

```
Set-ItemProperty -Path 'HKLM:\Software\Microsoft\Windows\CurrentVersion\Policies\System' -
Name 'EnableLUA' 0
```

  c Disable IPv6

```
Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Services\TCPIP6\Parameters' -Name
'DisabledComponents' -Value 0xff
```

- Download and install Java Runtime Environment version 1.8 Update 201 or later (64-bit) on the Microsoft Windows Server virtual machine.

  Note The Microsoft Windows Server virtual machine in this deployment was tested with Java Runtime Environment `jre-8u201-windows-x64.exe`. Use this version or later.

- Configure *JAVA_HOME* on the Microsoft Windows Server virtual machine.
  a Click **Start** and enter **`sysdm.cpl`** to open the **System Properties** dialog box.
  b Select the **Advanced** tab and click **Environment Variables**.

c Under **System Variables**, click **New** and configure the following:

- For variable name, specify **JAVA_HOME**.
- For variable value, specify **C:\Program Files\Java\jre1.8.0_201** (depending on your JRE version).

d Click **OK**.

- While still in the **System Properties** dialog box, add the Java Runtime Environment installation folder to the *Path* environment variable.
  a Under **System Variables**, locate the *Path* variable and click **Edit**.
  b Append the following to the path and click **OK**: **C:\Program Files\Java\jre1.8.0_201\bin**
  c Click **OK** until you exit the **System Properties** dialog box.
- Run the following command in a command prompt to validate the Java version:

```
java.exe –version
```

- Verify that the source path for Microsoft Windows Server is available offline.
  - Copy the Microsoft Windows Server source directory `\sources\sxs` from the Windows install media to the virtual machine folder `C:\sources\sxs`.
  - Update the registry string value for `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows \CurrentVersion\policies\Servicing\LocalSourcePath` to location of the installation files. For example, `C:\sources\sxs`. If the `Servicing` key is missing, create it. `LocalSourcePath` is a string value.
- On the Microsoft Windows Server virtual machine, enable secondary log-in with an automatic start-up type.
  a Open the **Services** panel in Windows Server (**Start > Services**) and right-click **Secondary Logon** and select **Properties**.
  b Change the **Startup type** setting to **Automatic**.
  c Click **OK** to exit the **Properties** dialog box.
- Reboot the Microsoft Windows Server virtual machine.
- Using the previously established user account (for example,**svc–vra**), join the newly configured Microsoft Windows Server virtual machine to the Active Directory domain.
- After joining, verify that there are no Active Directory group policies that will change the UAC or firewall configuration.

Note The newly joined Microsoft Windows Server virtual machine should remain with UAC and firewall disabled. If not, you must disable or suppress the Group Policy that enforces a firewall or UAC enforcement when a new computer object joins the Active Directory.

- Add the vRealize Automation service account to the Local Administrators group (set as **svc-vra** in previous examples).
- Log in using the vRealize Automation service account.
- Verify the proxy server configuration.

  If the configuration is enabled, virtual machines from the vRealize Suite network must be able to access the proxy server. As an alternative, you can configure direct communication in **Control Panel > Internet Settings** and configure no proxy.

  Caution Do not activate the Microsoft Windows Server operating system on the virtual machine or run `sysprep` or `generalise` on it before converting it to a template.

- Shut down the Microsoft Windows Server virtual machine and export as OVA template with `ovftool`.

```
ovftool --noSSLVerify
vi://'administrator@vsphere.local':'<VC_Password>'@<VC_IP_or_FQDN>/<Datacenter_Name>/vm/<VM_Name>
\
<IAAS_Template_Name>.ova
```

Capacity Planning for Management and Workload Domains

5

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

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, a single virtual infrastructure workload domain, and a single Horizon 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 5-1. Virtual Infrastructure Layer Footprint

Domain	Component	Installed In	vCPUs	Memory (GB)	Storage (GB)	Notes
Base Management Domain Footprint	SDDC Manager	Management domain	4	16	800	
	vCenter Server	Management domain	4	16	290	

Table 5-1. Virtual Infrastructure Layer Footprint (continued)

Domain	Component	Installed In	vCPUs	Memory (GB)	Storage (GB)	Notes
	Platform Services Controller	Management domain	2	4	60	
	Platform Services Controller	Management domain	2	4	60	
	NSX Manager	Management domain	4	16	60	
	NSX Controller 01	Management domain	4	4	28	
	NSX Controller 02	Management domain	4	4	28	
	NSX Controller 03	Management domain	4	4	28	
Each NSX for vSphere VI Workload Domain	vCenter Server	Management domain	8	24	500	
	NSX Manager	Management domain	4	16	60	
	NSX Controller 01	Workload domain	4	4	28	
	NSX Controller 02	Workload domain	4	4	28	
	NSX Controller 03	Workload domain	4	4	28	
First NSX-T VI Workload Domain	vCenter Server	Management domain	8	24	500	A vCenter Server is deployed in the management domain for each NSX-T VI workload domain.
	NSX Manager	Management domain	8	32	200	These components are deployed for the first NSX-T VI workload domain. Additional workload domains share these components.
	NSX Manager	Management domain	8	32	200	
	NSX Manager	Management domain	8	32	200	
	NSX Edge 01 (Optional)	Workload domain	8	16	120	
	NSX Edge 02 (Optional)	Workload domain	8	16	120	

Table 5-1. Virtual Infrastructure Layer Footprint (continued)

Domain	Component	Installed In	vCPUs	Memory (GB)	Storage (GB)	Notes
Each Horizon Domain See Sizing Guidelines in the *VMware Cloud Foundation Operations and Administration Guide*.	Each Connection Server	Management domain	2	10	Depends on the size of the system drive of OVA template. Recommend minimum is 80.	These components are deployed for each Horizon domain.
	Each Composer Server	Management domain	2	10	Depends on the size of the system drive of OVA template. Recommend minimum is 80.	
	Each App Volumes Manager	Management domain	2	10	Depends on the size of the system drive of OVA template. Recommend minimum is 80.	
	Each Unified Access Gateway appliance	Management domain	2	4	20	
	Each User Environment Manager	Management domain	2	10	Depends on the size of the system drive of OVA template. Recommend minimum is 80.	
TOTAL (does not include Horizon components)			110 vCPU	316 GB	3,338 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.

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

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

Table 5-2. Operations Management Layer Footprint

Product	Component	Operating System	vCPUs	Memory (GB)	Storage (GB)
vRealize Operations (Optional)	vRealize Operations Manager Analytics Node1	Virtual Appliance	8	32	1,024
	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	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.

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 5-3. 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
	vRealize Automation IaaS Manager Server 1	Windows VM	2	8	60
	vRealize Automation IaaS Manager Server 2	Windows VM	2	8	60

Table 5-3. Cloud Management Layer Footprint (continued)

Product	Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
	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

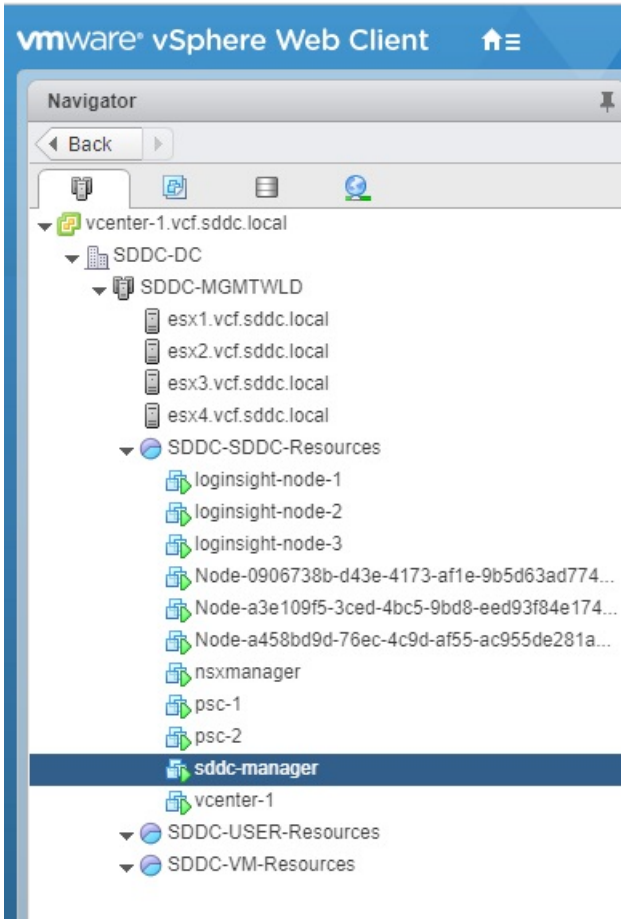
6

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:

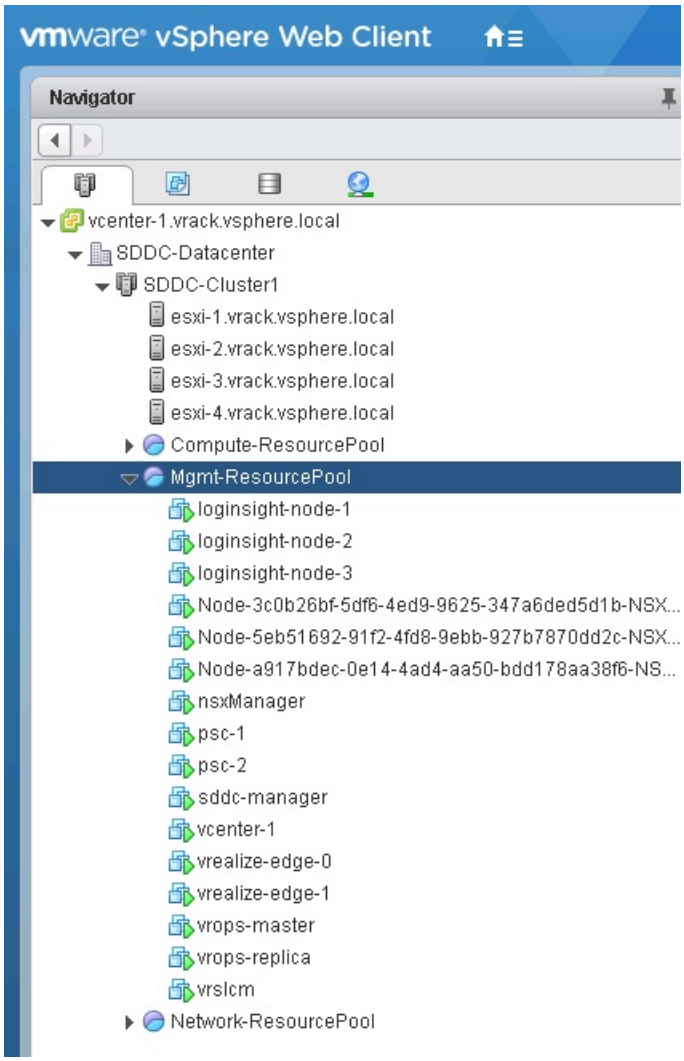
- SDDC Manager

- 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.

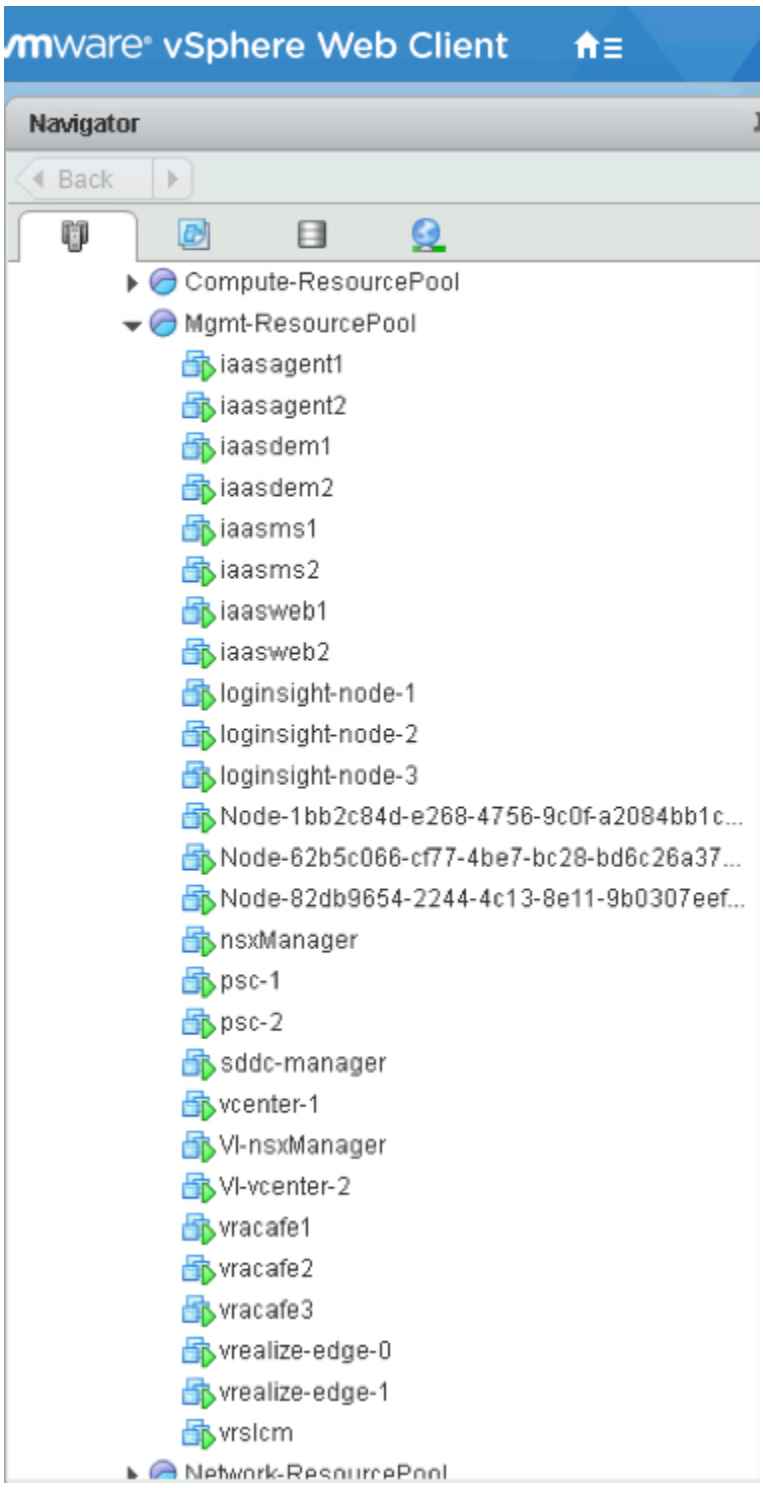


The deployment of vRealize Operations Manager within the environment is optional. In this example, vRealize Operations Manager was deployed with two nodes. You can define the number of nodes to be deployed as part of vRealize Operations Manager. See the *VMware Cloud Foundation Operations and Administration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


vmware vSphere Web Client
Navigator
Back
Compute-ResourcePool
Mgmt-ResourcePool
iaasagent1
iaasagent2
iaasdem1
iaasdem2
iaasms1
iaasms2
iaasweb1
iaasweb2
loginsight-node-1
loginsight-node-2
loginsight-node-3
Node-1bb2c84d-e268-4756-9c0f-a2084bb1c...
Node-62b5c066-cf77-4be7-bc28-bd6c26a37...
Node-82db9654-2244-4c13-8e11-9b0307eef...
nsxManager
psc-1
psc-2
sddc-manager
vcenter-1
VI-nsxManager
VI-vcenter-2
vracafe1
vracafe2
vracafe3
vrealize-edge-0
vrealize-edge-1
vrslcm
Network-ResourcePool

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.