Planning and Preparation

13 FEB 2018
VMware Validated Design 4.2
VMware Validated Design for Software-Defined Data Center 4.2

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 VMware Validated Design Planning and Preparation

The *VMware Validated Design Planning and Preparation for Software-Defined Data Center* documentation provides detailed information about the software, tools and external services that are required to implement a Standard Software-Defined Data Center (SDDC). In a Standard SDDC, management and tenant workloads run in different workload domains.

Before you start deploying the components of this VMware Validated Design, you must set up an environment that has a specific compute, storage and network configuration, and that provides services to the components of the SDDC. Carefully review the *VMware Validated Design Planning and Preparation for Software-Defined Data Center* documentation at least 2 weeks ahead of deployment to avoid costly re-work and delays.

Intended Audience

The *VMware Validated Design Planning and Preparation for Software-Defined Data Center* documentation is intended for cloud architects, infrastructure administrators and cloud administrators who are familiar with and want to use VMware software to deploy in a short time and manage an SDDC that meets the requirements for capacity, scalability, backup and restore, and extensibility for disaster recovery support.

Required VMware Software

The *VMware Validated Design Planning and Preparation for Software-Defined Data Center* documentation is compliant and validated with certain product versions. See *VMware Validated Design for Software-Defined Data Center Release Notes* for more information about supported product versions.

Hardware Requirements

To implement the SDDC from this VMware Validated Design, your hardware must meet certain requirements.

Management Workload Domain

When implementing a dual-region or single-region SDDC, the management workload domain in each region contains a management cluster which must meet the following hardware requirements.

Table 1-1. Hardware Requirements for the Management Cluster per Region

Component	Requirement per Region
Servers	Four vSAN ReadyNodes with hybrid (HY) profile. For information about vSAN ReadyNodes, see the VMware Compatibility Guide.
CPU per server	Dual-socket, 8 cores per socket
Memory per server	192 GB
Storage per server	16 GB SD for booting - One 200 GB SSD for the caching tier - Class D Endurance - Class E Performance - Two 1 TB HDD for the capacity tier 10K RPM See Designing and Sizing a vSAN Cluster from the VMware vSAN documentation for guidelines about cache sizing.
NICs per server	- Two 10 GbE NICs - One 1 GbE BMC NIC

Virtual Infrastructure Workload Domain

When implementing a dual-region or single-region SDDC, the virtual infrastructure workload domain contains a shared edge and compute cluster which must meet the following requirements.

Table 1-2. Hardware Requirements for the Shared Edge and Compute Cluster per Region

Component	Requirement per Region
Servers	Four supported servers
CPU, memory, and storage per server	Supported configurations
NICs per server	▪ Two 10 GbE NICs ▪ One 1 GbE BMC NIC

For information about supported servers, CPU, storage, IO devices, and so on, see vSAN ReadyNodes in the VMware Compatibility Guide.

Note If you scale the environment out with compute-only clusters, each server must meet the same requirements as a server in the shared edge and compute cluster. You can use as many compute servers as required.

Primary Storage Options

This design uses and is validated against vSAN as primary storage. However, in a workload domain you can use a supported storage solution that matches the requirements of your organization. Verify that the storage design supports the capacity and performance capabilities of the vSAN configuration in this design. Adjust appropriately the deployment and operational guidance.

Software Requirements

2

To implement the SDDC from this VMware Validated Design, you must download and license the following VMware and third-party software.

Download the software for building the SDDC to a Windows host system that has connectivity to the ESXi management network in the management pod.

This chapter includes the following topics:

- VMware Scripts and Tools
- Third-Party Software

VMware Scripts and Tools

Download the following scripts and tools that this VMware Validated Design uses for the SDDC implementation.

Table 2-1. VMware Scripts and Tools Required for the VMware Validated Design

SDDC Layer	Product Group	Script/Tool	Download Location	Description
SDDC	All	CertGenVVD	VMware Knowledge Base article 2146215	Use this tool to generate Certificate Signing Request (CSR), OpenSSL CA-signed certificates, and Microsoft CA-signed certificates for all VMware products that are included in the VMware Validated Design. In the context of VMware Validated Design, use the CertGenVVD tool to save time in creating signed certificates.

Third-Party Software

Download and license the following third-party software products.

Table 2-2. Third-Party Software Required for the VMware Validated Design for Software-Defined Data Center

SDDC Layer	Required by VMware Component	Vendor	Product Item	Product Version
Virtual Infrastructure	Windows host machine in the data center that has access to the ESXi management network.	Any Supported	Operating system that is supported for deploying VMware vSphere. See System Requirements for the vCenter Server Appliance Installer.	Operating system for vSphere deployment.
Operations Management	Update Manager Download Service (UMDS)	Ubuntu	Ubuntu Server 14.04	Ubuntu Server 14.04 LTS
		PostgreSQL	PostgreSQL	9.3
		Nginx	Nginx	1.4
	vRealize Operations Manager and vRealize Log Insight	Postman	Postman App	https://www.getpostman.com
Cloud Management	vRealize Automation	Microsoft	Windows 2012 R2 Standard	Windows Server 2012 R2 (64-bit)
		Microsoft	SQL Server 2012	SQL Server 2012 Enterprise edition (64-bit)
		Redhat	Red Hat Enterprise Linux 6	Red Hat Enterprise Linux 6 (64-bit)
Business Continuity	Site Recovery Manager	Microsoft	Windows 2012 R2 Standard	Windows Server 2012 R2 (64-bit)

External Services

You must provide a set of external services before you deploy the components of this VMware Validated Design.

This chapter includes the following topics:

- External Services Overview
- Physical Network Requirements
- VLANs, IP Subnets, and Application Virtual Networks
- Host Names and IP Addresses
- Time Synchronization
- Active Directory Users and Groups
- Certificate Replacement
- Datastore Requirements

External Services Overview

External services include Active Directory (AD), Dynamic Host Control Protocol (DHCP), Domain Name Services (DNS), Network Time Protocol (NTP), Simple Mail Transport Protocol (SMTP) Mail Relay, File Transfer Protocol (FTP), and Certificate Authority (CA).

Active Directory

This VMware Validated Design uses Active Directory (AD) for authentication and authorization to resources in the rainpole.local domain.

For a multi-region deployment, you use a domain and forest structure to store and manage Active Directory objects per region.

Table 3-1. Active Directory Requirements

Requirement	Domain Instance	DNS Zone	Description
Active Directory configuration	Parent Active Directory	rainpole.local	Contains Domain Name System (DNS) server, time server, and universal groups that contain global groups from the child domains and are members of local groups in the child domains.
	Region-A child Active Directory	sfo01.rainpole.local	Contains DNS records that replicate to all DNS servers in the forest. This child domain contains all SDDC users, and global and local groups.
	Region-B child Active Directory	lax01.rainpole.local	Contains DNS records that replicate to all DNS servers in the forest. This child domain contains all SDDC users, and global and local groups.
Active Directory users and groups	-		All user accounts and groups from the Active Directory Users and Groups documentation must exist in the Active Directory before installing and configuring the SDDC.
Active Directory connectivity	-		All Active Directory domain controllers must be accessible by all management components within the SDDC.

DHCP

This validated design requires Dynamic Host Configuration Protocol (DHCP) support for the configuration of each VMkernel port of an ESXi host with an IPv4 address. The configuration includes the VMkernel ports for the VXLAN (VTEP).

Table 3-2. DHCP Requirements

Requirement	Description
DHCP server	The subnets and associated VLANs that provide IPv4 transport for VXLAN (VTEP) VMkernel ports must be configured for IPv4 address auto-assignment by using DHCP.

DNS

For a multi-region deployment, you must provide a root and child domains which contain separate DNS records.

Table 3-3. DNS Server Requirements

Requirement	Domain Instance	Description
DNS host entries	rainpole.local	Resides in the rainpole.local domain.
	sfo01.rainpole.local and lax01.rainpole.local	Reside in the sfo01.rainpole.local and lax01.rainpole.local domains. Configure both DNS servers with the following settings: - Dynamic updates for the domain set to **Nonsecure and secure**. - Zone replication scope for the domain set to **All DNS server in this forest**. - Create all hosts listed in the Host Names and IP Addresses in Region A documentation.

If you configure the DNS servers properly, all nodes from the validated design are resolvable by FQDN as well as IP address.

NTP

All components in the SDDC must be synchronized against a common time by using the Network Time Protocol (NTP) on all nodes. Important components of the SDDC, such as, vCenter Single Sign-On, are sensitive to a time drift between distributed components. See Time Synchronization.

Table 3-4. NTP Server Requirements

Requirement	Description
NTP	An NTP source, for example, on a Layer 3 switch or router, must be available and accessible from all nodes of the SDDC.
	Use the ToR switches in the Management Workload Domain as the NTP servers or the upstream physical router. These switches should synchronize with different upstream NTP servers and provide time synchronization capabilities in the SDDC. As a best practice, make the NTP servers available under a friendly FQDN, for example, ntp.sfo01.rainpole.local.

SMTP Mail Relay

Certain components of the SDDC send status messages to operators and end users by email.

Table 3-5. SMTP Server Requirements

Requirement	Description
SMTP mail relay	Open Mail Relay instance, which does not require user name-password authentication, must be reachable from each SDDC component over plain SMTP (no SSL/TLS encryption). As a best practice, limit the relay function to the IP range of the SDDC deployment.

Certificate Authority

The majority of the components of the SDDC require SSL certificates for secure operation. The certificates must be signed by an internal enterprise CA or by a third-party commercial CA. In either case, 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.

Table 3-6. Certificate Authority Requirements

Requirement	Description
Certificate Authority	CA must be able to ingest a Certificate Signing Request (CSR) from the SDDC components and issue a signed certificate.
	For this VMware Validated Design, use the Microsoft Windows Enterprise CA that is available in the Windows Server 2012 R2 operating system of a root domain controller. The domain controller must be configured with the Certificate Authority Service and the Certificate Authority Web Enrollment roles.

FTP Server

Dedicate space on a remote FTP server to save data backups for the NSX Manager instances in the SDDC.

Table 3-7. FTP Server Requirements

Requirement	Description
FTP server	An FTP server must host NSX Manager backups. The server must support SFTP and FTP. NSX Manager instances must have connection to the remote FTP server.

Windows Host Machine

Provide a Microsoft Windows virtual machine or physical server that works as an entry point to the data center.

Table 3-8. Windows Host Machine Requirements

Requirement	Description
Windows host machine	Microsoft Windows virtual machine or physical server must be available to provide connection to the data center and store software downloads. The host must be connected to the external network and to the ESXi management network.

Physical Network Requirements

Before you start deploying the SDDC, provide certain physical network configuration.

Table 3-9. Requirements for the SDDC Physical Network

Requirement	Feature
IGMP snooping querier	Required for the following traffic types: ■ vSAN ■ VXLAN
Jumbo frames	Required for the following traffic types: ■ vSAN ■ vSphere vMotion ■ VXLAN ■ vSphere Replication ■ NFS
BGP adjacency and BGP autonomous system (AS) numbers	Dynamic routing in the SDDC

VLANs, IP Subnets, and Application Virtual Networks

Before you start deploying the SDDC, you must allocate VLANs and IP subnets to the different types of traffic in the SDDC, such as ESXi management, vSphere vMotion, and others. For application virtual networks, you must plan separate IP subnets for these networks.

VLAN IDs and IP Subnets

This VMware Validated Design requires that you allocate certain VLAN IDs and IP subnets for the traffic types in the SDDC.

VLANs and IP Subnets in Region A

According to the VMware Validated Design, you have the following VLANs and IP subnets in Region A:

Table 3-10. VLAN and IP Subnet Configuration in Region A

Cluster in Region A	VLAN Function	VLAN ID	Subnet	Gateway
Management Cluster	ESXi 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
	NFS	1615	172.16.15.0/24	172.16.15.253
	■ vSphere Replication ■ vSphere Replication NFC	1616	172.16.16.0/24	172.16.16.253
	Uplink01	2711	172.27.11.0/24	172.27.11.253
	Uplink02	2712	172.27.12.0/24	172.27.12.253
	External Management Connectivity	130	10.158.130.0/24	10.158.130.253
Shared Edge and Compute Cluster	ESXi Management	1631	172.16.31.0/24	172.16.31.253
	vSphere vMotion	1632	172.16.32.0/24	172.16.32.253

Table 3-10. VLAN and IP Subnet Configuration in Region A (Continued)

Cluster in Region A	VLAN Function	VLAN ID	Subnet	Gateway
	vSAN	1633	172.16.33.0/24	172.16.33.253
	VXLAN (NSX VTEP)	1634	172.16.34.0/24	172.16.34.253
	NFS	1625	172.16.25.0/24	172.16.25.253
	Uplink01	1635	172.16.35.0/24	172.16.35.253
	Uplink02	2713	172.27.13.0/24	172.27.13.253
	External Tenant Connectivity	140	10.158.140.0/24	10.158.140.253

VLAN IDs and IP Subnets in Region B

If you expand your design to two regions later, you have the following VLANs and IP subnets in Region B:

Table 3-11. VLAN and IP Subnet Configuration in Region B

Clusters in Region B	VLAN Function	VLAN ID	Subnet	Gateway
Management Cluster	ESXi Management	1711	172.17.11.0/24	172.17.11.253
	vSphere vMotion	1712	172.17.12.0/24	172.17.12.253
	vSAN	1713	172.17.13.0/24	172.17.13.253
	VXLAN (NSX VTEP)	1714	172.17.14.0/24	172.17.14.253
	NFS	1715	172.17.15.0/24	172.17.15.253
	■ vSphere Replication ■ vSphere Replication NFC	1716	172.17.16.0/24	172.17.16.253
	Uplink01	2714	172.27.14.0/24	172.27.14.253
	Uplink02	2715	172.27.15.0/24	172.27.15.253
	External Management Connectivity	150	10.158.150.0/24	10.158.150.253
Shared Edge and Compute Cluster	ESXi Management	1731	172.17.31.0/24	172.17.31.253
	vSphere vMotion	1732	172.17.32.0/24	172.17.32.253
	vSAN	1733	172.17.33.0/24	172.17.33.253
	VXLAN (NSX VTEP)	1734	172.17.34.0/24	172.17.34.253
	NFS	1725	172.17.25.0/24	172.17.25.253
	Uplink01	1735	172.17.35.0/24	172.17.35.253
	Uplink02	2721	172.27.21.0/24	172.27.21.253
	External Tenant Connectivity	160	10.158.160.0/24	10.158.160.253

Note Use these VLAN IDs and IP subnets as samples. Configure the actual VLAN IDs and IP subnets according to your environment.

Names and IP Subnets of Application Virtual Networks

You must allocate an IP subnet to each application virtual network and the management applications that are in this network.

Table 3-12. IP Subnets for the Application Virtual Networks

Application Virtual Network	Subnet in Region A	Subnet in Region B
Mgmt-xRegion01-VXLAN	192.168.11.0/24	192.168.11.0/24
Mgmt-RegionA01-VXLAN	192.168.31.0/24	-
Mgmt-RegionB01-VXLAN	-	192.168.32.0/24

Note Use these IP subnets as samples. Configure the actual IP subnets according to your environment.

Host Names and IP Addresses

Before you deploy the SDDC following this VMware Validated Design, you must define the host names and IP addresses for the each of the management components deployed. Some of these host names must also be configured in DNS with a fully qualified domain names (FQDN) that maps the hostname to the IP address.

In a multi-region deployment with domain and forest structure, you must assign own IP subnets and DNS configuration to each sub-domain, sfo01.rainpole.local and lax01.rainpole.local. The only DNS entries that reside in the rainpole.local domain are the records for the virtual machines within the network containers that support disaster recovery failover between regions such as vRealize Automation and vRealize Operations Manager.

Host Names and IP Addresses in Region A

In Region A of the SDDC, you must define the host names and IP addresses of the management components before the SDDC deployment. For some components, you must configure fully qualified domain names (FQDN) that map to their IP addresses on the DNS servers.

- Host Names and IP Addresses for External Services in Region A

  Allocate host names and IP addresses to all external services required by the SDDC according to this VMware Validated Design.

- Host Names and IP Addresses for the Virtual Infrastructure Layer in Region A

  Allocate host names and IP addresses to all components you deploy for the virtual infrastructure layer of the SDDC according to this VMware Validated Design.

- Host Names and IP Addresses for the Operations Management Layer in Region A

  Allocate host names and IP addresses to all components you deploy for the operations management layer of the SDDC according to this VMware Validated Design.

- Host Names and IP Addresses for the Cloud Management Layer in Region A

  Allocate host names and IP addresses to all components you deploy for the cloud management layer of the SDDC according to this VMware Validated Design.

- Host Names and IP Addresses for the Business Continuity Layer in Region A

  Allocate host names and IP addresses to all components you deploy for the business continuity layer of the SDDC according to this VMware Validated Design.

Host Names and IP Addresses for External Services in Region A

Allocate host names and IP addresses to all external services required by the SDDC according to this VMware Validated Design.

Allocate host names and IP addresses to the following components in Region A and configure DNS with a FQDN that maps to the IP address where defined:

Components	Requires DNS Configuration
NTP	X
Active Directory	X

Table 3-13. Host Names and IP Addresses for the External Services

Component Group	Host Name	DNS Zone	IP Address	Description
NTP	ntp	sfo01.rainpole.local	▪ 172.16.11.251 ▪ 172.16.11.252	▪ NTP server selected using Round Robin ▪ NTP server on a ToR switch in the management pod
	0.ntp	sfo01.rainpole.local	172.16.11.251	NTP server on a ToR switch in the management pod
	1.ntp	sfo01.rainpole.local	172.16.11.252	NTP server on a ToR switch in the management pod
AD/DNS/CA	dc01rpl	rainpole.local	172.16.11.4	Windows 2012 R2 host that contains the Active Directory configuration and DNS server for the rainpole.local domain, and the Microsoft Certificate Authority for signing management SSL certificates.
	dc01sfo	sfo01.rainpole.local	172.16.11.5	Active Directory and DNS server for the sfo01 child domain.

Host Names and IP Addresses for the Virtual Infrastructure Layer in Region A

Allocate host names and IP addresses to all components you deploy for the virtual infrastructure layer of the SDDC according to this VMware Validated Design.

Allocate host names and IP addresses to the following components in Region A and configure DNS with a FQDN that maps to the IP address where defined:

Components	Requires DNS Configuration
Platform Services Controllers	X
vCenter Servers	X
NSX Managers	X
NSX Edge Services Gateways	-

Table 3-14. Host Names and IP Addresses for the Virtual Infrastructure Layer in Region A

Component Group	Host Name	DNS Zone	IP Address	Description
vSphere	sfo01m01psc01	sfo01.rainpole.local	172.16.11.61	Platform Services Controller for the management cluster
	sfo01m01vc01	sfo01.rainpole.local	172.16.11.62	Management vCenter Server
	sfo01m01esx01	sfo01.rainpole.local	172.16.11.101	ESXi hosts in the management pod
	sfo01m01esx02	sfo01.rainpole.local	172.16.11.102	
	sfo01m01esx03	sfo01.rainpole.local	172.16.11.103	
	sfo01m01esx04	sfo01.rainpole.local	172.16.11.104	
	sfo01w01psc01	sfo01.rainpole.local	172.16.11.63	Platform Services Controller for the shared edge and compute cluster.
	sfo01w01vc01	sfo01.rainpole.local	172.16.11.64	Compute vCenter Server
	sfo01w01esx01	sfo01.rainpole.local	172.16.31.101	ESXi hosts in the shared edge and compute pod
	sfo01w01esx02	sfo01.rainpole.local	172.16.31.102	
	sfo01w01esx03	sfo01.rainpole.local	172.16.31.103	
	sfo01w01esx04	sfo01.rainpole.local	172.16.31.104	
NSX for vSphere	sfo01m01nsx01	sfo01.rainpole.local	172.16.11.65	NSX Manager for the management cluster
	sfo01m01nsxc01	-	172.16.11.118	NSX Controller instances for the management cluster
	sfo01m01nsxc02	-	172.16.11.119	
	sfo01m01nsxc03	-	172.16.11.120	
	sfo01w01nsx01	sfo01.rainpole.local	172.16.11.66	NSX Manager for the shared edge and compute cluster
	sfo01w01nsxc01	-	172.16.31.118	NSX Controller instances for the shared edge and compute cluster
	sfo01w01nsxc02	-	172.16.31.119	
	sfo01w01nsxc03	-	172.16.31.120	
	sfo01psc01	sfo01.rainpole.local	172.16.11.71	NSX Edge device for load balancing the Platform Services Controller instances
	sfo01m01esg01	-	▪ 172.27.11.2 ▪ 172.27.12.3 ▪ 192.168.10.1	ECMP-enabled NSX Edge device for North-South management traffic
	sfo01m01esg02	-	▪ 172.27.11.3 ▪ 172.27.12.2 ▪ 192.168.10.2	ECMP-enabled NSX Edge device for North-South management traffic

Table 3-14. Host Names and IP Addresses for the Virtual Infrastructure Layer in Region A (Continued)

Component Group	Host Name	DNS Zone	IP Address	Description
	sfo01m01udlr01	-	▪ 192.168.10.3 ▪ 192.168.11.1 ▪ 192.168.31.1	Universal Distributed Logical Router (UDLR) for East-West management traffic
	sfo01w01esg01	-	▪ 172.16.35.2 ▪ 172.27.13.3 ▪ 192.168.100.1 ▪ 192.168.101.1	ECMP-enabled NSX Edge device for North-South compute and edge traffic
	sfo01w01esg02	-	▪ 172.16.35.3 ▪ 172.27.13.2 ▪ 192.168.100.2 ▪ 192.168.101.2	ECMP-enabled NSX Edge device for North-South compute and edge traffic
	sfo01w01udlr01	-	192.168.100.3	Universal Distributed Logical Router (UDLR) for East-West compute and edge traffic
	sfo01w01dlr01	-	192.168.101.3	Distributed Logical Router (DLR) for East-West compute and edge traffic
	sfo01m01lb01	-	192.168.11.2	NSX Edge device for load balancing management applications

Host Names and IP Addresses for the Operations Management Layer in Region A

Allocate host names and IP addresses to all components you deploy for the operations management layer of the SDDC according to this VMware Validated Design.

Allocate host names and IP addresses to the following components in Region A and configure DNS with a FQDN that maps to the IP address where defined:

Components	Requires DNS Configuration
vRealize Operations Manager	X
vSphere Update Manager Download Service	X
vRealize Log Insight	X

Table 3-15. Host Names and IP Addresses for Operations Management Layer in Region A

Component Group	Host Name	DNS Zone	IP Address	Description
vRealize Operations Manager	vrops01svr01	rainpole.local	192.168.11.35	VIP address of load balancer for the analytics cluster of vRealize Operations Manager
	vrops01svr01a	rainpole.local	192.168.11.31	Master node of vRealize Operations Manager
	vrops01svr01b	rainpole.local	192.168.11.32	Master replica node of vRealize Operations Manager

Table 3-15. Host Names and IP Addresses for Operations Management Layer in Region A (Continued)

Component Group	Host Name	DNS Zone	IP Address	Description
	vrops01svr01c	rainpole.local	192.168.11.33	Data node 1 of vRealize Operations Manager
	sfo01vropsc01a	sfo01.rainpole.local	192.168.31.31	Remote Collector 1 of vRealize Operations Manager
	sfo01vropsc01b	sfo01.rainpole.local	192.168.31.32	Remote Collector 2 of vRealize Operations Manager
vSphere Update Manager	sfo01umds01	sfo01.rainpole.local	192.168.31.67	vSphere Update Manager Download Service (UMDS)
vRealize Log Insight	sfo01vrli01	sfo01.rainpole.local	192.168.31.10	VIP address of the integrated load balancer of vRealize Log Insight
	sfo01vrli01a	sfo01.rainpole.local	192.168.31.11	Master node of vRealize Log Insight
	sfo01vrli01b	sfo01.rainpole.local	192.168.31.12	Worker node 1 of vRealize Log Insight
	sfo01vrli01c	sfo01.rainpole.local	192.168.31.13	Worker node 2 of vRealize Log Insight

Host Names and IP Addresses for the Cloud Management Layer in Region A

Allocate host names and IP addresses to all components you deploy for the cloud management layer of the SDDC according to this VMware Validated Design.

Allocate host names and IP addresses to the following components in Region A and configure DNS with a FQDN that maps to the IP address where defined:

Components	Requires DNS Configuration
vRealize Automation	X
Microsoft SQL Server for vRealize Automation	X
vRealize Business for Cloud	X

Table 3-16. Host Names and IP Addresses for the Cloud Management Layer in Region A

Component Group	Host Name	DNS Zone	IP Address	Description
vRealize Automation	vra01svr01	rainpole.local	192.168.11.53	VIP address of the vRealize Automation Appliance
	vra01svr01a	rainpole.local	192.168.11.51	vRealize Automation Appliances
	vra01svr01b	rainpole.local	192.168.11.52	
	vra01iws01	rainpole.local	192.168.11.56	VIP address of the vRealize Automation IaaS Web Server
	vra01iws01a	rainpole.local	192.168.11.54	vRealize Automation IaaS Web Servers
	vra01iws01b	rainpole.local	192.168.11.55	
	vra01ims01	rainpole.local	192.168.11.59	VIP address of the vRealize Automation IaaS Manager Service

Table 3-16. Host Names and IP Addresses for the Cloud Management Layer in Region A (Continued)

Component Group	Host Name	DNS Zone	IP Address	Description
	vra01ims01a	rainpole.local	192.168.11.57	vRealize Automation IaaS Manager Service and DEM Orchestrators
	vra01ims01b	rainpole.local	192.168.11.58	
	vra01dem01a	rainpole.local	192.168.11.60	vRealize Automation DEM Workers
	vra01dem01b	rainpole.local	192.168.11.61	
	sfo01ias01a	sfo01.rainpole.local	192.168.31.52	vRealize Automation Proxy Agents
	sfo01ias01b	sfo01.rainpole.local	192.168.31.53	
Microsoft SQL Server	vra01mssql01	rainpole.local	192.168.11.62	Microsoft SQL Server for vRealize Automation
vRealize Business for Cloud	vrb01svr01	rainpole.local	192.168.11.66	vRealize Business for Cloud Server
	sfo01vrbc01	sfo01.rainpole.local	192.168.31.54	vRealize Business for Cloud Data Collector

Host Names and IP Addresses for the Business Continuity Layer in Region A

Allocate host names and IP addresses to all components you deploy for the business continuity layer of the SDDC according to this VMware Validated Design.

For a dual-region SDDC, allocate host names and IP addresses to the nodes that run Site Recovery Manager and vSphere Replication in Region A and configure DNS with a FQDN that maps to the IP address where defined:

Components	Requires DNS Configuration
Site Recovery Manager	X
vSphere Replication	X

Table 3-17. Host Names and IP Addresses for the Business Continuity Layer in Region A

Component Group	Host Name	DNS Zone	IP Address	Description
Site Recovery Manager	sfo01m01srm01	sfo01.rainpole.local	172.16.11.124	Site Recovery Manager connected to the Management vCenter Server
vSphere Replication	sfo01m01vrms01	sfo01.rainpole.local	172.16.11.123	vSphere Replication connected to the Management vCenter Server

Host Names and IP Addresses in Region B

In Region B of the SDDC, you must define the host names and IP addresses of the management components before the SDDC deployment. For some components, you must configure fully qualified domain names (FQDNs) that map to their IP addresses on the DNS servers.

- Host Names and IP Addresses for External Services in Region B

  Allocate host names and IP addresses to all external services required by the SDDC according to this VMware Validated Design.

- Host Names and IP Addresses for the Virtual Infrastructure Layer in Region B

  Allocate host names and IP addresses to all components you deploy for the virtual infrastructure layer of the SDDC according to this VMware Validated Design.

- Host Names and IP Addresses for the Operations Management Layer in Region B

  Allocate host names and IP addresses to all components you deploy for the operations management layer of the SDDC according to this VMware Validated Design.

- Host Names and IP Addresses for the Cloud Management Layer in Region B

  Allocate host names and IP addresses to all components you deploy for the cloud management layer of the SDDC according to this VMware Validated Design.

- Host Names and IP Addresses for the Business Continuity Layer in Region B

  Allocate host names and IP addresses to all components you deploy for the business continuity layer of the SDDC according to this VMware Validated Design.

Host Names and IP Addresses for External Services in Region B

Allocate host names and IP addresses to all external services required by the SDDC according to this VMware Validated Design.

Allocate host names and IP addresses to the following components in Region B and configure DNS with a FQDN that maps to the IP address where defined:

Components	Requires DNS Configuration
NTP	X
Active Directory	X

Table 3-18. Host Names and IP Addresses for the External Services in Region B

Component Group	Host Name	DNS Zone	IP Address	Description
NTP	ntp	lax01.rainpole.local	■ 172.17.11.251 ■ 172.17.11.252	■ NTP server selected using Round Robin ■ NTP server on a ToR switch in the management pod
	0.ntp	lax01.rainpole.local	172.17.11.251	NTP server on a ToR switch in the management pod
	1.ntp	lax01.rainpole.local	172.17.11.252	NTP server on a ToR switch in the management pod

Table 3-18. Host Names and IP Addresses for the External Services in Region B (Continued)

Component Group	Host Name	DNS Zone	IP Address	Description
AD/DNS/CA	dc51rpl	rainpole.local	172.17.11.4	Windows 2012 R2 host that contains the Active Directory configuration and DNS server for the rainpole.local domain and the Microsoft Certificate Authority for signing management SSL certificates.
	dc51lax	lax01.rainpole.local	172.17.11.5	Active Directory and DNS server for the lax01 child domain.

Host Names and IP Addresses for the Virtual Infrastructure Layer in Region B

Allocate host names and IP addresses to all components you deploy for the virtual infrastructure layer of the SDDC according to this VMware Validated Design.

Allocate host names and IP addresses to the following components in Region B and configure DNS with a FQDN that maps to the IP address where defined:

Components	Requires DNS Configuration
Platform Services Controllers	X
vCenter Servers	X
NSX Managers	X
NSX Edge Services Gateways	-

Table 3-19. Host Names and IP Addresses for the Virtual Infrastructure Layer in Region B

Component Group	Host Name	DNS Zone	IP Address	Description
vSphere	lax01m01psc01	lax01.rainpole.local	172.17.11.61	Platform Services Controller for the management cluster
	lax01m01vc01	lax01.rainpole.local	172.17.11.62	Management vCenter Server
	lax01m01esx01	lax01.rainpole.local	172.17.11.101	ESXi hosts in the management pod
	lax01m01esx02	lax01.rainpole.local	172.17.11.102	
	lax01m01esx03	lax01.rainpole.local	172.17.11.103	
	lax01m01esx04	lax01.rainpole.local	172.17.11.104	
	lax01w01psc01	lax01.rainpole.local	172.17.11.63	Platform Services Controller for the shared edge and compute cluster
	lax01w01vc01	lax01.rainpole.local	172.17.11.64	Compute vCenter Server
	lax01w01esx01	lax01.rainpole.local	172.17.31.101	ESXi hosts in the shared edge and compute pod
	lax01w01esx02	lax01.rainpole.local	172.17.31.102	
	lax01w01esx03	lax01.rainpole.local	172.17.31.103	
	lax01w01esx04	lax01.rainpole.local	172.17.31.104	
NSX for vSphere	lax01m01nsx01	lax01.rainpole.local	172.17.11.65	NSX Manager for the management cluster

Table 3-19. **Host Names and IP Addresses for the Virtual Infrastructure Layer in Region B (Continued)**

Component Group	Host Name	DNS Zone	IP Address	Description
	lax01m01nsxc01	-	172.17.11.118	NSX Controller instances for the management cluster
	lax01m01nsxc02	-	172.17.11.119	
	lax01m01nsxc03	-	172.17.11.120	
	lax01w01nsx01	lax01.rainpole.local	172.17.11.66	NSX Manager for the shared edge and compute cluster
	lax01w01nsxc01	-	172.17.31.118	NSX Controller instances for the shared edge and compute cluster
	lax01w01nsxc02	-	172.17.31.119	
	lax01w01nsxc03	-	172.17.31.120	
	lax01psc01	lax01.rainpole.local	172.17.11.71	NSX Edge device for load balancing the Platform Services Controller instances
	lax01m01esg01	-	▪ 172.27.14.2 ▪ 172.27.15.3 ▪ 192.168.10.50	ECMP-enabled NSX Edge device for North-South management traffic
	lax01m01esg02	-	▪ 172.27.14.3 ▪ 172.27.15.2 ▪ 192.168.10.51	ECMP-enabled NSX Edge device for North-South management traffic
	lax01w01esg01	-	▪ 172.17.35.2 ▪ 172.27.21.3 ▪ 192.168.100.50 ▪ 192.168.102.1	ECMP-enabled NSX Edge device for North-South compute and edge traffic
	lax01w01esg02	-	▪ 172.17.35.3 ▪ 172.27.21.2 ▪ 192.168.100.51 ▪ 192.168.102.2	ECMP-enabled NSX Edge device for North-South compute and edge traffic
	lax01w01dlr01	-	192.168.102.3	Distributed Logical Router (DLR) for East-West compute and edge traffic.
	lax01m01lb01	-	192.168.11.2	NSX Edge device for load balancing management applications

Host Names and IP Addresses for the Operations Management Layer in Region B

Allocate host names and IP addresses to all components you deploy for the operations management layer of the SDDC according to this VMware Validated Design.

Allocate host names and IP addresses to the following components in Region B and configure DNS with a FQDN that maps to the IP address where defined:

Components	Requires DNS Configuration
vRealize Operations Manager	X
vSphere Update Manager Download Service	X
vRealize Log Insight	X

Table 3-20. Host Names and IP Addresses for Data Protection and Operations Management Layer in Region B

Component Group	Host Name	DNS Zone	IP Address	Description
vRealize Operations Manager	lax01vropsc01a	lax01.rainpole.local	192.168.32.31	Remote Collector 1 of vRealize Operations Manager
	lax01vropsc01b	lax01.rainpole.local	192.168.32.32	Remote Collector 2 of vRealize Operations Manager
vSphere Update Manager	lax01umds01	lax01.rainpole.local	192.168.32.67	vSphere Update Manager Download Service (UMDS)
vRealize Log Insight	lax01vrli01	lax01.rainpole.local	192.168.32.10	VIP address of the integrated load balancer of vRealize Log Insight
	lax01vrli01a	lax01.rainpole.local	192.168.32.11	Master node of vRealize Log Insight
	lax01vrli01b	lax01.rainpole.local	192.168.32.12	Worker node 1 of vRealize Log Insight
	lax01vrli01c	lax01.rainpole.local	192.168.32.13	Worker node 2 of vRealize Log Insight

Host Names and IP Addresses for the Cloud Management Layer in Region B

Allocate host names and IP addresses to all components you deploy for the cloud management layer of the SDDC according to this VMware Validated Design.

Allocate host names and IP addresses to each of the following components in Region B and configure DNS with a FQDN that maps to the IP address where defined:

Components	Requires DNS Configuration
vRealize Automation	X
vRealize Business for Cloud	X

Table 3-21. Host Names and IP Addresses for the Cloud Management Components in Region B

Component Group	Host Name	DNS Zone	IP Address	Description
vRealize Automation	lax01ias01a	lax01.rainpole.local	192.168.32.52	vRealize Automation Proxy Agents
	lax01ias01b	lax01.rainpole.local	192.168.32.53	
vRealize Business for Cloud	lax01vrbc01	lax01.rainpole.local	192.168.32.54	vRealize Business for Cloud Data Collector

Host Names and IP Addresses for the Business Continuity Layer in Region B

Allocate host names and IP addresses to all components you deploy for the business continuity layer of the SDDC according to this VMware Validated Design.

For a dual-region SDDC, allocate host names and IP addresses to the nodes that run Site Recovery Manager and vSphere Replication in Region B and configure DNS with a FQDN that maps to the IP address where defined:

Components	Requires DNS Configuration
Site Recovery Manager	X
vSphere Replication	X

Table 3-22. Host Names and IP Addresses for Disaster Recovery Applications in Region B

Component Group	Host Name	DNS Zone	IP Address	Description
Site Recovery Manager	lax01m01srm01	lax01.rainpole.local	172.17.11.124	Site Recovery Manager connected to the Management vCenter
vSphere Replication	lax01m01vrms01	lax01.rainpole.local	172.17.11.123	vSphere Replication connected to the Management vCenter

Time Synchronization

Synchronized systems over NTP are essential for vCenter Single Sign-On certificate validity, and for the validity of other certificates. Consistent system clocks are important for the proper operation of the components in the SDDC because in certain cases they rely on vCenter Single Sign-on.

Using NTP also makes it easier to correlate log files from multiple sources during troubleshooting, auditing, or inspection of log files to detect attacks.

Requirements for Time Synchronization

All management components need to be configured to use NTP for time synchronization.

NTP Server Configuration

- Configure two time sources per region that are external to the SDDC. These sources can be physical radio or GPS time servers, or even NTP servers running on physical routers or servers.

- Ensure that the external time servers are synchronized to different time sources to ensure desirable NTP dispersion.

DNS Configuration

Configure a DNS Canonical Name (CNAME) record that maps the two time sources to one DNS name.

Table 3-23. NTP Server FQDN and IP Configuration in Region A

NTP Server FQDN	Mapped IP Address
ntp.sfo01.rainpole.local	■ 172.16.11.251 ■ 172.16.11.252
0.ntp.sfo01.rainpole.local	172.16.11.251
1.ntp.sfo01.rainpole.local	172.16.11.252

Table 3-24. NTP Server FQDN and IP Configuration in Region B

NTP Server FQDN	Mapped IP Address
ntp.lax01.rainpole.local	■ 172.17.11.251 ■ 172.17.11.252
0.ntp.lax01.rainpole.local	172.17.11.251
1.ntp.lax01.rainpole.local	172.17.11.252

Time Synchronization on the SDDC Nodes

- Synchronize the time with the NTP servers on the following systems:

    - ESXi hosts

    - AD domain controllers

    - Virtual appliances of the management applications

- Configure each system with the two regional NTP server aliases

    - ntp.sfo01.rainpole.local

    - ntp.lax01.rainpole.local

Time Synchronization on the Application Virtual Machines

- Verify that the default configuration on the Windows VMs is active, that is, the Windows VMs are synchronized with the NTP servers.

- As a best practice, for time synchronization on virtual machines, enable NTP-based time synchronization instead of the VMware Tools periodic time synchronization because NTP is an industry standard and ensures accurate timekeeping in the guest operating system.

Configure NTP-Based Time Synchronization on Windows Hosts

Ensure that NTP has been configured properly in your Microsoft Windows Domain.

See https://blogs.technet.microsoft.com/nepapfe/2013/03/01/its-simple-time-configuration-in-active-directory/.

Active Directory Users and Groups

Before you deploy and configure the SDDC in this VMware Validated Design, you must provide specific configuration of Active Directory users and groups. You use these users and groups for application login, for assigning roles in a tenant organization and for authentication in cross-application communication.

In a multi-region or single-region environment that has parent and child domains in a single forest, store service accounts in the parent domain and user accounts in each of the child domains. By using the group scope attribute of Active Directory groups you manage resource access across domains.

Active Directory Administrator Account

Certain installation and configuration tasks require a domain administrator account that is referred to as `svc-domain-join` in the Active Directory domain.

Active Directory Groups

To grant user and service accounts the access that is required to perform their task, create Active Directory groups according to certain rules.

Create Active Directory groups according to the following rules:

1   Add user and service accounts to universal groups in the parent domain.

2   Add the universal groups to global groups in each child domain.

3   Where applicable, assign access rights and permissions to the global groups, located in the child domains, and the universal groups, located in the parent domain (rainpole.local) to specific products according to their role.

Universal Groups in the Parent Domain

In the rainpole.local domain, create the following universal groups:

Table 3-25. Universal Groups in the rainpole.local Parent Domain

Group Name	Group Scope	Description
ug-SDDC-Admins	Universal	Administrative group for the SDDC
ug-SDDC-Ops	Universal	SDDC operators group
ug-vCenterAdmins	Universal	Group with accounts that are assigned vCenter Server administrator privileges.
ug-vra-admins-rainpole	Universal	Tenant administrators group
ug-vra-archs-rainpole	Universal	Tenant blueprint architects group
ug-vROAdmins	Universal	Groups with vRealize Orchestrator Administrator privileges

Global Groups in the Child Domains

In each child domain, add the role-specific universal group from the parent domain to the relevant role-specific global group in the child domain.

Table 3-26. Global Groups in the Child Domains

Group Name	Group Scope	Description	Member of Groups
SDDC-Admins	Global	Administrative group for the SDDC	RAINPOLE\ug-SDDC-Admins
SDDC-Ops	Global	SDDC operators group	RAINPOLE\ug-SDDC-Ops
vCenterAdmins	Global	Accounts that are assigned vCenter Server administrator privileges.	RAINPOLE\ug-vCenterAdmins

Active Directory Users

A service account provides non-interactive and non-human access to services and APIs to the components of the SDDC. You must create service accounts for accessing functionality on the SDDC nodes, and user accounts for operations and tenant administration.

Service Accounts

A 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.

In addition, a special service account is also required to perform domain join operations if a component registers itself in Active Directory as a computer object. This account must have the right to join computers to the Active Directory domain.

Service Accounts in This VMware Validated Design

This validated design introduces a set of service accounts that are used in a one- or bi-directional fashion to enable secure application communication. You use custom roles to ensure that these accounts have only the least permissions that are required for authentication and data exchange.

Figure 3-1. Service Accounts in VMware Validated Design for Software-Defined Data Center
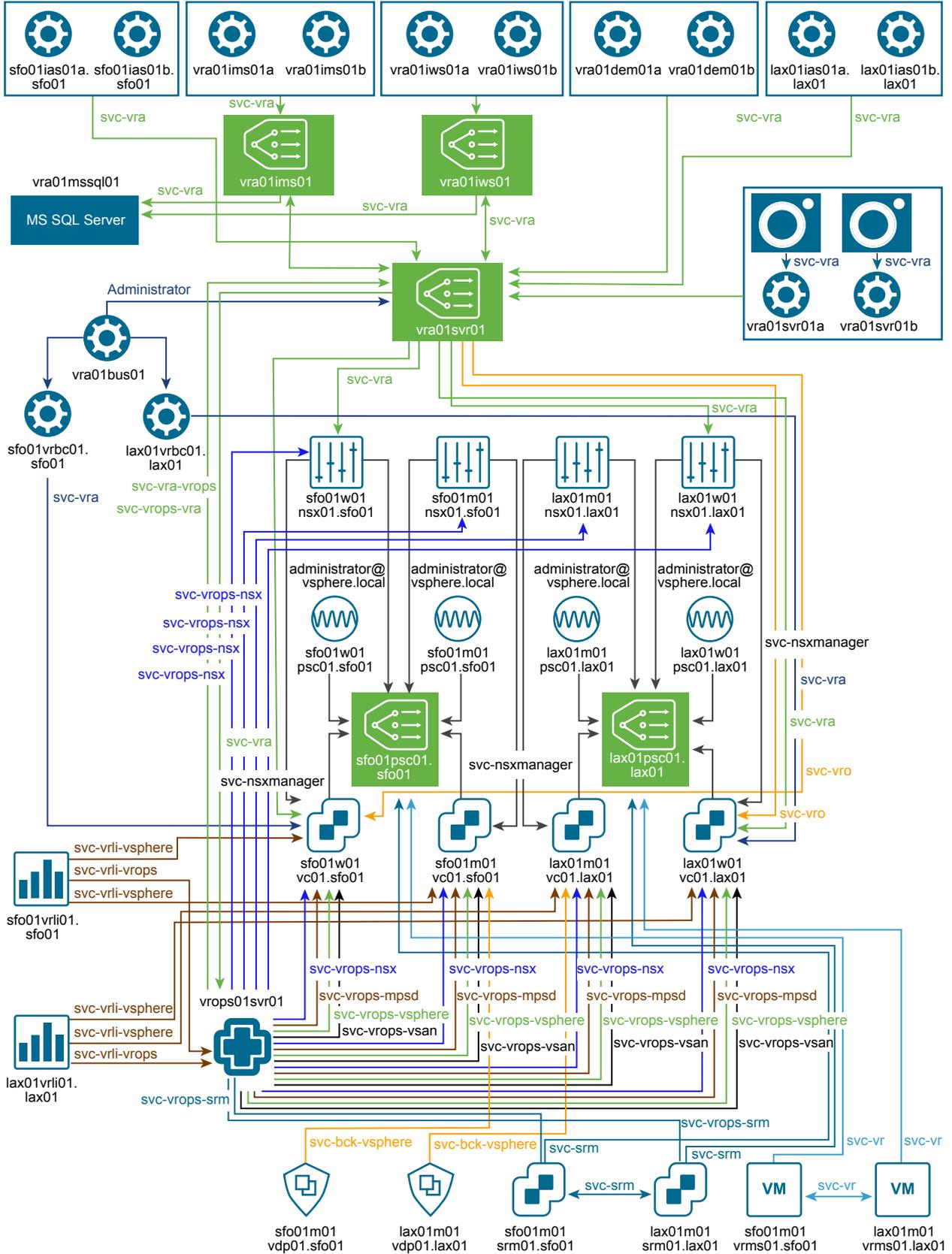
Table 3-27. Application-to-Application or Application Service Accounts in the VMware Validated Design

Username	Source	Destination	Description	Required Role
svc-domain-join	Various management components (one-time domain join action)	Active Directory	Service account for performing domain-join operations from certain SDDC management components.	■ Account Operators Group ■ Delegation to Join Computers to Domain for both the parent and child domains ■ Special access as according to https://support.microsoft.com/en-gb/kb/932455
svc-nsxmanager	NSX for vSphere Manager	vCenter Server	Service account for registering NSX Manager with vCenter Single Sign-on on the Platform Services Controller and vCenter Server for the management cluster and for the shared compute and edge cluster	Administrator
svc-vrli	vRealize Log Insight	Active Directory	Service account for using the Active Directory as an authentication source in vRealize Log Insight	-
svc-vrli-vsphere	vRealize Log Insight	vCenter Server	Service account for connecting vRealize Log Insight to vCenter Server and ESXi for forwarding log information	Log Insight User (vCenter Server)
svc-vrli-vrops	vRealize Log Insight	vRealize Operations Manager	Service account for connecting vRealize Log Insight to vRealize Operations Manager for log forwarding, alerts, and for Launch in Context integration	Administrator
svc-bck-vsphere	vSphere Storage API - Data Protection	vCenter Server	Service account for performing backups using the vSphere Storage API - Data Protection with vCenter Server for the management cluster	VADP Backup Solution Requirements
svc-srm	Site Recovery Manager	vCenter Server	Service account for connecting Site Recover Manager to vCenter Server and for pairing sites in Site Recovery Manager	Single Sign-On Administrator
svc-vr	vSphere Replication	vCenter Server	Service account for connecting vSphere Replication to vCenter Server and for pairing vSphere Replication instances	Single Sign-On Administrator

Table 3-27. Application-to-Application or Application Service Accounts in the VMware Validated Design (Continued)

Username	Source	Destination	Description	Required Role
svc-vra	vRealize Automation	■ vCenter Server ■ vRealize Automation	Service account for access from vRealize Automation to vCenter Server. This account is a part of the vRealize Automation setup process.	■ Administrator ■ vRealize Orchestrator Administrator
svc-vro	vRealize Orchestrator	vCenter Server	Service account for access from vRealize Orchestrator to vCenter Server	Administrator
svc-vrops	vRealize Operations Manager	Active Directory	Service account for Active Directory integration in vRealize Operations Manager for user authentication	-
svc-vrops-vsphere	vRealize Operations Manager	vCenter Server	Service account for monitoring and collecting general metrics about vSphere objects, including infrastructure and virtual machines, from vCenter Server in to vRealize Operations Manager	Read-Only
svc-vrops-nsx	vRealize Operations Manager	■ vCenter Server ■ NSX for vSphere	Local service account for connecting the NSX for vSphere adapter for vRealize Operations Manager to the NSX Manager instances in the SDDC	■ Read-Only (vCenter Server) ■ Enterprise Administrator (NSX)
svc-vrops-vsan	vRealize Operations Manager	vCenter Server	Service account for monitoring and collecting metrics about vSAN components from vCenter Server in to vRealize Operations Manager	MPSD Metrics User
svc-vrops-mpsd	vRealize Operations Manager	vCenter Server	Service account for storage device monitoring of the vCenter Server instances in the SDDC from vRealize Operations Manager	MPSD Metrics User
svc-vrops-srm	vRealize Operations Manager	Site Recovery Manager	Service account for monitoring site recovery of the Management vCenter Server from vRealize Operations Manager	SRM Read-only
svc-vrops-vra	vRealize Operations Manager	vRealize Automation	Service account for connecting the vRealize Automation adapter for vRealize Operations Manager to vRealize Automation	■ IaaS Administrator ■ Infrastructure Architect ■ Software Architect ■ Tenant Administrator ■ Fabric Administrator

Table 3-27. Application-to-Application or Application Service Accounts in the VMware Validated Design (Continued)

Username	Source	Destination	Description	Required Role
svc-vra-vrops	vRealize Automation	vRealize Operations Manager	Service account for integration of health statistics from vRealize Operations Manager in the vRealize Automation portal	Read-Only
svc-umds	vSphere Update Manager Download Service	--	Local service account for configuring the Update Manager Download Service on the host virtual machine	Administrator

User Accounts in the Parent Domain

Create the following user accounts in the parent Active Directory domain rainpole.local:

Table 3-28. User Accounts in the rainpole.local Parent Domain

User Name	Description	Service Account	Member of Groups
vra-admin-rainpole	Tenant administrator role in the SDDC for configuring vRealize Automation according to the needs of your organization including user and group management, tenant branding and notifications, and business policies	No	▪ RAINPOLE\ug-vra-admins-rainpole ▪ RAINPOLE\ug-vROAdmins
vra-arch-rainpole	Tenant blueprint architect role in the SDDC for creating the blueprints that tenants request from the service catalog	No	RAINPOLE\ug-vra-archs-rainpole

Users in the Child Domains

Create the following accounts for user access in each of the child Active Directory domain to provide centralized user access to the SDDC. In the Active Directory, you do not assign any special rights to these accounts other than the default ones.

Table 3-29. User Accounts in the Child Domains

User Name	Description	Service Account	Member of Groups
SDDC-Admin	Global administrative account across the SDDC.	No	RAINPOLE\ug-SDDC-Admins

Certificate Replacement

Before you deploy the SDDC, you must configure a certificate authority and generate certificate files for the management products. According to this validated design you replace the default VMCA- or self-signed certificates of the SDDC management products with certificates that are signed by a certificate authority (CA) during deployment.

- Use the Certificate Generation Utility `CertGenVVD` for automatic generation of Certificate Signing Requests (CSRs) and CA-signed certificate files for all VMware management products that are deployed in this validated design.

  VMware Validated Design comes with the `CertGenVVD` utility that you can use to save time in creating signed certificates. The utility generates CSRs, OpenSSL CA-signed certificates, and Microsoft CA-signed certificates. See VMware Knowledge Base article 2146215.

1 **Create and Add a Microsoft Certificate Authority Template**

  The first step in certificate generation and replacement is setting up a Microsoft Certificate Authority template on the Active Directory (AD) servers for the region. The template contains the certificate authority (CA) attributes for signing certificates of VMware SDDC solutions. After you have created the new template, you add it to the certificate templates of the Microsoft CA.

2 **Use the Certificate Generation Utility to Generate CA-Signed Certificates for the SDDC Management Components**

  Use the VMware Validated Design Certificate Generation Utility (`CertGenVVD`) to generate certificates that are signed by the Microsoft certificate authority (MSCA) for all management product with a single operation.

Create and Add a Microsoft Certificate Authority Template

The first step in certificate generation and replacement is setting up a Microsoft Certificate Authority template on the Active Directory (AD) servers for the region. The template contains the certificate authority (CA) attributes for signing certificates of VMware SDDC solutions. After you have created the new template, you add it to the certificate templates of the Microsoft CA.

Creating a certificate authority template for this VMware Validated Design includes the following operations:

1 Set up a Microsoft Certificate Authority template.

2 Add the new template to the certificate templates of the Microsoft CA.

Prerequisites

This VMware Validated Design sets the Certificate Authority service on the Active Directory (AD) dc01rpl.rainpole.local (root CA) server. The AD server is running on the Microsoft Windows Server 2012 R2 operating system.

- Verify that you installed Microsoft Server 2012 R2 VM with Active Directory Domain Services enabled.

- Verify that the Certificate Authority Service role and the Certificate Authority Web Enrollment role is installed and configured on the Active Directory Server.

- Use a hashing algorithm of SHA-256 or higher on the certificate authority.

Procedure

1   Log in to the rainpole.local AD server by using a Remote Desktop Protocol (RDP) client.

    a   Open an RDP connection to **dc01rpl.rainpole.local**.

    b   Use the following credentials.

Setting	Value
User name	Active directory administrator
Password	*ad_admin_password*

2   Click Windows **Start > Run**, enter **certtmpl.msc**, and click **OK**.

3   In the **Certificate Template Console**, under **Template Display Name**, right-click **Web Server** and click **Duplicate Template**.

4   In the **Duplicate Template** window, leave **Windows Server 2003 Enterprise** selected for backward compatibility and click **OK**.

5   In the **Properties of New Template** dialog box, 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 **Key Usage** and click **Edit**.

    d   Select the **Signature is proof of origin (nonrepudiation)** check box.

    e   Leave the default for all other options.

    f   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 CA, 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 have just created and click **OK** .

Use the Certificate Generation Utility to Generate CA-Signed Certificates for the SDDC Management Components

Use the VMware Validated Design Certificate Generation Utility (`CertGenVVD`) to generate certificates that are signed by the Microsoft certificate authority (MSCA) for all management product with a single operation.

For information about the VMware Validated Design Certificate Generation Utility, see VMware Knowledge Base article 2146215.

Prerequisites

- Provide a Window Server 2012 host that is part of the rainpole.local domain.

- Install a Certificate Authority server on the rainpole.local domain.

Procedure

1   Log in as AD administrator to a Windows Server 2012 host that is a part of rainpole.local domain and has access to the data center.

2   Download the Certificate Generation Utility from the Knowledge Base article and extract it on the host.

    a   Open the VMware Knowledge Base article in a Web browser and download `CertGenVVD-version.zip`.

    b   Extract `CertGenVVD-version.zip` to the C: drive.

3   In the `c:\CertGenVVD-version` folder, open the `default.txt` file in a text editor.

4   Verify that following properties are configured.

```
ORG=Rainpole Inc.
OU=Rainpole.local
LOC=SFO
ST=CA
CC=US
CN=VMware_VVD
keysize=2048
```

5   Verify that only the following files are available in the `c:\CertGenVVD-version\ConfigFiles` folder.

Table 3-30. Certificate Generation Files for Region A

Host Name or Service in Region A		Configuration Files
Virtual Infrastructure Layer		
Platform Services Controller	■ sfo01psc01.sfo01.rainpole.local ■ sfo01m01psc01.sfo01.rainpole.local ■ sfo01w01psc01.sfo01.rainpole.local	sfo01psc01.txt

Table 3-30. Certificate Generation Files for Region A (Continued)

Host Name or Service in Region A		Configuration Files
vCenter Server	sfo01m01vc01.sfo01.rainpole.local	sfo01m01vc01.txt
	sfo01w01vc01.sfo01.rainpole.local	sfo01w01vc01.txt
NSX Manager	sfo01m01nsx01.sfo01.rainpole.local	sfo01m01nsx01.txt
	sfo01w01nsx01.sfo01.rainpole.local	sfo01w01nsx01.txt
Operations Management Layer		
vRealize Operations Manager	▪ vrops01svr01.rainpole.local	vrops-forVVD4.x.txt
	▪ vrops01svr01a.rainpole.local	
	▪ vrops01svr01b.rainpole.local	
	▪ vrops01svr01c.rainpole.local	
vRealize Log Insight	▪ sfo01vrli01.sfo01.rainpole.local	vrli.sfo01.txt
	▪ sfo01vrli01a.sfo01.rainpole.local	
	▪ sfo01vrli01b.sfo01.rainpole.local	
	▪ sfo01vrli01c.sfo01.rainpole.local	
Cloud Management Platform Layer		
vRealize Automation	▪ vra01svr01.rainpole.local	vra.txt
	▪ vra01svr01a.rainpole.local	
	▪ vra01svr01b.rainpole.local	
	▪ vra01iws01.rainpole.local	
	▪ vra01iws01a.rainpole.local	
	▪ vra01iws01b.rainpole.local	
	▪ vra01ims01.rainpole.local	
	▪ vra01ims01a.rainpole.local	
	▪ vra01ims01b.rainpole.local	
	▪ vra01dem01a.rainpole.local	
	▪ vra01dem01b.rainpole.local	
vRealize Business Server	vrb01svr01.rainpole.local	vrb.txt
Business Continuity Layer		
Site Recovery Manager and vSphere Replication	sfo01m01srm01.sfo01.rainpole.local	sfo01m01srm01.txt
	sfo01m01vrms01.sfo01.rainpole.local	sfo01m01vrms01.txt

Table 3-31. Certificate Generation Files for Region B

Host Name or Service in Region B		Configuration Files
Virtual Infrastructure Layer		
Platform Services Controller	▪ lax01psc01.lax01.rainpole.local	lax01psc01.txt
	▪ lax01m01psc01.lax01.rainpole.local	
	▪ lax01w01psc01.lax01.rainpole.local	
vCenter Server	lax01m01vc01.lax01.rainpole.local	lax01m01vc01.txt

Table 3-31. Certificate Generation Files for Region B (Continued)

Host Name or Service in Region B		Configuration Files
	lax01w01vc01.lax01.rainpole.local	lax01w01vc01.txt
NSX Manager	lax01m01nsx01.sfo01.rainpole.local	lax01m01nsx01.txt
	lax01w01nsx01.sfo01.rainpole.local	lax01w01nsx01.txt
Operations Management Layer		
vRealize Log Insight	▪ lax01vrli01.lax01.rainpole.local ▪ lax01vrli01a.lax01.rainpole.local ▪ lax01vrli01b.lax01.rainpole.local ▪ lax01vrli01c.lax01.rainpole.local	vrli.lax01.txt
Business Continuity Layer		
Site Recovery Manager and vSphere Replication	lax01m01srm01.lax01.rainpole.local	lax01m01srm01.txt
	lax01m01vrms01.lax01.rainpole.local	lax01m01vrms01.txt

6　Verify that each configuration file includes FQDNs and host names in the dedicated sections.

For example, the configuration files for the Platform Service Controller instance must contain the following properties:

sfo01psc01.txt	lax01psc01.txt
| ```
[CERT]
NAME=default
ORG=default
OU=default
LOC=SFO
ST=default
CC=default
CN=sfo01psc01.sfo01.rainpole.local
keysize=default
[SAN]
sfo01psc01
sfo01m01psc01
sfo01w01psc01
sfo01psc01.sfo01.rainpole.local
sfo01m01psc01.sfo01.rainpole.local
sfo01w01psc01.sfo01.rainpole.local
``` | ```
[CERT]
NAME=default
ORG=default
OU=default
LOC=LAX
ST=default
CC=default
CN=lax01psc01.lax01.rainpole.local
keysize=default
[SAN]
lax01psc01
lax01m01psc01
lax01w01psc01
lax01psc01.lax01.rainpole.local
lax01m01psc01.lax01.rainpole.local
lax01w01psc01.lax01.rainpole.local
``` |

7　Open a Windows PowerShell prompt and navigate to the `CertGenVVD` folder.

```
cd C:\CertGenVVD-version
```

8　Grant permissions to run third-party PowerShell scripts.

```
Set-ExecutionPolicy Unrestricted
```

9   Validate if you can run the utility using the configuration on the host and verify if VMware is included
    in the printed CA template policy.

```
.\CertgenVVD-version.ps1 -validate
```

10 Generate the MSCA-signed certificates.

```
.\CertGenVVD-version.ps1 -MSCASigned -attrib 'CertificateTemplate:VMware'
```

11 In the `C:\CertGenVVD-version` folder, verify that the utility has created the `SignedByMSCACerts`
    sub-folder.

What to do next

Replace the default product certificates with the certificates that the `CertGenVVD` utility has generated at
deployment time or later if a certificate expires.

Datastore Requirements

For certain features of the SDDC, such as backup and restore, log archiving and content library, you must
provide secondary storage.

This VMware Validated Design uses NFS as its secondary storage. While vRealize Automation supports
any type of secondary storage, using vRealize Log Insight requires NFS storage for archive purposes.

For information about the approximate sizes of all management components, see Chapter 5 Management
Workload Footprint. Consider these sizes in the storage requirements for your VMware vSphere Storage
APIs for Data Protection-based backup solution.

You must also provide a validated datastore to the shared edge and compute cluster for storing NSX
Controller and edge instances, and tenant workloads.

NFS Exports for Management Components

The management applications in the SDDC use NFS exports with the following paths:

Table 3-32. NFS Export Configuration

Region	VLAN	Server	Export	Size	Map As	Cluster	Component
Region A	1615	172.16.15.251	/V2D_vRLI_MgmtA_400GB	400 GB	NFS datastore for log archiving in vRealize Log Insight	Management cluster	vRealize Log Insight
	1625	172.16.25.251	/V2D_vRA_ComputeA_1TB	1 TB	sfo01-w01-lib01	Shared edge and compute cluster	vRealize Automation

Table 3-32. NFS Export Configuration (Continued)

Region	VLAN	Server	Export	Size	Map As	Cluster	Component
Region B	1715	172.17.15.251	/V2D_vRLI_MgmtB_400GB	400 GB	NFS mount for log archiving in vRealize Log Insight	Management cluster	vRealize Log Insight
	1725	172.17.25.251	/V2D_vRA_ComputeB_1TB	1 TB	lax01-w01-lib01	Shared edge and compute cluster	vRealize Automation

Customer-Specific Datastore for the Shared Edge and Compute Clusters

To enable the deployment of virtual appliances that are a part of the NSX deployment and to provide storage for tenant workloads, before you begin implementing your SDDC, you must set up datastores for the shared edge and compute cluster for each region. This validated design contains guidance for datastore setup only for the SDDC management components. For more information about the datastore types that are supported for the shared and edge cluster, see *Shared Storage Design* in the *VMware Validated Design Architecture and Design* documentation.

Virtual Machine Specifications 4

This validated design uses a set of virtual machines for management components and tenant blueprints. Create these virtual machines, configure their virtual hardware, and install the required guest operating system.

Management Virtual Machine Specifications

You must create virtual machines for Site Recovery Manager, vSphere Update Manager Download Service (UMDS), and Microsoft SQL Server before you start the deployment of these management components.

For information on the networking configuration of the virtual machines, such as host name, IPv4 address, default gateway, and so on, see Host Names and IP Addresses in Region A and Host Names and IP Addresses in Region B.

Table 4‑1. Specifications of Management Virtual Machines in Region A

Attribute	Region	Site Recovery Manager	vSphere Update Manager Download Service	Microsoft SQL Server
Number of virtual machines	-	1	1	1
Guest OS	-	Windows Server 2012 R2 (64-bit)	Ubuntu Server 14.04 LTS	Windows Server 2012 R2 (64-bit)
VM name	Region A	sfo01m01srm01	sfo01umds01	vra01mssql01
VM folder	Region A	sfo01-m01fd-bcdr	sfo01-m01fd-mgmt	sfo1-m01fd-vra
Cluster	Region A	sfo01-m01-mgmt01	sfo01-m01-mgmt01	sfo01-m01-mgmt01
Datastore	Region A	sfo01-m01-vsan01	sfo01-m01-vsan01	sfo01-m01-vsan01
Number of CPUs	-	2	2	8
Memory (GB)	-	4	2	16
Disk space (GB)	-	40	120	200
SCSI Controller	-	LSI Logic SAS	LSI Logic SAS	LSI Logic SAS

Table 4-1. Specifications of Management Virtual Machines in Region A (Continued)

Attribute	Region	Site Recovery Manager	vSphere Update Manager Download Service	Microsoft SQL Server
Virtual machine network adapter	-	VMXNET3	VMXNET3	VMXNET3
Virtual machine network	Region A	sfo01-m01-vds01-management	Mgmt-RegionA01-VXLAN	Mgmt-xRegion01-VXLAN
Active Directory domain	Region A	sfo01.rainpole.local	sfo01.rainpole.local	rainpole.local
Service account	-	Windows administrator	svc-umds	svc-vra
VMware Tools	Latest version	Latest version	Latest version	Latest version

Table 4-2. Specifications of Management Virtual Machines in Region B

Attribute	Region	Site Recovery Manager	vSphere Update Manager Download Service
Number of virtual machines	-	1	1
Guest OS	-	Windows Server 2012 R2 (64-bit)	Ubuntu Server 14.04 LTS
VM name	Region B	lax01m01srm01	lax01umds01
VM folder	Region B	lax01-m01fd-bcdr	lax01-m01fd-mgmt
Cluster	Region B	lax01-m01-mgmt01	lax01-m01-mgmt01
Datastore	Region B	lax01-m01-vsan01	lax01-m01-vsan01
Number of CPUs	-	2	2
Memory (GB)	-	4	2
Disk space (GB)	-	40	120
SCSI Controller	-	LSI Logic SAS	LSI Logic SAS
Virtual machine network adapter	-	VMXNET3	VMXNET3
Virtual machine network	Region B	lax01-m01-vds01-management	Mgmt-RegionB01-VXLAN
Active Directory domain	Region B	lax01.rainpole.local	lax01.rainpole.local
Service account	-	Windows administrator	svc-umds
VMware Tools	Latest version	Latest version	Latest version

Specifications for Tenant Blueprints

To create a tenant blueprint in vRealize Automation, this validated design uses a set of virtual machines according to predefined specifications.

Table 4-**3.** **Specifications for the VM Blueprint Templates**

Required by VMware Component	VM Template Name	Guest OS	CPUs	Memory (GB)	Virtual Disk (GB)	SCSI Controller	Virtual Machine Network Adapter
vRealize Automation	redhat6-enterprise-64	Red Hat Enterprise Linux 6 (64-bit)	1	6	20	LSI Logic SAS	VMXNET3
	windows-2012 r2-64	Windows Server 2012 R2 (64-bit)	1	4	50	LSI Logic SAS	VMXNET3
	windows-2012 r2-64-sql2012	Windows Server 2012 R2 (64-bit)	1	8	100	LSI Logic SAS	VMXNET3

Management Workload Footprint

5

Before you deploy the SDDC, you must allocate enough compute and storage resources to accommodate the footprint of the management workloads.

This chapter includes the following topics:

- Management Workload Footprint in Region A
- Management Workload Footprint for Region B

Management Workload Footprint in Region A

Before you deploy the SDDC, you must allocate enough compute and storage resources to accommodate the footprint of the management workloads .

Note Storage footprint shows allocated space. Do not consider it if you use thin provisioning according to this validated design.

Virtual Infrastructure Layer

Allocate the following number of virtual CPUs, amount of RAM and storage space for the management components of the virtual Infrastructure layer in Region A of the SDDC:

Table 5-1. Virtual Infrastructure Layer Footprint for Region A

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
Management vCenter Server	Virtual Appliance	4	16	270
Management Platform Services Controller	Virtual Appliance	2	4	55
Management NSX Manager	Virtual Appliance	4	16	60
Management NSX Controller 01	Virtual Appliance	4	4	28
Management NSX Controller 02	Virtual Appliance	4	4	28

Table 5-1. Virtual Infrastructure Layer Footprint for Region A (Continued)

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
Management NSX Controller 03	Virtual Appliance	4	4	28
Management NSX Edge Services Gateway 1 - ECMP	Virtual Appliance	2	1	2
Management NSX Edge Services Gateway 2 - ECMP	Virtual Appliance	2	1	2
Management NSX Edge Services Gateway 1 - Load Balancer	Virtual Appliance	2	1	2
Management NSX Edge Services Gateway 2 - Load Balancer	Virtual Appliance	2	1	2
Management NSX Edge Services Gateway 1 - UDLR	Virtual Appliance	2	1	2
Management NSX Edge Services Gateway 2 - UDLR	Virtual Appliance	2	1	2
Management NSX Edge Services Gateway 1 - OneArm Load Balancer	Virtual Appliance	2	1	2
Management NSX Edge Services Gateway 2 - OneArm Load Balancer	Virtual Appliance	2	1	2
Compute vCenter Server	Virtual Appliance	16	32	599
Compute Platform Services Controller	Virtual Appliance	2	4	55
Compute NSX Manager	Virtual Appliance	4	16	60
Compute NSX Controller 01	Virtual Appliance	4	4	28
Compute NSX Controller 02	Virtual Appliance	4	4	28
Compute NSX Controller 03	Virtual Appliance	4	4	28
Compute NSX Edge Services Gateway 1 - ECMP	Virtual Appliance	2	1	2
Compute NSX Edge Services Gateway 2 - ECMP	Virtual Appliance	2	1	2

Table 5-1. Virtual Infrastructure Layer Footprint for Region A (Continued)

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
Compute NSX Edge Services Gateway 1 - UDLR	Virtual Appliance	2	1	2
Compute NSX Edge Services Gateway 2 - UDLR	Virtual Appliance	2	1	2
Compute NSX Edge Services Gateway 1 - DLR	Virtual Appliance	2	1	2
Compute NSX Edge Services Gateway 2 - DLR	Virtual Appliance	2	1	2
Update Manager Download Service	Linux Virtual Machine	2	2	120
Total		86	128	1,415

Operations Management Layer

Allocate the following number of virtual CPUs, amount of RAM and storage space for the management components of the operations management layer in Region A of the SDDC:

Table 5-2. Operations Management Layer Footprint for Region A

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
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 Operations Manager Remote Collector 1	Virtual Appliance	2	4	274
vRealize Operations Manager Remote Collector 2	Virtual Appliance	2	4	274
vRealize Log Insight Node 1	Virtual Appliance	8	16	530.5

Table 5-2. Operations Management Layer Footprint for Region A (Continued)

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
vRealize Log Insight Node 2	Virtual Appliance	8	16	530.5
vRealize Log Insight Node 3	Virtual Appliance	8	16	530.5
Total		52	152	5,211.5

Cloud Management Layer

Allocate the following number of virtual CPUs, amount of RAM and storage space for the management components of the cloud management layer in Region A of the SDDC:

Table 5-3. Cloud Management Layer Footprint for Region A

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
vRealize Automation Appliance 1	Virtual Appliance	4	18	140
vRealize Automation Appliance 2	Virtual Appliance	4	18	140
vRealize Automation IaaS Web Server 1	Windows Server Virtual Machine	2	4	60
vRealize Automation IaaS Web Server 2	Windows Server Virtual Machine	2	4	60
vRealize Automation IaaS Manager Server 1	Windows Server Virtual Machine	2	4	60
vRealize Automation IaaS Manager Server 2	Windows Server Virtual Machine	2	4	60
vRealize Automation IaaS DEM Worker 1	Windows Server Virtual Machine	2	6	60
vRealize Automation IaaS DEM Worker 2	Windows Server Virtual Machine	2	6	60
vRealize Automation Proxy Agent 1	Windows Server Virtual Machine	2	4	60
vRealize Automation Proxy Agent 2	Windows Server Virtual Machine	2	4	60
vRealize Business for Cloud Server	Virtual Appliance	4	8	50
vRealize Business for Cloud Data Collector	Virtual Appliance	4	2	50
Microsoft SQL Server	Windows Server Virtual Machine	8	16	200

Table 5-3. Cloud Management Layer Footprint for Region A (Continued)

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
Total		40	98	1,060

Business Continuity Layer

Allocate the following number of virtual CPUs, amount of RAM and storage space for the management components of the business continuity layer of the SDDC in Region A:

Table 5-4. Business Continuity Layer Footprint for Region A

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
Management Site Recovery Manager	Windows Server Virtual Machine	2	4	40
Management vSphere Replication	Virtual Appliance	4	4	18
Total		6	8	58

Management Workload Footprint for Region B

Before you deploy the SDDC, you must allocate enough compute and storage resources to accommodate the footprint of the management workloads in Region B.

Note Storage footprint shows allocated space. Do not consider it if you use thin provisioning according to this validated design.

Virtual Infrastructure Layer

Allocate the following number of virtual CPUs, amount of RAM and storage space for the management components of the virtual infrastructure layer of the SDDC in Region B:

Table 5-5. Virtual Infrastructure Layer Footprint for Region B

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
Management vCenter Server	Virtual Appliance	4	16	270
Management Platform Services Controller	Virtual Appliance	2	4	55
Management NSX Manager	Virtual Appliance	4	16	60

Table 5-5. Virtual Infrastructure Layer Footprint for Region B (Continued)

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
Management NSX Edge Services Gateway 1 - ECMP	Virtual Appliance	2	1	2
Management NSX Edge Services Gateway 2 - ECMP	Virtual Appliance	2	1	2
Management NSX Edge Services Gateway 1 - Load Balancer	Virtual Appliance	2	1	2
Management NSX Edge Services Gateway 2 - Load Balancer	Virtual Appliance	2	1	2
Management NSX Edge Services Gateway 1 - UDLR	Virtual Appliance	2	1	2
Management NSX Edge Services Gateway 2 - UDLR	Virtual Appliance	2	1	2
Management NSX Edge Services Gateway 1 - OneArm Load Balancer	Virtual Appliance	2	1	2
Management NSX Edge Services Gateway 2 - OneArm Load Balancer	Virtual Appliance	2	1	2
Compute vCenter Server	Virtual Appliance	16	32	599
Compute Platform Services Controller	Virtual Appliance	2	4	55
Compute NSX Manager	Virtual Appliance	4	16	60
Compute NSX Controller 01	Virtual Appliance	4	4	28
Compute NSX Controller 02	Virtual Appliance	4	4	28
Compute NSX Controller 03	Virtual Appliance	4	4	28
Compute NSX Edge Services Gateway 1 - ECMP	Virtual Appliance	2	1	2
Compute NSX Edge Services Gateway 2 - ECMP	Virtual Appliance	2	1	2

Table 5-5. Virtual Infrastructure Layer Footprint for Region B (Continued)

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
Compute NSX Edge Services Gateway 1 - UDLR	Virtual Appliance	2	1	2
Compute NSX Edge Services Gateway 2 - UDLR	Virtual Appliance	2	1	2
Compute NSX Edge Services Gateway 1 - DLR	Virtual Appliance	2	1	2
Compute NSX Edge Services Gateway 2 - DLR	Virtual Appliance	2	1	2
Update Manager Download Service	Linux Virtual Machine	2	2	120
Total		74	116	1,331

Operations Management Layer

Allocate the following number of virtual CPUs, amount of RAM and storage space for the management components of the operations management layer of the SDDC in Region B:

Table 5-6. Operations Management Layer Footprint for Region B

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
vRealize Operations Manager Remote Collector 1	Virtual Appliance	2	4	274
vRealize Operations Manager Remote Collector 2	Virtual Appliance	2	4	274
vRealize Log Insight Node 1	Virtual Appliance	8	16	530.5
vRealize Log Insight Node 2	Virtual Appliance	8	16	530.5
vRealize Log Insight Node 3	Virtual Appliance	8	16	530.5
Total		28	56	2,139.5

Cloud Management Layer

Allocate the following number of virtual CPUs, amount of RAM and storage space for the management components of the cloud management layer of the SDDC:

Table 5-7. Cloud Management Layer Footprint for Region B

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
vRealize Automation Proxy Agent 1	Windows Server Virtual Machine	2	4	60
vRealize Automation Proxy Agent 2	Windows Server Virtual Machine	2	4	60
vRealize Business for Cloud Data Collector	Virtual Appliance	4	2	50
Total		8	10	170

Business Continuity Layer

Allocate the following number of virtual CPUs, amount of RAM and storage space for the management components of the business continuity layer of the SDDC:

Table 5-8. Business Continuity Layer Footprint for Region B

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
Management Site Recovery Manager	Windows Server Virtual Machine	2	4	40
Management vSphere Replication	Virtual Appliance	4	4	18
Total		6	8	58

Additional Footprint for Disaster Recovery

Allocate the following number of virtual CPUs, amount of RAM and storage space for the management components of the SDDC that are replicated and failed over to Region B as part of the disaster recovery plans.

Table 5-9. Disaster Recovery Footprint in Region B

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
Management NSX Controller 01	Virtual Appliance	4	4	28
Management NSX Controller 02	Virtual Appliance	4	4	28

Table 5-9. Disaster Recovery Footprint in Region B (Continued)

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
Management NSX Controller 03	Virtual Appliance	4	4	28
vRealize Operations Manager Node 1	Virtual Appliance	8	32	1,048
vRealize Operations Manager Node 2	Virtual Appliance	8	32	1,048
vRealize Operations Manager Node 3	Virtual Appliance	8	32	1,048
vRealize Automation Appliance 1	Virtual Appliance	4	18	140
vRealize Automation Appliance 2	Virtual Appliance	4	18	140
vRealize Automation IaaS Web Server 1	Windows Server Virtual Machine	2	4	60
vRealize Automation IaaS Web Server 2	Windows Server Virtual Machine	2	4	60
vRealize Automation IaaS Manager Server 1	Windows Server Virtual Machine	2	4	60
vRealize Automation IaaS Manager Server 2	Windows Server Virtual Machine	2	4	60
vRealize Automation IaaS DEM Worker 1	Windows Server Virtual Machine	2	6	60
vRealize Automation IaaS DEM Worker 2	Windows Server Virtual Machine	2	6	60
vRealize Business for Cloud Server	Virtual Appliance	4	8	50
Microsoft SQL Server	Windows Server Virtual Machine	8	16	200
Total		68	196	4,118