Planning and Preparation

Modified on 21 DEC 2017
VMware Validated Design 4.1
VMware Validated Design for Micro-Segmentation 4.1

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 Planning and Preparation

The *Planning and Preparation* document for the VMware Validated Design for Micro-Segmentation provides detailed information about the requirements for software, tools and external services for this use case.

Before you start deploying the components of the 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 in the data center. Carefully review the *Planning and Preparation* documentation to avoid costly rework and delays

Intended Audience

This information is intended for anyone who wants to install, upgrade, or use the VMware Validated Design for Micro-Segmentation. The information is written for experienced Windows or Linux system administrators who are familiar with virtual machine technology and data center operations.

VMware Validated Design for the SDDC and this Use Case Documentation

For details on product deployment, see the sections on vSphere, NSX and vRealize LogInsight in the VMware Validated Design for Software-Defined Data Center Deployment for Region A documentation. After initial deployment, the product documentation for vSphere and for NSX for vSphere enables you to set up your environment. Because this documentation is already available, the Validated Design for Micro-Segmentation does not include detailed step-by-step instructions for each task.

1 Software Requirements

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

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

Table 1-1. 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 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 1-2. Third-Party Software Required for the VMware Validated Design

SDDC Layer	Required by VMware Component	Vendor	Product Item	Product Version
Virtual Infrastructure	An end user 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.

External Services

2

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

This chapter includes the following topics:

External Services Overview

External services include Active Directory, DHCP, DNS, NTP, SMTP Mail Relay, an FTP server, and certificate services.

Active Directory

This validated design uses Microsoft Active Directory (AD) for authentication and authorization to resources within 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 2-1. Requirements for the Active Directory Service

Requirement	Domain Instance	Domain Name	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 2-2. 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

DNS is an important component for the operation of the SDDC. For a multi-region deployment, you must provide a root and child domains which contain separate DNS records.

Table 2-3. DNS Configuration Requirements

Requirement	Domain Instance	Description
DNS host entries	rainpole.local	Resides in the rainpole.local domain.
	sfo01.rainpole.local and lax01.rainpole.local	DNS servers 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 documentation.

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

NTP

All components within 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 2-4. NTP Server Configuration Requirements

Requirement	Description
NTP	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 pods as the NTP servers or the upstream physical router. These switches should synchronize with different upstream NTP servers and provide time synchronization capabilities within the SDDC. As a best practice, make the NTP servers available under a friendly FQDN, for example, ntp.sfo01.rainpole.local for Region A, or ntp.lax01.rainpole.local for Region B.

SMTP Mail Relay

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

Table 2-5. 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 Certificate Authority (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 2-6. CA Requirements for Signing Certificates of Management Applications

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 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 2-7. FTP Server Requirements

Requirement	Description
FTP server	An FTP server must host NSX Manager backups. The server must support SFTP and FTP. The 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 2-8. Requirements for a Windows Host Machine

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 2-9. 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 allocated 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 2-10. VLAN and IP Subnet Configuration in Region A

Pod in Region A	VLAN Function	VLAN ID	Subnet	Gateway
Management Pod	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 Pod	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 2-10. VLAN and IP Subnet Configuration in Region A (Continued)

Pod 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 2-11. VLAN and IP Subnet Configuration in Region B

Region B	VLAN Function	VLAN ID	Subnet	Gateway
Management Pod	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 Pod	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 2-12. 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 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 fully qualified domain names (FQDNs) that map them to the IP addresses.

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 provide host names and IP addresses that are required for the SDDC deployment in the region.

Host Names and IP Addresses for External Services in Region A

Allocate DNS names and IP addresses to the NTP and Active Directory servers in Region A.

Table 2-13. Host Names and IP Addresses for the External Services in Region A

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

Table 2-13. Host Names and IP Addresses for the External Services in Region A (Continued)

Component Group	Host Name	DNS Zone	IP Address	Description
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 Components in Region A

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

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

- Platform Services Controllers
- vCenter Servers
- NSX Managers
- NSX Controllers
- NSX Edge Services Gateways
- Site Recovery Manager
- vSphere Replication

Table 2-14. Host Names and IP Addresses for the Virtual Infrastructure Components 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 vCenter Server
	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 Compute vCenter Server
	sfo01w01vc01	sfo01.rainpole.local	172.16.11.64	Compute vCenter Server
	sfo01w01esx01	sfo01.rainpole.local	172.16.31.101	ESXi host in the shared edge and compute pod
	sfo01w01esx02	sfo01.rainpole.local	172.16.31.102	

Table 2-14. Host Names and IP Addresses for the Virtual Infrastructure Components in Region A (Continued)

Component Group	Host Name	DNS Zone	IP Address	Description
	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 Controllers 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 Controllers 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 Controllers.
	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
	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 Components in Region A

Allocate host names and IP addresses for vRealize Log Insight.

In Region A, allocate host names and IP addresses to vRealize Log Insight and configure DNS with a FQDN that maps to the IP address where defined.

Table 2-15. Host Names and IP Addresses for the Operations Management Component in Region A

Component Group	Host Name	DNS Zone	IP Address	Description
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 in Region B

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

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

Allocate DNS names and IP addresses to the NTP and Active Directory servers in Region B.

Table 2-16. 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
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 Components in Region B

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

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

- Platform Services Controllers
- vCenter Servers
- NSX Managers
- NSX Controllers
- NSX Edge Services Gateways

Table 2-17. Host Names and IP Addresses for the Virtual Infrastructure Components 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 vCenter Server
	lax01m01vc01	lax01.rainpole.local	172.17.11.62	Management vCenter Server
	lax01m01esx01	lax01.rainpole.local	172.17.11.101	ESXi host 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 Compute vCenter Server
	lax01w01vc01	lax01.rainpole.local	172.17.11.64	Compute vCenter Server
	lax01w01esx01	lax01.rainpole.local	172.17.31.101	ESXi host 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
	lax01m01nsxc01	-	172.17.11.118	NSX Controllers 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 Controllers for the shared edge and compute cluster
	lax01w01nsxc02	-	172.17.31.119	

Table 2-17. Host Names and IP Addresses for the Virtual Infrastructure Components in Region B (Continued)

Component Group	Host Name	DNS Zone	IP Address	Description
	lax01w01nsxc03	-	172.17.31.120	
	lax01psc01	lax01.rainpole.local	172.17.11.71	NSX Edge device for load balancing the Platform Services Controllers.
	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 the Operations Management Components in Region B

Allocate DNS names and IP addresses to vRealize Log Insight nodes in Region B before you deploy these SDDC management applications.

In Region B, allocate host names and IP addresses to vRealize Log Insight and configure DNS with a FQDN that maps to the IP address where defined.

Table 2-18. Host Names and IP Addresses for Operations Management Components in Region B

Component Group	Host Name	DNS Zone	IP Address	Description
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

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 critical for the proper operation of the components in the SDDC because in certain cases they rely on vCenter Single Sign-on.

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 2-19. 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 2-20. 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 within 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 validated design, you must provide a 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 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 `ad_admin_acct` of 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 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 Assign access right and permissions to the local groups in the child domains according to their role.

Universal Groups in the Parent Domain

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

Table 2-21. 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.

Global Groups in the Child Domains

In each child domain, sfo01.rainpole.local and lax01.rainpole.local, add the role-specific universal group from the parent domain to the relevant role-specific global group in the child domain.

Table 2-22. Global Groups in the sfo01.rainpole.local and lax01.rainpole.local 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.
- The 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 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.

Table 2-23. Application-to-Application or Application Service Accounts in the VMware Validated Design

Username	Source	Destination	Description	Required Role
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 compute and edge clusters	Administrator
svc-vrli	vRealize Log Insight	vCenter Server	Service account for using the Active Directory as an authentication source in vRealize Log Insight and for connecting vRealize Log Insight to vCenter Server and ESXi in order to forwarding log information	Log Insight User (vCenter Server)

Users in the Child Domains

Create the following accounts for user access in each of the child Active Directory domain, sfo01.rainpole.local and lax01.rainpole.local, 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 2-24. User Accounts in the sfo01.rainpole.local and lax01.rainpole.local 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.

- If the `CertGenVVD` utility is not an option for deployment, follow the validated manual steps to create certificates.

1 Create and Add a Microsoft Certificate Authority Template

   You create a Microsoft Certificate Authority Template to contain the certificate authority (CA) attributes for signing certificates of VMware SDDC solution.

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.

3 Generate CA-Signed Certificates for the SDDC Management Components

   When you replace the default certificates of the SDDC management products, you can manually generate certificate files that are signed by the intermediate Certificate Authority (CA). You have set up the Certificate Authority earlier on the Active Directory server.

Create and Add a Microsoft Certificate Authority Template

You create a Microsoft Certificate Authority Template to contain the certificate authority (CA) attributes for signing certificates of VMware SDDC solution.

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 CA up on both Active Directory (AD) servers: the main domain dc01rpl.rainpole.local (root CA) and the Region A subdomain dc01sfo.sfo01.rainpole.local (the intermediate CA). Both AD servers are running the Microsoft Windows Server 2012 R2 operating system.

- Verify that you installed Microsoft Server 2012 R2 VMs with Active Directory Domain Services enabled.
- Verify that тhe Certificate Authority Service role and the Certificate Authority Web Enrolment role is installed and configured on both Active Directory Server.
- Verify that dc01sfo.sfo01.rainpole.local has been set up to be the intermediate CA of the root CA dc01rpl.rainpole.local.
- Use a hashing algorithm of SHA-2 or higher on the certificate authority.

Procedure

1 Log in to the AD server by using a Remote Desktop Protocol (RDP) client as the AD administrator with the *ad_admin_password* password.
   - If you use the intermediate CA, connect to dc01sfo.sfo01.rainpole.local.
   - If you use only the root CA, connect dc01rpl.sfo01.rainpole.local.

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 **Enable Certificate Templates** dialog box, select the VMware certificate that you just created in the **Name** column 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 complete information about the VMware Validated Design Certificate Generation Utility, see VMware Knowledge Base article 2146215.

Procedure

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

2 Download and extract the Certificate Generation Utility from VMware Knowledge Base article 2146215.

   a Open the VMware Knowledge Base article in a Web browser.

   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.

- comp01nsxm01.sfo01.txt
- comp01nsxm51.lax01.txt
- comp01vc01.sfo01.txt
- comp01vc51.lax01.txt
- mgmt01nsxm01.sfo01.txt
- mgmt01nsxm51.lax01.txt
- sfo01psc01.sfo01.txt
- lax01psc51.lax01.txt
- mgmt01srm01.sfo01.txt
- mgmt01srm51.lax01.txt
- mgmt01vc01.sfo01.txt
- mgmt01vc51.lax01.txt
- mgmt01vdp01.sfo01.txt
- mgmt01vdp51.lax01.txt
- mgmt01vrms01.sfo01.txt
- mgmt01vrms51.lax01.txt
- vra.txt
- vrb.txt
- vrli.lax01.txt
- vrli.sfo01.txt

- vro.txt
- vrops.txt

6 If `sfo01psc01.txt` or `lax01psc01.txt` does not exist, make a copy of `sfo01m01vc01.txt` and save it as `sfo01psc01.txt` or `lax01psc01.txt`.

7 Open the copied file in a text editor, and verify that the following properties are configured.

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

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

For example, run the following command if you use version 3.0.1 of the Certificate Generation Utility.

```
cd c:\CertGenVVD-3.0.1
```

9 Run the following command to grant PowerShell permissions to run third -party shell scripts.

```
Set-ExecutionPolicy RemoteSigned
```

10 Run the following command to validate prerequisites for running the utility.

Verify that VMware is included in the available CA Template Policy.

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

11 Run the following command to generate MSCA-signed certificates.

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

12 In the `c:\CertGenVVD-version` folder, verify that the utility 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.

Generate CA-Signed Certificates for the SDDC Management Components

When you replace the default certificates of the SDDC management products, you can manually generate certificate files that are signed by the intermediate Certificate Authority (CA). You have set up the Certificate Authority earlier on the Active Directory server.

Prerequisites

Generate a CSR for the certificate that you want to replace. You generate the CSR on the machine where the certificate is installed.

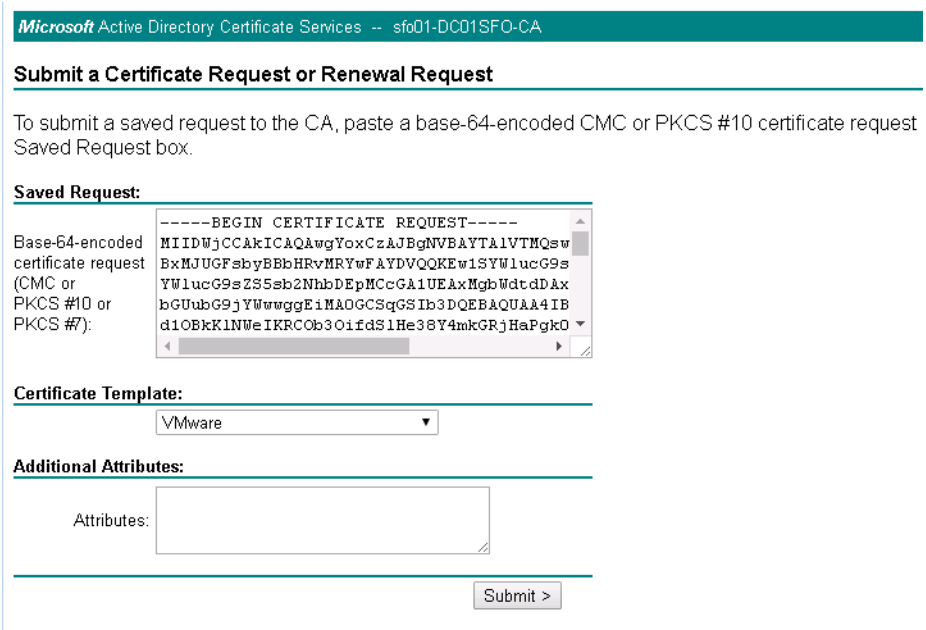
Procedure

1. Log in to the Windows host that has access to the AD server as an administrator.
2. Submit a request and download the certificate chain that contains the CA-signed certificate and the CA certificate.
   a. Open a Web Browser and go to **`http://dc01sfo.sfo01.rainpole.local/CertSrv/`** to open the Web interface of the CA server.
   b. Log in using the following credentials.

Setting	Value
User name	AD administrator
Password	*ad_admin_password*

   c. Click the **Request a certificate** link.
   d. Click **advanced certificate request**.
   e. Open the CSR file `.csr` in a plain text editor.
   f. Copy everything from `-----BEGIN CERTIFICATE REQUEST-----` to `-----END CERTIFICATE REQUEST-----` to the clipboard.
   g. On the **Submit a Certificate Request or Renewal Request** page, paste the contents of the CSR file into the **Saved Request** box.

h From the **Certificate Template** drop-down menu, select **VMware** and click **Submit**.



i On the **Certificate issued** screen, click **Base 64 encoded**.

j Click the **Download Certificate chain** link and save the certificate chain file `certnew.p7b` to the `Downloads` folder.

3 Export the machine certificate to the correct format.

a Double-click the `certnew.p7b` file to open it in the Microsoft Certificate Manager.

b Navigate to **certnew.p7b > Certificates** and notice the three certificates.

c Right-click the machine certificate and select **All Tasks > Export**.

d In the **Certificate Export Wizard**, click **Next**.

e Select **Base-64 encoded X.509 (.CER)** and click **Next**.

f Browse to `C:\certs` and specify the certificate name in the **File name** text box.

g Click **Next** and click **Finish**.

The certificate file is saved to the `C:\certs` folder.

4 Export the intermediate CA certificate file to the correct format.

a Double-click the `certnew.p7b` file to open it in the Microsoft Certificate Manager.

b Navigate to **certnew.p7b** > **Certificates** and notice the three certificates.

c Right-click the intermediate CA certificate and select **All Tasks > Export**.

d In the **Certificate Export Wizard**, click **Next**.

e Select **Base-64 encoded X.509 (.CER)** and click **Next**.

f Browse to `C:\certs` and enter **`Intermediate`** in the **File name** text box.

g Click **Next** and click **Finish**.

The `Intermediate.cer` file is saved to the `C:\certs` folder.

5 Export the root CA certificate file in the correct format.

a Right-click the root certificate and select **All Tasks > Export**.

b In the **Certificate Export Wizard**, click **Next**.

c Select **Base-64 encoded X.509 (.CER)** and click **Next**.

d Browse to `C:\certs` and enter **`Root64`** in the **File name** text box.

e Click **Next** and click **Finish**.

The `Root64.cer` file is saved to the `C:\certs` folder.

Datastore Requirements

For certain features of the SDDC, such as backup and restore, log archiving and content library, you must provide secondary storage. You must also provide a validate datastore to the shared edge and compute cluster for storing NSX Controller and edge instances and tenant workloads.

This VMware Validated Design uses NFS as its secondary storage. While vRealize Automation and vSphere Data Protection support any type of secondary storage, using vRealize Log Insight requires NFS storage.

NFS Exports for Management Components

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

Table 2-25. 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
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

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.

Management Workload Footprint

Management Workload Footprint for Region A

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

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

Virtual Infrastructure Footprint

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 A:

Table 2-26. Virtual Infrastructure 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
Management NSX Controller 03	Virtual Appliance	4	4	28
Management NSX Edge Services Gateway 1 - ECMP	Virtual Appliance	2	1	2

Table 2-26. Virtual Infrastructure Footprint for Region A (Continued)

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
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
Management Site Recovery Manager	Windows Server Virtual Machine	2	4	40
Management vSphere Replication	Virtual Appliance	4	4	18
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 2-26. Virtual Infrastructure 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
Total	-	90	134	1,353

Operations Management

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 A:

Table 2-27. Operations Management Footprint for Region A

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
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	-	24	48	1,591.5

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.

Virtual Infrastructure Footprint

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 2-28. Virtual Infrastructure 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
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
Management Site Recovery Manager	Windows Server Virtual Machine	2	4	40
Management vSphere Replication	Virtual Appliance	4	4	18
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

Table 2-28. Virtual Infrastructure Footprint for Region B (Continued)

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
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
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 Gateway2 - DLR	Virtual Appliance	2	1	2
Total	-	78	122	1,269

Operations Management

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 2-29. Operations Management Footprint for Region B

Management Component	Operating System	vCPUs	vRAM (GB)	Storage (GB)
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	-	24	48	1,353