VMware Validated Design™ Planning and Preparation Guide

VMware Validated Design for Software-Defined Data Center 3.0

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-002250-00

vmware®

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:
docfeedback@vmware.com

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

© 2016 VMware, Inc. All rights reserved.

Contents

1. Purpose and Intended Audience

VMware Validated Design Planning and Preparation Guide provides detailed information about the requirements to software, tools and external services required to successfully implement the VMware Validated Design for Software-Defined Data Center platform.

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 of the SDDC. Review carefully the *VMware Validated Design Planning and Preparation Guide* documentation at least 2 weeks ahead of deployment to avoid costly re-work and delays.

Note The *VMware Validated Design Planning and Preparation Guide* is compliant and validated with certain product versions. See VMware Validated Design Release Notes for more information about supported product versions.

VMware Validated Design Planning and Preparation Guide 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.

2. 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 machine that is connected to the ESXi management network in the management pod.

2.1 VMware Software

Download and license the VMware software products that this VMware Validated Design uses for deploying an SDDC. For information about the required VMware software, see *VMware Validated Design Release Notes*.

2.2 VMware Scripts and Tools

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

Table 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.
Cloud Management	vRealize Automation	`certgen.sh` script	VMware Knowledge Base article 2107816	Script for automated generation of a Certificate Signing Request (CSR) for CA-signed SSL certificates.

2.3 Third-Party Software

Download and license the following third-party software products.

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

SDDC Layer	Required by VMware Component	Vendor	Product Item	Product Version
Virtual Infrastructure	Windows host that is connected to the ESXi management network and has access to the data center	Microsoft	Windows OS that is supported for the vSphere Client 6.0 U2. See VMware Knowledge Base article 2100436.	Version of the Windows OS that is supported for the vSphere Client 6.0 U2
	VMware Site Recovery Manager	Microsoft	Windows 2012 R2 Standard	Windows Server 2012 R2 Update (x64)
Cloud Management	vRealize Automation	Microsoft	Windows 2012 R2 Standard	Windows Server 2012 R2 Update (x64)
		Microsoft	SQL Server 2012	SQL Server 2012 Standard
		Redhat	Red Hat Enterprise Linux 6.7	Red Hat Enterprise Linux 6.7 (x64)

3. External Service Dependencies

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

3.1 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 3. 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 components within the management pod.

3.2 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 ESXi management network, vSphere vMotion, VXLAN (VTEP) and NFS.

Table 4. DHCP Requirements

Requirement	Description
DHCP server	The subnets and associated VLANs that provide IPv4 transport for the ESXi VMkernel ports in all pods must be configured for IPv4 address auto-assignment by using DHCP.

3.3 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 5. 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 *DNS Names* documentation.

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

3.4 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 6. 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.

3.5 SMTP Mail Relay

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

Table 7. 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.

3.6 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 8. 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.

3.7 FTP Server

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

Table 9. FTP Server Requirements

Requirement	Description
FTP server	Space for NSX Manager backups must be available on an FTP server. The server must support SFTP and FTP. The NSX Manager instances must have connection to the remote FTP server.

3.8 Windows Host Machine

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

Table 10. 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. For information about the Windows OS requirements for the host and the software downloads for this SDDC validated design, see *Software Requirements*.

4. Physical 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.

4.1 VLAN IDs and IP Subnets for System Traffic

This VMware Validated Design requires that the following VLAN IDs and IP subnets be allocated for the traffic types in the SDDC.

4.1.1 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 11. VLAN and IP Subnet Configuration in Region A

POD	VLAN Function	VLAN	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
	Virtual SAN	1613	172.16.13.0/24	172.16.13.253
	VXLAN (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
	Virtual SAN	1633	172.16.33.0/24	172.16.33.253
	VXLAN (VTEP)	1634	172.16.34.0/24	172.16.34.253
	NFS	1625	172.16.25.0/24	172.16.25.253
	External Tenant Connectivity	140	10.158.140.0/24	10.158.140.253

4.1.2 VLAN IDs and IP Subnets in Region B

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

Table 12. VLAN and IP Subnet Configuration in Region B

Region B	VLAN Function	VLAN	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
	Virtual SAN	1713	172.17.13.0/24	172.17.13.253
	VXLAN (VTEP)	1714	172.17.14.0/24	172.17.14.253
	NFS	1715	172.17.15.0/24	172.17.15.253
	vSphere Replication and 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
	Virtual SAN	1733	172.17.33.0/24	172.17.33.253
	VXLAN (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

4.2 Names and IP Subnets of Application Virtual Networks

This VMware Validated Design uses the following IP subnets in the application virtual networks for the management applications in the SDDC.

Table 13. Application Network Names and IP Subnets

Application Virtual Networks	Subnet Region A	Subnet 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

5. DNS Names

Before you deploy the SDDC by following this validated design, you must create a DNS configuration of fully qualified domain names (FQDNs) and map them to the IP addresses of the management application nodes.

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.

5.1 DNS Names and IP Addresses in Region A

In Region A of the SDDC, you must provide DNS names and IP addresses that are required for the SDDC deployment in the region.

5.1.1 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 14. Host Names and IP Addresses for the External Services in Region A

Component Group	DNS Name in Region A	IP Address in Region A	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 sub-domains

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

Allocate DNS names and IP addresses to ESXi hosts, vCenter Server instances and connected Platform Services Controller instances, and NSX components in Region A. For a dual-region SDDC, allocate also host names and IP addresses to the nodes that run Site Recovery Manager and vSphere Replication in the region.

Table 15. Host Name and IP addresses for the Virtual Infrastructure Components in Region A

Component Group	DNS Name in Region A	IP Address in Region A	Description
vSphere	mgmt01esx01.sfo01.rainpole.local	172.16.11.101	ESXi host in the management pod
	mgmt01esx02.sfo01.rainpole.local	172.16.11.102	ESXi host in the management pod
	mgmt01esx03.sfo01.rainpole.local	172.16.11.103	ESXi host in the management pod
	mgmt01esx04.sfo01.rainpole.local	172.16.11.104	ESXi host in the management pod
	comp01esx01.sfo01.rainpole.local	172.16.31.101	ESXi host in the shared edge and compute pod
	comp01esx02.sfo01.rainpole.local	172.16.31.102	ESXi host in the shared edge and compute pod
	comp01esx03.sfo01.rainpole.local	172.16.31.103	ESXi host in the shared edge and compute pod
	comp01esx04.sfo01.rainpole.local	172.16.31.104	ESXi host in the shared edge and compute pod
	mgmt01psc01.sfo01.rainpole.local	172.16.11.61	Platform Services Controller for the Management vCenter Server
	mgmt01vc01.sfo01.rainpole.local	172.16.11.62	Management vCenter Server
	comp01psc01.sfo01.rainpole.local	172.16.11.63	Platform Services Controller for the Compute vCenter Server
	comp01vc01.sfo01.rainpole.local	172.16.11.64	Compute vCenter Server
NSX for vSphere	mgmt01nsxm01.sfo01.rainpole.local	172.16.11.65	NSX Manager for the management cluster
	mgmt01nsxc01.sfo01.rainpole.local	172.16.11.118	Reserved.
	mgmt01nsxc02.sfo01.rainpole.local	172.16.11.119	NSX Controllers for the management cluster
	mgmt01nsxc03.sfo01.rainpole.local	172.16.11.120	
	comp01nsxm01.sfo01.rainpole.local	172.16.11.66	NSX Manager for the shared edge and compute cluster
	comp01nsxc01.sfo01.rainpole.local	172.16.31.118	Reserved
	comp01nsxc02.sfo01.rainpole.local	172.16.31.119	
	comp01nsxc03.sfo01.rainpole.local	172.16.31.120	NSX Controllers for the compute and edge clusters

Component Group	DNS Name in Region A	IP Address in Region A	Description
	SFOMGMT-ESG01	172.27.11.2 172.27.12.3 192.168.10.1	ECMP-enabled NSX Edge device for North-South management traffic
	SFOMGMT-ESG02	172.27.11.3 172.27.12.2 192.168.10.2	ECMP-enabled NSX Edge device for North-South management traffic
	UDLR01	192.168.10.3	Universal Distributed Logical Router (UDLR) for East-West management traffic.
	SFOCOMP-ESG01	172.16.35.2 172.27.13.3 192.168.100.1	ECMP-enabled NSX Edge device for North-South compute and edge traffic
	SFOCOMP-ESG02	172.16.35.3 172.27.13.2 192.168.100.2	ECMP-enabled NSX Edge device for North-South compute and edge traffic
	UDLR01	192.168.100.3	Universal Distributed Logical Router (UDLR) for East-West compute and edge traffic.
	SFOMGMT-LB01	192.168.11.2	NSX Edge device for load balancing management applications.
Site Recovery Manager	mgmt01srm01.sfo01.rainpole.local	172.16.11.124	Site Recovery Manager
vSphere Replication	mgmt01vrms01.sfo01.rainpole.local	172.16.11.123	vSphere Replication

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

Allocate DNS names and IP addresses to the vRealize Automation Appliance instances and IaaS nodes, Microsoft SQL Server, vRealize Orchestrator nodes and vRealize Business nodes in Region A.

Table 16. Host Name and IP address for the Cloud Management Components in Region A

Component Group	DNS Name in Region A	IP Address in Region A	Description
vRealize Automation	vra01svr01a.rainpole.local	192.168.11.51	vRealize Automation Appliance
	vra01svr01b.rainpole.local	192.168.11.52	vRealize Automation Appliance

Component Group	DNS Name in Region A	IP Address in Region A	Description
	vra01svr01.rainpole.local	192.168.11.53	VIP address of the vRealize Appliance
	vra01iws01a.rainpole.local	192.168.11.54	vRealize Automation IaaS Web Server
	vra01iws01b.rainpole.local	192.168.11.55	vRealize Automation IaaS Web Server
	vra01iws01.rainpole.local	192.168.11.56	VIP address of the vRealize Automation IaaS Web Server
	vra01ims01a.rainpole.local	192.168.11.57	vRealize Automation IaaS Manager Service & DEM Orchestrator
	vra01ims01b.rainpole.local	192.168.11.58	vRealize Automation IaaS Manager Service & DEM Orchestrator
	vra01ims01.rainpole.local	192.168.11.59	VIP address of the vRealize Automation IaaS Manager Service
	vra01dem01.rainpole.local	192.168.11.60	vRealize Automation IaaS DEM Worker
	vra01dem02.rainpole.local	192.168.11.61	vRealize Automation IaaS DEM Worker
Microsoft SQL Server	vra01mssql01.rainpole.local	192.168.11.62	Microsoft SQL Server
vRealize Orchestrator	vra01vro01a.rainpole.local	192.168.11.63	vRealize Orchestrator Appliance
	vra01vro01b.rainpole.local	192.168.11.64	vRealize Orchestrator Appliance
	vra01vro01.rainpole.local	192.168.11.65	VIP address of vRealize Orchestrator
vRealize Business	vra01bus01.rainpole.local	192.168.11.66	vRealize Business Server
vRealize Automation Proxy Agents	vra01ias01.sfo01.rainpole.local	192.168.31.52	vRealize Automation Proxy Agent
	vra01ias02 .sfo01.rainpole.local	192.168.31.53	vRealize Automation Proxy Agent
vRealize Business Remote Collectors	vra01buc01.sfo01.rainpole.local	192.168.31.54	vRealize Business Data Collector

5.1.4 Host Names and IP Addresses for the Business Continuity and Operations Management Components in Region A

Allocate DNS names and IP addresses to vSphere Data Protection, vRealize Operations Manager and vRealize Log Insight in Region A.

Table 17. Host Name and IP address for the Business Continuity and Operations Management Components in Region A

Component Group	DNS Name in Region A	IP Address in Region A	Description
vSphere Data Protection	mgmgt01vdp01.sfo01.rainpole.local	172.16.11.81	vSphere Data Protection primary appliance in the management pod
vRealize Operations Manager	vrops-cluster-01.rainpole.local	192.168.11.35	Virtual IP address of external load balancer for the analytics cluster of vRealize Operations Manager
	vrops-mstrn-01.rainpole.local	192.168.11.31	Master node of vRealize Operations Manager
	vrops-repln-02.rainpole.local	192.168.11.32	Master replica node of vRealize Operations Manager
	vrops-datan-03.rainpole.local	192.168.11.33	Data node 1 of vRealize Operations Manager
	vrops-datan-04.rainpole.local	192.168.11.34	Data node 02 of vRealize Operations Manager
	vrops-rmtcol-01.sfo01.rainpole.local	192.168.31.31	Remote collector 1 of vRealize Operations Manager
	vrops-rmtcol-02.sfo01.rainpole.local	192.168.31.32	Remote collector 2 of vRealize Operations Manager
vRealize Log Insight	vrli-cluster-01.sfo01.rainpole.local	192.168.31.10	VIP address of the integrated load balancer of vRealize Log Insight
	vrli-mstr-01.sfo01.rainpole.local	192.168.31.11	Master Node of vRealize Log Insight
	vrli-wrkr-01.sfo01.rainpole.local	192.168.31.12	Worker node 01 of vRealize Log Insight
	vrli-wrkr-02.sfo01.rainpole.local	192.168.31.13	Worker node 02 of vRealize Log Insight

5.2 DNS Names and IP Addresses in Region B

In dual-region SDDC deployment, you must also dedicate DNS names and IP addresses that are required for the SDDC management components in Region B.

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

Component Group	DNS Name in Region B	IP Address in Region B	Description
NTP	ntp.lax01.rainpole.local	172.17.11.251 172.17.11.252	NTP server selected via Round Robin NTP server on a ToR switch in the management pod
	0.ntp.lax01.rainpole.local	172.17.11.251	NTP server selected using Round Robin 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
	dc01lax.lax01.rainpole.local	172.17.11.5	Active Directory and DNS server for the sub-domains

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

Allocate DNS names and IP addresses to ESXi hosts, vCenter Server instances and connected Platform Services Controller instances, NSX components, Site Recovery Manager and vSphere Replication in Region B.

Table 19. Host Names and IP Addresses for the Virtual Infrastructure Components in Region B

Component Group	DNS Name in Region B	IP Address in Region B	Description
vSphere	mgmt01esx51.lax01.rainpole.local	172.17.11.101	ESXi host in the management pod
	mgmt01esx52.lax01.rainpole.local	172.17.11.102	ESXi host in the management pod
	mgmt01esx53.lax01.rainpole.local	172.17.11.103	ESXi host in the management pod
	mgmt01esx54.lax01.rainpole.local	172.17.11.104	ESXi host in the management pod

Component Group	DNS Name in Region B	IP Address in Region B	Description
	comp01esx51.lax01.rainpole.local	172.17.31.101	ESXi host in the shared edge and compute pod
	comp01esx52.lax01.rainpole.local	172.17.31.102	ESXi host in the shared edge and compute pod
	comp01esx53.lax01.rainpole.local	172.17.31.103	ESXi host in the shared edge and compute pod
	comp01esx54.lax01.rainpole.local	172.17.31.104	ESXi host in the shared edge and compute pod
	mgmt01psc51.lax01.rainpole.local	172.17.11.61	Platform Services Controller for the Management vCenter Server
	mgmt01vc51.lax01.rainpole.local	172.17.11.62	Management vCenter Server
	comp01psc51.lax01.rainpole.local	172.17.11.63	Platform Services Controller for the Compute vCenter Server
	comp01vc51.lax01.rainpole.local	172.17.11.64	Compute vCenter Server
NSX for vSphere	mgmt01nsxm51.lax01.rainpole.local	172.17.11.65	NSX Manager for the management cluster
	mgmt01nsxc51.lax01.rainpole.local mgmt01nsxc52.lax01.rainpole.local mgmt01nsxc53.lax01.rainpole.local	172.17.11.118 172.17.11.119 172.17.11.120	Reserved NSX Controllers for the management cluster
	comp01nsxm51.lax01.rainpole.local	172.17.11.66	NSX Manager for the shared edge and compute cluster
	comp01nsxc51.lax01.rainpole.local comp01nsxc52.lax01.rainpole.local comp01nsxc53.lax01.rainpole.local	172.17.31.118 172.17.31.119 172.17.31.120	Reserved. NSX Controllers for the shared edge and compute cluster
	LAXMGMT-ESG01	172.27.14.2 172.27.15.3 192.168.10.50	ECMP-enabled NSX Edge device for North-South management traffic
	LAXMGMT-ESG02	172.27.14.3 172.27.15.2 192.168.10.51	ECMP-enabled NSX Edge device for North-South management traffic
	LAXCOMP-ESG01	172.17.35.2 172.27.21.3 192.168.100.50	ECMP-enabled NSX Edge device for North-South compute and edge traffic

Component Group	DNS Name in Region B	IP Address in Region B	Description
	LAXCOMP-ESG02	172.17.35.3 172.27.21.2 192.168.100.51	ECMP-enabled NSX Edge device for North-South compute and edge traffic
	LAXMGMT-LB01	192.168.11.2	NSX Edge device for load balancing management applications.
Site Recovery Manager	mgmt01srm51.lax01.rainpole.local	172.17.11.124	Site Recovery Manager
vSphere Replication	mgmt01vrms51.lax01.rainpole.local	172.17.11.123	vSphere Replication

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

Allocate DNS names and IP addresses to the vSphere Proxy Agents for vRealize Automation and to the vRealize Business Data Collector in Region B.

Table 20. Host Names and IP Addresses for the Cloud Management Components in Region B

Component Group	DNS Name in Region B	IP Address in Region B	Description
vRealize Automation Proxy Agents	vra01ias51.lax01.rainpole.local	192.168.32.52	vRealize Automation Proxy Agent
	vra01ias52 .lax01.rainpole.local	192.168.32.53	vRealize Automation Proxy Agent
vRealize Business Data Collectors	vra01buc51.lax01.rainpole.local	192.168.32.54	vRealize Business Data Collector

5.2.4 Host Names and IP Addresses for the Business Continuity and Operations Management Components in Region B

Allocate DNS names and IP addresses to the vSphere Data Protection appliance, vRealize Operations Manager remote collectors and vRealize Log Insight nodes in Region B.

Table 21. Host Names and IP Addresses for the Business Continuity and Operations Management Components in Region B

Component Group	DNS Name in Region B	IP Address in Region B	Description
vSphere Data Protection	mgmgt01vdp51.lax01.rainpole.local	172.17.11.81	vSphere Data Protection primary appliance in the management pod
vRealize Operations Manager Remote Collectors	vrops-rmtcol-51.lax01.rainpole.local	192.168.32.31	Remote collector 1 of vRealize Operations Manager
	vrops-rmtcol-52.lax01.rainpole.local	192.168.32.32	Remote collector 2 of vRealize Operations Manager
vRealize Log Insight	vrli-cluster-51.lax01.rainpole.local	192.168.32.10	VIP address of the integrated load balancer of vRealize Log Insight
	vrli-mstr-51.lax01.rainpole.local	192.168.32.11	Master Node of vRealize Log Insight
	vrli-wrkr-51.lax01.rainpole.local	192.168.32.12	Worker node 01 of vRealize Log Insight
	vrli-wrkr-52.lax01.rainpole.local	192.168.31.13	Worker node 02 of vRealize Log Insight

6. 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.

6.1 Requirements for Time Synchronization

All management components need to be configured with NTP.

Apply the following approach to reduce the impact of time synchronization issues in the SDDC.

- 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.
- Configure a DNS CNAME that maps the two time sources to one DNS name.

Table 22. NTP Server FQDN and IP Configuration

NTP Server FQDN	Mapped IP Address	Region
ntp.sfo01.rainpole.local	172.16.11.251 172.16.11.252	Region A
ntp.lax01.rainpole.local	172.17.11.251 172.17.11.252	Region B
0.ntp.sfo01.rainpole.local	172.16.11.251	Region A
1.ntp.sfo01.rainpole.local	172.16.11.252	Region A
0.ntp.lax01.rainpole.local	172.17.11.251	Region B
1.ntp.lax01.rainpole.local	172.17.11.252	Region B

- 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`
- 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.

6.2 Configure NTP-Based Time Synchronization on Windows Hosts

On Windows, enable NTP-based synchronization.

1. Open the command prompt as Administrator.
2. Run the following console command to enable time synchronization with the NTP servers on the ToR switches.

```
w32tm /config /manualpeerlist:"ntp.sfo01.rainpole.local
ntp.lax01.rainpole.local" /syncfromflags:manual /reliable:YES /update
```

3. Restart the Windows Time service to apply the changes.

```
net stop w32time
net start w32time
```

4. Verify the time synchronization configuration.
   a. Run the following console.

```
w32tm /query /status
```

   b. Verify that the **ReferenceId**: attribute in the output contains one of these servers in each region: 172.16.11.251, 172.16.11.252, 172.17.11.251 or 172.16.17.252.
   c. If the `ReferenceId:` attribute contains `LOCL` instead of the IP address of at least one of the 4 NTP servers, run the following command and wait for the re-synchronization to complete.

```
w32tm /resync
```

   d. Query the status of the Windows Time service again:

```
w32tm /query /status
```

7. Active Directory Users and Groups

Before you deploy and configure the SDDC from this validated design, you must provide a specific configuration of Active Directory users and groups. 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.

7.1 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.

7.2 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.

7.3 Universal Groups in the Parent Domain

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

Table 23. 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-ITAC-TenantAdmins	Universal	Tenant administrators group
ug-ITAC-TenantArchitects	Universal	Tenant architects group
ug-vCAdmins	Universal	Read-only accounts for vCenter Server administrators for monitoring vCenter Server instances in vRealize Operations Manager
ug-vCenterAdmins	Universal	Group with accounts that are assigned vCenter Server administrator privileges.
ug-vROAdmins	Universal	Groups with vRealize Orchestrator Administrator privileges

7.4 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 24. Local 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
ITAC-TenantAdmins	Global	Tenant administrators group	RAINPOLE\ug-ITAC-TenantAdmins
ITAC-TenantArchitects	Global	Tenant architects group	RAINPOLE\ug-ITAC-TenantArchitects
vCAdmins	Global	Read-only group for monitoring vCenter Server instances in vRealize Operations Manager	RAINPOLE\ug-vCAdmins
vCenterAdmins	Global	Group with accounts that are assigned vCenter Server administrator privileges	RAINPOLE\ug-vCenterAdmins

7.5 Active Directory Users

7.5.1 Service Accounts

A service account provides components of the SDDC with non-interactive and non-human access to services and APIs. 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.

7.5.2 Service Accounts in the Parent Domain

Create the following service accounts in the parent Active Directory domain `rainpole.local` to provide centralized authentication of SDDC products.

Table 25. Service Accounts in the rainpole.local Parent Domain

User Name	Description	Service Account	Member of Groups
svc-loginsight	Read-only service account for using the Active Directory as an authentication source in vRealize Log Insight and for forwarding log information from vCenter Server and ESXi to vRealize Log Insight.	Yes	
svc-vrops	Read-only service account for access to the Management vCenter Server and Compute vCenter Server from vRealize Operations Manager.	Yes	RAINPOLE\ug-vCAdmins
svc-mpsd-vrops	Service account for storage device monitoring of the Management vCenter Server and Compute vCenter Server from vRealize Operations Manager. In vSphere, this account is assigned a custom user role whose privileges comply with the requirements to access data about storage devices.	Yes	RAINPOLE\ug-vCAdmins
svc-vra	Service account for using Active Directory as an authentication source and for accessing the nodes of vRealize Automation. This service account is used as a Windows service to run the management agents and IaaS Components for the vRealize Automation Infrastructure.	Yes	RAINPOLE\ug-vCenterAdmins RAINPOLE\ug-vROAdmins
svc-vro	Service account for accessing the nodes of vRealize Orchestrator.	Yes	
svc-nsxmanager	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 edge and compute cluster.	Yes	RAINPOLE\ug-vCenterAdmins

7.5.3 User Accounts in the Parent Domain

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

Table 26. User Accounts in the rainpole.local Parent Domain

User Name	Description	Service Account	Member of Groups

ITAC-TenantAdmin	Tenant administrator role in the SDDC for configuring vRealize Automation for the needs of your organization including user and group management, tenant branding and notifications, and business policies.	No	RAINPOLE\ug-ITAC-TenantAdmins RAINPOLE\ug-vROAdmins
ITAC-TenantArchitect	Tenant architect role in the SDDC for creating the blueprints that tenants request from the service catalog.	No	RAINPOLE\ug-ITAC-TenantArchitects

7.5.4 Users Accounts 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 27. 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
vROPS-Admin	Administrator account for vRealize Operations Manager.	No	RAINPOLE\ug-SDDC-Admins RAINPOLE\ug-SDDC-Ops

8. Datastore Requirements

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

8.1 NFS Exports for Management Components

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

Table 28. NFS Export Configuration

VLAN	Server	Export	Size	Map As	Region	Cluster	Component
1615	172.16.15.251	/V2D_vRLI_MgmtA_1TB	1TB	NFS datastore for log archiving in vRealize Log Insight	Region A	Management cluster	vRealize Log Insight
1615	172.16.15.251	/V2D_vDP_MgmtA_4TB	4TB	SFO01A-NFS01-VDP01	Region A	Management cluster	vSphere Data Protection
1625	172.16.25.251	/V2D_vRA_ComputeA_1TB	1TB	SFO01A-NFS01-VRALIB01	Region A	Shared edge and compute cluster	vRealize Automation
1715	172.17.15.251	/V2D_vRLI_MgmtB_1TB	1TB	NFS mount for log archiving in vRealize Log Insight	Region B	Management cluster	vRealize Log Insight
1715	172.17.15.251	/V2D_vDP_MgmtB_4TB	4TB	LAX01A-NFS01-VDP01	Region B	Management cluster	vSphere Data Protection
1725	172.17.25.251	/V2D_vRA_ComputeB_1TB	1TB	LAX01A-NFS01-VRALIB01	Region B	Shared edge and compute cluster	vRealize Automation

8.2 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 Reference Architecture* Guide.

9. Virtual Machine Template Specifications

This validated design uses a set of virtual machines according to predefined specifications to create tenant blueprint in vRealize Automation. Create virtual machine templates according to these specifications.

Table 29. Specifications for the VM Templates Required in the VMware Validated Design

SDDC Layer	Required by VMware Component	VM Template Name	Guest OS	CPUs	Memory GB	Virtual Disk, GB	SCSI Controller	Virtual Machine Network Adapter
Cloud Management	vRealize Automation	redhat6-enterprise-64	Red Hat Enterprise Server 6.7(64-bit)	1	6	20	LSI Logic SAS	VMXNET3
		windows-2012r2-64	Windows Server 2012 R2 (64-bit)	1	4	50	LSI Logic SAS	VMXNET3
		windows-2012r2-64-sql2012	Windows Server 2012 R2 (64-bit)	1	8	100	LSI Logic SAS	VMXNET3