Planning and Preparation

VMware Validated Design 4.0
VMware Validated Design for Software-Defined Data Center 4.0

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Copyright © 2016–2017 VMware, Inc. All rights reserved. Copyright and trademark information.

Contents

About VMware Validated Design Planning and Preparation

VMware Validated Design Planning and Preparation 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 this VMware Validated Design, you must set up an environment that has a specific compute, storage and network configuration, and that provides services to the components of the SDDC. Review carefully the *VMware Validated Design Planning and Preparation* documentation at least 2 weeks ahead of deployment to avoid costly re-work and delays.

Intended Audience

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

Required VMware Software

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

Updated Information

This *VMware Validated Design Planning and Preparation* documentation is updated with each release of the product or when necessary.

This table provides the update history of the *VMware Validated Design Planning and Preparation* documentation.

Revision	Description
EN-002463-01	The fully qualified domain name (FQDN) of the Platform Services Controller load balancer in Region B is updated to `LAX01PSC51` in the following documentation: ■ Host names in Table 2-14 ■ Service accounts diagram Figure 2-1 ■ Configuration text file `lax01psc51.lax01.txt` for configuring Platform Services Controller certificate generation in the Certificate Generation Utility. See Use the Certificate Generation Utility to Generate CA-Signed Certificates for the SDDC Management Components.
EN-002463-00	Initial release.

Software Requirements

1

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.

This chapter includes the following topics:

- VMware Scripts and Tools
- Third-Party Software

VMware Scripts and Tools

Download the following scripts and tools that this VMware Validated Design uses for 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.
Business Continuity	VMware Site Recovery Manager	Microsoft	Windows 2012 R2 Standard	Windows Server 2012 R2 Update (64-bit)
Operations Management	Update Manager Download Service (UMDS)	Ubuntu	Ubuntu Server 14.04	Ubuntu Server 14.04 LTS
		PostgreSQL	PostgreSQL	9.3
		Nginx	Nginx	1.4
Cloud Management	vRealize Automation	Microsoft	Windows 2012 R2 Standard	Windows Server 2012 R2 Update (64-bit)
		Microsoft	SQL Server 2012	SQL Server 2012 Standard edition
		Redhat	Red Hat Enterprise Linux 6.7	Red Hat Enterprise Linux 6.7 (64-bit)

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 for Consolidated SDDC

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

Active Directory

This validated design uses Microsoft Active Directory (AD) for authentication and authorization to resources within the rainpole.local domain.

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.
	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.

Table 2-1. Requirements for the Active Directory Service (Continued)

Requirement	Domain Instance	Domain Name	Description
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 the VXLAN (VTEP) VMkernel ports must be configured for IPv4 address auto-assignment by using DHCP.

DNS

For a single-region deployment that you can scale out to a dual-region deployment, you must provide root and child domain 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	Resides in the sfo01.rainpole.local domain. Configure 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 that are listed in the DNS Names and IP Addresses in Region A documentation.

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

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 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.

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 or 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.

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 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.

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 2-9. 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
	vSAN	1633	172.16.33.0/24	172.16.33.253
	VXLAN (NSX VTEP)	1634	172.16.34.0/24	172.16.34.253

Table 2-9. VLAN and IP Subnet Configuration in Region A (Continued)

Pod in Region A	VLAN Function	VLAN ID	Subnet	Gateway
	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 2-10. 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 These VLAN IDs and IP subnets are examples. The actual implementation depends on 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 2-11. 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.

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.

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.

- 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.

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

  Allocate DNS names and IP addresses to the vSphere, NSX and disaster recovery components in Region A.

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

  Allocate DNS names and IP addresses before you deploy the cloud management components of the SDDC according to this VMware Validated Design.

- Host Names and IP Addresses for the Data Protection and Operations Management Components in Region A

  Allocate DNS names and IP addresses to vSphere Data Protection appliance, vRealize Operations Manager and vRealize Log Insight nodes, and vSphere Update Manager Download Service in Region A before you deploy these SDDC management applications.

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.

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.

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

Allocate DNS names and IP addresses to the vSphere, NSX and disaster recovery components in Region A.

In Region A, allocate addresses to the ESXi hosts, vCenter Server and Platform Services Controller instances, and NSX nodes for either a single-region or dual-region environment.

Table 2-12. Host Names 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

Table 2-12. Host Names and IP Addresses for the Virtual Infrastructure Components in Region A (Continued)

Component Group	DNS Name in Region A	IP Address in Region A	Description
	mgmt01nsxc01.sfo01.rainpole.local	172.16.11.118	Reserved. NSX Controllers for the management cluster
	mgmt01nsxc02.sfo01.rainpole.local	172.16.11.119	
	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. NSX Controllers for the shared edge and compute cluster
	comp01nsxc02.sfo01.rainpole.local	172.16.31.119	
	comp01nsxc03.sfo01.rainpole.local	172.16.31.120	
	SFO01PSC01	172.16.11.71	NSX Edge device for load balancing the Platform Services Controllers.
	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
	SFOMGMT-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 ■ 192.168.101.1	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 ■ 192.168.101.2	ECMP-enabled NSX Edge device for North-South compute and edge traffic
	SFOCOMP-UDLR01	192.168.100.3	Universal Distributed Logical Router (UDLR) for East-West compute and edge traffic
	SFOCOMP-DLR01	192.168.101.3	Distributed Logical Router (DLR) for East-West compute and edge traffic.
	SFOMGMT-LB01	192.168.11.2	NSX Edge device for load balancing management applications

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 2-13. Host Names and IP Addresses for Disaster Recovery Applications in Region A

Component Group	DNS Name in Region A	IP Address in Region A	Description
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

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

Allocate DNS names and IP addresses before you deploy the cloud management components of the SDDC according to this VMware Validated Design.

For the Cloud Management Platform, this design uses specific IP addresses and DNS names to the following nodes in Region A:

- vRealize Automation Appliance instances, IaaS nodes, Proxy Agents and Microsoft SQL Server
- vRealize Orchestrator nodes
- vRealize Business nodes

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
	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

Component Group	DNS Name in Region A	IP Address in Region A	Description
	vra01ias02.sfo01.rainpole.local	192.168.31.53	vRealize Automation Proxy Agent
vRealize Business Data Collectors	vra01buc01.sfo01.rainpole.local	192.168.31.54	vRealize Business Data Collector

Host Names and IP Addresses for the Data Protection and Operations Management Components in Region A

Allocate DNS names and IP addresses to vSphere Data Protection appliance, vRealize Operations Manager and vRealize Log Insight nodes, and vSphere Update Manager Download Service in Region A before you deploy these SDDC management applications.

Component Group	DNS Name in Region A	IP Address in Region A	Description
vSphere Data Protection	mgmt01vdp01.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	VIP address of 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-0x.rainpole.local	192.168.11.34	Additional data node of Operations Manager (scaling out)
	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
vSphere Update Manager	mgmt01umds01.sfo01.rainpole.local	192.168.31.67	vSphere Update Manager Download Service (UMDS)
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 1 of vRealize Log Insight
	vrli-wrkr-02.sfo01.rainpole.local	192.168.31.13	Worker node 2 of vRealize Log Insight

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.

- 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.
- 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.
- 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.
- Host Names and IP Addresses for Data Protection and Operations Management Components in Region B

  Allocate DNS names and IP addresses to the vSphere Data Protection appliance, vRealize Operations Manager remote collectors, vRealize Log Insight nodes, and vSphere Update Manager Download Service in Region B before you deploy these SDDC management applications.

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.

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 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 sub-domains.

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 2-14. 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
	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	172.17.11.118	Reserved. NSX Controllers for the management cluster
	mgmt01nsxc52.lax01.rainpole.local	172.17.11.119	
	mgmt01nsxc53.lax01.rainpole.local	172.17.11.120	
	comp01nsxm51.lax01.rainpole.local	172.17.11.66	NSX Manager for the shared edge and compute cluster
	comp01nsxc51.lax01.rainpole.local	172.17.31.118	Reserved. NSX Controllers for the shared edge and compute cluster
	comp01nsxc52.lax01.rainpole.local	172.17.31.119	
	comp01nsxc53.lax01.rainpole.local	172.17.31.120	
	LAX01PSC51	172.17.11.71	NSX Edge device for load balancing the Platform Services Controllers.
	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

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

Component Group	DNS Name in Region B	IP Address in Region B	Description
	LAXCOMP-ESG01	■ 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
	LAXCOMP-ESG02	■ 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
	LAXCOMP-DLR01	192.168.102.3	Distributed Logical Router (DLR) for East-West compute and edge traffic.
	LAXMGMT-LB01	192.168.11.2	NSX Edge device for load balancing management applications

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 2-15. Host Names and IP Addresses for Disaster Recovery Applications in Region B

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

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.

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

Host Names and IP Addresses for Data Protection and Operations Management Components in Region B

Allocate DNS names and IP addresses to the vSphere Data Protection appliance, vRealize Operations Manager remote collectors, vRealize Log Insight nodes, and vSphere Update Manager Download Service in Region B before you deploy these SDDC management applications.

Component Group	DNS Name in Region B	IP Address in Region B	Description
vSphere Data Protection	mgmt01vdp51.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
vSphere Update Manager	mgmt01umds51.lax01.rainpole.local	192.168.32.67	vSphere Update Manager Download Service (UMDS)
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 1 of vRealize Log Insight
	vrli-wrkr-52.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 2-16. 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 2-17. 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 2-18. 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 blueprint architects group
ug-vCenterAdmins	Universal	Group with accounts that are assigned vCenter Server administrator privileges.
ug-vROAdmins	Universal	Groups with vRealize Orchestrator 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 2-19. 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
ITAC-TenantAdmins	Global	Tenant administrators group	RAINPOLE\ug-ITAC-TenantAdmins
ITAC-TenantArchitects	Global	Tenant blueprint architects group	RAINPOLE\ug-ITAC-TenantArchitects
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.

Figure 2-1. Service Accounts in VMware Validated Design for Software-Defined Data Center

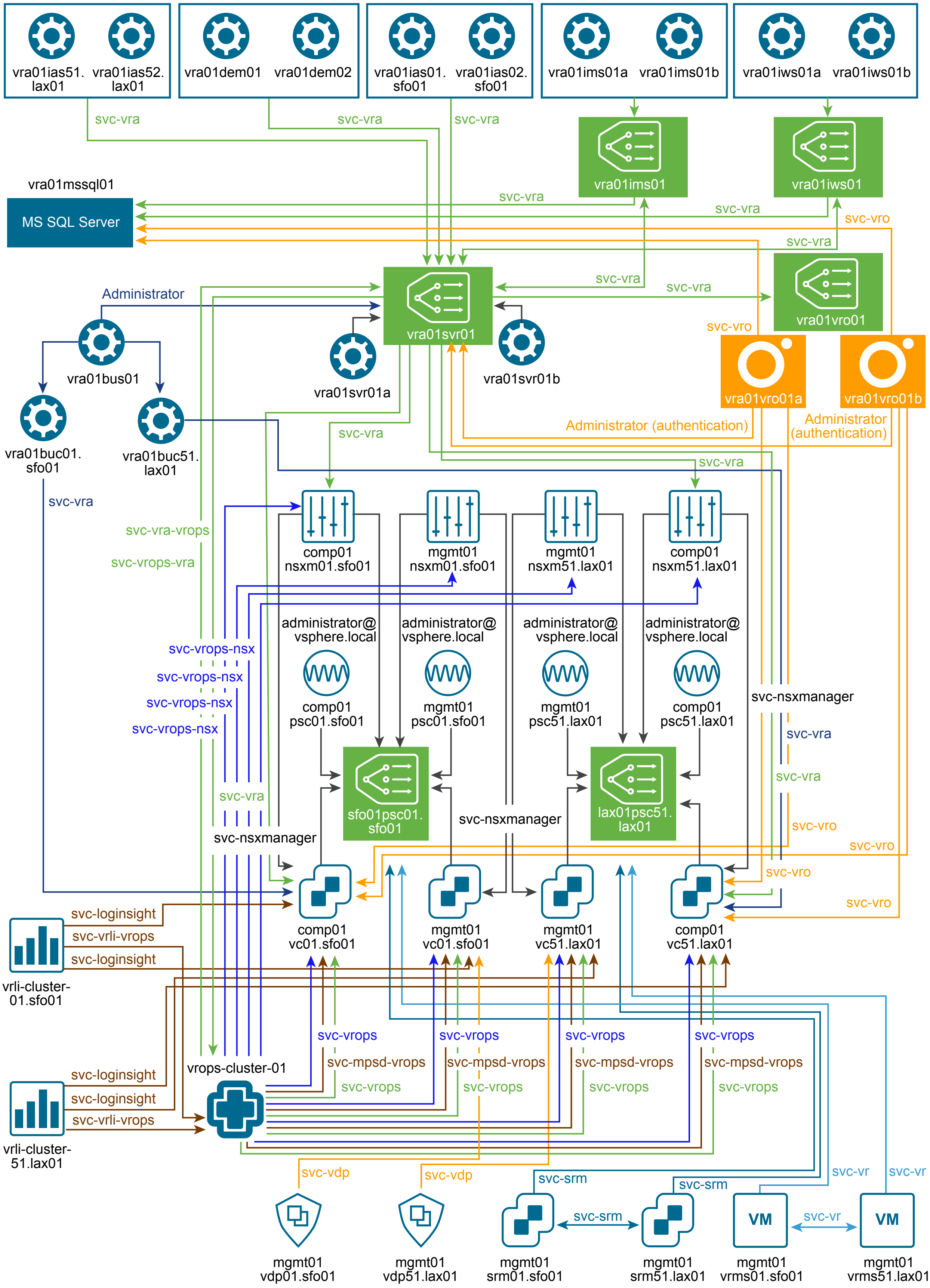


Table 2-20. Application-to-Application or Application Service Accounts in the VMware Validated Design

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-loginsight	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
svc-vdp	vSphere Data Protection	vCenter Server	Service account for registering vSphere Data Protection with vCenter Server for the management cluster	vSphere Data Protection User
svc-srm	Site Recovery Manager	vCenter Server	Service account for connecting Site Recover Manager to vCenter Server and to pair sites in Site Recovery Manager	Single Sign-On Administrator
svc-vr	vSphere Replication	vCenter Server	Service account for connecting vSphere Replication to vCenter Server and to pair vSphere Replication instances	Single Sign-On Administrator
svc-vra	vRealize Automation	■ vCenter Server ■ vRealize Automation	Service account for access from vRealize Automation to vCenter Server. This account is a part of the vRealize Automation setup process.	Administrator
svc-vro	vRealize Orchestrator	vCenter Server	Service account for access from vRealize Orchestrator to vCenter Server	Administrator
svc-vrops	vRealize Operation Manager Management Packs: vSphere, NSX-vSphere	vCenter Server	Service account for connecting vRealize Operations Manager to the Management vCenter Server and Compute vCenter Server	Read-Only
svc-mpsd-vrops	vRealize Operations Manager Management Pack: MPSD	vCenter Server	Service account for storage device monitoring of the Management vCenter Server and Compute vCenter Server from vRealize Operations Manager	MPSD Metrics User

Table 2-20. Application-to-Application or Application Service Accounts in the VMware Validated Design (Continued)

Username	Source	Destination	Description	Required Role
svc-vrops-nsx	vRealize Operations Manager Management Pack: NSX-vSphere	NSX for vSphere	Local service account for connecting the NSX for vSphere adapter for vRealize Operations Manager to the Management and Compute NSX Managers	Enterprise Administrator
svc-vrops-vra	vRealize Operations Manager Management Pack: vRA	vRealize Automation	Service account for connecting the vRealize Automation adapter for vRealize Operations Manager to vRealize Automation	■ Tenant administrator ■ IaaS administrator ■ Fabric administrator ■ Software Architect
svc-vrli-vrops	vRealize Log Insight	vRealize Operations Manager	Service account for connecting vRealize Log Insight to vRealize Operations Manager for log forwarding, and for alerts and Launch in Context integration	Administrator
svc-vra-vrops	vRealize Automation	vRealize Operations Manager	Service account for integration of health statistics from vRealize Operations Manager in the vRealize Automation portal	Read-Only
svc-umds	vSphere Update Manager Download Service	--	Local service account for configuring the Update Manager Download Service on the host virtual machine	Administrator

User Accounts in the Parent Domain

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

Table 2-21. 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 according to 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 blueprint architect role in the SDDC for creating the blueprints that tenants request from the service catalog.	No	RAINPOLE\ug-ITAC-TenantArchitects

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 2-22. 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.

- The first step is setting up a Microsoft Certificate Authority template through a Remote Desktop Protocol session.
- After you have created the new template, you add it 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 The 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.

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. Click 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.sfo01.txt` or `lax01psc51.lax01.txt` does not exist, make a copy of `mgmt01vc01.sfo01.txt` and save it as `sfo01psc01.sfo01.txt` or `lax01psc51.lax01.txt`.

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

sfo01psc01.sfo01.txt	lax01psc51.lax01.txt

`[CERT]`
`NAME=default`
`ORG=default`
`OU=default`
`LOC=SFO`
`ST=default`
`CC=default`
`CN=sfo01psc01.sfo01.rainpole.local`
`keysize=default`
`[SAN]`
`comp01psc01`
`mgmt01psc01`
`comp01psc01.sfo01.rainpole.local`
`mgmt01psc01.sfo01.rainpole.local`
`sfo01psc01`
`sfo01psc01.sfo01.rainpole.local`
	`[CERT]`
	`NAME=default`
	`ORG=default`
	`OU=default`
	`LOC=LAX`
	`ST=default`
	`CC=default`
	`CN=lax01psc51.lax01.rainpole.local`
	`keysize=default`
	`[SAN]`
	`comp01psc51`
	`mgmt01psc51`
	`comp01psc51.lax01.rainpole.local`
	`mgmt01psc51.lax01.rainpole.local`
	`lax01psc51`
	`lax01psc51.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 2.1 of the Certificate Generation Utility.

```
cd c:\CertGenVVD-2.1
```

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-2.1.ps1 -validate
```

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

```
.\CertGenVVD-2.1.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.

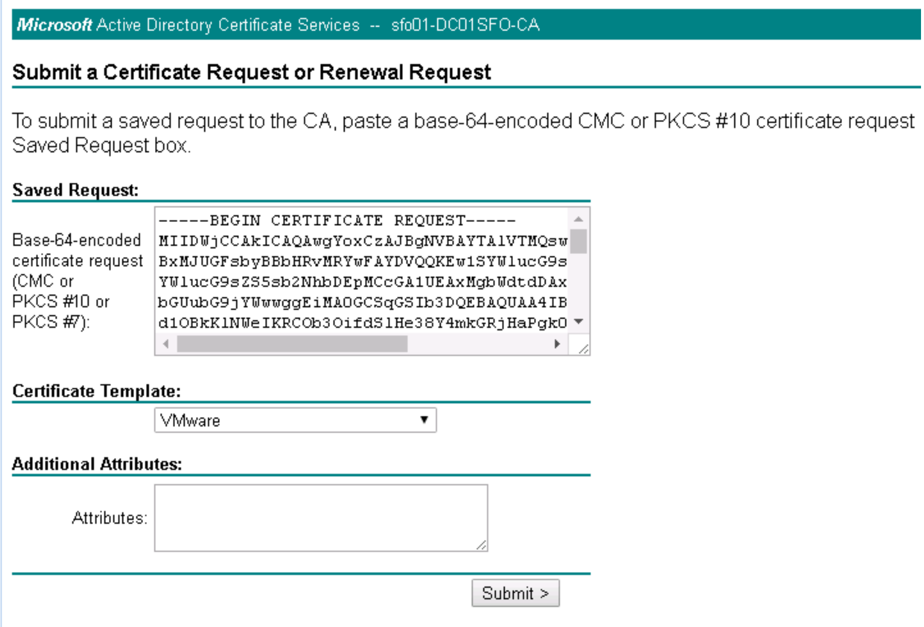
Procedure

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**.



Microsoft Active Directory Certificate Services -- sfo01-DC01SFO-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request
Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDWjCCAkICAQAwgYoxCzAJBgNVBAYTAlVTMQsw
BxMJUGFsbyBBbHRvMRYwFAYDVQQKEw1SYWlucG9s
YWlucG9sZS5sb2NhbDEpMCcGA1UEAxMgbWdtdDAx
bGUubG9jYWwwggEiMA0GCSqGSIb3DQEBAQUAA4IB
d1OBkKlNWeIKRCOb3OifdSlHe38Y4mkGRjHaPgkO
```

Certificate Template:

VMware ▼

Additional Attributes:

Attributes:

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 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.

NFS Exports for Management Components

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

Table 2-23. NFS Export Configuration

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

Customer-Specific Datastore for the Shared Edge and Compute Clusters

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

Virtual Machine Specifications 3

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

Management Virtual Machine Specifications

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

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

Table 3‑1. Specifications of Management Virtual Machines

Attribute	Region	Site Recovery Manager	vSphere Update Manager Download Service
Number of virtual machines	-	2 1 virtual machine in each region	2 1 virtual machine in each region
Guest OS	-	Windows Server 2012 R2 (64-bit)	Ubuntu Server 14.04 LTS
VM name	Region A	mgmt01srm01	mgmt01umds01.sfo01.rainpole.local
	Region B	mgmt01srm51	mgmt01umds51.lax01.rainpole.local
VM folder	Region A	BCDR01	MGMT01
	Region B	BCDR51	MGMT51
Cluster	Region A	SFO01-MGMT01	SFO01-MGMT01
	Region B	LAX01-MGMT01	LAX01-MGMT01
Datastore	Region A	SFO01A-VSAN01-MGMT01	SFO01A-VSAN01-MGMT01
	Region B	LAX01A-VSAN01-MGMT01	LAX01A-VSAN01-MGMT01
Number of CPUs	-	2	2
Memory (GB)	-	4	2
Disk space (GB)	-	40	120
SCSI Controller	-	LSI Logic SAS	LSI Logic SAS

Table 3-1. Specifications of Management Virtual Machines (Continued)

Attribute	Region	Site Recovery Manager	vSphere Update Manager Download Service
Virtual machine network adapter	-	VMXNET3	VMXNET3
Virtual machine network	Region A	vDS-Mgmt-Management	Mgmt-RegionA01-VXLAN
	Region B	vDS-Mgmt-Management	Mgmt-RegionB01-VXLAN
User account	-	Windows administrator	service-umds

Specifications for Tenant Blueprints

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

Table 3-2. Specifications for the VM Blueprint Templates

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